UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE CIÊNCIAS EXATAS E DA NATUREZA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

WÍRLAN CHAGAS DA SILVA

A CRIPTOGRAFIA E SEU DESENVOLVIMENTO MATEMÁTICO.

REDENÇÃO
2021

WÍRLAN CHAGAS DA SILVA

A CRIPTOGRAFIA E SEU DESENVOLVIMENTO MATEMÁTICO.

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional da Universidade da Integração Internacional da Lusofonia Afro Brasileira, como parte dos requisitos necessários para a obtenção do título de mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Joserlan Perote da Silva

REDENÇÃO

2021

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Silva, Wirlan Chagas da.

S578c

A Criptografia e seu desenvolvimento matemático / Wirlan Chagas da Silva. - Redenção, 2022.
108f: il.

Dissertação - Curso de Matemática em Rede Nacional, Mestrado Profissional em Matemática em Rede Nacional, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2022.

Orientador: Prof. Joserlan Perote da Silva.

1. Criptografia. 2. Curvas elípticas. 3. Códigos. I. Título

CE/UF/BSP CDD 510

WÍRLAN CHAGAS DA SILVA

A CRIPTOGRAFIA E SEU DESENVOLVIMENTO MATEMÁTICO

Dissertação apresentada como requisito para a obtenção do título de Mestre em Matemática, na Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Unilab – Campus Auroras.

Aprovada em: 21 / 12/ 2021.

BANCA EXAMINADORA

Joserlan Perote da Silva

Prof. Dr. Joserlan Perote da Silva (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Rafael Jorge Pontes Diógenes

Prof. Dr. Rafael Jorge Pontes Diógenes
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Prof. Dr. Diego de Sousa Rodrigues
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Dedico este trabalho a todas as pessoas que contribuíram direta ou indiretamente com a sua realização. Em especial à minha amada genitora Luzenilda, que sempre fez tudo que pôde por mim, inclusive ensinar que a educação transforma vidas.

AGRADECIMENTOS

Primeiramente a Deus, por ter me dado saúde, sabedoria e paciência durante todo o curso.

Ao Prof. Dr. Joserlan Perote da Silva, pela excelente orientação, sempre paciente e disponível.

Aos professores participantes da banca examinadora Rafael Jorge Pontes Diógenes e Diego de Sousa Rodrigues, pelo tempo e pelas valiosas colaborações e sugestões.

Aos colegas da turma Ananias, Dennis, Fábio, Felipe, Paulo, Renato, Salustriano e Silvio, que estiveram juntos em momentos de estudos, alegria, aflição e troca de experiências.

Aos professores Antonio Alisson, João Francisco, Marcelo Dário, Rodrigo Mendes, Weslley Marinho, José Robério, que juntamente com meu orientador Joserlan Perote e com o professor Rafael Diógenes, que contribuíram diretamente para minha formação.

À minha mãe Luzenilda, que sempre fez o que pôde para que eu pudesse alcançar meus objetivos.

À minha namorada Beatriz, que com sua paciência soube entender minha ausência em vários momentos.

"A matemática aplicada necessita da matemática pura tanto como os formigueiros necessitam das formigas. - Paul Halmos"

RESUMO

Este trabalho apresenta alguns tópicos de teoria dos números como os princípios da boa ordem e da indução direta, divisibilidade, máximo divisor comum, números primos, fatoração de inteiros e aritmética modular que será muito usada nos cálculos para encriptar e decriptar uma mensagem com os criptossistemas mais modernos. Além disso, pode-se encontrar algumas estruturas algébricas e uma apresentação concisa sobre curvas elípticas. O objetivo é criar um material bibliográfico para despertar interesse dos alunos da educação básica para a Matemática através de sua aplicação. Para isso, o trabalho aborda um pouco da história da utilização da criptografia ao apresentar algumas cifras utilizadas ao longo do tempo como a cifra de César, a de Vigenère e a utilização da Enigma pelos alemães durante a segunda guerra mundial. O problema do logaritmo discreto bem como o problema de fatoração de inteiros que são, respectivamente, os motivos da segurança da criptografia RSA e da criptografia por curvas elípticas também são apresentados no trabalho, bem como a matemática utilizada nelas. Alguns exemplos da utilização dos sistemas criptográficos e algoritmos de assinatura digital também são apresentados afim de integrar a Matemática à realidade por meio de sua aplicação.

Palavras-chave: Criptografia. Curvas Elípticas. Códigos.

ABSTRACT

This work presents some number theory topics such as the principles of well-ordering and induction, divisibility, greatest common divisor, prime numbers, integer factorization and modular arithmetic that will be will be used a lot in calculations to encrypt and decrypt a message with the most modern cryptosystems. In addition, one can find some algebraic structures and a concise presentation of elliptic curves. The objective is to create a bibliographic material to awaken the interest of students from basic education to Mathematics through its application. For this, the work addresses a little of the history of the use of cryptography by presenting some ciphers used over time, such as Caesar's cipher, Vigenère's and the use of Enigma by the Germans during World War II. The discrete logarithm problem as well as the integer factorization problem, which are, respectively, the reasons for the security of RSA cryptography and elliptic curve cryptography are also presented in the work, as well as the mathematics used in them. Some examples of the use of cryptographic systems and digital signature algorithms are also presented in order to integrate Mathematics into reality through its application.

Keywords: Cryptography. Elliptic curves . Codes.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BNCC	Base Nacional Comum Curricular
NBR	Norma Brasileira Regulamentar
UNILAB	Universidade da Integração Internacional da Lusofonia Afro-Brasileira

SUMÁRIO

1 INTRODUÇÃO

Recentemente pôde-se notar o aumento de anúncios de redes sociais ou instituições financeiras sobre a segurança de dados, visando sempre a credibilidade destas. Com isso, alguns questionamentos podem surgir, como por exemplo, o que é e como funciona a criptografia?

A criptografia é um assunto muito relevante e que pode despertar interesse dos alunos do ensino básico, uma vez que se fez presente em vários momentos significativos para a história mundial e se apresenta como um assunto contemporâneo. As pessoas estão utilizando cada vez mais a internet para realizar diversas tarefas, como por exemplo, uma simples compra. Porém, ninguém gostaria de que os dados de seu cartão de crédito ou de sua conta bancária fossem expostos. Vivemos diariamente uma guerra contra o vazamento de nossos dados. A forma segura que existe para manter informações sigilosas secretas, é a utilização da criptografia, que do grego significa escrita secreta.

É comum ouvirmos em sala de aula expressões do tipo "Eu nunca vou usar isso na minha vida!". Isso se deve ao fato de que muitos estudantes acreditam que a matemática não passa de uma disciplina do currículo da educação básica. Por isso, é fundamental que o professor relacione os conteúdos ministrados em sala de aula com situações do cotidiano dos alunos, dando mais sentido ao estudo realizado.

De acordo com a Base Nacional Comum Curricular (BNCC), "[...] no Ensino Médio o foco é a construção de uma visão integrada da Matemática, aplicada à realidade, em diferentes contextos."(BRASIL, 2018, p. 528)

Com o objetivo de despertar o interesse dos alunos do Ensino Médio da educação básica para a Matemática, resolvemos abordar a Criptografia como tema principal deste trabalho de caráter bibliográfico. Um assunto atual e diferente do que é visto em sala de aula, apresentando a utilização e importância da criptografia no passado, sua evolução e utilização na atualidade, onde a matemática tem uma importância significativa.

No segundo capítulo deste trabalho podemos encontrar conceitos básicos de aritmética que necessitamos para o entendimento da matemática utilizada na criptografia RSA. São eles a divisibilidade, os números primos, a fatoração de inteiros, bem como a aritmética modular, o pequeno Teorema de Fermat e o algoritmo de Euclides. Por ser um conteúdo importante para o entendimento de curvas elípticas, algumas estruturas algébricas também estão presentes no capítulo 2.

No terceiro capítulo encontra-se um pouco da história da criptografia, indo desde a Cifra de César, que é um sistema de criptografia que consistia apenas na substituição de cada uma das letras de uma mensagem por uma outra, até o sistema de troca de chaves de Diffie-Hellman, onde o problema do logaritmo discreto permite a criação de uma chave sem que as partes envolvidas se encontrem.

No quarto capítulo deste trabalho está exposto o sistema de criptografia RSA,

bem como exemplo de sua utilização e a matemática envolvida nesse sistema, que tem como base a aritmética modular, assunto não presente no ensino básico, mas que pode ser encontrado no capítulo 2 deste trabalho.

No quinto capítulo pode-se encontrar a definição de curvas elípticas e a operação da soma de pontos destas curvas. É apresentado ainda o comportamento de uma curva elíptica em um corpo $\mathbb{Z}_p$ e a utilização destas curvas para encriptar uma mensagem. Encontra-se também um algoritmo que permite mapear uma mensagem em pontos de uma curva elíptica.

Já no apêndice encontram-se exemplos de sistemas de assinaturas digitais, que são cada vez mais utilizadas, principalmente no momento atual de pandemia que vivemos, onde a não necessidade de se fazer presente fisicamente em um local para assinar um documento pode salvar vidas.

2 PRELIMINARES

Antes de iniciarmos a exposição do nosso tema, a criptografia, precisamos abordar alguns assuntos preliminares para que possamos construir argumentos matemáticos necessários para compreendermos a criptografia RSA e a criptografia por curvas elípticas. Abordaremos aqui tópicos de teoria dos números que também podem ser encontrados em Santos (2000) e Hefez (2016). Apresentaremos também, nesta seção, alguns conceitos de estruturas algébricas que necessitamos e que podem ser encontrados também em Domingues e Iezzi (2003). O leitor pode avançar para a próxima seção onde iniciamos a fala sobre a história da criptografia e retornar para esta seção quando sentir necessidade.

2.1 OS PRINCÍPIOS DA BOA ORDEM E DA INDUÇÃO FINITA.

Na matemática, algumas proposições são tomadas como verdade, independente de demonstrações, para que sirva como base lógica para muitas definições. Essas proposições são chamadas de axiomas. Um axioma que fundamenta o estudo dos números naturais é o Princípio da Boa Ordem (PBO), que nos diz que todo conjunto não vazio de números naturais contém um menor elemento.

Já o Princípio de Indução Finita (PIF), possui duas formas de ser enunciado, sendo as duas muito utilizadas para realizar demonstrações. Vejamos:

Proposição 2.1 (PIF 1ª forma) *Seja $\mathcal{A}$ um subconjunto dos naturais. Se $\mathcal{A}$ possui as propriedades 1 e 2, então $\mathcal{A}$ contém todos os naturais.*

1. $1 \in \mathcal{A}$.
2. $k+1 \in \mathcal{A}$ *quando* $k \in \mathcal{A}$.

Demonstração: Vamos supor que $\mathcal{A}$ possui as propriedades 1 e 2 mas que nem todo natural pertence a $\mathcal{A}$. Seja $\mathcal{B}$ o conjunto de naturais que não pertencem a $\mathcal{A}$. Pelo PBO, $\mathcal{B}$ possui um menor elemento e, como pela propriedade 1, $1 \in \mathcal{A}$, temos que o menor elemento de $\mathcal{B}$ é maior do que 1. Seja b o menor elemento de $\mathcal{B}$, então $b-1 \in \mathcal{A}$. Porém, $\mathcal{A}$ satisfaz à propriedade 2, então $(b-1)+1 = b$ também pertence a $\mathcal{A}$, o que é um absurdo pois $b \in \mathcal{B}$. Esta contradição nos diz que $\mathcal{B}$ é vazio, ou seja, $\mathcal{A}$ contém todos os naturais, o que conclui a demonstração. ∎

Proposição 2.2 (PIF 2ª forma) *Seja $\mathcal{A}$ um subconjunto dos naturais. Se $\mathcal{A}$ possui as propriedades 1 e 2, então $\mathcal{A}$ contém todos os naturais.*

1. $1 \in \mathcal{A}$.
2. $k+1 \in \mathcal{A}$, *quando* $1, 2, 3, ..., k \in \mathcal{A}$.

Demonstração: A demonstração é equivalente à da 1ª forma. ∎

2.2 DIVISIBILIDADE

Trataremos aqui das propriedades da divisibilidade que nos auxiliarão no entendimento da aritmética modular, que veremos mais a frente.

Definição 2.1 *Sendo a e b números inteiros, dizemos que a divide b, denotando por $a \mid b$, se existir um inteiro c tal que $b = ac$. Caso a não divida b, escrevemos $a \nmid b$.*

Proposição 2.3 *Para n inteiro, a divisão possui as seguintes propriedades:*

1. $n \mid n$ *e* $1 \mid n$.
2. $d \mid n \Rightarrow a \cdot d \mid n \cdot a$, *com* $a \in \mathbb{Z}$.
3. $a \cdot d \mid n \cdot a$ *e* $a \neq 0 \Rightarrow d \mid n$, *com* $a, d \in \mathbb{Z}$.
4. $n \mid 0$.
5. *Sendo a, b e c números inteiros, se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.
6. *Se a, b, c, i e j são números inteiros,* $c \mid a$ *e* $c \mid b$, *então* $c \mid (i \cdot a + j \cdot b)$.

Demonstração: 1: $n = 1 \cdot n$, então, por definição, $n \mid n$ e $1 \mid n$.

2: Se $d \mid n$, então existe um inteiro k tal que $n = k \cdot d$. Ao multiplicarmos ambos os membros da igualdade por a, temos que $a \cdot n = k \cdot a \cdot d$, o que implica que $a \cdot d \mid a \cdot n$.

3: Se $a \cdot d \mid a \cdot n$, então $a \cdot n = k \cdot a \cdot d$, o que implica que $a \cdot n - k \cdot a \cdot d = 0$. Logo, $a \cdot (n - k \cdot d) = 0 \Rightarrow a = 0$ ou $n - k \cdot d = 0$. Como $a \neq 0$, temos que $n - k \cdot d = 0$, então $n = k \cdot d$, o que implica que $d \mid n$.

4: $0 = 0 \cdot n$, então por definição, $n \mid 0$.

5: Se $a \mid b$ e $b \mid c$, então existem inteiros k_1 e k_2 tais que $b = a \cdot k_1$ e $c = b \cdot k_2$. Substituindo o valor de b em $c = b \cdot k_2$, temos que $c = a \cdot k_1 \cdot k_2$, logo $a \mid c$.

6: Se $c \mid a$ e $c \mid b$ então existem k_1 e k_2 inteiros tais que $a = ck_1$ e $b = ck_2$. Multiplicando $a = c \cdot k_1$ por i e $b = c \cdot k_2$ por j, temos $a \cdot i = c \cdot k_1 \cdot i$ e $b \cdot j = c \cdot k_2 \cdot j$. Somando membro a membro as duas equações, obtemos $a \cdot i + b \cdot j = c \cdot (k_1 \cdot i + k_2 \cdot j)$ o que implica que $c \mid (a \cdot i + b \cdot j)$. ∎

Teorema 2.1 (Divisão Euclidiana) *Sendo a e b dois números inteiros, com $a > 0$, existe um único par de inteiros q e r tais que $b = q \cdot a + r$, com $0 \leqslant r < a$, onde $r = 0$ implica que a divide b. Dizemos que q e r são, respectivamente, quociente e resto da divisão de b por a,*

Demonstração: Supondo que $b > a$, vamos considerar os números não negativos do tipo b, $b - a$, $b - 2 \cdot a$, ..., $b - n \cdot a$, $b - (n+1) \cdot a$, ... como todos os elementos de um conjunto $\mathcal{S}$. Pelo Princípio da Boa Ordem, o conjunto $\mathcal{S}$ possui um menor elemento $r = b - q \cdot a$.

1. Vamos provar que $r < a$:
   - Se $a \mid b$, então $r = 0$ e não precisamos provar mais nada.
   - Se $a \nmid b$, então $r \neq a$, portanto basta mostrar que não ocorre que $r > a$.
   - Se $r > a$, existiria um natural $c < r$ tal que $r = c + a$ e consequentemente teríamos $r = c + a = b - q \cdot a$, o que implicaria que $c = b - (q+1) \cdot a \in \mathcal{S}$, com $c < r$. Porém, como r é o menor elemento de $\mathcal{S}$, temos aqui uma contradição. Logo, temos que $b = a \cdot q + r$, com $r < a$, o que prova que existem tais q e r.
2. Agora vamos mostrar a unicidade de q e r:
   Dados dois elementos distintos de $\mathcal{S}$, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a, é pelo menos a. Portanto, se $r = b - a \cdot q$ e

$r' = b - a \cdot q'$, com $r < r' < a$, teríamos $r' - r = a \cdot (q - q')$ o que implica que $r' - r \geqslant a$, então $r' \geqslant r + a \geqslant a$, ou seja, um absurdo. Logo, $r = r'$. Daí temos que $b - a \cdot q = b - a \cdot q'$, o que implica que $q = q'$.

O caso em que $b < a$ pode ser demonstrado analogamente. ∎

Exemplo 2.1 *O quociente e o resto da divisão de* 23 *por* 4 *são* $q = 5$ *e* $r = 3$. *Já o quociente e o resto da divisão de* -23 *por* 4 *são* $q = -5$ *e* $r = 3$.

Definição 2.2 *O máximo divisor comum (MDC) de dois números inteiros* a *e* b, *com* a *ou* b *não negativo, é o maior inteiro que divide* a *e* b *e podemos denotá-lo por* $mdc(a, b)$.

Exemplo 2.2 *Os números* ± 1, ± 2 *e* ± 4 *são os divisores comuns de* 16 *e* 20. *Porém, o maior deles é o* 4. *Logo, podemos afirmar que o* $mdc(16, 20) = 4$.

Definição 2.3 *O mínimo múltiplo comum (MMC) de dois inteiros positivos* a *e* b, *denotado por* $mmc[a, b]$ *é o menor inteiro não negativo tal que* $a \mid mmc[a, b]$ *e* $b \mid mmc[a, b]$.

Exemplo 2.3 *Temos que o número* 20 *é um múltiplo comum de* 2 *e* 5. *Porém, não é o MMC desses números. O número* 10 *é o MMC desses números, já que é o menor número inteiro não negativo divisível por* 2 *e* 5.

Teorema 2.2 (Bachet-Bézout) *Sejam* a *e* b *dois números inteiros, existem* x *e* y *inteiros tais que* $a \cdot x + b \cdot y = mdc(a, b)$.

Demonstração: Definimos o conjunto $\mathcal{S} = \{a \cdot x + b \cdot y;\ x, y \in \mathbb{Z} \text{ e } a \cdot x + b \cdot y \geqslant 0\}$. Supondo que:

1. $a \cdot x + b \cdot y \in \mathcal{S}$
2. $a \cdot x' + b \cdot y' \in \mathcal{S}$
3. $a \cdot x + b \cdot y \geqslant a \cdot x' + b \cdot y'$

Ao subtrairmos (2) de (1), temos: $a \cdot x + b \cdot y - (a \cdot x' + b \cdot y') = a \cdot (x - x') + b \cdot (y - y') \in \mathcal{S}$. Se todos os múltiplos de a pertencem ao conjunto $\mathcal{S}$, então $\mathcal{S}$ é infinito. Sendo $d = a \cdot x + b \cdot y$ o menor elemento positivo de $\mathcal{S}$, podemos afirmar que $\mathcal{S} = \{k \cdot d; k \geqslant 0\}$. De fato, dado $m = ax_0 + by_0 \in \mathcal{S}$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leqslant r < d$. Com isso, temos que

$$r = m - dq = a(x_0 - xq) + b(y_0 - yq) \Rightarrow r \in \mathcal{S}.$$

Mas como $r < d$ e d é o menor elemento positivo de $\mathcal{S}$, temos que $r = 0$ e portanto, $d \mid m \Rightarrow \mathcal{S} = \{k \cdot d; k \geqslant 0\}$. O que implica que $mdc(a, b) \mid d$, então $mdc(a, b) \leqslant d$. Temos que todos os elementos de $\mathcal{S}$ são múltiplos de d e em particular, $a \in S$ pois $a = 1 \cdot a + 0 \cdot b \in \mathcal{S}$ e $b \in \mathcal{S}$ pois $b = a \cdot 0 + b \cdot 1 \in \mathcal{S}$, o que implica que $d \mid a$ e $d \mid b$ e, consequentemente, $d \leqslant mdc(a, b)$, logo, $d = mdc(a, b)$. ∎

Proposição 2.4 *Se* c *é um número inteiro tal que* $c \mid a$ *e* $c \mid b$, *então* $c \mid mdc(a, b)$.

Demonstração: A demonstração vem do fato de que se $d = mdc(a, b)$, então $d = a \cdot x + b \cdot y$, logo, $c \mid d$. ∎

Exemplo 2.4 *Já sabemos que* $mdc(16, 20) = 4$. *É fácil ver que* $2 \mid 16$ *e* $2 \mid 20$. *Portanto,*

pela Proposição 2.4 podemos afirmar que $2 \mid 4$*, o que é uma verdade.*

Corolário 2.1 *Sejam* a, b *e* c *números inteiros. A equação* $ax + by = c$ *admite solução inteira em* x *e* y *se, e somente se,* $mdc(a, b) \mid c$*.*

Demonstração: Se a equação admite solução inteira, então $mdc(a, b) \mid ax + by$, logo, $mdc(a, b) \mid c$. Por outro lado, se $mdc(a, b) \mid c$, então $c = k \cdot mdc(a, b)$ com k inteiro, e pelo Teorema 2.2 de Bachet-Bézout, existem x_0 e y_0 inteiros tais que $a \cdot x_0 + b \cdot y_0 = mdc(a, b)$. Ao multiplicarmos k a ambos os membros da última igualdade, temos que $x = k \cdot x_0$ e $y = k \cdot y_0$ são as soluções de $ax + by = c$. ∎

Teorema 2.3 (Lema de Gauss) *Se* $a \mid bc$ *e* $mdc(a, b) = 1$*, então* $a \mid c$*.*

Demonstração: Como $mdc(a, b) = 1$, então existem inteiros k_1 e k_2 tais que

$$k_1 \cdot a + k_2 \cdot b = 1.$$

Multiplicando ambos os membros da igualdade por c, temos

$$(k_1 \cdot a) \cdot c + (k_2 \cdot b) \cdot c = 1 \cdot c \Rightarrow k_1 \cdot (a \cdot c) + k_2 \cdot (b \cdot c) = c.$$

Como $a \mid a \cdot c$ e $a \mid b \cdot c$, então pela Proposição 2.3 item 6, temos que $a \mid c$. ∎

2.3 NÚMEROS PRIMOS

O conjunto dos números primos é um dos assuntos que mais intrigam os matemáticos devido ao fato de ainda não ter sido descoberto um padrão com que esses números aparecem. A dificuldade de fatorar um produto de primos é o que torna um dos sistemas criptográficos mais utilizados atualmente seguro.

Definição 2.4 *Um número primo é um número natural maior do que* 1 *que só é divisível por* 1 *e por si próprio.*

Proposição 2.5 *Sendo* p *e* q *números primos, temos que:*

1. *Se* $p \mid q$*, então* $p = q$*.*
2. *Se* $p \nmid q$*, então* $mdc(p, q) = 1$*.*

Demonstração: 1: Se q é primo e $p \mid q$, logo, por definição, $p = 1$ ou $p = q$ e como p também é primo, por definição, $p \neq 1$. Portanto, $p = q$.

2: Se $mdc(p, q) = d$, então $d \mid p$ e $d \mid q$, logo, $d = p$ ou $d = 1$. Porém, $d \neq p$ pois $p \nmid a$, logo $d = 1$. ∎

Observação 2.1 No caso em que $mdc(a, b) = 1$ dizemos que a e b são primos entre si ou relativamente primos, mesmo que a e b não sejam primos.

Proposição 2.6 (Lema de Euclides) *Seja* p *um número primo,* a *e* b *dois números naturais. Se* $p \mid a \cdot b$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração: Se p não divide a, como p é primo, então $mdc(p, a) = 1$. Pelo Teorema 2.3 temos que neste caso $p \mid b$. Analogamente, se $p \nmid b$, então $mdc(p, b) = 1$ o que implica

que $p \mid a$. ∎

Corolário 2.2 *Se $p, p_1, \ldots, p_n$ são números primos e $p \mid p_1 \ldots p_n$, então $p = p_i$, para algum $i = 1, 2, \ldots, n$.*

Demonstração: Faremos a demonstração utilizando o Princípio de Indução Finita sobre n.

- Para $n = 1$, temos que se $p \mid p_1$, pela Proposição 2.5 temos que $p = p_1$.
- Supondo que se $p \mid p_1 \ldots p_n$ então $p = p_i$ para algum $i = 1, ..., n$ e devemos mostrar que se $p \mid p_1 \ldots p_n \cdot p_{(n+1)}$ então $p = p_i$ para algum $i = 1, ..., n, n+1$. Sendo $q = p_1 \ldots p_n$, temos que pela hipótese de indução $p \mid q$ e $p = p_i$. Se $p \mid p_1 \ldots p_n \cdot p_{(n+1)}$ então $p \mid q \cdot p_{(n+1)}$, e pela Proposição 2.6, $p \mid q$ ou $p \mid p_{(n+1)}$ e, como sabemos que $p \mid q$, temos que: Se $p \mid q$, então $p = p_i$ para algum $i = 1, ..., n$. Se $p \mid p_{(n+1)}$, então $p = p_i$, para $i = n + 1$, o que conclui nossa demonstração por indução.

∎

Teorema 2.4 (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: Sendo $\mathcal{S}$ o conjunto de elementos maiores do que 1 que não podem ser representados como produto de fatores primos, temos que como $\mathcal{S}$ é subconjunto dos inteiros, então $\mathcal{S}$ possui um menor elemento. Seja a o menor elemento de $\mathcal{S}$, então $a \neq 2$, pois 2 é primo e possui fatoração em fatores primos. Além disso, $a = r.s$, com $r < a$ e $s < a$, r e s inteiros e não pertencentes a $\mathcal{S}$, já que a é o menor elemento de $\mathcal{S}$. Porém, como r e s não pertencem a $\mathcal{S}$, então tanto r como s podem ser representados como produto de primos, portanto, $a = r.s$ também pode ser representado como produto de primos, o que é um absurdo, já que $a \in \mathcal{S}$. Logo, $\mathcal{S}$ não possui menor elemento, portanto $\mathcal{S}$ é vazio, o que mostra que nenhum inteiro maior do que 1 não pode ser representado como produto de primos. Seja $a = p_1 \cdot p_2 \ldots p_n$ e $a = q_1 \cdot q_2 \ldots q_m$, temos que $p_1 \ldots p_n$ e $q_1 \ldots q_m$ são duas fatorações de a onde todos os p_i's e q_j's são primos e não necessariamente distintos. Como $p_1 \cdot p_2 \ldots p_n = q_1 \cdot q_2 \ldots q_m$ pela definição da divisibilidade $p_1 \mid q_1 \cdot q_2 \ldots q_m$ e pelo Corolário 2.2 , $p_1 \mid q_1 \ldots q_m \Rightarrow p_1 = q_j$ para algum j que, após reordenar $q_1, \ldots, q_m$, podemos supor que seja q_1. Logo, $p_2 \ldots p_n = q_2 \ldots q_m$. Portanto, para qualquer $i < n$, existe $j < m$ tal que $p_i \mid q_j \Rightarrow p_i = q_j$. Agora, basta provarmos que $m = n$, o que é trivial, já que se $m > n$, teríamos $q_1 \ldots q_n \ldots q_m = p_1 \cdot p_2 \ldots p_n = q_1 \cdot q_2 \ldots q_n$, o que é absurdo, já que $q > 1$. Ou seja, $m = n$ e os p_i's e q_j's são iguais aos pares. ∎

Teorema 2.5 *Existem infinitos números primos.*

Demonstração: Supondo que existe um número finito de números primos $p_1, p_2, \ldots, p_r$. Considerando o número natural n como $n = p_1 \cdot p_2 \ldots p_r + 1$. Pelo Teorema 2.4, existe um fator p_i de n que divide n, ou seja, $p_i \mid p_1 \cdot p_2 \ldots p_r + 1$, o que é um absurdo, pois p_i dividiria 1. Logo, existe um número infinito de números primos. ∎

2.4 FATORAÇÃO DE INTEIROS

Apresentaremos aqui um algoritmo denominado por "Achar fator" em Coutinho (2016), que encontra um fator primo p de um número inteiro n.

