UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

YURI MELHEIROS

DIVISIBILIDADE, NÚMEROS PRIMOS E SUAS APLICAÇÕES

SÃO CARLOS – SP
2025

YURI MELHEIROS

DIVISIBILIDADE, NÚMEROS PRIMOS E SUAS APLICAÇÕES

Monografia apresentada ao Curso de Licenciatura em Matemática da Universidade Federal de São Carlos.

Orientador: Prof. Dr. Alex Carlucci Rezende

SÃO CARLOS – SP
2025

FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

COORDENAÇÃO DOS CURSOS DE GRADUAÇÃO EM MATEMÁTICA - CCM/CCET
Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905
Telefone: (16) 33518221 - http://www.ufscar.br

DP-TCC-FA nº 10/2025/CCM/CCET

Graduação: Defesa Pública de Trabalho de Conclusão de Curso

Folha Aprovação (GDP-TCC-FA)

FOLHA DE APROVAÇÃO

YURI MELHEIROS

DIVISIBILIDADE, NÚMEROS PRIMOS E SUAS APLICAÇÕES

Trabalho de Conclusão de Curso

Universidade Federal de São Carlos – Campus São Carlos

São Carlos, 19 de fevereiro de 2025

ASSINATURAS E CIÊNCIAS

Cargo/Função	Nome Completo
Orientador	Alex Carlucci Rezende
Membro da Banca 1	Hellen Monção de Carvalho Santana
Membro da Banca 2	Pedro Souza Fagundes

Documento assinado eletronicamente por **Alex Carlucci Rezende**, **Professor(a) do Ensino Superior**, em 25/03/2025, às 11:55, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Hellen Monção de Carvalho Santana**, **Professor(a) Adjunto(a)**, em 25/03/2025, às 12:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Pedro Souza Fagundes**, **Professor(a) Adjunto(a)**, em 25/03/2025, às 16:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufscar.br/autenticacao, informando o código verificador **1782361** e o código CRC **C66577F6**.

Referência: Caso responda a este documento, indicar expressamente o Processo nº 23112.007535/2025-14 SEI nº 1782361

Modelo de Documento: Grad: Defesa TCC: Folha Aprovação, versão de 02/Agosto/2019

RESUMO

Este trabalho de conclusão de curso explora os conceitos de divisibilidade e números primos, desde suas origens na Matemática antiga até suas aplicações modernas. A divisibilidade, um dos pilares da teoria dos números, foi abordada por civilizações antigas e formalizada por matemáticos como Euclides e Gauss. O Teorema Fundamental da Aritmética, que afirma a decomposição única de números inteiros em fatores primos, é fundamental para entender a divisibilidade. O algoritmo de Euclides para o cálculo do Máximo Divisor Comum (MDC) é discutido, destacando sua importância histórica e suas aplicações em criptografia, especialmente no sistema RSA, onde números primos são essenciais para a segurança da informação. A partir da Base Nacional Comum Curricular (BNCC), o estudo da divisibilidade e números primos é abordado no ensino fundamental, com aplicação prática proposta através de atividades lúdicas. O trabalho finaliza com considerações sobre a relevância contínua desses conceitos na Matemática e na tecnologia, e sugere futuros projetos educacionais para aprofundar o conhecimento em sala de aula.

Palavras-chave: Divisibilidade. Números primos. Criptografia.

ABSTRACT

This thesis explores the concepts of divisibility and prime numbers, tracing their origins from ancient Mathematics to modern applications. Divisibility, a fundamental aspect of number theory, was addressed by ancient civilizations and formalized by mathematicians such as Euclid and Gauss. The Fundamental Theorem of Arithmetic, which states the unique factorization of integers into prime factors, is crucial for understanding divisibility. Euclid's algorithm for computing the Greatest Common Divisor (GCD) is discussed, highlighting its historical importance and its applications in cryptography, particularly in the RSA system where prime numbers are essential for information security. According to the Base National Common Curriculum (BNCC), the study of divisibility and prime numbers is integrated into fundamental education, with proposed practical activities for engaging students. The thesis concludes with reflections on the ongoing relevance of these concepts in Mathematics and technology and suggests future educational projects to deepen classroom knowledge.

Keywords: Divisibility. Prime numbers. Cryptography.

SUMÁRIO

1 INTRODUÇÃO

A história da divisibilidade remonta às origens da Matemática e está profundamente conectada com o desenvolvimento da teoria dos números, uma das áreas mais antigas da Matemática. A ideia de divisibilidade já era conhecida pelas civilizações antigas, como os egípcios, que desenvolveram técnicas para lidar com frações unitárias (frações onde o numerador é 1) e que, implicitamente, envolviam conceitos de divisibilidade. Os egípcios usavam tabelas de decomposição de frações que eram baseadas na divisibilidade.

O matemático grego Euclides, no seu livro "Elementos", apresentou o algoritmo de Euclides, um dos métodos mais antigos e eficientes para calcular o maior divisor comum (MDC) entre dois números. Este algoritmo é fundamental para o estudo da divisibilidade e ainda é utilizado hoje em dia. Euclides também explorou as propriedades dos números primos e demonstrou que existem infinitos números primos, um resultado que está intimamente ligado à divisibilidade.

Embora a ideia já estivesse implícita em trabalhos anteriores, o Teorema Fundamental da Aritmética, que afirma que todo número inteiro positivo pode ser decomposto de forma única (desconsiderando a ordem dos fatores) como um produto de números primos, foi formalizado por matemáticos como Carl Friedrich Gauss no início do século XIX. Este teorema é essencial para entender a divisibilidade, pois a decomposição em fatores primos é a base para verificar se um número é divisível por outro. Gauss, em seu trabalho seminal "Disquisitiones Arithmeticae", aprofundou a teoria dos números e sistematizou muitos conceitos de divisibilidade, incluindo o conceito de congruência, que é uma generalização da divisibilidade. A sua obra tornou-se uma referência fundamental para a teoria dos números e a aritmética modular, sendo amplamente utilizada em várias áreas da matemática moderna.

Matemáticos como Pierre de Fermat e Leonhard Euler contribuíram significativamente para a teoria dos números e para a compreensão da divisibilidade. Fermat, por exemplo, formulou o Pequeno Teorema de Fermat, que é uma importante aplicação da divisibilidade em números primos e que mais tarde se tornou crucial para a criptografia.

Na era moderna, a divisibilidade tem um papel crucial na criptografia, especialmente em sistemas como o RSA, que dependem da dificuldade de fatorar grandes números em seus primos constituintes. Isso mostra a relevância contínua dos conceitos de divisibilidade em áreas como a segurança da informação. O estudo da divisibilidade também se expandiu para áreas como a teoria dos códigos, onde se utilizam propriedades de divisibilidade para criar códigos de correção de erros, essenciais em comunicações digitais e transmissão de dados. Nos dias atuais, segundo a Base Nacional Comum Curricular (BNCC) (Brasil, 2018), os conceitos de divisibilidade e números primos são formalizados e trabalhados a partir do 6° ano do Ensino Fundamental (EF), onde os alunos aprendem sobre os critérios de divisibilidade, identificam múltiplos e divisores de números naturais, e exploram a decomposição em fatores primos. O algoritmo de Euclides é apresentado aos alunos no 8° ano do EF, juntamente com os conceitos

de MDC e mínimo múltiplo comum (MMC).

Dados os fatos, o objetivo deste trabalho será estudar o conceito de divisibilidade e de números primos, correlacionando-os e analisando desde os princípios teóricos até suas aplicações nos dias atuais, investigando o funcionamento do algoritmo da divisão, explorando suas propriedades e aplicando em problemas práticos e exemplos concretos.

