COLÉGIO PEDRO II

Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura
Mestrado Profissional em Matemática em Rede Nacional

Leandro Jeferson Tôrres Ferreira

NÚMEROS PRIMOS, CRIPTOGRAFIA RSA, PROBLEMAS DO MILÊNIO E A SEGURANÇA DA INFORMAÇÃO

Rio de Janeiro

2020

Leandro Jeferson Tôrres Ferreira

NÚMEROS PRIMOS, CRIPTOGRAFIA RSA, PROBLEMAS DO MILÊNIO E A SEGURANÇA DA INFORMAÇÃO

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, vinculado à Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Dr^{a}. Luciana Santos da Silva Martino

Rio de Janeiro

2020

COLÉGIO PEDRO II

PRÓ-REITORIA DE PÓS-GRADUAÇÃO, PESQUISA, EXTENSÃO E CULTURA

BIBLIOTECA PROFESSORA SILVIA BECHER

CATALOGAÇÃO NA FONTE

F383 Ferreira, Leandro Jeferson Tôrres
Números primos, criptografia RSA, problemas do milênio e a segurança da informação / Leandro Jeferson Tôrres Ferreira. – Rio de Janeiro, 2020.
85 f.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Colégio Pedro II. Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura.
Orientador: Luciana Santos da Silva Martino.

1. Matemática – Estudo e ensino. 2. Números primos. 3. Criptografia. 4. Segurança da informação. I. Martino, Luciana Santos da Silva. II. Colégio Pedro II. III. Título.

CDD 510

Ficha catalográfica elaborada pela Bibliotecária Simone Alves – CRB7 5692.

Leandro Jeferson Tôrres Ferreira

NÚMEROS PRIMOS, CRIPTOGRAFIA RSA, PROBLEMAS DO MILÊNIO E A SEGURANÇA DA INFORMAÇÃO

Dissertação de Mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional, vinculado à Pró-Reitoria de Pós-Graduação, Pesquisa, Extensão e Cultura do Colégio Pedro II, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em: _____/_____/_____.

Banca Examinadora:

Drª. Luciana Santos da Silva Martino
Colégio Pedro II

Drª. Maria de Lourdes Rocha de Assis Jean-renaud
Colégio Pedro II

Drª. Cristiane Oliveira de Faria
Universidade do Estado do Rio de Janeiro

Rio de Janeiro
2020

Dedico, primeiramente, à Deus e à minha linda família que tanto amo: Taís, Jacijane, Laura e Felipe.

AGRADECIMENTOS

Agradeço primeiramente a Deus por mais esta conquista e por ser O Autor da minha história.

Agradeço aos meus pais, Jacijane e Jessé (em memória), pelo incentivo que sempre deram em minha jornada acadêmica e em toda a minha vida. Meus amores, muito obrigado.

À minha esposa, Taís, e à minha filha, Laura, a paciência e o amor que sempre me dedicaram todos os dias, mesmo estando um pouco "ausente" devido aos meus estudos. Amo vocês demais.

À minha professora orientadora, Luciana Martino, pela paciência e incentivo na hora certa. Obrigado por sua dedicação.

Agradeço também aos colegas de minha turma.

Agradeço aos meus queridos professores do PROFMAT que me auxiliaram com muito zelo e dedicação tornando essa jornada mais agradável. Em particular, agradeço à professora Marilis Bahr Karam Venceslau, por todo auxílio, dedicação e carinho que sempre demonstrou a mim e a meus colegas de curso.

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

"Uma vez um matemático me falou que o verdadeiro prazer não está em achar a verdade, mas em procurar por ela".

(Leo Tolstoy)

RESUMO

FERREIRA, Leandro Jeferson Tôrres. Números primos, criptografia RSA, problemas do milênio e a segurança da informação. 2020. 85 f. Dissertação (Mestrado) – Colégio Pedro II, Pró-Reitoria de Pós- Graduação, Pesquisa, Extensão e Cultura, Programa de Mestrado Profissional em Matemática em Rede Nacional, Rio de Janeiro, 2020.

Números Primos é um conceito fundamental dentro da Aritmética, porém, pouco explorado no Ensino Básico. Muitas questões sobre estes números ainda encontram-se sem solução, no entanto, estudos têm sido realizados na busca pelo conhecimento de conjecturas, como a Hipótese de Riemann, um dos Problemas do Milênio, que apresenta relação direta com o comportamento dos Números Primos e sua distribuição dentro dos Números Naturais. Uma importante aplicação dos Números Primos é a Criptografia RSA, considerada um método seguro para troca de informações pela internet, incluindo transações bancárias, estratégias militares e informações governamentais. Este estudo, inicialmente, aborda os conceitos sobre os Números Inteiros e noções sobre Congruências Modulares que servem como base teórica para os outros capítulos. Logo após são apresentados o conceito de Números Primos, e também suas propriedades mais importantes e suas conjecturas em aberto. Em seguida, é abordado o estudo sobre a Criptografia, desde as técnicas mais primitivas até os estudos mais recentes e a técnica da Criptografia RSA e como sua base matemática a torna tão segura. Por fim, são apresentados dois Problemas do Milênio: A Hipótese de Riemann e o Problema P = NP que, se demonstrados, influenciarão toda a segurança dos métodos criptográficos atuais e, consequentemente, a segurança das informações que transitam pela rede mundial de computadores. Também são propostas atividades que têm, por finalidade, estimular estudantes de 6º ao 9º anos do Ensino Fundamental e também do Ensino Médio ao aprendizado dos Números Primos e suas aplicações.

Palavras-chave: Números Primos; Aritmética; Criptografia RSA; Hipótese de Riemann; Problemas do Milênio.

ABSTRACT

FERREIRA, Leandro Jeferson Tôrres. Números primos, criptografia RSA, problemas do milênio e a segurança da informação. 2020. 85 f. Dissertação (Mestrado) – Colégio Pedro II, Pró-Reitoria de Pós- Graduação, Pesquisa, Extensão e Cultura, Programa de Mestrado Profissional em Matemática em Rede Nacional, Rio de Janeiro, 2020.

Prime Numbers is a fundamental concept within Arithmetic, however, little explored in Basic Education. Many questions about these numbers are still unsolved, however, studies have been carried out in the search for knowledge of conjectures, such as the Riemann Hypothesis, one of the Millennium Problems, which is directly related to the behavior of Prime Numbers and their distribution within Natural Numbers. An important application of Prime Numbers is RSA Cryptography, considered a secure method for exchanging information over the internet, including bank transactions, military strategies and government information. This study initially addresses the concepts of Numbers Integers and notions about Modular Congruences that serve as a theoretical basis for the other chapters. Soon after, the concept of Prime numbers, as well as their most important properties and their open conjectures. Then, the study on the Cryptography, from the most primitive techniques to the most recent studies and the RSA Cryptography technique and as its mathematical basis a makes it so safe. Finally, two Millennium Problems are presented: The Riemann Hypothesis and the P = NP Problem which, if demonstrated, influence the security of current cryptographic methods and, consequently, the security of information world Wide Web. Activities are also proposed that aim to stimulate students from the 6th to the 9th grade of Education Elementary and also from High School to the learning of Prime Numbers and their applications.

Keywords: Prime numbers; Arithmetic; RSA encryption; Riemann Hypothesis; Millennium Problems.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

A Matemática é uma ciência muito rica em seu conteúdo e, principalmente, em suas aplicações. No entanto, no Ensino Básico, não é incomum que um professor de Matemática seja interpelado por um estudante sobre quais são as aplicações de um determinado conceito em seu cotidiano ou qual a necessidade do aprendizado de determinado assunto relacionado à Matemática. Estes casos são decorrentes de um currículo básico escolar de Matemática sem conexão com a realidade do estudante e sem motivação para o aprendizado. O indivíduo, em geral, procura aprender algo que seja importante, utilizável ou mesmo curioso. Qualidades que não são mais reconhecidas pela maioria de nossos jovens e adolescentes na Matemática.

Analisando este cenário de nosso Ensino Básico e refletindo acerca de conteúdos pouco explorados em nosso currículo escolar, destacamos os Números Primos. Neste caso específico, na maior parte das vezes o conteúdo abordado fica restrito à definição inicial de Número Primo e à decomposição de números naturais em fatores primos. Não são consideradas suas principais propriedades e curiosidades.

Sobre os Números Primos existem diversas conjecturas que poderiam estimular a curiosidade de um estudante por seu estudo. Por outro lado, estes números servem de base para diversas aplicações como a criptografia moderna, e que fazem parte do cotidiano de toda população mundial. Exemplo de tais aplicações se encontram na troca de *e-mails*, transações bancárias e no sigilos de conversas por aplicativos de mensagens, entre outras.

Assim, temos como objetivo nesta pesquisa, estimular nosso aluno do Ensino Básico ao estudo da Matemática por meio do conhecimento de propriedades, curiosidades e aplicações dos Números Primos. Vale ainda ressaltar nesta pesquisa, a importância dos Problemas do Milênio e como se relacionam com a criptografia RSA e os Números Primos.

Esta pesquisa é composta por sete capítulos, dos quais o primeiro está desenvolvido neste texto introdutório. No segundo capítulo, abordamos os conceitos e propriedades dos Números Inteiros e Congruência Modular, assuntos estes que são a base para resultados mais complexos sobre os Números Primos e sobre os cálculos da criptografia RSA. O terceiro capítulo é dedicado aos Números Primos: definição, principais propriedades e conjecturas em aberto. No quarto capítulo é desenvolvido o tema sobre a criptografia, desde a técnica esteganográfica até a criptografia RSA, e quais as implicações desta última na segurança da informação. No quinto capítulo apresentamos a Hipótese de Riemann e o problema $P = NP$, destacando sua relação com os Números Primos e sua importância para a segurança da informação. Vale ressaltar que a leitura deste capítulo, em questão, independe dos capítulos anteriores. No sexto capítulo, são listadas atividades que podem

ser implementadas em tempo apropriado com estudantes do Ensino Básico para estimular o estudo e aprendizagem da Matemática. Foram elaborados dois produtos pedagógicos: Cubo de Vigenère e Dominó de Goldbach para serem aplicados em sala de aula. No último capítulo, são realizadas as considerações finais desta pesquisa.

2 NÚMEROS INTEIROS E CONGRUÊNCIAS

Este capítulo inicial visa a construir uma base teórica em que todo o trabalho esteja sustentado. O conteúdo sobre Números Inteiros é a parte da Aritmética em que são baseados os conceitos de Número Primo e de Congruência Modular, princípios matemáticos da Criptografia RSA, a ser melhor formulada nos próximos capítulos.

2.1 Números Inteiros - História e Definição

Os Números Inteiros e suas propriedades formam os pilares para o estudo da Aritmética. Atualmente, o conceito de Número Inteiro se apoia em estudos que envolvem estruturas algébricas como Grupos e Anéis, o que pode ser visto em (CIPRIANO, 2016).

No entanto, nem sempre o conceito geral sobre tais números foi considerado aceito em termos formais. Na Antiguidade não há registros sobre o uso de números negativos pelos povos egípcios, gregos ou babilônicos (EVES, 2004). O mais antigo relato foi encontrado na China, entre o décimo e o segundo séculos de nossa Era, sendo utilizados na resolução de alguns problemas cotidianos.

Ao longo da história, diversos matemáticos estudaram os números negativos isoladamente ou como parte de outros estudos. Porém, em sua grande maioria, estes matemáticos, até o século XVII, consideravam os números negativos como "erros" ou raízes falsas de certas equações, como o matemático francês René Descartes ($1596 - 1650$), na obra *La Géométrie*, publicada em 1637.

A obra *Tratado da Álgebra*, do matemático Colin MacLaurin ($1698-1746$), publicada postumamente em 1748, teve um papel fundamental ao considerar a importância dos números negativos e dar os primeiros passos para um conceito matemático mais formal sobre os Números Inteiros (BOYER, 2012).

O grande matemático Augustin-Louis Cauchy ($1789 - 1857$) estudou os números negativos e se tornou o responsável pela definição de *quantidades negativas* que, segundo ele, seriam grandezas que diminuem, representadas pelo sinal (-), a definição de Cauchy trazia uma ambiguidade em relação aos números inteiros, quanto aos sentidos: operatórios (somar ou diminuir) e predicativos (positivo ou negativo). Posteriormente, chegou à conclusão que esta definição não era correta. Cauchy foi responsável por formalizar as quatro operações básicas utilizando números positivos e negativos.

Outra notável contribuição foi apresentada por Richard Dedekind ($1831 - 1916$), que estabeleceu uma relação de equivalência entre pares de números naturais, mostrando a subtração como operação inversa da adição.

Deve-se à Hermann Hankel $(1839 - 1873)$ a formulação de princípios e critérios que nortearam a compreensão sobre os números inteiros, em sua publicação *Teoria do Sistema dos Números Complexos*, de 1867 (EVES, 2004).

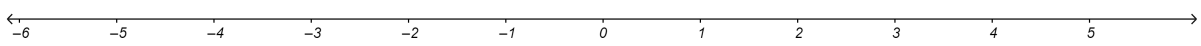
Outra definição importante foi a do número zero. Os indianos foram os primeiros a considerarem o zero no seu sistema numérico posicional, entre os séculos III e IV de nossa Era. O zero era chamado de *sünya*, que significa "vazio" (PADRÃO, 2008).

Finalmente, define-se o conjunto dos Números Inteiros, simbolizado pela letra $\mathbb{Z}$ (z de *zahlen*, "número" em alemão), como sendo o conjunto dos números positivos e negativos e o número zero:

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

Geometricamente, cada número inteiro pode ser associado a um ponto da reta numerada da Figura 1.

Figura 1 – Reta Numérica em $\mathbb{Z}$



Dentre os seus subconjuntos mais notáveis temos o conjunto dos Números Naturais $\mathbb{N} = \{1, 2, 3, 4, ...\}$.

2.1.1 Propriedades da Adição e Multiplicação

No conjunto dos Números Inteiros as operações de adição e multiplicação, entre a e b, são definidas da seguinte forma: $(a, b) \longmapsto a + b \in \mathbb{Z}$ e $(a, b) \longmapsto a \cdot b = ab \in \mathbb{Z}$. A seguir serão exibidos um conjunto de axiomas que caracterizam o conjunto dos Números Inteiros (HEFEZ, 2016):

a. As operações de adição e multiplicação são bem definidas

   $\forall a, b, a', b' \in \mathbb{Z}, a = a'$ e $b = b' \Rightarrow a + b = a' + b'$ e $a \cdot b = a' \cdot b'$

b. Fechamento dos Números Inteiros em relação às operações de adição e multiplicação.

   O conjunto dos Números Inteiros é fechado em relação às operações de adição e multiplicação, isto é, $\forall a, b \in \mathbb{Z}$, $a + b \in \mathbb{Z}$ e $ab \in \mathbb{Z}$

c. Comutatividade

   $\forall a, b \in \mathbb{Z}$, $a + b = b + a$ e $ab = ba$

d. Associatividade

   $\forall a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

e. Elemento Neutro

$\forall a \in \mathbb{Z}$, $a + 0 = a$ e $a \cdot 1 = a$

f. Elemento Simétrico da adição

$\forall a \in \mathbb{Z}$, $\exists b = -a$ tal que $a + b = 0$

g. Multiplicação distributiva em relação à adição

$\forall a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$

Essas primeiras propriedades caracterizam o conjunto dos Números Inteiros como um anel comutativo com unidade.

Pela definição de número inteiro, $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$, onde $-\mathbb{N}$ é o conjunto que representa os elementos simétricos (ou opostos) em $\mathbb{Z}$.

Outra definição importante é a de módulo de um número inteiro n (ou valor absoluto):

$$|n| = \begin{cases} n, & se \quad n \geq 0 \\ -n, & se \quad n < 0 \end{cases}$$

Dois inteiros distintos que possuem o mesmo módulo são simétricos (ou opostos) entre si.

A seguir serão exibidas propriedades que se referem à ordenação dos Números Inteiros:

h. Tricotomia.

Sejam $a, b \in \mathbb{Z}$, uma e somente uma das afirmações é verificada:

- $a = b$
- $b - a \in \mathbb{N}$, isto é, $a < b$. Denomina-se a diferença entre b e a como $b - a$. Consequentemente, define-se a subtração entre b e a, como a soma entre b e o simétrico de a.
- $-(b - a) = a - b \in \mathbb{N}$, isto é, $b < a$

i. Princípio da Boa Ordenação.

O princípio da Boa Ordenação em $\mathbb{Z}$ pode ser enunciado da seguinte forma:

Seja A um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente. Então A possui um menor elemento.

O conjunto $A \subset \mathbb{Z}$ é limitado inferiormente se existe $b \in \mathbb{Z}$ tal que $b \leq x$, $\forall x \in A$, ou seja, b é cota inferior de A. Dizemos que $a \in A$ é o menor elemento de A, se $a \leq x$, $\forall x \in A$, sendo a a maior das cotas inferiores.

2.1.2 Outros resultados importantes

Serão exibidos, em seguida, outros resultados importantes que servirão como base para o estudo das congruências.

Teorema 2.1.1. $\forall a \in \mathbb{Z},\ a \cdot 0 = 0$

Demonstração. Utilizando as propriedades anteriores:

$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

Somando $-(a \cdot 0)$ aos dois membros da igualdade, teremos: $-a \cdot 0 + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0) \Longrightarrow 0 = (-a \cdot 0 + a \cdot 0) + a \cdot 0 \Longrightarrow 0 = 0 + a \cdot 0 \Longrightarrow 0 = a \cdot 0, \forall a \in \mathbb{Z}$ □

Teorema 2.1.2. $\forall a, b, c \in \mathbb{Z},\ a = b \Leftrightarrow a + c = b + c$

Demonstração. ($\Rightarrow$) $a = b \Rightarrow a + c = b + c$ pois a operação de adição é bem definida em $\mathbb{Z}$

($\Leftarrow$) $a + c = b + c$, somando $(-c)$ em ambos os membros da igualdade:

$(a + c) + (-c) = (b + c) + (-c) \Longrightarrow a + (c - c) = b + (c - c) \Longrightarrow a + 0 = b + 0 \Longrightarrow a = b$ □

Teorema 2.1.3. $\forall a, b, c \in \mathbb{Z},\ a < b\ e\ b < c \Rightarrow a < c$

Demonstração. Seja $a < b$ e $b < c$, temos que $b - a \in \mathbb{N} \subset \mathbb{Z}$ e $c - b \in \mathbb{N} \subset \mathbb{Z}$

Logo, pela propriedade do fechamento:

$(b-a)+(c-b) \in \mathbb{N} \subset \mathbb{Z}$, logo $b-a+c-b = b-b-a+c = c-a+0 = c-a \in \mathbb{N} \subset \mathbb{Z}$

Portanto, $a < c$ □

Teorema 2.1.4. $\forall a, b, c \in \mathbb{Z},\ a < b \Leftrightarrow a + c < b + c$

Demonstração. ($\Rightarrow$) Se $a < b \Longrightarrow b - a \in \mathbb{N} \subset \mathbb{Z}$

Logo, $b - a = b - a + 0 = b - a + c - c = (b + c) - (a + c) \in \mathbb{N} \subset \mathbb{Z}$

Portanto, $a + c < b + c$

($\Leftarrow$) Supondo $a + c < b + c$, somando-se $-c$ em ambos os membros da desigualdade temos $a < b$ □

Teorema 2.1.5. $\forall a, b \in \mathbb{Z},\ \forall c \in \mathbb{N},\ a < b \Leftrightarrow ac < bc$

Demonstração. ($\Rightarrow$) Seja $a < b \Longrightarrow b - a \in \mathbb{N}$. Como $\mathbb{N}$ é fechado com relação à multiplicação, então $(b - a) \cdot c = bc - ac \in \mathbb{N}$. Logo, $ac < bc$.

($\Leftarrow$) Reciprocamente, se $ac < bc$, com $c \in \mathbb{N}$. Então, $bc - ac > 0 \Longrightarrow (b - a) \cdot c > 0$, como $c > 0$, logo $b - a > 0 \Longrightarrow a < b$. □

Teorema 2.1.6. $\forall a, b \in \mathbb{Z}$, $\forall c \in \mathbb{Z} - \{0\}$, $a = b \Leftrightarrow ac = bc$

Demonstração. ($\Rightarrow$) Supondo $a, b \in \mathbb{Z}$ e $c \in \mathbb{Z}$, $a = b \Longrightarrow ac = bc$, a afirmação é válida pelo fato da operação de multiplicação ser bem definida em $\mathbb{Z}$.

($\Leftarrow$) Se $ac = bc$, então $ac - bc = 0 \Longrightarrow (a - b) \cdot c = 0$, como $c \neq 0$, então, $a - b = 0$. Logo, $a = b$. □

Teorema 2.1.7. *Seja $a, b \in \mathbb{Z}$, se $ab = 0$ então $a = 0$ ou $b = 0$*

Demonstração. Supondo $a \neq 0$, então, como, por hipótese, $ab = 0$ e como, pelo Teorema 2.1.1, dado $a \in \mathbb{Z}^*$, $a \cdot 0 = 0$. tem-se $ab = 0 = a \cdot 0$, portanto, pelo Teorema 2.1.6, $b = 0$. □

O Teorema 2.1.7 implica no conjunto dos Números Inteiros ser um *domínio de integridade*. As estruturas matemáticas que são domínio de integridade não apresentam elementos denominados divisores de zero, ou seja, no caso dos inteiros, não existe nenhum produto entre fatores inteiros, todos não nulos, que resulte em zero.

Outro resultado importante sobre Números Inteiros é o seguinte:

Teorema 2.1.8. ***Propriedade Arquimediana***

Dados a, $b \in \mathbb{Z}$, com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $a < nb$.

Demonstração. Seja $a \in \mathbb{Z}$, como $a \leq |a|$. Sendo $b \neq 0$, então, $|b| \geq 1$. Portanto,

$$a \leq |a| < |a| + 1 \leq |b| \cdot (|a| + 1) \tag{2.1}$$

Se da desigualdade 2.1 tomarmos b positivo e $n = (|a| + 1)$, ou ainda, se tomarmos $b < 0$ e $n = -(|a| + 1)$. Logo, tem-se:

$$a \leq nb \Longrightarrow a < nb$$

□

2.2 Divisibilidade

Definição 2.2.1. Define-se divisibilidade em $\mathbb{Z}$, da seguinte forma:

$$\text{Dados } a, b \in \mathbb{Z} \text{ diz-se que } a \mid b \text{ se } \exists c \in \mathbb{Z} \text{ tal que } b = c \cdot a$$

$a \mid b$ significa que a *divide* b ou que b *é divisível* por a, ou então, a *é divisor* de b. Portanto, sua negação é $a \nmid b$, que significa que, para todo c em $\mathbb{Z}$, ocorre que $b \neq c \cdot a$.