O algoritmo é bem simples. Primeiramente verificamos se $2 \mid n$, que é o menor número primo. Se $2 \mid n$, então $p = 2$. Se $2 \nmid n$, verificamos se $3 \mid n$. Se sim, $p = 3$. Se não, verificamos se $4 \mid n$, e assim sucessivamente, verificando se n é divisível por cada inteiro subsequente. Se ao fazer essa verificação, chegarmos a verificar se um inteiro q divide n e tal q é maior do que $\sqrt{n}$, podemos concluir que n é primo.

Como o algoritmo consiste na busca de um fator de um número n, começando por 2, temos que o fator encontrado é sempre o menor fator p do primo n, pois se p não for primo, então existe um fator $a < p$. Porém, como $a \mid p$ e $p \mid n$, então pela Proposição 2.3 item 5, temos que $a \mid n$, o que não é possível, já que p é o menor fator de n.

Devido ao fato deste algoritmo achar sempre o menor fator do número n, podemos decretar que n é primo (se o for) muito antes de chegar a n. Por exemplo, supondo que n seja composto, podemos escrever $n = p \cdot c,\ c \in \mathbb{Z}$. Com isso, podemos afirmar que $c \mid n$, e como p é o menor fator de n, podemos afirmar que $p \leqslant c$. Logo,

$$n = p \cdot c \geqslant p \cdot p \Rightarrow n \geqslant p^2 \Rightarrow p \leqslant \sqrt{n}.$$

Portanto, ao chegarmos a um número maior que $\sqrt{n}$, podemos concluir que n é primo.

Exemplo 2.5 *Vamos verificar se o número* 31 *é primo: Como* $5 < \sqrt{31} < 6$, *vamos verificar* 31 *é divisível por* 2, 3, 4, 5 *e* 6. *Temos que*

$$\begin{aligned} 31 &= 15 \cdot 2 + 1 \Rightarrow 2 \nmid 31; \\ 31 &= 10 \cdot 3 + 1 \Rightarrow 3 \nmid 31; \\ 31 &= 7 \cdot 4 + 3 \Rightarrow 4 \nmid 31; \\ 31 &= 6 \cdot 5 + 1 \Rightarrow 5 \nmid 31; \\ 31 &= 5 \cdot 6 + 1 \Rightarrow 6 \nmid 31. \end{aligned}$$

Como 31 *não é divisível por nenhum inteiro até* $\sqrt{31}$, *então podemos concluir que* 31 *é primo.*

Exemplo 2.6 *Encontre um fator de* 91.

Solução:

$$\begin{aligned} 91 &= 45 \cdot 2 + 1 \Rightarrow 2 \nmid 91; \\ 91 &= 30 \cdot 3 + 1 \Rightarrow 3 \nmid 91; \\ 91 &= 22 \cdot 4 + 3 \Rightarrow 4 \nmid 91; \\ 91 &= 18 \cdot 5 + 1 \Rightarrow 5 \nmid 91; \end{aligned}$$

$$\begin{aligned} 91 &= 15 \cdot 6 + 1 \Rightarrow 6 \nmid 91; \\ 91 &= 13 \cdot 7 \Rightarrow 7 \mid 91. \end{aligned}$$

Portanto, temos que 7 é um fator de 91. Mais que isso, 7 é o menor fator de 91. ∎

Um outro método para a fatoração de inteiros é o algoritmo de Fermat, que pode ser encontrado em Clube de matemática da OBMEP (2010).

2.5 ARITMÉTICA MODULAR

Assim como em Sautoy (2007), iniciamos fazendo uma analogia da aritmética modular com a aritmética do relógio, onde consideramos um grupo finito de números dispostos num círculo, como em um relógio de parede. Por exemplo, em um relógio comum são mostradas 12 casas, numeradas de 1 a 12. Para calcularmos $7+8$, nós iniciamos no 7 e avançamos 8 casas, então alcançaremos a casa de número 3, o que é diferente do resultado obtido fazendo esse cálculo utilizando a aritmética usual, cujo resultado seria 15. Essa operação do relógio pode ser descrita como $7+8 \equiv 3 \mod 12$. O que fizemos foi observar o resto da soma de $7+8$ após a divisão por 12. Gauss percebeu que podemos utilizar relógios não convencionais, por exemplo, se usássemos um relógio de 10 horas, teríamos a seguinte operação: $7+8 \equiv 5 \mod 10$.

Ao desapegarmos da analogia do relógio, definimos congruência da seguinte forma:

Definição 2.5 *Dados dois inteiros a e b, dizemos que a é congruente a b módulo m quando $m > 0$ e $m \mid a-b$. Podemos denotar isto por $a \equiv b \mod m$. Do contrário, caso $m \nmid a-b$, podemos dizer que a é não congruente ou incongruente a b módulo m e podemos denotar isto por $a \not\equiv b \mod m$.*

Exemplo 2.7 *Como $5 \mid 10$ e $10 = 12-2$, então $12 \equiv 2 \mod 5$. Como $6 \nmid 10$, então $12 \not\equiv 2 \mod 6$.*

Proposição 2.7 *Dados a e b números inteiros, $a \equiv b \mod m$ se, e somente se, existir um inteiro k tal que $a = k \cdot m + b$.*

Demonstração: Se $a \equiv b \mod m$, então $m \mid a-b$, e portanto existe um inteiro k, tal que $a-b = k \cdot m$, ou seja, $a = k \cdot m + b$. Por outro lado, se $a = k \cdot m + b$, então $a-b = k \cdot m$, o que nos diz que $m \mid a-b$, o que implica que $a \equiv b \mod m$. ∎

Exemplo 2.8 *No caso em que $12 \equiv 2 \mod 5$, tal k é o número 2, pois $12 = 2 \cdot 5 + 2$.*

Proposição 2.8 *Se a, b, c e m são números inteiros, com $m > 0$, as sentenças a seguir são verdadeiras:*

1. *$a \equiv a \mod m$;*
2. *Se $a \equiv b \mod m$, então $b \equiv a \mod m$;*
3. *Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$.*

Demonstração: 1. Dado que $m \mid 0$, então $m \mid a-a$, portanto $a \equiv a \mod m$.

2. Se $a \equiv b \mod m$, então $a = t \cdot m + b$ para t inteiro. Logo, $b = a - t \cdot m$, que pela Proposição 2.7 implica que $b \equiv a \mod m$.
3. Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então existem k_1 e k_2 inteiros tais que $a = k_1 \cdot m + b$ e $b = k_2 \cdot m + c$, o que implica que $a - b = k_1 \cdot m$ e $b - c = k_2 \cdot m$. Ao somarmos membro a membro as duas últimas equações, temos: $(a - b) + (b - c) = k_1 \cdot m + k_2 \cdot m$, ou seja, $a - c = (k_1 + k_2) \cdot m$, o que implica que $a = (k_1 + k_2) \cdot m + c$ e consequentemente que $a \equiv c \mod m$. O que conclui nossa demonstração. ∎

Exemplo 2.9 *Como* $12 \equiv 2 \mod 5$, *então podemos afirmar que* $2 \equiv 12 \mod 5$.

Exemplo 2.10 *Temos que* $12 \equiv 2 \mod 5$ *e que* $17 \equiv 2 \mod 5 \Rightarrow 2 \equiv 17 \mod 5$. *Com isso, podemos afirmar que* $12 \equiv 17 \mod 5$.

Proposição 2.9 *Sejam* a, b, c *e* m *números inteiros tais que* $a \equiv b \mod m$, *então:*

1. $a + c \equiv b + c \mod m$;
2. $a \cdot c \equiv b \cdot c \mod m$.

Demonstração: 1. Como $a \equiv b \mod m$, temos que $a - b = k \cdot m$. Adicionando c a ambos os membros da igualdade, temos que $a + c - b = k \cdot m + c$, o que implica que $a + c = k \cdot m + b + c$. Logo, $a + c \equiv b + c \mod m$.
2. Como $a \equiv b \mod m$, temos que $a - b = k \cdot m$. Ao multiplicarmos ambos os membros da igualdade por c, temos que $a \cdot c - b \cdot c = k \cdot m \cdot c$, o que implica que $a \cdot c = k \cdot m \cdot c + b \cdot c$. Logo, $a \cdot c \equiv b \cdot c \mod m$. ∎

Exemplo 2.11 *Como* $12 \equiv 2 \mod 5$, *então* $12 + 1 \equiv 2 + 1 \mod 5 \Rightarrow 13 \equiv 3 \mod 5$. *Além disso, podemos afirmar que* $12 \cdot (-1) \equiv 2 \cdot (-1) \mod 5 \Rightarrow -12 \equiv -2 \mod 5$.

Proposição 2.10 *Se* a, b, c, d *e* m *são números inteiros, com* $m > 1$, *temos que:*

1. *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $a + c \equiv b + d \mod m$;
2. *Se* $a \equiv b \mod m$ *e* $c \equiv d \mod m$, *então* $a \cdot c \equiv b \cdot d \mod m$.

Demonstração: Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então existem k_1 e k_2 inteiros tais que

$$a = k_1 \cdot m + b \tag{1}$$

e

$$c = k_2 \cdot m + d. \tag{2}$$

1. Ao somarmos as equações (1) e (2) membro a membro, temos que

$$a + c = m \cdot (k_1 + k_2) + (b + d),$$

o que implica que

$$a + c \equiv b + d \mod m.$$

2. Ao multiplicarmos as equações (1) e (2) membro a membro, temos que

$$a \cdot c = k_1 \cdot k_2 \cdot m \cdot m + k_1 \cdot m \cdot d + b \cdot k_2 \cdot m + b \cdot d = m \cdot (k_1 \cdot k_2 \cdot m + k_1 \cdot d + k_2 \cdot b) + b \cdot d.$$

Logo,

$$a \cdot c \equiv b \cdot d \mod m,$$

concluindo assim nossa demonstração. ∎

Exemplo 2.12 *O fato de que* $12 \equiv 2 \mod 5$ *e* $13 \equiv 3 \mod 5$ *implica que*

$$\begin{cases} 12 + 13 \equiv 2 + 3 \mod 5 \\ 12 \cdot 13 \equiv 2 \cdot 3 \mod 5 \end{cases} \Rightarrow \begin{cases} 25 \equiv 5 \mod 5 \\ 156 \equiv 6 \mod 5 \end{cases} \Rightarrow \begin{cases} 25 \equiv 0 \mod 5 \\ 156 \equiv 1 \mod 5. \end{cases}$$

Corolário 2.3 *Sendo* a *e* b *dois números inteiros e* n *um natural, temos que*

$$a \equiv b \mod m \Rightarrow a^n \equiv b^n \mod m.$$

Demonstração: Faremos a demonstração utilizando o Princípio de Indução Finita sobre n.

- Para $n = 1$, temos que a afirmação é verdadeira pois $a^1 = a$ e $b^1 = b$.
- Supondo verdade que se $a \equiv b \mod m$, então $a^n \equiv b^n \mod m$, devemos mostrar que a afirmação é válida para $n + 1$.
  Ora, se $a \equiv b \mod m$ e $a^n \equiv b^n \mod m$, então pela Proposição 2.10 item 2, temos que $a \cdot a^n \equiv b \cdot b^n \mod m$, o que implica que $a^{(n+1)} \equiv b^{(n+1)} \mod m$.
  Como a afirmação é válida também para $n+1$, concluímos aqui nossa demonstração por indução finita.

∎

Exemplo 2.13 *Desde que* $12 \equiv 2 \mod 5$, *temos que*

$$12^3 \equiv 2^3 \mod 5 \Rightarrow 1728 \equiv 8 \equiv 3 \mod 5.$$

Proposição 2.11 *Dados* a, b, c *e* m *números naturais, com* $c \neq 0$ *e* $m > 1$, *temos que* $a \cdot c \equiv b \cdot c \mod m \Leftrightarrow a \equiv b \mod \dfrac{m}{mdc(c,m)}$.

Demonstração: Supondo, sem perda de generalidade que $b \cdot c \geqslant a \cdot c$. Como $\dfrac{m}{mdc(c,m)}$ e $\dfrac{c}{mdc(c,m)}$ são primos entre si, temos que

$$a \cdot c \equiv b \cdot c \mod m \Leftrightarrow m \mid (b-a) \cdot c \Leftrightarrow \frac{m}{mdc(c,m)} \mid (b-a) \cdot \frac{c}{mdc(c,m)} \Leftrightarrow$$

$$\Leftrightarrow \frac{m}{mdc(c,m)} \mid (b-a) \Leftrightarrow a \equiv b \mod \frac{m}{mdc(c,m)}.$$

Concluindo aqui nossa demonstração. ∎

Exemplo 2.14 *Como* $32 = 16 \cdot 2$ *e* $2 = 1 \cdot 2$, *temos que*

$$32 \equiv 2 \mod 6 \Leftrightarrow 16 \cdot 2 \equiv 1 \cdot 2 \mod 6 \Leftrightarrow 16 \equiv 1 \mod \frac{6}{2} \Leftrightarrow 16 \equiv 1 \mod 3.$$

Corolário 2.4 *Dados* a, b, c *e* m *números naturais, com* $m > 1$ *e* $mdc(c, m) = 1$, *tem-se que* $a \cdot c \equiv b \cdot c \mod m \Leftrightarrow a \equiv b \mod m$.

Demonstração: Segue imediatamente da Proposição 2.11. ∎

Exemplo 2.15

$$20 \equiv 2 \mod 3 \Leftrightarrow 10 \cdot 2 \equiv 1 \cdot 2 \mod 3 \Leftrightarrow 10 \equiv 1 \mod 3.$$

Proposição 2.12 *Sejam,* $a, b \in \mathbb{Z}$ *e* $m, n, m_1, \ldots, m_r$ *inteiros maiores do que* 1. *Temos que:*

1. *Se* $a \equiv b \mod m$ *e* $n \mid m$, *então* $a \equiv b \mod n$;
2. *Se* $a \equiv b \mod m_i$, *para todo* $i = 1, 2, \ldots, r \Leftrightarrow a \equiv b \mod mmc[m_1, \ldots, m_r]$.

Demonstração: 1. Como $a \equiv b \mod m$, temos que $m \mid b - a$. Além disso, como $n \mid m$, temos que $n \mid b - a$. Logo, $a \equiv b \mod n$.

2. Se $a \equiv b \mod m_i$, $i = 1, \ldots, r$, então $m_i \mid b - a$, para todo i. Sendo $b - a$ um múltiplo de cada m_i, temos que $mmc[m_1, \ldots, m_r] \mid b - a$. Logo, $a \equiv b \mod mmc[m_1, \ldots, m_r]$. Por outro lado, se $a \equiv b \mod mmc[m_1, \ldots, m_r]$, então $mmc[m_1, \ldots, m_r] \mid b - a$. Além disso, $m_i \mid mmc[m_1, \ldots, m_r]$, portanto, $m_i \mid b - a$. Logo, $a \equiv b \mod m_i$. ∎

Exemplo 2.16 *Como* $15 \equiv 3 \mod 4$ *e* $15 \equiv 3 \mod 2$, *então* $15 \equiv 3 \mod 2$ *pois* $2 \mid 4$.

Exemplo 2.17 *Temos que* $16 \equiv 1 \mod 5$ *e que* $16 \equiv 1 \mod 3$. *Portanto,*

$$16 \equiv 1 \mod mmc[5, 3] \Rightarrow 16 \equiv 1 \mod 15.$$

Proposição 2.13 *Sejam* a, b, c *e* m *números inteiros, com* $m > 1$. *Temos que*

$$a + c \equiv b + c \mod m \Leftrightarrow a \equiv b \mod m.$$

Demonstração: Se $a \equiv b \mod m$, pela Proposição 2.9 temos que $a + c \equiv b + c \mod m$. Se $a + c \equiv b + c \mod m$, então $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$, ou seja, $a \equiv b \mod m$. ∎

Exemplo 2.18

$$22 \equiv 5 \mod 17 \Leftrightarrow 19 + 3 \equiv 2 + 3 \mod 17 \Leftrightarrow 19 \equiv 2 \mod 17.$$

Proposição 2.14 *Se* a, b, k *e* m *são inteiros, com* $k > 0$ *e* $a \equiv b \mod m$, *então*

$$a^k \equiv b^k \mod m.$$

Demonstração: Segue imediatamente da identidade

$$a^k - b^k = (a-b)\cdot[a^{(k-1)} + a^{(k-2)}\cdot b + a^{(k-3)}\cdot b^2 + \ldots + a\cdot b^{(k-2)} + b^{(k-1)}].$$

■

Proposição 2.15 *Sejam a e m números naturais, com $m > 1$. Existe b_0 inteiro com $a \cdot b_0 \equiv 1 \mod m$ se, e somente se, $mdc(a,m) = 1$. Além disso, x é uma solução da congruência se, e somente se, $x \equiv b_0 \mod m$.*

Demonstração: A congruência possui uma solução b_0 se, e somente se, $m \mid a\cdot b_0 - 1$, ou seja, a equação $a\cdot x - m\cdot y = 1$ possui solução inteira. De acordo com o Corolário 2.1 do Teorema 2.2, isto ocorre se, e somente se, $mdc(a,m) = 1$.

Por outro lado, se b_0 e x são soluções de $a\cdot b \equiv 1 \mod m$, então $a\cdot x \equiv a\cdot b_0 \mod m$, o que implica que $x \equiv b_0 \mod m$. Temos ainda que, como b_0 é solução de $a\cdot b \equiv 1 \mod m$ e $x \equiv b_0 \mod m$, então x também é solução de $ab \equiv 1 \mod m$, pois temos que

$$a\cdot x \equiv a\cdot b_0 \equiv 1 \mod m.$$

■

Exemplo 2.19 *A congruência $4\cdot b \equiv 1 \mod 2$ não possui solução já que $mdc(4,2) = 2$.*

Definição 2.6 *Dizemos que a é invertível módulo m quando $mdc(a,m) = 1$. Além disso, chamamos b de inverso multiplicativo de a módulo m em $a\cdot b \equiv 1 \mod m$.*

Observação 2.2 Uma solução de $a\cdot b \equiv 1 \mod m$ determina e é determinada por qualquer outra solução de $a\cdot b \equiv 1 \mod m$ e o inverso é sempre único módulo m se $a\cdot b \equiv a\cdot b' \equiv 1 \mod m$ onde temos $b \equiv b\cdot 1 \equiv b\cdot a\cdot b' \equiv b\cdot a\cdot b' \equiv 1\cdot b' \equiv b' \mod m$.

Exemplo 2.20 *Como $6 = 2\cdot 3 \equiv 1 \mod 5$, temos que 2 é o inverso multiplicativo de 3 módulo 5.*

Definição 2.7 *A função de Euler é denotada por $\varphi(n)$, onde $\varphi(n)$ é o número de inteiros k tais que $k \leqslant n$ e $mdc(k,n) = 1$.*

Exemplo 2.21 *$\varphi(1) = \varphi(2) = 1$ e, para todo p primo, temos que $\varphi(p) = p - 1$.*

Definição 2.8 *Um sistema de resíduos módulo m é um conjunto de $\varphi(m)$ inteiros r_1, r_2, $\ldots$, $r_{\varphi(m)}$ tais que $mdc(r_i,m) = 1$, para $i = 1,2,3,\ldots,\varphi(m)$ e se $i \neq j$, então r_i é incongruente a r_j módulo m.*

Definição 2.9 *Um sistema completo de resíduos módulo m é todo conjunto de inteiros tais que os restos pela divisão por m são os números $0,1,2,\ldots,m$–1.*

Exemplo 2.22 *O conjunto $\mathcal{A} = \{0,1,2,3,4,5\}$ é um sistema completo de resíduos módulo 6, e $\mathcal{B} = \{1,5\}$ é um sistema reduzido de resíduos módulo 6.*

Proposição 2.16 *Sejam m e n números naturais tais que $mdc(m,n) = 1$. Então*

$$\varphi(m\cdot n) = \varphi(m)\cdot\varphi(n).$$

Demonstração: Vamos considerar os inteiros $1, 2, 3, \ldots, m, n$, onde $mdc(m, n) = 1$ e $1 \leqslant r < n$ dispostos na tabela abaixo:

Tabela 1 – Resíduos

$1,$	$2,$	...	$r,$	...	n
$1+n,$	$2+n,$	...	$r+n,$	...	$2 \cdot n$
$1+2 \cdot n,$	$2+2 \cdot n,$	...	$r+2 \cdot n,$	...	$3n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$1+(m-1) \cdot n,$	$2+(m-1) \cdot n,$	...	$r+(m-1) \cdot n,$	...	$m \cdot n$

Fonte: Proprio Autor

Note que cada coluna é um sistema completo de resíduos módulo m. Note também que os elementos da primeira coluna deixam resto 1 na divisão por n, os elementos da segunda coluna deixam resto 2 na divisão por n, os elementos da terceira coluna deixam resto 3 na divisão por n e assim segue até a coluna n-ésima onde os elementos deixam resto 0 na divisão por n. Como $mdc(m, n) = 1$, para que um número da tabela seja relativamente primo com $m \cdot n$, basta que seja relativamente primo com m e com n. Portanto, podemos eliminar todos os números de toda coluna cujos elementos não sejam relativamente primos com n, ou seja, restam apenas $\varphi(n)$ colunas. Eliminando de cada coluna restante os elementos que não são relativamente primos com m, nos restam $\varphi(m)$ números em cada uma das $\varphi(n)$ colunas que haviam restado anteriormente. Portanto, restaram $\varphi(m) \cdot \varphi(n)$ números relativamente primos com n e m simultaneamente, e como $mdc(m, n) = 1$, concluímos que $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$. ∎

Segundo Hefez (2016, p.217), no século I o matemático chinês Sun-Tsu propôs o seguinte problema: "Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7?" O Teorema a seguir nos ajuda a resolver o problema de Sun-Tsu sem que precisemos "testar" valores:

Teorema 2.6 (Teorema Chinês dos Restos) *O sistema*

$$\begin{cases} X \equiv c_1 \mod n_1 \\ X \equiv c_2 \mod n_2 \\ \qquad \vdots \\ X \equiv c_r \mod n_r \end{cases} \tag{3}$$

onde $mdc(n_i, n_j) = 1$ para todo par n_i, n_j com $i \neq j$, possui uma única solução módulo N, onde $N = n_1 n_2 \ldots n_r$. Tal solução é obtida pela expressão

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + \ldots + N_r y_r c_r,$$

onde $N_i = \dfrac{N}{n_i}$, e y_i é solução de $N_i Y \equiv 1 \mod n_i$, $i = 1, 2, \ldots, r$.

Demonstração: Inicialmente, mostraremos que x é solução do sistema (3):

De fato, como $n_i \mid N_j$, se $i \neq j$, e $N_i y_i \equiv 1 \mod n_i$, segue-se que

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + \ldots + N_r y_r c_r \equiv N_i y_i c_i \equiv c_i \mod n_i.$$

Agora, mostraremos a unicidade:
Se x' é solução de (3), então

$$x \equiv x' \mod n_i, \text{ para todo } i,\ i = 1, 2, \ldots, r.$$

Como $mdc(n_i, n_j) = 1$, para $i \neq j$, segue-se que $mmc[n_1, n_2, \ldots, n_r] = n_1 n_2 \ldots n_r = N$ e pela Proposição 2.12 item 2, temos que $x \equiv x' \mod N$. ∎

No exemplo a seguir reapresentaremos o problema de Sun-Tsu em linguagem matemática:

Exemplo 2.23 *Encontre as soluções para o sistema de congruências a seguir:*

$$\begin{cases} X \equiv 2 \mod 3; \\ X \equiv 3 \mod 5; \\ X \equiv 2 \mod 7. \end{cases} \tag{4}$$

Solução: Utilizando o Teorema Chinês dos Restos para resolver o sistema (4), temos que $c_1 = 2$, $c_2 = 3$, $c_3 = 2$, $n_1 = 3$, $n_2 = 5$ e $n_3 = 7$. Com isso, podemos calcular os valores dos N_i's e posteriormente dos y_i's. Calculando os N_i's:

$$N_1 = \frac{N}{n_1} = \frac{105}{3} = 35;$$

$$N_2 = \frac{N}{n_2} = \frac{105}{5} = 21;$$

$$N_3 = \frac{N}{n_3} = \frac{105}{7} = 15.$$

Agora vamos calcular os y_i's que são as soluções das congruências do tipo $N_i Y \equiv 1 \mod n_i$.

Como $35 \cdot 2 = 70 \equiv 1 \mod 3$, $21 \cdot 1 = 21 \equiv 1 \mod 5$ e $15 \cdot 1 = 15 \equiv 1 \mod 7$, então os valores de y_1, y_2 e y_3 são, respectivamente, 2, 1 e 1. Com isso temos condições de calcular a solução do sistema:

$$\begin{array}{rcccccc} x & = & N_1 y_1 c_1 & + & N_2 y_2 c_2 & + & N_3 y_3 c_3 \\ x & = & 35 \cdot 2 \cdot 2 & + & 21 \cdot 1 \cdot 3 & + & 15 \cdot 1 \cdot 2 \\ x & = & 140 & + & 63 & + & 30 \\ x & = & 233 & & & & \end{array}$$

Como $233 = 105 \cdot 2 + 23$, temos que $233 \equiv 23 \mod 105$. Logo, $x = 23$.

■

Observação 2.3 Apesar de 23 ser a solução única do sistema (4), o problema de Sun-Tsu admite outras soluções, são elas todos os inteiros da forma $105 \cdot t + 23$ com t também inteiro.

2.6 PEQUENO TEOREMA DE FERMAT

Antes mesmo que Gauss expusesse o conceito de aritmética do relógio, Fermat fez uma descoberta fundamental que é conhecida como o Pequeno Teorema de Fermat, que se trata de um relógio com um número p de horas onde p é primo. Fermat percebeu que ao elevarmos um número à potência p, sempre obteremos o número inicial. Por exemplo, em um relógio com 7 horas, ao elevarmos o número 2 à sétima potência, obteremos o número 128, que é o mesmo que $18 \cdot 7 + 2$, ou seja, $2^7 \equiv 2 \mod 7$. Fermat testou o comportamento das potências e percebeu que toda vez que multiplicava um determinado número por ele mesmo uma quantidade p de vezes, o ponteiro do relógio voltava para a posição inicial e esse padrão se repetia. A descoberta de Fermat expressa na aritmética modular fica da seguinte forma: $x^p \equiv x \mod p$, onde p é primo e x é inteiro.