No Capítulo 2, iremos formalizar os conceitos teóricos envolvendo a divisibilidade e os números primos. Falaremos inicialmente sobre definições e teoremas e, na sequência, faremos a relação entre o algoritmo da divisão e a decomposição em números primos. Exploraremos, também, um dos pilares da teoria dos números: o Teorema Fundamental da Aritmética (TFA). Esse teorema, que afirma que todo número inteiro maior que 1 pode ser representado de maneira única como um produto de números primos, é a base para muitos conceitos matemáticos e aplicações práticas, desde a criptografia até a computação segura. Ao longo deste capítulo, estudaremos a demonstração do TFA, compreendendo por que a fatoração em primos é única. Veremos também aplicações do TFA em problemas de divisibilidade e fatoração. Brevemente verificaremos o papel do TFA em sistemas criptográficos, que dependem da dificuldade de fatorar números grandes.

No Capítulo 3, exploraremos como os conceitos estudados sobre números primos são utilizados em áreas como a criptografia, a segurança digital e a geração de números aleatórios. Veremos como a estrutura única dos primos contribui para a proteção de dados na internet, garantindo transações seguras e comunicações sigilosas. Ao compreender essas aplicações, podemos perceber a importância dos números primos não apenas na matemática teórica, mas também na tecnologia e em diversos campos da ciência.

No Capítulo 4, apresentaremos uma sequência didática aplicada em sala de aula, voltada para o ensino de conceitos matemáticos fundamentais. Essa sequência foi desenvolvida e testada com alunos do ensino fundamental, com o objetivo de promover uma aprendizagem significativa e contextualizada. Neste capítulo, detalhamos o planejamento da sequência, incluindo seus objetivos, etapas e recursos utilizados. Além disso, descrevemos as atividades realizadas, desde a introdução do tema até a avaliação final, e apresentamos uma análise reflexiva sobre os resultados obtidos, destacando os acertos, desafios e lições aprendidas. Dessa forma, este capítulo busca demonstrar como a interação entre teoria e prática pode contribuir para experiências de aprendizagem enriquecedoras.

No Capítulo 5, abordaremos a elaboração de sequências didáticas inovadoras para o ensino da matemática. Com base em teorias pedagógicas e experiências práticas, apresentamos sugestões de atividades que podem ser adaptadas a diferentes contextos e níveis de ensino. Dentre os temas abordados, incluem-se números primos, fatoração, geometria e álgebra. Além disso, discutimos estratégias para aumentar o engajamento dos alunos, como o uso de jogos, projetos e investigações matemáticas. Também fornecemos orientações sobre avaliação e *feedback*, de modo a garantir que os alunos consolidem seus conhecimentos de forma eficaz. Assim, este capítulo tem como objetivo fornecer ferramentas para que professores possam dinamizar suas

aulas e torná-las mais alinhadas às necessidades dos estudantes.

No Capítulo 6, exploraremos criptossistemas que compartilham princípios semelhantes ao RSA, nos quais a decomposição desempenha um papel essencial, seja por meio da fatoração de números inteiros, da decomposição de matrizes ou de outras abordagens matemáticas. Esses sistemas desempenham um papel fundamental na segurança da informação, oferecendo soluções robustas para desafios como a criptografia assimétrica e a computação pós-quântica. Dessa forma, este capítulo visa destacar a importância da matemática na segurança digital e discutir como a teoria dos números continua a influenciar o desenvolvimento de novas tecnologias criptográficas.

No Capítulo 7, apresentaremos uma síntese dos principais conceitos abordados ao longo do projeto, destacando a importância da teoria dos números e de seus desdobramentos na criptografia e na segurança da informação. Revisamos como a divisibilidade, os números primos e a decomposição foram fundamentais para a compreensão dos criptossistemas estudados. Além disso, discutimos as contribuições do projeto, suas possíveis aplicações e sugestões para pesquisas futuras. Dessa forma, reforçamos a relevância do tema e seu impacto tanto na matemática teórica quanto em contextos práticos do mundo moderno.

Aproveitamos para agradecer aos professores da banca examinadora pelas valiosas sugestões e comentários, que contribuíram significativamente para o aprimoramento deste trabalho. As observações feitas não apenas enriqueceram a análise e a estrutura da pesquisa, mas também proporcionaram reflexões importantes para futuras aplicações e desenvolvimentos na abordagem do tema.

2 DIVISIBILIDADE E NÚMEROS PRIMOS

Vejamos a definição de divisibilidade baseada em (Domingues, 1991) e (Milies; Coelho, 2001).

Definição 2.1. O número inteiro $a \neq 0$ divide um número inteiro b se $b = ac$, para algum c pertencente ao conjunto dos números inteiros $\mathbb{Z}$. Neste caso, diz-se também que a é um divisor de b e que b é um múltiplo de a. Denotaremos por $a \mid b$ quando for este caso. Ou ainda, que b é divisível por a. Quando a não dividir b, denotaremos por $a \nmid b$.

O elemento $c \in \mathbb{Z}$, tal que $b = ac$, onde $a \neq 0$, é indicado por $c = \frac{b}{a}$, denominado por quociente de b por a.

Exemplo 2.1. Note que $4|8$, pois $8 = 4 \cdot 2$, e $3|9$ pois $9 = 3 \cdot 3$. Além disso, $3 \nmid 8$, pois não existe um número inteiro c tal que $8 = 3c$.

A divisibilidade satisfaz as seguintes propriedades:

(p_1) $a|a$, $\forall a \in \mathbb{Z}$, pois $a = 1 \cdot a$ (reflexiva);

(p_2) $a|b$ e $b|a \Rightarrow a = \pm b$ (antissimétrica);

(p_3) $a|b$ e $b|c \Rightarrow a|c$ (transitiva);

(p_4) Se $a|b$ e $a|c$, então $a|(bx+cy)$, $\forall x, y \in \mathbb{Z}$,

(p_5) Se $c|a$, $c|b$ e $a \leq b$, então $c|(b-a)$;

(p_6) Seja $a = b+c$ e suponha que $d|b$. Então, $d|a \Leftrightarrow d|c$ $(c = a-b)$;

(p_7) Se $a|b$ e $b \neq 0$, então $a \leq |b|$.

2.1 ALGORITMO DA DIVISÃO DE EUCLIDES

Quando abordamos o assunto de divisibilidade, para muitos uma associação rápida é feita com o algoritmo da divisão, mais conhecido também por algoritmo de Euclides.

Teorema 2.1. *Para quaisquer $x, y \in \mathbb{Z}$, $y \neq 0$, existe um único par de números q e r inteiros de maneira que $x = yq + r, (0 \leq r < |y|)$.*

Demonstração. Caso 1. $(y > 0)$. Neste caso considere $B = \{x - k \cdot y; k \in \mathbb{Z}, x - k \cdot y \geq 0\}$. Note que B é não vazio pois $x - (-|x|y) = x + |x|y \geq x + |x| \geq 0$. Claramente B é limitado inferiormente. Pelo princípio da boa ordem, B possui um menor elemento, digamos r. Portanto $\exists q \in \mathbb{Z}$, tal que $r = x - qy$. Para mostrar que $r < |y| = y$, note que $r = y \Rightarrow x = (1+q)y \Rightarrow r = 0 \Rightarrow y = 0$, o que é uma contradição. Note que, $r > y \Rightarrow \exists \sigma \in \mathbb{Z}$; $r = y + \sigma$, onde $0 < \sigma < r$. Assim

$y+\sigma = x-qy \Rightarrow \sigma = x-(q+1)y \in B$, o que é um absurdo, pois r é o menor elemento de B. Logo $0 \leq r < |y|$. Mostraremos agora que q e r são unicamente determinados. Suponha que $x = qy+r = q'y+r'$, com $0 \leq r, r' < |y| = y$. Neste caso, $0 \leq |r-r'| < y$. Por outro lado, $q'y+r' = qy+r \Rightarrow (q'-q)y = r-r' \Rightarrow |q-q'|y = |r-r'|$. Se fosse $r \neq r'$, teríamos $|q-q'| \geq 1$, Daí, $y \leq |q-q'|y = |r-r'| < y$, uma contradição. Portanto $r = r'$ e, consequentemente, $q = q'$.