Teorema 2.2.1. *Sejam $a, b, c \in \mathbb{Z}$, logo:*

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

ii. $0 \mid a \Leftrightarrow a = 0$

iii. $a \mid b \Leftrightarrow |a| \mid |b|$

iv. $a \mid b$ *e* $b \mid c \Rightarrow a \mid c$

Demonstração. i. $a = a \cdot 1$, então $1 \mid a$
$a = 1 \cdot a$, então $a \mid a$
$0 = 0 \cdot a$, então $a \mid 0$

ii. ($\Rightarrow$) Se $0 \mid a$, então $\exists c \in \mathbb{Z}$, tal que $a = c \cdot 0 = 0$

($\Leftarrow$) Se $a = 0$, então $a = 0 = c \cdot 0$, $\forall c \in \mathbb{Z}$, então, $a = c \cdot 0$, logo $0 \mid a$

iii. ($\Rightarrow$) Se $a \mid b$, então $\exists c \in \mathbb{Z}$ tal que $b = c \cdot a \Rightarrow |b| = |c \cdot a| = |c| \cdot |a|$, logo $|a| \mid |b|$

($\Leftarrow$) Se $|a| \mid |b|$, então $\exists c \in \mathbb{Z}$, tal que $|b| = c \cdot |a|$. Portanto, temos alguns casos a considerar:

a. Para $a = 0$
$a = 0 \Rightarrow |b| = c \cdot 0 = 0$, logo $a \mid b$

b. Para $a \neq 0$ e $b = 0$, temos:
$b = 0 \Rightarrow 0 = c \cdot |a|$, sendo $c = 0$, $a \mid 0 \Rightarrow a \mid b$

c. Para a e $b \neq 0$

- $a > 0$ e $b > 0 \Rightarrow b = c \cdot a \Rightarrow a \mid b$
- $a < 0$ e $b < 0 \Rightarrow -b = c \cdot (-a) \Rightarrow (-b) \cdot (-1) = c \cdot (-a) \cdot (-1) \Rightarrow b = c \cdot a \Rightarrow a \mid b$
- $a > 0$ e $b < 0 \Rightarrow -b = c \cdot a \Rightarrow a \mid -b \Rightarrow a \mid b$
- $a < 0$ e $b > 0 \Rightarrow b = c \cdot (-a) \Rightarrow -a \mid b \Rightarrow a \mid b$

iv. Se $a \mid b$ e $b \mid c$ então $\exists m, n \in \mathbb{Z}$ tais que $b = a \cdot m$ e $c = b \cdot n$. Portanto, $c = b \cdot n = (a \cdot m) \cdot n$. Pela propriedade associativa, $c = a \cdot (m \cdot n)$, então, $a \mid c$.

□

Teorema 2.2.2. *Se $a, b, c, d \in \mathbb{Z}$, $a \mid b$ e $c \mid d \Rightarrow ac \mid bd$*

Demonstração. Se $a \mid b$ e $c \mid d$ então $\exists m, n \in \mathbb{Z}$ tais que $b = am$ e $d = cn$. Portanto, $bd = (am) \cdot (cn) = (ac) \cdot (mn)$. Logo, $ac \mid bd$ □

Teorema 2.2.3. *Se $a, b, c \in \mathbb{Z}$, $a \mid b \Rightarrow a \mid bc$*

Demonstração. Se $a \mid b$ então $\exists n \in \mathbb{Z}$ tal que $b = an$, logo, $bc = (an) \cdot c = a \cdot (nc)$, portanto, $a \mid bc$ □

Teorema 2.2.4. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então:*

$$a \mid b \Leftrightarrow a \mid c$$

Demonstração. ($\Rightarrow$) Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid (b + c)$ e $a \mid b$. Logo, $\exists m, n \in \mathbb{Z}$ tais que $b + c = am$ e $b = an$.

Portanto, $b + c = an + c = am \Rightarrow c = am - an \Rightarrow c = a \cdot (m - n) \Rightarrow a \mid c$

($\Leftarrow$) O raciocínio é análogo.

O resultado é demonstrado, de forma análoga, para $a \mid (b - c)$. □

Teorema 2.2.5. *Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$:*

$$a \mid (xb + yc)$$

Demonstração. Se $a \mid b$ e $a \mid c$, então $\exists m, n \in \mathbb{Z}$ tais que $b = am$ e $c = an$. Logo, $xb + yc = x \cdot (am) + y \cdot (an) = a \cdot (xm) + a \cdot (yn) = a \cdot (xm + yn) \Rightarrow a \mid xb + yc$, $\forall x, y \in \mathbb{Z}$ □

Teorema 2.2.6. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então $a - b \mid a^n - b^n$*

Demonstração. Usando Indução em $n \in \mathbb{N}$: Para $n = 1$, têm-se que a afirmação é válida, pois $a - b \mid a^1 - b^1$. Suponha então que $a - b \mid a^n - b^n$, para algum $n \in \mathbb{N}$.
Assim, sendo $a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b) \cdot a^n + b \cdot (a^n - b^n)$

Como $a - b \mid (a - b) \cdot a^n$ e, pela hipótese de Indução $a - b \mid a^n - b^n$, então, $a - b \mid a^{n+1} - b^{n+1}$. □

2.2.1 Divisão Euclidiana

A Divisão Euclidiana refere-se ao fato que nem sempre existirá $c \in \mathbb{Z}$, tal que $a = b \cdot c$, ou seja, b pode não ser um divisor de a, o que significa que a divisão de a por $b \neq 0$ não é inteira e deixa um resto r com $r \in \mathbb{Z}$.

Teorema 2.2.7. *Sejam a e b dois números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que:*

$$a = bq + r, com \;\; 0 \leq r < |b|$$

Demonstração. Consideremos o conjunto S como sendo a interseção

$$\{x = a - by; y \in \mathbb{Z}\} \bigcap (\mathbb{N} \bigcup \{0\}).$$

Primeiramente, provando a Existência:

Pela Propriedade Arquimediana (Teorema 2.1.8), $\exists n \in \mathbb{Z}$ tal que $n \cdot (-b) > -a$, logo $a - nb > 0$, então S não é vazio. Por outro lado, o conjunto S é limitado inferiormente por 0 e portanto, pelo Princípio da Boa Ordenação, S possui um menor elemento r.

Supondo então $r = a - bq$ com $q \in \mathbb{Z}$, existe $w \in \mathbb{N} \bigcup \{0\}$ tal que $r = |b| + w$, logo $0 \leqslant w < r$. Porém, isto contradiz o fato de ser r o menor elemento de S, pois $w = a - (q \pm 1) \cdot b \in S$, com $w < r$.

Provando a Unicidade do quociente e do resto:

Supondo que dados $a, b \in \mathbb{Z}$ tem-se $a = bq + r$, com $0 \leqslant r < |b|$ e $a = bq' + r'$, com $0 \leqslant r' < |b|$, $r \geqslant r'$ e $q \geqslant q'$. Têm-se:

$$a = bq + r \Rightarrow r = a - bq \tag{2.2}$$

$$a = bq' + r' \Rightarrow r' = a - bq' \tag{2.3}$$

Subtraindo a Equação 2.3 da Equação 2.2:

$$r - r' = b \cdot (q' - q)$$

Sendo $r \geqslant r'$ então $r - r' \geqslant 0$. Como $r < |b|$ e $r' < |b|$ tem-se que $0 \leqslant r - r' < |b|$. Logo $0 \leqslant b \cdot (q' - q) < |b|$.

Sendo b, q' e $q \in \mathbb{Z}$, então a desigualdade acima só se verifica se $q' - q = 0 \Rightarrow q' = q$.

Logo, $r - r' = b \cdot (q' - q) = 0$, portanto, $r = r'$. □

Algumas observações podem ser feitas sobre o Teorema 2.2.7.

Primeiramente, é que para todo número inteiro n têm-se duas possibilidades: ou este é par, ou é ímpar.

Caso n seja par, este será da forma $2q$, com $q \in \mathbb{N}$, quando sua divisão por 2 deixar resto igual a zero. E será da forma $n = 2q + 1$, se na divisão de n por 2, este deixar resto igual a 1.

Como na divisão de n por 2, os possíveis restos pertencem ao conjunto $\{0, 1\}$, pode-se garantir que todo inteiro ou será par ou ímpar.

Outra importante observação é que todo inteiro n pode ser escrito na forma $n = t \cdot k + r$, onde $t \in \mathbb{N}$, $t \geqslant 2$ e $k, r \in \mathbb{Z}$, sendo $0 \leqslant r < t$. Por exemplo, todo $n \in \mathbb{Z}$ pode ser escrito em uma, e somente uma das formas $4k$, $4k+1$, $4k+2$ ou $4k+3$, quando $t = 4$.

2.2.2 Máximo Divisor Comum (MDC)

Dados $a, b \in \mathbb{Z}$ se $d \mid a$ e $d \mid b$, com $d \in \mathbb{Z}$, então d será considerado divisor comum de a e b.

Definição 2.2.2. Para que $d \geqslant 0$ seja o *máximo divisor comum* (mdc) de a e b é preciso atender às seguintes propriedades:

i. d é um divisor comum de a e b;

ii. d é divisível por todo divisor comum de a e b, ou seja, se $c \in \mathbb{Z}$ é um divisor comum de a e b, então $c \mid d$.

A notação que adotaremos para exibir o mdc entre a e b será $d = (a, b)$.

Através da definição de mdc podemos listar algumas propriedades para $a \in \mathbb{Z}$.

- $(0, a) = |a|$
- $(1, a) = 1$
- $(a, a) = |a|$

Mas ainda chega-se à conclusão que $\forall b \in \mathbb{Z}$, têm-se que:

$$a \mid b \Leftrightarrow (a, b) = |a|$$

Demonstração. ($\Rightarrow$) Se $a \mid b$ então $|a|$ é um divisor comum de a e b e se c é um divisor comum de a e b, então $c \mid |a|$, portanto, $(a, b) = |a|$

($\Leftarrow$) Se $(a, b) = |a|$, segue, então que $|a| \mid b$, logo $a \mid b$ □

2.2.3 Propriedades do MDC

Teorema 2.2.8. ***Teorema de Bezóut***

Sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $d \in \mathbb{Z}$ com $d = (a, b)$. Então, existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$.

Demonstração. Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, considere o conjunto $I(a,b) = \{ax + by; x, y \in \mathbb{Z}\}$. Tome um inteiro positivo em $I(a,b)$. Logo, $|b| \in I(a,b)$. Seja $d = ax_0 + by_0$ o menor inteiro positivo em $I(a,b)$.

Dado $n = ax_1 + by_1 \in I(a,b)$, sejam q e $r \in \mathbb{Z}$ tais que $n = qd + r$, com $0 \leqslant r < d$. Têm-se, então que, $n - qd = a \cdot (x_1 - qx_0) + b \cdot (y_1 - qy_0) = r \in I(a,b)$. Dessa forma, como d é o menor inteiro positivo em $I(a,b)$, então $r = 0$. Assim $d \mid n$, $\forall n \in I(a,b)$.

Sendo $a, b \in I(a,b)$, basta escolher $(x,y) = (1,0)$ e $(x,y) = (0,1)$, respectivamente, temos que $d \mid a$ e $d \mid b$. Logo, $d \leqslant (a,b)$.

Por outro lado, (a,b) divide a e b, de modo que, (a,b) divide d. Portanto, $(a,b) \leqslant d$.

Consequentemente, $d = (a,b)$. □

Lema 2.2.9. *Lema de Gauss*

Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a,b) = 1$, então $a \mid c$.

Demonstração. Se $a \mid bc$, então $bc = at, t \in \mathbb{Z}$ e, se $(a,b) = 1$, pelo Teorema 3.1.5, $\exists m, n \in \mathbb{Z}$, tais que $ma + nb = 1$. Multiplicando por c, temos $(ma) \cdot c + (nb) \cdot c = c \Rightarrow a \cdot (mc) + n \cdot (bc) = c \Rightarrow a \cdot (mc) + n \cdot (at) = c \Rightarrow a \cdot (mc) + a \cdot (nt) = c \Rightarrow a \cdot (mc + nt) = c \Rightarrow a \mid c$. □

Teorema 2.2.10. *$\forall a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$ tem-se que*

$$(na, nb) = n \cdot (a,b)$$

Demonstração. Sejam $k = (na, nb)$ e $t = (a,b)$. Como $t \mid a$ e $t \mid b$ então $nt \mid na$ e $nt \mid nb$, portanto $nt \leqslant k$, pois $k = (na, nb)$.

Por outro lado, pelo Teorema 2.2.8, existem x e y inteiros tais que $ax + by = t$. Multiplicando essa igualdade por n, temos $nax + nby = nt$, logo $k \leqslant nt$, pois é o menor número que pode ser escrito como essa soma. Então, $k = nt$, concluindo que $(na, nb) = n \cdot (a,b)$. □

Outra proposição importante é a seguinte:

Teorema 2.2.11. *Sejam $a, b \in \mathbb{N}$, com $(a,b) = 1$. Todo número $c \in \mathbb{Z}$ pode ser escrito de modo único da seguinte forma:*

$$c = ma + nb, \text{ com } 0 \leqslant m < b \text{ e } n \in \mathbb{Z}$$

Demonstração. Existência: Existem $u, v \in \mathbb{Z}$ tais que $ua + vb = (a,b) = 1$. Multiplicando por c, tem-se:

$$auc + bvc = c \tag{2.4}$$

Pela Divisão Euclidiana, tem-se que $\exists q, m \in \mathbb{Z}$ com $0 \leqslant m < b$ tais que $uc = qb + m$. Substituindo esse valor de uc na Equação 2.4, obtêm-se:

$$a \cdot (qb + m) + bvc = c \Longrightarrow aqb + am + bvc = c \Longrightarrow am + b \cdot (qa + vc) = c$$

Logo,

$$c = ma + nb, \text{ com } 0 \leqslant m < b \text{ e } n = qa + vc \in \mathbb{Z}$$

Unicidade: Suponha que existam $0 \leqslant m, m' < b$ e que $ma + nb = m'a + n'b \Longrightarrow (m - m') \cdot a = (n' - n) \cdot b$, com

$$|m - m'| < b \tag{2.5}$$

Por outro lado, por hipótese, $b \mid (m - m') \cdot a$, como $(a, b) = 1$, então,

$$b \mid m - m' \tag{2.6}$$

Portanto, da Equação 2.5 e Equação 2.6, tem-se que $m = m'$ e em tal caso, $n = n'$. □

2.2.4 Mínimo Múltiplo Comum (MMC)

Definição 2.2.3. Um inteiro é chamado *múltiplo comum* de $a, b \in \mathbb{Z}$, se for múltiplo simultaneamente de ambos.

Têm-se que $m \in \mathbb{Z}$, $m \geqslant 0$ é o *mínimo múltiplo comum* (MMC) de a e b, simbolizado por $m = [a, b]$, se:

i. m é múltiplo comum de a e b; e

ii. Se n é múltiplo comum de a e b, então $m \mid n$.

2.3 Congruências

Esta seção aborda a definição de um conceito matemático muito importante que é o de congruências. Este relaciona-se à estrutura da Criptografia RSA.

Definição 2.3.1. Dados $a, b, m \in \mathbb{Z}$ e $m > 1$, têm-se que a e b são *congruentes módulo* m, se os restos das divisões de a e b por m forem iguais.

$$a \equiv b \bmod m$$

Exemplo. i. $15 \equiv 3 \bmod 4$, significa que 15 é congruente a 3 módulo 4, ou seja, 15 e 3 deixam o mesmo resto na divisão por 4.

ii. $8 \not\equiv 1 \bmod 5$, significa que, 8 é incongruente a 1 módulo 5. Pois, 8 e 1 deixam restos distintos quando divididos por 5.

Outra forma de definir a congruência entre dois inteiros módulo m é:

Teorema 2.3.1. *Dado $a, b, m \in \mathbb{Z}$, $m > 1$. Tem-se $a \equiv b \bmod m$ se, e somente se, $m \mid b - a$.*

Demonstração. ($\Rightarrow$) Se $a \equiv b \bmod m$, então $a = mk + r$ e $b = mt + r$. Logo, $b - a = (mt + r) - (mk + r) = m(t - k)$. Portanto, $m \mid b - a$.

($\Leftarrow$) Sejam as divisões euclidianas de a e b por m:

$a = mk_1 + r_1$, com $0 \leq r_1 < m$ e $b = mk_2 + r_2$, com $0 \leq r_2 < m$.

Como $m \mid b - a$, então $m \mid (mk_2 + r_2) - (mk_1 + r_1)$, logo $m \mid m(k_2 - k_1) + (r_2 - r_1)$, tem-se que $m \mid m(k_2 - k_1)$, portanto, para que $m \mid m(k_2 - k_1) + (r_2 - r_1)$, então $m \mid (r_2 - r_1)$. No entanto, como r_1 e r_2 são estritamente menores que m, logo $r_2 - r_1 = 0 \Rightarrow r_1 = r_2$, ou seja, $a \equiv b \bmod m$. □

Decorrem da definição o seguinte teorema:

Teorema 2.3.2. *i. $a \equiv a \bmod m$, $\forall a \in \mathbb{Z}$, $m \in \mathbb{N}$.*

Demonstração. $m \mid 0 \Rightarrow m \mid a - a \Rightarrow a \equiv a \bmod m$ □

ii. Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$, $\forall a, b \in \mathbb{Z}$, $m \in \mathbb{N}$.

Demonstração. Se $a \equiv b \bmod m \Rightarrow m \mid b - a \Rightarrow m \mid |a - b| \Rightarrow a \equiv b \bmod m$. □

iii. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$, $\forall a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$.

Demonstração. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $m \mid b - a$ e $m \mid c - b$, portanto, $m \mid (b - a) + (c - b) \Rightarrow m \mid c - a$, logo, $a \equiv c \bmod m$. □

É importante notar que para todo inteiro a, da forma $a = mq + r$, $q \in \mathbb{Z}$, m e r números naturais, têm-se que a é congruente ao seu resto quando dividido por m. Considerando R, o conjunto de números naturais dos m possíveis restos numa divisão por m: $R = \{0, 1, 2, ..., m - 1\}$ tem-se $a \equiv r \bmod m$, $0 \leq r < m$. Este conjunto R é denominado de *sistema completo de resíduos módulo m*. Ao extrairmos desse conjunto R, todos os elementos que não são primos com m, obtém-se o conjunto S, que é o conjunto nomeado de *sistema reduzido de resíduos módulo m*. Este conjunto S obedece às seguintes características:

- Dois a dois elementos de S são incongruentes módulo m.
- Todos os elementos de S são primos com m.
- Para cada número inteiro n, primo com m que tomarmos, sempre existirá um elemento de S que será congruente a n módulo m.

Pode-se obter as demonstrações dos itens acima em Hefez (2016, p. 195).

Em relação ao número de elementos de S, pode-se definir a função fi de Euler $\phi : \mathbb{N} \longrightarrow \mathbb{N}$, como a função que corresponde à quantidade de elementos de R que são primos com m, ou seja, o número de elementos de S.

Portanto, a função ϕ é definida para $m > 1$ e, sendo $\phi(1) = 1$. Logo, decorre das definições acima, o seguinte resultado, segundo Hefez (2016, p. 195):

$$\phi(m) \leq m - 1, \forall m \geq 2, \text{ valendo a igualdade quando } m \text{ for primo.}$$

O resultado a seguir relaciona o cálculo de $\phi(m)$ à sua decomposição em fatores primos.

Teorema 2.3.3. *Dados $m > 1$ e sua decomposição em fatores primos $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_n^{\alpha_n}$. Então,*

$$\phi(m) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot p_3^{\alpha_3 - 1} \cdot ... \cdot p_n^{\alpha_n - 1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot (p_3 - 1) \cdot ... \cdot (p_n - 1)$$

A prova do Teorema 2.3.3 pode ser vista em Lima (2013, p. 11).

O Teorema a seguir é um resultado importante sobre a Função de Euler.

Teorema 2.3.4. ***Teorema de Euler***

Sejam m, $a \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então,

$$a^{\phi(m)} \equiv 1 \bmod m$$

Demonstração. Seja $s_1, s_2, s_3, ..., s_{\phi(m)}$ um sistema reduzido de resíduos módulo m. Portanto, os elementos $a \cdot s_1, a \cdot s_2, a \cdot s_3, a \cdot s_4, ..., a \cdot s_{\phi(m)}$ também formam um sistema reduzido de resíduos módulo m, pois:

$$a \cdot s_1, a \cdot s_2, a \cdot s_3, a \cdot s_4, ..., a \cdot s_{\phi(m)} \equiv s_1, s_2, s_3, ..., s_{\phi(m)} \tag{2.7}$$

Da Equação 2.7, tem-se

$$a^{\phi(m)} \cdot s_1, s_2, s_3, ..., s_{\phi(m)} \equiv s_1, s_2, s_3, ..., s_{\phi(m)} \bmod m \tag{2.8}$$

Como $(s_1, s_2, s_3, ..., s_{\phi(m)}, m) = 1$, então, pelo Teorema 2.3.8, a Equação 2.8 tem como resultado a congruência

$$a^{\phi(m)} \equiv 1 \bmod m$$

□

O Teorema de Euler é a generalização do Pequeno Teorema de Fermat. O Corolário 3.2.2.1 é o caso particular do Teorema de Euler, quando m for primo.

Em seguida, apresentamos alguns resultados importantes envolvendo congruências:

Teorema 2.3.5. *Sejam $a, b, c, d, m \in \mathbb{Z}$, $m > 1$. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$.*

Demonstração. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$, portanto, $m \mid (b - a) + (d - c) \Rightarrow m \mid (b + d) - (a + c) \Rightarrow a + c \equiv b + d \bmod m$ □

Teorema 2.3.6. *Sejam $a, b, c, d, m \in \mathbb{Z}$, $m > 1$. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.*

Demonstração. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$, portanto, $m \mid d(b - a) + a(d - c) \Rightarrow m \mid bd - ac \Rightarrow ac \equiv bd \bmod m$ □

Corolário 2.3.6.1. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$.*

Demonstração. Usando Indução: Para $n = 1$, a afirmação é válida, por hipótese.

Supondo a afirmação válida para algum $n > 1$, temos que se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$.

Portanto, se $a \equiv b \bmod m$ e $a^n \equiv b^n \bmod m$, logo, pelo Teorema 2.3.6, $a^n \cdot a \equiv b^n \cdot b \bmod m \Rightarrow a^{n+1} \equiv b^{n+1} \bmod m$. □

O Teorema 2.3.7 e o Teorema 2.3.8, referem-se às propriedades de cancelamento em relação às operações de adição e multiplicação utilizando congruências.

Teorema 2.3.7. *Sejam $a, b, c, m \in \mathbb{Z}$, $m > 1$. Vale que $a + c \equiv b + c \bmod m \Leftrightarrow a \equiv b \bmod m$.*

Demonstração. ($\Rightarrow$) $a + c \equiv b + c \bmod m$, então $m \mid (b + c) - (a + c)$, logo, $m \mid b - a \Rightarrow a \equiv b \bmod m$.