Fermat queria uma prova de que sua descoberta era válida para qualquer número primo, então escreveu uma carta para um amigo no ano de 1640 declarando ter encontrado uma prova, porém, a prova seria muito longa para ser descrita em um curto espaço e o mundo não conheceu uma prova do PTF feita por Fermat. Quase um século depois, em 1736, Euler apresentou uma prova do PTF e descobriu que o ponteiro dos relógios com um número primo p de horas retornava ao ponto inicial depois que a hora era multiplicada por si mesma um número p de vezes e, além disso, generalizou o trabalho de Fermat, para relógios com n horas, em que $n = p.q$, com p e q primos, onde disse que o mesmo padrão se repetiria após $(p-1) \cdot (q-1) + 1$ etapas. Daí segue o seguinte teorema:

Teorema 2.7 *Seja m um inteiro livre de quadrados (que não possui como fator um quadrado perfeito), então para todo a inteiro e todo n natural tem-se que $a^{(n \cdot \varphi(m)+1)} \equiv a \mod m$.*

Demonstração: Seja $m = p_1 \cdot p_2 \ldots p_r$, onde $p_1, \ldots, p_r$ são primos distintos. Como

$$\varphi(m) = \varphi(p_1) \ldots \varphi(p_r) = (p_1 - 1) \ldots (p_r - 1),$$

sendo

$$n_i = n \cdot (p_1 - 1) \ldots (p_{(i-1)} - 1) \cdot (p_{(i+1)} - 1) \ldots (p_r - 1),$$

temos que

$$a^{(n \cdot \varphi(m)+1)} = a^{(n_i \cdot (p_i - 1)+1)} \equiv a \mod p_i,$$

pois $mmc[p_1, \ldots, p_r] = p_1 \ldots p_r = m$, o que faz com que a Proposição 2.12 item 2 garanta

o resultado. ∎

Nos dias atuais, o Pequeno Teorema de Fermat é enunciado da seguinte forma:

Teorema 2.8 *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \mod p$.*

Demonstração: Ao realizar o desenvolvimento binomial, temos que

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} \cdot a^{p-k} \cdot 1^k = \sum_{k=0}^{p} \frac{p!}{k! \cdot (p-k)!} \cdot a^{(p-k)} = a^p + p \cdot a^{p-1} + p \cdot \frac{p-1}{2} \cdot a^{p-2} + \ldots + p \cdot a + 1.$$

Portanto,

$$(a+1)^p \equiv a^p + 1 \mod p. \tag{5}$$

Podemos observar também que $\binom{p}{k} \equiv 0 \mod p$, para $0 < k < p$. Subtraindo $(a+1)$ de ambos os membros da congruência 5, temos:

$$(a+1)^p - (a+1) \equiv a^p + 1 - (a+1) \mod p$$

o que implica que

$$(a+1)^p - (a+1) \equiv a^p - a \mod p. \tag{6}$$

Agora, usaremos o Princípio da Indução Finita para concluir a demonstração:

- Verificamos que para $a = 1$, temos que $a^p - a$ é divisível por p já que $1^p - 1 = 0$ e $p \mid 0$.

- Suponhamos agora que $p \mid a^p - a$, devemos mostrar que $p \mid (a+1)^p - (a+1)$. Utilizando a congruência 6, temos que

  $$a^p - a \equiv (a+1)^p - (a+1).$$

  Logo, se $p \mid a^p - a$, então $p \mid (a+1)^p - (a+1)$, o que conclui nossa demonstração por indução de que $a^p \equiv a \mod p$.

∎

Corolário 2.5 *Seja p primo, se $p \nmid a$, então $a^{(p-1)} \equiv 1 \mod p$.*

Demonstração: Basta utilizarmos o Corolário 2.4 no Teorema 2.8:
Seja $mdc(a, p) = 1$, então

$$a^p \equiv a \mod p \Leftrightarrow a^{(p-1)} \cdot a \equiv a \cdot 1 \mod p \Leftrightarrow a^{(p-1)} \equiv 1 \mod p.$$

∎

Para consultar outras demonstrações, veja Oliveira (2019).

Exemplo 2.24 *Por conta do Pequeno Teorema de Fermat podemos afirmar que*

$$167^{96} \equiv 1 \mod 97$$

sem precisar fazer cálculo algum.

2.7 ALGORITMO DE EUCLIDES ESTENDIDO

O algoritmo que apresentaremos a seguir é um método simples de encontrar o MDC de dois naturais.

O Lema a seguir foi usado por Euclides para provar a existência do MDC:

Lema 2.1 *Sejam* $a,\ b,\ n \in \mathbb{N}$ *com* $a < na < b$, *se existe* $mdc(a, b-na)$, *então* $mdc(a,b)$ *existe e* $mdc(a,b) = mdc(a, b-na)$.

Demonstração: Seja $d = mdc(a, b-na)$, então $d \mid a$ e $d \mid b-na$. Como $b = b-na+na$, $d \mid b-na$ e $d \mid a$. pela Proposição 2.3 item 6 temos que $d \mid b-na+na$, ou seja, $d \mid b$. Como d divide a e também divide b, então d é um divisor comum de a e b. Agora supondo que existe um natural c que é divisor comum de a e b, então c é divisor comum de a e $b-na$ e, portanto, $c \mid d$, o que prova que $d = mdc(a,b)$. ∎

O Algoritmo de Euclides Estendido é uma prova construtiva da existência do MDC de dois naturais, vejamos:

Dados $a,\ b \in \mathbb{N}$ e, supondo $a \leqslant b$. Se $a = 1$, então $a = b$, ou $a \mid b$. Portanto, o $mdc(a,b) = a$. Supondo que $1 < a < b$ e $a \nmid b$, pelo Teorema 2.1 podemos escrever

$$b = aq_1 + r_1,\ \text{com}\ r_1 < a.$$

Se $r_1 \mid a$, pelo Lema 2.1, $r_1 = mdc(a, r_1) = mdc(a, b-aq_1) = mdc(a,b)$. Caso contrário, fazemos a divisão de a por r_1, obtendo

$$a = r_1q_2 + r_2,\ \text{com}\ r_2 < r_1.$$

Repetindo o mesmo processo, temos que se $r_2 \mid r_1$, então

$$r_2 = mdc(r_1, r_2) = mdc(r_1, a-r_1q_2) = mdc(r_1, a) = mdc(a, r_1) = mdc(a, b-aq_1) = mdc(a,b).$$

Do contrário, fazemos a divisão de r_1 por r_2, obtendo

$$r_1 = q_3r_2 + r_3,\ \text{com}\ r_3 < r_2.$$

Repetimos o mesmo processo até obter $mdc(a,b)$. Pelo Princípio da Boa Ordem, a sequência de naturais $a > r_1 > r_2 > r_3 > \ldots$ possui mínimo, ou seja, para algum n, temos que $r_n \mid r_{n-1}$ e o $mdc(a,b) = r_n$.

A partir das equações obtidas no algoritmo estendido de Euclides e do Teorema 2.2 , pode-se obter inteiros x e y tais que

$$ax + by = mdc(a, b).$$

Exemplo 2.25 *Calcule o MDC de* 34 *e* 24 :
Solução: Neste caso, podemos escrever 34 como:

$$34 = 24 \cdot 1 + 10. \tag{7}$$

Como $10 \nmid 24$, temos que

$$24 = 10 \cdot 2 + 4. \tag{8}$$

Novamente, como $4 \nmid 10$, temos

$$10 = 4 \cdot 2 + 2. \tag{9}$$

Como $2 \mid 4$, e sabendo que as equações (7), (8) e (9), implicam, respectivamente, nas equações $10 = 34 - 24 \cdot 1$, $4 = 24 - 10 \cdot 2$ e $2 = 10 - 4 \cdot 2$, então, pelo Lema 2.1 temos que

$$\begin{aligned}
2 &= mdc(4, 2) \\
2 &= mdc(4, 10 - 4 \cdot 2) \\
2 &= mdc(4, 10) = mdc(10, 4) \\
2 &= mdc(10, 24 - 10 \cdot 2) \\
2 &= mdc(10, 24) = mdc(24, 10) \\
2 &= mdc(24, 34 - 24 \cdot 1) \\
2 &= mdc(24, 34) = mdc(34, 24).
\end{aligned}$$

Logo, $mdc(34, 24) = 2$. ∎

Além de nos auxiliar no cálculo do MDC de dois naturais, o Algoritmo de Euclides Estendido nos ajuda a encontrar o inverso modular de um número, como se segue no próximo exemplo:
Exemplo 2.26 *Obtenha o inverso de* 15 *módulo* 26 :
Solução: Utilizando o algoritmo de Euclides Estendido, obtemos as seguintes equações:

$$\begin{aligned}
26 &= 15 \cdot 1 + 11; && (10)\\
15 &= 11 \cdot 1 + 4; && (11)\\
11 &= 4 \cdot 2 + 3; && (12)\\
4 &= 3 \cdot 1 + 1. && (13)
\end{aligned}$$

Como $1 \mid 3$, então $mdc(26, 15) = 1$. De (13) obtemos

$$4 - 3 = 1. \tag{14}$$

De (12) obtemos $11 - 4 \cdot 2 = 3$, que ao substituirmos em (14) resulta em

$$4 - (11 - 4 \cdot 2) = 1. \tag{15}$$

De (11) obtemos $4 = 15 - 11$, que ao substituirmos em (15) obtemos

$$15 - 11 - (11 - 4 \cdot 2) = 1. \tag{16}$$

De (10) obtemos $11 = 26 - 15$, que ao substituirmos em (16) resulta em

$$\begin{aligned} 15 - (26 - 15) - [(26 - 15) - 4 \cdot 2] &= 1 \\ 15 - 2 \cdot 26 + 2 \cdot 15 + 2 \cdot 15 - 2 \cdot 26 + 2 \cdot 15 &= 1 \\ 7 \cdot 15 - 4 \cdot 26 &= 1. \end{aligned} \tag{17}$$

Aplicando módulo em (17) temos:

$$\begin{aligned} 7 \cdot 15 - 4 \cdot 26 &\equiv 1 \mod 26 \\ 7 \cdot 15 &\equiv 1 \mod 26. \end{aligned}$$

Com isso, temos que 7 é o inverso multiplicativo de 15 módulo 26. ∎

2.8 ESTRUTURAS ALGÉBRICAS

O estudo de algumas estruturas algébricas é necessário para que possamos abordar a criptografia por curvas elípticas.

Definição 2.10 *Seja G um conjunto não vazio e seja $* : G \times G \longrightarrow G$ uma operação sobre G. Dizemos que esta operação define uma estrutura de grupo sobre o conjunto G, e a denotamos por $(G, *)$ se, e somente se, verificam as seguintes propriedades:*

1. *Associatividade, ou seja, para todo $a, b, c \in G$ temos que $(a * b) * c = a * (b * c)$.*
2. *Existência de elemento neutro, ou seja, existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$.*
3. *Existência de um inverso para cada elemento de G. Ou seja, Para todo $a \in G$ existe $b \in G$ tal que $a * b = b * a = e$.*

Com intenção de simplificar nosso trabalho, daqui em diante denotaremos um grupo $(G, *)$ simplesmente por G, e se não houver perigo de confusão, $a * b$ por ab.

Exemplo 2.27 *Ao considerarmos o conjunto dos números inteiros $\mathbb{Z}$ com a operação de adição usual $(+)$. Temos que $(\mathbb{Z}, +)$ é um grupo, pois*

- *a adição é associativa, uma vez que*

$$x + (y + z) = (x + y) + z, \ \forall \ x, y, z \in \mathbb{Z};$$

- *o* 0 *é o elemento neutro, já que*

$$x + 0 = 0 + x = x, \ \forall \ x \in \mathbb{Z};$$

- *o inverso de* x *é* $-x$*, pois*

$$x + (-x) = (-x) + x = 0, \ \forall \ x \in \mathbb{Z}.$$

Alguns grupos possuem propriedades específicas, é o caso de um grupo abeliano, que definiremos a seguir:

Definição 2.11 *Se a operação de um grupo* G *for comutativa, ou seja, se para todo* $a, b \in G$ *tivermos que* $a * b = b * a$*, dizemos que* G *é um grupo abeliano.*

Precisamos definir também o que é a ordem de um grupo e de um elemento:

Definição 2.12 *Se um grupo* G *tiver um número finito de elementos, dizemos que* G *é um grupo finito. Sendo assim, dizemos que a ordem de* G *é a quantidade de elementos que* G *possui e a denotamos por* $|G|$*.*

Definição 2.13 *Sejam* G *um grupo e* a *um elemento de* G*. Dizemos que* a *tem ordem finita se existe um inteiro positivo* n *tal que* $a^n = e$*. Sendo assim, o menor inteiro positivo* n_0 *tal que* $a^{n_0} = e$*, é o que chamamos de ordem de* a*, e denotamos por* $o(a) = n_0$*.*

Dizemos que o grupo $(\mathbb{Z}, +)$ é cíclico, pois todos os seus elementos são "múltiplos" de 1.

Definição 2.14 *Se todos os elementos de um grupo* G *puderem ser gerados por um determinado elemento* $g \in G$*, dizemos então que* G *é um grupo cíclico e que* g *é seu gerador.*

Da mesma forma que existem subconjuntos, existem também subgrupos:

Definição 2.15 *Seja* G *um grupo. Um subgrupo é um subconjunto* H *não vazio de* G*, quando, com a operação de* G*,* H *também é grupo, então denotamos por* $H < G$*.*

Vamos definir agora uma relação de equivalência para que possamos ter base para demonstrar o Teorema de Lagrange que precisaremos mais a frente:

Definição 2.16 *Uma relação sobre um conjunto* A *é chamada de relação de equivalência se ela é reflexiva, simétrica e transitiva.*

Definição 2.17 *Seja* R *uma relação de equivalência sobre um conjunto* A*, o conjunto de todos os elementos que são relacionados a um elemento* $a \in A$ *é chamado de classe de equivalência de* a*.*

Seja G um grupo e H um subgrupo de G. Definimos a relação R_H sobre G da seguinte forma:

$$xR_Hy \Leftrightarrow \exists h \in H; \ x = yh.$$

De fato, R_H é uma relação de equivalência, pois é:

1. Reflexiva. Ou seja, $xR_Hx \Leftrightarrow \exists h \in H$ tal que $x = xh$. Basta tomar $h = e$, onde e é o elemento neutro de H.
2. Simétrica. Ou seja, $xR_Hy \Leftrightarrow \exists h \in H$ tal que $x = yh \Leftrightarrow xh^{-1} = y \Leftrightarrow yR_Hx$.
3. Transitiva. Ou seja, xR_Hy e $yR_Hz \Leftrightarrow \exists h_1, h_2 \in H$ tais que $x = yh_1$ e $y = zh_2 \Leftrightarrow x = yh_1 = zh_1h_2 = z(h_1h_2) \Leftrightarrow xR_Hz$.

Analogamente, podemos definir a seguinte relação R'_H :

$$xR'_Hy \Leftrightarrow \exists h \in H;\ x = hy.$$

Que também é uma relação de equivalência.

Definição 2.18 *A classe de equivalência, segundo a relação R_H, que contém o elemento x é o conjunto*

$$\overline{x} = \{y \in G;\ yR_Hx\} = \{xh;\ h \in H\}$$

e denominamos classe lateral à esquerda de H. Analogamente, a classe lateral à direita de H é definida por:

$$\overline{x} = \{y \in G;\ yR'_Hx\} = \{hx;\ h \in H\}.$$

Denotaremos a classe lateral à esquerda de H em G de x por xH e a classe lateral à direita de H em G de x por Hx.

Lema 2.2 *Sejam x e y dois elementos quaisquer de um Grupo G, e H um subgrupo de G. Temos que $xH = yH$ se, e somente se, $Hx^{-1} = Hy^{-1}$.*

Demonstração: Seja $xH = yH$, temos que $x^{-1}y \in H$. Logo, $y^{-1}(x^{-1})^{-1} = (x^{-1}y)^{-1} \in H$, portanto, $Hx^{-1} = Hy^{-1}$. Por outro lado, supondo que $Hx^{-1} = Hy^{-1}$, temos que $y^{-1}x = y^{-1}(x^{-1})^{-1} \in H$. Logo, $x^{-1}y = (y^{-1}x)^{-1} \in H$, portanto, $xH = yH$. ∎

Considere a relação R_H determinada por H, que é um subgrupo de G. Denotamos todas as classes de equivalência segundo esta relação por G/R_H. Além disso, dizemos que H tem índice à esquerda finito se, e somente se, o conjunto G/R_H é finito e, neste caso, dizemos que o índice à esquerda de H em G é o número de elementos do conjunto G/R_H. Do contrário, dizemos que H tem índice à esquerda infinito. De forma análoga, essa noção também se aplica para índice à direita ao considerarmos o conjunto HR'_H.

O Lema 2.2 nos mostra que a aplicação $xH \mapsto Hx^{-1}$ é uma bijeção de G/R_H em G/R'_H, portanto, temos que G/R_H é finito se, e somente se, G/R'_H também for. Sendo assim, não existe a necessidade de distinguirmos índice à direita ou à esquerda de H em G. Portanto, diremos apenas que H tem índice finito ou infinito em G e o denotamos por $(G : H)$.

Lema 2.3 *Se H é um subgrupo finito de G, então para todo $a \in G$ temos*

$$|H| = |aH| = |Ha|.$$

Demonstração: Note que as aplicações $x \mapsto ax$ e $x \mapsto xa$ são, respectivamente, bijeções de H em aH e de H em Ha. ∎

Se H é um subgrupo de um grupo finito G, então G/R_H é finito. Além disso, G/R_H é a reunião de $(G : H)$ classes laterais disjuntas duas a duas, e como estas classes possuem o mesmo número de elementos, que é igual a $|H|$, temos que $|G| = (G : H)|H|$. Com isso, fica demonstrado o Teorema 2.9 que anunciaremos a seguir:

Teorema 2.9 *Para todo subgrupo H de um grupo finito G, tem-se que*

$$|G| = (G : H)|H|.$$

Enunciaremos agora uma forma equivalente ao Teorema 2.9:

Teorema 2.10 *Se G é um grupo finito e H é um subgrupo de G com ordens $|G|$ e $|H|$ respectivamente, então*

$$|H| \mid |G|.$$

Corolário 2.6 *Se G é um grupo finito e $a \in G$, então $o(a) \mid |G|$.*

Demonstração: Seja $a \in G$ e (a) o subgrupo cíclico gerado por a em G. Sendo $o(a)$ a ordem de a, então temos que $a^{o(a)} = e$ implica que (a) tem no máximo $o(a)$ elementos. Então $a^i = a^j$ para alguns inteiros $0 < i < j < o(a)$, daí $a^{j-i} = e$, porém, $0 < j - i < o(a)$, o que não pode ocorrer. Portanto, $|(a)| = o(a)$ e pelo Teorema 2.10, temos que

$$o(a) = |G|.$$

∎

Teorema 2.11 *Se G é um grupo abeliano de ordem prima, então G é cíclico.*

Demonstração: Seja p um número primo tal que $|G| = p$, e seja a um elemento qualquer de G, pelo Teorema 2.10, temos que $|a| \mid p$. Como p é primo, então há duas possibilidades:

1. $|a| = 1$, o que implica que a é o elemento neutro. Ou
2. $|a| = p$, o que implica que a gera todos os elementos de G.

Logo, G é cíclico. ∎

Trabalharemos agora com uma estrutura algébrica que consiste em um conjunto munido de duas operações:

Definição 2.19 *Dizemos que um conjunto R munido das operações de adição $(+)$ e multiplicação $(\cdot)$ é um Anel se:*

1. *É um grupo abeliano quanto à adição;*
2. *A multiplicação é associativa;*
3. *Vale a distributividade da adição em relação a multiplicação.*

Alguns anéis são ditos comutativos e/ou com unidade.

Definição 2.20 *Um anel R é dito comutativo se a operação $(\cdot)$ for comutativa, ou seja,*

se

$$a \cdot b = b \cdot a \ \forall \ a, b \in R.$$

Definição 2.21 *Se existe um elemento $a' \in R$ tal que $a \cdot a' = a' \cdot a = a \ \forall a \in R$, então chamamos o elemento a' de unidade do anel R. Além disso, dizemos que R é um anel com unidade.*

Pela Proposição 2.8, temos que a congruência modular é uma relação de equivalência. Além disso, dizer que x é congruente a y significa dizer que os restos da divisão de x e de y por m são iguais. Assim, podemos construir as classes de equivalência $\overline{z}$ para cada $z \in \mathbb{Z}$.

Definição 2.22 *Pela definição de classes de equivalência, temos que $\overline{z}$ consiste em todos os números inteiros relacionados com z, no caso da congruência modular, todos os números inteiros que deixam o mesmo resto que z na divisão por m. Desse modo, temos que*

$$\begin{aligned}
\overline{0} &= \{0, \pm m, \pm 2m, \pm 3m, \ldots\}; \\
\overline{1} &= \{1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \ldots\}; \\
\overline{2} &= \{2, 2 \pm m, 2 \pm 2m, 2 \pm 3m, \ldots\}; \\
&\vdots \\
\overline{m-1} &= \{m-1, m-1 \pm m, m-1 \pm 2m, m-1 \pm 3m, \ldots\}; \\
\overline{m} &= \{m, m \pm m, m \pm 2m, m \pm 3m, \ldots\};
\end{aligned}$$

onde as classes começam a se repetir.

Observe que a classe $\overline{m-1} = \{-1, -1 \pm m, -1 \pm 2m, -1 \pm 3m, \ldots\}$, ou seja, $\overline{m-1} = \overline{-1}$. Observe ainda que a classe $\overline{m} = \{0, \pm m, \pm 2m, \pm 3m, \ldots\}$, ou seja, $\overline{m} = \overline{0}$. Portanto, temos m classes de equivalências distintas, denominadas classes de equivalência módulo m. Denotamos o conjunto dessas classes por $\mathbb{Z}_m$. Logo, temos que

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}\}.$$

Exemplo 2.28 *O conjunto $\mathbb{Z}_m$ é um anel comutativo com unidade.*

Solução: Definiremos primeiramente as operações de soma e de produto em $\mathbb{Z}_m$:

Para cada $\overline{a}, \overline{b} \in \mathbb{Z}_m$, definimos a soma $\overline{a} + \overline{b} = \overline{a+b}$, e o produto $\overline{a}\overline{b} = \overline{a} \cdot \overline{b}$ por $\overline{a}\overline{b} = \overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{ab}$.

Dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_m$, temos que

$$\overline{a} + \overline{b} = \overline{a+b} = \overline{b+a} = \overline{b} + \overline{a},$$

e também que

$$(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c}),$$

o que nos mostra a comutatividade e associatividade da soma em $\mathbb{Z}_m$.

Vamos agora em busca de um elemento neutro $e \in \mathbb{Z}_m$ tal que $\overline{a}+e=e+\overline{a}=\overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$. Como $e \in \mathbb{Z}_m$, então $e=\overline{z}$ para algum $z \in \mathbb{Z}$. Portanto, temos que a igualdade $\overline{a}+e=\overline{a}$ implica que $\overline{a}+\overline{z}=\overline{a}=\overline{a+z}=\overline{a}$, o que pela definição de congruência nos diz que $m|(a+z-a)$, ou seja, $m|z$. Logo, $z=km$, para qualquer $k \in \mathbb{Z}$. Com isso, podemos concluir que z pertence à classe $\overline{0}$. Portanto, o elemento neutro da soma em $\mathbb{Z}_m$ é $e=\overline{z}=\overline{0}$.

Dado $\overline{a} \in \mathbb{Z}_m$, procuraremos agora o simétrico de $\overline{a}$, ou seja, um elemento $\overline{a'} \in \mathbb{Z}_m$ tal que $\overline{a}+\overline{a'}=\overline{0}$. Dessa forma, temos que $\overline{a+a'}=\overline{0} \Rightarrow m|(a+a'-0)$, ou seja, $a+a'$ é um múltiplo de m, com isso, temos que $a+a'=km \Rightarrow a'=-a+km$ para $k \in \mathbb{Z}$. Observe que os números da forma $-a+km$ pertencem à classe $\overline{m-a}$ ou $\overline{-a}$, onde todo elemento $\overline{a} \in \mathbb{Z}_m$ é simetrizável, sendo $-\overline{a}=\overline{-a}=\overline{m-a}$ o seu simétrico. Com isso, concluímos a prova de que a adição torna $\mathbb{Z}_m$ um grupo abeliano.

Provaremos agora que a multiplicação é associativa, comutativa, distributiva em relação à adição e que também admite elemento neutro:

Dados $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}_m$, temos que

$$\overline{a}\cdot\overline{b}=\overline{ab}=\overline{ba}=\overline{b}\cdot\overline{a},$$

e também que

$$(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{ab}\cdot\overline{c}=\overline{(ab)c}=\overline{a(bc)}=\overline{a}\cdot\overline{bc}=\overline{a}\cdot(\overline{b}\cdot\overline{c}),$$

o que nos mostra a comutatividade e associatividade da multiplicação em $\mathbb{Z}_m$.

A distributividade em relação à adição também é verdade pois

$$\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{b+c}=\overline{a(b+c)} \Rightarrow$$

$$\Rightarrow \overline{a}\cdot(\overline{b}+\overline{c})=\overline{ab+ac}=\overline{ab}+\overline{ac}=(\overline{a}\cdot\overline{b})+(\overline{a}\cdot\overline{c}).$$

Vamos agora em busca de um elemento neutro $e \in \mathbb{Z}_m$ tal que $\overline{a}\cdot e=e\cdot\overline{a}=\overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$. Como $e \in \mathbb{Z}_m$, então $e=\overline{z}$ para algum $z \in \mathbb{Z}$. Portanto, temos que a igualdade $\overline{a}\cdot e=\overline{a}$ implica que $\overline{a}\cdot\overline{z}=\overline{a}=\overline{az}=\overline{a}$, o que pela definição de congruência nos diz que $m|(az-a)$, ou seja, $m|a(z-1)$. Para que isso seja verdade para todo $\overline{a} \in \mathbb{Z}_m$ é necessário que m divida $(z-1)$. Logo, $\overline{z}=\overline{1}$. Portanto, o elemento neutro da multiplicação em $\mathbb{Z}_m$ é $e=\overline{z}=\overline{1}$.

