UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO DE ASSIS PAULO LIMA

NÚMEROS PRIMOS: FUNDAMENTOS, PROPRIEDADES E POTENCIAL DIDÁTICO

FORTALEZA
2025

FRANCISCO DE ASSIS PAULO LIMA

NÚMEROS PRIMOS: FUNDAMENTOS, PROPRIEDADES E POTENCIAL DIDÁTICO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática na Educação Básica.

Orientador: Prof. Dr. Marcelo Ferreira de Melo.

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

L698n Lima, Francisco de Assis Paulo.
Números primos : fundamentos, propriedades e potencial didático / Francisco de Assis Paulo Lima. – 2025.
83 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2025.
Orientação: Prof. Dr. Marcelo Ferreira de Melo.

1. Teoria dos números. 2. Números primos. 3. Matemática - Estudo e ensino. 4. Sequência didática. 5. Matemática - História. I. Título.

CDD 510

FRANCISCO DE ASSIS PAULO LIMA

NÚMEROS PRIMOS: FUNDAMENTOS, PROPRIEDADES E POTENCIAL DIDÁTICO

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Centro de Ciências da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática na Educação Básica.

Aprovada em: 18/07/2025.

BANCA EXAMINADORA

_____
Prof. Dr. Marcelo Ferreira de Melo (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Antonio Caminha Muniz Neto
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Flávio Alexandre Falcão Nascimento
Universidade Estadual do Ceará (UECE)

À minha esposa Natália, pelo amor, paciência e companheirismo. Seu apoio foi fundamental em cada etapa desta caminhada. Aos meus filhos Albert e Lara, fontes constantes de inspiração, alegria e motivação.

AGRADECIMENTOS

Ao acaso, por cada dia e por cada encontro que me trouxe até aqui.

À minha mãe Francisca (*in memoriam*), cuja presença continua viva em mim. Sou grato pelos ensinamentos, pela força e pelo amor que seguem me guiando, mesmo na ausência.

Aos meus familiares, que sempre me apoiaram e torceram por minhas conquistas.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) – Código de Financiamento 001.

Ao Prof. Dr. Marcelo Ferreira de Melo, pelo percurso trilhado desde a escolha do tema. Sou grato pela orientação generosa e pela disponibilidade ao longo do trabalho.

Aos professores e colegas da turma do mestrado, em especial ao amigo Thyago, cuja leveza e bom humor foram fundamentais nos momentos difíceis do curso.

E ao colega Túlio, meu sincero agradecimento pelos resumos maravilhosos, que tanto me ajudaram.

Enfim, a todos os amigos da turma do PROFMAT 2023, que compartilharam comigo o processo de um trabalho árduo e desafiador: Meu muito obrigado!

“Ninguém ignora tudo. Ninguém sabe tudo. Todos nós sabemos alguma coisa. Todos nós ignoramos alguma coisa. Por isso aprendemos sempre” (Freire, 1982 p. 52).

RESUMO

Esta dissertação realiza um estudo abrangente sobre os números primos, unindo sua base teórica e histórica com a prática pedagógica no ensino básico. O objetivo central do trabalho é desenvolver uma abordagem de ensino que supere a memorização, investigando o potencial do tema para promover uma aprendizagem mais contextualizada. A pesquisa inicia com a história da Teoria dos Números, traçando a evolução do conceito de número primo desde os pitagóricos e a formalização rigorosa de Euclides, até o seu renascimento no século XVII, por meio dos trabalhos de Fermat e Mersenne. A base matemática foi construída em capítulos dedicados aos fundamentos da divisibilidade. O estudo aprofunda-se em propriedades essenciais, como o Teorema Fundamental da Aritmética (TFA), que garante a decomposição única de um número em fatores primos, a clássica demonstração da infinitude dos primos, o método do Crivo de Eratóstenes e o Pequeno Teorema de Fermat. Para ilustrar a pesquisa viva da área, são apresentadas conjecturas famosas e ainda não resolvidas, como a de Goldbach e a dos primos gêmeos. A dissertação volta-se para o cenário educacional brasileiro, analisando a presença do tema na Base Nacional Comum Curricular (BNCC) e discutindo as dificuldades recorrentes no ensino e na aprendizagem. Uma análise de livros didáticos revela que, embora sigam uma estrutura lógica, frequentemente perdem a oportunidade de conectar o conteúdo às suas aplicações modernas e à sua beleza intrínseca. Como principal contribuição, o trabalho apresenta um produto educacional, uma sequência didática detalhada, com cinco aulas. A proposta utiliza estratégias investigativas, como a construção do Crivo de Eratóstenes, a exploração da prova da infinitude dos primos e a discussão de conjecturas, buscando despertar a curiosidade e desenvolver o pensamento crítico dos estudantes.

Palavras–chave: números primos; matemática - estudo e ensino; teoria dos números; sequência didática; matemática - história.

ABSTRACT

This report conducts a comprehensive study on prime numbers, linking its theoretical and historical bases with pedagogical practice in basic education. The central purpose of the work is to develop a teaching approach that goes beyond rote memorization, investigating the subject's potential to promote a more contextualized learning experience. The research begins with the history of Number Theory, tracing the evolution of the concept of a prime from the Pythagoreans and the rigorous formalization of Euclid, up to its renaissance in the 17th century through the works of Fermat and Mersenne. The mathematical foundation is built in chapters dedicated to the fundamentals of divisibility. The study delves into essential properties, such as the Fundamental Theorem of Arithmetic (FTA), which guarantees the unique decomposition of a number into prime factors, the classic proof of the infinitude of primes, the Sieve of Eratosthenes method, and Fermat's Little Theorem. To illustrate this living area of research, famous and still unsolved conjectures are presented, such as Goldbach's and the twin primes.
The dissertation then shifts its focus to the Brazilian educational scenario, analyzing the subject's inclusion in the Common National Curricular Basis (BNCC) and discussing the recurrent difficulties in teaching and learning. An analysis of textbooks reveals that, although they follow a logical structure, they frequently miss the opportunity to connect the content to its modern applications and its intrinsic beauty. As its main contribution, the work presents an educational product: a detailed didactic sequence with five lessons. The proposal uses investigative strategies, such as the construction of the sieve of Eratosthenes, the exploration of the proof of the infinitude of primes, and the discussion of conjectures, aiming to spark curiosity and develop students' critical thinking.

Keywords: prime numbers; mathematics-study and teaching; number theory; didactic sequence; history-mathematics.

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
LDB	Lei de Diretrizes e Bases da Educação Nacional
MDC	Máximo Divisor Comum
MMC	Mínimo Múltiplo Comum
MEC	Ministério da Educação
OBMEP	Olimpíada Brasileira de Matemática das Escolas Públicas
PROFMAT	Programa de Pós-Graduação em Matemática em Rede Nacional
PISA	Programme for International Student Assessment
RSA	Rivest-Shamir-Adleman
TFA	Teorema Fundamental da Aritmética
UFC	Universidade Federal do Ceará

LISTA DE SÍMBOLOS

$\mathbb{Z}$ Conjunto dos números inteiros

$\mathbb{N}$ Conjunto dos números naturais

SUMÁRIO

1 INTRODUÇÃO

O Ensino da Matemática nas escolas brasileiras sempre enfrentou um grande obstáculo: a fama de ser uma disciplina abstrata e desconectada da vida real. Muitos alunos olham para ela e só veem uma enxurrada de cálculos repetitivos ou fórmulas para decorar, o que acaba tirando qualquer vontade de aprender de verdade. É aí que entra a ideia de contextualizar, trazer a Matemática para perto do dia a dia dos estudantes, mostrando que ela faz sentido e pode até ser interessante.

A urgência de transformar essa realidade fica evidente nos dados do PISA 2022, que revelaram um cenário preocupante (Brasil, 2023).

> De acordo com os resultados do PISA 2022, o Brasil obteve uma média de 379 pontos em matemática, ficando abaixo de países latino-americanos como Chile, Uruguai e Peru. Além disso, 73% dos estudantes brasileiros ficaram abaixo do nível 2**,** considerado o patamar mínimo de proficiência pela OCDE. Apenas 1% dos alunos alcançou alto desempenho na área. Esses dados revelam a urgência de repensar o ensino da matemática no país, especialmente no que diz respeito à motivação e ao engajamento dos estudantes (Brasil, 2023).

A Base Nacional Comum Curricular (BNCC) deixa bem claro que a Matemática precisa fazer sentido na vida dos alunos, sendo apresentada de forma que se conecte com o dia a dia deles. O documento reforça que esse contexto é essencial para que o aprendizado ganhe vida e faz questão de valorizar o papel ativo do estudante, colocando-o como o verdadeiro protagonista da sua própria jornada de descoberta (Brasil, 2018). Com este propósito foi pensada esta dissertação.

Na teoria dos números, os números primos ocupam uma posição muito importante, despertando curiosidade e admiração ao longo da história da Matemática. Apesar de sua definição ser simples, a distribuição e as características desses números revelam uma complexidade que vem admirando pesquisadores por milênios.

Desde as primeiras civilizações que registraram a Matemática até as aplicações atuais sofisticadas, os números primos têm desafiado pesquisadores ao longo das gerações, tanto em suas propriedades teóricas quanto em suas aplicações práticas.

Embora seja essencial, o ensino de números primos na educação básica geralmente encontra obstáculos. Frequentemente, o assunto é abordado de maneira mecânica e desconectado de seu contexto histórico rico e de seus problemas fascinantes, o que pode resultar em uma aprendizagem superficial por parte dos estudantes.

Nesse contexto, o objetivo principal desta dissertação é examinar os princípios e as características dos números primos, avaliando seu potencial didático para o ensino de

Matemática no Ensino Fundamental e, possivelmente, do Médio. Os objetivos específicos que orientam este estudo são:

- ✓ Expor a evolução histórica do estudo dos números primos, desde a Antiguidade Clássica até a atualidade.
- ✓ Definir os princípios básicos da teoria da divisibilidade, incluindo o algoritmo de divisão e a determinação do Máximo Divisor Comum (MDC) e do Mínimo Múltiplo Comum (MMC).
- ✓ Explicar os conceitos e características fundamentais dos números primos, abrangendo o Teorema Fundamental da Aritmética (TFA), a demonstração da infinitude dos números primos e o pequeno teorema de Fermat.
- ✓ Examinar a abordagem do tema nas diretrizes curriculares brasileiras, os desafios no processo de ensino-aprendizagem e a maneira como os livros didáticos expõem o conteúdo.
- ✓ Criar e aplicar um recurso educacional, na forma de uma sequência didática, que aproveite o potencial do assunto em sala de aula, em conformidade com as competências da BNCC.

A justificativa para esta pesquisa é a necessidade de criar conexões entre a Matemática acadêmica e a Matemática escolar, demonstrando que um tópico clássico como os números primos pode ser abordado de forma investigativa, contextualizada e estimulante.

Ao explorar a história, os teoremas e as conjecturas que envolvem esses números, pretende-se fornecer aos educadores recursos para transformar um conteúdo curricular em uma experiência de descoberta, incentivando o pensamento lógico e o encantamento dos estudantes.

2 OS NÚMEROS PRIMOS NA ANTIGUIDADE CLÁSSICA

Conforme discutido na introdução, os números primos mantêm relevância histórica e contemporânea. Este capítulo propõe uma imersão na trajetória histórica do estudo desses números especiais, em seus primeiros desenvolvimentos.

2.1 Os Pitagóricos e os Primórdios da Teoria dos Números

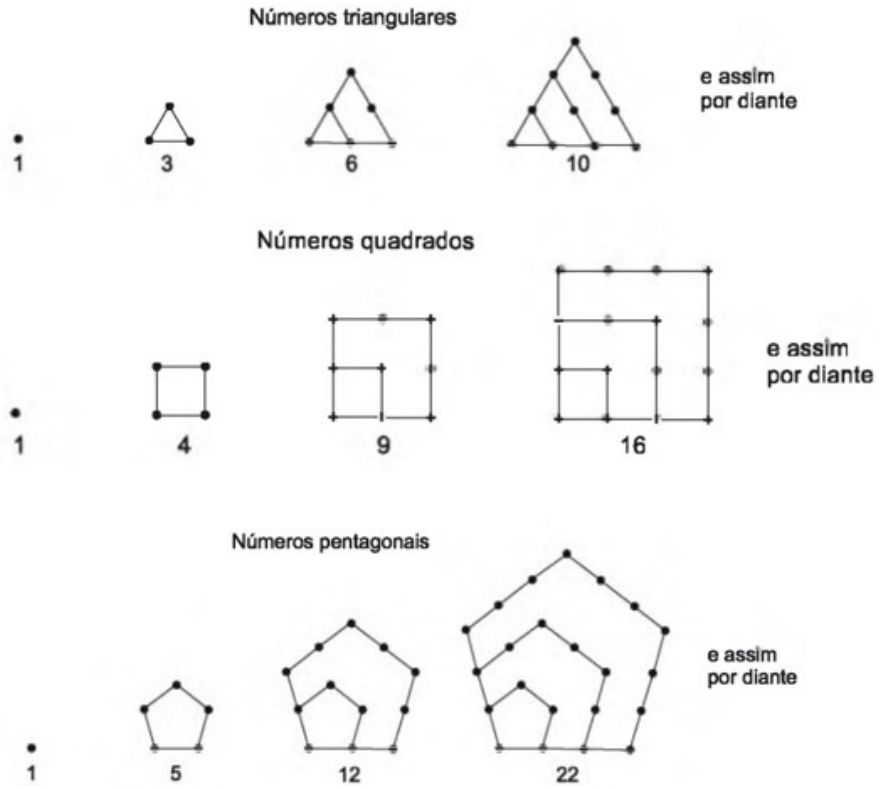
A investigação das propriedades dos números, e o início do conceito de número primo, têm suas raízes mais documentadas na Grécia Antiga, particularmente na escola filosófica e matemática fundada por Pitágoras de Samos (c. 570-500 a.C.). Embora a figura histórica de Pitágoras seja parcialmente obscurecida por lendas, o impacto da Irmandade Pitagórica no desenvolvimento da Matemática é amplamente reconhecido por historiadores como Carl Boyer (2012) e Howard Eves (2011).

Conforme Boyer e Merzbach (2012), para os pitagóricos, os números não eram meras abstrações ou ferramentas de cálculo, mas sim os constituintes da própria realidade, a base da ordem e harmonia do universo. A máxima "tudo é número" resume essa visão.

Dentro dessa filosofia, eles desenvolveram uma distinção importante, conforme aponta Boyer e Merzbach (2012), entre a Aritmética, que se dedicava ao estudo das propriedades abstratas dos números, e a Logística, que tratava das técnicas práticas de cálculo. O foco principal da escola pitagórica residia na Aritmética, considerada uma das disciplinas do

Quadrivium (Aritmética, Geometria, Música e Astronomia). No âmbito da Aritmética, os pitagóricos dedicaram-se a classificar os números segundo suas propriedades. A distinção mais fundamental era entre números pares e números ímpares, aos quais atribuíam qualidades místicas, sendo o par associado ao feminino e o ímpar ao masculino (Boyer e Merzbach, 2012). Outra classificação importante era a dos números figurados, que representavam números como arranjos geométricos de pontos, como os números triangulares (1, 3, 6, 10,...), quadrados (1, 4, 9, 16,...), pentagonais (1, 5, 12, 22,...), refletindo a forte conexão entre aritmética e geometria no pensamento grego (Eves, 2011). A Figura 1 justifica essa nomenclatura.

Figura 1 - Números triangulares, números quadrados, números pentagonais



Fonte: Eves (2011, p.100).

Foi no estudo dos divisores que surgiram conceitos importantes para a nossa investigação. Os pitagóricos e seus sucessores identificaram os números perfeitos, definidos como aqueles números inteiros positivos cuja soma de seus divisores próprios (todos os divisores positivos, exceto o próprio número) é igual a ele mesmo. Os primeiros exemplos, conhecidos desde a antiguidade, são 6 (1+2+3 = 6) e 28 (1+2+4+7+14 = 28). Os próximos dois, 496 e 8128, também já eram conhecidos pelos gregos (Boyer e Merzbach, 2012). Esses números exerceram um fascínio místico e numerológico por séculos, como nota Eves (2011).

A importância matemática dos números perfeitos vai muito além das interpretações numerológicas. Eles mantêm uma ligação profunda com os números primos, o que só foi plenamente compreendido séculos depois (Boyer e Merzbach, 2012).

Mesmo sem registros diretos dos ensinamentos de Pitágoras, já que muito do que sabemos nos chega por meio de autores posteriores, é inegável que sua escola desempenhou um papel importante ao inaugurar o estudo das propriedades dos números. Foram eles que começaram a classificar os números, abrindo caminho para o surgimento do conceito de número primo e lançando as bases do que viria a se tornar a teoria dos números (Boyer e Merzbach, 2012).

2.2 Euclides de Alexandria: A Formalização e os Teoremas Fundamentais

A transição de um estudo místico-filosófico dos números para uma teoria matemática rigorosa e organizada ocorreu com Euclides de Alexandria (c. 300 a.C.). Sua obra magna, *Os Elementos*, embora mais famosa pela geometria, dedica três de seus treze livros (VII, VIII e IX) exclusivamente à aritmética (Boyer e Merzbach, 2012).

No Livro VII, Euclides apresenta as definições cruciais. A Definição VII.12 estabelece o que é um número primo: "Um número primo é o medido por uma unidade só" (Euclides, 2009, p. 269). A Definição VII.14 define número composto como " Um número composto é o medido por algum número" (Euclides, 2009, p. 270). Euclides usa o termo "medido por" para indicar divisibilidade (Boyer e Merzbach, 2012).

De acordo com Eves (2011), ainda no Livro VII proposições iniciais, Euclides descreve um método para encontrar o máximo divisor comum de dois ou mais números através de subtrações sucessivas, conhecido hoje como Algoritmo de Euclides. Este algoritmo é uma ferramenta essencial na teoria dos números e suas aplicações.

O Livro IX contém resultados notáveis sobre números primos. O mais célebre é a Proposição IX.20, que demonstra a infinitude dos números primos. A prova, um exemplo clássico de argumentação por redução ao absurdo, é admirada por sua elegância e simplicidade (Eves, 2011). A demonstração, conforme descrita por Boyer e Merzbach, é a seguinte:

> Seja P o produto de todos os primos, supostos em número finito, e consideremos o número N = P + 1. N não pode ser primo, pois isso contradiria a hipótese de P ser o produto de todos os primos. Logo, N é composto e deve ser medido por algum número p. Mas p não pode ser nenhum dos fatores primos que entram em P, senão seria um fator de 1. Logo, p deve ser um primo diferente de todos os fatores de P; portanto, a hipótese de P ser o produto de todos os primos é falsa (Boyer e Merzbach, 2012, p.98).

Outro resultado fundamental da teoria dos números, cujas bases estão estabelecidas nos *Elementos*, no Livro IX, é algo similar ao Teorema Fundamental da Aritmética (TFA): “todo inteiro maior que 1 pode se expressar como produto de primos de uma e, salvo quanto à ordem dos fatores, uma só maneira” (Eves, 2011, p. 175). A Proposição VII.30, conhecida como Lema de Euclides, afirma em linguagem moderna que, se um número primo p divide o produto ab, então p divide a ou p divide b. Combinada com a Proposição VII.32 que afirma que todo número maior que 1 é primo ou tem um divisor primo (Euclides, 2009), pode-se demonstrar a existência da fatoração em primos. A demonstração rigorosa desse teorema só foi explicitamente formulada muito mais tarde por Carl Friedrich Gauss (1777-1855) em suas *Disquisitiones Arithmeticae* (1801) (Boyer e Merzbach, 2012).