Caso 2. ($y < 0$). Para $y < 0$, aplicamos o caso anterior com x e $|y|$. Assim existem únicos q,$r \in \mathbb{Z}$, tais que $x = q|y|+r$, com $0 \leq r < |y|$. Se colocamos $q_1 = -q$, então $x = q_1 y + r$, com $0 \leq r < |y|$. Claramente, q_1 é unicamente determinado. □

O MDC (Máximo Divisor Comum) de dois ou mais números é o maior número inteiro que pode dividir todos esses números ao mesmo tempo, sem deixar resto. Em outras palavras, é o maior divisor comum entre eles. O algoritmo da divisão é um método eficiente para encontrar o MDC entre dois números inteiros. O algoritmo baseia-se no princípio de que o MDC de dois números não muda se o maior número for substituído pela diferença entre os dois números.

Agora, explicaremos como funciona o algoritmo da divisão pensado por Euclides. Dados dois números inteiros a e b, onde $a \geq b$, temos:

1. Divida a por b, obtendo um quociente q e um resto r, tal que: $a = bq+r$, onde $0 \leq r < |b|$;
2. Substitua a por b e b por r;
3. Repita o processo até que $r = 0$. Nesta etapa, b será o MDC entre a e b.

Conseguiremos chegar sempre em $r = 0$, pois a cada passo, o valor de r (o novo divisor) é sempre menor que o valor do b anterior, eventualmente, chegamos a um ponto onde o divisor exato é o próprio MDC, tornando o resto zero.

Exemplo 2.2. Encontre o MDC de 252 e 105 utilizando o algoritmo de Euclides.

$252 = 105 \cdot 2 + 42$ ($a = 252$, $b = 105$, $q = 2$ e $r = 42$)
$105 = 42 \cdot 2 + 21$
$42 = 21 \cdot 2 + 0$
Assim, temos que o MDC de 252 e 105 é 21.

Exemplo 2.3. Encontre o MDC de 408 e 187 utilizando o algoritmo de Euclides.

$408 = 187 \cdot 2 + 34$
$187 = 34 \cdot 5 + 17$
$34 = 17 \cdot 2 + 0$
Assim, temos que o MDC de 408 e 187 é 17.

O algoritmo da divisão de Euclides é um dos métodos mais antigos, porém muito eficaz, para calcular o MDC de dois números inteiros, sendo amplamente utilizado devido à sua simplicidade, especialmente em sistemas de criptografia e teoria dos números.

2.2 NÚMEROS PRIMOS

Vejamos primeiro o que é um número primo.

Definição 2.2. Um número $p \in \mathbb{N}$ se diz **primo** se:

1. $p \neq 0$ e $p \neq 1$;
2. Os únicos divisores positivos de p são 1 e p.

Os números primos podem ser pensados como a menor "partícula" que compõe um número inteiro. Veja a próxima definição.

Definição 2.3. Um número $a \in \mathbb{N}$, $a \neq 0$ e $a \neq 1$, é chamado de **composto** se não for primo. Assim, um número composto sempre pode ser fatorado num produto $a = bc$, onde $b \neq 1$ e $c \neq 1$ (b,$c \in \mathbb{N}$).

Note que o inteiro 1 é divisível por 1 e por ele mesmo. Pela Definição 2.3, o número 1 deveria ser classificado como número primo. No entanto, neste trabalho, adotaremos que os inteiros 0 e 1 não são primos nem compostos.

Exemplo 2.4. O número inteiro 2 é primo, pois, se $a|2$, então $0 < a \leq 2$ e, portanto, $a = 1$ ou $a = 2$. Além disso, o número 2 é um primo muito especial, pois se trata do único primo par.

Demonstremos o seguinte teorema.

Teorema 2.2. *Se p é primo e $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Suponhamos $a \neq 0$ e $b \neq 0$. Admitamos que $p \nmid a$ e provemos que $\text{MDC}(a,p) = 1$. De fato, se $c|a$ e $c|p$, então $c = 1$ ou $c = p$ (pois p é primo). Porém, como $p \nmid a$, então $c = 1$. Se $p|ab$ e $\text{MDC}(a,p) = 1$, então $a|c$, logo $p|b$. □

Quando falamos de números primos é impossível deixar de citar um teorema extremamente importante, conhecido como Teorema Fundamental da Aritmética (TFA).

Teorema 2.3. *Para todo número natural $a > 1$, existem números primos $p_1, p_2, \ldots, p_r$ ($r \geq 1$), de maneira que $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Além disso, se também $a = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ ($s \geq 1$), onde os q_i também são primos, então $r = s$ e cada p_i é igual a algum dos q_i.*

Demonstração. Para $a = 2$, a afirmação é verdadeira, pois 2 é primo e, portanto, ele mesmo é a sua fatoração. Para a existência, suponha, por hipótese indutiva, que todo número composto a tal que $2 \leq a \leq n$ admite uma fatoração em primos. Agora, considere $n+1$: se $n+1$ for primo, a fatoração é trivial; caso contrário, $n+1$ é composto e pode ser escrito como $n+1 = p_1 \cdot p_2$, onde $2 \leq p_1, p_2 < n+1$. Pela hipótese indutiva, p_1 e p_2 podem ser fatorados se não forem primos, logo $n+1$ também pode. Portanto, pelo princípio da indução, todo número composto maior que

1 admite uma fatoração em primos. Já para sua unicidade, se $p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$, conforme o enunciado, então p_1 divide $q_1 \cdot q_2 \cdot \ldots \cdot q_s$ e, portanto, pelo Teorema 2.2, p_1 divide um de seus fatores, digamos q_1. Sendo apenas 1 e q_1 os divisores de q_1 e sendo $p_1 \neq 1$, então $p_1 = q_1$. Simplificando p_1 com q_1 na igualdade inicial, obtemos $p_2 \cdot p_3 \cdot \ldots \cdot p_r = q_2 \cdot q_3 \cdot \ldots \cdot q_s$. Repetindo este argumento o quanto for necessário, chegaremos à unicidade conforme o enunciado. É claro que não poderá ocorrer ao fim algo como $1 = q_r + q_{r+1} \cdot \ldots \cdot qs$, pois isto implicaria $q_s|1$, o que não é possível, pois q_s é primo. Logo $r = s$. □

2.3 DECOMPOSIÇÃO EM FATORES PRIMOS

A decomposição de um número inteiro positivo em fatores primos será baseada nos resultados anteriores. Dado a um número inteiro positivo, se p_1 é um número primo que o divide, consideramos q_1 o quociente da divisão de a por p_1. Em seguida, consideramos p_2 um número primo tal que $p_2 \mid q_1$ e $p_2 \geq p_1$. Seja q_2 o quociente da divisão de q_1 por p_2. Seguimos esse processo até que tenhamos obtido um quociente $q_r = 1$. Dessa forma, o número a será escrito como $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Note que é possível que $p_i = p_j$, para $i, j = 1, \ldots, r$.