Concluímos aqui que $\mathbb{Z}_m$ é um anel comutativo com unidade. ∎

Definição 2.23 *Seja* $\mathbb{K}$ *um anel comutativo com unidade, se para todo elemento não nulo* $b \in \mathbb{K}$ *existe um elemento* $b' \in \mathbb{K}$ *tal que* $b \cdot b' = b' \cdot b = 1$, *dizemos que* $\mathbb{K}$ *é um corpo.*

Teorema 2.12 *O conjunto* $\mathbb{Z}_m$ *é um corpo se, e somente se,* m *é um número primo.*

Demonstração: Inicialmente vamos supor que $\mathbb{Z}_m$ é um corpo. Se mostrarmos que m não é divisível por $2, 3, 4, \ldots, m-1$, estaremos mostrando que m é primo. Considere $a \in \{2, 3, 4, \ldots, m-1\}$. Daí, temos que $\overline{a} \neq \overline{0}$. Como $\mathbb{Z}_m$ é um corpo, então existe $\overline{x} \in \mathbb{Z}_m - \{\overline{0}\}$ em que $\overline{ax} = \overline{1}$. Portanto, $m \mid (ax - 1)$. Logo, existe $y \in \mathbb{Z}$ tal que $ax + ym = 1$. O que implica que $mdc(a, m) = 1$, portanto, $a \nmid m$, ou seja, m é primo.

Como provamos no Exemplo 2.28 que $\mathbb{Z}_m$ é anel comutativo com unidade, se mostrarmos que todo elemento de $\mathbb{Z}_m - \{\overline{0}\}$ é invertível, podemos concluir que $\mathbb{Z}_m$ é um corpo.

Seja $m = p$ um número primo e, a um número inteiro tal que $1 \leqslant a \leqslant p - 1$, temos que $(a, p) = 1$. Logo, existem inteiros x, y tais que $ax + yp = 1$. Sendo assim, temos que

$$\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{x} + \overline{y} \cdot \overline{p} = \overline{a \cdot x} + \overline{y \cdot p} = \overline{ax + yp} = \overline{1}.$$

O que nos mostra que todo elemento de $\mathbb{Z}_m - \{\overline{0}\}$ é invertível. Logo, $\mathbb{Z}_m$ é um corpo. ∎

3 UM POUCO DE HISTÓRIA

A necessidade que tiveram Reis, Rainhas, Imperadores e Generais de guardar segredos de seus inimigos foi o que levou à invenção da criptografia, derivada da palavra grega "kriptos" que significa "oculto". Era indispensável a comunicação destes com seus subordinados ou aliados de forma segura, sem que se deixasse escapar seus segredos, tornando frágil seus impérios, monarquias e exércitos. Para isso, uma das primeiras formas utilizadas para ocultar uma mensagem foi a "esteganografia", como por exemplo, escrever uma mensagem na cabeça raspada de um mensageiro, esperar que seu cabelo crescesse afim de esconder tal mensagem e enviá-lo ao encontro do destinatário. Existiram também outras formas de esteganografia, como o uso de tabuletas de madeira, ou tinta invisível. No caso de tabuletas de madeira, a cera destas era raspada, uma mensagem era escrita na tabuleta que em seguida era coberta por cera novamente e, em caso de interceptação, a tabuleta parecia estar em branco. Em outras situações foram usadas tinta invisível para a escrita de uma mensagem em papel, como por exemplo, o "leite" de algumas plantas ou até mesmo urina, que após escrita no papel, a mensagem some quando o líquido seca, porém, após um aquecimento, pode-se observar novamente o conteúdo escrito. Esta forma de esconder uma mensagem é perigosa, uma vez que caso um mensageiro seja revistado e encontram consigo a mensagem oculta, esta pode ser revelada instantaneamente. Sendo assim, havia a necessidade de garantir uma melhor segurança para uma mensagem secreta, foi aí que iniciou-se a utilização da criptografia de transposição e de substituição.

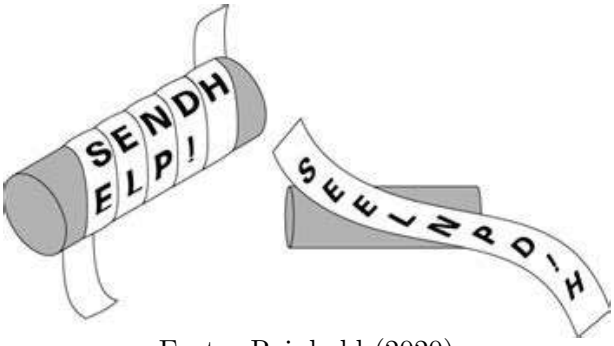
Na criptografia de transposição, eram utilizados anagramas das palavras que queriam esconder seu significado, como por exemplo, a palavra "livro" poderia ser substituída por "virlo". Dessa forma, o nível de segurança ao utilizar a criptografia de transposição é maior à medida que a quantidade de letras da mensagem aumenta, já que estamos trabalhando com permutação. O lado negativo desse tipo de criptografia é que a dificuldade de encontrar o significado da mensagem oculta é grande tanto para um eventual interceptador quanto para o destinatário. Para resolver este problema é necessário que haja uma certa "regra" para a encriptação da mensagem, chamamos tal "regra" de "algoritmo".

Um algoritmo possível é alternar as letras de uma mensagem em duas sequências, onde a mensagem encriptada é a sequência de letras de posição ímpar seguida da sequência de letras de posição par. Vejamos: Para encriptarmos a frase "todas as coisas são números", fazemos uma sequência de letras de posição ímpar, "TDSSOSSANMRS" e uma sequência de letras de posição par, "OAACIASOUEO", e escrevemos uma sequência seguida da outra, formando assim a encriptação da mensagem " TDSSOSSANMRSOAACIASOUEO".

Um outro exemplo do uso de criptografia de transposição data do século V a.C. e é o primeiro registro de um aparelho criptográfico de uso militar, a "cítala espartana".

O objeto consiste em um bastão de madeira que é envolto com uma tira de couro onde a mensagem era escrita no sentido de seu comprimento, depois a tira era desenrolada e transportada como um cinto com letras sem sentido e, após enrolá-la novamente em um outro bastão de mesmo diâmetro, podia-se encontrar o significado da mensagem.

Figura 1 – Cítala espartana



Fonte: Reinhold (2020)

3.1 A CIFRA DE CÉSAR

Na criptografia de substituição, cada letra do alfabeto é substituída por uma outra letra ou símbolo. A forma mais conhecida de criptografia de substituição é a "Cifra de César", utilizada pelo líder romano Júlio César para propósitos militares, onde cada letra do "alfabeto original" era substituída por uma letra três casas a frente, formando o "alfabeto cifrado". Vejamos:

Tabela 2 – Cifra de César

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P
Alfabeto original	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fonte: Singh (2020) .

Observação 3.1 Daqui pra frente, usaremos letras minúsculas sempre que estivermos tratando de letras de um texto original e letras maiúsculas sempre que estivermos tratando de um texto cifrado. Com exceção de quando estivermos usando sistemas criptográficos que substituam letras por números.

Sendo assim, a frase "a educação pode tudo: ela faz dançar os ursos." encriptada utilizando a Cifra de César é: "D HGX FDFDR SRGH WXGR: HOD IDW GDQFDU RU XUVRRV." Para encontrar o significado da mensagem, basta que o destinatário faça o caminho contrário, conhecendo ele os alfabetos em questão. Esse tipo de criptografia é chamado de "Cifra de substituição monoalfabética", por ter sido utilizado um único alfabeto cifrado.

A Cifra de César não foi utilizada apenas por ele e nem sempre a letra original era representada pela três casas subsequente, qualquer letra do alfabeto poderia ser

representada por uma outra. Foi aí que houve a necessidade de ser criado um sistema com uma "palavra-chave", pois toda a rede de comunicação que utilizava a cifra precisava saber qual o alfabeto cifrado utilizado. Funciona da seguinte forma: remetente e destinatário concordam em uma chave secreta que serve como base para a criação do alfabeto cifrado, a chave pode ser uma palavra, onde as primeiras letras do alfabeto original são substituídas pelas letras da chave, sem repetir letra (caso a palavra tenha letras repetidas), seguidas das letras restantes do alfabeto original. Por exemplo, se usarmos a palavra "CERTEZA" como chave, utilizaremos a sequência de letras "CERTZA", obtendo assim, o seguinte alfabeto cifrado:

Tabela 3 – Cifra de César com a chave "CERTEZA".

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto cifrado	C	E	R	T	Z	A	B	D	F	G	H	I	J
Alfabeto original	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	K	L	M	N	O	P	Q	S	U	V	W	X	Y

Fonte: Próprio autor.

Por exemplo, a palavra "matemática" criptografada é "JCQZJCQFRC". Para encontrar o significado da mensagem, o destinatário precisa apenas saber qual foi a chave utilizada para produzir o alfabeto cifrado. É bem mais fácil compartilhar uma chave (que deve ficar em segredo entre emissor e receptor da mensagem) do que um alfabeto cifrado inteiro.

Esse tipo de criptografia que utiliza apenas uma chave secreta, que é usada tanto para criptografar quanto para descriptografar, é chamado de criptografia simétrica.

No século XVIII iniciou a "era de ouro" da civilização islâmica, fruto de uma sociedade rica, organizada e pacífica, onde se investiu muito em ciências, inclusive em criptografia. Eles utilizavam não apenas letras em um alfabeto cifrado, mas também outros símbolos.

Os cientistas árabes deixaram um grande legado para a matemática, incluindo nele está a invenção da "criptoanálise", a ciência de decifrar uma mensagem sem que se conheça a chave da cifra usada para sua encriptação. A técnica utilizada pelos árabes para analisar uma mensagem criptografada com cifra monoalfabética, conhecida por "análise de frequências" foi descrita por al-Kindi, conhecido como "o filósofo dos árabes". A técnica consiste em analisar a frequência com que cada letra aparece em um texto original arbitrário. Faz-se o mesmo com um texto cifrado e, a partir daí, faz-se a substituição da letra mais frequente no texto cifrado pela letra mais frequente no texto original. Observa-se algumas particularidades das palavras de determinada língua, como no caso da língua portuguesa, as letras "r" e "s" costumam aparecer em dobro em palavras como "carro" e "disseminar". Além disso, pode-se observar também o uso do "ão", dentre outras particularidades. Dessa forma , descobre-se a verdadeira identidade de algumas letras, daí vai surgindo a verdadeira identidade de algumas palavras e consequentemente, de

novas letras, até que se consegue decifrar todo o texto.

Faremos a seguir um exemplo de como utilizar a análise de frequência para decifrar uma mensagem em português:

Exemplo 3.1 *Decifre a mensagem abaixo:*

Z DQ JQK KGBQTQ Q HQNOCJBQ IKH Q LOCHCRCTQ ZWLOZPPQK QPPSPRQNQ. RCJBQ LQOQ ZGQ KGBQOZP QAOQNZICNKP Z HZCAKP, MSZ Q QIKHLQJBQTQH Q ICOISGQO JK MSQORK, Z NZHKOQTQH GKJAQHZJRZ, IKH SHQ ECWCNZY UOCGBQJRZ, JQP LOZAQP NK PZS TZPRCNK UOQJIK, JKP GQIKP NZ PSQP ROQJIQP.

Solução:

Primeiramente, selecionamos um texto qualquer escrito em língua portuguesa e analisamos a frequência com que cada letra aparece nesse texto e faremos o mesmo com o texto encriptado. Para isso, quão maior for o texto em português analisado, melhor será a precisão dos dados obtidos. O texto utilizado aqui é um trecho do livro Iracema, de José de Alencar.

Andira, o velho Andira, bebeu mais sangue na guerra do que já beberam cauim nas festas de Tupã, todos quantos guerreiros alumia agora a luz de seus olhos. Ele viu mais combates em sua vida, do que luas lhe despiram a fronte. Quanto crânio de potiguara escalpelou sua mão implacável, antes que o tempo lhe arrancasse o primeiro cabelo? E o velho Andira nunca temeu que o inimigo pisasse a terra de seus pais; mas alegrava-se quando ele vinha, e sentia com o faro da guerra a juventude renascer no corpo decrépito, como a árvore seca renasce com o sopro do inverno. A nação tabajara é prudente. Ela deve encostar o tacape da luta para tanger o membi da festa. Celebra, Irapuã, a vinda dos emboabas e deixa que cheguem todos aos nossos campos. Então Andira te promete o banquete da vitória.

Tabela 4 – Frequência das letras do alfabeto no trecho do livro Iracema.

Letra	a	b	c	d	e	f	g	h	i	j	k	l	m
Frequência	98	12	22	27	85	4	10	7	32	3	0	19	24
Letra	n	o	p	q	r	s	t	u	v	w	x	y	z
Frequência	33	60	18	9	43	44	28	34	13	0	1	0	1

Fonte: Próprio autor.

Tabela 5 – Frequência das letras do alfabeto no trecho criptografado.

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Frequência	4	6	12	1	1	0	7	11	9	12	18	5	2
Letra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Frequência	9	14	17	40	8	7	5	2	0	2	0	1	19

Fonte: Próprio autor.

Observe as cinco letras mais frequentes nos dois textos:

Tabela 6 – Letras mais frequentes.

	Trecho de Iracema	Mensagem cifrada
1ª	a	Q
2ª	e	Z
3ª	o	K
4ª	s	P
5ª	r	O

Fonte: Próprio autor.

Se fizermos uma substituição da primeira letra mais frequente no texto cifrado pela primeira letra mais frequente no trecho de Iracema e em seguida substituir as segundas letras mais frequentes, depois as terceiras letras mais frequentes e assim por diante, provavelmente não conheceremos o significado do texto cifrado, pois a frequência com que cada letra aparece em um texto pode variar. Por isso, devemos analisar antes de fazer as substituições. Mostraremos aqui os passos utilizados nesse caso:

1. Observe que em ambos os textos, uma letra foi bem mais frequente que as demais, foram elas "**a**" e "**Q**". Como essas letras destoaram das demais, muito provavelmente "**Q**" represente "**a**". Portanto, faremos a substituição no texto cifrado:
   Z Da JaK KGBaTa a HaNOCJBa IKH a LOCHCRCTa ZWLOZPPaK aPPSPRaNa. RCJBa LaOa ZGa KGBaOZP aAOaNZICNKP Z HZCAKP, MSZ a aIKHLaJBaTaH a ICOISGaO JK MSaORK, Z NZHKOaTaH GKJAaHZJRZ, IKH SHa ECWCNZY UOCGBaJRZ, JaP LOZAaP NK PZS TZPRCNK UOaJIK, JKP GaIKP NZ PSaP ROaJIaP.

2. Veja que em "ZWLOZPPaK" e "aPPSPRaNa" a letra "**P**" aparece repetida, o que nos leva a crer que "**P**" deve representar "**r**" ou "**s**", que são letras que têm essa característica em um texto da língua portuguesa.

3. Observe também que as próximas letras mais frequentes no trecho de Iracema foram o "e" e o "o". Já no texto cifrado, foram o "Z" e o "K". O fato de no trecho de Iracema encontrarmos mais palavras terminadas com a letra "o" em relação a palavras terminadas com a letra "e", seguido do fato que no fim de uma palavra, após "rr" ou "ss" ser comum encontrarmos "ão", nos leva a crer que no texto cifrado, a letra "**K**" representa a letra "**o**", já que a letra "K" aparece no fim de palavras com mais frequência que a letra "Z", e na palavra "ZWLOZPPaK", supomos que "PP" seja "rr" ou "ss" seguido de "ão". Sendo assim, a letra "**Z**" deve representar a letra "**e**". Faremos as devidas substituições:
   e Da Jao oGBaTa a HaNOCJBa IoH a LOCHCRCTa eWLOePPao aPPSPRaNa. RCJBa LaOa eGa oGBaOeP aAOaNeICNoP e HeCAoP, MSe a aIoHLaJBaTaH a ICOISGaO Jo MSaORo, e NeHoOaTaH GoJAaHeJRe, IoH SHa ECWCNeY UOCGBaJRe, JaP LOeAaP No PeS TePRCNo UOaJIo, JoP GaIoP Ne PSaP RO-

aJIaP.

4. A palavra “eGa” deve significar “ela”, portanto, vamos supor que a letra “**G**” representa a letra “**l**”. Logo, ao fazermos as substituições, temos:
   e Da Jao olBaTa a HaNOCJBa IoH a LOCHCRCTa eWLOePPao aPPSPRaNa. RCJBa LaOa ela olBaOeP aAOaNeICNoP e HeCAoP, MSe a aIoHLaJBaTaH a ICOISlaO Jo MSaORo, e NeHoOaTaH loJAaHeJRe, IoH SHa ECWCNeY UOClBaJRe, JaP LOeAaP No PeS TePRCNo UOaJIo, JoP laIoP Ne PSaP ROaJIaP.

5. Como supomos que “P” seja “r” ou “s”, ao observarmos que algumas palavras seguidas terminam em “P” o que indica possíveis plurais, vamos supor que “**P**” representa a letra “**s**”, obtendo assim:
   e Da Jao olBaTa a HaNOCJBa IoH a LOCHCRCTa eWLOessao assSsRaNa. RCJBa LaOa ela olBaOes aAOaNeICNos e HeCAos, MSe a aIoHLaJBaTaH a ICOISlaO Jo MSaORo, e NeHoOaTaH loJAaHeJRe, IoH SHa ECWCNeY UOClBaJRe, Jas LOeAas No seS TesRCNo UOaJIo, Jos laIos Ne sSas ROaJIas.

6. As palavras “Jao”, “Jo”, “Jas” e “Jos” muito provavelmente devem significar “não”, “no”, “nas” e “nos”, o que nos faz supor que a letra “**J**” deve representar a letra “**n**”. Ficando nosso texto cifrado da seguinte forma:
   e Da nao olBaTa a HaNOCnBa IoH a LOCHCRCTa eWLOessao assSsRaNa. RCnBa LaOa ela olBaOes aAOaNeICNos e HeCAos, MSe a aIoHLanBaTaH a ICOISlaO no MSaORo, e NeHoOaTaH lonAaHenRe, IoH SHa ECWCNeY UOClBanRe, nas LOeAas No seS TesRCNo UOanIo, nos laIos Ne sSas ROanIas.

7. As monossílabas “No” e “Ne” devem representar as palavras “do” e “de”, logo, a letra “**N**” deve significar “**d**”. Faremos então a substituição:
   e Da nao olBaTa a HadOCnBa IoH a LOCHCRCTa eWLOessao assSsRada. RCnBa LaOa ela olBaOes aAOadeICdos e HeCAos, MSe a aIoHLanBaTaH a ICOISlaO no MSaORo, e deHoOaTaH lonAaHenRe, IoH SHa ECWCdeY UOClBanRe, nas LOeAas do seS TesRCdo UOanIo, nos laIos de sSas ROanIas.

8. A palavra “laIos” pode ser “lagos” ou “laços”, porém, como no texto aparece por duas vezes a palavra “IoH”, que suspeitamos que seja a palavra “com”, o que nos leva a crer que a letra “**I**” significa “**c**”, e que “**H**” significa “**m**”. Faremos essas substituições:
   e Da nao olBaTa a madOCnBa com a LOCmCRCTa eWLOessao assSsRada. RCnBa LaOa ela olBaOes aAOadecCdos e meCAos, MSe a acomLanBaTam a cCOcSlaO no MSaORo, e demoOaTam lonAamenRe, com Sma ECWCdeY UOClBanRe, nas LOeAas do seS TesRCdo UOanco, nos lacos de sSas ROancas.

9. Das cinco letras mais frequentes no trecho de Iracema, ainda nos resta a letra “r”.

Já no texto cifrado, dentre as cinco letras mais frequentes, ainda não encontramos o significado de "O". Supondo que "O" represente realmente a letra "r", temos que a palavra "ROancas" ficaria "Rrancas", que ao trazermos pro contexto, a última frase "nos lacos de sSas ROancas" deve significar "nos laços de suas tranças". Logo, as letras "**O**", "**S**" e "**R**" representam, respectivamente, as letras "**r**", "**u**"e "**t**". Vejamos como fica o texto após essas substituições:
e Da nao olBaTa a madrCnBa com a LrCmCtCTa eWLressao assustada. tCnBa Lara ela olBares aAradecCdos e meCAos, Mue a acomLanBaTam a cCrcular no Muarto, e demoraTam lonAamente, com uma ECWCdeY UrClBante, nas LreAas do seu TestCdo Uranco, nos laços de suas tranças.

10. Os trechos "eWLressao assustada", "cCrcular no Muarto" e " demoraTam lonAamente" devem significar, respectivamente, "expressão assustada", "circular no quarto" e "demoravam longamente". Portanto, as letras "**W**", "**L**", "**C**", "**M**", "**T**" e "**A**" devem representar, respectivamente, "**x**", "**p**", "**i**", "**q**", "**v**" e "**g**". Vejamos como fica o texto:
e Da nao olBava a madrinBa com a primitiva expressao assustada. tinBa para ela olBares agradecidos e meigos, que a acompanBavam a circular no quarto, e demoravam longamente, com uma EixideY UrilBante, nas pregas do seu vestido Uranco, nos laços de suas tranças.

11. As palavras "olBava" e "madrinBa" nos indicam que a letra "**B**" reprenta a letra "**h**". Além disso, as palavras "UrilBante" e "Uranco" nos fazem supor que a letra "**U**" esteja substituindo a letra "**b**". Com isso, nosso texto está praticamente todo decriptado, vejamos:
e Da não olhava a madrinha com a primitiva expressão assustada. tinha para ela olhares agradecidos e meigos, que a acompanhavam a circular no quarto, e demoravam longamente, com uma EixideY brilhante, nas pregas do seu vestido branco, nos laços de suas tranças.

12. Ainda não encontramos quais letras representam "f", "j", "k", "y" e "z". A letra "j" cabe na palavra "Da", já as letras "f" e "z" cabem na palavra "EixideY", formando as palavras "já" e "fixidez", respectivamente. Portanto, temos que "**D**" representa "**j**", "**E**" representa "**f**"e "**Y**" representa "**z**". Com isso, concluímos a decriptação da mensagem. Veja agora a mensagem na íntegra:

    E já não olhava a madrinha com a primitiva expressão assustada. Tinha para ela olhares agradecidos e meigos, que a acompanhavam a circular no quarto, e demoravam longamente, com uma fixidez brilhante, nas pregas do seu vestido branco, nos laços de suas tranças.

Na Tabela 7 fizemos uma associação das letras do alfabeto original com as do alfabeto cifrado, onde podemos identificar qual chave foi usada para encriptar esta mensagem.

Tabela 7 – Cifra utilizada para encriptar o texto do Exemplo 3.1.

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto cifrado	Q	U	I	N	Z	E	A	B	C	D	F	G	H
Alfabeto original	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	J	K	L	M	O	P	R	S	T	V	W	X	Y

Fonte: Próprio autor.

Podemos então observar que a chave utilizada foi a palavra "QUINZE", e não por acaso, já que o texto decriptado é um trecho do livro O quinze de Rachel de Queiroz.

■

O método de análise de frequências utilizado pelos árabes logo foi também muito utilizado na Europa, onde as grandes potências tinham suas "câmaras negras", centros para decifrar mensagens e reunir informações. A eficiência das câmaras negras fez com que as cifras monoalfabéticas já não tivessem um nível de segurança desejado. Foi aí que houve a necessidade de ser criada uma cifra onde o método de análise de frequências não fosse suficiente para decifrá-la. No século XVI o diplomata francês Blaise de Vigenère deixou a função de diplomata, onde muitas vezes se deparou com criptografia e passou a se dedicar aos estudos, formando uma nova cifra, que chegou a ser chamada de "Cifra indecifrável".

3.2 A CIFRA DE VIGENÈRE

A Cifra de Vigenère utiliza um quadro com um alfabeto original seguido de 26 alfabetos cifrados. Na primeira linha fica o alfabeto original, na segunda, encontra-se o alfabeto cifrado de número 1, iniciado não mais pela letra A, e sim pela letra B. Na terceira linha fica o alfabeto cifrado de número 2, iniciado pela letra C. Seguindo a mesma lógica, a penúltima linha da tabela é o alfabeto cifrado de número 25, iniciado pela letra Z, e a última é o alfabeto cifrado de número 26, iniciado pela letra A, ou seja, é o mesmo alfabeto original. Vejamos a tabela da Figura 2 abaixo:

Figura 2 – Tabela 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**
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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
26	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

Fonte: Singh (2020).

Para cifrar uma mensagem, temos a disposição 26 alfabetos diferentes, se usarmos apenas um deles, estaremos utilizando uma cifra monoalfabética, como a de César, que pode ser quebrada utilizando o método de análise de frequências como já vimos anteriormente. Porém, se para cifrar uma mensagem utilizarmos mais de um alfabeto cifrado, estaremos desfrutando de uma "cifra polialfabética", dificultando assim a utilização da análise de frequências como vimos no Exemplo 3.1. Funciona da seguinte maneira: Se quisermos cifrar a palavra "voo", ao utilizarmos o alfabeto de número 1 para cifrar a letra "v", o alfabeto de número 2 para cifrar a primeira letra "o" e o alfabeto de número 3 para cifrar a segunda letra "o", substituiríamos cada uma dessas letras, respectivamente, por "W", "Q" e "R", formando assim a palavra "WQR". Observe que mesmo que a palavra "voo" tenha duas letras "o", após cifrada não possui símbolos repetidos, dificultando assim a utilização do método de análise de frequências dos árabes.

A utilização de chave simétrica na Cifra de Vigenère, funciona da seguinte forma: é feita uma tabela onde na primeira linha é colocada a mensagem a ser criptografada, na segunda linha é colocada repetidas vezes a chave, associando cada letra da

mensagem a ser cifrada com uma letra da chave. A letra da chave associada à letra a ser codificada é a inicial do alfabeto cifrado que iremos utilizar para encriptar aquela letra. Por exemplo, se queremos encriptar a letra "g" e a ela está associada a letra "K", então usaremos o alfabeto de número 10 para fazer a encriptação, dessa forma, a letra "g" encriptada é "Q".

Exemplo 3.2 *Utilize a Cifra de Vigenère com a chave "LIVRO" para encriptar a palavra "abacatada".*

Solução: Para encriptar a palavra, faremos a Tabela 8 abaixo:

Tabela 8 – Cifrando a palavra "abacatada".

Mensagem original	a	b	a	c	a	t	a	d	a
Chave	L	I	V	R	O	L	I	V	R
Alfabeto cifrado a ser utilizado	11	08	21	17	14	11	08	21	17
Mensagem cifrada	L	J	V	T	O	E	I	Y	R

Fonte: Próprio autor.

■

Observe que mesmo a letra "a" sendo muito frequente na palavra "abacatada", após a encriptação desta, cada "a" foi substituído por uma letra distinta. Ou seja, o criptoanalista que tentar utilizar o método de análise de frequências dos árabes para decriptar esta palavra não terá uma tarefa fácil.

Por ser imune à análise de frequências vista no Exemplo 3.1, os criptógrafos estavam um passo a frente dos criptoanalistas e a Cifra de Vigenère passou a ser amplamente utilizada na Europa. Porém, isso demorou a acontecer, pois a Cifra que posteriormente seria chamada de "indecifrável" ficou dois séculos sem atrair a atenção daqueles que precisavam esconder suas informações sigilosas.