Nesse contexto de divisibilidade, emerge a distinção entre números primos e números compostos. Conforme Eves (2011), um número primo é entendido como um inteiro positivo, maior que a unidade, que só podia ser dividido pela unidade e por si mesmo. Um número composto era aquele que admitia outros divisores. Coutinho nos traz um fato histórico sobre a origem do termo primo:

> Finalmente, uma questão histórica (ou melhor dizendo, etimológica), você já se perguntou porque os números primos têm este nome? O nome é uma herança grega e, naturalmente, não se refere a nenhuma relação de parentesco. Os gregos classificavam os números em primeiros ou indecomponíveis e secundários ou compostos. Os números compostos são secundários por serem formados a partir dos primos. Os romanos apenas traduziram literalmente a palavra grega para primeiro, que em latim é primus. É daí que vêm nossos números primos. (Coutinho, 2015 p. 19)

Foi Euclides, em seus Elementos, quem estabeleceu a primeira conexão fundamental entre números primos e perfeitos, na Proposição IX.36, que afirma que, se $2^n - 1$ é um número primo, então o número N = $2^{n-1}(2^n - 1)$ é um número perfeito (Boyer e Merzbach, 2012). Veremos, na seção 2.4, que os números primos da forma $2^n - 1$, onde n é primo, ficaram conhecidos mais tarde como primos de Mersenne.

Quase dois milênios depois de Euclides, Leonhard Euler (1707-1783) provou a recíproca dessa afirmação para os números pares: todo número perfeito par necessariamente é da forma descrita por Euclides (Eves, 2011). Assim, a busca por novos números perfeitos pares equivale à busca por novos primos de Mersenne. Apesar desses avanços, existem questões fundamentais sobre números perfeitos ainda em aberto, como a existência ou não de números perfeitos ímpares (Coutinho, 2005). Até a data das publicações consultadas e até o presente momento, abril de 2025, a questão ainda não tinha sido respondida.

O legado deixado por Euclides é muito grande. Além de ter dado uma definição formal aos números primos e de ter demonstrado que são infinitos, ele também forneceu uma estrutura lógica e um conjunto de conhecimento matemático elementar que dominou o pensamento e o ensino matemático por mais de dois milênios, servindo como alicerce para grande parte da matemática subsequente.

2.3 Desenvolvimentos Posteriores: Idade Média e Renascimento

O período que se seguiu ao declínio da Matemática grega clássica, abrangendo a maior parte da Idade Média europeia, aproximadamente séculos V ao XI, foi caracterizado mais pela preservação e transmissão do conhecimento do que por avanços originais significativos na

teoria dos números (Eves, 2011).

Figuras como Boécio (c. 480-524) tiveram um papel fundamental ao traduzir para o latim obras de Nicômaco e partes de Euclides, mantendo viva uma centelha da tradição aritmética grega no Ocidente Medieval. A *Introductio Arithmeticae* de Nicômaco de Gerasa (c. 100 d.C.), que apresentava as classificações pitagóricas de números (pares, ímpares, primos, perfeitos, etc.), tornou-se o manual padrão de aritmética por séculos, embora fosse considerado menos rigoroso que *Os Elementos* de Euclides (Boyer e Merzbach, 2012).

Enquanto a Europa Ocidental experimentava uma retração na produção matemática, o Mundo Islâmico, não só preservou as obras gregas, muitas vezes através de traduções siríacas e depois árabes, mas também fez contribuições originais importantes, especialmente em álgebra com Al-Khwarizmi. Na aritmética, houve trabalhos sobre as operações elementares (Boyer e Merzbach, 2012). Entretanto, avanços específicos sobre a natureza ou a distribuição dos primos parecem ter sido limitados nesse período.

A partir do século XII, com o renascimento cultural e comercial na Europa e o aumento do contato com o conhecimento árabe, houve um interesse renovado pela Matemática.

Figura 2 - Leonardo Fibonacci

Fonte: Eves (2011, p.293)

Leonardo de Pisa ou Leonardo Fibonacci (c. 1175-1250) (Figura 2), em seu *Liber Abaci* (1202), introduziu os numerais hindu-arábicos e apresentou uma vasta coleção de problemas aritméticos e algébricos, incluindo alguns relacionados à Teoria dos Números, mas sem descobertas transformadoras sobre primos (Eves, 2011).

O período do Renascimento foi marcado por grandes avanços em Álgebra, como a resolução de equações de 3º e 4º graus por Cardano, Tartaglia e Ferrari, mas também pela

aplicação da matemática às Artes e à Engenharia. Luca Pacioli (c. 1445-1514), em sua *Summa de Arithmetica* (1494), compilou o conhecimento matemático da época, incluindo Aritmética e Álgebra, mas era, em grande parte, uma síntese de trabalhos anteriores (Boyer e Merzbach, 2012).

Em resumo, do período pós-grego até o século XVII, a principal contribuição foi preservar e divulgar o que já se conhecia sobre os primos. As grandes perguntas sobre a natureza e a distribuição deles, ficaram praticamente em espera, aguardando que surgissem novas ideias e instrumentos para serem exploradas de fato.

2.4 O Renascimento da Teoria dos Números: Fermat e Mersenne

O século XVII teve uma transformação muito grande no cenário intelectual da Europa com a Revolução Científica. Neste contexto de intensa atividade matemática, impulsionada por figuras como Descartes com a Geometria Analítica e Kepler com as leis do movimento planetário, a Teoria dos Números experimentou um renascimento notável, liderado principalmente por Pierre de Fermat e Marin Mersenne (Eves, 2011).

Figura 3 - Pierre de Fermat

Fonte: Eves (2011, p.390)

Pierre de Fermat (1601-1665), um advogado francês que praticava matemática como hobby, é frequentemente chamado de príncipe dos amadores e considerado, junto com Pascal, cofundador da teoria das probabilidades, além de ser uma figura central na retomada da teoria dos números. Fermat não publicou suas descobertas matemáticas formalmente, comunicando-as por cartas, especialmente a Mersenne, ou anotando-as nas margens de seus

livros, como a famosa cópia da *Aritmética* de Diofanto (Boyer e Merzbach, 2012).

Uma de suas contribuições mais duradouras é o teorema hoje conhecido como Pequeno Teorema de Fermat. Em uma carta de 1640, ele afirmou que se p é um número primo e a é um inteiro não divisível por p, então $a^{p-1} - 1$ é divisível por p. Ele somente enunciou o teorema, não forneceu a prova (Eves, 2011). Nas palavras de Eves (2011, p. 391) "A primeira demonstração publicada desse teorema data de 1736 e é devida a Euler". Este teorema provou ser de imensa importância teórica e prática, formando a base para testes de primalidade e sendo um componente essencial do algoritmo de criptografia RSA, como explorado por Coutinho (2005).

Fermat também investigou os números da forma $F_n = 2^{2^n} + 1$, hoje chamados números de Fermat. Após verificar que $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257\ e\ F_4 = 65537$ são todos primos, ele conjecturou que todos os números F_n seriam primos. Contudo, Leonhard Euler demonstrou em 1730 que $F_5 = 2^{32} + 1$ é composto, pois é divisível por 641, para uma prova simples deste fato, veja o problema 7 da seção 5.1 de Muniz Neto (2022) (Tópicos de Matemática Elementar, volume 5). Nenhum outro número de Fermat primo foi encontrado até hoje, embora a busca continue (Coutinho, 2005).

Marin Mersenne (1588-1648), um frade da ordem dos mínimos, foi contemporâneo de Fermat e Descartes. Embora suas próprias contribuições matemáticas originais sejam modestas, ele desempenhou um papel indispensável como um "secretário científico" para a Europa, mantendo uma vasta rede de correspondência que ajudava a disseminar rapidamente ideias, problemas e resultados (Boyer e Merzbach, 2012). Mersenne era um amigo próximo de Fermat e de muitos outros matemáticos da época. Fermat, inclusive, costumava escrever a Mersenne sobre suas ideias (Coutinho, 2005).

Mersenne interessou-se particularmente pelos números da forma $M(n) = 2^n - 1$, onde n é um número primo (veja demonstração abaixo), hoje chamados números de Mersenne. A conexão desses números com os números perfeitos já era conhecida desde Euclides: se $M(n)$ é primo, então $(2^{n-1})M(n)$ é perfeito (Coutinho, 2005). Prova de que n deve ser primo.

> Segundo ele, os números da forma $M(n) = 2^n - 1$ seriam primos quando:
> $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257;
> e compostos para os outros 44 valores primos de n menores que 257.
> A primeira coisa a observar é que todos os expoentes a que se refere Mersenne são primos. Isto porque se n for composto, então $M(n)$ também será composto. É fácil provar este fato. Se $n = rs$ é composto, então
> $$M(n) = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1)$$
> Portanto, se r divide n então $M(r)$ divide $M(n)$.
> A segunda coisa a observar, é que a recíproca é falsa. Em outras palavras,
> se n for primo isto não significa que $M(n)$ tem que ser primo (Coutinho, 2005 p. 57).

Segundo Coutinho (2005) a lista de Mersenne, no entanto, continha erros. Investigações posteriores mostraram que M(67) e M(257) são compostos, enquanto M(61), M(89) e M(107), que ele omitiu, são primos.

Os trabalhos de Fermat e Mersenne, portanto, levantaram a teoria dos números após séculos de relativa paralisação. Juntamente com matemáticos como Euler, Lagrange, Legendre e Gauss, estabeleceram a Teoria dos Números como uma disciplina matemática profunda e sofisticada, revelando cada vez mais a beleza e a complexidade dos números primos.

Este capítulo buscou traçar a evolução histórica inicial do conceito e estudo dos números primos, desde as primeiras noções na Grécia Antiga até o renascimento do interesse no século XVII.

3 FUNDAMENTOS DA TEORIA DOS NÚMEROS E DIVISIBILIDADE

Depois da jornada histórica descrita no Capítulo 2, este novo capítulo nos incentiva a explorar ainda mais os alicerces matemáticos que respaldam esses números especiais. A teoria dos números, amigavelmente referida como a "Rainha da Matemática" pela sua beleza, proporciona a linguagem e a ferramenta necessárias para explorar a face oculta dos números.

3.1 Divisibilidade

A teoria elementar dos números se inicia com a análise das propriedades da divisibilidade no conjunto dos números inteiros, representado por $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$. A relação da divisibilidade é a base em que se constroem muitos dos conceitos posteriores. Para este capítulo, como referências, utilizamos Muniz Neto (2022), Hefez (2022), Santos (1998) e Lemos (2010).

Definição 3.1.1. Considere a e b números inteiros. A expressão "a divide b", escrita como $a \mid b$, significa que existe um inteiro $c \in \mathbb{Z}$ para o qual $b = c \cdot a$. Nessas circunstâncias, a é um divisor ou fator de b, e b é um múltiplo de a. A notação $a \mid b$ é uma afirmação sobre a existência de tal inteiro c, e não uma operação ou fração. A sua negação, $a \nmid b$, indica que nenhum inteiro c satisfaz $b = c \cdot a$.

Exemplo 3.1.1. Temos $3 \mid 12$, pois $12 = 4 \cdot 3$; $-5 \mid 30$, pois $30 = (-6) \cdot (-5)$; mas $4 \nmid 10$, pois não existe inteiro c tal que $10 = c \cdot 4$.

Algumas propriedades básicas da divisibilidade, que decorrem diretamente da definição, são dadas pela seguinte proposição:

Proposição 3.1.1. Para quaisquer inteiros a, b e c, as seguintes propriedades são válidas:

i) $1 \mid a$, $a \mid a$ e $a \mid 0$.

ii) $0 \mid a \iff a = 0$.

iii) Se $a \mid 1$, então $a = \pm 1$.

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

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

vi) Se $a \mid b$, com $b \neq 0$, então $|a| \leq |b|$.

Demonstração:

i) Esta afirmação é uma consequência direta das seguintes identidades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

ii) Suponhamos que $0 \mid a$; logo, existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0 = 0$. Conclui-se que $a = 0$. Para a recíproca basta observar que $0 \mid 0$, o que foi provado no item anterior.

iii)Dado que $a|1$, sabemos, pela definição de divisibilidade, que $1 = a \cdot k$ para algum inteiro k. Como a e k são inteiros, a única forma de o produto deles ser 1 é se ($a = 1$ e $k = 1$) ou se ($a = -1$ e $k = -1$). Portanto, os únicos valores possíveis para a são 1 ou -1, ou seja, $a = \pm 1$.

iv)Se $a \mid b$ e $b \mid c$, então, por definição, existem números inteiros x e y para os quais $b = xa$ e $c = yb$. Ao inserir a expressão de b (da primeira igualdade) na segunda igualdade, temos $c = y(xa)$. Como a multiplicação de inteiros é associativa, podemos reorganizar os termos $c = (yx)a$**.** Sendo x e y inteiros, o produto xy também é um número inteiro. Isso demonstra que a divide c, pela definição de divisibilidade.

v) A primeira condição, $a|b$, implica a existência de um inteiro k_1 tal que $b = ak_1$. A segunda condição, $b \mid a$, implica a existência de um inteiro k_2 tal que $a = bk_2$. Se substituirmos a expressão de b, da primeira implicação, na segunda equação, obtemos $a = (ak_1)k_2$. O que pode ser reescrito como $a = a(k_1k_2)$. Agora, analisamos duas situações possíveis. Se $a \neq 0$, podemos dividir ambos os lados da equação $a = a(k_1k_2)$ por a, resultando em $1 = k_1k_2$. Como k_1 *e* k_2 são números inteiros, a única maneira de o produto deles ser 1 é se ambos forem 1 ou se ambos forem -1. Retomando a equação $a = bk_2$, e sabendo que $k_2 = \pm 1$, concluímos que $a = \pm b$. Se $a = 0$, a condição $a|b$ se torna $0|b$. Para que 0 divida b, b necessariamente deve ser 0. A condição $b|a$, com $a = 0$ e $b = 0$, torna-se 0|0. Neste caso, temos $a = 0$ e $b = 0$, o que satisfaz a relação $a = \pm b$.

vi)Se $a|b$, então, por definição, existe um inteiro k tal que $b = ak$. Dado que $b \neq 0$, o inteiro k também deve ser diferente de zero. Ao considerarmos os valores absolutos de ambos os lados da equação $b = ak$, obtemos $|b| = |ak|$. Utilizando a propriedade do módulo de um produto, isso se torna $|b| = |a||k|$. Como k é um inteiro não nulo, então $|k| \geq 1$. Assim, podemos afirmar que $|b| = |a||k| \geq |a| \cdot 1 \geq |a|$. Isso demonstra que $|a| \leq |b|$.

□

A seguir, apresentamos algumas proposições úteis sobre divisibilidade, conforme expostas por Hefez (2022).

Proposição 3.1.2. Sejam $a, b, c, d \in \mathbb{Z}$, se $a|b$ e $c|d$, então $ac|bd$.

Demonstração: Suponha $a|b$ e $c|d$. Então existem inteiros x, y tais que $b = xa$ e $d = yc$. Multiplicando, obtemos $bd = (xa)(yc) = (xy)(ac)$. Como $xy \in \mathbb{Z}$,concluímos que $ac \mid bd$. Em particular, se $a \mid b$, então para todo $c \in \mathbb{Z}$, vale que $ac \mid bc$.

□

Proposição 3.1.3. Sejam $a, b, c \in \mathbb{Z}$, tais que a divide $(b \pm c)$. Então, temos a seguinte equivalência: $a|b \Leftrightarrow a|c$.

Demonstração: Primeiro, suponha que $a|(b + c)$. Isso significa que existe um inteiro k tal que $b + c = ka$. Se $a|b$, então existe um inteiro j tal que $b = ja$. Substituindo b na equação inicial, temos $ja + c = ka \Longrightarrow c = (k - j)a$, o que mostra que $a|c$.

A demonstração da implicação inversa é análoga. Além disso, se $a|(b - c)$ e $a|b$, aplicando o raciocínio anterior, segue que $a|-c$ e, portanto, $a|c$.

□

Proposição 3.1.4. Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para quaisquer inteiros x e y vale que: $a|(xb + yc)$.

Demonstração: Como $a|b$ e $a|c$, existem me n inteiros tais que $b = ma$ e $c = na$. Multiplicando por x e y, respectivamente, temos: $xb + yc = x(ma) + y(na) = (xm + yn)a$. Como $xm + yn$ é um número inteiro, concluímos que $a|(xb + yc)$.

□

Embora não seja sempre possível dividir exatamente em $\mathbb{Z}$, podemos sempre realizar uma divisão com resto. O famoso resultado é chamado de algoritmo da divisão ou teorema da divisão euclidiana. Antes de enunciar e provar o teorema, veremos o Princípio da Boa Ordenação.

Esse princípio afirma que todo subconjunto não vazio dos números inteiros que possui uma cota inferior contém um elemento mínimo. Como os números naturais são, por definição, limitados inferiormente (por exemplo, por 1), esse princípio garante que qualquer subconjunto não vazio de $\mathbb{N}$ sempre terá um menor elemento (Hefez, 2022).

Teorema 3.1.1. (Algoritmo da Divisão). Dados dois inteiros a e b, com $b > 0$, existem únicos inteiros q (quociente) e r (resto) tais que: $a = bq + r$ e $0 \leq r < b$.

Vejamos uma demonstração dada por Lemos (2010).

Demonstração: (Lemos, 2010) Seja S o seguinte conjunto:

$S = \{a - qb: q \in \mathbb{Z}\ e\ a - qb \geq 0\}$.

Observe que $S \neq \emptyset$ pois $a - qb \in S$ quando $q = -a^2$, já que $a - qb = a + a^2 b \geq a + a^2 \geq 0$. Pelo princípio da boa ordenação, existe um menor elemento $r \in S$. Como $r \in S$, existe $q \in \mathbb{Z}$ tal que $r = a - bq$. Observe que $r < b$, caso contrário $0 \leq r - b = a - qb - b = a - (q + 1)b \in S$ e $r - b \in S$, o que não pode ocorrer pois r é o menor elemento de S. Acabamos de demonstrar que a pode ser escrito na forma $qb + r$ com $0 \leq r < b$. Vamos mostrar que essa decomposição é feita de maneira única. Suponha que $a = qb + r = q'b + r'$ com $0 \leq r < b$ e $0 \leq r' < b$. Caso $q = q'$, temos que $r = r'$ como queríamos demonstrar. Podemos supor que $q \neq q'$, mais ainda, que $q > q'$. Obtemos que $(q - q')b = r' - r$. Observe que o lado esquerdo dessa igualdade é maior ou igual a b e o direito menor que b. Chegamos a uma contradição e o resultado segue.

□

O corolário abaixo estende o algoritmo para o caso em que b é um inteiro qualquer não nulo ($b \neq 0$):

Corolário 3.1.1. Se a e b são dois inteiros, com $b \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições: $a = bq + r$ e $0 \leq r < |b|$.

Demonstração: (Muniz Neto, 2022) Se $b > 0$, então $|b| = b$, e o teorema já foi demonstrado. Se $b < 0$, então $|b| > 0$. Pelo teorema 3.1.1, existem e são únicos os inteiros q' e r tais que $a = |b|q' + r$ e $0 \leq r < |b|$. Como $b < 0$, temos $|b| = -b$. Então, $a = -bq' + r = b(-q') + r$. Seja $q = -q'$. Então, $a = bq + r$, com $0 \leq r < |b|$. Os inteiros q e r são únicos.

□

Exemplo 3.1.1. Para $a = 27$ e $b = 6$, a divisão euclidiana é dada por $27 = 6 \cdot 4 + 3$, onde o quociente é $q = 4$ e o resto é $r = 3$, satisfazendo a condição $0 \leq r < |b|$. De modo semelhante, para $a = -27$ e $b = 6$, temos $-27 = 6 \cdot (-5) + 3$, com quociente q = -5 e resto r = 3, também obedecendo à restrição $0 \leq r < |b|$. Note que a condição $0 \leq r < |b|$ é crucial para a unicidade.

O algoritmo da divisão é a base para muitos outros conceitos e algoritmos na teoria dos números, incluindo o cálculo do máximo divisor comum.

3.2 Máximo Divisor Comum (MDC) e Algoritmo de Euclides

Dados dois inteiros, frequentemente estamos interessados em seus divisores comuns, e em particular, no maior deles.