($\Leftarrow$) $a \equiv b \bmod m$ e $c \equiv c \bmod m$, pelo Teorema 2.3.2, logo pelo Teorema 2.3.5, $a + c \equiv b + c \bmod m$. □

Teorema 2.3.8. *Sejam $a, b, c, m \in \mathbb{Z}$, $m > 1$. $ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod \left(\frac{m}{(c,m)}\right)$*

Demonstração. ($\Rightarrow$) $ac \equiv bc \bmod m \Rightarrow m \mid bc - ac \Rightarrow m \mid (b - a)c \Rightarrow \frac{m}{(c,m)} \mid (b - a) \cdot \frac{c}{(c,m)}$.

Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são números coprimos, então, $\frac{m}{(c,m)} \mid b - a \Rightarrow a \equiv b \bmod \left(\frac{m}{(c,m)}\right)$.

($\Leftarrow$) $a \equiv b \bmod \left(\frac{m}{(c,m)}\right) \Rightarrow \frac{m}{(c,m)} \mid b - a \Rightarrow \frac{m}{(c,m)} \mid (b - a) \cdot \frac{c}{(c,m)} \Rightarrow m \mid (b - a)c \Rightarrow m \mid bc - ac \Rightarrow ac \equiv bc \bmod (m)$.

Em particular, sejam $a, b, c, m \in \mathbb{Z}$, $m > 1$ e $(c, m) = 1$: $ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod m$. □

Teorema 2.3.9. *Sejam $a, b, m, n \in \mathbb{Z}$, $m > 1$, $n > 1$. Se $a \equiv b \bmod m$ e $n \mid m$, então $a \equiv b \bmod n$.*

Demonstração. Se $a \equiv b \bmod m$, então $m \mid b - a$, logo $b - a = mk$, $k \in \mathbb{Z}$. Portanto, como $n \mid m$, tem-se $m = nq$, $q \in \mathbb{Z}$, e assim, $b - a = mk = (nq)k = n(qk) \Rightarrow n \mid b - a \Rightarrow a \equiv b \bmod n$. □

Teorema 2.3.10. *Sejam $a, b, m_1, m_2, ..., m_r \in \mathbb{Z}$, com $m_i > 1$, $\forall i = 1, 2, ..., r$.*

$a \equiv b \bmod m_i \Leftrightarrow a \equiv b \bmod [m_1, m_2, ..., m_r]$.

Demonstração. ($\Rightarrow$) Se $a \equiv b \bmod m_i$, $\forall i = 1, 2, ..., r$, então $m_i \mid b - a$, $\forall i$. Sendo assim, $b - a$ é um múltiplo de cada m_i, portanto, $[m_1, m_2, ..., m_r] \mid b - a$, logo $a \equiv b \bmod [m_1, m_2, ..., m_r]$.

($\Leftarrow$) A recíproca é proveniente do Teorema 2.3.9. □

2.3.1 Resolução de Congruências Lineares

Considerando as congruências da forma $aX \equiv b \bmod m$, onde $a, b, m \in \mathbb{Z}$, $m > 1$, denominadas *congruências lineares*, deseja-se identificar um critério para a verificação da existência de soluções, ou seja, se existem $x \in \mathbb{Z}$, tais que $ax \equiv b \bmod m$.

Sendo assim, eis uma proposição que apresenta tal critério:

Teorema 2.3.11. *Sejam $a, b, m \in \mathbb{Z}$, $m > 1$. Tem-se que $aX \equiv b \bmod m$ possui solução se, e somente se, $(a, m) \mid b$.*

Demonstração. ($\Rightarrow$) Supondo que x seja a solução da congruência $aX \equiv b \bmod m$, ou seja, $\exists y \in \mathbb{Z}$, tal que $ax - b = my$, tem-se que a equação $aX - mY = b$ admite solução.

Como $(a, m) \mid a$ e $(a, m) \mid m$, logo $(a, m) \mid aX - mY$, então $(a, m) \mid b$.

($\Leftarrow$) Como por hipótese, $(a, m) \mid b$ e como $(a, m) \mid a$, e então $(a, m) \mid ax$, tem-se $(a, m) \mid ax - b$. Logo $\exists t \in \mathbb{Z}$, tal que

$$ax - b = (a, m)t \tag{2.9}$$

Como $(a, m) \mid m$, então $(a, m) \mid my$, $y \in \mathbb{Z}$. Sendo assim, seja

$$my = (a, m)q, q \in \mathbb{Z} \tag{2.10}$$

Admitamos que exista uma única solução x_0, y_0 na qual $t = q$ para a Equação 2.9 e Equação 2.10, então $ax_0 - b = (a, m)t = my_0$ portanto, $m \mid ax_0 - b$ e, consequentemente, $ax_0 \equiv b \bmod m$, com $a, b, m \in \mathbb{Z}$, $m > 1$. □

É notável que, se x_0 é solução particular de $aX \equiv b \bmod m$, então $x \equiv x_0 \bmod m$ é também uma solução e, portanto, gera todas as soluções também congruentes a esta.

Portanto, é necessário utilizar o Teorema 2.3.12 a seguir, para encontrar quais e quantas são as soluções incongruentes duas a duas da congruência $aX \equiv b \bmod m$.

Teorema 2.3.12. *Sejam $a, b, m \in \mathbb{Z}$, $m > 1$ e $(a, m) \mid b$. Se x_0 é solução da congruência $aX \equiv b \bmod m$, então $x_0, x_0 + \frac{m}{d}, x_0 + 2 \cdot \frac{m}{d}, ..., x_0 + (d-1) \cdot \frac{m}{d}$, onde $d = (a, m)$, formam uma coleção completa de soluções de $aX \equiv b \bmod m$, duas a duas incongruentes módulo m.*

Demonstração. Seja x_0 uma solução da congruência $aX \equiv b \bmod m$. Nesse caso toda solução x desta é congruente , módulo m, a $x_0 + i \cdot \frac{m}{d}$, para algum i, onde $0 \leq i < d$, sendo $d = (a, m)$. Logo, se $ax \equiv ax_0 \bmod m$, então $x \equiv x_0 \bmod m$. Sendo $x - x_0 \equiv t \cdot \frac{m}{d}$. Portanto, $\exists i$, $0 \leq i < d$, tal que $t = kd + i$. Então, $x = x_0 + km + i \cdot \frac{m}{d} \equiv x_0 + i \cdot \frac{m}{d} \bmod m$. Têm-se que, $x_0 + i \cdot \frac{m}{d}$, $0 \leq i < d$, são soluções da congruência.

Concluindo, essas soluções são incongruentes duas a duas, módulo m, pois se $x_0 + y \cdot \frac{m}{d} \equiv x_0 + z \cdot \frac{m}{d} \bmod m$, com $0 \leq y, z < d$, então $y = z$. □

Corolário 2.3.12.1. *Se $(a, m) = 1$, então $aX \equiv b \bmod m$ possui uma única solução módulo m.*

Este Corolário decorre diretamente do Teorema 2.3.12, no caso particular de $(a, m) = 1$. Neste caso, esta solução única será chamada de *inverso multiplicativo de a* módulo m.

Teorema 2.3.13. *Dados a, $m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \bmod m$ possui solução se, e somente se, $(a, m) = 1$.*

Demonstração. Seja x_0 uma solução da congruência $aX \equiv 1 \bmod m$. Esta congruência possui solução se, e somente se, $m \mid ax_0 - 1$. Portanto, existe y_0 tal que $ax_0 - 1 = my_0$, então, a congruência $aX - mY = 1$ possui solução inteira. Pelo Teorema 3.1.5, isso ocorre se, e somente se, $(a, m) = 1$. □

Exemplo. Resolução de uma congruência linear.

Seja a congruência $20X \equiv 4 \bmod 16$ e $d = (4, 20) = 4$. Garantimos, portanto, a existência de 4 soluções. Por rápida inspeção, encontra-se a solução $x_0 = 1$. Utilizando o Teorema 2.3.12, as soluções são:

- $x_0 = 1$
- $x_0 + \frac{m}{d} = 1 + \frac{16}{4} = 5$
- $x_0 + 2 \cdot \frac{m}{d} = 1 + 2 \cdot \frac{16}{4} = 9$
- $x_0 + 3 \cdot \frac{m}{d} = 1 + 3 \cdot \frac{16}{4} = 13$

Então, as soluções serão $\{1, 5, 9, 13\}$.

3 NÚMEROS PRIMOS

3.1 Números Primos

Segundo Coutinho (2014, p. 19), "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". Ainda segundo Coutinho (2014, p. 19), os romanos chamavam esses números de "*primus*" que, em latim, significa primeiro. Logo, os números primos têm essa nomenclatura, pois, estes são considerados os primeiros.

São números naturais que só possuem dois divisores naturais: 1 e o próprio número. Como veremos adiante por meio do Teorema Fundamental da Aritmética, os números primos formam todos os outros que não o são.

As propriedades dos números primos são fundamentais no estudo da Aritmética e de outras áreas do conhecimento como Criptografia, Ciência da Computação e Segurança da Informação. No entanto, há muitos anos, algumas conjecturas importantes relacionadas à esses números estão em aberto, como por exemplo, o padrão matemático responsável por sua distribuição e regularidade no conjunto dos números naturais, o que será melhor explorado nos próximos capítulos.

Exemplo. O número 5 é primo, pois apresenta como divisores positivos somente os números 1 e 5. O número 6 não é primo. Pois, apresenta os seguintes divisores positivos $\{1, 2, 3, 6\}$. Todo número que não for primo é chamado *composto*.

Alguns resultados que decorrem da definição:

Sejam p e q primos, com $n \in \mathbb{Z}$:

i. Se $p \mid q$, então $p = q$.

Demonstração. Como q é primo e $p \mid q$ então $p = 1$ ou $p = q$, mas sendo p também primo, tem-se, $p = q$. □

ii. Se $p \nmid n$, então $(p, n) = 1$.

Demonstração. Seja $d = (p, n)$, então $d \mid p$ e $d \mid n$, logo $d = p$ ou $d = 1$.

Como $p \nmid n$, então $d \nmid p$. Portanto $d = 1$. □

Lema 3.1.1. *Lema de Euclides*

$\forall a, b, p \in \mathbb{Z}$, *com* p *primo. Se* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

Demonstração. Seja p primo e $p \mid ab$, e suponha que $p \nmid a$. Então $(p, a) = 1$. Pelo Lema de Gauss, $p \mid b$. □

Corolário 3.1.1.1. *Se $p, p_1, p_2, p_3, ..., p_n$ são números primos e $p \mid p_1 \cdot p_2 \cdot ... \cdot p_n$, então $p = p_i$ para algum $i = 1, 2, 3, ..., n$.*

Demonstração. Utilizando o Princípio de Indução: Sejam $p, p_1, p_2, ..., p_n, p_{n+1}$ números primos.

Se $p \mid p_1$, como p e p_1 são primos, por hipótese, então $p = p_1$.

Suponha que $p \mid p_1 \cdot p_2 \cdot ... \cdot p_n$, então $p = p_i$, para algum $i = 1, 2, ..., n$.

Logo, se $p \mid p_1 \cdot p_2 \cdot ... \cdot p_n$, então $p \mid p_1 \cdot p_2 \cdot ... \cdot p_n \cdot p_{n+1}$ e, portanto, $p = p_i$, para algum $i = 1, 2, 3, ..., n, n + 1$. □

O Teorema 3.1.2 fundamenta os números primos como as estruturas mais simples que formam todos os números naturais. Eis o seu enunciado:

Teorema 3.1.2. ***Teorema Fundamental da Aritmética***

Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Demonstração. Pelo Princípio de Indução:

Se $n = 2$, temos válido o resultado, pois, 2 é primo.

Supondo que a afirmação é válida para qualquer número natural menor que n, então teremos que analisar e provar para n quando este for composto, pois se n é primo já verifica a afirmação.

Se n é composto, logo $\exists n_1, n_2 \in \mathbb{N}$, tais que $n = n_1 n_2$, $1 < n_1 < n$ e $1 < n_2 < n$.

Pela hipótese de indução, $\exists p_1, p_2, ..., p_r$ e $q_1, q_2, ..., q_s$, tais que $n_1 = p_1 \cdot p_2 \cdot ... \cdot p_r$ e $n_2 = q_1 \cdot q_2 \cdot ... \cdot q_s$.

Portanto, $n = p_1 \cdot p_2 \cdot ... \cdot p_r \cdot q_1 \cdot q_2 \cdot ... \cdot q_s$.

Unicidade da escrita: Suponhamos que $n = p_1 \cdot p_2 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot ... \cdot q_s$ e que p_i e q_j são números primos. Como $p_1 \mid q_1 \cdot q_2 \cdot ... \cdot q_s$, pelo Corolário 3.1.1.1, temos que $p_1 = q_j$ para algum j, que supomos ser q_1.

Logo, agora restam $p_2 \cdot p_3 \cdot ... \cdot p_r = q_2 \cdot q_3 \cdot ... \cdot q_s$.

Como $p_2 \cdot p_3 \cdot ... \cdot p_r < n$, pela hipótese de indução, têm-se que $r = s$ e que todos p_i e q_j são iguais aos pares. □

Exemplo. i. O número 13 é primo.

ii. O número 15 é composto, pois pode ser escrito na forma $15 = 3 \cdot 5$, onde 3 e 5 são primos.

iii. O número 900 pode ser escrito na forma fatorada (produto) como $900 = 2{\cdot}2{\cdot}3{\cdot}3{\cdot}5{\cdot}5 = 2^2 \cdot 3^2 \cdot 5^2$.

O Exemplo iii nos conduz ao próximo resultado, cuja demonstração pode ser vista em Hefez (2005, p. 84).

Teorema 3.1.3. *Dado $n \in \mathbb{Z} - \{-1, 0, 1\}$, existem primos $p_1 < p_2 < ... < p_r$ e $\alpha_1, \alpha_2, ..., \alpha_r \in \mathbb{N}$ univocamente determinados, tais que:*

$$n = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$$

A seguir duas observações sobre o resultado anterior:

- Sejam $n, m \in \mathbb{N}$ e $m > 1$ e $n > 1$, em se tratando da decomposição em fatores primos, teremos:

  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$ e $m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r}$, utilizando os primos $p_1, p_2, ..., p_r$ e os expoentes $\alpha_1, \alpha_2, ..., \alpha_r$ e $\beta_1, \beta_2, ..., \beta_r$ variando em $\mathbb{N} \cup \{0\}$.

- Com relação a $n \in \mathbb{N}$, $n > 1$, escrito na forma $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$, será quadrado perfeito se, e somente se, α_i forem pares, para todos $i = 1, 2, 3, ..., r$.

Teorema 3.1.4. *Seja $n \in \mathbb{N}$, $n > 1$, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r}$, sendo p_i, primo, com $i = 1, 2, 3, ..., r$. Se $n' \mid n$ e $n' > 0$ (divisor positivo de n), então:*

$$n' = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_r^{\beta_r},\ 0 \leq \beta_i \leq \alpha_i,\ \textit{para}\ i = 1, 2, ..., r.$$

Demonstração. Seja n' um divisor positivo de n e seja p^β a potência de um primo p que figura na decomposição de n' em fatores primos. Como p^β divide algum $p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$, então, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. □

Um resultado importante que relaciona o Teorema de Bezóut e os números considerados primos entre si é:

Teorema 3.1.5. *Dois números inteiros a e b são primos entre si (ou coprimos) se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração. ($\Rightarrow$) Suponha que a e b são primos entre si. Logo, $(a, b) = 1$. Pelo Teorema 2.2.8 $\exists m, n \in \mathbb{Z}$ tais que $ma + nb = (a, b) = 1$.

($\Leftarrow$) Suponha que $\exists m, n \in \mathbb{Z}$ tais que $ma + nb = 1$. Se $d = (a, b)$, temos que, pelo Teorema 2.2.5, $d \mid (ma + nb)$, o que implica que $d \mid 1$, e, portanto $d = 1$. □

Outra ferramenta importante é o Teorema fornecido por Pierre de Fermat, conhecido como *Pequeno Teorema de Fermat* que relaciona divisibilidade, números primos e congruências.

3.2 Pequeno Teorema de Fermat

Pierre de Fermat, grande matemático francês que viveu entre 1601 e 1665, ofereceu notável contribuição em diversas áreas da matemática.

Em 1640, Fermat enunciou uma proposição importantíssima no estudo de congruências, o Pequeno Teorema de Fermat.

Segundo Hefez (2016, p. 135), "500 anos antes de nossa Era, os chineses já sabiam que se p é primo então $p \mid 2^p - 2$", e o trabalho de Fermat deu-se em generalizar esse resultado.

Para provar o Pequeno Teorema de Fermat, utiliza-se o seguinte Lema:

Lema 3.2.1. *Seja p, primo. Os números binomiais $\binom{p}{i} = \frac{p!}{i!\cdot(p-i)!}$, com $i \in \mathbb{N}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. Por Indução matemática:

$i = 1$, o resultado é válido.

Supondo $1 < i < p$, então $i! \mid p \cdot (p-1) \cdot ... \cdot (p-i+1)$, como $(i!, p) = 1$, pelo Lema de Euclides, $i! \mid (p-1) \cdot ... \cdot (p-i+1)$, logo:

$$\binom{p}{i} = p \cdot \frac{(p-1)\cdot...\cdot(p-i+1)}{i!}$$

□

Teorema 3.2.2. ***Pequeno Teorema de Fermat***

Dado p, primo, tem-se $p \mid a^p - a$, $\forall a \in \mathbb{Z}$.

Demonstração. Se $p = 2$ a afirmação é válida, pois $a^2 - a = a(a-1)$ é par.

Supondo, então, p ímpar e $a \geqslant 0$.

Pela Indução matemática em relação à a:

- $a = 0$, $p \mid 0$, logo é válida.
- Supondo válida a afirmação válida para a, logo $p \mid a^p - a$.
- Então, $(a+1)^p - (a+1) = a^p - a + \binom{p}{1} \cdot a^{p-1} + ... + \binom{p}{p-1} \cdot a$

Logo, pela hipótese de indução e pelo Lema anterior, então, $p \mid (a+1)^p - (a+1)$, $\forall a \in \mathbb{Z}$ e p primo. □

Do resultado acima, pode-se obter o Corolário 3.2.2.1 um novo enunciado para o Pequeno Teorema de Fermat.

Corolário 3.2.2.1. *Pequeno Teorema de Fermat*

Se p é primo, $a \in \mathbb{N}$ e $(p, a) = 1$, então $p \mid a^{p-1} - 1$.

Demonstração. Como pelo Teorema 3.2.2, tem-se $p \mid a^p - a$, para algum p primo. Então, $p \mid a^p - a \Rightarrow p \mid a(a^{p-1} - 1)$, sendo $(p, a) = 1$, portanto $p \mid a^{p-1} - 1$. □

3.2.1 Pequeno Teorema de Fermat - Congruências

Diante dos conceitos aqui expostos, segue uma reformulação do Pequeno Teorema de Fermat (Teorema 3.2.2), com foco na notação de congruências.

Teorema 3.2.3. *Pequeno Teorema de Fermat - Congruência*

Se p é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \bmod p$.

Em particular, se $p \nmid a$, então $a^{p-1} \equiv 1 \bmod p$.

3.3 Alguns resultados importantes sobre os Números Primos

3.3.1 Teorema de Euclides

Os números Primos sempre constituíram um grande mistério para os matemáticos. Muitos estudiosos brilhantes, como Fermat, Euler, entre outros, aventuraram-se em conhecer as principais características destes números.

Euclides foi um dos primeiros a estudar o comportamento dos primos quanto à sua cardinalidade e demonstrou o seguinte resultado 300 anos antes de nossa Era:

Teorema 3.3.1. ***Teorema de Euclides***

Existem infinitos números primos.

Demonstração. Utilizando o método de redução ao absurdo. Supondo que existam k primos (quantidade finita), sendo estes: $p_1, p_2, p_3, ..., p_k$.

Sejam $n = p_1 \cdot p_2 \cdot ... \cdot p_k + 1$ e q o menor divisor primo de n. Logicamente, q é diferente de todos os primos p_i, $1 \leq i \leq k$, pois, como $q \mid n$, então q teria que dividir 1, logo, impossível. Portanto, tem-se uma contradição na afirmação que existem uma quantidade finita de primos. □

Este resultado traz à tona uma importante caracterização dos números primos quanto à sua cardinalidade. Porém, outra questão notável é quanto a distribuição dos primos dentro do conjunto dos naturais.

Ao longo dos tempos, diversas conjecturas foram alçadas, neste sentido, como o Crivo de Eratóstenes, o Teorema dos números primos, entre outros.

3.3.2 Crivo de Eratóstenes

Segundo Oliveira; Fernández (2012, p. 127) "o Crivo de Eratóstenes é um algoritmo que nos permite achar todos os números primos que são menores ou iguais que um natural N dado". O matemático grego Eratóstenes (285 - 194 antes da Era Comum) criou este método utilizando uma tabela ordenada de inteiros positivos, iniciando no número 2 até o número N, ou seja,

$$2, 3, 4, 5, 6, ..., N$$

Tabela 1 – Crivo de Eratóstenes

	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

Após criada a Tabela 1, serão determinados todos os primos menores que 100.

O procedimento em si é bem simples. Primeiramente, destaca-se o número 2, que é o primeiro primo e único par e depois cancelam-se todos os múltiplos de 2 restantes, ou seja, $4, 6, 8, ..., 98, 100$. Em seguida, destaca-se o número 3 e cancelam-se todos os múltiplos de 3 restantes: $9, 15, 21, ..., 93, 99$. Este procedimento continua até um determinado número $k \in \mathbb{N}$ (ver Teorema 3.3.2), onde pode-se concluir que todos os números compostos até 100 foram cancelados e os números destacados são todos os primos menores que 100, conforme Tabela 2.

Tabela 2 – Crivo de Eratóstenes - tabela com os primos menores que 100

	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			

Logo, os números primos entre 2 e 100, conforme a Tabela 2, são:

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}.$$

Não é possível identificar um padrão, mesmo organizando primos em uma tabela.

Matemáticos têm realizado descobertas importantíssimas no campo da Aritmética, porém, a distribuição dos primos dentro dos números naturais continua sendo uma questão em aberto. No entanto, esta descoberta poderia acarretar diversas outras realizações matemáticas mais significativas, como por exemplo, a prova da Conjectura de Riemann e outras conjecturas em aberto.

O teorema a seguir nos fornece resultados importantes sobre a caracterização da primalidade de números inteiros e conceitualiza o inteiro positivo $k < N$ abordado acima como o número pelo qual devemos usar como limite na busca do conhecimento se um determinado número é ou não primo.

Teorema 3.3.2. *Seja $n > 1$ um número inteiro. Então:*

a. O menor divisor de n, diferente de 1, é um número primo.

Demonstração. Seja um número natural $k > 1$, que é o menor divisor de n.

Suponhamos que k seja composto, então $\exists m \in \mathbb{N}$, onde $1 < m < k$, sendo m um divisor de k, logo $m \mid k$ e $k \mid n$, portanto, $m \mid n$, o que contradiz o fato de que k é o menor divisor de n, ou seja, k é primo. □

b. Se n é composto, este possui um menor divisor (diferente de 1), que é menor que ou igual a $\sqrt{n}$.