Já após ser utilizada amplamente, por considerar a Cifra de Vigenère indecifrável, vários criptoanalistas desistiram da tentativa de decifrá-la, porém, de forma independente, o oficial da reserva do exército prussiano Friedrich Wilhem Kasiski e o gênio britânico Charles Babbage conseguiram vencer a Cifra de Vigenère. Babbage percebeu que no processo de codificação de uma mensagem com a cifra de Vigenère, apesar de ser utilizado vários alfabetos cifrados, uma letra pode ser codificada várias vezes com o mesmo alfabeto cifrado por conta de sua natureza cíclica. Por exemplo, se uma mensagem for codificada pela palavra-chave "ROSA", então a primeira letra será codificada com o alfabeto criptografado cuja inicial é a letra "R", além dela a quinta letra da mensagem, assim como a nona letra também serão criptografadas pelo mesmo alfabeto cifrado. Ou seja, em uma mensagem criptografada por uma palavra-chave de 4 letras distintas, de quatro em quatro letras é usado o mesmo alfabeto cifrado. Sendo assim, descobrindo o tamanho da palavra-chave, pode-se utilizar a análise de frequência em cada um dos alfabetos utilizados para a encriptação. Além disso, existem poucos arranjos possíveis para determinadas palavras comuns, como por exemplo, para a palavra "não", que se for

criptografada com a palavra-chave “ROSA”, poderá ser representada por “EOG”, “BSO”, “FAF” ou “NCR”. Dessa forma, se a palavra “não” aparecer mais de uma vez em uma mensagem, muito provavelmente poderá ser identificada. Com isso, Babbage buscou por sequências de letras que aparecem mais de uma vez em uma mensagem encriptada. No Exemplo 3.3 a seguir tentamos decifrar uma mensagem utilizando as técnicas de Babbage, vejamos:

Exemplo 3.3 *Decifre a mensagem a seguir:*

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

Solução: Primeiramente, procuramos por sequências de letras que aparecem repetidas ve-

zes e contamos quantas letras após a primeira ocorrência acontece a segunda. A sequência "IBANSXTWFP" aparece pela segunda vez 20 letras após o primeiro aparecimento. Já a sequência "SOQFTPGFIOTWDDCGD" dista 516 letras após seu primeiro aparecimento. A sequência "DKTXCWZSAFS" só aparece pela terceira vez após 32 letras do segundo aparecimento. A sequência "PQWWAO" aparece no texto duas vezes, sendo que o segundo aparecimento ocorre 852 letras após o primeiro. Já a sequência "XFKQ" aparece pela terceira vez 428 letras após seu segundo aparecimento.

Muito provavelmente, o fato dessas sequências de letras aparecerem mais de uma vez no texto significa que elas representam uma mesma sequência no texto original. Nosso foco aqui é encontrar o tamanho da palavra-chave utilizada para encriptar a mensagem, para isso verificaremos agora um termo em comum entre as distâncias encontradas anteriormente.

Como a menor distância entre a repetição de uma sequência encontrada no texto é 20, então a palavra-chave usada tem no máximo 20 letras. Observe que o número 20 tem como possíveis fatores os números 1, 2, 4, 5, 10 e 20. Dentre os fatores do número 516, os possíveis são 1, 2, 3, 4, 6 e 12. Os fatores possíveis de 32 são 1, 2, 4 e 8. Já os do número 852 são 1, 2, 3, 4, 6 e 12. Finalmente, os fatores possíveis do número 428 são 1, 2 e 4. Observe que todos esses números possuem três fatores em comum, são eles os números 1, 2 e 4.

Se a palavra chave tem tamanho 1, então estaríamos tratando de uma cifra monoalfabética, o que provavelmente não seja o caso. Uma chave de tamanho 2 indica que apesar de ser utilizada uma cifra polialfabética, apenas dois alfabetos cifrados foram utilizados, o que não é tão seguro. Portanto, presumimos aqui que o tamanho da palavra-chave é 4. Dessa forma, dividiremos o texto cifrado em quatro blocos e faremos uma análise de frequência em cada um desses blocos. O primeiro bloco conterá as letras de número 1, 5, 9, 13, ...; o segundo bloco conterá as letras de número 2, 6, 10, 14, ... ; o terceiro, as letras de número 3, 7, 11, 15, ...; e o quarto, as letras de número 4, 8, 12, 16, ... Cada um dos blocos foram encriptados por um alfabeto criptografado de inicial ainda desconhecida, por isso, chamaremos cada inicial, respectivamente, de A_1, A_2, A_3 e A_4.

Bloco 1:

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

Bloco 2:

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

Bloco 3:

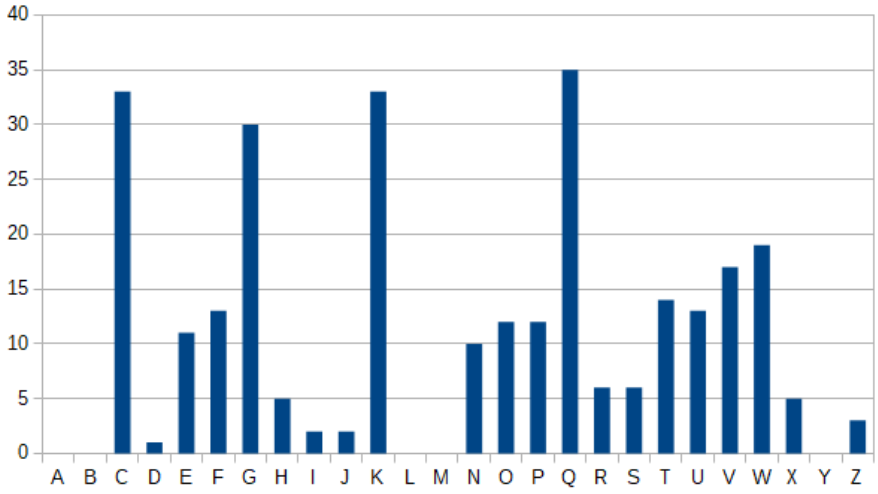
X P A T T T T I X J S H H K C S B X P X R B X P I B D U P R D P I S A D B I J I I J C T X S F S D D B P P D H I R R P T D P J M T D X W D S D X G T J P B X P P B T S R P A D P H S D H T E D T P T T I D X S D D J X P J D D J X X A S T I D D X T P C T I D X X H X P P X S C H P T T P X S T K G U D X J D D J X S E S S I G G X H D X T T T P D D T G I B G G D T S G T T H W W X F P A G H C F I D P X E S R P T T T P A D H F P G G J P A B X G P D T F P D G T R T A T P R D X H G X X T P T D W S T I D D D X G I D C J H T P B H B D P T D T C B U A X P I D P H S B T G

Bloco 4:

T Q O S P A S A F L E N E E F I A T D C O A T C A A Q O L R T L U E I D T O M I R M T D C A U O T S I R D M S O O O N T S S M T F S A I R E L A A A E C A T E L N L I U D T E N E I S S S E A L A L S E A N O D I E S B A M C L O A I O P O D N T L O S R E D C S I F Q D C A A T N X M D C A S A A A N M I D C L O A A A E E E A L T C G I R T O D D I A A A E I Q B I E D X E A A S U O E I E A U E F D C E I U D I R T O E R P U U E E M Q O A R U D M I U O C E S O S O N P I S V E N F L D Q U T O O P O D D S N P A Q D P O L I C C U U D N E T A A A A T P A E Q T E P S C

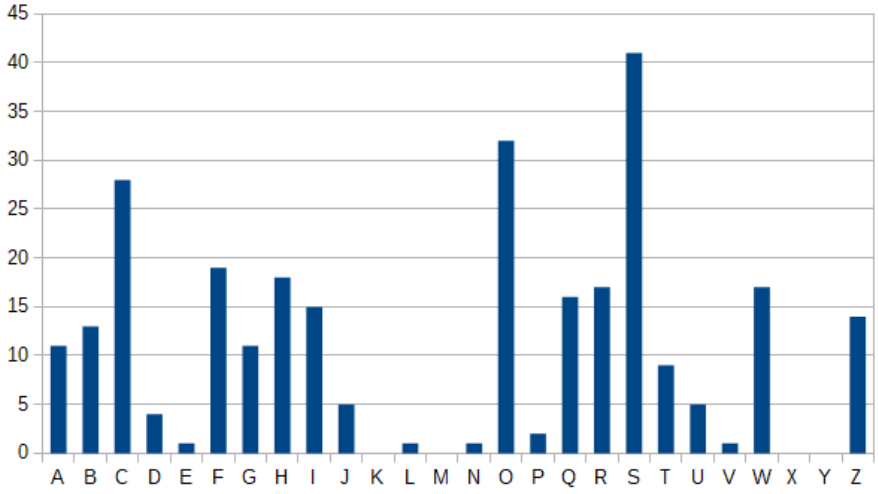
As Figuras 3 , 4 , 5 e 6 , trazem o gráfico obtido após a análise de frequência de cada letra em cada um dos blocos. Já a Figura 7 traz um gráfico com a frequência que cada letra aparece na língua portuguesa. Vejamos:

Figura 3 – Frequência das letras do bloco 1



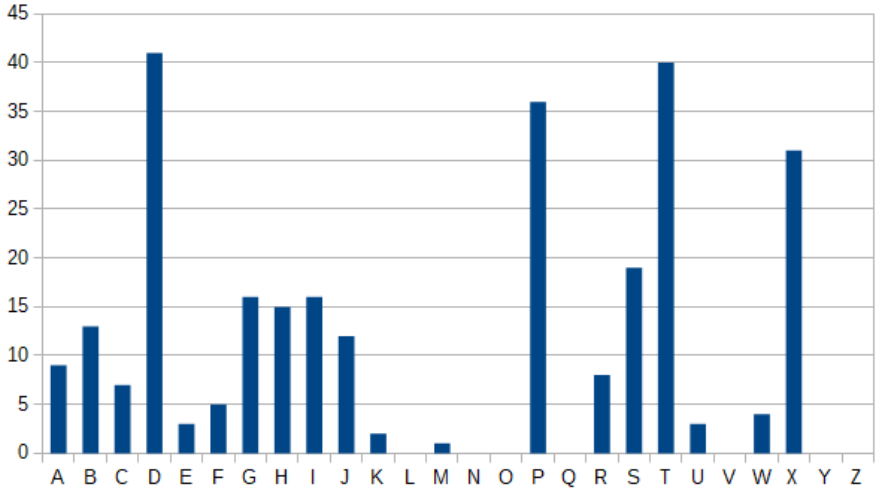
Fonte: Próprio autor.

Figura 4 – Frequência das letras do bloco 2



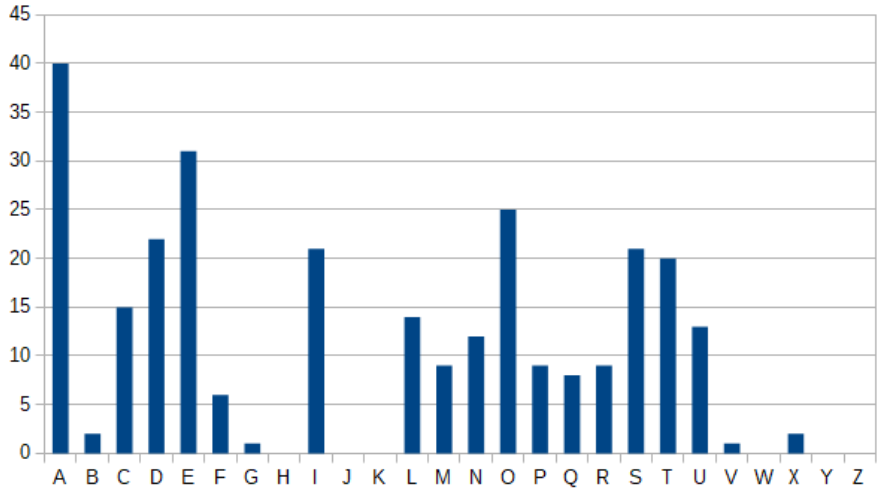
Fonte: Próprio autor.

Figura 5 – Frequência das letras do bloco 3



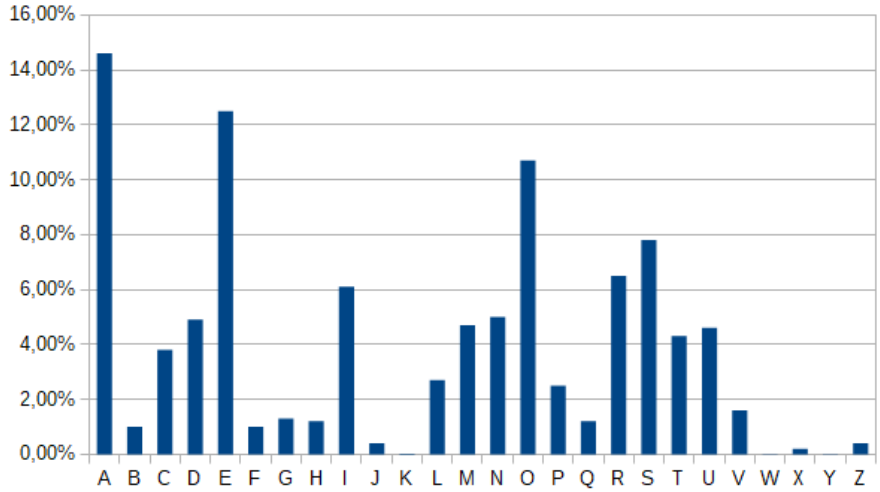
Fonte: Próprio autor.

Figura 6 – Frequência das letras do bloco 4



Fonte: Próprio autor.

Figura 7 – Frequência das letras na Língua Portuguesa



Fonte: Adaptado de Coutinho (2016).

Observe que as letras mais frequentes em um texto na Língua portuguesa são "a" e "e". Entres elas existem três letras, a primeira, letra "b", é pouco frequente, e as letras "c" e "d", bem mais frequentes que "b". Por conta da Cifra de Vigenère ser cíclica, devemos observar as letras antes do "a", são elas "v", "w", "y", "x" e "z", cinco letras pouquíssimo frequentes. Com isso, observe que no bloco 1, as letras mais frequentes são "C", "G", "K" e "Q", porém, as letras "C", "G" e "K" possuem três letras entre elas, o que sugere que uma delas representa a letra "a" e a subsequente representa a letra "e". Observando as cinco letras anteriores a "C", "G" e "K", apenas a letra "C" possui os cinco antecessores pouco frequentes. Portanto, concluímos que "**C**" deve representar "**a**". Logo, temos que a primeira letra da palavra-chave é "**C**". De modo análogo podemos identificar que as outras letras da palavra-chave são, respectivamente, "**O**", "**P**" e "**A**", formando assim a palavra "**COPA**".

De posse da palavra chave, pode-se identificar o texto original:

Muito daquilo que se lê pode apresentar dificuldade, mas não se deve confundir uma leitura difícil com uma leitura chata, com algo que foi mal escrito. Toda leitura de um livro, de um texto, de um artigo, traz um ponto de dificuldade, quando não temos familiaridade com o assunto. No começo do ano letivo se passa um texto de filosofia, de historia, de biologia, para que alguém faça uma leitura e há ali um nível de dificuldade alto. No entanto, se pedirmos a essa mesma pessoa que leia aquele mesmo texto ao final do ano, depois que vai se habituar com o vocabulário, vai ampliando o repertório de conceitos, ela não considera o texto difícil. Isso significa que a dificuldade não estava no texto em si. A dificuldade estava na rarefação, na diminuição de vocabulário ou da capacidade de interpretar aquilo. Isto é, o código de interpretação, o código de leitura estava mais restrito; o que é bem diferente do texto ser chato. Há coisas que são mal escritas, e aí não é que o texto fica difícil pela dificuldade de interpretação do leitor, mas porque o autor escreveu mal aquilo, de maneira truncada, com ideias que não são coerentes, ou com o estilo que não apreciamos. O livro se torna difícil à medida que eu não tenho todo o repertório de códigos de interpretação. Quando eu passo a tê-los, aí sim cresce em uma outra dimensão e ele torna-se mais fácil. A leitura, portanto, é uma questão de tempo e esforço.

Trata-se de um texto de Mário Sérgio Cortella, filósofo, professor e escritor brasileiro. ■

Após a segurança da cifra de Vigenère ser quebrada, em meados do século XIX ela continuou sendo utilizada, muitas vezes com algumas variações, por aqueles que queriam dificultar o entendimento de suas mensagens, mas era claro que havia a necessidade de produzir um sistema criptográfico seguro. Neste período utilizava-se muito o Telégrafo, um meio de comunicação rápido para curtas distâncias. Porém, para enviar uma mensagem por meio do telégrafo, era necessário repassar tal mensagem a um operador, um telegrafista. Os usuários tinham medo de que telegrafistas aceitassem suborno de pessoas interessadas no conteúdo das mensagens, com isso, era comum que as mensagens fossem criptografadas antes de serem repassadas aos telegrafistas.

Já na virada do século XIX, o físico italiano Guglielmo Marconi inventou o rádio, proporcionando uma comunicação muito mais rápida e em distâncias muito maiores, possibilitando assim uma maior comunicação entre os militares e consequentemente um maior número de mensagens interceptadas, já que qualquer um que estivesse na mesma frequência de rádio em que uma conversa estivesse ocorrendo poderia ouvi-la.

3.3 A ENIGMA

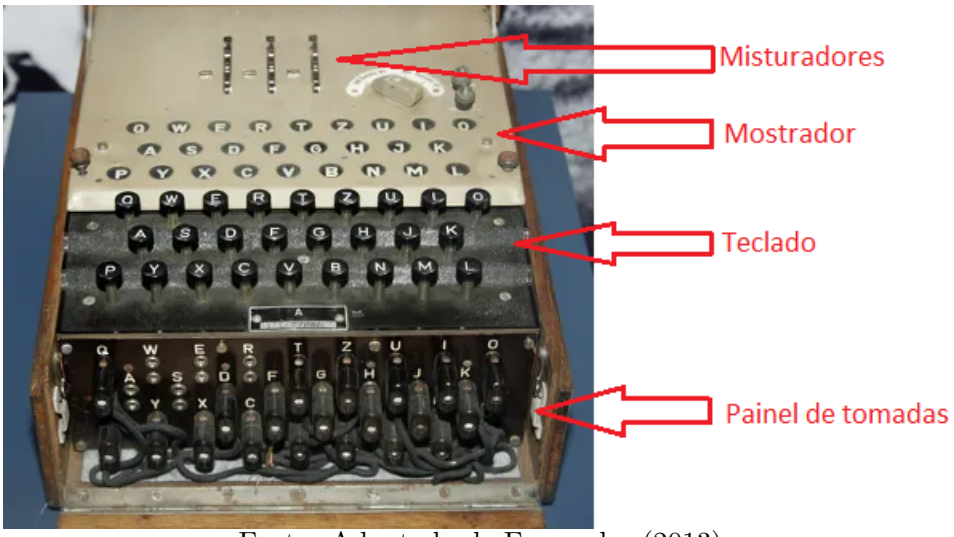
O rumo da Primeira guerra mundial foi mudado por conta de um Telegrama enviado pelo ministro das relações exteriores da Alemanha, Arthur Zimmermann, ao embaixador alemão em Washington onde planejavam atacar os Estados Unidos com a ajuda do México e do Japão. O "Telegrama Zimmermann" foi interceptado e decifrado

pelos ingleses que logo alertaram os Estados Unidos que tiveram de agir e entrar de vez na grande guerra.

Mesmo após o fim da Primeira guerra mundial, os ingleses continuaram interceptando e decifrando mensagens alemãs até que em 1926, passaram a não conseguir mais decifrar as mensagens interceptadas. O motivo era que os militares alemães passaram a utilizar a "Enigma" para encriptar suas mensagens.

A Enigma era uma máquina de criptografar mensagens com vários componentes engenhosos, como um teclado para digitar o texto de entrada, misturadores que giravam cada vez que seu usuário apertasse uma tecla, alterando a cifra utilizada, um painel de tomadas onde poderia trocar a fiação de uma letra por outra. Além disso existia um refletor que ajudava a decifrar uma mensagem e um mostrador que consistia em várias lâmpadas que indicavam a mensagem cifrada.

Figura 8 – Máquina Enigma



Fonte: Adaptado de Fernandes (2013).

Funcionava da seguinte maneira: ao apertar a letra "a" no teclado, o misturador girava e a transformava em uma outra letra, por exemplo, na letra "W" que aparecia no mostrador. Apertando novamente a letra "a", o misturador gira e a transforma em outra letra, diferente de "W" e que também apareceria no mostrador. Utilizando apenas um misturador, a máquina estaria sendo usada como a cifra de Vigenère. Por isso, a enigma possuía três misturadores, onde a chave utilizada nela seria a posição inicial de cada misturador. Por exemplo, a chave "KJU" indica que o primeiro misturador deve ser posicionado inicialmente com a letra "K", o segundo com a letra "J" e o terceiro com a letra "U". No painel de tomadas poderia ser trocada uma letra por outra, como por exemplo, ao trocar "s" por "g", ao teclar em "s" a máquina entenderia que a letra digitada na verdade era "g". Além disso, cada misturador poderia ser usado em qualquer uma das três posições.

A Enigma foi inventada por Arthur Scherbius, um inventor alemão, em 1918.

Tratava-se de uma máquina pequena, semelhante a uma máquina de datilografar. Scherbius cobrava caro por uma Enigma, sendo este o principal motivo para que vendesse pouco para civis e comerciantes. Porém, nas duas décadas seguintes os militares alemães compraram cerca de 30 mil máquinas enigma adaptadas para o uso militar, que dispunham de 5 misturadores onde poderiam escolher um arranjo de 3 deles para usar. Com a Enigma os militares alemães tinham o mais seguro sistema criptográfico do mundo.

Afim de conseguir quebrar o novo sistema de cifragem alemão, o governo inglês criou uma nova organização para quebra de códigos em Buckinghamshire e que ficou conhecida como Bletchley Park. Na organização trabalhavam pessoas com diversas especialidades como linguistas, enxadristas, matemáticos, cientistas e pessoas boas em resolver palavras cruzadas. Dentre eles precisamos destacar Alan Turing, um matemático brilhante que trabalhava como professor em Cambridge e em 1839 foi convidado para Bletchley Park.

A principal função de Bletchley Park era decifrar a Enigma, para isso era necessário encontrar a chave diária utilizada pelos Alemães. Analisando mensagens decifradas anteriormente, Turing percebeu que era possível decifrar parte de uma mensagem encriptada alemã considerando a hora e o local de onde aquela mensagem foi enviada. Por exemplo, todos os dias após as 6 horas da manhã os alemães enviavam relatórios sobre a previsão do tempo. Portanto, era muito provável que naquela mensagem tivesse a palavra "**wetter**" que significa "tempo". Essas palavras eram conhecidas como "colas". Com isso, identificando o local exato em que a cola estivesse no texto cifrado, Turing conseguia encontrar a sequência de seis letras que representava a palavra-cola "**wetter**", sendo assim, cada letra da palavra cifrada tinha uma ligação com cada letra da palavra original. Dessa forma, Turing precisava encontrar qual configuração da máquina estabeleceria o elo entre "wetter" e o código que o representara. Para isso, Turing desenvolveu uma máquina conhecida como "bomba", que tinha o propósito de encontrar tal configuração.

A primeira bomba de Turing chegou a Bletchley Park em março de 1940 e foi apelidada de "Victory". Consistia em 12 conjuntos de misturadores Enigma que buscavam encontrar os elos. Turing continuou trabalhando para aperfeiçoar o projeto de sua bomba até que em Agosto do mesmo ano chegou a Bletchley Park uma nova bomba, a "Agnes". Dezoito meses depois Bletchley Park contava com mais de 15 bombas que funcionando em perfeito estado encontravam a chave diária da enigma em aproximadamente uma hora, possibilitando assim, a leitura de todas as mensagens alemãs interceptadas no mesmo dia. Já no fim de 1942 haviam 49 bombas em Bletchley Park e uma nova estação de bombas foi inaugurada ao norte de Bletchley.

A enigma utilizada pela marinha alemã era mais moderna e consequentemente mais difícil de ser decifrada, uma vez que seus operadores dispunham de oito misturadores ao invés de cinco, e de um refletor que poderia ser colocado em 26 posições distintas. Contudo, era possível decifrá-la com a ajuda das colas. Bletchley Park também decifrou

mensagens de outros rivais como o México e o Japão.

O que era feito em Buckinghamshire era secreto e minucioso, em um trabalho de inteligência os ingleses utilizavam do que Bletchley descobria para estrategicamente conquistar vitórias na guerra sem que os nazistas percebessem que a Enigma havia sido decifrada. Os alemães até levantaram essa hipótese, porém, para eles era impossível que a Enigma tivesse sido vencida. Com isso, historiadores afirmam que a segunda grande guerra foi encurtada aproximadamente 2 anos.

Apesar da importância do trabalho de todos aqueles que estiveram em Bletchley Park, alguns deles nunca tiveram o devido reconhecimento, já que apenas em 1970 o segredo sobre Bletchley Park foi revelado. Alan Turing, por exemplo, que após a guerra passou a trabalhar em pesquisas sobre o desenvolvimento do computador, foi impedido de fazer suas pesquisas em 1952 após ter sido descoberta sua homossexualidade, bem como foi obrigado a passar por um processo de castração química o que o levou a cometer suicídio dois anos mais tarde.

Observação 3.2 As histórias apresentadas neste Capítulo, bem como outras histórias a respeito da Criptografia podem ser encontradas em Singh(2020).

3.4 O PROBLEMA DO LOGARITMO DISCRETO

A segurança de alguns criptossistemas de chave pública depende da dificuldade de resolver o problema do logaritmo discreto. Portanto, precisamos abordá-lo aqui.

Definição 3.1 *Seja p um número primo e $a, b \in \mathbb{Z}$ tais que $a \not\equiv 0 \mod p$ e $b \not\equiv 0 \mod p$. Se existe k tal que $a^k \equiv b \mod p$, o problema do logaritmo discreto é encontrar k. Dizemos que o logaritmo discreto de b na base a é o inteiro k não negativo que obedece $a^k \equiv b \mod p$.*

Como pelo Pequeno Teorema de Fermat temos que $a^{p-1} \equiv 1 \mod p$, então para todo inteiro s, $a^{k+s(p-1)}$ também é côngruo a b módulo p. Vejamos:

$$a^{k+s(p-1)} \equiv a^k \cdot (a^{p-1})^s \equiv b \cdot 1^s \equiv b \cdot 1 \equiv b \mod p.$$

Por exemplo, temos que

$$3^3 \equiv 3^{3+4} \equiv 3^{3+2\cdot 4} \equiv 3^{3+s\cdot 4} \equiv 2 \mod 5.$$

Portanto, existem infinitos valores possíveis para k.

É importante destacar que, diferentemente do logaritmo contínuo definido nos reais ou complexos, o logaritmo discreto se comporta de maneira aleatória módulo p.

Exemplo 3.4 *Seja* $a = 5$ *e* $p = 7$, *obtemos as seguintes congruências:*

$$\begin{aligned}
5^0 &\equiv 1 \mod 7;\\
5^1 &\equiv 5 \mod 7;\\
5^2 &\equiv 4 \mod 7;\\
5^3 &\equiv 6 \mod 7;\\
5^4 &\equiv 2 \mod 7;\\
5^5 &\equiv 3 \mod 7;\\
5^6 &\equiv 1 \mod 7;\\
5^7 &\equiv 5 \mod 7;\\
5^8 &\equiv 4 \mod 7;\\
5^9 &\equiv 6 \mod 7;\\
&\vdots
\end{aligned}$$

Observe que as potências de 5 *módulo* 7 *geraram todos os inteiros não nulos e não negativo menores que* 7, *em casos assim, dizemos que o número* 5 *é um elemento primitivo módulo* 7. *Além disso, podemos observar que tais inteiros foram aparecendo de forma aleatória.*

O Problema do logaritmo discreto se encaixa na categoria de problemas "P versus NP", que está na lista dos "Problemas do prêmio Millenium" que oferece um milhão de dólares para quem encontrar uma forma mais "simples" de resolvê-lo.