Definição 3.2.1. (Máximo Divisor Comum): Sejam $a, b \in \mathbb{Z}$, não ambos nulos. O máximo divisor comum de a e b, denotado por $mdc(a,b)$ ou (a,b), é o inteiro $d > 0$ que satisfaz as seguintes condições:

i) $d|a$ e $d|b$ (d é um divisor comum).

ii) Se c é um inteiro tal que $c|a$ e $c|b$, então $c|d$ (todo divisor comum divide d).

Algumas propriedades que decorrem imediatamente da definição são:

a) O $mdc(a,b) = mdc(b,a)$.

b) O $mdc(0,0)$ não existe.

c) O $mdc(a,1) = 1$.

d) Se $a \neq 0$, então o $mdc(a,0) = |a|$.

e) Se $a|b$, então o $mdc(a,b) = |a|$.

Para qualquer inteiro a, os divisores de a são idênticos aos divisores de $-a$. Como resultado, o máximo divisor comum entre dois inteiros a e b não se altera se mudarmos o sinal de um ou de ambos os inteiros. Portanto, temos que:

$mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b)$

Esta igualdade é válida para quaisquer inteiros a e b, contanto que a e b não sejam ambos iguais a zero simultaneamente.

Definição 3.2.2. Dois números inteiros, a e b, são considerados primos entre si (ou coprimos) quando o Máximo Divisor Comum (MDC) entre eles é igual a 1. Em outras palavras, isso significa que o único número inteiro positivo que divide simultaneamente a e b é o próprio 1. Matematicamente, a e b são primos entre si se $mdc(a,b) = 1$.

Exemplo 3.2.1. Sejam os inteiros $a = 15$ e $b = 18$. Os divisores comuns positivos de 15 e 18 são 1 e 3. Como o maior deles é 3, segue-se que o $mdc(15,18) = 3$. Observa-se também que $mdc(15,18) = mdc(-15,18) = mdc(15,-18) = mdc(-15,-18)$.

Exemplo 3.2.2. Sejam os inteiros $a = -36$ e $b = 60$. Os divisores comuns positivos de -36 e 60 são 1, 2, 3, 4, 6 e 12. Como o maior deles é 12, segue-se que o $mdc(-36,60) = 12$. O $mdc(8,15) = 1$, logo 8 e 15 são primos entre si.

Um lema muito importante para o cálculo do mdc é:

Proposição 3.2.1. Para inteiros $a, b\ e\ r$, se o máximo divisor comum de a e $b - ra$ existir, então o $mdc(a, b)$ também existirá, e ambos serão iguais, ou seja: $mdc(a, b) = mdc(a, b - ra)$.

Demonstração: Vamos assumir que $d = mdc(a, b - ra)$ existe. Por definição de mdc, $d|a$ e $d|b - ra$. Sabemos que d também deve dividir qualquer combinação linear desses dois números. Então d deve dividir a soma $b - ra + ra$, que é b. Portanto, $d|b$. Já que $d|a$ e agora mostramos que $d|\ b$, concluímos que d é um divisor comum de a e b . Agora, precisamos mostrar que d é o *maior* divisor comum de a e b. Para isso, considere um inteiro qualquer c que seja um divisor comum de a e b. Assim, $c|a$ e $c|b$. Daí, c também deve dividir ra. Consequentemente, c deve dividir a diferença $b - ra$. Então, c é um divisor comum de a e de $b - ra$. Logo, c deve dividir d, ou seja, $c|d$.

□

Exemplo 3.2.3. Vamos calcular o $mdc(24, 60)$ usando o Lema 3.2.1.

$mdc(24,60) = mdc(24, 60 - 2 \cdot 24) = mdc(24, 12) = 12$. Portanto, $mdc(24, 60) = 12$.

Apresentaremos a seguir o algoritmo de Euclides, que segundo Boyer e Merzbach (2012), embora haja indícios de que o processo para determinar o maior divisor comum entre dois números fosse conhecido anteriormente, foi Euclides quem o articulou com clareza em sua obra *Os Elementos*. A abordagem euclidiana, originalmente de natureza geométrica, é facilmente traduzível para a forma algébrica moderna e permite, inclusive, verificar se dois números são primos entre si.

Segundo Hefez (2022), o Algoritmo de Euclides é um método eficiente para calcular o máximo divisor comum de dois números naturais a e b. E a demonstração construtiva de Euclides para a existência do mesmo, conforme apresentada em sua obra "Os Elementos" (Livro VII, Proposição 2), será detalhada a seguir. A descrição do algoritmo é a seguinte:

Dados dois números naturais a e b , podemos supor que $b \leq a$.

Se $b = 1$, então $mdc(a, b) = 1$. Se $b = a$, então $mdc(a, b) = a$. Se b divide a (ou seja, $a = bq$ para algum inteiro q), então $mdc(a, b) = b$. Para o processo iterativo do algoritmo, supõe-se que $1 < b < a$ e que b não divide a.

Divide-se a por b e obtém-se o quociente q_1 e o resto r_1: $a = bq_1 + r_1$, onde $0 < r_1 < b$. A proposição 3.2.1 é importante aqui, pois ele estabelece que $mdc(a, b) = mdc(b, r_1)$.

Se r_1 divide b, então r_1 é o $mdc(a, b)$. O algoritmo termina.

Se r_1 não divide b, divide-se b por r_1 para obter o quociente q_2 e o resto r_2: $b = r_1q_2 + r_2$, onde $0 < r_2 < r_1$. Agora, $mdc(b, r_1) = mdc(r_1, r_2)$. Se r_2 divide r_1, então r_2 é o $mdc(a, b)$. O algoritmo termina.

Se r_2 não divide r_1, continua-se o processo, dividindo r_1 por r_2 para obter r_3: $r_1 = r_2q_3 + r_3$, onde $0 < r_3 < r_2$.

O processo continua gerando uma sequência de restos estritamente decrescentes e positivos: $b > r_1 > r_2 > r_3 > \cdots > 0$. Pelo Princípio da Boa Ordenação, esta sequência não pode continuar indefinidamente e deve, portanto, terminar. O algoritmo para quando um resto r_n divide o resto anterior r_{n-1}, o que significa que o resto seguinte, r_{n+1}, seria 0. O último resto não nulo, r_n, é o $mdc(a, b)$. Esse processo é também uma prova construtiva da existência do $mdc(a, b)$.

O algoritmo pode ser usado na prática com o auxílio de uma tabela da seguinte maneira:

Efetuando a primeira divisão $a = bq_1 + r_1$ e colocando como abaixo, temos

	q_1	
a	b	
r_1		

Efetuamos a segunda divisão $b = r_1q_2 + r_2$ e acrescentamos mais linhas e colunas, ficamos

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Continuando até o processo parar, teremos

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

Exemplo 3.2.4. Vamos calcular o $mdc(48{,}18)$ usando o Algoritmo de Euclides.

Resolução. Primeiro vamos resolver usando as divisões sucessivas.

$$\begin{array}{r|l} 48 & 18 \\ \cline{2-2} 12 & 2 \end{array} \qquad \begin{array}{r|l} 18 & 12 \\ \cline{2-2} 6 & 1 \end{array} \qquad \begin{array}{r|l} 12 & 6 \\ \cline{2-2} 0 & 2 \end{array}$$

Em seguida colocamos tudo em uma tabela, como abaixo.

	2	1	2
48	18	12	6
12	6	0	

Agora pelo algoritmo de Euclides, temos

$$48 = 18 \cdot 2 + 12$$

$$18 = 12 \cdot 1 + 6$$

$$12 = 6 \cdot 2 + 0$$

Como o resto é 0, o mdc é o último divisor utilizado, que é o último valor na linha do meio, ou o último resto não nulo. Portanto, $mdc(48{,}18) = 6$.

Agora observe que se substituímos "de trás para a frente", obtemos da segunda linha: $6 = 18 - 12 \cdot 1$ e da primeira linha: $12 = 48 - 18 \cdot 2$. Substituindo 12 na expressão da segunda linha:

$$6 = 18 - (48 - 18 \cdot 2) = 18 - 48 + 18 \cdot 2 = -48 + 18 \cdot 3 = 48(-1) + 18(3).$$

Após encontrar o máximo divisor comum de a e b através do algoritmo de Euclides, sempre se pode determinar inteiros x e y que satisfazem $ax + by = mdc(a, b)$. Essa propriedade é conhecida como Teorema de Bachet-Bézout. Será o nosso próximo resultado.

Teorema 3.2.1. (Bachet-Bézout) Sejam a e b dois números inteiros não ambos nulos. Então, existem inteiros x e y tais que: $ax + by = mdc(a, b)$. Em outras palavras, o

máximo divisor comum de a e b pode ser expresso como uma combinação linear de a e b com coeficientes inteiros.

Demonstração: Considere o conjunto S de todas as combinações lineares positivas de a e b: $S = \{as + bt/s\,, t \in \mathbb{Z}\; e\; as + bt > 0\}$.

Vamos mostrar que S não é vazio. Se $a \neq 0$, então $|a| \in S$. Se $b \neq 0$, então $|b| \in S$. Como a e b não são ambos nulos, S é um conjunto não vazio de inteiros positivos. Pelo princípio da Boa Ordenação, S possui um menor elemento, que chamaremos de d. Como $d \in S$, existem inteiros x e y tais que $d = ax + by$. Pelo algoritmo da divisão, podemos escrever $a = qd + r$, onde q é o quociente e r é o resto, com $0 \leq r < d$. Substituindo $d = ax + by$, temos:

$$r = a - qd = a - q(ax + by) = a - qax - qby = a(1 - qx) + b(-qy).$$

Se $r > 0$, então r seria um elemento de S. No entanto, $r < d$, o que contradiz o fato de d ser o menor elemento de S. Portanto, $r = 0$. Se $r = 0$, então significa que d divide a. De forma análoga, podemos mostrar que d divide b. Agora seja c um divisor comum qualquer de a e b. Então, existem inteiros m e n tais que $a = cm$ e $b = cn$. Substituindo na equação $d = ax + by$, temos que $d = (cm)x + (cn)y = c(mx + ny)$, como $mx + ny$ é um inteiro, isso implica que c divide d. Portanto, qualquer divisor comum de a e b também é um divisor de d. Isso significa que d é o maior de todos os divisores comuns, ou seja, $d = mdc(a, b)$. Concluímos então que existem inteiros x e y tais que $ax + by = mdc(a, b)$.

□

Corolário 3.2.1. O $mdc(a, b) = 1$ se, e somente se, existem inteiros u e v tais que $au + bv = 1$.

Demonstração: (⇒) Suponha o $mdc(a, b) = 1$, então pelo teorema 3.2.1(Bézout) existem inteiros u, v tais que $au + bv = 1$. (⇐) Suponha que existem inteiros u e v tais que $au + bv = 1$. Seja $mdc(a, b) = d$. Por definição, d é um divisor comum de u e v. Como d divide au e d divide bv, então d deve dividir a soma deles: $d|(au + bv)$. Portanto, $d|1$. Os únicos divisores inteiros de 1 são 1 e -1. Como $d > 0$, a única possibilidade é $d = 1$. Portanto, $mdc(a, b) = 1$.

□

3.3 Mínimo Múltiplo Comum (MMC)

Para entender o conceito de mínimo múltiplo comum, primeiro precisamos saber o que são múltiplos de um inteiro. O conjunto de todos os inteiros que são múltiplos de um inteiro n é representado por $n\mathbb{Z}$, que é o conjunto de todos os nk onde k é um inteiro. Um inteiro c é considerado um múltiplo comum de dois inteiros não nulos a e b se ambos a e b dividem c. Isso implica que c faz parte da interseção dos conjuntos de múltiplos de a e de b.

Para ilustrar vejamos um exemplo.

Exemplo 3.3.1. Vejamos os múltiplos comuns de 4 e 6.

Primeiro, listamos alguns múltiplos de 4: $4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, 12, 16, 20, 24, \dots\}$

Em seguida, listamos alguns múltiplos de 6: $6\mathbb{Z} = \{\dots, -12, -6, 0, 6, 12, 18, 24, \dots\}$

Os múltiplos comuns de 4 e 6 são os números que aparecem em ambas as listas. Neste caso, alguns exemplos de múltiplos comuns são:

12: Pois 12 é divisível por 4 e 12 é divisível por 6.

24: Pois 24 é divisível por 4 e 24 é divisível por 6.

Outros múltiplos comuns incluem 0, -12, -24, e assim por diante. O menor múltiplo comum positivo aqui seria 12.

Definição 3.3.1. (Mínimo Múltiplo Comum): Sejam $a, b \in \mathbb{Z}$, ambos não nulos. O mínimo múltiplo comum de a e b, denotado por $mmc(a, b)$, é o inteiro positivo m que satisfaz:

i) $a|m$ e $b|m$ (m é um múltiplo comum).

ii) Se c é um inteiro tal que $a|c$ e $b|c$, então $m|c$ (todo múltiplo comum é divisível por m).

A condição ii) implica que m é o menor dos múltiplos comuns positivos. Uma relação fundamental conecta o mdc e o mmc de dois inteiros positivos a e b. Antes veremos dois resultados. As demonstrações e enunciados que daremos aqui constam essencialmente em Hefez (2022).

Proposição 3.3.1. Dados $a, b \in \mathbb{Z}$, não ambos nulos, e seja $d = mdc(a, b)$ tem-se que, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Demonstração: Como $d = mdc(a, b)$ e $d \neq 0$. Pelo teorema 3.2.1(Bézout), existem inteiros x e y tais que $ax + by = d$. Dividindo ambos os lados por d, obtemos $\frac{a}{d}x +$

$\frac{b}{d}y = 1$. Sejam $a' = \frac{a}{d}$ e $b' = \frac{b}{d}$. Então, a equação se torna: $a'x + b'y = 1$. Logo, pelo corolário 3.2.1 o resultado segue $mdc(a', b') = 1$.

□

Teorema 3.3.1. (Lema de Gauss): Sejam a, b e c números inteiros. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração: Dado que $mdc(a, b) = 1$, pelo corolário 3.2.1, existem inteiros x e y tais que, $ax + by = 1$. Multiplicando ambos os lados desta equação por c, obtemos $acx + bcy = c$. Sabemos por hipótese que $a|bc$. Isso significa que existe um inteiro k tal que $bc = ak$. Substituindo na equação $acx + bcy = c$, temos $acx + (ak)y = c \Rightarrow a(cx + ky) = c$. Como $(cx + ky)$ também é um inteiro. Portanto, $a|c$

□

Teorema 3.3.2. Para inteiros positivos a e b, $mdc(a, b) \cdot mmc(a, b) = ab$.

Demonstração: Primeiro, consideramos os casos em que a ou b são zero. Nessas situações, o mmc é 0, e o produto ab também é 0, então a igualdade é válida.

Definimos um número $m = \frac{ab}{d}$. Podemos expressar m de duas formas: $m = a \cdot \frac{b}{d}$ e $m = b \cdot \frac{a}{d}$. Como d divide tanto a quanto b, as frações $\frac{b}{d}$ e $\frac{a}{d}$ são inteiras. Isso demonstra que m é um múltiplo de a e também um múltiplo de b, ou seja, m é um múltiplo comum de a e b.

Agora, precisamos mostrar que m é o menor múltiplo comum positivo. Para isso, tomamos c como um múltiplo comum qualquer de a e b. Isso significa que existem inteiros n e n' tais que $c = na$ e $c = n'b$. Consequentemente, $na = n'b$. Dividindo essa igualdade por d, obtemos $n\frac{a}{d} = n'\frac{b}{d}$. Sabemos, pela proposição 3.3.1, que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. Como $\frac{a}{d}$ divide o produto $n'\frac{b}{d}$ e é primo com $\frac{b}{d}$, o teorema 3.3.1 nos assegura que $\frac{a}{d}$ deve dividir n'. Assim, $n' = k\frac{a}{d}$ para algum inteiro k. Substituindo essa expressão de n' em $c = n'b$, temos $c = \left(k\frac{a}{d}\right)b = k\left(\frac{a}{d}b\right) = km$. Isso mostra que m divide c.

Como m é um múltiplo comum positivo de a e b, e m divide qualquer outro múltiplo comum c, concluímos que m é o $mmc(a, b)$. Portanto, $mmc(a, b) = m = \frac{ab}{d}$.

□

A compreensão desses conceitos de divisibilidade, é um pré-requisito importante antes que se possa mergulhar no estudo dos próprios números primos. Intimamente relacionados entre eles, em uma estrutura elegante na teoria dos números. Pular essa cadeia

lógica pode ser uma das causas importantes das dificuldades no ensino dos números primos e das suas propriedades mais importantes para os alunos.

Para o professor, é importante que, antes de proceder ao estudo dos números primos no contexto escolar, reserve uma sessão séria para retomar e aprofundar com os alunos os conceitos básicos de divisibilidade, máximo divisor comum, mínimo múltiplo comum. Para apresentar o Algoritmo de Euclides, utilize o algoritmo da divisão para mostrar, no contexto, a identidade de Bézout, aplicando-a em alguns exercícios. Certifique-se que os alunos compreendam essa cadeia conceitual ao longo da qual o nível de complexidade está sendo elevado. Para isso, sugira exercícios que investiguem essa relação entre esses conceitos e utilize exemplos específicos e contextualizados.

Não é aconselhável seguir uma estrutura de teoremas, proposições, lemas e corolários. Os alunos ainda não têm essa maturidade.

4 NÚMEROS PRIMOS: CONCEITOS FUNDAMENTAIS E PROPRIEDADES

Com os fundamentos da divisibilidade postos no capítulo anterior, este apresenta oficialmente os principais atores desta dissertação, os números primos. Vamos discutir sua definição, seu papel central na estrutura multiplicativa dos inteiros pelo uso do Teorema Fundamental da Aritmética (TFA), a notável prova da infinitude e seu antigo, mas eficiente Crivo de Eratóstenes para seu descobrimento. Neste capítulo, utilizaremos essencialmente como referência o livro Aritmética de Abramo Hefez (2022).

4.1 Definição de Número Primo e Número Composto

Definição 4.1.1. (Número primo): Um número natural é considerado primo se satisfizer duas condições essenciais:

i) Ser maior que 1;

ii) Possuir exatamente dois divisores positivos distintos, o número 1 e ele mesmo.

Vejamos duas propriedades decorrentes dessa definição:

Divisibilidade entre números primos: Sejam p e q dois números primos tais que $p \mid q$. Nesse caso, necessariamente $p = q$. Justificativa: Como q é primo, seus únicos divisores positivos são 1 e q. Logo, para que p divida q, p deve ser igual a 1 ou a q. Como p também é primo, $p > 1$, portanto só pode ser $p = q$.

Primalidade relativa ou coprimalidade: Se um número primo $p \nmid a$, então p e a são coprimos, isto é, seu máximo divisor comum é 1, $mdc(p, a) = 1$.

Argumentação: Seja $d = mdc(p, a)$. Por definição, d divide p e divide a. Como p é primo, os únicos divisores possíveis de p são 1 e p. Se $d \neq p$, pois $p \nmid a$, então necessariamente $d = 1$.

Um número natural maior que 1 que não é primo é chamado de composto. Formalmente, um número n é composto se pode ser expresso como o produto de dois inteiros n_1 e n_2, ambos maiores que 1 e menores que n.

Exemplo 4.1.1. A lista de números primos entre 1 e 100 é: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Sendo o 2 o único primo par.

Do ponto de vista da multiplicação, os números primos são os elementos básicos que compõem todos os demais números naturais. Eles são fundamentais para a construção dos números naturais não nulos, conforme formalizado no Teorema Fundamental da Aritmética (Hefez, 2022).