Demonstração. Seja n um número composto e $k > 1$, o menor divisor de n. Portanto, seja $n = k \cdot q$, com $q \geq k$ dessa forma temos $n = k \cdot q \geq k^2 \Longrightarrow n \geq k^2$.

Logo, $\sqrt{n} \geq k$. □

Sendo assim, pode-se associar este último Teorema ao Crivo de Eratóstenes, onde percebe-se que não é necessário, numa tabela que se inicia no número 2 até o 100, verificarmos cada número e, sim, até um determinado $k \leq \sqrt{N} = \sqrt{100} = 10$. Ou seja, no exemplo anterior, seria preciso verificar os primos até o número primo menor que 10, logo, $k = 7$, alcançando, assim, todos os primos nesta tabela.

Compreende-se que o método realizado por Eratóstenes seria eficaz para números pequenos, mas como a ideia central seria a de encontrar um procedimento que exprimisse qualquer primo, por maior que este o seja, o Crivo de Eratóstenes não se qualifica como método mais eficiente.

Porém, existem outros métodos e relações que foram sendo analisadas para descobrir a primalidade de um número n, como também sua localização entre os números naturais.

3.3.3 Primos Gêmeos

Segundo Viana (2018) esta nomenclatura foi utilizada pela primeira vez pelo matemático alemão Paul Stäckel $(1862 - 1919)$, em 1916.

Primos gêmeos são dois números primos ímpares e consecutivos, como os pares $(3, 5)$, $(5, 7)$, $(11, 13)$ e assim por diante, cuja diferença seja igual a 2. Ainda segundo Viana (2018) é sabido que existem 27.412.679 primos gêmeos com 10 dígitos ou menos. Porém, ainda não existe uma prova definitiva se a quantidade de números primos gêmeos é infinita, ou mesmo como se dá sua distribuição entre os próprios números primos. Ou seja, se existe alguma relação matemática que defina qual a distância entre pares de primos gêmeos entre os números primos suficientemente grandes.

Algumas informações importantes são conhecidas por meio do avanço tecnológico, como o maior primo gêmeo que possui 388.342 dígitos. Este resultado foi calculado em setembro de 2016 por Tom Greer, um voluntário norte-americano participante do projeto PrimeGrid que investiga os maiores primos e conjecturas em aberto.

No entanto, o resultado enunciado por Euclides, conhecido como Conjectura dos Primos Gêmeos, ainda não foi provado. Esta Conjectura afirma que: "Existem infinitos $p \in \mathbb{N}$ primos tais que $p + 2$ também é primo".

O matemático francês Alphonse de Polignac $(1826 - 1863)$, conjecturou que para cada número k, existem infinitos pares de primos cuja diferença é igual a $2k$. O caso $k = 1$ é a Conjectura dos Primos Gêmeos.

Em 2013, o matemático chinês Yitang Zhang, provou que para algum N menor que 70 milhões, existem infinitos pares de primos cuja diferença é N. Daí o matemático de origem chinesa Terence Tao começou a estudar a prova de Zhang a fim de apresentar

um valor menor para N. Terence Tao em colaboração com Zhang, conseguiu em 2014, demonstrar que o valor de N é menor que 246. A prova definitiva da Conjectura dos Primos Gêmeos, quando $N = 2$, ainda encontra-se em aberto.

3.4 Testes de Primalidade

Muitos matemáticos têm procurado identificar padrões numéricos que reconheçam números primos. Ainda hoje existem diversas conjecturas (ou hipóteses) em análise e sem uma comprovação matemática. No entanto, algumas técnicas podem ser utilizadas para caracterizar um número, principalmente, números muito grandes em primos ou compostos.

3.4.1 Teorema para caracterização de números primos

O Teorema 3.3.2 descreve que se n é um número inteiro composto, com $n > 1$, então este possui um menor divisor, diferente de 1, que é menor que ou igual a $\sqrt{n}$. Segundo Oliveira; Fernández (2012, p. 125): "Se n não possui divisores diferentes de 1, menores que ou iguais a $\sqrt{n}$, então n é primo". Assim, caracteriza-se, então se um inteiro maior que 1 é primo através da quantidade de divisores menores que um determinado parâmetro que é $\sqrt{n}$.

Porém, este método ainda apresenta certa insatisfação quando n é um inteiro muito grande, pois $\sqrt{n}$ seria, portanto, um número ainda muito grande para identificar seus divisores.

3.4.2 Identidade de Sophie Germain

Outro critério importante que pode ser utilizado para identificar se um número não é primo é a identidade apresentada pela matemática francesa Sophie Germain $(1776 - 1831)$.

Teorema 3.4.1. *Identidade de Sophie Germain*

Dados $a, b \in \mathbb{R}$, têm-se que:

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$$

Demonstração. $a^4 + 4b^4 = a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = (a^2 + 2b^2)^2 - 4a^2b^2 = (a^2 + 2b^2 + 2ab) \cdot (a^2 + 2b^2 - 2ab)$ □

É importante observar que esta identidade demonstra que todo número da forma $a^4 + 4b^4$, com $a, b \in \mathbb{R}$, pode ser escrito na forma de um produto, ou seja, é um número composto. Outrossim, a utilização dessa relação é válida para $a, b \in \mathbb{N}$, pois $\mathbb{N} \subset \mathbb{R}$.

Exemplo. O número $3^{12} + 2^{18}$ não é primo, pois, $3^{12} + 2^{18} = (3^3)^4 + 2^{2+16} = (3^3)^4 + 4 \cdot (2^4)^4$, com $a = 3^3$ e $b = 2^4$, portanto, esse número é da forma $a^4 + 4b^4$. Logo, pela identidade de Sophie Germain, é composto.

3.4.3 Teste de Primalidade de Fermat

Um teste de primalidade muito útil, assim como a Identidade de Sophie, *não determinístico*, ou seja, que apenas exclui a possibilidade de um determinado número de ser primo, caso não atenda à certa propriedade, é o teste realizado utilizando como base o Pequeno Teorema de Fermat, analisado no início deste capítulo, que se

$a \in \mathbb{Z}$ e $m \in \mathbb{N}$, com $m > 1$, então $a^m \equiv a \bmod m$, ou ainda, no caso em que a e m sejam primos entre si, $a^{m-1} \equiv 1 \bmod m$, para algum $a \in \mathbb{N}$.

Têm-se que, todo número m que não atenda às condições acima, não será primo.

Por outro lado, esse resultado diz que existem infinitos números que atendem à condição do Teorema acima, mas não são primos, ou seja, existem infinitos números m onde $(a, m) = 1$ e $a \in \mathbb{N}$, $a^{m-1} \equiv 1 \bmod m$, porém m não é primo. Estes números são chamados de *pseudoprimos*, ou então *Números de Carmichael* em homenagem ao matemático americano Robert Carmichael $(1879 - 1967)$.

Os números de Carmichael, segundo Figueiredo (2010, p. 91), são números compostos $(m \in \mathbb{Z}_+^*)$ que satisfazem a congruência $a^{m-1} \equiv 1 \bmod m$, para alguma base $a \in \mathbb{Z}$ e $(a, m) = 1$. Por exemplo, o número 341 é pseudoprimo para a base 2, ou seja, este número atende às condições que $2^{341-1} = 2^{340} \equiv 1 \bmod 341$ e o mdc $(2, 341) = 1$, porém, 341 é composto, pois $341 = 31 \cdot 11$. Logo, o teste de primalidade de Fermat não torna-se viável para determinar se um número é realmente primo por causa dos números de Carmichael (os pseudoprimos). Porém, pode fornecer a informação se um número não é primo.

3.4.4 Algoritmos de testes de primalidade

Atualmente, são utilizados diversos algoritmos que permitem determinar com certa facilidade se um número suficientemente grande é primo ou não.

Atualmente, o maior primo conhecido é $2^{82.589.933} - 1$, com 24.862.048 dígitos, segundo o sítio eletrônico IMPA (Instituto de Matemática Pura e Aplicada), descoberto em 15 de janeiro de 2019, através da pesquisa nomeada de GIMPS (*Great Internet Mersenne Prime Search*), sendo este o 51º primo de Mersenne (matemático francês que estudou os primos da forma $2^n - 1$).

É relevante observar a importância dos algoritmos de pesquisa sobre números primos e quão complexas tem sido as descobertas de novos primos cada vez maiores. Por exemplo, o maior primo descoberto anterior à este, foi calculado em 2017. A partir do início do uso do *software* GIMPS, por seu inventor Patrick Laroche, deu-se quase quatro meses e algumas tentativas frustradas até a descoberta do então maior primo.

3.5 Polinômio de Euler

Outra questão ainda sem resposta é se existe algum polinômio que gere todos os números primos. Sabe-se que alguns polinômios, chamados de *polinômios geradores de primos*, permitem determinar uma certa quantidade de números primos como imagem de n números pertencentes ao domínio dos inteiros positivos.

Um dos polinômios geradores de primos mais conhecido é o *Polinômio de Euler*:

$$P(n) = n^2 - n + 41, \text{ com } n \in \mathbb{N}$$

Porém, nem todas as imagens de P são números primos. Segundo Fornari (2017, p. 4), analisando $P(n)$, têm-se que:

- $1 \leq n \leq 40 \implies P(n)$ são todos números primos.
- $P(41) = 1681$ número composto.
- $P(42) = 1763$ número composto.
- $P(43) = 1847$ número primo.
- $P(44) = 1933$ número primo.
- $P(45) = 2021$ número composto.

$P(n)$ gera 40 números primos como imagem de $n \in \mathbb{N}$ variando de 1 a 40. Mas, logo em seguida, apresenta como imagens números compostos e ainda não é possível determinar se a partir de um determinado número este polinômio irá gerar somente números primos ou não. Ainda segundo Fornari (2017, p. 4) é notório que todas as imagens de múltiplos de 41 serão compostos, pois, se $k \in \mathbb{N}$ e $P(41k) = (41k)^2 - (41k) + 41 \implies P(41k) = 41 \cdot (41k^2) - 41k + 41 \implies P(41k) = 41 \cdot (41k^2 - k + 1)$, logo $41 \mid P(41k)$, $\forall k \in \mathbb{N}$.

3.6 Conjectura de Goldbach

Diversas conjecturas (ou hipóteses) sobre os números primos foram alçadas, mas ainda se encontram sem solução. Muitas dessas conjecturas, caso comprovadas, poderiam esclarecer dúvidas importantes acerca da distribuição dos números primos dentro dos números naturais, como também fornecer padrões numéricos para identificar a primalidade de números suficientemente grandes e até serem utilizadas como base para a aceitação de outros estudos ainda não demonstrados.

Uma importante hipótese, ainda em aberto, é a Conjectura de Goldbach, formulada pelo matemático prussiano Christian Goldbach, em 1742. Segundo Alencar Filho (1981, p.

129), em carta ao matemático Leonhard Euler, Goldbach conjecturou que “todo inteiro par maior que 5 pode ser escrito como a soma de 3 números primos”. Em resposta, Euler afirmou que tal conjectura, em caráter mais geral, seria equivalente à afirmação que “todo inteiro par maior que 2 pode ser escrito como a soma de 2 números primos”, conhecida como Conjectura forte de Goldbach.

Apesar dos esforços empreendidos por muitos matemáticos ao longo dos anos, não foi possível concluir a validade dessas afirmações, mesmo tendo sido provada a hipótese inicial para diversos números.

Já em 1923, segundo Perin (2017, p. 6) os matemáticos Godfrey Hardy e Jhon E. Littlewood, propuseram uma nova versão para a hipótese de Goldbach em que “todo número ímpar maior que 7 pode ser escrito como a soma de 3 números primos”. Estes provaram essa conjectura para todo n ímpar maior que um determinado m natural, ou seja, para naturais ímpares suficientemente grandes. Outro matemático Ivan M. Vinagradov, independentemente, chegou ao mesmo resultado daqueles. A versão de Hardy e Littlewood é conhecida como Conjectura fraca de Goldbach, assim chamada, pois caso a conjectura forte seja provada, esta automaticamente torna-se válida por ser uma consequência da hipótese denominada forte.

Recentemente, segundo Hefez (2016, p. 134), em 2013, o matemático peruano Harald Helfgott conseguiu demonstrar a versão de Vinagradov da Conjectura de Goldbach, onde “reduziu-se para maior do que 5 a restrição de o número ser suficientemente grande”.

4 CRIPTOGRAFIA E A SEGURANÇA DA INFORMAÇÃO: DA ESTEGANOGRAFIA À CRIPTOGRAFIA RSA

A preocupação com a segurança das informações (ou mensagens) trocadas sempre foi prioridade entre pessoas, governos e, principalmente, lideranças militares. Durante o curso histórico, muitas guerras foram vencidas através de informações recebidas por estrategistas militares, ou até por meio de informantes inimigos. Porém, mensagens interceptadas por exércitos inimigos podiam gerar consequências catastróficas para a força militar que tentava comunicar-se com suas tropas.

Assim, o medo de que suas mensagens fossem interceptadas, gerou a necessidade de tornar o envio o mais secreto possível. Segundo Singh (2011, p. 21), Heródoto foi um dos primeiros a retratar em seu livro *As Histórias*, técnicas para ocultar mensagens. Uma das técnicas utilizadas, segundo Heródoto, na guerra entre gregos e persas, foi empregada por "Histaeu que raspou a cabeça de um mensageiro e depois escreveu a mensagem em seu couro cabeludo, esperando até seu cabelo crescer".

Outras técnicas de ocultação de mensagens utilizadas durante a história foram o uso da tinta invisível e do microponto pelos alemães durante a Segunda Guerra Mundial. O primeiro microponto que foi utilizado pelos alemães e descoberto pelo FBI, em 1941, tinha menos de 1 milímetro de diâmetro e foi colocado sobre um ponto final de um texto em uma carta, interceptada pelo governo americano, entre espiões alemães que operavam na América Latina.

Esta técnica de ocultação da mensagem é conhecida como *esteganografia*, palavra composta pelas seguintes palavras gregas: *steganos* (coberto) e *graphein* (escrita). A técnica da esteganografia perdurou durante um longo período histórico, porém, sua grande falha era a de que, quando descoberta, a mensagem que estava oculta, tornava-se legível ao interceptador, perdendo toda a sua eficiência.

Ao mesmo tempo que as técnicas esteganográficas eram utilizadas, desenvolviam-se também técnicas que ocultavam as mensagens à olho nu, ou seja, mesmo visível ao interceptador, as informações não eram legíveis a menos que fosse identificada a forma na qual a mensagem havia sido "embaralhada".

Esta técnica é conhecida como *criptografia* e, segundo Singh (2011, p. 22), "é derivada da palavra grega *kryptos*, que significa *oculto*". Ou seja, encriptar ou codificar alguma mensagem é escrevê-la de forma que somente outra pessoa (o destinatário) que conheça o algoritmo (ou a chave) seja capaz de desencriptá-la (ou decodificá-la) evitando assim que mesmo que estas informações fossem interceptadas por outras pessoas, não poderiam ser lidas sem uma chave de decodificação.

A criptologia é o estudo da criptografia e de suas técnicas. Já a criptoanálise é o ramo responsável por identificar as falhas e fraquezas de cada técnica encriptação para "quebra" os códigos descobrindo a chave de desencriptação.

A criptografia tem duas técnicas principais: a *transposição* e a *substituição*. A técnica de criptografia de transposição é baseada na troca das letras de uma mensagem formando anagramas. Considerando uma palavra ou frase (mensagem) com n letras e p_i (quantidade de letras repetidas) de i letras distintas, têm-se, então, $\frac{n!}{p_1!\cdot p_2!\cdot \ldots \cdot p_i!}$ anagramas distintos.

Exemplo. A frase: "vamos atacar" possui $\frac{12!}{4!} = 19.958.400$ anagramas distintos desta mensagem. Por exemplo, MVASO ACARAT é um dos anagramas.

Já a criptografia de substituição utiliza a troca das letras da mensagem pelas letras de um código (codificação) ou cifra ou até pelas letras do alfabeto, em ordem distinta, fazendo, assim, corresponder cada letra da mensagem com uma letra diferente do alfabeto.

Os termos cifra e código se confundem muitas vezes, mas pela definição de Singh (2011, p. 47), *código* é utilizado quando substituem-se palavras ou frases e *cifra*, quando são substituídas as letras.

As cifras monoalfabéticas apresentam o uso de apenas um sistema para encriptação. Quando a cifra é polialfabética, significa que cada letra codificada da mensagem pode ter sido gerada por uma regra distinta de substituição.

Observação. Serão utilizados ao longo deste trabalho de pesquisa sempre letras minúsculas para letras da mensagem original e maiúsculas para a mensagem codificada.

a. Cifra monoalfabética de substituição:

Tabela 3 – Exemplo de Cifra de Substituição monoalfabética

Mensagem original	a	t	a	c	a	r		a	g	o	r	a
Mensagem criptografada	B	U	B	D	B	S		B	H	P	S	B

Na mensagem criptografada (ver Tabela 3) utilizou-se apenas um alfabeto para encriptar todas as letras da mensagem original. O algoritmo (ou a chave) utilizada é a mesma para encriptar ou desencriptar e é notório que as letras da mensagem original foram substituídas pelas letras subsequentes destas no alfabeto.

b. Cifra de substituição polialfabética:

Tabela 4 – Exemplo de Cifra de Substituição polialfabética

Mensagem original	b	a	t	e	r		e	m		r	e	t	i	r	a	d	a
Mensagem criptografada	D	Z	V	D	T		D	O		Q	G	S	K	Q	C	C	C

Na encriptação desta mensagem (ver Tabela 4) foram utilizadas duas chaves. Uma delas para as letras de ordem ímpar: 1ª letra, 3ª letra, 5ª letra, em diante, onde foram substituídas, por letras que distavam duas casas à direita no alfabeto, ou seja, a por C; b por D e assim sucessivamente. Já para encriptar as letras da mensagem original de ordem par: 2ª letra, 4ª letra e etc., estas foram substituídas pelas letras que estavam imediatamente à esquerda no alfabeto considerando como um ciclo, ou seja, a por Z; b por A; c por B e assim em diante.

É importante observar que nos dois casos a mesma chave encriptadora é a mesma desencriptadora. E que no item b (acima) a dificuldade de encontrar o padrão utilizado na codificação (algoritmo) deve-se ao fato de serem utilizados um sistema de substituição polialfabético.

Um criptosistema engloba todos esses fatores como algoritmo (chave), alfabeto e mensagem original que são utilizados na codificação de uma mensagem.

A criptografia tornou-se uma técnica mais interessante que a esteganografia, devido à rapidez para a troca de mensagens secretas e também sua momentânea confiabilidade no caso de interceptação. No entanto, as técnicas criptográficas, ao longo dos séculos, foram sendo aprimoradas para garantir a segurança das informações transmitidas.

O principal agente de aprimoramento das cifras foi a necessidade de trocas de informações rápidas e seguras entre governos e forças militares durante grandes conflitos, onde estas informações estratégicas em posses de mãos inimigas custariam o sucesso da guerra. Assim, esse agente impulsionou o crescimento dos estudos criptográficos. Em contrapartida, cresceu também os estudos para a quebra de cifras inimigas (criptoanálise).

4.1 Exemplos de técnicas criptográficas antigas

4.1.1 Citale espartano ou Bastão de Licurgo

Datado do século cinco antes da Era Comum, o citale espartano era um bastão de madeira no qual era enrolada uma tira de couro com letras em sequência que não apresentavam sentido algum fora do bastão, porém, quando enrolada a tira no citale (ver Figura 2) aparecia a mensagem original. O citale do emissor e do receptor deveriam possuir o mesmo tamanho e diâmetro. Esta técnica é um exemplo de criptografia de transposição.

Figura 2 – Citale Espartano

4.1.2 Cifra de César

A Cifra de César ou Cifra de deslocamento de César, foi utilizada pelo imperador romano Júlio César, onde este utilizava a cifra de substituição monoalfabética, trocando as letras da mensagem original por letras que distavam três casas no alfabeto utilizado, ou seja, a por D; b por E, e assim, sucessivamente. É importante ressaltar que essa cifra pode ser utilizada trocando as letras do alfabeto original por letra de uma a 25 casas de distância dentro do alfabeto utilizado. Considerando, ainda, que pode-se permutar todas as posições das letras do alfabeto chega-se a $26! = 403.291.461.126.605.635.584.000.000$ rearranjos possíveis de cifras distintos.

Porém, a cifra de César apresentava diversas fraquezas. Uma delas é a associação de cada letra da mensagem original a uma única do alfabeto cifrado, ou seja, cada letra do alfabeto cifrado sempre pode ser associada a uma e somente uma da mensagem original, tornando mais fácil a sua identificação.

Por volta do ano 750 de nossa Era os criptoanalistas árabes desenvolveram um método de decifração conhecido como análise de frequência que basicamente, pode ser utilizado em qualquer cifra de substituição monoalfabética. Esse método estuda a quantidade de repetições de uma determinada letra na mensagem cifrada e suas posições possíveis (por exemplo, diferenciando consoantes e vogais), como também a probabilidade do uso de cada letra de acordo com a frequência de cada letra no idioma da mensagem. No caso da Língua Portuguesa, as frequências são apresentadas na Tabela 5 a seguir:

Tabela 5 – Estatística da Frequência das letras em textos em Língua Portuguesa

Letra	Frequência	Letra	Frequência
A	$14,63\%$	N	$5,05\%$
B	$1,04\%$	O	$10,73\%$
C	$3,88\%$	P	$2,52\%$
D	$4,99\%$	Q	$1,20\%$
E	$12,57\%$	R	$6,53\%$
F	$1,02\%$	S	$7,81\%$
G	$1,30\%$	T	$4,34\%$
H	$1,28\%$	U	$4,63\%$
I	$6,18\%$	V	$1,67\%$
J	$0,40\%$	W	$0,01\%$
K	$0,02\%$	X	$0,21\%$
L	$2,78\%$	Y	$0,01\%$
M	$4,74\%$	Z	$0,47\%$

Observe que a frequência da letra a na literatura brasileira é de $14,63\%$ sendo a letra de maior frequência em textos de língua portuguesa.

Utilizando essa análise, se um texto, criptografado usando a cifra de substituição monoalfabética, apresentar com maior frequência a letra T, então, existe uma grande probabilidade, segundo a análise de frequência, dessa letra T representar a letra a da mensagem original e assim por diante.