Uma das maneiras de tentar resolver este problema é fazendo diversas tentativas, testando todos os valores possíveis para k. Tal método pode ser bastante exaustivo e até mesmo impraticável, uma vez que a resposta para k pode ser um inteiro com centenas de dígitos, o que é comumente usado nos sistemas criptográficos. Por isso, foram feitas várias tentativas de ataques ao Problema do logaritmo discreto como os métodos de Pollard e de Pohlig-Hellman, dentre outros, que podem ser vistos em Washington (2008). Nenhum deles encontrou uma forma fácil e rápida de resolver o Problema do logaritmo discreto. Vejamos agora como funciona o algoritmo "Passo de bebê, passo de gigante" que pode ser encontrado em Coron, Lefran e Poupard (2005) de uma outra forma.

Dado um corpo $\mathbb{Z}_n$, seja $m = \lceil \sqrt{n-1} \rceil$ a parte inteira de $\sqrt{n-1}$. Para algum $v \in \mathbb{Z}_n$, temos que $k = \log_g v < n$, então podemos afirmar que $k = a + bm,\ a, b < m$. Com isso, de $v = g^{\log_g v}$ temos que $v = g^{a+bm}$, obtendo assim,

$$g^a = vg^{-bm}.$$

Sendo assim, fazemos as duas listas a seguir:

$$(1, g, g^2, \ldots, g^{m-2}, g^{m-1})$$

e

$$(v, vg^{-m}, vg^{-2m}, \ldots, vg^{-(m-2)m}, vg^{-(m-1)m}).$$

Fazemos a primeira lista e em seguida fazemos a segunda, iniciando do primeiro elemento e partindo pro elemento seguinte se houver necessidade, pois podemos parar assim que encontrarmos um par $(g^{a_i}, vg^{-b_j m})$ tal que $g^{a_i} = vg^{-b_j m}$. O valor k é obtido ao usar a_i **e** b_j e calcular $k = a_i + b_j m$.

Exemplo 3.5 *Calcule o valor* $x \in \mathbb{Z}_{23}$, *tal que* $8^x = 16$.

Solução: Neste caso, utilizando o algoritmo "Passo de bebê, passo de gigante" temos que $m = \lceil \sqrt{23-1} \rceil = 4$, $v = 16$ e $g = 8$. Para fazer a primeira lista, devemos encontrar os valores g, g^2 e g^3 módulo 23. Para formar a segunda lista, precisamos encontrar os valores de v, vg^{-4}, vg^{-8} e vg^{-12} também módulo 23.

Como $g = 8$, temos que

$$g \equiv 8 \mod 23 \Rightarrow g^2 = 8^2 = 64 \equiv 18 \mod 23 \Rightarrow$$

$$\Rightarrow g^3 = 8^3 = 8^2 \cdot 8 \equiv 18 \cdot 8 = 144 \equiv 6 \mod 23.$$

Logo, a primeira lista fica da seguinte forma:

$$(1, 8, 18, 6).$$

Como $v = 16$ e $g = 8$, temos que $v \equiv 16 \mod 23$, e

$$\begin{aligned}
vg^{-4} = 16 \cdot 8^{-4} &\equiv 16 \cdot 8^{-4} \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv 16 \cdot 8^{-4} \cdot 1 \cdot 1 \cdot 1 \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv 16 \cdot 8^{-4} \cdot 24 \cdot 24 \cdot 24 \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv 16 \cdot 8^{-4} \cdot 24^3 \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv (8 \cdot 2) \cdot 8^{-4} \cdot (8 \cdot 3)^3 \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv 8^1 \cdot 2 \cdot 8^{-4} \cdot 8^3 \cdot 3^3 \mod 23 \\
vg^{-4} = 16 \cdot 8^{-4} &\equiv 2 \cdot 3^3 \equiv 2 \cdot 27 \equiv 2 \cdot 4 \equiv 8 \mod 23.
\end{aligned}$$

Já que 8 está presente na primeira lista, podemos parar por aqui, porém irei concluir a segunda lista.

Efetuando novos cálculos, obtemos

$$\begin{aligned}
vg^{-8} = 16 \cdot 8^{-8} &\equiv 16 \cdot 8^{-8} \mod 23 \\
vg^{-8} = 16 \cdot 8^{-8} &\equiv 16 \cdot 8^{-8} \cdot 24^7 \mod 23 \\
vg^{-8} = 16 \cdot 8^{-8} &\equiv (8 \cdot 2) \cdot 8^{-8} \cdot (8 \cdot 3)^7 \mod 23
\end{aligned}$$

$$\begin{aligned} vg^{-8} = 16 \cdot 8^{-8} &\equiv 8^1 \cdot 2 \cdot 8^{-8} \cdot 8^7 \cdot 3^7 \mod 23 \\ vg^{-8} = 16 \cdot 8^{-8} &\equiv 2 \cdot (3^3)^2 \cdot 3 \mod 23 \\ vg^{-8} = 16 \cdot 8^{-8} &\equiv 2 \cdot 4^2 \cdot 3 \mod 23 \\ vg^{-8} = 16 \cdot 8^{-8} &\equiv 2 \cdot 48 \equiv 2 \cdot 2 \equiv 4 \mod 23. \end{aligned}$$

Temos ainda que

$$\begin{aligned} vg^{-12} = 16 \cdot 8^{-12} &\equiv 16 \cdot 8^{-12} \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv 16 \cdot 8^{-12} \cdot 24^{11} \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv (8 \cdot 2) \cdot 8^{-12} \cdot (8 \cdot 3)^{11} \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv 8^1 \cdot 2 \cdot 8^{-12} \cdot 8^{11} \cdot 3^{11} \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv 2 \cdot 3^7 \cdot 3^3 \cdot 3 \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv 2 \cdot 2 \cdot 4 \cdot 3 \mod 23 \\ vg^{-12} = 16 \cdot 8^{-12} &\equiv 48 \equiv 2 \mod 23. \end{aligned}$$

Com isso, nossa segunda lista fica

$$(16, 8, 4, 2).$$

Sendo assim, temos o par $(g^1, vg^{-(1)\cdot 4}) \Rightarrow a_0 = 1$ e $-b_0 = 1$. Logo,

$$x = 1 + 1 \cdot 4 = 5.$$

■

3.5 TROCA DE CHAVES DIFFIE-HELLMAN

Desde que Alice pretende enviar uma mensagem a Bob de modo que Eva não possa saber do conteúdo desta mensagem, eles precisam trocar uma chave secreta afim de que consigam codificar e decodificar tal mensagem, para isso, precisam se encontrar fisicamente ou enviar a chave secreta um para o outro por meio de terceiros, o que diminui a segurança da criptografia. A dificuldade de resolver o Problema do logaritmo discreto deu a Whitfield Diffie e Martin Hellman a possibilidade de elaborar um sistema de criação de chave em que o emissor e o receptor de uma mensagem secreta não precisam se encontrar para realizar a troca dessa chave. O sistema funciona da seguinte forma:

1. Alice e Bob concordam em dois valores não secretos, Y e p.
2. Alice escolhe um valor secreto A e Bob escolhe um valor secreto B.
3. Alice e Bob encontram, respectivamente os valores α e β calculando, respectivamente, $Y^A \equiv \alpha \mod p$ e $Y^B \equiv \beta \mod p$ e os enviam um para o outro.

4. Com os valores de β e α em mãos, Alice e Bob calculam, respectivamente, os valores β^A módulo p e α^B módulo p, encontrando assim o mesmo valor C, que é a chave que será usada para criptografar a mensagem a ser escondida.

Uma vez que A e B são secretos, por mais que a intrusa Eva consiga os valores de Y, p, α e β, ela precisaria encontrar o valor de β^A módulo p ou α^B módulo p para encontrar a chave C. Como Eva não conhece A e B, a menos que ela consiga resolver o Problema do logaritmo discreto de forma rápida, ela terá muito trabalho até conseguir encontrar a chave C. Diffie e Hellman desenvolveram um sistema eficiente e que funcionava, porém, não era perfeito.

Exemplo 3.6 *Vejamos uma situação de Troca de chaves Diffie-Hellman realizada por Alice e Bob:*

1. *Alice e Bob concordam nos valores* $Y = 7$ *e* $p = 17$.
2. *Alice escolhe* $A = 4$ *e Bob escolhe* $B = 9$ *como seus valores secretos.*
3. *Alice calcula* 7^4 *módulo* 13, *encontrando* $\alpha = 4$ *e Bob calcula* 7^9 *módulo* 13, *encontrando* $\beta = 10$ *e os enviam um para o outro.*
4. *Agora Alice calcula* 10^4 *módulo* 13 *encontrando* $C = 4$, *e Bob calcula* 4^9 *módulo* 13 *encontrando também* $C = 4$.

   Sendo assim, Alice e Bob possuem uma chave segura para criptografar uma mensagem e não precisaram se encontrar fisicamente para isso.

4 CRIPTOGRAFIA RSA

Apesar de Diffie e Hellman conseguirem desenvolver um sistema de troca de chaves em que não era necessário o encontro físico entre Emissor e Receptor, isso ainda não era suficiente para um sistema criptográfico perfeito, existia a necessidade de um emissor enviar uma mensagem secreta para um receptor a qualquer momento, sem que fosse necessário que ambos concordassem em alguns parâmetros para a criação de uma chave secreta, um sistema assimétrico, onde é possível a utilização de uma chave que pudesse ser de domínio público para criptografar uma mensagem, porém, para descriptografar, é necessário uma chave secreta que apenas o receptor da mensagem conhece. Com isso, eles continuaram suas pesquisas para desenvolver tal sistema.

Apesar dos esforços de Diffie e Hellman em encontrar um sistema assimétrico, segundo Sautoy (2007), os primeiros a encontrarem tal sistema foram Ron Rivest, Adi Shamir e Leonard Adleman, três pesquisadores do Instituto de tecnologia de Massachusetts (MIT), que desenvolveram o mais utilizado sistema de criptografia atualmente, o RSA, que é assim denominado por conta das iniciais dos nomes de seus desenvolvedores.

A seguir vamos descrever a mecânica utilizada na cifragem e decifragem da criptografia RSA:

Vamos imaginar a seguinte situação: Bob, um agente secreto especial, recebe todo mês de sua superior Alice, uma mensagem com o nome de uma pessoa que deve ser recrutada. Seus inimigos tentam a todo custo interceptar e decifrar a mensagem enviada para Bob, de forma a evitar o sucesso da missão.

Com intenção de dificultar o entendimento do conteúdo da mensagem, Bob e Alice optam pelo uso da criptografia RSA. Para isso, Bob deve escolher dois números primos grandes p e q e mantê-los em segredo. Quão maiores forem os primos p e q, maior será a segurança da cifragem, porém, para facilitar o entendimento, vamos supor que Bob escolheu os primos $p = 7$ e $q = 11$.

Em seguida, Bob multiplica os primos escolhidos, obtendo o valor N. Neste caso, $N = pq = 7 \cdot 11 = 77$. Bob deve escolher um número e tal que $mdc(e, \varphi(N)) = 1$. Como $\varphi(N) = (p-1)(q-1) = 6 \cdot 10 = 60$, então o valor de e escolhido é o número 7, que é o menor primo que não divide $\varphi(N) = 60$. O par N e e que nesse caso são, respectivamente, 77 e 7, é a chave pública de Bob, que deve ser disponibilizada em algum lugar público, como em uma lista telefônica ou nos classificados de um jornal impresso, de modo que Alice tenha acesso.

Agora Alice deve codificar a mensagem utilizando a chave pública que Bob deixou disponível. Primeiramente, Alice deve converter a mensagem em um número, esse passo é chamado por Coutinho (2011) de pré-codificação. Por exemplo, transformar a mensagem em dígitos decimais ASCII. Sendo assim, se Alice quer enviar o nome “MARIA” a Bob, ela deve transformar o nome “MARIA” em dígitos decimais da Tabela ASCII, que

pode ser vista na Figura 9. Temos a seguir cada letra do nome MARIA seguida de sua representação decimal ASCII: M = 77; A = 65; R = 82; I = 73; A = 65. Dessa forma, a pré-codificação de MARIA é o número 7765827365.

Observação 4.1 A Tabela American Standard Code for Information Interchange (ASCII) abaixo é muito usada pela indústria de computadores para a troca de informações. Alguns caracteres são representados na forma de um número binário, decimal ou até mesmo hexadecimal. Ela foi criada para padronizar a representação de caracteres alfanuméricos em computadores. A tabela ASCII original possui 128 caracteres, distribuídos em códigos de 0 a 127. Na tabela abaixo podemos ver os caracteres representados pelos números de 32 a 127. O número 32 representa o "espaço em branco" e o caractere 127 varia de computador para computador. Os demais, de 0 a 31, são funções de controle, ou seja, de algum comando que a impressora ou monitor de vídeo deve executar, como por exemplo, pular uma linha ou voltar um caractere. Sendo assim, quando você digita a letra "**W**" no seu teclado, o seu computador armazena em sua memória o número "**87**". A evolução dos códigos utilizados para caracteres pode ser vista no artigo (FISCHER, 2015).

Figura 9 – Tabela ASCII

032	! 033	" 034	# 035	$ 036	% 037	& 038	’ 039
(040	) 041	* 042	+ 043	, 044	- 045	. 046	/ 047
0 048	1 049	2 050	3 051	4 052	5 053	6 054	7 055
8 056	9 057	: 058	; 059	< 060	= 061	> 062	? 063
@ 064	A 065	B 066	C 067	D 068	E 069	F 070	G 071
H 072	I 073	J 074	K 075	L 076	M 077	N 078	O 079
P 080	Q 081	R 082	S 083	T 084	U 085	V 086	W 087
X 088	Y 089	Z 090	[091	\ 092	] 093	^ 094	_ 095
‘ 096	a 097	b 098	c 099	d 100	e 101	f 102	g 103
h 104	i 105	j 106	k 107	l 108	m 109	n 110	o 111
p 112	q 113	r 114	s 115	t 116	u 117	v 118	w 119
x 120	y 121	z 122	{ 123	| 124	} 125	~ 126	127

Fonte: Morimoto e Hashimoto (2010).

Após a pré-codificação, Alice deve separar os algarismos do número obtido em blocos de números menores, de forma que o número de cada bloco seja menor do que N e que não comece por zero. Fazendo isso, Alice obtém os blocos $7-76-58-27-36-5$. Chamaremos cada bloco de b_i, $i \in \mathbb{N}$.

Agora Alice deve codificar cada bloco, obtendo assim um valor $c(b_i)$ que é igual ao resto da divisão de $(b_i)^e$ por N. Ou seja, $(b_i)^e \equiv c(b_i) \mod N$. Calcular isso de forma direta numa calculadora não é tão simples por conta da quantidade de dígitos, porém utilizando as propriedades da aritmética modular, conseguimos realizar tais cálculos.

Os blocos a serem codificados são os seguintes: $b_1 = 7$, $b_2 = 76$, $b_3 = 58$, $b_4 = 27$, $b_5 = 36$ e $b_6 = 5$. Vamos codificá-los:

- Codificando $b_1 = 7$: Temos que

$$\begin{aligned} 7 &\equiv 7 \mod 77 \\ 7^3 &\equiv 7^3 \equiv 343 \equiv 35 \mod 77 \\ 7^6 &\equiv (7^3)^2 \equiv 35^2 \equiv 1\,225 \equiv 70 \mod 77 \\ 7^7 &\equiv 7^6 \cdot 7 \equiv 70.7 \equiv 490 \equiv 28 \mod 77. \end{aligned}$$

  Portanto, $c(b_1) = 28$.

- Codificando $b_2 = 76$: Temos que

$$\begin{aligned} 76 &\equiv 76 \mod 77 \\ 76^3 &\equiv 76^3 \equiv 438\,976 \equiv 76 \mod 77 \\ 76^6 &\equiv (76^3)^2 \equiv 76^2 \equiv 5\,776 \equiv 1 \mod 77 \\ 76^7 &\equiv 76^6 \cdot 76 \equiv 1.76 \equiv 76 \mod 77. \end{aligned}$$

  Portanto, $c(b_2) = 76$.

- Codificando $b_3 = 58$: Temos que

$$\begin{aligned} 58 &\equiv 58 \mod 77 \\ 58^3 &\equiv 58^3 \equiv 195\,112 \equiv 71 \mod 77 \\ 58^6 &\equiv (58^3)^2 \equiv 71^2 \equiv 5\,041 \equiv 36 \mod 77 \\ 58^7 &\equiv 58^6 \cdot 58 \equiv 36.58 \equiv 2\,088 \equiv 9 \mod 77. \end{aligned}$$

  Portanto, $c(b_3) = 9$.

- Codificando $b_4 = 27$: Temos que

$$\begin{aligned} 27 &\equiv 27 \mod 77 \\ 27^3 &\equiv 27^3 \equiv 19\,683 \equiv 48 \mod 77 \\ 27^6 &\equiv (27^3)^2 \equiv 48^2 \equiv 2\,304 \equiv 71 \mod 77 \\ 27^7 &\equiv 27^6 \cdot 27 \equiv 71.27 \equiv 1\,917 \equiv 69 \mod 77. \end{aligned}$$

  Portanto, $c(b_4) = 69$.

- Codificando $b_5 = 36$: Temos que

$$\begin{aligned} 36 &\equiv 36 \mod 77 \\ 36^3 &\equiv 36^3 \equiv 46\,656 \equiv 71 \mod 77 \\ 36^6 &\equiv (36^3)^2 \equiv 71^2 \equiv 5\,041 \equiv 36 \mod 77 \\ 36^7 &\equiv 36^6 \cdot 36 \equiv 36.36 \equiv 1\,296 \equiv 64 \mod 77. \end{aligned}$$

  Portanto, $c(b_5) = 64$.
- Codificando $b_6 = 5$: Temos que

$$\begin{aligned} 5 &\equiv 5 \mod 77 \\ 5^3 &\equiv 5^3 \equiv 125 \equiv 48 \mod 77 \\ 5^6 &\equiv (5^3)^2 \equiv 48^2 \equiv 2\,304 \equiv 71 \mod 77 \\ 5^7 &\equiv 5^6 \cdot 5 \equiv 71.5 \equiv 355 \equiv 47 \mod 77. \end{aligned}$$

  Portanto, $c(b_6) = 47$.

Os blocos cifrados enviados para Bob são : $28 - 76 - 9 - 69 - 64 - 47$.

Bob recebe a mensagem cifrada e de posse de sua chave pessoal secreta inicia o processo de decodificação para compreender o conteúdo da mensagem. Para isso, deve formar sua chave pessoal de decodificação, encontrando um número d tal que

$$d \cdot e \equiv 1 \mod \varphi(N).$$

Nesse caso, $d \cdot 7 \equiv 1 \mod 60$. Ou seja, Bob deve encontrar o inverso multiplicativo de 7 módulo 60, o que pode ser feito utilizando o Algoritmo de Euclides Estendido. Vejamos:

$$60 = 7 \cdot 8 + 4 \tag{18}$$

$$7 = 4 \cdot 1 + 3 \tag{19}$$

$$4 = 3 \cdot 1 + 1 \tag{20}$$

Como $1 \mid 3$, então $mdc(60, 7) = 1$. De (20) obtemos

$$4 - 3 = 1. \tag{21}$$

De (19) obtemos $7 - 4 \cdot 1 = 3$, que ao substituirmos em (21) resulta em

$$4 - (7 - 4 \cdot 1) = 1. \tag{22}$$

De (18) obtemos $4 = 60 - 7 \cdot 8$, que ao substituirmos em (22) resulta em

$$60 - 7 \cdot 8 - (7 - (60 - 7 \cdot 8) \cdot 1) = 1$$

$$-17 \cdot 7 + 2 \cdot 60 = 1 \tag{23}$$

Aplicando módulo em (23) temos:

$$\begin{aligned}
-17 \cdot 7 + 2 \cdot 60 &\equiv 1 \mod 60 \\
-17 \cdot 7 &\equiv 1 \mod 60 \\
(-17 \cdot 7)^2 &\equiv 1^2 \mod 60 \\
289 \cdot 7 \cdot 7 &\equiv 1 \mod 60 \\
2023 \cdot 7 &\equiv 1 \mod 60 \\
(60 \cdot 33 + 43) \cdot 7 &\equiv 1 \mod 60 \\
60 \cdot 33 \cdot 7 + 43 \cdot 7 &\equiv 1 \mod 60 \\
43 \cdot 7 &\equiv 1 \mod 60.
\end{aligned}$$

Com isso, temos que 43 é o inverso multiplicativo de 7 módulo 60. Logo, $d = 43$. Portanto, a chave pessoal secreta de João é o par N e d, que nesse caso são, respectivamente, 77 e 43. O valor de cada bloco b_i, é o resto da divisão de $[c(b_i)]^d$ por N. Ou seja,

$$[c(b_i)]^d \equiv b \mod N.$$

Vamos iniciar a decodificação dos blocos que Bob recebeu:

- Decodificando $c(b_1) = 28$: Temos que

$$\begin{aligned}
28 &\equiv 28 \mod 77 \\
28^6 &\equiv 28^6 \equiv 481\ 890\ 304 \equiv 49 \mod 77 \\
28^{30} &\equiv (28^6)^5 \equiv 49^5 \equiv 282\ 475\ 249 \equiv 56 \mod 77 \\
28^{42} &\equiv 28^{30} \cdot 28^6 \cdot 28^6 \equiv 56 \cdot 49 \cdot 49 \equiv 134\ 456 \equiv 14 \mod 77 \\
28^{43} &\equiv 28^{42} \cdot 28 \equiv 14 \cdot 28 \equiv 392 \equiv 7 \mod 77.
\end{aligned}$$

  Portanto, $b_1 = 7$.

- Decodificando $c(b_2) = 76$: Temos que

$$\begin{aligned}
76 &\equiv 76 \mod 77 \\
76^4 &\equiv 76^4 \equiv 33\ 362\ 176 \equiv 1 \mod 77 \\
76^{40} &\equiv (76^4)^{10} \equiv 1^{10} \equiv 1 \mod 77 \\
76^{43} &\equiv 76^{40} \cdot 76^3 \equiv 1 \cdot 76^3 \equiv 76^3 \equiv 438\ 976 \equiv 76 \mod 77.
\end{aligned}$$

Portanto, $b_2 = 76$.

- Decodificando $c(b_3) = 9$: Temos que

$$\begin{aligned} 9 &\equiv 9 \mod 77 \\ 9^9 &\equiv 9^9 \equiv 387\,420\,489 \equiv 71 \mod 77 \\ 9^{36} &\equiv (9^9)^4 \equiv 71^4 \equiv 25\,411\,681 \equiv 64 \mod 77 \\ 9^{43} &\equiv 9^{36} \cdot 9^7 \equiv 64 \cdot 4\,782\,969 \equiv 306\,110\,016 \equiv 58 \mod 77. \end{aligned}$$

Portanto, $b_3 = 58$.

- Decodificando $c(b_4) = 69$: Temos que

$$\begin{aligned} 69 &\equiv 69 \mod 77 \\ 69^4 &\equiv 69^4 \equiv 22\,667\,121 \equiv 15 \mod 77 \\ 69^{28} &\equiv (69^4)^7 \equiv 15^7 \equiv 170\,859\,375 \equiv 71 \mod 77 \\ 69^{40} &\equiv 69^{28} \cdot (69^4)^3 \equiv 71 \cdot 15^3 \equiv 239\,625 \equiv 1 \mod 77 \\ 69^{43} &\equiv 69^{40} \cdot 69^3 \equiv 1 \cdot 69^3 \equiv 69^3 \equiv 328\,509 \equiv 27 \mod 77. \end{aligned}$$

Portanto, $b_4 = 27$.

- Decodificando $c(b_5) = 64$: Temos que

$$\begin{aligned} 64 &\equiv 64 \mod 77 \\ 64^4 &\equiv 64^4 \equiv 16\,777\,216 \equiv 71 \mod 77 \\ 64^{16} &\equiv (64^4)^4 \equiv 71^4 \equiv 25\,411\,681 \equiv 64 \mod 77 \\ 64^{21} &\equiv 64^{16} \cdot 69^4 \cdot 64 \equiv 64 \cdot 71 \cdot 64 \equiv 290\,816 \equiv 64 \mod 77 \\ 64^{43} &\equiv (64^{21})^2 \cdot 64 \equiv 64^2 \cdot 64 \equiv 64^3 \equiv 262\,144 \equiv 36 \mod 77. \end{aligned}$$

Portanto, $b_5 = 36$.

- Decodificando $c(b_6) = 47$: Temos que

$$\begin{aligned} 47 &\equiv 47 \mod 77 \\ 47^5 &\equiv 47^5 \equiv 229\,345\,007 \equiv 45 \mod 77 \\ 47^{21} &\equiv (47^5)^4 \cdot 47 \equiv 45^4 \cdot 47 \equiv 4\,100\,625 \cdot 47 \equiv 192\,729\,375 \equiv 69 \mod 77 \\ 47^{43} &\equiv (47^{21})^2 \cdot 47 \equiv 69^2 \cdot 47 \equiv 4\,761 \cdot 47 \equiv 223\,767 \equiv 5 \mod 77. \end{aligned}$$

Portanto, $b_6 = 5$.

Dessa forma, a mensagem decodificada por Bob é 7765827365 que após usar a ASCII pode ser lida como MARIA.

4.1 POR QUÊ O RSA FUNCIONA?

Primeiramente, Bob escolheu dois primos p e q, calculou $N = pq$, divulgou N mas deixou p e q em sigilo. Em seguida, Bob escolheu um valor e, com a restrição de que $mdc(e, \varphi(N))$ seja 1 e também o divulgou. (Lembrando que $\varphi(N) = (p-1)(q-1)$.)

Alice, de posse do par N e e, que é a chave pública de Bob, codificou cada bloco b_i, obtendo o código $c(b_i)$, onde $c(b_i) \equiv (b_i)^e \mod N$. Em seguida, Alice enviou cada bloco $c(b_i)$ para Bob.

Para que Bob entenda a mensagem, ele deve decodificar $c(b_i)$, ou seja, encontrar b_i tal que $c(b_i) \equiv (b_i)^e \mod N$. Para isso, Bob precisa encontrar um número d tal que $de \equiv 1 \mod \varphi(N)$. Como apenas Bob conhece os valores p e q, então apenas ele conhece $\varphi(N)$. Sendo assim, Bob é o único capaz de encontrar o valor de d, que faz parte de sua chave de decodificação.