4.2 O Teorema Fundamental da Aritmética (TFA)

Antes de enunciar e demonstrar o TFA, veremos um lema importante. De acordo com Coutinho (2005) o Lema de Euclides, também conhecido como a propriedade fundamental dos primos, estabelece que se um número primo é divisor do produto de dois inteiros positivos, então esse primo necessariamente divide ao menos um desses inteiros. Esta propriedade, que remonta à Proposição 30 do Livro VII dos Elementos de Euclides, é de grande importância, sendo um dos pilares para demonstrar a unicidade da fatoração em primos de um número inteiro.

Lema 4.2.1(Euclides): Seja p um número primo e a e b inteiros positivos. Se p divide o produto ab, então p divide a ou p divide b.

Demonstração: Precisamos mostrar que se $p|ab$ e $p \nmid$ a, então $p|b$. Mas se $p \nmid$ a o $mdc(a,p) = 1$ e pelo teorema 3.3.1 temos que $p|b$.

□

De acordo com Coutinho (2005), embora o conceito expresso no teorema fundamental da aritmética já fosse utilizado de maneira implícita desde a Grécia Antiga, foi Carl Friedrich Gauss o primeiro a enunciá-lo em sua forma precisa na obra *Disquisitiones arithmeticae*. A atribuição a Gauss se justifica por ele ter sido o pioneiro no desenvolvimento da aritmética como uma ciência sistemática. Vamos ao teorema.

Para efeito de melhor entendimento vamos definir o Princípio de Indução Finita.

Definição 4.2.1. Seja $P(n)$ uma proposição formulada para todos os inteiros $n \geq n'$, onde $n' \in \mathbb{N}$ é fixado. Suponha que se verifiquem as duas condições:

Base: $P(n')$ é verdadeira;

Passo indutivo: para cada $k \geq n'$, a veracidade de $P(k)$ implica a veracidade de $P(k+1)$.

Nessas hipóteses, conclui-se que $P(n)$ é verdadeira para todos os $n \geq n'$. Em particular, se $n' = 1$, então $P(n)$ vale para todo $n' \in \mathbb{N}$.

Teorema 4.2.1 (Teorema Fundamental da Aritmética): Todo número inteiro $n >$

1 ou é primo ou pode ser escrito como um produto de números primos. Essa representação como produto de primos é única, a menos da ordem dos fatores.

Demonstração: Baseada em Santos (1998). A prova é dividida em duas partes.

Existência da fatoração. Empregaremos o princípio da boa ordem.

Caso n primo. Se n já é primo, sua fatoração consiste apenas dele próprio, nada resta demonstrar.

Caso n composto. Peguemos o menor divisor positivo de n que seja maior que 1, e vamos chamá-lo de p_1.O número p_1 é primo, pois, se não fosse, possuiria um divisor $1 < a < p_1$ que também dividiria n, contradizendo a minimalidade de p_1. Escreva $n = p_1 \cdot n_1$ com $1 < n_1 < n$. Se n_1 é primo, temos $n = p_1 \cdot n_1$. Caso contrário, aplique o mesmo processo a n_1, obtendo uma sequência estritamente decrescente $n > n_1 > n_2 > \cdots > n_k > 1$. Essa sequência é finita. Logo, em algum passo obtemos um n_k primo. Assim, como os primos na seqüência $p_1, p_2, \ldots, p_k$ não são, necessariamente, distintos, n terá, em geral, a forma, $n = {p_1}^{a_1} \cdot {p_2}^{a_2} \cdots {p_k}^{a_k}$ chamada de decomposição canônica, com p_i primos e $a_i \in \mathbb{N}$. Portanto, toda fatoração existe.

Unicidade da Fatoração.

Aplicaremos indução sobre n.

Base. Para $n = 2$, a decomposição é exclusivamente 2.

Hipótese indutiva. Suponha que todo k com $2 \leq k < n$ possua decomposição única em primos.

Passo indutivo. Se n é primo, a unicidade é imediata. Se n é composto, admita duas decomposições distintas, $n = p_1 p_2 \ldots p_s = q_1 q_2 \ldots q_r$. O primo p_1 divide $q_1 q_2 \ldots q_r$, pelo Lema de Euclides, divide algum q_j. Reordenando os q, pode-se supor $p_1 \mid q_1$, logo $p_1 = q_1$. Dividindo ambos os lados por p_1, obtém-se $\frac{n}{p_1} = p_2 \ldots p_s = q_2 \ldots q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese indutiva garante que $s = r$ e, salvo ordem, os fatores restantes coincidem. Assim, a fatoração de n é única.

□

O teorema acima nos permite obter dois resultados importantes para o cálculo do número de divisores, máximo divisor comum e o mínimo múltiplo comum. A unicidade permite contar divisores com exatidão e aplicar regras claras para obter o mdc e o mmc, tornando esses cálculos precisos e bem definidos. Os resultados abaixo podem ser encontrados em Hefez (2022).

Proposição 4.2.1. Seja $n = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r}$ um número natural escrito como produto de potências de primos distintos p_i com expoentes $\alpha_i \in \mathbb{N}$. Se m é um divisor positivo de n, então m tem a forma, $m = {p_1}^{\beta_1}.{p_2}^{\beta_2} \ldots {p_r}^{\beta_r}$ onde $0 \leq \beta_i \leq \alpha_i$ para cada $i = 1, \ldots, r$.

Demonstração: Seja m um divisor positivo de n. Se p é um fator primo de m com expoente β, ou seja, p^{β} é a maior potência de p que divide m, então p^{β} também deve dividir n. Como $p^{\beta} | n$ e $n = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r}$, e os p_i são primos distintos, o primo p deve ser igual a um dos p_i. Digamos $p = p_j$ para algum j. Então, a potência ${p_j}^{\beta}$ deve dividir ${p_j}^{\alpha_j}$. Isso implica que o expoente β não pode ser maior que α_j, ou seja, $0 \leq \beta \leq \alpha_j$. Isso se aplica a todos os fatores primos de m. Se um primo p_k da fatoração de n não aparece na fatoração de m, seu expoente β_k em m é 0, o que ainda satisfaz $0 \leq \beta_k \leq \alpha_k$.

□

O número de divisores positivos de um inteiro n, cuja fatoração em primos distintos é $n = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r}$,onde cada $\alpha_i \in \mathbb{N}$, é dado pela fórmula:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Uma justificativa seria que qualquer divisor positivo m de n terá a forma $m = {p_1}^{\beta_1}.{p_2}^{\beta_2} \ldots {p_r}^{\beta_r}$, onde cada expoente β_i deve satisfazer a condição $0 \leq \beta_i \leq \alpha_i$. Isso significa que para cada primo p_i na fatoração de n, o expoente β_i no divisor m pode assumir $\alpha_i + 1$ valores possíveis, ou seja, $0,1,2, \ldots, \alpha_i$. Como a escolha de cada expoente β_i é independente das escolhas dos outros expoentes, o número total de divisores positivos de n é obtido multiplicando-se o número de escolhas possíveis para cada expoente.

Exemplo 4.2.1. Você já se perguntou por que uma volta completa tem 360°, e não um número como 100º, que parece mais exato para nós? A resposta está na quantidade de divisores que um número possui. Vamos investigar o número 360.

Solução. Primeiro, escrevemos sua fatoração em primos, $360 = 2^3 \cdot 3^2 \cdot 5^1$. Aqui, $\alpha_1 = 3$, $\alpha_2 = 2$ e $\alpha_3 = 1$. Aplicando a fórmula, $d(360) = (3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = 24$. Portanto, o número 360 possui 24 divisores positivos. Agora, vamos comparar com o número 100. Por que não uma volta de 100°? A fatoração de 100 é $100 = 2^2 \cdot 5^2$. Os expoentes são $\alpha_1 = 2$ e $\alpha_2 = 2$. Aplicando a fórmula: $d(100) = (2 + 1)(2 + 1) = 3 \cdot 3 = 9$. O número 100 possui apenas 9 divisores positivos.

Um círculo de 360º é muito flexível. Ele pode ser dividido de maneira exata em metades, terços, quartos, quintos, sextos, oitavos e diversas outras frações. Os povos antigos,

como os babilônios, consideravam essa alta divisibilidade muito útil em campos como a astronomia, arquitetura e marcação do tempo (Eves, 2011).

Exemplo 4.2.2. Um número inteiro m tem exatamente 18 divisores positivos. Sabendo que $m = 2^2 \cdot 3^{\alpha} \cdot 5^{\beta}$, onde $\alpha, \beta \in \mathbb{N}$, determine todos os pares (α, β) possíveis.

Solução. Temos que $d(m) = 18$. Usando a fórmula, temos que $d(m) = (2+1)(\alpha+1)(\beta+1) = 3(\alpha+1)(\beta+1) = 18 \Rightarrow (\alpha+1)(\beta+1) = 6$. Agora, procuramos todos os pares de inteiros positivos que multiplicados dão 6. Portanto, os pares (α, β) possíveis são, (0,5), (1,2), (2,1), (5,0).

Sejam dois números naturais com suas decomposições canônicas, $n = {p_1}^{\alpha_1}.{p_2}^{\alpha_2} \ldots {p_r}^{\alpha_r}$ e $m = {p_1}^{\beta_1}.{p_2}^{\beta_2} \ldots {p_r}^{\beta_r}$ onde $p_1, p_2, \ldots, p_r$ são primos distintos, e $\alpha_i, \beta_i \in \mathbb{N}$, podendo ser zero se o primo não aparecer. Para calcular o mdc, encontre os fatores primos comuns às duas decomposições. Para cada fator primo comum, tome a menor potência (menor expoente) com que ele aparece nas decomposições. O mdc é o produto dos fatores primos comuns, cada um elevado à sua respectiva potência menor.

Para calcular o mmc encontre todos os fatores primos aparecendo em pelo menos uma das decomposições (fatores comuns e não comuns). Para cada fator primo, tome a maior potência (maior expoente) com que ele aparece nas decomposições. O mmc é o produto dos fatores primos, cada um elevado sua maior potência. Simplificando, temos $mdc(m,n) = \prod_{i=1}^{r} {p_i}^{\min(\alpha_i, \beta_i)}$ e o $mmc(m,n) = \prod_{i=1}^{r} {p_i}^{\max(\alpha_i, \beta_i)}$. Uma demonstração deste fato pode ser encontrada em Hefez (2022).

Exemplo 4.2.3. Sejam os inteiros positivos 360 e 210. Calcule o $mdc(360,210)$ e o $mmc(360,210)$.

Solução. Decomposição em fatores primos. Para 360, $360 = 2^3 \cdot 3^2 \cdot 5^1$. Para 210, $210 = 2 \cdot 3 \cdot 5 \cdot 7$. O mdc é o produto dos fatores primos comuns, cada um elevado ao menor expoente, $mdc(360,210) = 2 \cdot 3 \cdot 5 = 30$. O mmc é o produto de todos os fatores primos envolvidos (comuns e não comuns), cada um elevado ao maior expoente, $mmc(360,210) = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7 = 2520$.

O TFA é fundamental porque muitas das propriedades dos inteiros e de operações tal como o cálculo do mdc e mmc podem ser derivadas, ou simplificados, do teorema da

fatoração em primos. Isto leva-nos a concluir que o ensino do TFA não deve restringir-se apenas à sua enunciação, mas, sim, incluir atividades que permitam aos alunos explorar a fatoração e experimentar concretamente a unicidade. A simplicidade do teorema termina por disfarçar a sua profundeza, e na incapacidade para aplicação do mesmo em contextos também muito diversos.

4.3 A Infinitude dos Números Primos

O fato de existirem infinitos números primos, ou seja, de que a sequência de números primos $2, 3, 5, 7, 11, 13, \ldots$ não tem fim, constitui um dos teoremas mais antigos e importantes da Matemática. Conforme mencionado no capítulo histórico, foi Euclides quem primeiro registrou uma prova desse resultado, no Livro IX d'*Os Elementos*. Sua demonstração é muito bonita pela simplicidade e elegância, frequentemente citada como um exemplo de prova por contradição. A seguir, reapresentamos essa prova com a linguagem moderna.

Teorema 4.3.1 (Euclides): O conjunto dos números primos é infinito.

Demonstração (Euclides, c. 300 a.C.): Suponha, por absurdo, que o conjunto dos números primos é finito. Sejam eles $P = \{p_1, p_2, \ldots\ p_k\}$, onde p_k é o maior primo. Considere o número N formado pelo produto de todos esses primos mais um, $N = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1$. Temos dois casos a considerar.

Caso 1: N é primo. Mas N é maior que qualquer primo da lista P. Isso contradiz a suposição de que p_k é o maior primo e que a lista P contém todos os primos.

Caso 2: N é composto. Se N é composto, então N deve ser divisível por algum primo p da nossa lista finita P pois, por suposição, P contém todos os primos. Seja $p_j \in P$ tal que $p_j | N$. Sabemos também que p_j divide o produto $(p_1 \cdot p_2 \cdot \ldots \cdot p_k)$ pois, p_j é um dos fatores. Se $p_j | N$ e $p_j | (p_1 \cdot p_2 \cdot \ldots \cdot p_k)$, então p_j deve dividir a diferença entre eles, $p_j | N - (p_1 \cdot p_2 \cdot \ldots \cdot p_k)$. Mas $N - (p_1 \cdot p_2 \cdot \ldots \cdot p_k) = 1$. Então, $p_j | 1$. Isso é impossível, pois todo número primo é maior que 1. Ambos os casos levam a uma contradição. Portanto, a suposição inicial de que o conjunto dos números primos é finito deve ser falsa. Logo, existem infinitos números primos.

□

Esta demonstração é acessível a estudantes do Ensino Médio e poderia, com uma adaptação adequada, ser feita em sala de aula, os alunos já têm familiaridade com divisão e noções básicas de lógica. Ela introduz de forma interessante a prova por absurdo. Uma possível atividade que está descrita na sequência didática do capítulo 6.

Ferreira (2014) compila seis demonstrações distintas da infinitude dos números primos. A primeira é a clássica prova que fizemos acima. A segunda abordagem recorre aos Números de Fermat, mostrando que, como quaisquer dois desses números são primos entre si, deve haver uma infinidade de divisores primos distintos. A terceira prova utiliza os Números de Mersenne, argumentando que qualquer fator primo de 2^{p-1}, onde p é primo é maior que p, o que seria impossível se existisse um maior primo.

Ainda de acordo com o mesmo autor, a quarta demonstração emprega o cálculo elementar, estabelecendo uma relação entre o logaritmo natural e a função de contagem de primos $\pi(x)$ para concluir que, sendo o logaritmo ilimitado, $\pi(x)$ também o é. Uma quinta prova, de Furstenberg, utiliza a topologia, definindo uma topologia nos inteiros onde a finitude dos primos implicaria que o conjunto $\{-1,1\}$ seria aberto, uma contradição.

Por fim, a sexta demonstração, atribuída a Paul Erdős, prova que a série dos inversos dos números primos diverge; se a série convergisse, seria possível mostrar que a contagem de números inteiros até um N arbitrário seria inconsistente. Essa prova foi dada primeiro por Euler (séc. XVIII).

4.4 O Crivo de Eratóstenes: Um Algoritmo para Encontrar Primos

Um método prático para identificar números primos foi desenvolvido por Eratóstenes de Cirene (c. 276-194 a.C.), um erudito que dirigiu a Biblioteca de Alexandria e se destacou em diversas áreas como geografia e astronomia. Seu procedimento, conhecido como Crivo de Eratóstenes, é o um algoritmo sistemático conhecido para gerar uma lista de todos os números primos até um determinado limite (Boyer e Merzbach, 2012). E segundo Eves (2011, p. 623) “Os principais resultados obtidos na Antiguidade foram a prova da infinitude dos primos e o Crivo de Eratóstenes”.

O método, conforme descrito por Boyer e Merzbach (2012) e Coutinho (2015), funciona da seguinte maneira:

1. Liste todos os números naturais de 2 até n.
2. Identifique o primeiro número da lista, 2, como primo. Em seguida, risque todos os múltiplos de 2 maiores que ele (4, 6, 8, ...).
3. Identifique o próximo número não riscado, 3, como primo. Risque todos os múltiplos de 3 maiores que ele (6, 9, 12, ...).
4. Identifique o próximo número não riscado, 5, como primo. Risque todos os múltiplos de 5 maiores que ele (10, 15, 20, ...).

5. Continue este processo. O próximo número não riscado será 7, depois 11, e assim por diante.

6. O processo de identificar o próximo primo p e riscar seus múltiplos pode parar quando p for tal que $p^2 > n$. Todos os números que permanecerem sem ser riscados na lista são os primos menores ou iguais a n.

Exemplo 4.4.1. Tomando $n = 30$, temos

Lista inicial:

$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30$

Risque os múltiplos de 2:

Ficam: $2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29$

Risque os múltiplos de 3:

Ficam: $2, 3, 5, 7, 11, 13, 17, 19, 23, 25, 29$

Risque os múltiplos de 5:

Ficam: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$

Como $7^2 = 49 > 30$, então pare. Não é preciso continuar.

Os números que sobraram são os primos até 30: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$

A justificativa para a condição de parada $p^2 > n$ é que qualquer número composto $k \leq n$ deve ter pelo menos um fator primo q tal que $q \leq \sqrt{n}$ (ou $q^2 \leq n$). Se todos os fatores primos de k fossem maiores que $\sqrt{n}$, seu produto seria maior que n . Portanto, ao eliminar os múltiplos de todos os primos até $\sqrt{n}$, garantimos a eliminação de todos os números compostos até n (Coutinho, 2015).

Coutinho (2015) menciona que o nome "crivo" significa peneira, pois o método funciona deixando passar apenas os primos. O Crivo de Eratóstenes, embora ineficiente para números muito grandes, é conceitualmente importante como algoritmo de geração de primos.

4.5 O Pequeno Teorema de Fermat

De acordo com Boyer e Merzbach (2012), apesar de o teorema levar o nome de Fermat, foi Leonhard Euler quem publicou a primeira demonstração em 1736. Contudo, Gottfried Wilhelm Leibniz já havia deixado registrada uma versão anterior em um de seus manuscritos. A demonstração de Euler é considerada "surpreendentemente elementar" e utiliza o método da Indução Matemática. Posteriormente, Euler ampliou o teorema por meio de sua

função φ de Euler, demonstrando que $a^{\varphi(m)} - 1$ é divisível por m, desde que a seja primo com m.

Esta seção fundamenta-se nos resultados apresentados por Hefez (2022). Antes de enunciar e demonstrar o teorema principal, faz-se necessário apresentar o seguinte lema:

Lema 4.5.1. Seja p um número primo, então p divide $\binom{p}{k}$, onde $0 < k < p$.

Demonstração: Sabemos que o número binomial pode ser escrito como, $\binom{p}{k} = \frac{p(p-1)\ldots(p-k+1)}{k!}$. Isso implica que $k!\binom{p}{k} = p(p-1)\ldots(p-k+1)$, então p divide $k!\binom{p}{k}$. Como p é primo e $k < p$, p não divide nenhum dos fatores de $k! = 1 \cdot 2 \cdot \ldots \cdot k$. Portanto, o máximo divisor comum de p e $k!$ é 1. Uma vez que p divide o produto $k!\binom{p}{k}$ e é primo com $k!$, pelo Lema de Gauss, p deve dividir $\binom{p}{k}$.

□

Teorema 4.5.1.(Fermat) Seja p um número primo e a um número inteiro, então $a^p - a$ é divisível por p.

Demonstração: Esta prova, atribuída a Euler, utiliza o Princípio da Indução Matemática sobre $a \geq 0$.

Base da Indução: Para $a = 0$, temos que p divide $0^p - 0 = 0$, verdadeiro. Para $a = 1$, temos que p divide $1^p - 1 = 0$, verdadeiro.

Hipótese Indutiva: Suponha que $a^p - a$ é divisível por p para algum inteiro $a \geq 0$.