4.1.3 Cifra de Vigenère

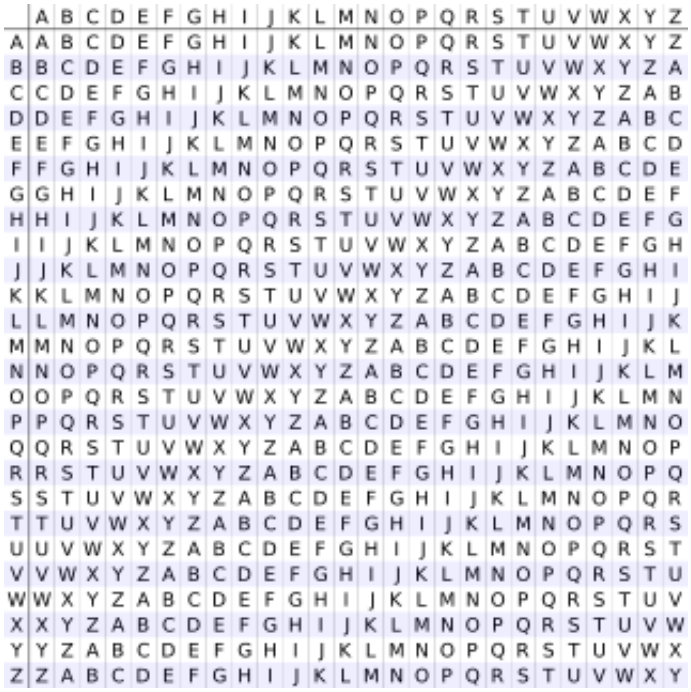
A Cifra de Vigenère também conhecida como *"Le Chiffre Indéchiffrable"* ou "A Cifra Indecifrável", começou a ser estudada em meados do século XV pelo arquiteto italiano Leon Battista Alberti $(1404 - 1472)$, onde este concebeu a possibilidade da utilização de mais de um alfabeto para cifrar letras distintas da mensagem original. Por exemplo, Alberti estudou alternar a mudança entre alfabetos distintos, conforme exemplo da Tabela 6.

Tabela 6 – Tabela de Alternância entre alfabetos originais e cifrados

Alfabeto original	A	B	C	D	E	....	Z
Alfabeto cifrado 1	O	A	Z	F	W	....	B
Alfabeto cifrado 2	C	E	G	P	S	.....	Y

No entanto, o método foi retomado apenas no séc. XVI por Blaise Vigenère, um diplomata francês. Vigenère utilizava o chamado *Quadrado de Vigenère* para cifrar as mensagens, onde cada linha do alfabeto apresentava o início na letra seguinte do alfabeto, como na Figura 3.

Figura 3 – Quadrado de Vigenère



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Ou seja, essa cifra era imune ao ataque de análise de frequência, pois, cada letra da mensagem original poderia aparecer como mais de uma letra diferente da mensagem cifrada, por exemplo, se num texto cifrado, a letra que mais aparece for a letra M, isso levará a um criptoanalista concluir que a letra M tem uma grande probabilidade de ser a letra a (pela frequência na Língua Portuguesa). Mas, se a cifra utilizada for uma cifra polialfabética, a letra M pode representar mais de uma letra distinta da mensagem original.

A chave é utilizada para indicar a linha na qual a letra da mensagem original será cifrada. No exemplo da Tabela 7, a chave corresponde à palavra **dígito**. Logo a letra a da mensagem original corresponde à letra d da chave. Assim, a letra a será trocada pela letra correspondente da linha considerada na Figura 3, que se inicia pela letra D e assim por diante. A chave utilizada para cifrar uma mensagem através da cifra de Vigenère pode ser uma palavra ou frase.

Tabela 7 – Exemplo de Mensagem cifrada com a Cifra de Vigenère

chave	d	i	g	i	t	o	d		i		g	i	t	o	d	i	g
mensagem original	a	t	a	q	u	e	m		o		c	a	s	t	e	l	o
mensagem cifrada	D	B	G	Y	N	S	P		W		I	I	L	H	H	T	U

Pode-se observar que neste exemplo, a letra H aparece 2 vezes na mensagem cifrada. Porém, a primeira letra H representa a letra t e a segunda, a letra e da mensagem original.

A Cifra de Vigenère foi utilizada em comunicações secretas por muito tempo, porém, sua implementação era complexa por causa da cifragem pouco prática.

Essa cifra perdurou indecifrável até o século XIX, quando Charles Babbage (1791 – 1871), estudioso britânico, dedicado a resolver diversos problemas em áreas distintas, começou a se dedicar à análise criptológica dessa cifra. Este observou que mesmo que letras cifradas possam representar letras distintas da mensagem original, ainda assim, poderiam ser analisadas as frequências nas quais as mesmas letras apareciam juntas e tentar encontrar, desta forma, o tamanho da chave, demonstrando o momento em que a mesma linha do alfabeto cifrado seria utilizado, gerando pistas da mensagem que fora cifrada. Logo, uma chave curta e uma mensagem longa favoreceria a decifragem da mensagem.

4.1.4 Enigma

Depois de muitas tentativas de elaborar uma técnica eficiente de codificação por linguistas e matemáticos por todo o mundo, em 1918 o engenheiro alemão Arthur Scherbius projetou uma máquina de encriptação de mensagens chamada *Enigma* (ver Figura 4). Esta máquina começou a ser utilizada para transmitir mensagens entre espiões alemães antes da Segunda Guerra Mundial e, durante a guerra, tornou-se uma das ferramentas estratégicas mais importantes do governo nazista.

A máquina Enigma apresentava um teclado e um letreiro luminoso, no qual após teclada a letra da mensagem original, iluminava-se a letra correspondente da mensagem cifrada. No entanto, seu funcionamento não era tão simples assim, já que dentro da Enigma havia vários fios elétricos, misturadores e discos que rotacionavam, de acordo com uma ordem pré-determinada gerando cifras distintas.

Figura 4 – Máquina Enigma

A Enigma recebia, primeiramente, uma regulação primária, ou seja, a cada dia um operador da Enigma mudava todas as configurações, como misturadores, fios e rotores. A máquina era composta por cinco rotores, mas só três eram usados a cada dia, cada um desses rotores continha as 26 letras do alfabeto alemão e quando pressionada uma

letra da mensagem original no teclado os rotores giravam independentes uns dos outros gerando, assim, $26^3 = 17.576$ possibilidades de encriptação. Além dos rotores, a máquina contava com misturadores das letras que aumentavam consideravelmente o número de possibilidades de codificação. As configurações diárias eram previstas em um manual que era utilizado tanto pelo emissor quanto pelo receptor da mensagem, que datilografava as letras cifradas em uma máquina configurada igualmente à máquina usada para cifrar tal mensagem. No painel luminoso acendiam as letras correspondentes à mensagem original.

Após muitos estudos realizados por organizações criadas pelos países aliados para interceptar e desencriptar as mensagens trocadas pelos países inimigos, conseguiu-se avanços na intenção de revelar as informações trocadas pelos militares alemães.

Em 1939, a Escola de Cifras e Códigos do Governo Britânico recrutou o matemático britânico e professor de Cambridge *Alan Turing*, conhecido como o pai da computação, para participar de uma unidade de criptoanalistas em *Bletchley Park*. Essa unidade, devido principalmente ao trabalho de Turing, conseguiu depois de muitos esforços descobrir as falhas no método de transmissão das cifras da Enigma Desta forma, conseguiram criar outra máquina, chamada de Bomba Eletromecânica, que conseguia, a partir de interceptações de mensagens cifradas pela Enigma, descrever as configurações que haviam sido realizadas para aquele dia específico. Assim, com outra máquina Enigma de posse dos criptoanalistas de *Bletchley Park*, esses conseguiam decifrar as mensagens interceptadas, configurando esta máquina de acordo com as configurações diárias expostas pela máquina produzida por Turing e seus colaboradores.

No livro de Singh (2011, p. 209) há uma referência a Sir Harry Hinsley que diz que: "a guerra que terminou em 1945, só teria terminado em 1948", ou seja, sem os quebradores de códigos de *Bletchley Park* a guerra poderia ter durado mais 3 anos.

Mesmo após a guerra, as operações de *Bletchley Park* mantiveram-se em segredo por vontade do governo britânico. No entanto, em 1974, após permissão do governo, o capitão Winsterbothan, responsável pela distribuição das informações obtidas para os países aliados, escreveu o livro *The Secret Ultra*, onde revelou toda a história dos criptoanalistas de *Bletchley Park* e deu destaque ao trabalho realizado por Alan Turing postumamente.

4.2 História da Criptografia RSA

A criptografia moderna passou por vários estágios durante a história. Deve-se observar porém que a maior parte dos métodos criptográficos utilizados até o final da Segunda Guerra tinham por base chaves simétricas. Neste caso, tanto a codificação quanto a decodificação de uma determinada mensagem dependia de apenas uma chave e os métodos de codificação e decodificação eram inversos. Ou seja, quem utilizasse uma chave para

codificar uma mensagem qualquer através de um processo de chave simétrica utilizaria exatamente o processo inverso para decodificá-la. Como vimos anteriormente, por exemplo, a Cifra de César utiliza um deslocamento das letras para uma determinada posição como a para C, b para D e assim sucessivamente, deslocando três posições do alfabeto no sentido do início para o fim do mesmo. Na decodificação bastará então deslocar as mesmas três posições sentido contrário, ou seja, do fim para o início do alfabeto. Com o desenvolvimento da criptoanálise, principalmente, durante a Segunda Guerra e a Guerra Fria, o método criptográfico com chaves simétricas tornou-se mais simples de ser analisado e ter seu método descoberto.

Outra importante questão a ser alçada em relação a esses métodos com chaves simétricas é a troca de chaves. Um determinado indivíduo que quisesse utilizar algum método criptográfico baseado em chave simétrica deveria informar ao destinatário qual a chave que utilizou para codificar a mensagem a fim de que este pudesse decodificá-la.

Com o advento da internet e a troca de informações por *e-mail*, por exemplo, o processo de troca de chaves tornou-se cada vez mais inseguro, devido à facilidade de interceptação. Por isso, um método de troca de chaves mais seguro e a forma de implementação deste obteve cada vez mais importância.

4.2.1 Algoritmo DHM

Após a Segunda Guerra Mundial houve um avanço significativo no estudo de técnicas de codificação. Porém, com o advento da internet, tornou-se cada vez mais necessária a utilização de chaves de codificação (ou decodificação) que pudessem ser compartilhadas entre indivíduos que estivessem distantes, por *e-mail*, por exemplo. No entanto, essa troca de chaves aumentava a probabilidade destas serem interceptadas por algum indivíduo (*hackers*).

Logo, era crescente a necessidade de reinventar esse processo de troca de chaves de forma que as informações que viessem a ser interceptadas não dessem condições de algum indivíduo vir a decodificar uma mensagem codificada.

Entre 1974 e 1976, três criptógrafos norte-americanos: Whitfield Diffie, Martin Hellman e Ralph Merkle, conceberam a ideia de troca de chaves de forma inovadora. Este conceito ficou conhecido como Protocolo Diffie-Hellman-Merkle ou, simplesmente, Algoritmo DHM, por causa das iniciais de seus inventores.

O Algoritmo DHM teve um papel importantíssimo no desenvolvimento de novas teorias para a criptografia, como por exemplo, o RSA.

Segundo Hefez (2016, p. 272), o funcionamento do Algoritmo DHM é o seguinte:

- Dois indivíduos: PEDRO e LUÍSA precisam trocar informações de forma segura. Então, eles escolhem dois números naturais x e y e os tornam públicos.
- Em seguida, PEDRO escolhe um número natural α_P que seja secreto e LUÍSA também escolhe, secretamente, um número α_L.
- Após a escolha de α_P, PEDRO calcula o único número $\beta_P < Y$, na qual

  $$x^{\alpha_P} \equiv \beta_P \bmod y$$

  e repassa β_P para LUÍSA que, por sua vez, também calcula o único número $\beta_L < y$, na qual $x^{\alpha_L} \equiv \beta_L \bmod y$ e repassa β_L para PEDRO. Estes números β_P e β_L são os únicos naturais menores que y que satisfazem a congruência $x^{\alpha_i} \equiv \beta_i \bmod y$, com $i = P$ ou L, ou seja, são os resíduos modulares (restos) da divisão de x^{α_i} por y.
- Por último, PEDRO e LUÍSA realizam, respectivamente, os cálculos:

  $$\beta_L^{\alpha_P} \equiv (x^{\alpha_L})^{\alpha_P} \equiv x^{\alpha_L \alpha_P} \equiv \lambda \bmod y, \text{ com } \lambda < y$$

  e

  $$\beta_P^{\alpha_L} \equiv (x^{\alpha_P})^{\alpha_L} \equiv x^{\alpha_P \alpha_L} \equiv \lambda \bmod y, \text{ com } \lambda < y$$

Ou seja, os dois obtêm o mesmo resultado λ, sem divulgarem os números α_P e α_L, que são as chaves secretas.

O Algoritmo DHM resolveu o problema da troca de chaves, possibilitando que dois indivíduos utilizassem a mesma chave num sistema de criptografia simétrica. Os métodos de criptografia de **chave simétrica** utiliza a mesma chave para codificar e decodificar mensagens.

O conceito elaborado por Diffie e seus colaboradores foi considerado inovador, pois, resolvera o problema de troca de chaves. Porém, este processo ainda precisava que houvesse uma troca de informações entre indivíduos para que a mensagem pudesse ser encriptada, o que poderia demandar tempo, além de relacionar a criptografia da mensagem somente entre dois indivíduos de cada vez.

Em 1975, Diffie publicou um resumo sobre o conceito de **chaves assimétricas** que, diferentemente, dos métodos criptográficos utilizados até então, apropriava-se de duas chaves: uma **Pública** (que seria de livre acesso) e outra **Privada** (que somente o destinatário teria acesso). Estas chaves apresentavam diferentes funções, uma (a pública) seria para encriptação e a outra (privada) para desencriptação.

Com a concepção de chaves assimétricas, Diffie conseguiu viabilizar a troca de mensagens criptografadas através do sistema de troca de chaves, por mais de dois indivíduos ao mesmo tempo, pois, a chave pública de um indivíduo A pode estar acessível para diversos outros indivíduos B, C, D e assim sucessivamente, que a utilizariam para encriptar a mensagem e e enviá-la de volta a A que, por sua vez, utilizaria a sua chave privada para desencriptar cada mensagem recebida. Nesse conceito de chaves assimétricas, os métodos de encriptação e desencriptação são distintos, ou seja, precisa-se de uma função ou conceito matemático que seja considerado de "mão única", uma função em que o cálculo de volta seja extremamente difícil. Embora Diffie tenha elaborado o conceito de chaves assimétricas, este não conseguiu implementar uma função de "mão única" que viabilizasse esse processo. Ou seja, a implementação do conceito elaborado por Diffie necessitava de uma função matemática que quando fossem aplicados os dados para codificação se obtivesse um resultado de forma fácil, porém, sua decodificação (ou sua operação inversa) fosse extremamente difícil ou praticamente irreversível, em tempo razoável.

4.2.2 Rivest, Shamir e Adleman

Mesmo após o Algoritmo criado por Diffie, Hellman e Merkle, ainda permanecia a dificuldade de implementar a técnica de chaves assimétricas, devido à falta de conhecimento sobre qual a função mais apropriada para este fim.

Mais tarde, em 1978, Ronald Rivest e Adi Shamir (ambos estudantes do curso de Ciências da Computação) e Leonard Adleman (estudante de Matemática), todos do Laboratório de Ciência da Computação do MIT (*Massachusetts Institute of Technology*), implementaram uma técnica criptográfica utilizando chaves assimétricas, através de Congruências Modulares.

O conceito de Congruências Modulares tornou-se o mais apropriado para garantir a segurança do método que ficou conhecido como **Criptografia RSA**, devido às iniciais dos sobrenomes dos seus inventores.

Além disso, a segurança do método RSA deve-se, sobretudo, à utilização do produto de dois primos p e q suficientemente grandes como chave de criptografia, sendo este produto $n = p \cdot q$ de acesso público, porém, inviável a sua fatoração devido às características dos números primos.

4.3 Método de Criptografia RSA

O grande avanço da Criptografia RSA em relação aos outros métodos mencionados nesta pesquisa é a utilização de chaves assimétricas, ou seja, duas chaves que são aplicadas de forma a realizarem técnicas distintas de codificação e decodificação.

O método RSA, em geral, é implementado por meio de programas computacionais

que, obviamente, utilizam a base binária como fundamento das representações simbólicas. O sistema de códigos binários mais utilizado para o RSA é o ASCII (*American Standard Code for Information Interchange*), onde cada sequência de 0 e 1 corresponde a um determinado símbolo (ou caractere). Porém, para fins de cálculo utilizaremos uma simbologia com números na base decimal.

Segundo Coutinho (2014, p. 147) é necessária a utilização de uma tabela de pré-codificação (ver Tabela 8), onde cada letra do alfabeto está associada a um número na base 10, iniciando por $10 - A$, $11 - B$, até $35 - Z$.

São utilizados números de dois algarismos, pois, se a tabela iniciasse pelo número 1, por exemplo, associado à letra A, poderíamos encontrar ambiguidades no momento da conversão da mensagem criptografada para o alfabeto original. Por exemplo, se tivéssemos a seguinte mensagem codificada 112915, utilizando a tabela a cima, teríamos ambiguidades em relação à transcrição destes números para letra do alfabeto original, pois, não é compreensível se tivermos $1 - 12 - 9 - 1 - 5$ ou $11 - 29 - 15$ entre outras possibilidades.

Tabela 8 – Tabela de Pré-Codificação

10	A	24	O
11	B	25	P
12	C	26	Q
13	D	27	R
14	E	28	S
15	F	29	T
16	G	30	U
17	H	31	V
18	I	32	W
19	J	33	X
20	K	34	Y
21	L	35	Z
22	M	99	ESPAÇO
23	N		

Finalmente, deve-se conceber o método de criptografia RSA seguindo três etapas bem definidas:

- Pré-Codificação
- Codificação
- Decodificação

4.3.1 Análise Matemática do Método RSA

Na etapa de Pré-Codificação a mensagem original é convertida em uma sequência numérica. Esta é "quebrada" em blocos com m números naturais, onde $1 \leq m < n$.

O procedimento da escolha da quebra dos blocos deve respeitar o critério de cada bloco ser menor que n e de que não se deve escolher m iniciando com algarismo zero, pois no momento da decodificação pode haver perda de informações.

Para a codificação e decodificação, são determinados dois primos p e q distintos e suficientemente grandes. Segundo Bose (2008, p. 259), atualmente, com o avanço de técnicas de fatoração e o uso de força bruta por meio de computadores cada vez mais potentes, torna-se necessário o comprimento de uma chave pública não inferior a 1024 bits, o que corresponde a 309 dígitos para utilizar em segurança de informações pessoais, chaves com 2048 bits (ou 617 dígitos decimais) para sigilo de informações empresariais e 3072 bits, em diante, para chaves de chave para dados governamentais importantes. Em seguida, obtemos dois importantes resultados que são os valores de $n = p \cdot q$ e $\phi(n) = (p-1) \cdot (q-1)$.

Na codificação, escolhe-se o número $e \in \mathbb{N}$, $1 < e < \phi(n)$, tal que o mdc $(e, \phi(n)) = 1$, ou seja, os números e e $\phi(n)$ são primos entre si. Vale ressaltar que não existe $e \in \mathbb{N}$ quando $1 < e < \phi(4)$, ou seja, $p = 2$ e $q = 2$, ou ainda, quando $1 < e < \phi(6)$, portanto, com $n = 2 \cdot 3$. Assim, temos a chave de codificação (chave pública) que é composta por dois valores: e e n. Ambos valores são públicos, fornecidos pelo receptor e necessários para que o emissor possa codificar a mensagem.

Para se determinar a chave de decodificação d_k, precisa-se obter o número $d \in \mathbb{N}$, $0 < d < \phi(n)$, tal que $e \cdot d \equiv 1 \bmod \phi(n)$, ou seja, o número d é o inverso múltiplo de e módulo $\phi(n)$. Vale ressaltar que, pelo Teorema 2.3.13, como $(e, \phi(n)) = 1$, então, o valor de d sempre existe, como também é único pelo Corolário 2.3.12.1. Assim, a chave de decodificação (chave privada) d_k é composta por dois valores d e $\phi(n)$. Assim, o receptor, que detém esses valores, poderá decodificar a mensagem recebida.

Segue, então, a codificação de cada bloco m:

$$c_k(m) \equiv m^e \mod n,$$

sendo $c_k(m)$ a codificação de cada bloco m pela chave de codificação c_k.

Analisando a congruência acima pode-se inferir que $c_k(m)$, que é a codificação do bloco m, é o resto da divisão de m^e por n. Logo, a decodificação de $c_k(m)$ será:

$$d_k(c_k(m)) \equiv (c_k(m))^d \bmod n,$$

onde $d_k(c_k(m))$ é a decodificação da mensagem codificada. É necessário observar que $d_k(c_k(m))$ é o resto da divisão de $(m^e)^d = m^{ed}$ por n.

Vale ressaltar que a demonstração seguirá, primeiramente, analisando a validade das congruências $d_k(c_k(m)) \equiv m \bmod p$ e $d_k(c_k(m)) \equiv m \bmod q$, o que implicará na validade de $d_k(c_k(m)) \equiv m \bmod n$

Sendo $c_k(m) \equiv m^e \bmod n$, queremos mostrar que $d_k(c_k(m)) \equiv m \bmod n$, ou seja, que a codificação e a decodificação são operações inversas e que, conseguimos, ao decodificar a codificação de cada bloco m, retornar à mensagem original. Mostraremos, inicialmente que, $d_k(c_k(m)) \equiv m \bmod p$, com p primo.

Sendo d o inverso multiplicativo de e módulo $\phi(n)$, têm-se $ed \equiv 1 \bmod \phi(n)$, na qual existe $t \in \mathbb{N}$ tal que $ed = 1 + t \cdot \phi(n)$.

Considerando os seguintes casos:

- Se o mdc $(m, p) = 1$, utilizando o Pequeno Teorema de Fermat têm-se que $m^{p-1} \equiv 1 \bmod p$ e elevando ambos os membros da congruência ao expoente $t(q-1)$, obtemos $(m^{p-1})^{t(q-1)} = m^{t(p-1)(q-1)} \equiv 1 \bmod p$. Assim, multiplicando ambos os membros por m, têm-se $m^{1+t(p-1)(q-1)} \equiv m \bmod p$. Como $1 + t(p-1)(q-1) = 1 + t \cdot \phi(n) = ed$. Logo, têm-se que $d_k(c_k(m)) \equiv m^{ed} = m^{1+t(p-1)(q-1)} \equiv m \bmod p$.
- Se o mdc $(m, p) = p$, então $m^{ed} = m^{1+t\cdot\phi(n)} \equiv m \bmod p$ é verdadeira, pois, ambos os lados são congruentes a zero módulo p.

Logo, $d_k(c_k(m)) \equiv m \bmod p$, para qualquer bloco m da mensagem original. De modo análogo, têm-se que $d_k(c_k(m)) \equiv (m^e)^d = m^{ed} \equiv m \bmod q$, com q primo.

Como $d_k(c_k(m)) \equiv m \bmod p$ e $d_k(c_k(m)) \equiv m \bmod q$ implicam que $p \mid [d_k(c_k(m)) - m]$ e $q \mid [d_k(c_k(m)) - m]$, sendo p e q primos, tem-se que $n = p \cdot q \mid [d_k(c_k(m)) - m]$, ou seja, $d_k(c_k(m)) \equiv m \bmod n$.