Exemplo 2.5. Vamos decompor o número $a = 150$ em fatores primos. Note que o primeiro número primo que divide 150 é $p_1 = 2$, resultando em $q_1 = 75$. Em seguida, observamos que 75 não é divisível por 2, mas é divisível por $p_2 = 3$, resultando em $q_2 = 25$. Novamente, notamos que 3 não divide 25, mas esse é divisível por $p_3 = 5$, implicando que $q_3 = 5$. Por fim, $p_4 = p_3 = 5$ divide $q_3 = 5$, resultando em $q_4 = 1$. Veja um dispositivo prático para o procedimento:

150	2
75	3
25	5
5	5
1	

Dessa forma, temos $150 = 2 \cdot 3 \cdot 5 \cdot 5 = 2 \cdot 3 \cdot 5^2$

Ao observarmos a decomposição anterior, podemos perceber que há alguns fatores que se repetem, por exemplo, o número 5. Quando isso ocorre utilizamos a potenciação para unir os fatores iguais. Números inteiros diferentes têm decomposições em números primos diferentes, mas com fatores primos iguais. Por exemplo, os números 360 e 700 são diferentes, mas, em ambas as decomposições, aparecem os fatores primos 2, 3, 5 e 7. Obviamente, as potências de cada fator são diferentes, ou seja,

$$360 = 2^2 \cdot 3^2 \cdot 5 \cdot 7^0 \qquad \text{e} \qquad 700 = 2^2 \cdot 3^0 \cdot 5^2 \cdot 7^1.$$

Ao seguir o algoritmo tal como está descrito no início desta seção, o fator 3 não deveria

aparecer na decomposição de 700, assim como o fator 7 não deveria surgir quando decompomos 360. No entanto, eles podem ser incluídos com potência 0 (zero) a fim de comparação de decomposições.

A estrutura dos números primos é fundamental para diversas áreas da matemática, mas sua verdadeira importância se revela ao considerarmos a fatoração de números inteiros. A seguir, exploraremos o Teorema Fundamental da Aritmética, que estabelece a decomposição única dos números naturais em fatores primos, fornecendo a base para inúmeros resultados teóricos e aplicações práticas.

2.4 TEOREMA FUNDAMENTAL DA ARITMÉTICA E SUAS APLICAÇÕES

O Teorema Fundamental da Aritmética (TFA) é um dos pilares da Teoria dos Números, garantindo que todo número natural maior que 1 pode ser expresso de forma única como um produto de números primos, salvo a ordem dos fatores. Nesta seção, apresentaremos duas aplicações importantes desse resultado: sua relação com o máximo divisor comum e equações diofantinas, e seu papel na criptografia RSA.

2.4.1 Máximo divisor comum e equações diofantinas

Uma aplicação imediata do TFA é a determinação do *máximo divisor comum* (mdc) entre dois números naturais. Sejam a e b dois números naturais com decomposições em primos:

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}, \tag{2.1}$$

onde os p_i são primos comuns a ambos os números (se um primo não aparece em um dos números, consideramos o respectivo expoente como zero). O máximo divisor comum de a e b pode ser expresso como:

$$\text{mdc}(a,b) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}. \tag{2.2}$$

Essa decomposição permite a resolução de equações diofantinas do tipo $ax+by=d$, com $d = \text{mdc}(a,b)$, pois sabemos que essa equação tem soluções inteiras se, e somente se, d divide o termo independente do lado direito. Utilizando o *Algoritmo de Euclides* e sua versão estendida, podemos encontrar tais soluções, que são fundamentais para várias aplicações em teoria dos números e criptografia (Hardy; Wright, 2008).

2.4.2 Criptografia RSA

O Teorema Fundamental da Aritmética também é essencial na criptografia moderna, especialmente no *criptossistema RSA*, que baseia sua segurança na dificuldade de fatoração de números grandes em seus primos constituintes.

A segurança do RSA depende da dificuldade computacional de fatorar um número grande n nos primos p e q que o compõem. Como o Teorema Fundamental da Aritmética garante que essa fatoração é única, qualquer tentativa de quebrar o RSA precisa necessariamente encontrar esses primos, o que é inviável para números suficientemente grandes (Rivest; Shamir; Adleman, 1978). Abordaremos mais sobre a criptografia RSA no Capítulo 3.

3 APLICAÇÕES DOS NÚMEROS PRIMOS NOS DIAS DE HOJE

Quando analisamos a utilidade dos números primos nos dias atuais, prontamente podemos falar da criptografia. Mas o que é isso? (Galdino, 2014) aborda a criptografia e os números primos; a seguir faremos uma discussão sobre isso.

Criptografia é o campo da ciência que estuda técnicas para proteger a comunicação e a informação, garantindo que somente as partes autorizadas possam acessar e compreender os dados. A criptografia se baseia em transformar uma mensagem original (texto claro) em uma forma ilegível (texto cifrado ou criptografado) usando um algoritmo e uma chave criptográfica. Essa transformação visa proteger a informação contra acessos não autorizados, tornando difícil ou impossível para terceiros decifrar o conteúdo sem o conhecimento da chave correta.

Dentre os principais objetivos da criptografia estão a confidencialidade, integridade, autenticidade e irretratabilidade. Essas quatro palavras garantem que a informação seja acessível apenas às pessoas autorizadas, que a informação não seja alterada ou manipulada durante a transmissão ou o armazenamento, verificando a identidade das partes envolvidas na comunicação garantindo que uma ou ambas as partes não possam negar ter realizado uma determinada ação. Um exemplo prático e muito atual é o envio de mensagens escritas ou por áudio usando aplicativos de mensagens instantâneas por redes sociais.

Os números primos desempenham um papel fundamental na criptografia moderna, especialmente nos sistemas de criptografia assimétrica, como o RSA (Rivest–Shamir–Adleman). Nesses sistemas, a segurança da criptografia baseia-se na dificuldade de fatorar números grandes em seus fatores primos.

3.1 RSA, ALGORITMO DA DIVISÃO E NÚMEROS PRIMOS

No RSA, dois grandes números primos p e q são escolhidos. A partir desses números, calcula-se o produto $n = p \cdot q$, que é usado como parte da chave pública. O número n é grande o suficiente para que a fatoração de n em p e q seja computacionalmente impraticável, garantindo a segurança do sistema. A chave pública é usada para criptografar as mensagens, enquanto a chave privada, que depende dos números primos p e q, é usada para decifrar as mensagens. Somente o detentor da chave privada, que conhece os valores de p e q, podem decifrar o texto cifrado.

O algoritmo da divisão de Euclides é crucial na criptografia RSA, especialmente no cálculo do inverso multiplicativo modular, que é usado para criar a chave privada. Este processo é fundamental para garantir que a criptografia RSA funcione corretamente. Entendemos por inverso multiplicativo modular do número natural a como sendo o inteiro x tal que o produto ax é congruente a 1 módulo m, ou seja, $ax \equiv 1 (\text{mod } m)$, que é equivalente a dizer que m divide $ax - 1$. Para mais detalhes sobre o inverso multiplicativo modular, veja (Rosen, 1993).

No contexto do sistema RSA, o inverso multiplicativo modular é necessário para encontrar a chave privada. Consideremos a função totiente de Euler, definida para um número natural x

como sendo igual à quantidade de números menores ou iguais a x co-primos com respeito a ele, ou seja, $\phi(x) = \#\{1 \leq n \leq x \text{ e } \text{mdc}(n,x) = 1\}$.

Dado um número ε (parte da chave pública) e o valor de $\phi(n) = (p-1)(q-1)$, o inverso de ε módulo $\phi(n)$ é o valor d tal que:

$$\varepsilon \cdot d \equiv 1 \mod (\phi(n)).$$

O algoritmo da divisão de Euclides estendido é utilizado para encontrar este d. Tal número d é então usado como a chave privada, permitindo a decodificação da mensagem criptografada.