Passo Indutivo: Devemos mostrar que $(a+1)^p - (a+1)$ é divisível por p. Para isso, usamos a fórmula do binômio de Newton para expandir $(a+1)^p$:

$(a+1)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a^1 + \binom{p}{p}a^0 = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1$. Agora somamos $-(a+1)$ dos dois lados, teremos $(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1 - (a+1) = (a^p - a) + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$. Agora, analisamos a divisibilidade por p de cada parte da soma do lado direito. O termo $a^p - a$ é divisível por p pela nossa hipótese de indução. Os termos $\binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a$ são todos divisíveis por p, pelo lema anterior. Portanto, $p|(a+1)^p - (a+1)$.

□

Corolário 4.5.1. Se um número primo p não é um divisor de um número natural a, então p necessariamente divide o número $a^{p-1} - 1$.

Demonstração: O pequeno teorema de Fermat nos garante que, para qualquer primo p e um inteiro a, p divide o produto $a(a^{p-1} - 1)$. Como por hipótese p não divide a.

Como p é um número primo, então o $mdc(a,p) = 1$. Como sabemos que p divide o produto $a(a^{p-1} - 1)$, então pelo Lema de Gauss $p|\ (a^{p-1} - 1)$.

□

Exemplo 4.5.1. (Hefez, 2022 p. 134) Ache o resto da divisão de 12^{p-1} por p quando p é primo.

Solução: Se o primo p é um divisor de 12. Os únicos primos que dividem 12 são 2 e 3. Se $p = 2$, estamos dividindo $12^{2-1} = 12$ por 2, o resto é 0. Se $p = 3$, estamos dividindo $12^{3-1} = 144$ por 3, o resto é 0. Se o primo p não é um divisor de 12. Pelo corolário acima, sabemos que p divide $12^{p-1} - 1$. Isso significa que existe um inteiro $k \neq 0$ tal que $12^{p-1} - 1 = kp$, ou $12^{p-1} = kp + 1$. Logo, pela divisão euclidiana, o resto é 1.

Segundo Coutinho (2005) o pequeno teorema de Fermat tem uma ampla variedade de aplicações na teoria dos números. Ele destaca que o teorema é usado como uma ferramenta para facilitar o cálculo de potências elevadas na aritmética modular. Além disso, o teorema serve como base para testes que detectam números compostos sem a necessidade de fatoração, o que leva ao conceito de pseudoprimos e a algoritmos mais avançados, como o teste de Miller.

Ainda segundo o autor sua utilidade também se estende à fatoração de números com estruturas específicas, como os números de Mersenne e de Fermat. Por fim, o teorema é fundamental para o teorema de Euler, uma generalização crucial para comprovar a eficácia da criptografia RSA.

4.6 O Teorema dos Números Primos (TNP)

Com a certeza da infinitude dos números primos dada na seção 4.3, o próximo desafio é entender sua densidade e distribuição. Existe alguma ordem ou padrão na sua distribuição aparentemente aleatória entre os inteiros? A resposta a esta pergunta é encontrada em um dos resultados mais importantes da teoria analítica dos números, o teorema dos números primos.

Este teorema não oferece uma fórmula para encontrar o próximo primo, mas descreve a densidade assintótica dos primos, revelando uma regularidade. A jornada para a sua demonstração final, conforme detalhado em Boyer e Merzbach (2012), foi um esforço gigantesco que se estendeu por mais de um século, envolvendo as contribuições de algumas das mentes matemáticas mais brilhantes da Europa.

Ainda de acordo com Boyer e Merzbach (2012) o primeiro passo à formulação do teorema surgiu no final do século XVIII, a partir de observações empíricas. O matemático francês Adrien Marie Legendre (1752-1833), após a contagem de um grande número de primos, propôs uma conjectura para aproximar a quantidade de primos existentes até um determinado número. Em sua obra de 1797-1798, ele sugeriu que o número de primos menores ou iguais a um inteiro n, uma função denotada por $\pi(n)$, poderia ser aproximado pela fórmula $\pi(n) \sim \frac{n}{\ln(n) - 1{,}08366}$.

Para quantificar o número de primos até um certo ponto, define-se a função de contagem de primos, denotada por $\pi(x)$ (lê-se "pi de x", sem relação com a constante $\pi \approx 3{,}14159$ ...). Para qualquer número inteiro $x > 0$, $\pi(x)$ é definida como o número de primos p tais que $p \leq x$.

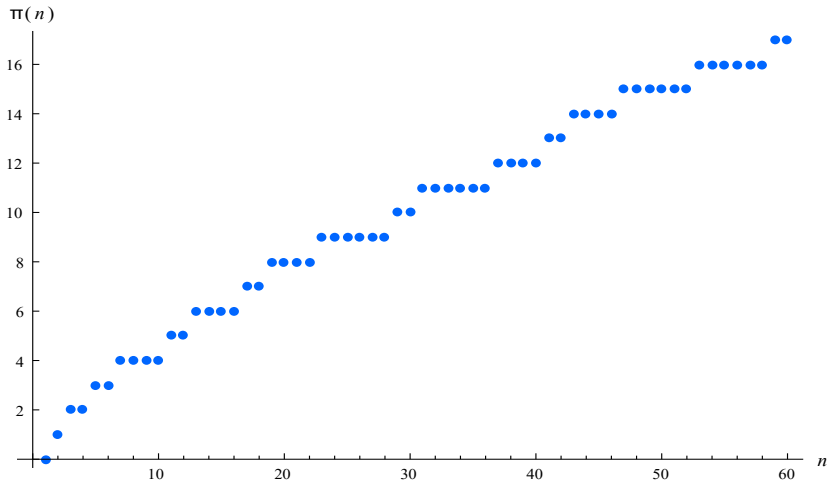
Exemplo 4.6.1.

a) Os primos menores ou iguais a 10 são 2, 3, 5 e 7. Portanto, π(10)=4.

b) Os primos menores ou iguais a 20 são 2, 3, 5, 7, 11, 13, 17 e 19. Assim, π(20)=8.

Graficamente, a função $\pi(x)$ comporta-se como uma função escada. Ver Gráfico 1.

Gráfico 1 - Os valores de $\pi(x)$ para os primeiros 60 inteiros positivos



Fonte: https://clik.now/IS5m

A mesma ideia de Legendre já havia sido pensada a uma mente mais afiada, de forma independente e talvez bem antes. Carl Friedrich Gauss (1777-1855), ainda em sua adolescência, investigou a distribuição dos primos e, em uma anotação em uma tabela de logaritmos, formulou o que é essencialmente o enunciado moderno do teorema (Boyer e Merzbach, 2012).

Ele afirmou que o número de primos menores que um dado inteiro a se aproxima assintoticamente do quociente $\frac{a}{\ln(a)}$ à medida que a cresce indefinidamente. A formulação de Gauss era mais simples e mais precisa em seu caráter assintótico do que a de Legendre. No entanto, Gauss, nunca publicou este resultado. Não se sabe se ele possuía uma demonstração formal para sua conjectura, que permaneceu desconhecida para o mundo matemático por muitos anos (Boyer e Merzbach, 2012).

Conforme Hefez (2022) em uma formulação mais moderna, esta observação de Gauss sugeria que a própria função $\pi(x)$ poderia ser bem aproximada pela expressão $\frac{x}{lnx}$. Esta conjectura foi finalmente provada de forma independente por J. Hadamard e Ch. de la Vallée-Poussin por volta de 1900, dando origem ao teorema dos números primos. Formalmente, o teorema afirma que, $\lim_{x\to\infty} \frac{\pi(x)}{x}\left(\frac{1}{lnx}\right)^{-1} = 1$. Ou seja, o limite da razão entre $\pi(x)$ e a aproximação $\frac{x}{lnx}$ tende a 1 à medida que x tende ao infinito. Isso significa que, embora a aproximação não seja exata, o erro relativo torna-se cada vez menor para números maiores.

A demonstração original do teorema era muito complexa. Um avanço significativo ocorreu em 1949, quando P. Erdős e A. Selberg desenvolveram uma prova mais "simples", um feito tão notável que rendeu a Selberg a prestigiosa medalha Fields (Hefez, 2022).

A demonstração original é extremamente complexa, mesmo a prova mais "simples" de P. Erdős e A. Selberg ainda é muito complicada para nossos objetivos aqui. Portanto uma demonstração do TNP pode ser encontrada em Vieira (2023).

4.7 Conjecturas Célebres sobre Números Primos

Apesar de muitos teoremas terem sido comprovados, a teoria dos números primos é reconhecida por suas conjecturas duradouras, algumas permanecem sem solução e continuam a impulsionar a pesquisa matemática. Nesta seção, abordaremos algumas delas. O fato de o professor mencioná-las em sala despertará a curiosidade dos alunos.

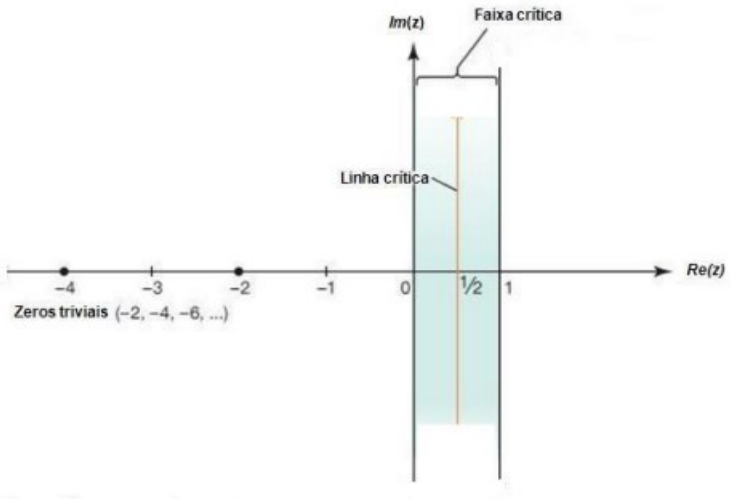
A Hipótese de Riemann: De acordo com Gaspareti (2014) foi elaborada pelo matemático alemão Bernhard Riemann (1826-1866) em 1859, é considerada como um dos desafios mais importantes da Matemática Moderna. Sua importância é tão grande que se destaca como o único desafio presente tanto na lista de 23 problemas de David Hilbert, apresentada em 1900, quanto na relação dos sete Problemas do Milênio, divulgada em 2000 pelo Instituto Clay de Matemática disponível em (https://clik.now/mGDc). A procura pela solução, que é

recompensada com um prêmio de um milhão de dólares, é impulsionada pela íntima relação que a hipótese mantém com a distribuição dos números primos, o que lhe conferiu a denominação de "O Santo Graal da Matemática".

Segundo Eves (2011) o estudo que levou à hipótese de Riemann teve suas raízes nos trabalhos de Leonhard Euler, que investigou as conexões entre a teoria dos números primos e a série $\sum \frac{1}{s^2}$. "A soma da série define a função $\zeta(s)$, que veio a se tornar conhecida como função zeta de Riemann" (Eves, 2011 p.614).

Ao analisar a função zeta de variável complexa, ζ(z), Riemann descobriu que ela possui zeros triviais (os números inteiros pares negativos) e uma infinidade de zeros não triviais, localizados em uma região específica do plano complexo, ver Figura 4 abaixo, denominada faixa crítica (Gaspareti, 2014).

Figura 4 - Domínio da função zeta



Fonte: Gaspareti (2014, p. 44)

A hipótese de Riemann, conforme descrita por Gaspareti (2014), é a conjectura de que a parte real de todos os zeros não triviais da função zeta é exatamente $\frac{1}{2}$, o que os alinharia perfeitamente sobre a chamada linha crítica.

A capacidade de Riemann, conforme mencionado por Gaspareti (2014), consistiu em identificar que os zeros não triviais da função zeta atuam como fatores de correção para a fórmula aproximada de Gauss. A posição de cada zero é fundamental para determinar a quantidade precisa de números primos até um valor N especificado. Assim, a confirmação da hipótese não apenas atestaria a posição dos zeros, como também proporcionaria um controle exato acerca do erro na contagem dos números primos, mostrando a ordem oculta ao seu aparente desarranjo.

Conjectura dos Primos Gêmeos: Um conhecido problema não resolvido na teoria dos números é a conjectura dos primos gêmeos. Ela se pergunta se há infinitos pares de números primos que diferem entre si por 2. Embora seja uma das conjecturas mais antigas da Matemática, originando-se na Grécia Antiga por volta de 250 a.C., ainda não existe uma prova que a confirme ou a refute (Coelho, 2021). Vejamos os exemplos iniciais de primos gêmeos.

(3, 5); (5, 7); (11, 13); (17, 19); (29, 31); (41, 43) ;(59, 61) ;(71, 73).

De acordo com Boyer e Merzbach (2012) Hilbert acreditava que,

> uma demonstração da conjetura de Riemann, de que os zeros da função zeta, excetuados os zeros inteiros negativos, têm todos a parte real igual a um meio. Uma demonstração disso, ele pensava, poderia levar a uma demonstração da familiar conjetura sobre a infinidade de pares de primos (Boyer e Merzbach, 2012 p. 413).

Em 1915, o matemático Viggo Brun provou que a soma dos inversos dos primos gêmeos converge para um valor finito, denominado Constante de Brun, que é cerca de 1,9021605823…. Se a série divergir, isso demonstraria a presença de infinitos pares de primos gêmeos. Apesar de significativo, o resultado de Brun não resolve a conjectura. No entanto, indica que, se houver infinitos pares de primos, eles se afastam cada vez mais uns dos outros. Um avanço considerável ocorreu em 2013, quando o matemático Yitang Zhang provou que existem infinitos pares de primos cuja diferença não excede 70 milhões (Coelho, 2021).

Ainda conforme Coelho (2021) inspirado pelo trabalho de Zhang, o projeto PolyMath8b, com a participação de James Maynard, conseguiu reduzir essa lacuna máxima para 246.

Apesar desses progressos na compreensão das lacunas entre os primos, a conjectura original, que se refere especificamente à lacuna de tamanho 2, permanece sem solução.

Conjectura de Goldbach: A Conjectura de Goldbach é um dos problemas não resolvidos mais interessantes da Matemática, sendo importante por sua durabilidade e pela simplicidade de sua formulação.

Sua origem no século XVIII é um episódio importante na história da teoria dos números, área que estava ganhando novo impulso naquele período. A conjectura teve origem em uma carta datada de 1742, trocada entre o matemático prussiano Christian Goldbach (1690-1764) e o renomado Leonhard Euler, conforme relatam historiadores como Eves (2011) e Boyer e Merzbach (2012). Euler foi o responsável por atribuir à proposição sua forma mais elegante e duradoura, convertendo uma questão específica em um desafio universal.

A versão mais famosa, conhecida como conjectura forte, afirma algo que pode ser verificado por qualquer estudante do Ensino Médio, mas que ainda não foi provado de forma geral. Conforme define Pereira (2017): “Todo número par maior ou igual a 4 pode ser escrito

como a soma de dois números primos" (Pereira, 2017, p. 27). Veja a Tabela 1 para alguns exemplos.

Tabela 1 - Exemplos da Conjectura Forte de Goldbach

Número par	Decomposições como soma de dois primos
4	2+2
6	3+3
8	3 + 5
10	3 + 7, 5 + 5
12	5 + 7
14	3 + 11, 7 + 7
16	3 + 13, 5 + 11

Fonte: elaborada pelo autor.

Além da conjectura forte, existe uma versão ternária. De acordo com Pereira (2017), a conjectura fraca de Goldbach, que postula que todo número ímpar maior que 5 é a soma de três primos, teve um destino diferente. Após séculos de incerteza, essa versão foi finalmente demonstrada em 2013 pelo matemático peruano Harald Helfgott, um avanço importante que resolveu uma parte significativa do legado de Goldbach.

Apesar desse avanço, a prova da conjectura fraca não forneceu um caminho para a solução da forte. Assim, o problema original permanece um problema em aberto na Matemática.

A duração dessas conjecturas, algumas por mais de dois séculos, mostra a incrível complexidade escondidas na aparente simplicidade dos números primos. A busca por suas soluções tem sido um incentivo para o desenvolvimento de muitas áreas da Matemática.

5 O POTENCIAL DIDÁTICO DOS NÚMEROS PRIMOS NO ENSINO BÁSICO

Após a breve descrição da matemática dos números primos, concentremo-nos no contexto educacional. Como esse tópico está presente no currículo escolar brasileiro? Quais desafios ou estratégias podem ser destacados no ensino deste tema? Como este tema é apresentado nos livros didáticos? Este capítulo tenta responder a estes e outros questionamentos, e discute o potencial didático do tema.

5.1 Análise das Diretrizes Curriculares Nacionais

O ensino da Matemática no Brasil é orientado por documentos oficiais que definem diretrizes, competências e habilidades a serem aprimoradas. Para contextualizar qualquer proposta didática, é essencial examinar como esses documentos abordam o estudo dos números primos e da divisibilidade.

5.1.1 LDB (Lei de Diretrizes e Bases da Educação Nacional - Lei 9.394/96)

A LDB não detalha conteúdos específicos para a Matemática, como números primos, mas em seus artigos citados abaixo dá a finalidade da educação e a obrigatoriedade de se estudar Matemática.

> Art. 2º. A educação, dever da família e do Estado, inspirada nos princípios de liberdade e nos ideais de solidariedade humana, tem por finalidade o pleno desenvolvimento do educando, seu preparo para o exercício da cidadania e sua qualificação para o trabalho (Brasil, 1996 p.1).

A LDB estabelece, em seu artigo 26, §1º, que a organização curricular é uma responsabilidade compartilhada, dividindo-a entre uma Base Nacional Comum obrigatória e uma parte diversificada, que fica a cargo dos sistemas de ensino para atender às peculiaridades locais e regionais (Brasil, 1996).

> §1º Os currículos a que se refere o caput devem abranger, obrigatoriamente, o estudo da língua portuguesa e da matemática, o conhecimento do mundo físico e natural e da realidade social e política, especialmente do Brasil (Brasil, 1996 p.10).

Assim, a LDB dá à Matemática um status de componente curricular essencial, delegando a definição de conteúdos e habilidades específicas a outras normas e aos sistemas de ensino.

5.1.2 PCN (Parâmetros Curriculares Nacionais - Matemática)

Publicados a partir de 1997, os PCN foram, por muitos anos, o principal referencial para a elaboração de currículos e materiais didáticos. No que tange aos números e operações para o Ensino Fundamental, os PCN do Terceiro Ciclo (correspondente aproximadamente ao 6º e 7º anos) mencionam que

> Conceitos como os de múltiplo e divisor de um número natural ou o conceito de número primo podem ser abordados neste ciclo como uma ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores, e não como assunto novo, desvinculado dos demais. Além disso, é importante que tal trabalho não se resuma à apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum sem compreender as situações-problema que esses conceitos permitem resolver (Brasil, 1998 p.66).

De acordo com Farias (2016) apesar dessas orientações, a falta de uma orientação padronizada nos PCNs sobre como ensinar os números primos resulta na transferência da responsabilidade de definir a abordagem pedagógica para as próprias escolas.

E esta falta de especificidade e detalhamento pode ter contribuído para a persistência de abordagens superficiais em muitos materiais didáticos.

5.1.3 BNCC (Base Nacional Comum Curricular - Matemática)

Homologada em 2017 (Ensino Fundamental) e 2018 (Ensino Médio), a BNCC é o documento normativo mais recente que define o conjunto de aprendizagens essenciais que todos os alunos devem desenvolver ao longo das etapas e modalidades da Educação Básica.

Vejamos um detalhamento quanto aos números inteiros. No Ensino Fundamental, anos finais na unidade temática números, a BNCC aborda explicitamente os conceitos relacionados à divisibilidade e, implicitamente, aos números primos. Para o 6º Ano, temos as seguintes habilidades:

> (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 (Brasil, 2018 p.301).

Para o 7º Ano, a habilidade,

> (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos (Brasil, 2018 p.307).

Embora números primos não sejam o foco central explícito desta habilidade no 7º ano, o estudo aprofundado de divisores e múltiplos, incluindo MDC e MMC, naturalmente conduz à necessidade de compreender os números primos e a fatoração.