Em resumo, o receptor fornece os valores de e e de $n = p \cdot q$ de forma pública para um possível emissor. Em seguida, o receptor calcula os valores de d e $\phi(n)$ que este utilizará para decodificar a mensagem recebida do emissor.

4.4 Exemplo de codificação de uma mensagem

Considerando as três principais etapas do método RSA: Pré-Codificação, Codificação e Decodificação torna-se necessária a utilização de um exemplo prático de codificação/decodificação de uma mensagem, chamada original.

4.4.1 Pré-Codificação

Codificaremos a seguinte mensagem: *"ataquem hoje"*. Será utilizada a Tabela 8, com valores pré-definidos com dois algarismos cada, que correspondem às letras do alfabeto e ao caractere espaço.

Na etapa de Pré-Codificação são necessários alguns cuidados para não haver perda de informações na etapa de decodificação da mensagem, informação ambígua ou mesmo comprometida. Alguns cuidados necessários:

- Utilização de números com dois algarismos iniciando no número 10 (representando a letra a) até o número 35 (representa a letra z) e o número 99 que representa o espaço entre duas palavras, para que não haja ambiguidades.
- Não iniciar nenhum bloco da mensagem com algarismo zero.
- Não dividir nenhum bloco da mensagem codificada de forma que, esse bloco, seja maior que o produto entre os primos escolhidos, ou seja, cada bloco deve ser menor que $n = p \cdot q$.

Logo, a mensagem *"ataquem hoje"*, pré-codificada através da tabela 8 é:

$$10291026301422991724 1914$$

A sequência numérica acima é uma sequência pré-codificada. A quebra em blocos desta sequência não é única, por exemplo:

$$102 - 910 - 26 - 301 - 42 - 2 - 99 - 17 - 241 - 9 - 14$$

ou ainda,

$$10 - 29 - 102 - 630 - 14 - 22 - 9 - 91 - 72 - 419 - 14$$

são exemplos de quebras da sequência pré-codificada em blocos.

Porém, a escolha de cada bloco m deve ser menor que $n = p \cdot q$. Então, escolhendo-se dois primos $p = 13$ e $q = 17$, têm-se $n = 13 \cdot 17 = 221$.

Logo, pode-se escolher a seguinte quebra em blocos da sequência numérica que representa a pré-codificação:

$$102 - 9 - 10 - 26 - 30 - 142 - 29 - 91 - 72 - 41 - 9 - 14$$

4.4.2 Codificação

Para codificar a sequência acima temos que codificar cada bloco m utilizando a chave de codificação c_k. Para isso, é necessário obter o valor de e, ou seja, encontrar o resto da divisão de m^e por n. Portanto,

$$m^e \equiv c_k(m) \bmod n.$$

Escolhamos a chave $e \in \mathbb{N}$, sendo $1 < e < \phi(n)$, com mdc $(e, \phi(n)) = 1$. Como $\phi(221) = (13-1)\cdot(17-1) = 16 \cdot 12 = 192$ e sendo $(e, 192) = (e, 2^6 \cdot 3) = 1$, o valor de e não tem fatores 2 e 3. Logo, e pode ser $35 = 5 \cdot 7 < 192$.

Calculando cada bloco m de acordo com a congruência $m^e \equiv c_k(m) \bmod n$, obtêm-se $c_k(m)$ que é a codificação de cada bloco m:

- $102^{35} \equiv c_k(102) \bmod 221 \Longrightarrow 102^{35} = (102^2)^{17} \cdot 102 \equiv 17^{17} \cdot 102 = (17^2)^8 \cdot 17 \cdot 102 \equiv 68^8 \cdot 1734 = (68^2)^4 \cdot 1734 \equiv 204^4 \cdot 187 = (204^2)^2 \cdot 187 \equiv 68^2 \cdot 187 \equiv 204 \cdot 187 = 38148 \equiv 136 \bmod 221$. Ou seja, $c_k(102) = 136$.

- $9^{35} \equiv c_k(9) \bmod 221 \Longrightarrow 9^{35} = (9^3)^{11} \cdot 9^2 \equiv 66^{11} \cdot 81 = (66^2)^5 \cdot 66 \cdot 81 \equiv 157^5 \cdot 5346 = (157^2)^2 \cdot 157 \cdot 5346 \equiv 118^2 \cdot 157 \cdot 42 = 13924 \cdot 6594 \equiv 1 \cdot 185 \equiv 185 \bmod 221$. Ou seja, $c_k(9) = 185$.

- $10^{35} \equiv c_k(10) \bmod 221 \Longrightarrow (10^5)^7 \equiv 108^7 = (108^2)^3 \cdot 108 \equiv 172^3 \cdot 108 \equiv 144 \cdot 108 = 15552 \equiv 82 \bmod 221$. Ou seja, $c_k(10) = 82$.

- $26^{35} \equiv c_k(26) \bmod 221 \Longrightarrow 26^{35} = (26^2)^{17} \cdot 26 \equiv 13^{17} \cdot 26 = (13^3)^5 \cdot 13^2 \cdot 26 \equiv 208^5 \cdot 4394 = (208^2)^2 \cdot 208 \cdot 4394 \equiv 169^2 \cdot 208 \cdot 195 = 28561 \cdot 40560 \equiv 52 \cdot 117 = 6084 \equiv 117 \bmod 221$. Ou seja, $c_k(26) = 117$.

- $30^{35} \equiv c_k(30) \bmod 221 \Longrightarrow 30^{35} = (30^3)^{11} \cdot 30^2 \equiv 38^{11} \cdot 16 = (38^3)^3 \cdot 38^2 \cdot 16 \equiv 64^3 \cdot 23104 \equiv 64^3 \cdot 120 = 262144 \cdot 120 \equiv 38 \cdot 120 = 4560 \equiv 140 \bmod 221$. Ou seja, $c_k(30) = 140$.

- $142^{35} \equiv c_k(142) \bmod 221 \Longrightarrow 142^{35} = (142^2)^{17} \cdot 142 \equiv 53^{17} \cdot 142 = (53^3)^5 \cdot 53^2 \cdot 142 \equiv 144^5 \cdot 157 \cdot 142 = (144^2)^2 \cdot 144 \cdot 22294 \equiv 183^2 \cdot 144 \cdot 194 = 33489 \cdot 27936 \equiv 118 \cdot 90 = 10620 \equiv 12 \bmod 221$. Ou seja, $c_k(142) = 12$.

- $29^{35} \equiv c_k(29) \bmod 221 \Longrightarrow 29^{35} = (29^3)^{11} \cdot 29^2 \equiv 79^{11} \cdot 178 = (79^2)^5 \cdot 79 \cdot 178 \equiv 53^5 \cdot 14062 \equiv (53^2)^2 \cdot 53 \cdot 139 = 2809^2 \cdot 7367 \equiv 157^2 \cdot 74 = 24649 \cdot 74 = 1824026 \equiv 113 \bmod 221$. Ou seja, $c_k(29) = 113$.

- $91^{35} \equiv c_k(91) \bmod 221 \Longrightarrow 91^{35} = (91^3)^{11} \cdot 91^2 = 753571^{11} \cdot 8281 \equiv 182^{11} \cdot 104 = (182^2)^5 \cdot 182 \cdot 104 = 33124^5 \cdot 18928 \equiv (195^2)^2 \cdot 195 \cdot 143 = 38025^2 \cdot 27885 \equiv 13^2 \cdot 39 = 169 \cdot 39 = 6591 \equiv 182 \bmod 221$. Ou seja, $c_k(91) = 182$.

- $72^{35} \equiv c_k(72) \bmod 221 \Longrightarrow 72^{35} = (72^3)^{11} \cdot 72^2 = 373248^{11} \cdot 5184 \equiv 200^{11} \cdot 101 = (200^2)^5 \cdot 200 \cdot 101 = 40000^5 \cdot 20200 \equiv 220^5 \cdot 89 = (220^2)^2 \cdot 220 \cdot 89 = 48400^2 \cdot 19580 \equiv 1^2 \cdot 132 \equiv 132 \bmod 221$. Ou seja, $c_k(72) = 132$.

- $41^{35} \equiv c_k(41) \bmod 221 \Longrightarrow 41^{35} = (41^3)^{11} \cdot 41^2 = 68921^{11} \cdot 1681 \equiv 190^{11} \cdot 134 = (190^2)^5 \cdot 190 \cdot 134 = 36100^5 \cdot 25460 \equiv 77^5 \cdot 45 = (77^2)^2 \cdot 77 \cdot 45 = 5929^2 \cdot 3465 \equiv 183^2 \cdot 150 = 33489 \cdot 150 \equiv 118 \cdot 150 = 17700 \equiv 20 \bmod 221$. Ou seja, $c_k(41) = 20$.

- Este bloco é idêntico à outro bloco já codificado. Logo, $c_k(9) = 185$.
- $14^{35} \equiv c_k(14) \bmod 221 \implies 14^{35} = (14^3)^{11} \cdot 14^2 = 2744^{11} \cdot 196 \equiv 92^{11} \cdot 196 = (92^2)^5 \cdot 92 \cdot 196 = 8464^5 \cdot 18032 \equiv 66^5 \cdot 131 = (66^2)^2 \cdot 66 \cdot 131 = 4356^2 \cdot 8464 \equiv 157^2 \cdot 27 = 24649 \cdot 27 = 665523 \equiv 92 \bmod 221$. Ou seja, $c_k(14) = 92$.

Vale ressaltar que as etapas dos cálculos acima foram realizados considerando as propriedades mencionadas nos capítulos anteriores, a fim de manipular valores sem a utilização de máquinas para calcular e sem excesso de tempo. Por exemplo, $14^{35} = (14^3)^{11} \cdot 14^2$, pois foi observado que seria mais fácil para uma pessoa efetuar os cálculos 14^3 e 14^2 sem o auxílio de calculadoras e chegar a um valor de resto, quando divido pelo valor de $n = 221$.

Logo, concluí-se que a codificação da mensagem original é:

$$136 - 185 - 82 - 117 - 140 - 12 - 113 - 182 - 132 - 20 - 185 - 92$$

A mensagem codificada acima é que será enviada ao destinatário. É importante observar que, para que não haja perda de informações, deve-se manter a ordem dos blocos codificados.

4.4.3 Decodificação

Em posse da mensagem codificada acima, o receptor decodificará a mensagem utilizando a chave privada d, onde d é o inverso multiplicativo de e módulo $\phi(n)$,

$$e \cdot d \equiv 1 \bmod \phi(n),$$

onde $d \in \mathbb{N}$ e $0 < d < \phi(n)$. Logo, calculando o valor de d, tem-se:

$35d \equiv 1 \bmod \phi(221) \implies 35d \equiv 1 \bmod 192 \implies 35 \cdot 11 = 385 \equiv 1 \bmod 192$. Então, $d = 11$.

O valor de d é encontrado utilizando o valor de $\phi(n)$. Em particular, este valor de $d = 11$ foi encontrado utilizando tentativa e erro, porém existem outras técnicas como o Algoritmo de Euclides. Conhecido o valor de d, tem-se a seguinte congruência que relaciona o valor de d e n, sendo $d_k(c_k(m))$ o resto da divisão de cada bloco codificado m^{ed} por n. Então, a decodificação da sequência codificada é igual ao próprio bloco m original, ou seja, $d_k(c_k(m)) = m$. Logo,

$$(m^e)^d \equiv d_k(c_k(m)) \bmod n \implies (c_k(m))^d \equiv d_k(c_k(m)) \equiv m \bmod n$$

Calculando a decodificação de cada bloco da sequência codificada tem-se:

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 136^{11} = (136^2)^5 \cdot 136 = 18496^5 \cdot 136 \equiv 153^5 \cdot 136 = (153^4) \cdot 153 \cdot 136 = 547981281 \cdot 20808 \equiv 68 \cdot 34 = 2312 \equiv 102 \bmod 221$. Ou seja, $d_k(136) = 102$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 185^{11} = (185^2)^5 \cdot 185 = 34225^5 \cdot 185 \equiv 191^5 \cdot 185 = 191^4 \cdot 191 \cdot 185 \equiv 35 \cdot 191 \cdot 185 = 1236725 \equiv 9 \bmod 221$. Ou seja, $d_k(185) = 9$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 82^{11} = (82^2)^5 \cdot 82 = 6724^5 \cdot 82 = (6724^2)^2 \cdot 6724 \cdot 82 \equiv 217^2 \cdot 551368 \equiv 217^2 \cdot 194 = 47089 \cdot 194 = 9135266 \equiv 10 \bmod 221$. Ou seja, $d_k(82) = 10$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 117^{11} = (117^2)^5 \cdot 117 = 13689^5 \cdot 117 = (13689^2)^2 \cdot 13689 \cdot 117 \equiv 169^2 \cdot 1601613 \equiv 52 \cdot 26 = 1352 \equiv 26 \bmod 221$. Ou seja, $d_k(117) = 26$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 140^{11} = (140^2)^5 \cdot 140 = 19600^5 \cdot 140 = (19600^2)^2 \cdot 19600 \cdot 140 = 384160000^2 \cdot 2744000 \equiv 120^2 \cdot 64 = 14400 \cdot 64 = 921600 \equiv 30 \bmod 221$. Ou seja, $d_k(140) = 30$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 12^{11} = (12^2)^5 \cdot 12 = 144^5 \cdot 12 = (144^2)^2 \cdot 144 \cdot 12 = 20736^2 \cdot 1728 \equiv 183^2 \cdot 181 = 33489 \cdot 181 = 6061509 \equiv 142 \bmod 221$. Ou seja, $d_k(12) = 142$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 113^{11} = (113^2)^5 \cdot 113 = 12769^5 \cdot 113 \equiv 172^5 \cdot 113 = (172^2)^2 \cdot 172 \cdot 113 = 29584^2 \cdot 19436 \equiv 191^2 \cdot 209 = 36481 \cdot 209 = 7624529 \equiv 29 \bmod 221$. Ou seja, $d_k(113) = 29$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 182^{11} = (182^2)^5 \cdot 182 = 33124^5 \cdot 182 \equiv 195^5 \cdot 182 = (195^2)^2 \cdot 195 \cdot 182 = 38025^2 \cdot 35490 \equiv 13^2 \cdot 130 = 21970 \equiv 91 \bmod 221$. Ou seja, $d_k(182) = 91$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 132^{11} = (132^2)^5 \cdot 132 = 17424^5 \cdot 132 \equiv 186^5 \cdot 132 = (186^2)^2 \cdot 186 \cdot 132 = 34596^2 \cdot 24552 \equiv 120^2 \cdot 21 = 302400 \equiv 72 \bmod 221$. Ou seja, $d_k(132) = 72$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 20^{11} = (20^2)^5 \cdot 20 = 400^5 \cdot 20 \equiv (400^2)^2 \cdot 400 \cdot 20 = 160000^2 \cdot 8000 \equiv 217^2 \cdot 44 = 2071916 \equiv 41 \bmod 221$. Ou seja, $d_k(20) = 41$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 185^{11} = (185^2)^5 \cdot 185 = 34225^5 \cdot 185 \equiv 191^5 \cdot 185 = 191^4 \cdot 191 \cdot 185 \equiv 35 \cdot 191 \cdot 185 = 1236725 \equiv 9 \bmod 221$. Ou seja, $d_k(185) = 9$.

- $(c_k(m))^d \equiv m \bmod n \Longrightarrow 92^{11} = (92^2)^5 \cdot 92 = 8464^5 \cdot 92 \equiv 66^5 \cdot 92 = 66^3 \cdot 66^2 \cdot 92 = 287496 \cdot 4356 \cdot 92 \equiv 196 \cdot 157 \cdot 92 = 2831024 \equiv 14 \bmod 221$. Ou seja, $d_k(92) = 14$.

Observa-se que a decodificação de cada bloco $c_k(m)$, ou seja, cada bloco codificado da mensagem original, é idêntico ao bloco m da mensagem original. Assim, $d(c_k(m)) = m$, o que verifica a validade das chaves e método utilizados para encriptar mensagens.

4.5 Segurança do Método RSA e a Segurança da Informação

4.5.1 Segurança do Método RSA

Existem diversos métodos que são utilizados na segurança de dados da internet e até de informações confidenciais de países. Entre esses, o Método RSA é um dos mais utilizados pela sua característica de ser implementado através de chaves assimétricas, onde uma destas chaves é pública e outra é privada, possibilitando, assim, a rapidez na comunicação.

Por outro lado, a sua ampla utilização se deve também à sua segurança, ou seja, à capacidade de proteção das informações transmitidas ou armazenadas de forma considerada invulnerável. Essa invulnerabilidade é baseada, principalmente, no tamanho de suas chaves, ou seja, na quantidade de algarismos que os números p e q primos possuem. Quanto maiores esses primos, previamente escolhidos, maior será o produto n entre eles que será a chave pública.

Daí então surgem diversas indagações sobre a vulnerabilidade do conhecimento de p e q primos através da divulgação de n. E é exatamente esse o segredo da segurança deste método. Uma vez escolhidos p e q muito grandes com 100 ou mais algarismos cada, tem-se uma chave n também muito grande (com muitos algarismos) e, por causa das características dos números primos e da ineficiência de métodos de decomposição de inteiros tão grandes torna-se improvável a sua descoberta.

Portanto, a segurança deste método de criptografia consiste na utilização de primos com muitos algarismos e na falta de eficiência de métodos (ou algoritmos) que consigam decompor o produto desses primos pelo menos de forma razoavelmente rápida. Coutinho (2014, p. 158) afirma que só para testar se suas chaves eram realmente seguras o *RSA Laboratory*, empresa que obtém os direitos de implementação do código RSA, apresentava, de tempos em tempos, um código com chaves de tamanhos não tão grandes para saber se algum indivíduo conseguiria decompor em tempo hábil os fatores primos. Em 2005, alguns cientistas do Escritório Federal de Segurança da Informação da Alemanha (*Bundesamt für Informationssicherheit*) conseguiram decompor o último destes códigos cuja chave possuía 193 algarismos. Os cálculos foram feitos em nada menos que 5 meses, utilizando 80 computadores com alta velocidade. Ou seja, a rapidez da troca de informações com a utilização de um produto de dois primos muito grande supera extremamente a sua decodificação.

4.5.2 Segurança da Informação no cotidiano

Para Ferreira (2003, p. 162), a segurança da informação "protege a informação de diversos tipos de ataques que surgem no ambiente organizacional, garante a continuidade dos negócios, reduz as perdas e maximiza o retorno dos investimentos e das oportunidades".

Em outra definição, Sêmola (2003, p. 43) diz que a segurança da informação é "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".

O Método RSA é baseado em cálculos matemáticos, o que possibilita maior proteção das informações. Desta forma, ficam garantidos os princípios da segurança da informação estabelecidos pela ABNT NBR ISO/IEC 27002:2013 (ver (ABNT, 2013)), correspondente aos três primeiros princípios citados a seguir e ainda os princípios acrescentados por Sêmola (2003, p. 11), que segundo Fernandes (2013, p. 20), são:

- **Confidencialidade** - garante o acesso das informações à somente pessoas autorizadas.
- **Disponibilidade** - permite que as informações desejadas sejam acessadas a qualquer momento.
- **Integridade** - garante a exatidão e inviolabilidade das informações.
- **Legalidade** - garante que as informações estejam de acordo com a lei vigente.
- **Autenticidade** - garante a veracidade das informações transmitidas e recebidas, como também, a legitimidade dos usuários envolvidos.

A segurança da informação afeta-nos em diversas situações cotidianas e, por muitas vezes, nem percebemos. Quando falamos em *firewall*, por exemplo, estamos citando um programa de proteção de nossos dados em nosso computador, mas quando enviamos esses dados pela rede precisamos também garantir que estes, se interceptados, não sejam revelados. Assim, a necessidade da criptografia se apresenta como proteção.

Citando um exemplo prático relacionado à proteção de dados pessoais enviados pela rede, destaca-se o caso dos bloqueios realizados pela justiça brasileira ao aplicativo de mensagens *WhatsApp*, considerado um dos mais utilizados no mundo para sua função, entre os anos de 2015 e 2016, onde haviam quatro ordens judiciais que exigiam o acesso, por parte da Polícia Federal, à contas suspeitas de serem utilizadas por criminosos. Na época, as ações foram baseadas na Lei Nº 12.965 de 2014, conhecida como Marco Civil da internet, disponível em Brasil (2014), onde são apregoados os princípios norteadores para expansão da comunicação de rede no Brasil. No artigo 7º desta Lei é dito: "O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos...". No mesmo artigo, no inciso III é dito: "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial".

Como resposta às solicitações da justiça, o *WhatsApp* informou que não conseguiria repassar essas informações (conversas trocadas por meio de tais contas), pois nem o próprio

aplicativo teria acesso a elas, uma vez que são criptografadas de “ponta a ponta” (ou, em inglês, *“end-to-end”*). Ou seja, a criptografia utilizada não permite que a mensagem trocada entre dois indivíduos, quando interceptada, seja legível, incluindo os servidores do próprio *WhatsApp*.

O tipo de criptografia utilizada é a assimétrica, chamada *end-to-end encryption* ou *E2EE*, onde dois indivíduos A e B em uma conversa pelo *WhatsApp* possuem suas chaves privadas e públicas, como na RSA.

Assim, quando A quer mandar uma mensagem para B, o aplicativo de A “busca” a chave pública de B, através do servidor do aplicativo, e codifica a mensagem que é transmitida para B. A partir daí, o aplicativo de B, utiliza sua chave privada para decodificar a mensagem recebida.

Assim, os responsáveis pelo *WhatsApp* alegaram que as informações solicitadas pela Justiça estavam debaixo de muitas camadas de criptografia e que não seria possível fornecê-las.

O método para verificar se uma conversa entre dois indivíduos realmente está criptografada é conferir se o código de segurança que aparece no aplicativo de ambos são iguais ou também um dos indivíduos pode utilizar o seu aparelho para escanear o código *QR* do outro aparelho (ver Figura 5) e, então aparecerá um sinal da cor verde, caso esta conversa esteja segura. Por outro lado, a criptografia de ponta a ponta só assegura a confidencialidade das informações quando são transmitidas. Ou seja, caso um hacker acesse o celular de um indivíduo e este não possua um sistema de segurança em seu aparelho, as informações do *WhatsApp* poderão ser acessadas. Por esta razão, o próprio aplicativo recomenda ao usuário ativar a “verificação em duas etapas”, ou seja, de tempos em tempos o aplicativo requer uma senha que o usuário cadastrou no aplicativo. Essa funcionalidade também impede que uma pessoa que queira instalar o *WhatsApp* de outro indivíduo no aparelho deste, sem o conhecimento daquele, tenha êxito, pois serão necessário, além do código enviado ao aparelho, a senha cadastrada no aplicativo, evitando possíveis clonagens.