Observe que

$$de \equiv 1 \mod \varphi(N) \Rightarrow de - 1 = k\varphi(N) = k(p-1)(q-1),\ k \in \mathbb{Z}.$$

Portanto,

$$de = 1 + k(p-1)(q-1) \Rightarrow X^{de} = (b_i)^1[(b_i)^{k(q-1)(p-1)}] \Rightarrow$$

$$\Rightarrow [(b_i)^e]^d = (b_i)^1[(b_i)^{k(q-1)}]^{p-1} \text{ ou } [(b_i)^e]^d = (b_i)^1[(b_i)^{k(p-1)}]^{q-1}.$$

Sabemos que $b_i \equiv b_i \mod p$ e $b_i \equiv b_i \mod q$. Além disso, p e q são primos, então, pelo Corolário 2.5 do Teorema 2.8, obtemos

$$[(b_i)^{k(q-1)}]^{p-1} \equiv 1 \mod p \text{ e } [(b_i)^{k(p-1)}]^{q-1} \equiv 1 \mod q.$$

Logo, temos que

$$[(b_i)^e]^d = (b_i)^1[(b_i)^{k(q-1)}]^{p-1} \equiv b_i \mod p \text{ e } [(b_i)^e]^d = (b_i)^1[(b_i)^{k(p-1)}]^{q-1} \equiv b_i \mod q.$$

Então, pela Proposição 2.12 item 2, temos $[(b_i)^e]^d \equiv b_i \mod pq$. Como $pq = N$ e $c(b_i) \equiv (b_i)^e \mod N$, então

$$[c(b_i)]^d \equiv [(b_i)^e]^d \equiv b_i \mod N.$$

Portanto, após obter d, Bob precisa apenas calcular o resto da divisão de $[c(b_i)]^d$ por N.

4.2 A SEGURANÇA DO RSA

É claro que a eficiência de um sistema criptográfico depende da dificuldade de decifrá-lo. No caso do RSA, encontrando o valor d em questão consegue-se decifrar a mensagem encriptada. Porém, para calcular tal d é necessário encontrar os primos p e q que são fatores de N. Sabemos que o valor N faz parte da chave pública, ou seja,

não é difícil encontrá-lo. Por outro lado, para encontrar os valores de p e q é necessário fatorar N. O problema disto é que não se conhece nenhum algoritmo que permita fatorar um inteiro muito grande que não tenha fatores pequenos, como os usados na criptografia RSA. Segundo Coutinho (2016), as implementações comerciais do RSA utilizam chaves com cerca de 200 algarismos, sendo que algumas delas utilizam até 2467 algarismos.

Como há a necessidade de que se tenha um valor muito grande para N para que haja uma boa segurança criptográfica, computadores precisam realizar cálculos com números muito grandes, o que exige muito da capacidade destes. Pensando nisso, foram criados criptossistemas capazes de manter a mesma segurança do RSA mesmo ao utilizar chaves consideravelmente menores. Tais criptossistemas utilizam Curvas Elípticas.

5 CRIPTOGRAFIA POR CURVAS ELÍPTICAS

O sistema de criptografia RSA apresenta um alto nível de segurança e é amplamente utilizado. Porém, segundo Mahto e Yadav (2017), para atingir o mesmo nível de segurança alcançado pela RSA, a criptografia utilizando curvas elípticas necessita de parâmetros significativamente menores. Por exemplo, para atingir 112 *bits* de nível de segurança na RSA precisamos de um tamanho de chave de 2048 *bits*, enquanto na criptografia por curvas elípticas precisa-se de um tamanho de chave de apenas 224 bits. Sendo assim, o uso de criptografia por curvas elípticas é interessante em dispositivos que tenham restrições de recursos, como por exemplo, em celulares ou *tablets*.

A Criptografia utilizando curvas elípticas foi proposta inicialmente em 1985 por Neal Koblitz e Victor Miller. Iniciaremos aqui abordando algumas características das curvas elípticas para em seguida aplicar à criptografia.

5.1 CURVAS ELÍPTICAS

Faremos aqui um resumo da teoria básica sobre curvas elípticas para aplicação criptográfica, uma vez que este assunto abrange uma grande quantidade de matemática.

Definição 5.1 *Uma curva Elíptica E é o conjunto de soluções para uma equação da forma*

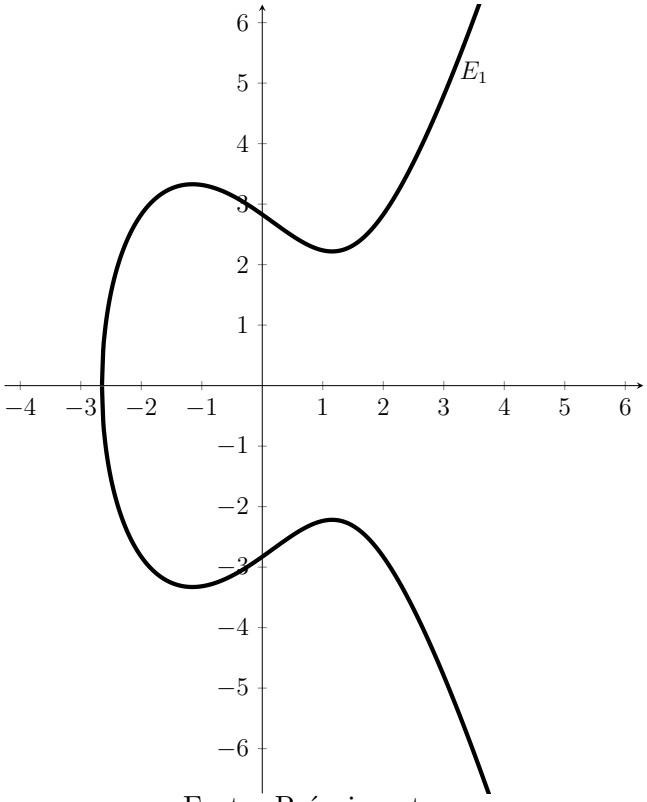
$$E: \ Y^2 = X^3 + AX + B,$$

junto com um ponto extra $\mathcal{O}$, localizado no infinito, em que as constantes A e B satisfazem $4A^3 + 27B^2 \neq 0$.

As Figuras 10 e 11 a seguir são exemplos de Curvas Elípticas, cujas equações são, respectivamente,

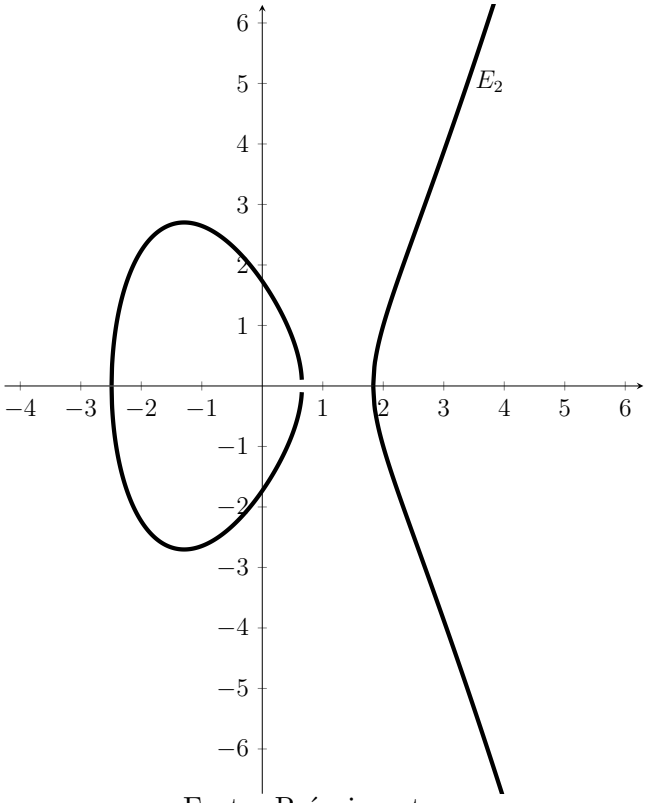
$$E_1 : Y^2 = X^3 - 4X + 8 \text{ e } E_2 : Y^2 = X^3 - 5X + 3.$$

Figura 10 – $E_1 : Y^2 = X^3 - 4X + 8$



Fonte: Próprio autor.

Figura 11 – $E_2 : Y^2 = X^3 - 5X + 3$



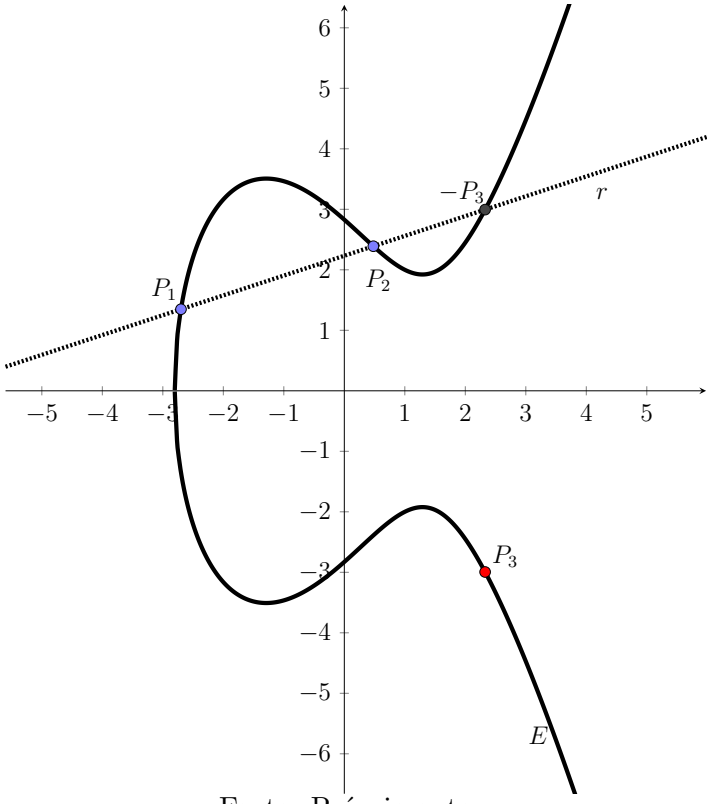
Fonte: Próprio autor.

O que faz das curvas elípticas interessantes para a criptografia é que dados dois pontos de uma curva elíptica, podemos "somar" estes dois pontos, obtendo um terceiro ponto sobre a curva. Colocamos o termo "somar" entre aspas porque trata-se de uma operação análoga à adição em alguns aspectos, como a comutatividade, associatividade e identidade, porém, muito diferente da adição em outros aspectos.

Usaremos argumento geométrico para descrever a "lei da adição" em curvas elípticas: Sejam P_1 e P_2 dois pontos em uma curva elíptica E, iniciaremos desenhando a reta r que contém P_1 e P_2. Como podemos ver na Figura 12, esta reta intercepta E em três pontos. Refletindo este terceiro ponto em relação ao eixo das abcissas, obtemos um novo ponto P_3, que é chamado de soma de P_1 e P_2. Denotaremos esta operação por

$$P_1 \oplus P_2 = P_3.$$

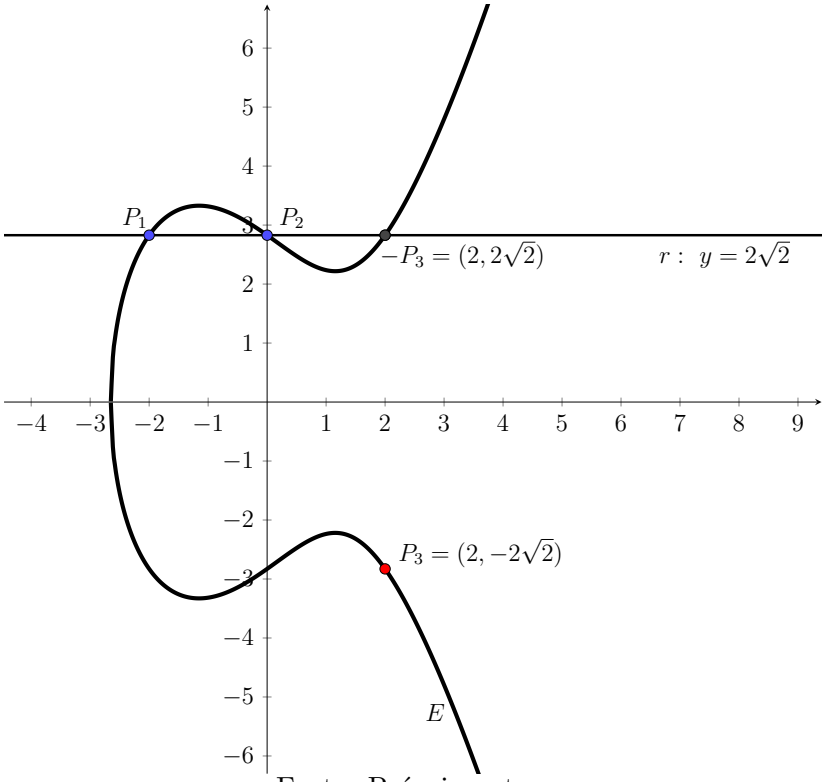
Figura 12 – A "lei da adição" em uma curva elíptica



Fonte: Próprio autor.

Exemplo 5.1 *Seja E a curva elíptica $y^2 = x^3 - 4x + 8$, os pontos $P_1 = (-2, 2\sqrt{2})$ e $P_2 = (0, 2\sqrt{2})$ estão contidos em E, como podemos observar na Figura 13. Traçamos uma reta r que passa por P_1 e P_2. A reta r intersecta E em três pontos, sendo o terceiro o ponto $-P_3$. Ao refletir $-P_3$ em relação ao eixo das abcissas, encontramos o ponto P_3, que é o resultado da soma de P_1 e P_2, apesar deste processo não seja parecido como uma adição comum. Podemos observar aqui que seja $P_3 = (x_3, y_3)$, temos que $-P_3 = (x_3, -y_3)$.*

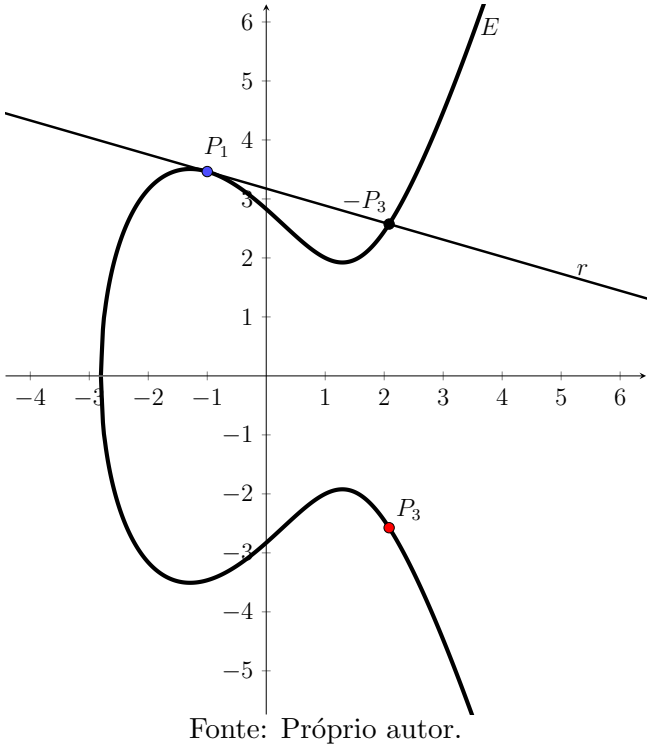
Figura 13 – A "lei da adição" em uma curva elíptica quando $P_1 \neq P_2$.



Fonte: Próprio autor.

Vimos um exemplo da soma de pontos de uma Curva Elíptica onde $P_1 \neq P_2$. E se $P_1 = P_2$? Nestes casos, devemos encontrar a reta que passa por P_1 e que é tangente à curva E. Vejamos:

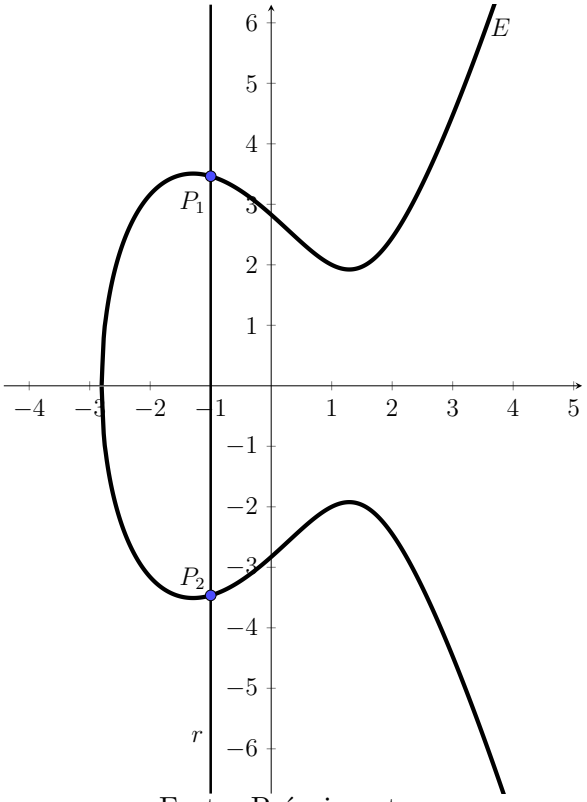
Figura 14 – A "lei da adição" em uma curva elíptica quando $P_1 = P_2$.



Fonte: Próprio autor.

Quando dois pontos estão alinhados em uma reta do tipo $x = a$, com $a \in \mathbb{R}$, ou seja, pertencem a uma reta perpendicular ao eixo das abcissas, estes pontos serão os únicos dois pontos de interseção da reta com a curva elíptica que conseguimos visualizar, observe a Figura 15:

Figura 15 – A "lei da adição" em uma curva elíptica quando P_1 e P_2 pertencem à uma reta do tipo $x = a$.



Fonte: Próprio autor.

Diante desta situação, a solução é utilizar o ponto extra $\mathcal{O}$ que está no infinito. Este ponto $\mathcal{O}$ não existe no plano, mas está presente em toda reta vertical. Portanto, temos que, nestes casos, $P_1 \oplus P_2 = \mathcal{O}$.

É coerente falarmos deste ponto no infinito $\mathcal{O}$ quando tratamos de Geometria Projetiva, cujo um de seus axiomas afirma que duas retas distintas determinam um e somente um ponto com a qual são incidentes. Em outras palavras, diferentemente da Geometria Euclidiana, onde retas paralelas não se interceptam, na Geometria Projetiva admite-se o fato de que quaisquer duas retas coincidem em um ponto e, no caso de retas paralelas, estas coincidem em um ponto no infinito.

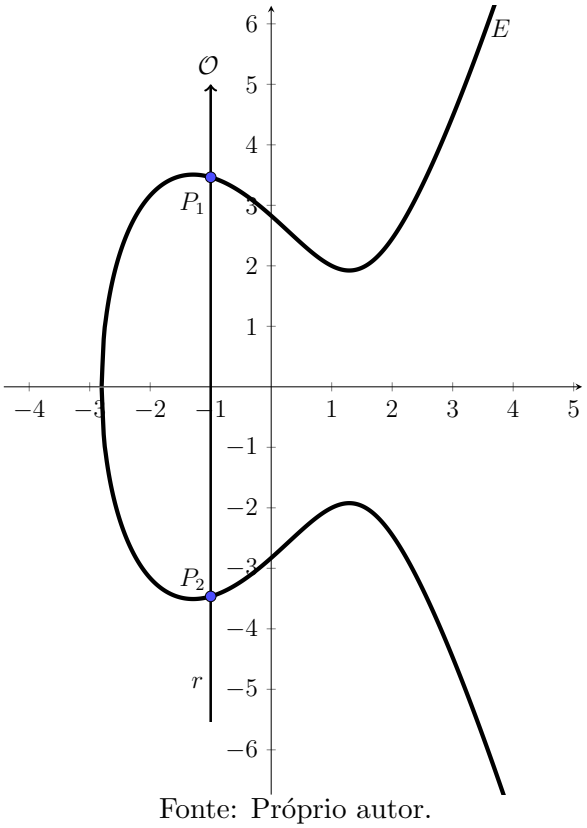
Segundo Andrade e Barros (2010, p.93) " Quando estamos numa longa estrada em linha reta, seus lados são assumidos paralelos, mas a nossa sensação nos diz que elas concorrem num ponto muito longe, chamado ponto de fuga. No ponto de fuga as duas retas estão se interceptando."

Figura 16 – Ponto de Fuga

Fonte: Google Imagens.

É interessante sabermos também que uma reta possui apenas um ponto no infinito, e como uma reta possui duas extremidades, na Geometria projetiva admite-se que ambas as extremidades se encontram nesse ponto no infinito. Sendo assim, podemos imaginar que uma reta projetiva é uma circunferência. Para mais informações sobre Geometria Projetiva, veja (GONÇALVES, 2013).

Figura 17 – Criando o Ponto $\mathcal{O}$ no infinito.



Fonte: Próprio autor.

Como duas retas paralelas se interceptam em um ponto no infinito e cada uma

destas retas possuem apenas um ponto no infinito, seja $\mathcal{O}$ tal ponto, podemos afirmar que $\mathcal{O}$ está presente em todas as retas verticais, já que todas elas são paralelas duas a duas.

Desde que $\mathcal{O}$ está presente em toda reta vertical, temos que a soma de $\mathcal{O}$ com qualquer ponto P_i resulta em P_i, pois ao traçarmos uma reta vertical passando por P_i, esta também interceptará o ponto $\mathcal{O}$ no infinito e encontraremos como ponto de interseção da reta com a curva elíptica, o ponto $-P_i$, que refletido em relação ao eixo das abcissas, retornaremos ao ponto P_i. Sendo assim, o ponto $\mathcal{O}$, funciona como o elemento neutro da adição de pontos de uma curva elíptica.

Observação 5.1 Na curva elíptica que definimos aqui, a condição $4A^3+27B^2 \neq 0$ existe para garantir que o polinômio $X^3 + AX + B$ não tenha raízes repetidas, ou seja, ao fatorarmos $X^3 + AX + B$, obtemos $(X - a_1)(X - a_2)(X - a_3)$, onde a_1, a_2 e a_3 podem ser números complexos, então temos que ocorre $4A^3 + 27B^2 \neq 0$ se, e somente se, a_1, a_2 e a_3 forem todos distintos.

Demonstração: Desde que

$$X^3 + AX + B = (X - a_1)(X - a_2)(X - a_3),$$

se $a_1 = a_2$, temos que

$$X^3 + AX + B = (X - a_1)^2(X - a_3) = X^3 + (-2a_1 - a_3)X^2 + (a_1^2 + 2a_1a_3)X - a_1^2a_3$$

$$\Rightarrow \begin{cases} -2a_1 - a_3 = 0 \\ a_1^2 + 2a_1a_3 = A \\ -a_1^2a_3 = B \end{cases} \Rightarrow a_3 = -2a_1 \Rightarrow \begin{cases} A = a_1^2 + 2a_1(-2a_1) \\ B = -a_1^2(-2a_1) \end{cases} \Rightarrow \begin{cases} A = -3a_1^2 \\ B = 2a_1^3 \end{cases}$$

$$\Rightarrow 4A^3 + 27B^2 = 4(-3a_1^2)^3 + 27(2a_1^3)^2 = 4(-27)a_1^6 + 27 \cdot 4a_1^6 = 0.$$

Os casos em que $a_1 = a_3$ e $a_2 = a_3$ são análogos. Já o caso em que $a_1 = a_2 = a_3$ é bem mais simples. Desde que

$$X^3 + AX + B = (X - a_1)(X - a_2)(X - a_3),$$

se $a_1 = a_2 = a_3$, temos que

$$X^3 + AX + B = (X - a_1)^3 = X^3 + (-3a_1)X^2 + (3a_1^2)X - a_1^3$$

$$\Rightarrow \begin{cases} -3a_1 = 0 \\ 3a_1^2 = A \\ -a_1^3 = B \end{cases} \Rightarrow a_1 = 0 \Rightarrow A = B = 0$$

$$\Rightarrow 4A^3 + 27B^2 = 0.$$

Por outro lado, temos que

$$X^3 + AX + B = (X - a_1)(X - a_2)(X - a_3)$$

$$\Rightarrow X^3 + AX + B = X^3 + (-a_1 - a_1 - a_3)X^2 + (a_1a_2 + a_1a_3 + a_2a_3)X - a_1a_2a_3$$

$$\Rightarrow \begin{cases} -a_1 - a_1 - a_3 = 0 \\ a_1a_2 + a_1a_3 + a_2a_3 = A \\ -a_1a_2a_3 = B \end{cases}$$

$$\Rightarrow a_1 = -a_2 - a_3 \tag{24}$$

Substituindo a_1 por $-a_2 - a_3$ na equação $a_1a_2 + a_1a_3 + a_2a_3 = A$ obtemos que

$$A = -a_2^2 - a_2a_3 - a_3^2 \tag{25}$$

e ao substituirmos a_1 por $-a_2 - a_3$ na equação $-a_1a_2a_3 = B$ obtemos que

$$B = a_2^2a_3 + a_2a_3^2. \tag{26}$$

Seja $4A^3 + 27B^2 \neq 0$, utilizando as igualdades encontradas nas Equações (25) e (26), temos que

$$4(-a_2^2 - a_2a_3 - a_3^2)^3 + 27(a_2^2a_3 + a_2a_3^2)^2 \neq 0$$

$$\Rightarrow 3a_2^4a_3^2 + 26a_2^3a_3^3 + 3a_2^2a_3^4 - 4a_2^6 - 12a_2^5a_3 - 12a_2a_3^5 - 4a_3^6 \neq 0. \tag{27}$$

- Seja $a_2 = a_3$, podemos reescrever a Equação (27) da seguinte forma:

  $$3a_2^6 + 26a_2^6 + 3a_2^6 - 4a_2^6 - 12a_2^6 - 12a_2^6 - 4a_2^6 \neq 0 \Rightarrow 0 \neq 0,$$

  o que é um absurdo.

- Seja $a_2 = a_1$, pela equação (24) temos que $a_3 = -2a_2$, portanto, podemos reescrever a Equação (27) como

  $$3a_2^4(-2a_2)^2 + 26a_2^3(-2a_2)^3 + 3a_2^2(-2a_2)^4 - 4a_2^6 - 12a_2^5(-2a_2) - 12a_2(-2a_2)^5 - 4(-2a_2)^6 \neq 0$$

  $$\Rightarrow 12a_2^6 - 208a_2^6 + 48a_2^6 - 4a_2^6 + 24a_2^6 + 384a_2^6 - 256a_2^6 \Rightarrow 0 \neq 0,$$

  o que também é um absurdo.