O objetivo final é o desenvolvimento do letramento matemático, que capacita o estudante a raciocinar, representar e argumentar, utilizando os conceitos da Matemática para compreender e atuar sobre a realidade (Brasil, 2018).

Esta análise mostra uma progressão nas diretrizes, com a BNCC visando mais transparência nas competências a serem aprimoradas e fomentando métodos menos repetitivos e mais investigativos, o que é motivador para um ensino mais eficiente dos números primos.

5.2 Dificuldades de Ensino e Aprendizagem sobre Números Primos

A deficiência no ensino e aprendizado de números primos na educação básica é um problema complexo, que se revela tanto nas dificuldades enfrentadas pelos estudantes quanto nas falhas do sistema educacional. Quando os alunos chegam ao Ensino Médio sem dominar conceitos fundamentais, a aprendizagem se transforma em um desafio. Farias (2016) afirma que isso poderia ser reduzido se os estudantes fossem capazes de decompor um número em fatores primos.

Uma pesquisa aplicada por Farias (2016) com 100 estudantes revelou a dimensão dessa dificuldade, mostrando que a grande maioria “não tem o conhecimento mínimo esperado para a série na qual se encontram sobre os números primos" (Farias, 2016 p. 12). Os resultados indicam que apenas 12% dos alunos souberam definir corretamente o que é um número primo, e um percentual ainda menor, de 2%, conseguiu realizar a fatoração de 7000 (Farias, 2016).

Essa falha no aprendizado está diretamente ligada à forma como o conteúdo é apresentado. Farias (2016) argumenta que a abordagem dos livros didáticos é frequentemente superficial e repetitiva, com pouca ênfase na conceituação e sem um contexto histórico que demonstre a real importância do tema.

As dificuldades também se estendem aos futuros docentes. Oliveira e Fonseca (2017) identificaram que futuros professores exibem "substancial dificuldade na compreensão da unicidade da decomposição de números inteiros em fatores primos" (Oliveira e Fonseca, 2017 p. 885), um pilar do TFA. Essa dificuldade se manifesta na incapacidade de aplicar o próprio conceito de primalidade e de conectar a definição de número composto à sua decomposição única em fatores primos (Oliveira e Fonseca, 2017).

De acordo com Resende (2007), do ponto de vista do ensino, um dos principais desafios reside na formação do próprio professor, que frequentemente possui uma compreensão superficial sobre a importância do tema. Essa barreira é expressa na conjectura de um dos entrevistados de que a pouca presença de questões sobre inteiros na educação básica se deve ao fato de que "os professores não têm familiaridade para mexer com esse tipo de questão" (Resende, 2007, p. 141).

Adicionalmente, quando se fala sobre o ensino nas universidades, a abordagem pedagógica costuma ser um obstáculo, pois, segundo outro especialista, "a forma que eles estão ensinando é muito inacessível à maioria" (Resende, 2007, p. 159), em parte pela natureza abstrata do conteúdo, que carece de modelos visuais ou padrões de resolução fáceis de transmitir (Resende, 2007).

Outra dificuldade importante identificada pela autora diz respeito à própria concepção da demonstração matemática. Muitos licenciandos percebem as provas matemáticas apenas como procedimentos formais desconectados da prática docente real, negligenciando que as demonstrações têm funções diferenciadas na Matemática acadêmica e na escolar (Resende, 2007).

Portanto, é claro que a superação desse desafio requer uma abordagem abrangente, que inclua desde a revisão dos materiais didáticos até uma reestruturação significativa da formação de professores.

5.3 Análise da Abordagem dos Números Primos em Livros Didáticos

Esta análise reavalia a abordagem pedagógica utilizada para o tema dos números primos. O objetivo é analisar a eficácia pedagógica da jornada proposta ao aluno do 6º ano, observando como o conteúdo didático transforma um conceito abstrato em uma descoberta concreta e intelectualmente motivadora. Três livros didáticos foram analisados:

i) TEIXEIRA, Lilian Aparecida *et al.* (ed.). **Superação:** matemática 6. ano: manual do professor. 1. ed. São Paulo: Moderna, 2022.

ii) BIANCHINI, Edwaldo. **Matemática Bianchini**: 6. ano: manual do professor. 10. ed. São Paulo: Moderna, 2022.

iii) PATARO, Patricia Rosana Moreno; BALESTRI, Rodrigo Dias. **Matemática essencial**: 6. ano: ensino fundamental: anos finais. 1. ed. São Paulo: Scipione, 2018.

i) O assunto em questão é abordado na unidade 3. A estrutura da unidade se desenvolve por conduzir o estudante em um processo de construção do saber, em vez de apenas expor fatos. A definição de número primo não é apresentada no início da seção. O texto propõe que o estudante execute uma tarefa prática, enumerar os divisores de 1 a 10.

Ao realizar essa atividade, o aluno nota que alguns números têm apenas dois divisores, ao mesmo tempo que outros têm mais. A definição de primo e composto consiste em reconhecer um padrão que o estudante identificou, tornando o processo de aprendizagem mais dinâmico.

O livro apresenta duas maneiras de reconhecer números primos, o Crivo de Eratóstenes, que é um método visual e algorítmico, e a verificação por divisões sucessivas, que é um método de teste. O livro valida várias maneiras de pensar e demonstra que não existe um único jeito certo de solucionar problemas matemáticos.

As atividades são estruturadas, iniciando com a classificação de números e progredindo para perguntas que exigem um raciocínio mais elaborado, como "Por que o número 1 não é primo?" (Teixeira *et al*, 2022 p. 85) levando a desafios de alta complexidade, como os da OBMEP. Essa progressão atende aos diferentes ritmos de aprendizagem e mantém o aluno engajado, assegurando o incentivo ao raciocínio avançado.

A obra poderia melhorar em alguns aspectos. Por exemplo, a abertura da unidade cita a criptografia, que é uma das aplicações dos números primos. Entretanto, essa ligação não volta na parte dedicada ao assunto. Os números primos constituem uma área de pesquisa viva e contêm muitos enigmas não solucionados, como visto nas seções anteriores desta dissertação.

Para despertar a curiosidade, a abordagem poderia explorar mais esse ponto. Recomenda-se a adição de informações interessantes sobre a infinidade dos números primos, a conjectura de Goldbach, a conjectura dos primos gêmeos, etc. No mais o material tem o grande mérito de tratar o aluno como um ser pensante em uma jornada de construção do saber.

ii) A metodologia do livro é boa em desenvolver o conceito de número primo de forma lógica e gradual. O tema é abordado no Capítulo 4, divisibilidade, de forma adequada ao ensino. A obra estimula o aluno a ser ativo na aprendizagem. Os exercícios propostos ajudam o estudante a descobrir propriedades dos números primos. Esse método valoriza a inteligência do aluno e estimula o raciocínio em vez da memorização.

De modo geral, o livro adota uma filosofia que valoriza a Matemática como uma ciência humana, conforme descrito nas orientações. O livro contribui para tornar o conteúdo

mais humano ao situar os números e suas propriedades em um contexto, mesmo que geral, apresentando-o como uma invenção cultural e histórica.

Embora tenha uma base forte, a abordagem poderia ser mais humanizada ao relacionar os números primos com o mundo atual e com a beleza da Matemática. Perde-se a chance de relacionar números primos com o mundo digital do estudante. Uma aplicação interessante das características dos números primos é a criptografia, que garante a segurança de senhas, transações financeiras e mensagens.

Exibir essa ligação de maneira simplificada mostraria a relevância do conteúdo, alinhando-se à competência de identificar a Matemática como uma ciência capaz de solucionar os desafios tecnológicos contemporâneos.

Os números primos são um mistério matemático que intriga as pessoas há milênios. No entanto, a obra falha ao não abordar curiosidades sobre o tema, como a complexidade de prever a distribuição dos números primos, a busca pelo maior primo conhecido ou a Hipótese de Riemann. Esses tópicos poderiam despertar muita curiosidade nos alunos e transformar o assunto de um item curricular em uma jornada, um dos objetivos da disciplina.

A descoberta de números primos pode ser uma atividade interessante. Para isso, o Crivo de Eratóstenes é uma excelente ferramenta a qual não foi abordada na seção de números primos, diferentemente da obra anterior. Porém poderia ser acrescentada, o que incentivaria mais cooperação e diversão no processo de aprendizagem. Com essas observações, o material ensinaria os números primos e sua importância, despertando uma maior apreciação pela beleza dos mesmos.

iii) O conceito é apresentado somente após uma análise abrangente sobre múltiplos e divisores. A seção "Números primos e números compostos" começa com uma tabela que apresenta os divisores dos números de 1 a 12 a exemplo da primeira obra. Essa metodologia possibilita que o estudante identifique padrões e, de maneira quase independente, reconheça que determinados números (2, 3, 5, 7, 11) têm uma característica especial, são divisíveis por apenas dois números.

O material se diferencia por não considerar a Matemática uma ciência sem história. Existe a preocupação em esclarecer a origem do termo "primo", que vem do latim com o significado de "primeiro", o que contribui para desmistificar a palavra e torná-la mais concreta.

O livro apresenta o Crivo de Eratóstenes e atribui sua criação ao matemático grego Eratóstenes, que viveu aproximadamente 2.300 anos atrás. Isso transforma um processo

matemático em uma invenção histórica, demonstrando que a Matemática é uma construção humana dedicada à resolução de problemas.

Como nas outras obras, o material deixa passar a oportunidade de mostrar mais curiosidades sobre esses números, como as já citadas conjecturas e aplicações na era moderna.

A análise desses livros didáticos demonstra um padrão em suas metodologias, em vez de apenas apresentar a definição, eles orientam o estudante a entender o que são números primos através de atividades que estimulam o pensamento.

Entretanto, a principal falha de todas é a falta de conexão com o tema atual. Perde-se a chance de conectar os primos à criptografia, que protege o mundo digital do aluno, além de incentivar o interesse pelos conhecidos enigmas matemáticos.

Em resumo, os materiais são eficazes ao ensinar o quê, mas não conseguem explicar o motivo desses números serem tão interessantes atualmente, o que impede que um conteúdo obrigatório se torne uma aventura.

5.4 Potencial Didático

O ensino de números primos na educação básica traz diversos benefícios formativos, vejamos alguns exemplos.

Trabalhar com números primos, mesmo que de maneira simples por meio de exercícios de raciocínio lógico e demonstrações, pode ajudar os estudantes a entenderem o que é uma prova matemática. É importante entender que um número composto tem um fator que é menor ou igual à sua raiz quadrada. Isso ajuda a explicar como encontramos os fatores de um número. É importante mencionar que sempre há mais números primos. Isso pode não ser ensinado de maneira formal na escola, mas conversar sobre essas ideias ajuda a pensar melhor sobre Matemática.

Números primos e a maneira de dividir um número em partes menores estão em muitos outros assuntos. O mínimo múltiplo comum e o máximo divisor comum são bastante importantes para lidar com frações. Eles aprendem de maneira prática usando a fatoração em números primos.

Conexões com a história e a cultura da Matemática, conforme discutido na parte sobre história, os números primos foram importantes e fascinantes em resultados belíssimos. Contar uma história sobre Matemática pode deixar a aula mais atrativa. Um exemplo é Fermat. Ele teve uma ideia sobre números primos que deixou muitas pessoas curiosas. Ele fez uma

afirmação que não conseguiram provar por muito tempo. As pessoas tentam entender e descobrir mais sobre isso.

Atualmente, existe uma busca por números primos muito grandes. Algumas instituições oferecem prêmios para quem encontrar esses números, porque eles são especiais e úteis em muitas aplicações. Essas histórias mostram como a Matemática pode ser divertida e interessante.

Fazer atividades para encontrar números primos ajuda a melhorar as capacidades de fazer contas e de se organizar. O Crivo de Eratóstenes é um método que os estudantes utilizam em um papel com quadrados e números. Essa atividade faz com que eles cumpram regras bem definidas. Dessa forma, eles entendem de maneira fácil como um algoritmo funciona. No final, eles conseguem observar um resultado.

No próximo capítulo veremos, através de uma sequência didática, como tentar tornar esse potencial uma realidade em sala de aula.

6 PRODUTO EDUCACIONAL: SEQUÊNCIA DIDÁTICA

Como mencionado, o tema dos números primos tem um alto potencial pedagógico quando é abordado de forma planejada e contextualizada. Neste capítulo, introduzimos um recurso educacional na forma de uma sequência didática voltada para estudantes do Ensino Fundamental anos finais ou como uma espécie de reforço para alunos do Ensino Médio. Esta sequência foi criada para cumprir os objetivos da BNCC.

6.1 Objetivos Gerais e Competências Desenvolvidas

Os objetivos gerais da sequência didática incluem:

- ✓ Compreender o conceito de número primo e número composto.
- ✓ Desenvolver estratégias para determinar se um número é primo ou composto, incluindo o uso do método do Crivo de Eratóstenes e do teste de divisibilidade por primos sucessivos até a raiz quadrada.
- ✓ Reconhecer a importância dos números primos na fatoração de números naturais.
- ✓ Resolver problemas práticos que envolvam divisores, múltiplos e propriedades de números primos.
- ✓ Valorizar a história e a investigação Matemática.
- ✓ Desenvolver habilidades socioemocionais, como persistência, diante de desafios de identificar primos maiores, trabalho colaborativo e comunicação.
- ✓ Desenvolver o pensamento computacional.

Competências da BNCC atendidas. A sequência foi pensada para alinhar-se a diversas competências gerais da BNCC, tais como pensamento científico, crítico e criativo. Na parte específica da Matemática para o 6º ano, a sequência atende principalmente às habilidades EF06MA03, EF06MA04, EF06MA05 e EF06MA06 da BNCC:

> (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 (Brasil, 2018 p. 301).

6.2 Público-Alvo e Tempo Previsto

Público-alvo: Turmas de 6º ano do Ensino Fundamental. A sequência também pode ser aplicada em turmas do Ensino Médio para revisão/reforço, ou em projetos extracurriculares de Matemática.

Duração prevista: Aproximadamente 5 aulas de 50 minutos. Idealmente, cada aula corresponde a um bloco temático conforme detalhado adiante. Pode-se condensar em 4 aulas de 60 minutos, caso a escola trabalhe com tempos maiores, ou estender para 6 aulas incluindo mais exercícios e revisão, se julgar necessário.

6.3 Desenvolvimento da Sequência Didática

A seguir, descrevemos, em formato sequencial, as aulas e atividades planejadas:

Aula 1: A Descoberta dos Blocos de Construção dos Números

Objetivos Específicos:

- Identificar e listar os divisores de números naturais.
- Estabelecer a relação recíproca entre "ser múltiplo de" e "ser divisor de".
- Classificar os números naturais com base na quantidade de seus divisores.
- Definir, a partir da descoberta, o que é um número primo e um número composto, em alinhamento com a habilidade EF06MA05 da BNCC.

Materiais:

- Lápis e papel.
- Tabela impressa (modelo abaixo) ou desenhada no caderno.

Parte 1(20min): Mapeando os divisores.

Peça aos alunos que preencham a Tabela 2 do Anexo A, encontrando todos os divisores para os números de 1 a 20. Em seguida, devem contar quantos divisores cada número possui. Esta abordagem prática é o ponto de partida para a descoberta.

Parte 2(10min): Dando nomes às conexões.

Após o preenchimento, promova uma discussão focada nas relações observadas. Use o exemplo do número 12.

Introduza o vocabulário formal: "Nós vimos na tabela que 4 está no conjunto de divisores de 12. Quando isso acontece, dizemos que 4 é um divisor de 12. Ao mesmo tempo,

isso significa que 12 é um múltiplo de 4". Peça que os alunos deem outros exemplos da tabela usando essa dupla definição para consolidar o conceito.

Parte 3(10min): Descobrindo os primos.

Peça aos alunos para focarem exclusivamente na coluna "Quantidade de Divisores". Pergunte: "Que tipos de números vocês conseguem ver se olharmos apenas para quantos divisores eles têm?".

Ajude-os a separar os números em três grupos distintos:

Grupo 1: Números com apenas 1 divisor.

Grupo 2: Números com exatamente 2 divisores.

Grupo 3: Números com mais de 2 divisores.

Agora, conecte os grupos que eles criaram com as definições matemáticas formais.

Explique que os números do Grupo 2 são especiais. Um número natural é considerado primo se ele for maior que 1 e possuir exatamente dois divisores positivos distintos: o número 1 e ele mesmo.

Os números do Grupo 3 são chamados de compostos. Um número composto é um número natural maior que 1 que não é primo, ou seja, pode ser expresso como o produto de outros inteiros maiores que 1.

Explique que o número 1 do Grupo 1 não é nem primo nem composto, pois ele não se encaixa em nenhuma das duas definições, tendo apenas um divisor.

Para enriquecer a aula, mencione que a palavra primo vem do latim *primus*, que significa primeiro, porque os gregos os consideravam os números primeiros ou indecomponíveis a partir dos quais os outros eram formados.

Parte 4(10min): Aplicação.

Peça aos alunos para listarem os números primos que encontraram de 1 a 20.

Proponha um problema simples para aplicar o conceito de divisor, conforme a habilidade EF06MA06 da BNCC.

Exemplo: Uma florista tem 18 rosas. Ela quer montar buquês, todos com a mesma quantidade de rosas, sem que sobre nenhuma. Quais são as possíveis quantidades de rosas em cada buquê? Os alunos devem perceber que a resposta corresponde aos divisores de 18.

Avaliação: Recolher ou vistoriar a "Tabela Mapeando os Divisores" que os alunos preencheram. Ao final da aula, peça para responderem em um pequeno papel: O número 15 é primo ou composto? Justifique sua resposta usando a ideia de quantidade de divisores.

Aula 2: Peneirando os Números.

Objetivos Específicos:

- Construir, de forma colaborativa, a lista de números primos até um determinado valor.
- Compreender o que é um número primo e um número composto através de um processo de eliminação.
- Entender a lógica por trás da condição de parada do algoritmo.
- Apresentar a Matemática como uma construção humana, associando o método a seu criador, Eratóstenes.
- Alinhar com a habilidade EF06MA05 da BNCC.

Materiais:

- Uma tabela com os números de 1 a 100 (uma grade 10x10 é ideal).
- Lápis de cores diferentes.

Parte 1(10min): Preparação e Contexto Histórico.

Distribua a Tabela 3 do Anexo A com os números de 1 a 100.

Introduza a atividade explicando que eles usarão um método com mais de 2.000 anos, criado por um matemático grego chamado Eratóstenes de Cirene. Explique que o nome "crivo" significa peneira, pois o método "peneira" os números, deixando passar apenas os primos.

Peça para os alunos riscarem o número 1, pois, pela definição, ele não é primo.

Parte 2(20min): A Peneira em Ação.

Peneirando com o 2: Peça aos alunos para circularem o 2, o primeiro primo. Em seguida, com um lápis de cor, eles devem riscar todos os múltiplos de 2 maiores que ele (4, 6, 8, 10, etc.).

Peneirando com o 3: Peça que encontrem o próximo número que não foi riscado: o 3. Eles devem circulá-lo. Com outra cor, devem riscar todos os múltiplos de 3 maiores que ele (6, 9, 12, etc.).

Peneirando com o 5 e o 7: Repita o processo para o próximo número não riscado, o 5. Circule o 5 e risque seus múltiplos. Faça o mesmo para o 7.

Parte 3(20min): A Descoberta da Parada.

O próximo número não riscado é o 11. Pergunte aos alunos: "Quanto é 11 x 11?". A resposta é 121. Explique a regra de parada. A critério do professor.

Justificativa: qualquer número composto menor ou igual a 100 deve ter, pelo menos, um fator primo que seja menor ou igual a $\sqrt{100} = 10$. Como já riscamos todos os múltiplos dos primos até 10 (2, 3, 5 e 7), garantimos a eliminação de todos os compostos na nossa lista.

Como exercício, peça aos alunos que verifiquem a primalidade de alguns números, como por exemplo: 91, 231, 397, …. Use uma calculadora se possível.