A criptografia, especialmente a criptografia assimétrica, está profundamente conectada à Teoria dos Números e à Aritmética. Números primos desempenham um papel central na segurança de sistemas como o RSA, enquanto o algoritmo da divisão de Euclides fornece as ferramentas necessárias para a geração de chaves seguras. Esses conceitos matemáticos são fundamentais para proteger informações contra acessos não autorizados, tornando-se indispensáveis na segurança digital contemporânea.

A seguir, apresentamos um exemplo simplificado do funcionamento do criptossistema RSA:

Exemplo 3.1. O processo básico do RSA segue os seguintes passos:

1. **Escolha de números primos**: Selecionamos dois números primos p e q. Por exemplo, $p = 5$ e $q = 11$.

2. **Cálculo de n e $\phi(n)$**: Determinamos $n = p \cdot q$ e a função totiente $\phi(n) = (p-1)(q-1)$. Com os valores escolhidos, temos: $n = 5 \cdot 11 = 55$ e $\phi(n) = (5-1)(11-1) = 4 \cdot 10 = 40$.

3. **Escolha da chave pública**: Escolhemos um número x tal que $1 < x < \phi(n)$ e x seja coprimo com $\phi(n)$. Aqui, tomamos $x = 3$.

4. **Cálculo da chave privada**: Determinamos d tal que $1 \equiv x \cdot d \mod (\phi(n))$. Neste caso, $d = 37$.

5. **Criptografia**: Para cifrar uma mensagem m, calculamos $c \equiv m^x \mod (n)$. Se $m = 10$, então $c \equiv 10^3 \mod (55) = 10$.

6. **Descriptografia**: Para decifrar a mensagem, usamos a chave privada d e computamos $m \equiv c^d \mod (n)$, resultando em $m = 10^{37} \mod (55) = 10$.

A segurança do RSA reside na complexidade da fatoração de números grandes. Embora seja simples multiplicar dois números primos para obter n, a operação inversa — determinar p e q a partir de n — é extremamente difícil quando esses números são suficientemente grandes. Essa propriedade é o que torna o RSA um dos sistemas criptográficos mais seguros e amplamente utilizados na atualidade.

4 SEQUÊNCIA DIDÁTICA APLICADA EM UMA ESCOLA

As atividades práticas são fundamentais para complementar e aprimorar os estudos, pois transformam conceitos teóricos em experiências concretas e significativas. Enquanto a teoria fornece a base do conhecimento, a prática permite que os alunos vivenciem, experimentem e apliquem o que aprenderam, consolidando o entendimento e desenvolvendo habilidades essenciais. Ao envolver-se em atividades práticas, o estudante não apenas memoriza informações, mas também desenvolve o pensamento crítico, a criatividade e a capacidade de resolver problemas. Essas atividades estimulam a curiosidade, a investigação e a autonomia, tornando o aprendizado mais dinâmico e engajador. Além disso, a prática permite que os alunos percebam a relevância do conteúdo estudado, conectando-o a situações reais e aplicações cotidianas. No contexto da matemática, por exemplo, atividades como fatoração de números, resolução de problemas e simulações de algoritmos ajudam a solidificar conceitos abstratos, como o Teorema Fundamental da Aritmética, e a compreender sua utilidade em áreas como criptografia e segurança digital. Dessa forma, as atividades práticas não apenas complementam o estudo teórico, mas também preparam os alunos para desafios reais, fortalecendo sua confiança e competência.

A seguir, apresentamos uma sequência didática aplicada em ambiente escolar, detalhando a atividade realizada e oferecendo um relato acompanhado da análise dos dados obtidos durante sua implementação.

4.1 SEQUÊNCIA DIDÁTICA: DECIFRANDO O COFRE

Nesta seção, descrevemos a atividade **Decifrando o cofre**, que preparamos e aplicamos com os alunos de uma escola.

(1) **Conteúdos abordados:** Identificação dos números primos e compostos. Operações com números primos. Decomposição de números em seus fatores primos. Utilização do algoritmo de decomposição.

(2) **Objetivos:** Desenvolver o raciocínio lógico. Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos “é múltiplo de”, “é divisor de”. Decompor números em produto de primos.

(3) **Competências:**

   (a) Compreender a Matemática como ciência autônoma que investiga relações, formas e eventos e desenvolve maneiras próprias de descrever e interpretar o mundo.

   (b) Compreender símbolos, códigos e nomenclatura da linguagem científica e sua utilização na forma oral e escrita.

   (c) Solucionar situações-problema por meio da identificação de informações ou variáveis relevantes e possíveis estratégias para resolvê-las.

(4) **Habilidades:**

(a) Identificar e utilizar símbolos, códigos e nomenclaturas da linguagem matemática.

(b) Interpretar dados ou informações apresentadas em diferentes linguagens e representações.

(c) Identificar os dados relevantes e as relações envolvidas em uma dada situação-problema para buscar possíveis resoluções.

(d) Identificar conceitos, procedimentos e estratégias matemáticas e aplicá-las a situações diversas no contexto das ciências, da tecnologia e das atividades cotidianas.

(5) **Público-alvo:** Alunos do 8° ano, na faixa etária de 13 a 15 anos.

(6) **Perfil das turmas:** Turmas compostas por 20 a 30 alunos.

(7) **Recursos:**

(a) Para cada grupo formado pelos alunos deve haver 5 envelopes com 2 cartões de papel em cada envelope, lápis, caneta e folha de papel.

(b) Os envelopes e os cartões podem ser comprados ou confeccionados pelo professor. Como alternativa aos envelopes pequenas caixas podem ser usadas.

(8) **Avaliação:** Inicialmente aplica-se uma avaliação diagnóstica e ao final de toda atividade outra.

(9) **Atividade:**

(a) Esta atividade prática consiste em decompor números em primos e estes serão a senha para obter o prêmio.

(b) Será dado ao grupo de alunos um envelope com 2 cartões, um em branco e outro com 2 números que serão decompostos. Após fazerem a decomposição, devem escrever os resultados no cartão em branco e entregar ao professor, se as respostas estiverem corretas, eles receberão o próximo envelope para repetir o processo. Ao final de todas as decomposições, os números resultantes serão uma senha, que liberará um prêmio ao grupo. Todos os alunos receberão o prêmio, independente da velocidade em que resolverem as contas.

(c) O professor deverá previamente escrever os números nos cartões.

(d) Cada grupo receberá números diferentes, para que não copiem do grupo ao lado e se concentrem apenas em resolver as suas decomposições.

4.2 RELATÓRIO DA ATIVIDADE

4.2.1 Introdução

A sequência didática foi aplicada em duas turmas de 8º ano ao longo de três dias, utilizando um total de quatro aulas em cada sala. Antes do início das atividades, uma breve conversa com a professora permitiu identificar diferenças marcantes entre as turmas: a turma A era menos participativa e inquieta, mas apresentava bom desempenho em Matemática; já a turma B era mais participativa e disciplinada, mas continha mais alunos com dificuldades na disciplina.

4.2.2 Avaliação diagnóstica inicial

Na primeira aula, após a apresentação, foi aplicada uma avaliação diagnóstica em ambas as turmas, composta por dois exercícios:

– Identificar, entre 17 números, quais eram primos.

– Realizar a decomposição de sete números em fatores primos.

A avaliação diagnóstica inicial pode ser conferida na Seção 4.2.5. Os resultados dessa avaliação diagnóstica estão destacados na Tabela 1.

Tabela 1 – Resultados da avaliação diagnóstica inicial.