Figura 5 – Ilustração do Código de Segurança - *QR Code*

O Ministro do STF Ricardo Lewandowski, em 2016, impetrou uma medida liminar liberando o funcionamento do aplicativo. [1]

[1] Segundo o site do G1 da Globo, de acordo com o sítio eletrônico: <https://g1.globo.com/tecnologia/noticia/bloqueios-ao-whatsapp-no-brasil-chegam-ao-stf-entenda.ghtml>, com acesso em 25 de janeiro de 2020.

5 A HIPÓTESE DE RIEMANN E PROBLEMAS P VS NP

Em 1900, no ICM (*International Congress of Mathematicians*), em Paris, o matemático David Hilbert listou 23 problemas que, segundo ele, ocupariam os matemáticos durante o século XX. O problema de número oito foi a Hipótese de Riemann. De todos os problemas listados por Hilbert, somente a conjectura feita por Bernhard Riemann não foi ainda resolvida até a presente data.

Em 2000, o *Clay Mathematics Institute* (CMI), organização sem fins lucrativos, criada em 1998 pelo empresário Landon T. Clay, apresentou outra lista com 7 problemas em aberto da matemática. A Hipótese de Riemann era o único problema que fazia parte de ambas as listas. Essas questões em aberto foram chamadas de *Problemas do Milênio*.

Para incentivar a pesquisa matemática no mundo o *Clay Mathematics Institute* (CMI), prometeu premiar com 1 milhão de dólares quem conseguisse resolver qualquer um dos 7 problemas em aberto. Atualmente, somente a Conjectura de Poincaré foi resolvida pelo matemático russo Grigori Perelman, em 2010, que recusou a premiação.

5.1 Hipótese de Riemann

A Hipótese de Riemann é uma conjectura relacionada ao cálculo da densidade dos números primos por meio da determinação dos zeros da função zeta de Riemann dada pela soma infinita de potências de números complexos.

5.1.1 Bernoulli e Euler

Muitos matemáticos ao longo dos anos tiveram a curiosidade de estudar o conceito de séries infinitas. As séries são geradas pela soma dos termos de uma sequência. Algumas séries causam estranheza, por isso, o tempo dedicado por alguns brilhantes matemáticos em entender suas propriedades.

Muitos matemáticos já anunciaram ter resolvido a Hipótese de Riemann. Porém, porém quando seus estudos passaram por análise foram encontrados erros.

As séries infinitas podem convergir ou divergir. As séries convergentes são aquelas cujas somas parciais dos termos de uma sequência infinita vão se aproximando de um determinado número. Ou seja, o limite das somas parciais tendem a um determinado número. As séries que não são convergentes são denominadas divergentes, portanto, as somas parciais não tendem a um número específico. Logo, quanto mais somam-se parcelas a uma soma parcial mais este aumenta ou diminui infinitamente.

Em 1689, o matemático Jacob Bernoulli $(1655 - 1705)$ começou a estudar as séries do tipo:

$$1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n}..., \text{ para cada } n \in \mathbb{N} - \{1\}.$$

Já era conhecido desde 1650 que a série harmônica $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}...$ é divergente, ou seja, que essa soma cresce indefinidamente.

Em 1735, o matemático suíço Leonhard Euler $(1707 - 1783)$ começou a estudar a *função zeta* $\zeta(n) = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n}...$, para $n \in \mathbb{R}$.

Segundo Devlin (2004, p. 65), Euler provou que $\zeta(2) = \frac{\pi^2}{6}$ e logo depois chegou à conclusão que a função $\zeta(n) = 1 + \frac{1}{2^n} + \frac{1}{3^n} + \frac{1}{4^n}...$ era equivalente à

$$\zeta(n) = \prod_{p}^{\infty} \left(\frac{1}{1 - p^{-n}} \right) = \left(\frac{1}{1 - 2^{-n}} \right) \cdot \left(\frac{1}{1 - 3^{-n}} \right) \cdot \left(\frac{1}{1 - 5^{-n}} \right) \cdot \left(\frac{1}{1 - 7^{-n}} \right) ...$$

com $n \in \mathbb{R}, n > 1$ e p primo, conhecido como *produto euleriano*, indicando assim, a relação entre a função ζ de Euler e a distribuição dos números primos e indicando como essas séries poderiam ser escritas na forma de produto em que cada fator teria um número primo p (PERUZZO, 2012).

5.1.2 Conjectura de Gauss (Teorema dos Números Primos)

O matemático alemão Johann Carl Friedrich Gauss $(1777 - 1855)$, por volta dos seus 15 ou 16 anos conjecturou sem exibir uma prova formal e utilizando tabelas de primos, que a quantidade de primos de 1 até x, $x \in \mathbb{R}$ seria

$$\pi(x) \simeq \frac{x}{\ln x}$$

Anos depois, o matemático francês Adrien-Marie Legendre $(1752 - 1833)$ fez diversas descobertas importantes sobre números primos e, inclusive, realizou outra estimativa para $\pi(x)$ em sua obra *Essai sur la théorie des nombres*, que seria

$$\pi(x) \simeq \frac{x}{\ln x - 1{,}08366}$$

Já em 1896, dois matemáticos Hadamard e de la Vallée Poussin, independentemente, provaram que

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

baseados nas ideias do matemático Riemann.

Esse teorema ficou conhecido como Teorema dos Números Primos e mostra que a estimativa feita por Gauss $\frac{\pi(x)}{\ln x}$ para $\pi(x)$ é razoável, pois $\frac{\pi(x)}{\frac{x}{\ln x}} = 1$, para x real suficientemente grande.

A Tabela 9 apresenta os valores de $\pi(x)$ e a estimativa $\frac{x}{\ln x}$, feita por Gauss:

Tabela 9 – Valores de $\pi(x)$ e estimativa em relação a $\frac{x}{\ln x}$

x	$\pi(x)$	$\frac{x}{\ln x}$
10	4	$4,34$
100	25	$21,72$
1000	168	$144,76$
10000	1229	$1085,74$
100000	9592	$8685,83$
1000000	78498	$72358,9$
10000000	664579	$620424,37$
100000000	5761455	$5428881,65$
1000000000	50847534	$48255561,45$
10000000000	455052511	$434291670,28$

Mais tarde, Gauss formulou um conceito que trouxe um melhor refinamento à estimativa da quantidade de primos até um determinado $x \in \mathbb{R}$, ou seja, $L(x) = \int_2^x \frac{dt}{\ln t}$ é uma aproximação mais razoável para $\pi(x)$.

5.1.3 Bernhard Riemann

O matemático alemão Georg Friedrich Bernhard Riemann $(1826 - 1866)$ apresentou um artigo sobre a função zeta de Gauss em 1859, onde sua pretensão seria provar a Conjectura de Gauss. Mesmo não obtendo êxito neste objetivo, Riemann formulou um conceito importante que é conhecido como Função Zeta de Riemann.

Primeiramente, Riemann estudou a função $\zeta(n)$ de Gauss, para $n \in \mathbb{R}$ e estendeu o conceito para $s \in \mathbb{C}$, ou seja, a função zeta de Riemann é

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{ para cada } Re(s) > 1,$$

sendo $Re(s)$ parte real de um número complexo s.

Riemann definiu a função acima para números complexos maiores que 1 e observou que os valores de $s \in \mathbb{C}$ para os quais $\zeta(s) = 0$, ou seja, os chamados *zeros triviais* da função zeta seriam todos da forma $-2n$, $n \in \mathbb{N}$. Estes zeros seriam os inteiros pares negativos: $\{-2, -4, -6, ...\}$.

Finalmente, Riemann notou que os *zeros não triviais* da função zeta estavam entre os números complexos s, cuja parte real encontrava-se no intervalo entre 0 e 1. Daí

quando este conseguiu calcular alguns zeros não triviais de $\zeta(s)$ começou a obter valores posicionados não aleatoriamente no plano complexo, mas sim "enfileirados" em relação aos números complexos s, com parte real $Re(s) = \frac{1}{2}$, ou seja, os números da forma $s = \frac{1}{2} + k \cdot i$, sendo $k \in \mathbb{R}$ e i (unidade imaginária). Essa reta onde esses zeros de $\zeta(s)$ pareciam estar concentrados foi chamada de *reta crítica*.

Riemann conjecturou que então *"todos os zeros não triviais da função ζ estão na reta crítica"*. Esta afirmativa ficou conhecida como Hipótese de Riemann e é o mais famoso dos problemas em aberto (DEVLIN, 2004).

Esse comportamento não aleatório dos zeros não triviais da função zeta, se comprovada, demonstra a relação entre a função zeta e a distribuição dos números primos. Segundo Peruzzo (2012, p. 55) "A hipótese de Riemann é considerada o problema mais profundo e fundamental da teoria dos números, e está intimamente ligada à distribuição dos números primos". Embora Riemann tenha iniciado seus estudos sobre a função zeta com a intenção de concluir a Conjectura de Gauss, ele conseguiu estabelecer uma hipótese que pode ter aplicações em diversas áreas. Em relação à densidade dos números primos, pode-se concluir que a veracidade desta conjectura implicaria num padrão mais geral em relação à sua distribuição:

> Riemann mostrou que se todos os zeros complexos (não reais) da função zeta tiverem parte real igual a 1/2, então o grau segundo o qual a função densidade $D(n) = \frac{\phi(n)}{n}$ difere da curva $\frac{1}{ln(n)}$ varia de uma maneira aleatória, parecida com o modo como a proporção de caras que você obtém quando joga uma moeda varia em torno de $\frac{1}{2}$. Isso significa que ainda que você não possa prever de forma acurada quando é que o próximo primo ocorrerá, o padrão global é extremamente regular. (DEVLIN, 2004, p. 69)

Já em 1914, o matemático britânico Godfrey Hardy demonstrou que existem infinitos zeros não triviais da função zeta na reta crítica $Re(s) = \frac{1}{2}$. Porém, não obteve êxito na demonstração da Hipótese de Riemann.

5.2 Problemas P vs NP

5.2.1 Definições importantes

Assim como a Hipótese de Riemann, o Problema $P = NP$ é considerado um dos maiores problemas matemáticos do milênio. Porém, as aplicações deste problema abrangem outras áreas, como a Ciência da Computação, por exemplo.

A Ciência da Computação, segundo Martins (2019, p. 4), é "a ciência que estuda as técnicas, metodologias e instrumentos computacionais, visando automatizar os processos e desenvolver soluções com o uso de processamento de dados". A automatização de processos sejam eles quais forem, precisa de formulação teórica, ou seja, uma lista do "passo a passo" lógico que esse programa deve assumir. Passos lógicos são as operações que o computador irá realizar para chegar em uma solução. Na Matemática também utilizam-se técnicas bem

definidas logicamente para se chegar a alguma conclusão (solução) formal. Chama-se à essa sequência de passos lógicos de algoritmo. Um algoritmo computacional seriam os passos lógicos que devem ser processados pelo computador para obter soluções que atendam às condições de um determinado problema.

Um dos ramos mais importantes da Ciência Computacional é a Teoria da Complexidade Computacional, onde é estudada a viabilidade de um determinado problema ou conjunto de problemas serem resolvidos através de um determinado algoritmo. Ou seja, segundo Oliveira (2010, p. 4), mede "os recursos necessários e suficientes para solucionar problemas algorítmicos concretos".

O estudo da Complexidade Computacional visa relacionar a eficiência ou não de determinados problemas em serem resolvidos utilizando-se algoritmos relacionados aos mesmos em tempo razoável. Uma classe (conjunto) de problemas que os métodos computacionais empregados para solucioná-los não apresentam resultados eficientes (rápidos) são considerados não-determinísticos. Já aqueles que as técnicas computacionais implementadas (algoritmos) alcançam êxito em tempo razoável são denominados determinísticos (ou eficientes).

5.2.2 Tempo Polinomial

Segundo Oliveira (2010, p. 18), pesquisadores em Ciência da Computação descobriram diversos problemas em que seus algoritmos demoravam muito tempo para resolvê-los, tornando a busca por uma solução inviável.

Exemplo desse tipo de problema é o conhecido Problema do Caixeiro Viajante: um comerciante deseja fazer um itinerário partindo de uma determinada cidade A, passando por outras $n-1$ outras cidades e retornando para a cidade A, tudo isso percorrendo a menor distância total.

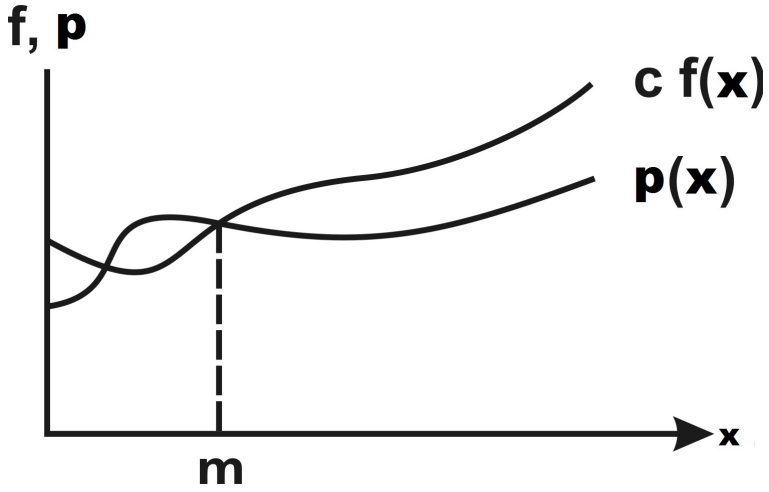
Aparentemente simples, este problema possui $n!$ possibilidades de escolhas para os possíveis trajetos, o que torna o trabalho de análise da menor distância muito demorado. Daí a necessidade de descobrir métodos computacionais (caso existam) com maior eficiência, ou seja, menor tempo de execução.

Definição 5.2.1. Seja $f(x)$ uma função dominante assintoticamente em relação à função $p(x)$. Então existem duas constantes c e m reais positivas tais que

$$|p(x)| \leq c \cdot |f(x)|, \forall\ x \geq m$$

A definição restringe as funções p e f às suas imagens não negativas. O gráfico da Figura 6 ilustra o comportamento assintótico dominante de f em relação à p, para todos os valores do domínio maiores que m.

Figura 6 – Gráfico do comportamento assintótico dominante da função f em relação à p



A partir da noção acima, podemos definir a Notação assintótica ou Notação de Bachmann-Landau O (O-Grande ou letra grega Ômicron) que descreve o comportamento limitante ou assintótico de uma função em relação à outra. Dizemos que uma função $p = O(f(x))$, ou seja, p está na ordem O de f, se f for uma função dominante assintoticamente em relação à p.

Um exemplo prático seriam de duas funções f e g, onde $f(x) = 3x^2 + 6x + 5$ e $g(x) = x^2$. Temos:

$$3x^2 + 6x + 5 \leq 3x^2 + 6x^2 + 5x^2 = 14x^2,$$

ou seja, $f(x) \leq 14 \cdot g(x)$, $\forall x \geq 1$ e portanto, $f(x) = O(g(x))$, ou ainda $f(x) = O(x^2)$.

Portanto, após a definição da notação assintótica (O), tem-se imediatamente a definição de eficiência (tempo) de execução de um determinado algoritmo. Destacam-se, duas classes de comportamento assintótico:

- $f(x) = O(c \cdot k^x)$, com $k > 1$ e c constante de acordo com o problema: algoritmos com essa função de complexidade são denominados algoritmos exponenciais em relação ao tempo de execução.
- $f(x) = O(p(x)) = O(c \cdot x^k)$, k (constante positiva) e c constante de acordo com o problema, sendo $p(x)$ um polinômio em x: algoritmos com essa função de complexidade são denominados algoritmos polinomiais em tempo de execução.

O algoritmo de um problema que possui função de complexidade igual a um polinômio tem um tempo polinomial de execução, o é considerado mais eficiente, pois proporciona um resultado (*output*) em tempo razoável. Já o algoritmo de um problema que apresenta função de complexidade exponencial possui um tempo de execução inviável,

denominado tempo exponencial. A Figura 7 a seguir apresenta o tempo de execução de diferentes algoritmos.

Figura 7 – Tempo de execução de algoritmos distintos em relação às suas classes de complexidades

Função tempo/ complexidade	Quantidade de dados: N				
	10	20	30	40	50
N	0,00001s	0,00002s	0,00003s	0,00004s	0,00005s
N^2	0,0001s	0,0004s	0,0009s	0,0016s	0,0036s
N^3	0,001s	0,008s	0,027s	0,064s	0,125s
2^N	0,001s	1,0s	17,19 min	12,7 dias	35,7 anos
3^N	0,059s	58 min	6,5 anos	3.855 séculos	200.000,000 séculos

Um problema é reconhecido como eficiente, ou seja, exibe menor tempo de execução quando existe um comportamento assintótico em relação a uma função polinomial $p(x)$, onde x são os valores de entrada (*input*) suficientemente grandes. Ou seja, existe uma função $f(x)$ que domina assintoticamente $p(x)$, $\forall x \geq m$, m constante.

5.2.3 Problemas P e NP

Pode-se, classificar alguns problemas computacionais como P (Problemas de tempo polinomial determinístico). Como exemplo de problema pertencente à classe de problemas P tem-se o de decidir se um inteiro é primo ou não.

Já os problemas cujos algoritmos possuem tempo de execução exponencial, mas dada uma solução, possui decisão da veracidade ou não desta em tempo polinomial, são classificados como problemas da classe NP, ou seja, problemas de tempo polinomial não-determinístico. Como exemplo de problema pertencente à classe de problemas NP tem-se o da fatoração de um inteiro dado.

Observando as duas classes definidas acima, pode-se inferir que $P \subseteq NP$, pois todos os problemas que são resolvidos em tempo polinomial também possuem tempo polinomial para verificação de uma solução dada.

5.2.4 Problema do Milênio P = NP?

Este é um dos Problemas do Milênio, formulado inicialmente por Stephen Cook e Leonid Levin em 1971. O problema $P = NP$ é o maior problema em aberto da Ciência da Computação.

O problema, em questão, consiste em saber se $P = NP$, ou seja, se os problemas de classe de complexidade NP também pertencem à classe P de complexidade. A questão

é se $NP \subseteq P$, ou seja, caso os problemas de classe NP pertençam à classe P, então a conclusão seria a igualdade entre ambas as classes.

A dúvida consiste em saber se os problemas de classe NP também podem ser resolvidos em tempo polinomial. Os problemas de classe NP possuem algoritmos que executam a procura por uma solução em tempo exponencial. Assim, a descoberta da veracidade do problema $P = NP$ traria a conclusão que para todos os problemas de classe NP existiria algum algoritmo que buscaria a solução em tempo polinomial. Desta forma, até os mais difíceis problemas teriam solução rápida.

Já se for comprovada que a questão é falsa, ou seja, $P \neq NP$, então, será admitido que existem problemas computacionais em que os algoritmos procuram soluções utilizando "força bruta" em tempo exponencial.

Ainda existem problemas de classe NP que são considerados muito difíceis, os denominados NP-completos, como o do Caixeiro Viajante. Esta classe possui uma importante característica: caso algum problema desta classe puder ser resolvido em tempo polinomial, então toda a classe NP também possui algum algoritmo que execute uma solução em tempo polinomial, ou seja, $P = NP$. Vale ressaltar que os problemas de classe NP-completos possuem a característica de que todos os outros problemas de classe NP se reduzem a ele.

5.3 Os Problemas do Milênio e a Criptografia RSA

A segurança da Criptografia RSA, a princípio, consiste em dois problemas. A primeira delas, identifica o cálculo da fatoração de um inteiro n suficientemente grande, como algo muito difícil de ser realizado até por meio computacional. O problema de decompor n em fatores primos, sendo n com mais de 1024 bits, é considerado de complexidade NP. Logo, teoricamente, é mais fácil, tendo p e q primos, conferir se $p \cdot q = n$ (complexidade polinomial). Porém, os algoritmos utilizados atualmente para a fatoração de n demorariam um tempo demasiadamente grande para chegar na decomposição $p \cdot q$ a partir de n.

Em Coutinho (2014, p. 158), podemos encontrar um dos desafios implementados pelo RSA *Laboratory*. Neste desafio público, o número inteiro possuía 193 algarismos e sua fatoração foi finalizada em novembro de 2005, por F.Bahr, M. Boehm, J. Franke e T. Kleinjung, após 5 meses e o uso de 80 computadores.

O problema refere-se à existência de alguma função que consiga representar um padrão em relação aos números primos. De forma que, seja possível encontrar qualquer número primo, maior que fosse, com rapidez. Vimos que muitos matemáticos tentaram implementar polinômios geradores de primos e funções que pudessem caracterizá-los quanto à sua distribuição dentro dos números naturais. Porém, algumas funções apresentavam primos até um certo valor do domínio, mas também apresentavam números compostos.

Pode-se observar, no entanto, que as conjecturas alçadas nesta pesquisa como a Hipótese de Riemann e o Problema $P = NP$ tem relações diretas com esses problemas mencionados acima. Em relação à Conjectura de Riemann, este afirmou que as soluções não triviais da função zeta de Riemann estão na reta crítica, ou seja, é um número complexo da forma $\frac{1}{2} + b \cdot i$, sendo $b \in \mathbb{R}$ e i número imaginário. Por outro lado, a função zeta de Riemann pode ser relacionada aos números primos. Caso esta conjectura seja provada, abrirá caminho para a descoberta de um padrão de distribuição dos números primos dentro dos números naturais. Logo, a própria descoberta da veracidade da Conjectura de Riemann, pode gerar mais técnicas matemáticas que implicariam num padrão geral sobre os números primos, conforme Devlin (2004, p. 74).

Desta forma, o problema $P = NP$ apresenta relevante importância pois sua comprovação significaria que qualquer problema NP também pertence à classe P. Ou seja, para qualquer problema com algoritmos de resolução que precisam de um tempo considerável ou mesmo impraticável para se chegar a um determinado resultado, existiria algum algoritmo mais eficaz que possuiria complexidade de tempo polinomial para gerar uma solução.

Portanto, todos os problemas, até aqueles considerados mais difíceis, poderiam ser solucionados. Bastaria apenas encontrar o algoritmo mais apropriado. A conclusão de que $P = NP$ impactaria consideravelmente o problema da segurança criptográfica, pois revelaria que o problema da fatoração de inteiros muito grandes é solucionável em tempo polinomial, sendo apenas necessária a utilização de novos algoritmos mais eficientes.

A prova da Conjectura de Riemann e do problema $P = NP$ traria uma nova perspectiva em relação aos números primos e à decomposição de inteiros em fatores primos. Ou seja, toda a base criptográfica, da mais atual a mais eficiente, que utiliza os números primos como composições para suas chaves de segurança ficaria exposta. Qualquer indivíduo que estivesse em posse de tais conhecimentos e algoritmos computacionais mais eficientes poderia acessar informações consideradas seguras, como senhas bancárias, informações pessoais e dados governamentais e até militares. Toda a noção e implementação da criptografia teria que ser repensada.

6 ATIVIDADES

As atividades a seguir são propostas para alunos do Ensino Básico (Ensino Fundamental II e Ensino Médio), tanto da rede pública quanto da privada. Temos, como objetivo geral, estimular o estudo da matemática, ao disseminar o conhecimento e incitar a curiosidade, tanto dos educandos como dos educadores, em relação aos números primos e suas propriedades.