A atividade pode ser realizada em duplas ou pequenos grupos para incentivar a cooperação e tornar a aprendizagem mais divertida. Estudantes mais rápidos podem ser desafiados a continuar o crivo até 200 ou 300, estendendo a tabela, ou a verificar manualmente a lista testando divisões.

Avaliação: Avaliar se os alunos aplicaram corretamente o algoritmo do Crivo de Eratóstenes e se compreenderam a lógica de sua condição de parada.

Aula 3: Existe um Último Número Primo?

Objetivos Específicos:

- Levar os estudantes a compreenderem, de forma investigativa e prática, o conceito da infinitude dos números primos, construindo o argumento lógico a partir de exemplos numéricos.
- Alinhar com as habilidades EF06MA05 e EF06MA06 da BNCC.

Materiais:

- Lápis e papel.
- Calculadora (opcional).
- Lista de números primos (pode ser a construída na atividade passada).

Parte 1(10min): A Suposição Inicial.

Comece com uma pergunta instigante: E se a lista de todos os números primos fosse finita? Vamos imaginar que só existem alguns primos e tentar ver se isso é possível.

Proponha um cenário hipotético. Diga aos alunos: Imaginem por um momento que os únicos números primos que existem são 2, 3 e 5. Escreva esta lista finita no quadro: P = {2, 3, 5}.

Parte 2(20min): O Teste de Euclides.

Peça aos alunos para aplicarem a construção sugerida por Euclides, multiplicar todos os primos da lista e somar 1.

$N = (2 \cdot 3 \cdot 5) + 1$

Os alunos calcularão o resultado: N = 30 + 1 = 31. Agora, inicie a investigação:

O número 31 está na nossa lista original de primos P = {2, 3, 5}? O número 31 é primo?

Conclua com eles que a suposição de que {2, 3, 5} era a lista de todos os primos estava errada, pois encontramos um novo primo, o 31, que não estava nela.

Para que os alunos percebam que não foi uma coincidência, proponha um novo cenário. Certo, então nossa lista estava incompleta. E se a lista completa de primos for {2, 3, 5, 7}?

Peça que repitam o processo de Euclides:

$N = (2 \cdot 3 \cdot 5 \cdot 7) + 1$

Os alunos encontrarão o resultado: N = 210 + 1 = 211. Faça a mesma investigação:

O número 211 está na nossa nova lista {2, 3, 5, 7}? Será que 211 é primo? O que podemos concluir? A suposição de que {2, 3, 5, 7} continha todos os primos também é falsa.

Parte 3(20min): E se o número que encontrarmos não for primo?

E se a nossa lista completa de primos fosse {2, 3, 5, 7, 11, 13}? Será que agora temos todos? Peça aos alunos que repitam o processo de Euclides mais uma vez:

$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13) + 1$.

Os alunos encontrarão o resultado: N=30030+1=30031.

Agora, faça a mesma investigação: O número 30031 está na nossa lista {2, 3, 5, 7, 11, 13}? Será que 30031 é primo? Este é o ponto importante. O número 30031 é um *número composto.* Peça aos alunos para verificarem ou informe diretamente a fatoração de 30031, $30031 = 59 \cdot 509$. O que podemos concluir? A conclusão é a mesma, mas o raciocínio é um pouco diferente e mais forte. O número que criamos, 30031, não é divisível por 2, 3, 5, 7, 11 ou 13, peça aos alunos que verifiquem.

Mas, como ele é um número composto, ele obrigatoriamente tem fatores primos, pelo Teorema Fundamental da Aritmética. Os seus fatores primos são 59 e 509. Nenhum desses dois fatores primos estava na nossa lista inicial.

Mesmo quando o resultado é um número composto, ele nos força a encontrar novos primos, neste caso 59 e 509, que não estavam na lista. Portanto, a suposição de que a lista {2, 3, 5, 7, 11, 13} continha todos os números primos também é falsa.

Não importa qual seja a nossa lista finita de primos, sempre podemos usar esse método para encontrar um número que nos força a admitir a existência de um primo que não estava na lista. Logo, a suposição de que a lista de primos é finita é falsa. O conjunto dos números primos é infinito.

Avaliação: Solicite que os alunos escrevam um parágrafo respondendo à pergunta: Imagine que um colega seu afirme que encontrou o maior número primo de todos. Com base no que fizemos na aula, como você explicaria a ele por que isso não é possível?

Aula 4: A Chave Mestra dos Números, Fatoração para MDC e MMC.

Objetivos Específicos:

- Revisar o processo de fatoração de um número em fatores primos (TFA).
- Aprender e aplicar o método de cálculo do mdc e mmc através da decomposição canônica.
- Resolver um problema contextualizado que mobilize os conceitos de MDC e MMC, compreendendo a utilidade prática de cada um.

Materiais:

- Lápis e papel.
- Calculadora (opcional).

Parte 1(10min): Aquecimento e apresentação do desafio.

Comece revisando o conceito de que todo número composto pode ser escrito de forma única como um produto de números primos. Isso é o Teorema Fundamental da Aritmética (TFA). Fatore um número simples no quadro, como $18 = 2{\cdot}3{\cdot}3 = 2{\cdot}3^2$, para revisar o conhecimento prévio.

Apresente uma situação-problema que demande o cálculo de mdc e mmc para ser resolvida.

Duas turmas, uma com 24 alunos e outra com 36 alunos, participarão de uma gincana. Todas as equipes devem ter o mesmo número de integrantes e não podemos misturar alunos de turmas diferentes.

Pergunta 1: Qual é o maior número possível de alunos em cada equipe?

Pergunta 2: Se as turmas fizerem atividades em ciclos, com a primeira completando um ciclo a cada 24 minutos e a segunda a cada 36 minutos, depois de quanto tempo elas terminarão um ciclo simultaneamente pela primeira vez?

Parte 2(15min): Fatoração para calcular mdc e mmc.

Peça aos alunos para fatorarem os números do problema 24 e 36 em fatores primos.

$24 = 2{\cdot}2{\cdot}2{\cdot}3 = 2^3{\cdot}3^1$ $\quad$ $36 = 2{\cdot}2{\cdot}3{\cdot}3 = 2^2{\cdot}3^2$

Apresente as regras para o cálculo do mdc e mmc usando a fatoração.

Para o mdc: Pegamos apenas os fatores primos comuns às duas decomposições, cada um elevado ao seu menor expoente.

mdc(24, 36) = 12, pois os fatores comuns de menor expoente são 2^2 e 3.

Para o mmc: Pegamos todos os fatores primos que aparecem em pelo menos uma das decomposições, cada um elevado ao seu maior expoente.

mmc(24, 36) = 72, pois os fatores com os maiores expoentes são 2^3 e 3^2.

Parte 3(25min): Aplicação e resolução do desafio.

Peça aos alunos que, em grupos, usem os valores de mdc e mmc que acabaram de calcular para responder às perguntas do problema inicial.

Resposta 1: O maior número possível de alunos em cada equipe é 12.

Resposta 2: As turmas terminarão um ciclo simultaneamente após 72 minutos.

Circule pela sala para garantir que os alunos estão conectando o valor calculado à pergunta correta do problema.

Sugestões de outros problemas,

Duas lâmpadas piscam em ritmos diferentes, uma a cada 84 segundos, outra a cada 60 segundos. As duas piscam juntas em algum instante; depois de quanto tempo isso ocorrerá novamente?

Temos 84 laranjas e 60 maçãs. Queremos montar cestas todas iguais, sem misturar frutas diferentes na mesma cesta, e sem sobras. Qual o máximo de frutas em cada cesta?

Reforce a ideia principal que a fatoração em primos é como encontrar o "DNA" de um número, e essa "chave mestra" nos permite resolver de forma eficiente problemas de divisão em partes iguais (MDC) e de ciclos que se repetem (MMC).

Destaque que este método é muito mais poderoso do que listar todos os divisores ou múltiplos, especialmente para números grandes.

Avaliação: Proponha um problema novo, mas com a mesma estrutura dos exemplos dados. Por exemplo. Dois ônibus partem de um terminal ao mesmo tempo. A linha A retorna ao terminal a cada 50 minutos e a linha B a cada 75 minutos. Depois de quanto tempo os dois ônibus se encontrarão no terminal novamente?

Aula 5: Explorando os Grandes Mistérios dos Números Primos

Objetivos Específicos:

- Introduzir os alunos a problemas famosos e não resolvidos da Matemática de forma lúdica e investigativa, despertando a curiosidade.
- Mostrar que a Matemática é uma ciência viva e cheia de desafios.

Materiais:

- Lápis e papel.

Parte 1(5min): A fronteira da Matemática.

Comece explicando o que é uma conjectura: uma afirmação matemática que muitos acreditam ser verdadeira, mas que ninguém no mundo ainda conseguiu provar.

Mencione que alguns desses problemas são tão importantes que o Instituto Clay de Matemática oferece um prêmio de um milhão de dólares para quem os resolver. Hoje, eles serão os matemáticos que investigarão alguns desses mistérios.

Parte 2(15min): A Conjectura de Goldbach.

Escreva no quadro a Conjectura Forte de Goldbach, descreva-a como um dos problemas não resolvidos mais interessantes pela simplicidade de sua formulação: *Todo número par maior ou igual a 4 pode ser escrito como a soma de dois números primos.*

Peça aos alunos que, em duplas e com uma lista de números primos em mãos, pode ser a lista da aula 2, testem a conjectura. Forneça uma lista de números pares para eles decomporem. Utilize a Tabela 4 do Anexo A.

Alguém encontrou um número par que não funcionou? A resposta será não.

Explique que, embora a conjectura tenha sido verificada por computadores para números enormes, isso não conta como uma prova matemática.

Conte a eles que uma versão "fraca" da conjectura*, todo número ímpar maior que 5 é a soma de três primos*, foi finalmente provada em 2013 pelo matemático Harald Helfgott, mostrando como a Matemática avança.

Parte 3(15min): Em busca dos primos gêmeos.

Defina primos gêmeos como pares de números primos que diferem entre si por 2. Apresente a conjectura: *Será que existem infinitos pares de primos gêmeos?*

Usando a lista de primos até 100 da aula 2, peça aos alunos para encontrarem todos os pares de primos gêmeos que conseguirem. Eles devem encontrar:

(3, 5); (5, 7); (11, 13); (17, 19); (29, 31); (41, 43); (59, 61); (71, 73).

Pergunte o que eles notam. Os pares de gêmeos ficam mais comuns ou mais raros à medida que os números aumentam? Explique que os pares se tornam mais espaçados.

Parte 4(15min): Encerramento e reflexão.

Reúna a turma e comente que eles acabaram de explorar dois problemas que intrigam os matemáticos há séculos. Conclua que essas conjecturas mostram a incrível complexidade escondida na aparente simplicidade dos números primos.

Mencione rapidamente a Hipótese de Riemann como "O Santo Graal da Matemática", um problema ainda mais complexo sobre a distribuição dos primos, para mostrar que a busca por entender esses números continua sendo uma das áreas mais ativas da Matemática moderna.

Avaliação: Peça aos alunos que escrevam uma resposta curta para a seguinte pergunta: Das duas conjecturas que investigamos hoje (Goldbach e Primos Gêmeos), qual você achou mais curiosa? Por quê? O que essa aula lhe ensinou sobre o trabalho dos matemáticos?

7 RELATÓRIO DE APLICAÇÃO E ANÁLISE DA SEQUÊNCIA DIDÁTICA

7.1 Introdução

Este relatório registra a implementação da sequência didática apresentada na dissertação de mestrado do autor. A intervenção foi conduzida em uma classe do segundo ano do Ensino Médio da Escola Estadual Santo Amaro, onde sou docente responsável. O objetivo principal foi empregar a sequência, inicialmente concebida para o Ensino Fundamental, como um instrumento de reforço e revisão conceitual, tratando os princípios da teoria dos números de forma investigativa e prática.

As atividades foram realizadas no Laboratório de Matemática da instituição, o que possibilitou a utilização de recursos audiovisuais e um ambiente adequado para trabalho coletivo e individual.

A seleção do tema e da abordagem acompanham o produto educacional exposto nesta dissertação, levando em conta não apenas as propriedades matemáticas, mas também os aspectos históricos e as aplicações em sala de aula.

7.2 Objetivos da Aplicação

A aplicação da sequência didática para esta turma de Ensino Médio visou:

✓ Consolidar o entendimento de conceitos fundamentais, como a definição de números primos e compostos, divisibilidade, e os conceitos de mdc e mmc.

✓ Analisar a efetividade de uma estratégia prática para o engajamento de estudantes mais velhos com conteúdos essenciais, trocando a memorização pela construção lógica.

✓ Fomentar o protagonismo estudantil, encorajando os estudantes a exporem suas ideias.

✓ Examinar a receptividade e os desafios enfrentados pelos estudantes ao revisitar um assunto do 6º ano com uma perspectiva mais detalhada e contextualizada.

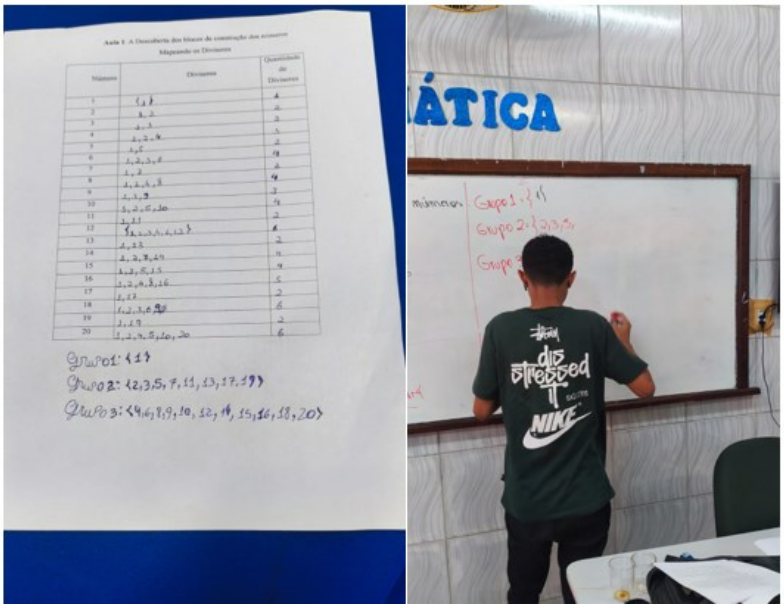
✓ Investigar conjecturas matemáticas (como a de Goldbach) e incentivar a argumentação.

7.3 Metodologia e Execução

A sequência foi implementada em cinco aulas temáticas, respeitando a estrutura da dissertação. Como professor facilitador, minha função foi orientar as descobertas por meio de perguntas, enquanto os estudantes anotavam suas conclusões em materiais impressos e cadernos.

Aula 1: A Descoberta dos Blocos de Construção: A aula começou com a exploração dos divisores, como demonstram as anotações na Figura 5. O ponto mais importante

Figura 5 – A descoberta dos blocos de construção

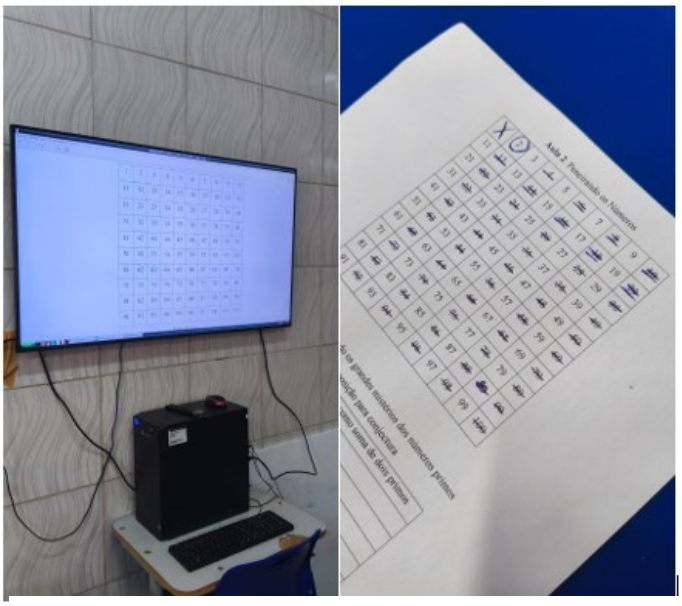


Fonte: Acervo da Pesquisa

foi a participação dos alunos, com alguns estudantes indo ao quadro para organizar os números nos três grupos distintos (com 1, 2, ou mais de 2 divisores). Mesmo sendo uma turma do Ensino Médio, muitos alunos tiveram dificuldades em identificar os divisores. Entretanto, a folha de atividades preenchida confirma que a meta de reconstruir autonomamente os conceitos foi atingida. Essa etapa incentivou a participação oral, a argumentação e a correção colaborativa dos registros.

Aula 2: Peneirando os Números: A tabela para ajudar a executar o Crivo de Eratóstenes foi exibida na tela do laboratório conforme a Figura 6, funcionando como um recurso visual coletivo. Os alunos, por sua vez, realizaram o algoritmo manualmente em suas folhas de atividades, o que possibilitou a internalização do procedimento de maneira visual e rápida.

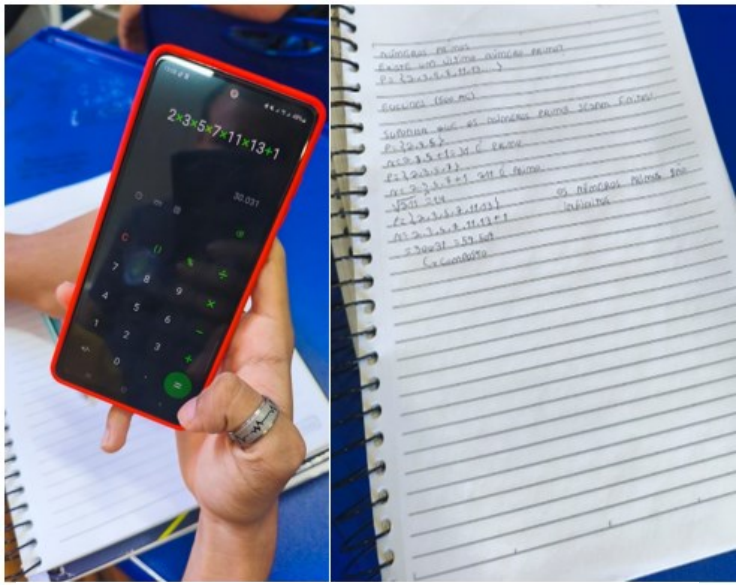
Figura 6 - Peneirando os números



Fonte: Acervo da Pesquisa

Aula 3: Existe um Último Número Primo? Esta aula, de caráter mais abstrato, obteve sucesso graças à metodologia prática. Os estudantes exploraram o raciocínio de Euclides, empregando calculadoras de celular para manipular números maiores, como o 30031. As anotações em seus cadernos, de acordo com a Figura 7, evidenciam a compreensão do processo lógico, diferenciando os casos em que os resultados são primos daqueles que são compostos.

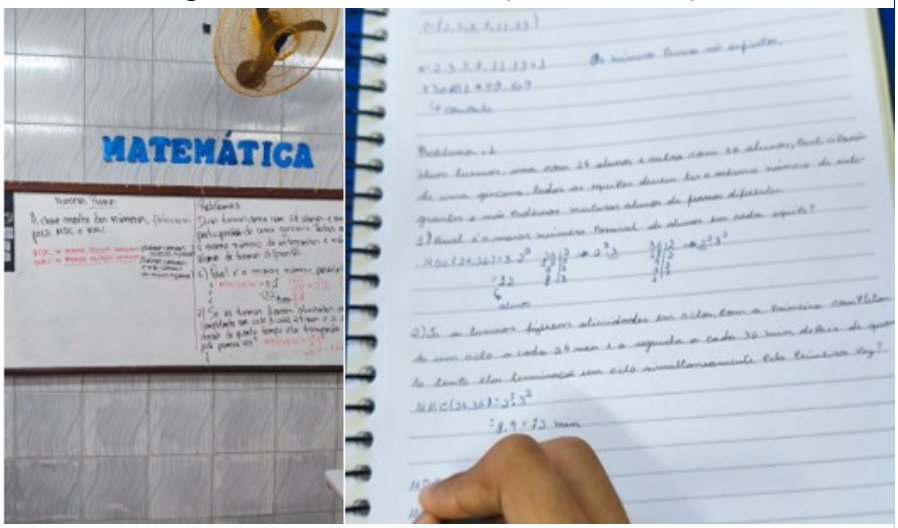
Figura 7 - Existe um último número primo?