Turma	Taxa de Acerto	Observações
8ºA	62%	Dificuldade na identificação de números primos e erros em divisões.
8ºB	50%	Alguns alunos não conheciam números primos; duas alunas destacaram-se com 91% de acertos.

Um erro comum em ambas as turmas foi a associação equivocada de números ímpares a números primos, devido ao uso do critério de divisibilidade por 2 como primeiro teste.

4.2.3 Aulas explicativas e atividade lúdica

No segundo dia, foram ministradas duas aulas em cada turma. A primeira aula focou na explicação dos conceitos de números primos e compostos, além da decomposição em fatores primos. Após a explanação, os alunos resolveram exemplos na lousa. No 8ºA, houve resistência inicial, mas a participação aumentou com a abordagem descontraída em estilo *talk show*. No 8ºB, a participação ocorreu naturalmente.

Na segunda aula, foi introduzida a criptografia como aplicação dos conceitos trabalhados. Os alunos foram divididos em grupos e receberam envelopes com desafios de diferentes níveis de dificuldade, conforme a Tabela 2.

Tabela 2 – Distribuição das Atividades Lúdicas

Turma	Grupos	Total de Decomposições	Distribuição dos Níveis
8ºA	6 grupos (5 a 7 alunos)	10 por grupo	2 fáceis, 2 médios, 1 difícil
8ºB	6 grupos (2 a 6 alunos)	12 por grupo	2 fáceis, 2 médios, 2 difíceis

Durante a atividade, a turma A obteve um aproveitamento de 96% e a turma B, 91%. Os erros concentraram-se nos desafios mais difíceis. Ao final, foi anunciado que os alunos realizariam uma nova avaliação e receberiam prêmios pela conclusão da atividade.

4.2.4 Avaliação diagnóstica final

No terceiro dia, aplicou-se uma nova avaliação diagnóstica, contendo 15 questões. Os alunos receberam os prêmios ao final da prova. Os exercícios dessa avaliação diagnóstica final estão na Seção 4.2.5 e os resultados estão na Tabela 3.

Tabela 3 – Comparação entre avaliação inicial e final.

Turma	Aproveitamento inicial	Aproveitamento final
8ºA	62%	73%
8ºB	50%	66%

O aumento do número de acertos foi mais significativo na decomposição em fatores primos, pois, na primeira avaliação, muitos alunos deixaram questões em branco, enquanto na segunda avaliação tentaram resolvê-las e obtiveram êxito.

4.2.5 Enunciados das avaliações diagnósticas

Aqui, apresentarei o conteúdo das avaliações diagnósticas aplicadas no início e ao final da sequência didática, com o objetivo de mapear a evolução do conhecimento dos alunos sobre o tema.

AVALIAÇÃO DIAGNÓSTICA INICIAL

1. Identifique quais desses números abaixo são primos:

10 -	64 -	103 -	301 -	397 -
11 -	73 -	115 -	309 -	

33 - 81 - 121 - 337 -

37 - 97 - 151 - 359 -

2. Decomponha os seguintes números compostos em seus fatores primos:

14 - 102 - 512 -

25 - 112 -

54 - 204 -

AVALIAÇÃO DIAGNÓSTICA FINAL

1. Identifique quais desses números abaixo são primos:

18 - 211 -

56 - 333 -

71 - 343 -

105 - 429 -

149 - 546 -

2. Decomponha os seguintes números compostos em seus fatores primos:

135 - 392 - 714 -

231 - 637 -

4.2.6 Conclusão

A aplicação da sequência didática mostrou-se eficaz no aprimoramento do aprendizado sobre números primos e decomposição em fatores primos. A abordagem lúdica e interativa contribuiu para o engajamento dos alunos e facilitou a assimilação dos conceitos. O aumento da taxa de acertos na avaliação final evidencia a evolução dos alunos ao longo do processo. Além disso, considera-se que o objetivo da atividade foi plenamente alcançado, pois os alunos que não costumavam ser participativos se envolveram ativamente, enquanto aqueles com mais dificuldades demonstraram ter assimilado os conceitos trabalhados. Ambas as turmas apresentaram uma evolução notória na compreensão do tema, reforçando a efetividade da metodologia adotada.

5 SUGESTÕES DE SEQUÊNCIAS DIDÁTICAS

Além da atividade relatada anteriormente, desenvolvemos algumas outras propostas pedagógicas que buscam tornar o aprendizado mais dinâmico, interativo e significativo. Cada sequência foi cuidadosamente planejada para atender os temas e objetivos iniciais, sempre com foco na integração entre teoria e prática, no estímulo à curiosidade e na aplicação do conhecimento em contextos reais. Elas abrangem desde conceitos matemáticos fundamentais, como números primos e fatoração, até tópicos mais avançados, como criptografia, modelagem matemática e resolução de problemas. Todas são estruturadas com base em metodologias ativas e modelos pedagógicos consagrados, como os 5 Passos de Herbart e a Aprendizagem Significativa, garantindo uma progressão lógica e eficaz no processo de ensino-aprendizagem.

5.1 SEQUÊNCIA DIDÁTICA: CRIPTOGRAFIA COM NÚMEROS PRIMOS

(1) **Público-alvo:** Alunos do Ensino Fundamental II (8º e 9º ano) e Ensino Médio.

(2) **Duração:** Entorno de 2 a 3 aulas de 50 minutos cada.

(3) **Preparação - Ativação de conhecimentos prévios:** Relembrar o conceito de números primos e introduzir a ideia de criptografia e sua importância.

(4) **Atividade - primos *vs.* compostos:** Escreva números no quadro (até 50). Em seguida, diga, ao acaso, os números, quando os alunos acharem que o número for primo eles levantam e quando for compostos permanecem sentados. Durante e ao final, discuta o que diferencia primos e compostos.

(5) **Tabela de números primos:** Entregue uma tabela de números de 1 a 50 para que os alunos encontrem os primos.

(6) **Introdução à criptografia:** Pergunte: “Como podemos transformar mensagens em códigos secretos?”. Mostre exemplos simples, como a cifra de César.

(7) **Recursos:**

   (a) Quadro ou slides com números primos e compostos.

   (b) Tabelas impressas de números de 1 a 50.

   (c) Exemplos visuais de códigos criptográficos.

(8) **Apresentação (introdução ao conteúdo):** Explicar a fatoração e sua relação com criptografia.

(9) **Atividade - explicação interativa sobre fatoração:**

   (a) Mostre exemplos de decomposição de números em fatores primos:
   $15 = 3 \cdot 5$
   $28 = 2 \cdot 2 \cdot 7$
   (b) Peça que os alunos fatorarem outros números em duplas.
   (c) Pergunte: "Se eu disser que um número grande é o produto de dois primos, vocês conseguem descobrir quais são?"
   (d) Dê um exemplo fácil (exemplo: $391 = 17 \cdot 23$) e outro difícil.

(10) **Associação (ligação com criptografia):** Mostrar como a fatoração de números primos está ligada à segurança digital.

(11) **Atividade - simulação do RSA com alunos:**

   (a) Escolha dois alunos para serem "remetente" e "destinatário".
   (b) Eles escolhem dois primos pequenos e multiplicam.
   (c) A turma tenta quebrar o código.

(12) **Pesquisa sobre criptografia no dia a dia:** Em grupos, os alunos investigam onde a criptografia é usada (WhatsApp, bancos, senhas).

(13) **Recursos:**

   (a) Cartões com números primos para a simulação.
   (b) Acesso a computadores ou celulares para pesquisa (opcional).

(14) **Generalização - consolidação do conhecimento:** Relacionar a dificuldade de fatoração com segurança digital.