A Matemática é considerada uma disciplina de difícil compreensão por muitos. É comum o questionamento, por parte dos educandos, acerca da utilidade de determinados conceitos matemáticos. Com os números primos essa realidade não é diferente. Muitas vezes, seu estudo se restringe a fatorar de números naturais pequenos e nem sequer são abordadas as diversas aplicações cotidianas de suas propriedades, como a criptografia inclusa em nossas transações bancárias, por exemplo.

Jogos e curiosidades matemáticas podem ser utilizados pelo educador como estímulo ao educando no processo de ensino e aprendizagem da Matemática. Exemplos práticos como dominós de frações, jogos de perguntas e respostas baseados em conceitos matemáticos e oficinas sobre a montagem de cubos mágicos, são apenas alguns destes estímulos. Segundo Grando (2000, p. 17):

> As posturas, atitudes e emoções demonstradas pelas crianças, enquanto se joga, são as mesmas desejadas na aquisição do conhecimento escolar. Espera-se um aluno participativo, envolvido na atividade de ensino, concentrado, atento, que elabore hipóteses sobre o que interage,que estabeleça soluções alternativas e variadas, que se organize segundo algumas normas e regras e, finalmente, que saiba comunicar o que pensa, as estratégias de solução de seus problemas.

A criptografia também pode desempenhar grande papel motivacional na aprendizagem de Matemática. Embora não pertença ao currículo do Ensino Básico, o desenvolvimento de técnicas criptográficas, mesmo que primitivas, podem servir de estímulo para o educando numa aula de Matemática. O conceito de criptografia pode ser utilizado na resolução de problemas matemáticos, como ressaltou Groenwald; Olgin (2011, p. 20): “metodologia de resolução de problemas é indicada para o desenvolvimento de atividades didáticas com o tema Criptografia”.

Um problema matemático apresenta sempre um método de resolução dentro de conceitos e fórmulas estabelecidas (na criptografia, um algoritmo). Além disso, o educando para resolver um problema precisa “decodificar” o enunciado e depois chegar à alguma conclusão.

Ainda sobre resolver problemas matemáticos tem-se Polya (1978) que relata a resolução das questões matemáticas através de quatro “passos” gerais, os quais podem ser

reformulados assim:

- Primeiramente, a leitura e interpretação do enunciado do problema.
- Seguindo, a compreensão de qual método seja mais eficaz na resolução de uma determinada questão.
- A seguir, a resolução em si, ou seja, a aplicação do método para a resolução.
- Depois de alcançar um resultado é importante que este seja verificado se condizente com a resposta esperada para o problema em questão.

Nas atividades aqui propostas são apresentados um jogo de dominó matemático inspirado na Conjectura de Goldbach e uma atividade com cubo mágico, sendo utilizando para codificação e decodificação de mensagens, baseado no Quadrado de Vigenère. São atividades lúdicas e divertidas que ressaltam o aprendizado da matemática, como também a curiosidade sobre os números primos e a criptografia.

6.1 Detalhamento das atividades

As atividades podem ser aplicadas aos estudantes do Ensino Básico, de acordo com as seguintes propostas.

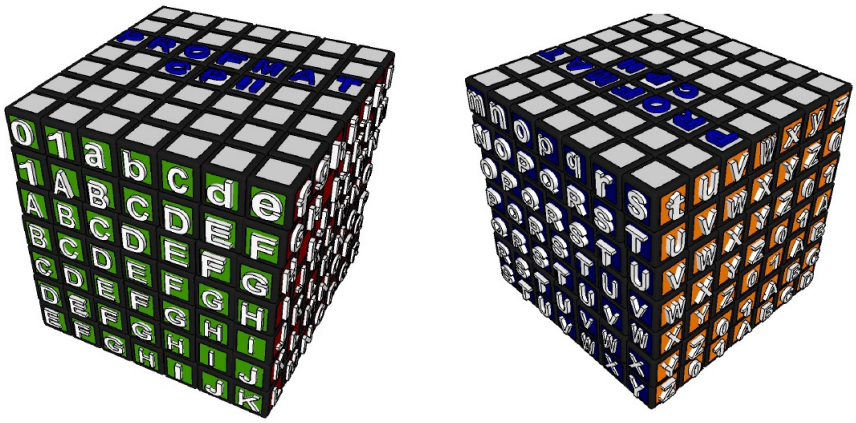
- **Objetivos**: Desenvolver o raciocínio lógico dos estudantes, bem como estimular o interesse destes pela Matemática.
- **Público-Alvo**: Estudantes, das redes pública e privada, do Ensino Básico (Ensino Fundamental II e Ensino médio).
- **Metodologia**: Primeiramente, serão ministradas 2 aulas (de 50 minutos cada) sobre os números primos e suas principais propriedades e aplicações (criptografia, por exemplo), bem como sua relação com os Problemas do Milênio. Em seguida, serão apresentadas as duas atividades, com tempo máximo de 50 minutos de duração para realização, em grupo de 2 a 4 estudantes, escolhidos aleatoriamente. As atividades são práticas e seguem um determinado roteiro.
- **Avaliação**: Durante o processo de realização das atividades os estudantes serão avaliados constantemente quanto ao interesse pelos conteúdos propostos e quanto à criatividade em solucionar os problemas apresentados.

6.1.1 Cubo de Vigenère

Após a apresentação do conteúdo sobre números primos e suas propriedades, os estudantes estarão aptos a participar da atividade denominada de Cubo de Vigenère, inspirada na versão bidimensional do Quadrado de Vigenère.

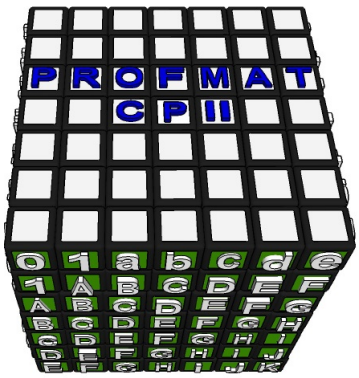
É utilizado um cubo de Rubik (ou cubo mágico), com dimensões 7x7x7 para aproveitar as 28 faces dos cubos menores que ficam no entorno de cada camada lateral ($7 \cdot 4 = 28$). Em cada face pequena é apresentada uma letra (de A a Z) ou um número (0 ou 1). A primeira camada superior do cubo apresenta o alfabeto minúsculo (representando as letras da mensagem original). Já as outras camadas apresentam letras maiúsculas que representam as letras da mensagem cifrada. No entanto, cada camada de cima para baixo, tem o alfabeto deslocado uma casa para a esquerda, conforme a Figura 8. Ou seja, o Cubo de Vigenère também é um sistema criptográfico polialfabético, necessitando de técnicas de decodificação mais complexas. Porém, as atividades serão práticas e os estudantes poderão utilizar o próprio cubo para codificar e decodificar a mensagem.

Figura 8 – Faces do Cubo de Vigenère



O processo de codificação se desenvolve da seguinte forma: primeiramente, voltamos a face verde onde é apresentado o início do alfabeto original para frente (face verde = face frontal), conforme Figura 9. As faces vermelha, azul e laranja são as faces laterais. Em seguida, escolhe-se, aleatoriamente, seis números naturais, que compõem a chave de codificação/decodificação.

Figura 9 – Face Frontal (verde) e Superior do Cubo de Vigenère



Por exemplo, para codificar a palavra *profmat* são escolhidos, aleatoriamente, os números

$$4 - 10 - 1 - 2 - 3 - 8 \text{ (chave)}$$

Cada número corresponde, respectivamente, às camadas de cima para baixo (exceto a camada superior). Esse número representa a quantidade de vezes que aquela camada será girada da esquerda para direita. Por exemplo, a 2^{a} camada de cima para baixo tem como chave o número 4, ou seja, esta será movimentada horizontalmente 4 vezes e será observado que a camada voltará ao seu estado inicial. A 3^{a} camada (de cima para baixo) tem como chave o número 10, então será movida horizontalmente 10 vezes (esquerda para direita), o que será o mesmo que mover a camada somente 2 vezes a partir do estágio inicial, e assim, sucessivamente.

Um dos objetivos mais específicos é que o estudante perceba esta particularidade: o número n natural escolhido não gerará n diferentes movimentos e sim, na verdade, r movimentos distintos, sendo r o resto da divisão de n por 4, ou seja, $r = \{0, 1, 2, 3\}$, onde zero representa o estágio inicial. Esta relação pode ser observada da seguinte forma:

$$4 \equiv 0 \bmod 4 \text{ e } 10 \equiv 2 \bmod 4 \text{ e assim sucessivamente.}$$

Vale ressaltar que foi tomado um sentido positivo, ou seja, da esquerda para direita e, por esta razão, n positivo. No entanto, poderia ser usado $n \in \mathbb{Z}$. Por exemplo, a chave -1, corresponderia à uma volta de determinada camada no sentido da direita para a esquerda. Pois,

$$3 \equiv -1 \bmod 4$$

Portanto, a chave 3 corresponde ao mesmo giro do que a chave -1.

Seguindo, tem-se cada letra da palavra *profmat* que corresponde ao alfabeto de codificação de uma das camadas iniciando sempre de cima para baixo e no caso de palavras com mais de 6 letras, a sétima letra retorna à primeira camada de codificação. Ou seja,

- p corresponde à segunda camada, chave 4.
- r corresponde à terceira camada, chave 10.
- o corresponde à quarta camada, chave 1.
- f corresponde à quinta camada, chave 2.
- m corresponde à sexta camada, chave 3.
- a corresponde à sétima camada, chave 8.
- t corresponde à segunda camada, chave 4.

Para codificar, o estudante se apropriará do cubo voltado para sua face frontal (verde) e moverá cada camada o número de vezes que escolher de chave. Em seguida, observará a letra p na primeira camada (que não foi movida) e qual letra (codificada) lhe corresponde na camada pós movimento, ou seja, a letra Q, como vemos na Figura 10.

Figura 10 – Codificação da letra p

Da mesma forma, a letra r pode ser codificada por F na terceira camada, conforme Figura 11.

Figura 11 – Codificação da letra r

Seguindo, a codificação da letra o, conforme Figura 12.

Figura 12 – Codificação da letra o

Segue a codificação da letra f na letra X, de acordo com Figura 13.

Figura 13 – Codificação da letra f

A codificação da letra m na letra Y, conforme Figura 14.

Figura 14 – Codificação da letra m

A codificação da letra a na letra G, conforme Figura 15.

Figura 15 – Codificação da letra a

Finalmente, a codificação da letra t na letra U, conforme Figura 16.

Figura 16 – Codificação da letra t

Finalizado o processo de codificação, a mensagem codificada será

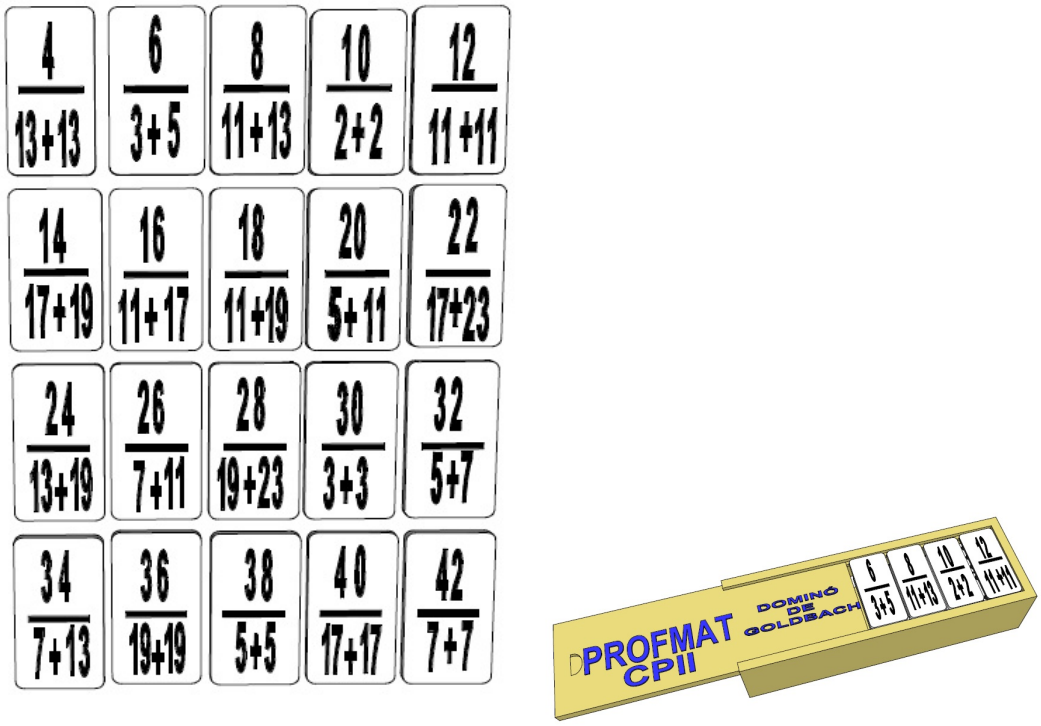
$$QFKXXGU$$

Esta mensagem que será repassada para outro estudante que será responsável por sua decodificação utilizando o próprio cubo. Para isso, bastará praticar o processo inverso, ou seja, procurar a letra Q na segunda camada e ver a qual letra do alfabeto original (na primeira camada) esta corresponde (letra p), e assim, sucessivamente.

6.1.2 Dominó de Goldbach

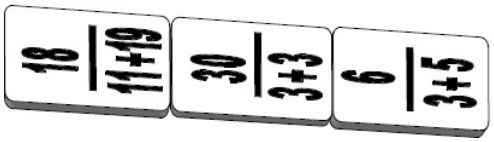
A atividade a seguir, é baseada na Conjectura de Goldbach e nomeada de *Dominó de Goldbach*. Este produto pedagógico matemático apresenta 20 peças, conforme Figura 17. Em cada peça retangular tem-se duas partes, numa das quais é apresentado um número para entre 4 e 42.

Figura 17 – Jogo completo com as 20 peças do Dominó de Goldbach



Na outra parte, cada peça tem uma soma de dois números primos. As regras são, praticamente, idênticas ao de um dominó comum, conforme jogada ilustrada pela Figura 18. Cada grupo com 4 estudantes inicia o jogo com cinco peças. O estudante que jogar todas as suas peças primeiro vence.

Figura 18 – Forma de jogo do Dominó de Goldbach



6.2 Lista de Atividades

6.2.1 Atividade do Dominó de Goldbach

Cada grupo de quatro estudantes receberá um jogo de dominó com vinte peças que devem ser divididas igualmente entre os participantes.

(A) O grupo deve jogar, no mínimo, uma partida.

(B) O grupo deverá relatar suas percepções em relação às peças do jogo. O que pode ser observado em relação aos números de cada peça? E sobre os números que estão sendo somados?

(C) Em grupo, elaborem esquemas (desenhos) de mais, no mínimo, cinco peças que poderiam compor esse mesmo dominó.

(D) Na opinião, de cada membro do grupo por que não há nas peças números ímpares (na parte do número isolado)?

6.2.2 Atividade do Cubo de Vigenère

Cada grupo de estudantes (de 2 a 4 em cada grupo) receberá um cubo com dimensões 7x7x7. Depois de explicado o modo de codificação e decodificação utilizando o cubo, cada grupo deverá se dividir, em um primeiro momento, em codificadores e decodificadores. Os codificadores escolherão uma chave de seis números aleatórios e uma palavra secreta para ser codificada utilizando o cubo. Os decodificadores deverão decodificar a palavra secreta utilizando, por sua vez, o cubo. Depois, uma segunda rodada é realizada, invertendo-se os codificadores e decodificadores.

A seguir, deverão ser respondidos os seguintes questionamentos:

(A) Para cada membro do grupo, qual atividade foi mais difícil, codificar ou decodificar?

(B) A chave é composta por números aleatórios que, inclusive, podem ser muito grandes. Como poderíamos descobrir a quantidade de movimentos necessários para cada número da chave? Por exemplo, digamos que escolhemos o número 80. Será realmente necessário movimentar a camada do cubo oitenta vezes? Por quê?

6.2.3 Avaliação

Os produtos pedagógicos criados acima (Dominó de Goldbach e Cubo de Vigenère) foram elaborados no programa em 3D do Sketchup [2]. Devido à falta de tempo hábil para implementação desses produtos em sala de aula ressalto que, posteriormente a este projeto de pesquisa, será realizada a implementação desses produtos, de forma física, para aplicação pedagógica em sala de aula do Ensino Básico. A análise dos resultados efetivos será publicada posteriormente em artigos.

Vale ressaltar, porém, que são esperados diversas respostas por parte dos estudantes quanto às atividades propostas. Em relação à primeira atividade, é relevante que os alunos observem a relação da soma de dois primos com o resultado par. Na segunda atividade é importante que estes cheguem à conclusão que o número de voltas eficientes de cada

[2] Este programa apresenta versão gratuita e paga e pode ser baixado através do link: *<https://www.sketchup.com/pt-BR>*.

camada é o resto da divisão do número de voltas (chave) por quatro (número de faces laterais).

7 CONCLUSÃO

Esta pesquisa aborda o tema números primos de forma diferenciada, buscando suas propriedades e aplicações, como na área da criptologia. O aprofundamento teórico bem como suas aplicações demonstram a importância deste conceito matemático que, em diversas situações, é ignorado no Ensino Básico.

Esse estudo e sua implementação na criptografia RSA apresentam a utilização destes em nosso cotidiano. Embora muitos estudantes não conheçam a criptografia RSA, é possível associá-la à segurança da informação: transações bancárias, informações comerciais sigilosas, dados pessoais em rede e até informações governamentais.

Os Problemas do Milênio ressaltam a importância dos Números Primos e sua relação com diversas áreas do conhecimento. Por outro lado, demonstram os esforços contínuos a fim de solucioná-los bem como os impactos, destes estudos, na segurança da informação.

Por fim, esta pesquisa relaciona o prazer que a curiosidade e a busca por uma solução podem produzir não só nos brilhantes matemáticos que estudam os Números Primos e suas aplicações, mas também em estudantes do Ensino Básico. As atividades aqui propostas visam estimular estudantes a aprender através de jogos que despertem a curiosidade sobre a Matemática.

REFERÊNCIAS

ALENCAR FILHO, E. D. **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002**: Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação. [S.l.], 2013. 120 p.

BOSE, R. **Information Theory, Coding and Cryptography**. 2ª. ed. Nova Delhi (Índia): The McGraw-Hill Companies, 2008.

BOYER, C. B. **História da Matemática**. 3ª. ed. São Paulo: Blucher, 2012.

BRASIL. **LEI Nº 12.965, de 23 de abril de 2014**. [S.l.], 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

CIPRIANO, V. M. B. S. **A construção dos Números Inteiros e Racionais pelo Método da Simetrização e Aplicações**. Dissertação (Mestrado) — UFPI, Teresina, ago. 2016.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2ª. ed. Rio de Janeiro: IMPA, 2014.

CRYPTO, M. **Quadrado de Vigenère**. 2019. Wikipedia. Disponível em: <https://commons.wikimedia.org/wiki/File:Vigen%C3%A8re_square_shading.svg>. Acesso em: 20 set 2019.

DEVLIN, K. **Os Problemas do Milênio**: sete grandes enigmas matemáticos do nosso tempo. Rio de Janeiro: Editora Record, 2004.

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

FERNANDES, N. O. C. **Segurança da Informação**. Cuiabá (MT), 2013.

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FIGUEIREDO, L. M. **Iniciação à Matemática: um curso com problemas e soluções**. Rio de Janeiro: UFF/CEP-EB, 2010. v. 2.

FORNARI, A. **Polinômios Geradores de Números Primos**. Campinas, 2017.

FORTES, R. **Estrutura de Dados I - Análise de Dados**. Ouro Preto (MG), 2013.

FOUNDATION, F. S. **Figura Citale Espartano**. 2019. Wikipedia. Disponível em: <https://upload.wikimedia.org/wikipedia/commons/thumb/5/51/Skytale.png/199px-Skytale.png>. Acesso em: 29 set 2019.

GOEBEL, G. **Máquina Enigma**. 2019. Wikipedia. Disponível em: <https://commons.wikimedia.org/wiki/File:Four-rotor-enigma.jpg>. Acesso em: 30 set 2019.

GRANDO, R. C. **O Conhecimento Matemático e o Uso dos Jogos na Sala de Aula**. Dissertação (Mestrado) — Unicamp, Campinas, ago. 2000.

GROENWALD, C. L. O.; OLGIN, C. A. **Criptografia e o Currículo de Matemática no Ensino Médio**. [S.l.]: Revista de Educação Matemática, 2011.

GTA-UFRJ. **Frequência das Letras em Textos em Língua Portuguesa**. 2019. GTA-UFRJ. Disponível em: <https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html>. Acesso em: 29 set 2019.

HEFEZ, A. **Elementos de Aritmética**. Rio de Janeiro: SBM, 2005.

HEFEZ, A. **Aritmética**. 2ª. ed. Rio de Janeiro: SBM, 2016.

LIMA, R. D. C. **Criptografia RSA e a Teoria dos Números**. Dissertação (Mestrado) — UFPB, João Pessoa, ago. 2013.

MARTINS, E. R. **Fundamentos da Ciência da Computação**. Ponta Grossa (PR): Atena Editora, 2019.

OLIVEIRA, I. C. **Complexidade Computacional e o Problema P vs NP**. Campinas, 2010.

OLIVEIRA, K. I. M.; FERNÁNDEZ, A. J. C. **Iniciação à Matemática: um curso com problemas e soluções**. 2ª. ed. Rio de Janeiro: SBM, 2012.

PADRÃO, D. L. **A Origem do Zero**. Dissertação (Mestrado) — PUC/SP, São Paulo, ago. 2008.

PERIN, A. et al. **Conjectura de Goldbach**. Campinas, 2017.

PERUZZO, J. **O Fascínio dos Números Primos**. Irani (SC): Clube dos Autores, 2012.

POLYA, G. **A Arte de Resolver Problemas**. Rio de Janeiro: Editora Interciência, 1978.

SIMÕES, P. **Ilustração do Código de Segurança - Código QR**. 2019. PPLWARE. Disponível em: <https://pplware.sapo.pt/smartphones-tablets/conversas-whatsapp-seguras-dica/>. Acesso em: 28 nov 2019.

SINGH, S. **O Livro dos Códigos (The Code Book)**. 9ª. ed. Rio de Janeiro: Record, 2011.

SÊMOLA, M. **Gestão da Segurança da Informação: uma visão executiva**. Rio de Janeiro: Campus, 2003.

VIANA, M. **Primos gêmeos constituem um dos mistérios mais intrigantes da aritmética**. 2018. SBM. Disponível em: <https://www.sbm.org.br/noticias/primos-gemeos-constituem-um-dos-misterios-mais-intrigantes-da-aritmetica>. Acesso em: 27 jul 2019.