Fonte: Acervo da Pesquisa

Aula 4: A Chave Mestra (MDC e MMC): A aplicação dos conceitos foi trabalhada através de problemas contextualizados conforme a Figura 8. O registro no caderno de um aluno mostra claramente a resolução dos problemas propostos na dissertação, com o cálculo do $mdc(24,36)$ e $mmc(24,36)$ utilizando a fatoração em primos.

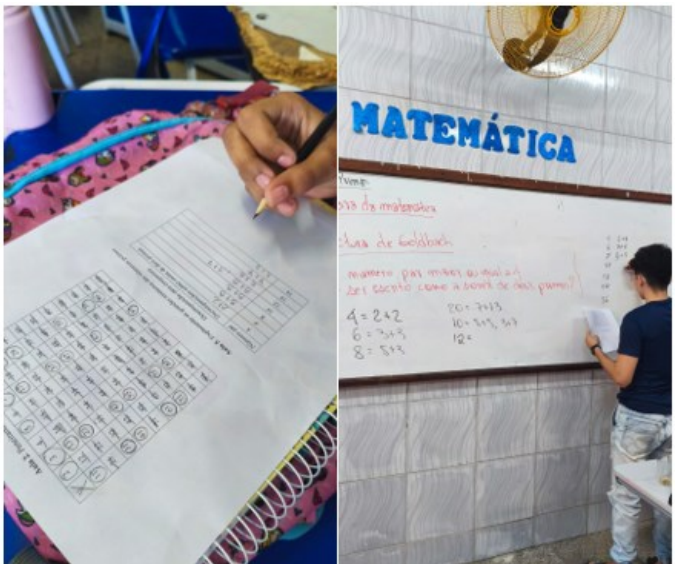
Figura 8 - A chave mestra (MDC e MMC)



Fonte: Acervo da Pesquisa

Aula 5: Explorando os Grandes Mistérios: Houve um bom grau de envolvimento. A principal prova de que a metodologia teve sucesso em incentivar o protagonismo é a imagem (Figura 9) de um estudante no quadro apresentando a Conjectura de Goldbach e no caderno a Conjectura dos Primos Gêmeos. Ao investigar um problema matemático em aberto, os alunos demonstraram bastante curiosidade. Ficaram ainda mais interessados ao saber que alguns

Figura 9 - Explorando os grandes mistérios



Fonte: Acervo da Pesquisa

desses problemas em aberto podem valer milhões de dólares.

Incentivou-se que cada aluno anotasse em seu caderno as definições, exemplos resolvidos em grupo e os principais resultados das atividades. Por fim, houve um momento para refletir sobre os desafios enfrentados e a relevância dos números primos na Matemática.

7.4 Reação e Análise de Desempenho dos Alunos

Como era de se esperar, a turma teve reações variadas. Alguns estudantes apresentaram dúvidas ao identificar divisores de números maiores e em diferenciar números primos dos compostos. Para os estudantes que já tinham um bom conhecimento da Matemática Básica, as primeiras aulas serviram como uma revisão dinâmica e interessante. A abordagem prática e histórica foi considerada "diferente e mais interessante" do que a mera repetição de regras.

Parte da turma concluiu rapidamente as etapas iniciais, evidenciando domínio dos conteúdos do 6º ano. Esses alunos se destacaram principalmente nos desafios avançados e na apresentação de explicações para os colegas.

Para alguns, o desafio não estava no conteúdo, mas na mudança de estratégia. A maior dificuldade foi ter que justificar o porquê, elaborar um argumento (como na Aula 3) e enfrentar questões sem uma resposta "certa" (Aula 5). Isso indica que a dependência de métodos mecânicos continua sendo um desafio, e a sequência foi bem sucedida em enfrentar essa atitude.

O ambiente do laboratório favoreceu o trabalho coletivo, o diálogo e a construção conjunta do conhecimento. O uso de tabelas impressas, quadro, cadernos, projetor e até calculadora do celular foram essenciais para diversificar as estratégias e manter a atenção dos alunos.

Para concluir, a implementação da sequência didática na turma do segundo ano do Ensino Médio da EEM Santo Amaro demonstrou a notável flexibilidade e eficiência da proposta. A metodologia não apenas se revelou apropriada para a revisão de conteúdos, mas também conseguiu aprofundar a compreensão conceitual dos estudantes, gerando uma boa participação.

A abordagem centrada no estudante é confirmada pelo protagonismo demonstrado, com alunos esclarecendo conceitos no quadro e conduzindo investigações. Em suma, a sequência cumpre seu propósito de transformar o estudo dos números primos em uma jornada de descoberta lógica e histórica, servindo como uma ferramenta pedagógica valiosa e adaptável a diferentes contextos e níveis de ensino.

8 TRABALHOS FUTUROS

Esta dissertação mostrou as principais ideias e a importância dos números primos no Ensino Fundamental. Para o futuro, a ideia é olhar mais para o Ensino Médio. Serão adicionados temas mais complexos, como a aritmética modular e a criptografia RSA. O objetivo será mostrar como esses assuntos são usados nas tecnologias de hoje.

Essa ampliação tem como objetivo preencher uma necessidade que foi percebida ao analisar os livros didáticos. Os livros costumam abordar o tema de maneira simples e desconectada da realidade dos alunos. Eles não mostram como o assunto se relaciona com o mundo digital.

O Pequeno Teorema de Fermat e a Teoria dos Números são muito importantes para o algoritmo RSA. Eles mostram como a Matemática pode ajudar na tecnologia de hoje. Criar uma sequência didática focada nesses assuntos poderá ajudar muito a tornar o aprendizado mais conectado com a vida das pessoas e mais interessante.

9 CONSIDERAÇÕES FINAIS

Ao final desta exploração dos números primos, desde a Grécia Antiga até seu uso educativo, reafirma-se o objetivo principal que foi analisar os fundamentos e propriedades desses números especiais, visando uma abordagem além do ensino mecânico.

A análise teórica mostrou que os números primos são fundamentais na aritmética e estão ligados a grandes mistérios da Matemática. A investigação do cenário educacional, ao analisar diretrizes curriculares e livros didáticos, mostrou uma lacuna significativa. Os materiais didáticos, apesar de organizados logicamente, muitas vezes não conectam o conteúdo à sua história ou aplicações atuais, nem conseguem despertar fascínio e curiosidade.

Com o diagnóstico, a principal contribuição desta dissertação foi a criação de uma sequência didática para o Ensino Fundamental. Esta proposta, que vai além de um plano de aulas, é uma resposta aos problemas identificados, alinhando-se às competências da BNCC para um aprendizado mais investigativo.

Reconhecem-se, porém, as limitações deste trabalho. A análise focou no Ensino Fundamental, abrindo espaço para abordagens em outros níveis.

Espera-se que esta dissertação incentive professores e pesquisadores da Educação Matemática a ver os números primos como uma porta de entrada para a beleza, a história e os desafios do pensamento matemático.

REFERÊNCIAS

BENDER2K14. **PrimePi.svg**. [*S. l.*], 2011. Disponível em: https://commons.wikimedia.org/wiki/File:PrimePi.svg. Acesso em: 9 abr. 2025.

BIANCHINI, Edwaldo. **Matemática Bianchini**: 6. ano: manual do professor. 10. ed. São Paulo: Moderna, 2022.

BOYER, Carl B.; MERZBACH, Uta C. **História da Matemática**. Tradução Helena Castro. 3. ed. São Paulo: Edgard Blücher, 2012.

BRASIL. **Lei nº 9.394**, de 20 de dezembro de 1996. Estabelece as diretrizes e bases da educação nacional. Diário Oficial da União, Brasília, DF, 23 dez. 1996.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**: Educação é a base. Brasília, DF: MEC, 2018.

BRASIL. Ministério da Educação. **Divulgados os resultados do PISA 2022**. Brasília, DF: MEC, 2023. Disponível em: https://www.gov.br/mec/pt-br/assuntos/noticias/2023/dezembro/divulgados-os-resultados-do-pisa-2022. Acesso em: 31 abr. 2025.

BRASIL. Secretaria de Educação Fundamental. **Parâmetros curriculares nacionais**: **Matemática**. Brasília: MEC/SEF, 1998. 148 p.

CLAY MATHEMATICS INSTITUTE. **Official website of the Clay Mathematics Institute**. Disponível em: https://www.claymath.org/. Acesso em: 16 mai. 2025.

COELHO, João Eugênio Camilo. **Uma introdução aos primos gêmeos**: caracterizações e ilustrações. 2021. 68 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Tecnológica Federal do Paraná, Curitiba, 2021.

COUTINHO, S. C. **Criptografia**. 1. ed. (11. imp., versão 2015). Rio de Janeiro: IMPA/OBMEP, 2015.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2. ed. (3. imp.). Rio de Janeiro: IMPA, 2005. (Série de Computação e Matemática).

EUCLIDES. **Os elementos**. Tradução e Introdução Irineu Bicudo. São Paulo: Editora Unesp, 2009.

EVES, Howard. **Introdução à história da matemática**. Tradução: Hygino H. Domingues. Campinas, SP: Editora da UNICAMP, 2011.

FARIAS, Djalma Gomes de. **Um Estudo do Ensino de Números Primos na Educação Básica**. 2016. 95 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituto de Matemática, Universidade Federal de Alagoas, Maceió, 2016.

FERREIRA, Antonio Eudes. **Números Primos e o Postulado de Bertrand**. 2014. 44 f. Dissertação (Mestrado em Matemática) – Universidade Federal da Paraíba, Centro de

Ciências Exatas e da Natureza, João Pessoa, 2014.

FREIRE, Paulo. **A importância do ato de ler**: em três artigos que se completam. São Paulo, SP: Autores Associados: Cortez, 1982. 96p. (Polêmicas do nosso tempo, 4).

GASPARETI, Leandro. **O Santo Graal da Matemática**: a Hipótese de Riemann. 2014. 50 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Tecnológica Federal do Paraná, Curitiba, 2014.

HEFEZ, Abramo. **Aritmética**. 3. ed. Rio de Janeiro: SBM, 2022. (Coleção PROFMAT).

LEMOS, Manoel. **Criptografia, Números Primos e Algoritmos**. 4. ed. Rio de Janeiro: IMPA, 2010. (Publicações Matemáticas).

MUNIZ NETO, Antonio Caminha. **Tópicos de Matemática Elementar**: Volume 5: Teoria dos Números. 3. ed. Rio de Janeiro: SBM, 2022.

OLIVEIRA, Gerson Pastre; FONSECA, Rubens Vilhena. A teoria dos números na formação de professores de matemática: (in)compreensões acerca da primalidade e do teorema fundamental da Aritmética. **Ciência & Educação**, Bauru, v. 23, n. 4, p. 881-898, 2017. DOI: 10.1590/1516-731320170040015.

PATARO, Patricia Rosana Moreno; BALESTRI, Rodrigo Dias. **Matemática essencial**: 6. ano: ensino fundamental: anos finais. 1. ed. São Paulo: Scipione, 2018.

PEREIRA, Andressa de Lima. **Números primos e a conjectura de Goldbach**. 2017. 74 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal do ABC , Santo André , 2017.

RESENDE, Marilene Ribeiro. **Re-significando a disciplina teoria dos números na formação do professor de matemática na licenciatura**. 2007. Tese (Doutorado em Educação Matemática) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2007.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada; CNPq, 1998. 199 p. (Coleção Matemática Universitária). ISBN 85-244-0142-7.

TEIXEIRA, Lilian Aparecida *et al* (ed.). **Superação:** matemática: 6.ano: manual do professor. 1. ed. São Paulo: Moderna, 2022.

VIEIRA, Márcia Oliveira. **O Teorema dos Números Primos**. 2023. 99 f. Dissertação (Mestrado Profissional em Matemática); Programa de Pós-Graduação em Matemática, Universidade Federal de Sergipe, São Cristóvão, 2023.

APÊNDICE A – TABELAS PARA IMPRESSÃO

Tabela 2 - Mapeando os divisores

Número	Divisores	Quantidade de Divisores
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		

Fonte: elaborada pelo autor.

Tabela 3 - Números de 1 a 100

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

Fonte: elaborada pelo autor.

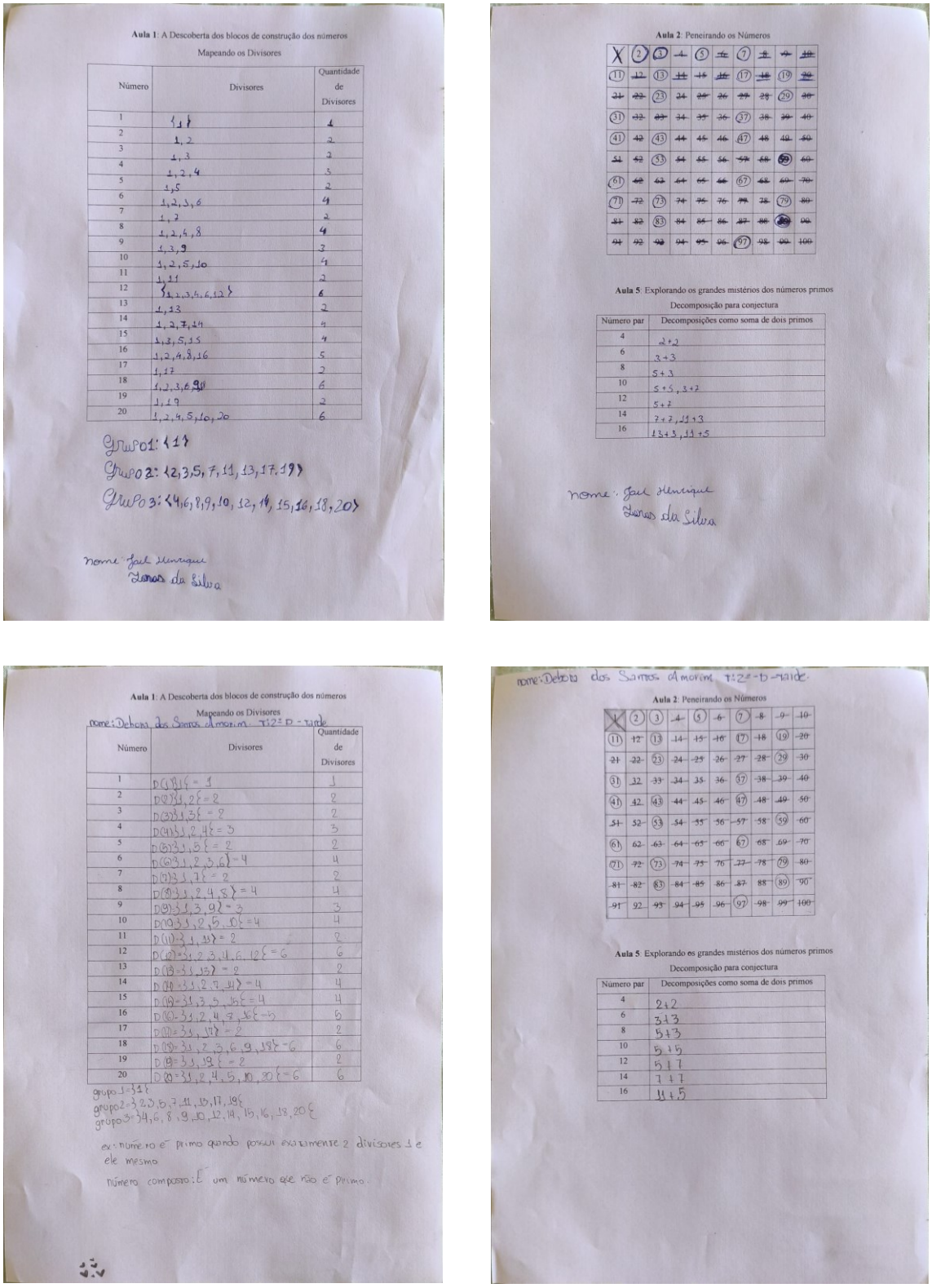
Tabela 4 - Decomposição para conjectura

Número par	Decomposições como soma de dois primos
4	
6	
8	
10	
12	
14	
16	
18	
20	
22	
24	

Fonte: elaborada pelo autor.

APÊNDICE B – EXEMPLOS DE REGISTROS DOS ALUNOS

Figura 10 – Alguns registros dos alunos



Aula 1: A Descoberta dos blocos de construção dos números

Mapeando os Divisores

Número	Divisores	Quantidade de Divisores
1	{1}	1
2	1, 2	2
3	1, 3	2
4	1, 2, 4	3
5	1, 5	2
6	1, 2, 3, 6	4
7	1, 7	2
8	1, 2, 4, 8	4
9	1, 3, 9	3
10	1, 2, 5, 10	4
11	1, 11	2
12	{1, 2, 3, 4, 6, 12}	6
13	1, 13	2
14	1, 2, 7, 14	4
15	1, 3, 5, 15	4
16	1, 2, 4, 8, 16	5
17	1, 17	2
18	1, 2, 3, 6, 9, 18	6
19	1, 19	2
20	1, 2, 4, 5, 10, 20	6

Grupo 01: {1}

Grupo 2: {2, 3, 5, 7, 11, 13, 17, 19}

Grupo 3: {4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20}

nome: José Henrique Lemos da Silva

Aula 2: Peneirando os Números

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

Aula 5: Explorando os grandes mistérios dos números primos

Decomposição para conjectura

Número par	Decomposições como soma de dois primos
4	2+2
6	3+3
8	5+3
10	5+5, 3+7
12	5+7
14	7+7, 11+3
16	13+3, 11+5

nome: José Henrique Lemos da Silva

Aula 1: A Descoberta dos blocos de construção dos números

Mapeando os Divisores

nome: Debora dos Santos Amorim T12ºD - turde

Número	Divisores	Quantidade de Divisores
1	D(1)={1} = 1	1
2	D(2)={1,2} = 2	2
3	D(3)={1,3} = 2	2
4	D(4)={1,2,4} = 3	3
5	D(5)={1,5} = 2	2
6	D(6)={1,2,3,6} = 4	4
7	D(7)={1,7} = 2	2
8	D(8)={1,2,4,8} = 4	4
9	D(9)={1,3,9} = 3	3
10	D(10)={1,2,5,10} = 4	4
11	D(11)={1,11} = 2	2
12	D(12)={1,2,3,4,6,12} = 6	6
13	D(13)={1,13} = 2	2
14	D(14)={1,2,7,14} = 4	4
15	D(15)={1,3,5,15} = 4	4
16	D(16)={1,2,4,8,16} = 5	5
17	D(17)={1,17} = 2	2
18	D(18)={1,2,3,6,9,18} = 6	6
19	D(19)={1,19} = 2	2
20	D(20)={1,2,4,5,10,20} = 6	6

grupo 1={1}

grupo 2={2,3,5,7,11,13,17,19}

grupo 3={4,6,8,9,10,12,14,15,16,18,20}

ex: número é primo quando possui exatamente 2 divisores 1 e ele mesmo

número composto: é um número que não é primo.

nome: Debora dos Santos Amorim T12ºD - turde

Aula 2: Peneirando os Números

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

Aula 5: Explorando os grandes mistérios dos números primos

Decomposição para conjectura

Número par	Decomposições como soma de dois primos
4	2+2
6	3+3
8	5+3
10	5+5
12	5+7
14	7+7
16	11+5

Fonte: Acervo da Pesquisa