(15) **Atividade - exemplo do RSA simplificado:**

   (a) Escolha dois números primos (ex: 3 e 5).
   (b) Multiplique-os (15) e use isso como chave pública.
   (c) Discuta por que é difícil quebrar esse código com números grandes.
   (d) Pergunte: "Por que acham que usamos números grandes para segurança digital?".
   (e) Relacione com a pesquisa dos alunos sobre criptografia no dia a dia.
   (f) Recursos: vídeo curto ou slides sobre criptografia RSA.

(16) **Aplicação - atividade prática:** Aplicar os conceitos criando e decifrando códigos.

(17) **Atividade - criação de códigos:**

   (a) Cada grupo escolhe uma palavra e transforma em números ($A = 1, B = 2, \ldots, Z = 26$).

(b) Depois, fatoram os números para esconder a mensagem.

(c) Os grupos trocam mensagens e tentam decifrar as dos colegas.

(d) Os alunos compartilham dificuldades e reflexões sobre a atividade.

(e) Recursos: folhas com tabelas de números primos e alfabeto, e calculadoras (opcional).

(18) **Dicas para tornar a atividade mais engajadora:**

(a) Competição: os grupos que decifrarem mais mensagens ganham pontos.

(b) Uso de tecnologia: aplicativos ou sites que simulam criptografia.

(c) Contextualização: casos reais de onde a criptografia é usada.

(19) **Avaliação:**

(a) Participação nas atividades em grupo.

(b) Apresentação dos códigos criados e explicação do processo.

(c) Desafio final: fatorar um número e criar uma mensagem curta.

5.2 SEQUÊNCIA DIDÁTICA: NÚMEROS PRIMOS

(1) **Público-alvo:** alunos do Ensino Fundamental II (8º e 9º ano) e Ensino Médio.

(2) **Duração:** entorno de 2 a 3 aulas de 50 minutos cada.

(3) **Preparação - ativação de conhecimentos prévios:** introduzir a ideia de números primos e sua importância e relembrar conceitos de divisibilidade e fatores.

(4) **Atividade - desafio inicial: O que é um número primo?**

(a) Escreva no quadro os números 1 a 20 e pergunte quais são primos

(b) Peça que justifiquem suas respostas

(5) **Jogo "Quem sou eu?":** cada aluno recebe um cartão com um número e deve descobrir, com dicas dos colegas, se é primo ou composto.

(6) **Discussão:**

(a) O que diferencia primos de compostos?

(b) Por que 1 não é primo?

(7) **Recursos:** quadro ou projetor, e cartões com números de 1 a 50.

(8) **Apresentação (introdução ao conteúdo):** explicar formalmente o conceito de números primos e mostrar seu papel fundamental na matemática.

(9) **Atividade - definição de número primo:**

(a) Número primo é aquele que tem exatamente dois divisores: 1 e ele mesmo.

(b) Exploração com exemplos: liste alguns números primos e compostos e peça que os alunos os classifiquem.

(c) Tabela de crivo de Eratóstenes: peça que os alunos descubram números primos até 100 eliminando os múltiplos dos menores primos.

(d) Recursos: quadro ou slides com definição e exemplos, e folhas com a tabela de 1 a 100 para aplicação do crivo.

(e) Associação (conexão com outros conceitos matemáticos): relacionar números primos com divisibilidade e fatoração.

(10) **Atividade - fatoração em primos:**

(a) Peça que os alunos decomponham números em fatores primos.

(b) Exemplo: $30 = 2 \cdot 3 \cdot 5$ e $42 = 2 \cdot 3 \cdot 7$.

(11) **Desafio: Quem chega mais longe?**

(a) Cada grupo recebe um número grande e deve fatorá-lo corretamente.

(b) O primeiro grupo a concluir corretamente ganha pontos.

(c) Pergunte: Todos os números compostos podem ser escritos como produtos de primos? Isso é sempre único? (Teorema Fundamental da Aritmética)

(d) Recursos: fichas com números para fatoração e calculadoras opcionais para números maiores.

(e) Generalização - consolidação do conhecimento: mostrar a importância dos números primos na matemática e em aplicações do dia a dia.

(12) **Atividade - exploração histórica:**

(a) Pergunte: Quem foi Eratóstenes? Como os números primos aparecem na natureza e na tecnologia?

(b) Os alunos pesquisam e apresentam onde os números primos são utilizados (exemplo: criptografia, segurança digital, padrões na natureza).

(c) Na sequência pergunte: “O que aconteceria se não houvesse números primos?”.

(d) Recursos: textos curtos sobre a história dos números primos e acesso à internet ou materiais impressos sobre aplicações.

(e) Aplicação - atividade prática: aplicar o conhecimento sobre números primos em desafios práticos.

(13) **Atividade - jogo de desafio rápido:**

(a) Os alunos recebem cartões com números e devem agrupá-los rapidamente em primos e compostos.

(b) Cada grupo cria e resolve problemas sobre primos e fatoração.

(c) Dado um conjunto de números grandes, os alunos devem identificar quais são primos.

(d) Recursos: cartões e fichas com números e calculadoras (opcional)

(14) **Dicas para tornar a atividade mais engajadora:**

(a) Gamificação: transformar desafios em uma competição com pontuação.

(b) Uso de tecnologia: aplicativos ou sites para verificar as respostas.

(c) Curiosidades: apresentar padrões dos números primos e conjecturas abertas.

(15) **Avaliação:**

(a) Participação nas discussões e atividades.

(b) Resolução correta de desafios matemáticos.

(c) Capacidade de explicar e aplicar os conceitos em novos contextos.

6 CRIPTOSSISTEMAS SEMELHANTES

6.1 INTRODUÇÃO

A decomposição de números inteiros em fatores primos é um problema central em diversas abordagens criptográficas. Criptossistemas como os de Rabin e Blum-Goldwasser utilizam essa propriedade em sua estrutura (Alfred J. Menezes Paul C. van Oorschot, 1996). Dentre esses, destaca-se o criptossistema de Paillier (Paillier, 1999), amplamente utilizado em aplicações como votações eletrônicas e computação segura em nuvem.

Os criptossistemas de Rabin e Blum-Goldwasser são baseados no Problema da Residuosidade Quadrática (QRP), enquanto o criptossistema de Paillier fundamenta-se no Problema da Residuosidade Composta (CRP). A seguir, discutimos esses problemas em detalhes.

6.2 PROBLEMA DA RESIDUOSIDADE QUADRÁTICA

O Problema da Residuosidade Quadrática consiste em determinar, dado um número inteiro a e um módulo n, se existe um inteiro x tal que:

$$x^2 \equiv a \mod (n). \tag{6.1}$$

Se tal x existir, dizemos que a é um resíduo quadrático módulo n. Caso contrário, a é um não-resíduo quadrático módulo n.

6.2.1 Exemplo

Considere $n = 7$ e $a = 2$. Precisamos verificar se existe um x tal que:

$$x^2 \equiv 2 \mod (7). \tag{6.2}$$

Testando alguns valores, temos:

- $x = 1$: $1^2 = 1 \equiv 1 \mod (7)$;
- $x = 2$: $2^2 = 4 \equiv 4 \mod (7)$;
- $x = 3$: $3^2 = 9 \equiv 2 \mod (7)$.

Como $x = 3$ satisfaz a equação, concluímos que 2 é um resíduo quadrático módulo 7. Além disso, se testarmos $x = 4$, obtemos:

$$4^2 = 16 \equiv 2 \mod (7). \tag{6.3}$$

Isso evidencia que a equação pode ter múltiplas soluções, o que impacta diretamente a segurança de criptossistemas baseados nesse problema.

6.3 PROBLEMA DA RESIDUOSIDADE COMPOSTA

O Problema da Residuosidade Composta (CRP) é uma generalização do QRP. Dado um número composto n (geralmente o produto de dois ou mais primos grandes) e um número inteiro a, o problema consiste em determinar se a é um resíduo de ordem superior módulo n, ou seja, se existe um número inteiro x tal que:

$$x^k \equiv a \mod (n), \tag{6.4}$$

para algum $k \geq 2$.

6.3.1 Exemplo

Considere $n = 15$ e $a = 8$. Precisamos verificar se existe um x tal que:

$$x^3 \equiv 8 \mod (15). \tag{6.5}$$

Testando alguns valores, encontramos:

- $x = 2$: $2^3 = 8 \equiv 8 \mod (15)$;
- $x = 3$: $3^3 = 27 \equiv 12 \mod (15)$;
- $x = 4$: $4^3 = 64 \equiv 4 \mod (15)$;
- $x = 5$: $5^3 = 125 \equiv 5 \mod (15)$.

Além disso, para $x = 17$ e $x = 32$, também obtemos:

- $x = 17$: $17^3 = 4913 \equiv 8 \mod (15)$;
- $x = 32$: $32^3 = 32768 \equiv 8 \mod (15)$.

Isso mostra que o problema pode apresentar múltiplas soluções, o que influencia a segurança de criptossistemas baseados nessa abordagem.

6.4 A RELAÇÃO COM NÚMEROS PRIMOS

A segurança dos criptossistemas baseados no QRP e no CRP está intimamente ligada à fatoração de números compostos. Em geral, os módulos n utilizados nesses sistemas são

escolhidos como produtos de dois grandes números primos p e q, de modo que:

$$n = p \cdot q. \tag{6.6}$$

A dificuldade de fatorar n impede que um atacante determine diretamente os resíduos quadráticos ou compostos, garantindo a segurança do sistema. Além disso, a distribuição dos resíduos quadráticos e compostos depende das propriedades aritméticas dos primos envolvidos, tornando a resolução desses problemas computacionalmente difícil sem o conhecimento da fatoração de n.

Essa dificuldade está no cerne de muitos protocolos criptográficos modernos, como a criptografia homomórfica e os sistemas de assinatura digital, onde a segurança repousa na ineficiência de algoritmos clássicos para fatoração de inteiros.

6.5 CONCLUSÃO

O Problema da Residuosidade Composta (CRP) pode ser visto como uma generalização do Problema da Residuosidade Quadrática (QRP). Dessa forma, criptossistemas como os de Rabin, Blum-Goldwasser e Paillier derivam sua segurança da dificuldade computacional associada à determinação de resíduos quadráticos ou compostos módulo n. Em particular, a segurança desses sistemas depende fortemente da dificuldade de fatorar números compostos, o que reforça sua aplicabilidade na criptografia moderna.

7 CONSIDERAÇÕES FINAIS

De maneira objetiva, podemos afirmar que o conceito de divisibilidade precede o de número primo, uma vez que este último é definido com base no primeiro. Assim, os números primos emergem naturalmente do estudo da divisibilidade, pois, ao realizarmos sucessivas divisões de um número até que não seja mais possível prosseguir, chegamos inevitavelmente a um número indivisível além de por si próprio e pela unidade, caracterizando-o como primo.

A interdependência entre divisibilidade e números primos é inegável, especialmente considerando a decomposição em fatores primos, que utiliza ambos os conceitos de forma essencial. Esse vínculo fundamental transcende a teoria dos números e encontra aplicações diretas em áreas como a criptografia, onde a fatoração de números inteiros desempenha um papel crucial na segurança da informação.

Com os avanços tecnológicos e o desenvolvimento de novas linguagens de programação, o uso da teoria dos números, em particular a fatoração em primos, tornou-se cada vez mais recorrente, sobretudo na criptografia moderna. A necessidade de métodos seguros para transmissão de dados e autenticação levou à criação de sistemas criptográficos robustos, entre os quais se destaca o RSA, cuja segurança baseia-se na dificuldade computacional de fatorar grandes números compostos em seus fatores primos.

Apesar de a divisibilidade e os números primos serem conceitos matemáticos estudados há mais de dois mil anos, sua relevância permanece incontestável na contemporaneidade. Mesmo que seu impacto passe despercebido no cotidiano, sua presença é fundamental para o funcionamento de dispositivos eletrônicos, redes de comunicação e transações digitais seguras.

O Teorema Fundamental da Aritmética (TFA) constitui um dos pilares da teoria dos números, ao garantir que todo número inteiro positivo maior que um pode ser decomposto de maneira única (salvo a ordem dos fatores) em fatores primos. Ao longo deste estudo, analisamos suas implicações teóricas e exploramos sua aplicação na criptografia, evidenciando como a fatoração prima pela simplicidade conceitual, mas se torna computacionalmente complexa quando aplicada a números suficientemente grandes.

Durante a elaboração deste trabalho, encontramos uma vasta literatura abordando a teoria dos números primos e da divisibilidade, dado que esses temas são amplamente estudados desde o Ensino Fundamental até o Ensino Superior. No entanto, ao buscar aplicações contemporâneas acessíveis para um público não especializado, observamos uma carência significativa de materiais didáticos que expliquem, de forma clara, o papel dos números primos na criptografia e na segurança digital. Embora o uso de mensagens criptografadas seja amplamente difundido, a compreensão dos fundamentos matemáticos por trás dessas tecnologias ainda é limitada para a maioria das pessoas.

Essa constatação ressalta a importância de desenvolver conteúdos e estratégias pedagógicas que tornem os criptossistemas mais compreensíveis, conectando-os a conceitos fundamentais como o TFA. Isso não apenas amplia o conhecimento sobre matemática aplicada, mas também

capacita estudantes e profissionais a compreender a importância da segurança da informação no mundo digital.

Por fim, a elaboração deste estudo proporcionou um enriquecimento significativo da minha compreensão sobre o tema. A investigação de diferentes abordagens e aplicações consolidou meu conhecimento e ampliou minha perspectiva sobre o ensino da teoria dos números. Durante minha graduação, devido à pandemia, não tive a oportunidade de aplicar atividades em sala de aula, mas, com a conclusão deste trabalho, sinto-me mais preparado para atuar no ensino, promovendo uma aprendizagem significativa sobre um tema de grande relevância teórica e prática.

REFERÊNCIAS

ALFRED J. MENEZES PAUL C. VAN OORSCHOT, Scott A. Vanstone. **Handbook of Applied Cryptography**. [S.l.]: CRC Press, 1996. Citado na p. 27.

BRASIL. **Base Nacional Comum Curricular (BNCC). Educação é a Base**. [S.l.]: MEC/CONSED/UNDIME, 2018. Citado na p. 6.

DOMINGUES, Hygino H. **Fundamentos de Aritmética**. São Paulo: Editora Atual, 1991. Citado na p. 9.

GALDINO, Uelder Alves. **Teoria dos Números e Criptografia com Aplicações Básicas**. 2014. Trabalho de Conclusão de Curso (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) – Universidade Federal da Paraíba. Citado na p. 15.

HARDY, G. H.; WRIGHT, E. M. **An Introduction to the Theory of Numbers**. 6th. [S.l.]: Oxford University Press, 2008. Citado na p. 13.

MILIES, César Polcino; COELHO, Sônia Pitta. **Números: Uma introdução à Matemática**. 3. ed. São Paulo: EdUSP, 2001. Citado na p. 9.

PAILLIER, Pascal. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. **IEEE Xplore**, 1999. Citado na p. 27.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. **Communications of the ACM**, 1978. Citado na p. 14.

ROSEN, Kenneth H. **Elementary Number Theory and its Applications**. [S.l.]: ddison-Wesley, 1993. Citado na p. 15.