- Seja $a_3 = a_1$, pela equação (24) temos que $a_2 = -2a_3$, portanto, podemos reescrever

a Equação (27) como

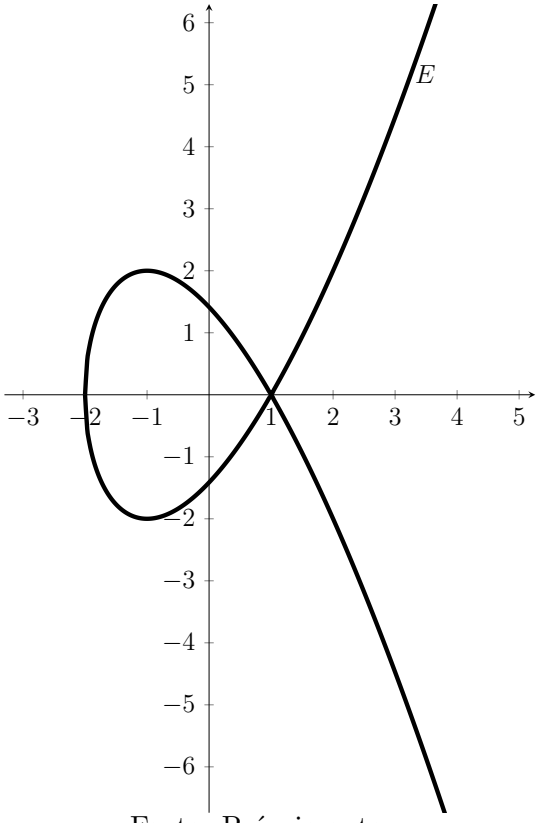
$$3(-2a_3)^4a_3^2+26(-2a_3)^3a_3^3+3(-2a_3)^2a_3^4-4(-2a_3)^6-12(-2a_3)^5a_3-12(-2a_3)a_3^5-4a_3^6$$

$$\Rightarrow 48a_3^6 - 208a_3^6 + 12a_3^6 - 256a_3^6 + 384a_3^6 + 24a_3^6 - 4a_3^6 \Rightarrow 0 \neq 0,$$

o que novamente é um absurdo.
Portanto, temos que a desigualdade $4A^3 + 27B^2 \neq 0$ ocorre apenas se a_1, a_2 e a_3 forem todos distintos. ■

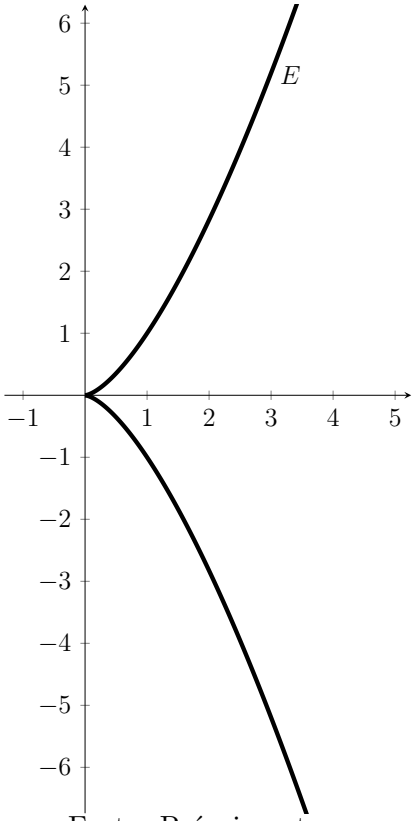
Nos casos em que $4A^3+27B^2 = 0$, o gráfico da curva possui um ponto incomum, chamado de ponto singular. Vejamos os gráficos das curvas abaixo:

Figura 18 – Gráfico da curva $E: \ Y^2 = X^3 - 3X + 2$.



Fonte: Próprio autor.

Figura 19 – Gráfico da curva $E: \ Y^2 = X^3$.



Fonte: Próprio autor.

A lei da adição não funciona bem nesses tipos de curvas, portanto, foi incluída a restrição $4A^3 + 27B^2 \neq 0$ na nossa definição de Curva Elíptica.

Teorema 5.1 *Seja E uma curva Elíptica. A lei da adição em E possui as seguintes propriedades:*

1. $P_1 \oplus \mathcal{O} = \mathcal{O} \oplus P_1 = P_1$ *para todo* $P_1 \in E$. *(Elemento Neutro)*
2. $P_1 \oplus (-P_1) = \mathcal{O}$ *para todo* $P_1 \in E$. *(Elemento Simétrico)*
3. $(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3)$ *para todo* $P_1, P_2, P_3 \in E$. *(Associatividade)*
4. $P_1 \oplus P_2 = P_2 \oplus P_1$ *para todo* $P_1, P_2 \in E$. *(Comutatividade)*

Ou seja, a lei da adição transforma o conjunto de pontos de E em um grupo abeliano.

Demonstração: 1 e 2: Como já falamos anteriormente, $\mathcal{O}$ está presente em toda reta vertical, o que torna estas duas propriedades verdadeiras.

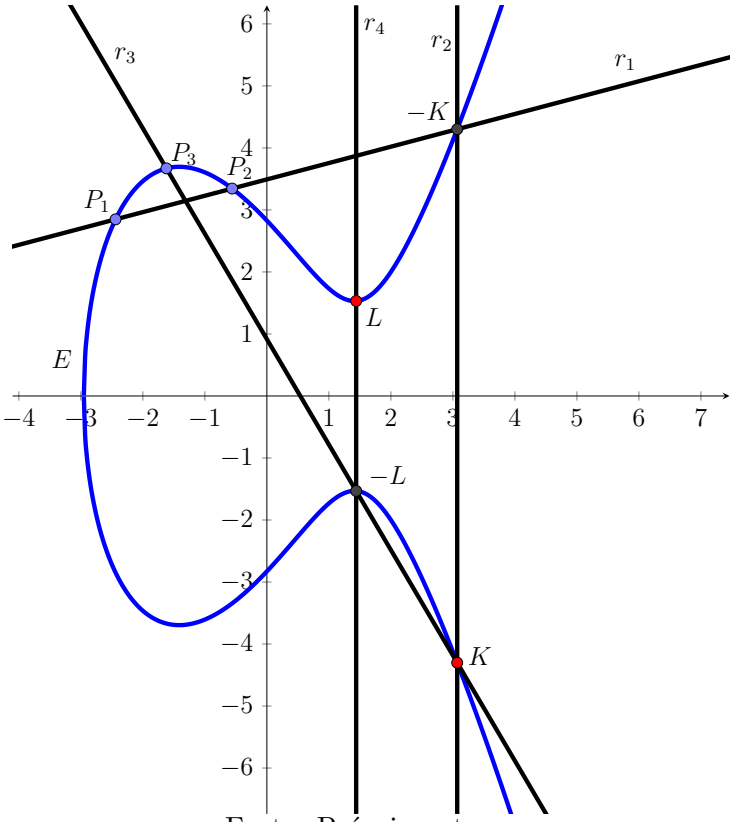
3: Faremos aqui a tentativa de verificar geometricamente que a associatividade é válida. Porém, a prova para todos os casos possíveis é muito extensa, o que ocuparia grande parte de nosso trabalho. A prova completa pode ser vista em Washington (2008).

Dados os pontos P_1, P_2 e P_3 na Curva Elíptica E da Figura 20, para encontrarmos um ponto de E que represente $P_1 \oplus P_2$ traçamos a reta r_1 por P_1 e P_2 onde encontramos o ponto $-K$ de interseção de r_1 com E, e em seguida traçamos a reta r_2

perpendicular ao eixo das abcissas e passando por $-K$, encontrando assim o ponto K em E que representa $P_1 \oplus P_2$.

Para encontrarmos um ponto em E que represente $(P_1 \oplus P_2) \oplus P_3 = K \oplus P_3$, traçamos a reta r_3 por K e P_3 encontrando o ponto $-L$ de interseção de r_3 com E. Em seguida traçamos a reta r_4 perpendicular ao eixo das abcissas e que passa por $-L$, encontrando assim, o ponto L que representa a soma $(P_1 \oplus P_2) \oplus P_3$.

Figura 20 – Soma $(P_1 \oplus P_2) \oplus P_3$.



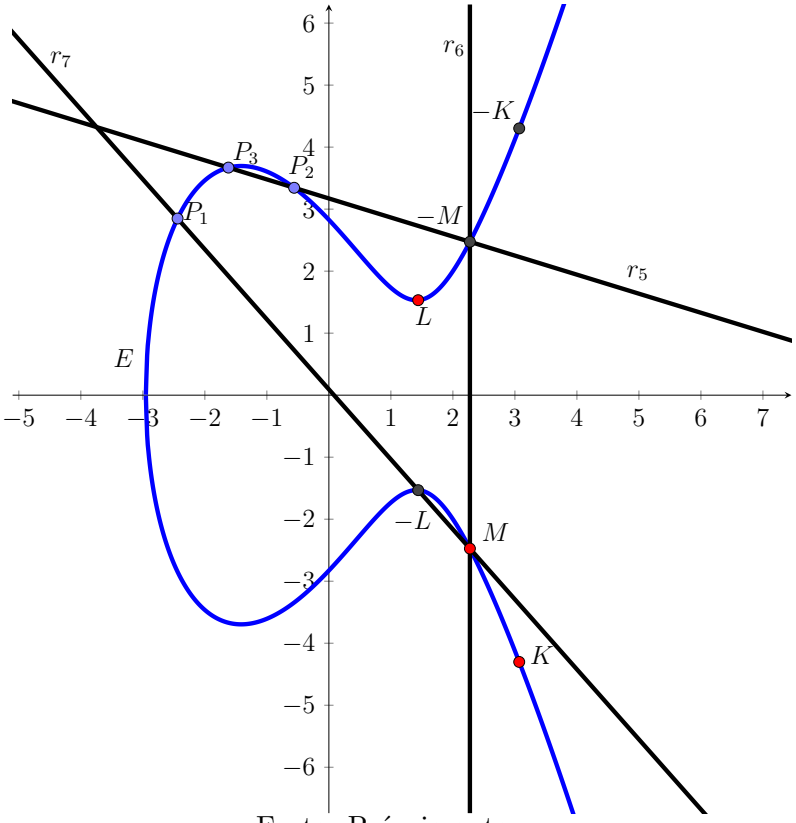
Fonte: Próprio autor.

Vamos encontrar agora um ponto em E que represente a soma $P_2 \oplus P_3$. Para isso, na Figura 21 traçamos a reta r_5 onde encontramos o ponto $-M$ de interseção de r_5 com E. O simétrico de $-M$ foi obtido ao traçarmos a reta r_6 perpendicular ao eixo das abcissas e que passa pelo ponto $-M$. Portanto, o ponto M representa a soma $P_2 \oplus P_3$.

Afim de encontrarmos um ponto que represente $P_1 \oplus (P_2 \oplus P_3) = P_1 \oplus M$, traçamos a reta r_7 por P_1 e M, encontrando assim o ponto de interseção com E. Observe que tal ponto é o ponto $-L$ já encontrado na figura anterior, onde sabemos que seu simétrico é o ponto L. Logo, temos que

$$P_1 \oplus (P_2 \oplus P_3) = L = (P_1 \oplus P_2) \oplus P_3.$$

Figura 21 – Soma $P_1 \oplus (P_2 \oplus P_3)$.



Fonte: Próprio autor.

4: A reta que passa por P_1 e P_2 é a mesma que passa por P_2 e P_1. Logo, a ordem não importa.

Concluímos aqui a demonstração de que a Lei da Adição transforma E em um grupo abeliano. ■

Necessitamos encontrar fórmulas explícitas que nos facilite fazer a adição de pontos de uma curva elíptica. Anunciaremos aqui um algoritmo na forma de Teorema e em seguida sua demonstração:

Teorema 5.2 (Algoritmo da Adição de Curva Elíptica) *Seja*

$$E: \ Y^2 = X^3 + AX + B$$

uma curva Elíptica, P_1 e P_2 pontos sobre ela, temos que:

1. *Se $P_1 = \mathcal{O}$, então $P_1 \oplus P_2 = P_2$;*

2. *Por outro lado, se $P_2 = \mathcal{O}$, então $P_1 \oplus P_2 = P_1$. Caso contrário, escreva $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ e avance para o próximo passo;*

3. *Se $x_1 = x_2$ e $y_1 = -y_2$, temos $P_1 \oplus P_2 = \mathcal{O}$;*

4. Caso contrário, defina λ por

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \ \textit{se } P_1 \neq P_2, \\ \\ \dfrac{3x_1^2 + A}{2y_1} \ \textit{se } P_1 = P_2, \end{cases} \tag{28}$$

onde λ é o coeficiente angular da reta que intercepta a curva E nos pontos P_1 e P_2. Sejam

$$x_3 = \lambda^2 - x_1 - x_2 \tag{29}$$

e

$$y_3 = \lambda(x_1 - x_3) - y_1. \tag{30}$$

Então, temos que $P_1 \oplus P_2 = (x_3, y_3)$.

Demonstração: 1 e 2: Estes casos são claros e já foram demonstrados no Teorema 5.1 . 3: Este é o caso em que a reta que passa por P_1 e P_2 é vertical. Portanto, $P_1 \oplus P_2 = \mathcal{O}$. 4: Analisando cada caso:

- Se $P_1 \neq P_2$: Seja $r : Y = \lambda X + \beta$ a reta que intercepta a curva elíptica E nos pontos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ então

$$(\lambda X + \beta)^2 = X^3 + AX + B$$

$$\Rightarrow X^3 - \lambda^2 X^2 + (A - 2\lambda\beta)X + B = 0, \tag{31}$$

que é uma equação do 3° grau. Como x_1 e x_2 são raízes da equação 31, que é de grau 3, considere x_3 como sendo a terceira raiz e $(-P_3) = (x_3, -y_3)$. Com isso, das identidades de Girard, como x_1, x_2 e x_3 são raízes da equação (31), temos que

$$x_1 + x_2 + x_3 = \frac{\lambda^2}{1}$$

$$\Rightarrow x_3 = \lambda^2 - x_1 - x_2. \tag{32}$$

Temos ainda que

$$y_1 = \lambda x_1 + \beta \Rightarrow \beta = y_1 - \lambda x_1. \tag{33}$$

Além disso,

$$-y_3 = \lambda x_3 + \beta \Rightarrow y_3 = -\lambda x_3 - \beta, \tag{34}$$

Que ao substituirmos β pelo seu valor dado pela equação (33), obtemos

$$y_3 = -\lambda x_3 - (y_1 - \lambda x_1)$$

$$\Rightarrow y_3 = \lambda(x_1 - x_3) - y_1. \tag{35}$$

Portanto, $P_1 \oplus P_2 = P_3 = (x_3, y_3) = (\lambda^2 - x_1 - x_2,\ \lambda(x_1 - x_3) - y_1)$.

- Se $P_1 = P_2$: Neste caso, a reta que intercepta a curva elíptica E nos pontos $P_1 = (x_1, y_1)$, $P_2 = (x_1, y_1)$ e $(-P_3) = (x_3, -y_3)$ é tangente à curva E. Portanto, para encontrar seu coeficiente angular, basta calcularmos a derivada de $Y^2 = X^3 + AX + B$ no ponto $P_1 = (x_1, y_1)$. Fazendo isso, obtemos $\lambda = \dfrac{3x_1^2 + A}{2y_1}$ e o processo de encontrar os valores de x_3 e y_3 é o mesmo dos casos em que $P_1 \neq P_2$.

■

Observação 5.2 A derivada de uma função $y = f(x)$ no ponto P é o coeficiente angular da reta tangente à curva no ponto P e denotamos a derivada de $f(x)$ por $f'(x)$. Por exemplo, $f(x) = 3x \Rightarrow f'(x) = (3x)'$. Algumas regras de derivação facilitam o cálculo da derivada de algumas funções. Segue no Teorema abaixo algumas dessas regras que utilizamos para encontrar o coeficiente angular da reta tangente à curva elíptica:

Teorema 5.3 *Sejam $f(x)$ e $g(x)$ funções deriváveis e $n \in \mathbb{R}$, são válidas as formulas de derivação a seguir:*

- $f(x) = n \Rightarrow f'(x) = 0$;
- $f(x) = x^n \Rightarrow f'(x) = nx^{n-1}$;
- $[f(x) + g(x)]' = f'(x) + g'(x)$;
- $[kf(x)]' = kf'(x)$;
- $[f(x) \cdot g(x)]' = f'(x)g(x) + f(x)g'(x)$.

Demonstração: *A demonstração do Teorema acima bem como definições formais de derivada e outras regras de derivação podem ser encontradas em um livro de Cálculo ou de Análise real. Para o leitor com interesse no assunto, veja Guidorizzi, (1995).* ■

Na demonstração do Item 4 do Teorema 5.2, utilizamos as regras de derivação presentes no Teorema 5.3 para calcular o coeficiente angular da reta tangente à curva elíptica. Vejamos:

$$y_0^2 = x_0^3 + Ax_0 + B \Rightarrow (y_0 \cdot y_0)' = (x_0^3 + Ax_0 + B)' \Rightarrow$$

$$\Rightarrow (y_0)' \cdot y_0 + y_0 \cdot (y_0)' = 3x_0^2 + A \Rightarrow (y_0)' \cdot (y_0 + y_0) = 3x_0^2 + A \Rightarrow$$

$$\Rightarrow (y_0)' = \frac{3x_0^2 + A}{2y_0}.$$

5.2 CURVA ELÍPTICA SOBRE UM CORPO $\mathbb{Z}_p$.

Anteriormente, desenvolvemos a teoria das curvas elípticas geometricamente. Porém, para aplicar à criptografia, precisamos trabalhar com curvas elípticas cujos pontos têm coordenadas em um corpo finito $\mathbb{Z}_p$.

Definição 5.2 *Uma curva elíptica sobre $\mathbb{Z}_p$ é o conjunto de pontos que satisfazem uma equação da forma*

$$E:\ Y^2 = X^3 + AX + B,$$

junto com um ponto extra $\mathcal{O}$*, localizado no infinito, com* $X, Y, A, B \in \mathbb{Z}_p$*, satisfazendo* $4A^3 + 27B^2 \not\equiv 0 \mod p$.

O conjunto de pontos em E com coordenadas em $\mathbb{Z}_p$ é

$$E(\mathbb{Z}_p) = \{(x, y) : x, y \in \mathbb{Z}_p;\ y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

É fácil ver que o conjunto de pontos $E(\mathbb{Z}_p)$ é finito, uma vez que existem finitas possibilidades para as coordenadas X e Y. Como existem p possibilidades para X e, para cada X, a equação $Y^2 = X^3 + AX + B$ indica que existem no máximo duas possibilidades para Y, ao incluirmos o ponto extra $\mathcal{O}$, $E(\mathbb{Z}_p)$ terá no máximo $2p+1$ pontos. No entanto, essa estimativa é consideravelmente maior do que a quantidade real.

Observação 5.3 Se E é uma curva elíptica definida sobre $\mathbb{Z}_2$, então $E(\mathbb{Z}_2)$ contém no máximo 5 pontos, sendo assim, fica difícil a utilização destas curvas na criptografia. Porém, há a possibilidade da utilização de curvas elípticas definidas sobre $\mathbb{Z}_{2^k}$ com $k > 1 \in \mathbb{N}$. Veja Hoffstein, Pipher e Silverman (2008).

Uma vez que $E(\mathbb{Z}_p)$ é um conjunto finito de pontos, então podemos encontrar todos esses pontos realizando alguns cálculos, vejamos:

Exemplo 5.2 *Considere a curva elíptica* $E(\mathbb{Z}_{11})$ *de equação* $Y^2 = X^3 + 5X + 1$*. Podemos encontrar os pontos de* $E(\mathbb{Z}_{11})$ *substituindo* X *por todos os valores possíveis, ou seja, por* $0, 1, 2, \ldots, 10$ *e verificando para quais valores a quantidade* $X^3 + 5X + 1$ *é um quadrado módulo* 11*. Para facilitar, faremos uma lista dos quadrados módulo* 11 :

$$\begin{aligned}
0^2 &\equiv 0 \mod 11;\\
1^2 &\equiv 1 \mod 11;\\
2^2 &\equiv 4 \mod 11;\\
3^2 &\equiv 9 \mod 11;\\
4^2 &\equiv 16 \equiv 5 \mod 11;\\
5^2 &\equiv 25 \equiv 3 \mod 11;\\
6^2 &\equiv 36 \equiv 3 \mod 11;\\
7^2 &\equiv 49 \equiv 5 \mod 11;\\
8^2 &\equiv 64 \equiv 9 \mod 11;\\
9^2 &\equiv 81 \equiv 4 \mod 11;\\
10^2 &\equiv 100 \equiv 1 \mod 11.
\end{aligned}$$

Portanto, $0, 1, 3, 4, 5$ *e* 9 *são os quadrados módulo* 11*.*

Faremos agora uma lista com os valores módulo 11 *que obtemos ao substituirmos* X *por* $0, 1, 2, \ldots, 10$ *em* $X^3 + 5X + 1$:

- *Se* $X = 0$, *temos*
$$0^3 + 5 \cdot 0 + 1 = 1 \equiv 1 \mod 11;$$
- *Se* $X = 1$, *temos*
$$1^3 + 5 \cdot 1 + 1 = 7 \equiv 7 \mod 11;$$
- *Se* $X = 2$, *temos*
$$2^3 + 5 \cdot 2 + 1 = 19 \equiv 8 \mod 11;$$
- *Se* $X = 3$, *temos*
$$3^3 + 5 \cdot 3 + 1 = 43 \equiv 10 \mod 11;$$
- *Se* $X = 4$, *temos*
$$4^3 + 5 \cdot 4 + 1 = 85 \equiv 8 \mod 11;$$
- *Se* $X = 5$, *temos*
$$5^3 + 5 \cdot 5 + 1 = 151 \equiv 8 \mod 11;$$
- *Se* $X = 6$, *temos*
$$6^3 + 5 \cdot 6 + 1 = 247 \equiv 5 \mod 11;$$
- *Se* $X = 7$, *temos*
$$7^3 + 5 \cdot 7 + 1 = 379 \equiv 5 \mod 11;$$
- *Se* $X = 8$, *temos*
$$8^3 + 5 \cdot 8 + 1 = 553 \equiv 3 \mod 11;$$
- *Se* $X = 9$, *temos*
$$9^3 + 5 \cdot 9 + 1 = 775 \equiv 5 \mod 11;$$
- *Se* $X = 10$, *temos*
$$10^3 + 5 \cdot 10 + 1 = 1051 \equiv 6 \mod 11.$$

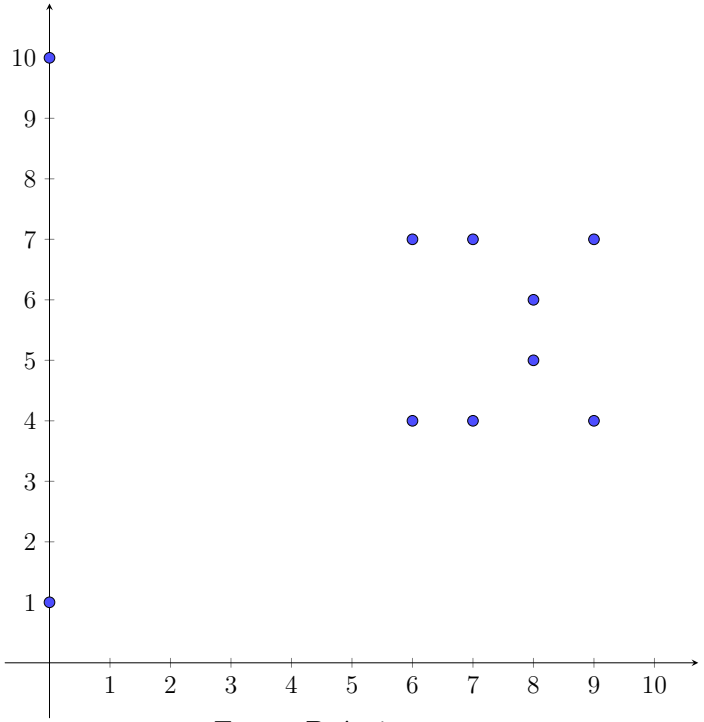
Com isso, percebemos que para $X = 0$, 6, 7, 8, 9 *e* 10, *obtemos valores quadrados módulo* 11 *ao calcularmos* $X^3 + 5X + 1$. *Observe que para* $X = 0$, *obtemos o valor* 1 mod 11 *que é o quadrado módulo* 11 *de* 1 *e de* 10. *Isso nos mostra dois pontos em* $E(\mathbb{Z}_{11})$, *são eles* $(0, 1)$ *e* $(0, 10)$. *Continuando a associação, encontramos a lista completa:*

$$E(\mathbb{Z}_{11}) = \{\mathcal{O}, (0,1), (0,10), (6,4), (6,7), (7,4), (7,7), (8,5), (8,6), (9,4), (9,7)\}.$$

Portanto, $E(\mathbb{Z}_{11})$ *consiste em* 11 *pontos.*

O quão maior for o valor do primo p, maior será a cardinalidade de $E(\mathbb{Z}_p)$. Ao trabalharmos com curvas elípticas em $\mathbb{Z}_p$, o gráfico da curva se torna simplesmente uma plotagem de pontos. Vejamos:

Figura 22 – Gráfico da curva $E(\mathbb{Z}_{11}):\ Y^2 = X^3 + 5X + 1$.



Fonte: Próprio autor.

Podemos utilizar o Teorema (5.2) para somar dois pontos de uma curva elíptica sobre um corpo $\mathbb{Z}_p$. Vejamos o exemplo a seguir:

Exemplo 5.3 *Vamos realizar algumas somas de pontos da curva citada no Exemplo (5.2):*

- *Se* $P_1 = (0,1)$ *e* $P_2 = \mathcal{O}$, *então* $P_1 \oplus P_2 = P_3 = P_1 = (0,1)$;
- *Se* $P_1 = (0,1)$ *e* $P_2 = (0,10)$, *então* $P_1 \oplus P_2 = P_3 = \mathcal{O}$;
- *Se* $P_1 = (0,1)$ *e* $P_2 = (6,4)$, *fazemos*

$$\lambda = \frac{4-1}{6-0} = \frac{3}{6} \Rightarrow 6\lambda \equiv 3 \mod 11 \Rightarrow \lambda \equiv 6 \mod 11.$$

Daí temos que

$$x_3 = 6^2 - 6 - 0 = 30 \equiv 8 \mod 11$$

e que

$$y_3 = 6 \cdot (0-8) - 1 = -49 \equiv 6 \mod 11.$$

Sendo assim, $P_1 \oplus P_2 = P_3 = (8,6)$.

- *Se* $P_1 = P_2 = (0,1)$, *fazemos*

$$\lambda = \frac{3 \cdot 0^2 + 5}{2 \cdot 1} = \frac{5}{2} \Rightarrow 2\lambda \equiv 5 \mod 11 \Rightarrow \lambda \equiv 8 \mod 11.$$

Daí temos que

$$x_3 = 8^2 - 0 - 0 = 64 \equiv 9 \mod 11$$

e que

$$y_3 = 8 \cdot (0 - 9) - 1 = -73 \equiv 4 \mod 11.$$

Sendo assim, $P_1 \oplus P_2 = 2P_1 = 2P_2 = P_3 = (9, 4)$.

Efetuando o calculo das demais somas de pontos possíveis nessa curva elíptica obtemos tabela da Figura 23:

Figura 23 – Somas de pontos da Curva Elíptica $E(\mathbb{Z}_{11})$: $Y^2 = X^3 + 5X + 1$.

$\oplus$	$\mathcal{O}$	**(0,1)**	**(0,10)**	**(6,4)**	**(6,7)**	**(7,4)**	**(7,7)**	**(8,5)**	**(8,6)**	**(9,4)**	**(9,7)**
$\mathcal{O}$	$\mathcal{O}$	(0,1)	(0,10)	(6,4)	(6,7)	(7,4)	(7,7)	(8,5)	(8,6)	(9,4)	(9,7)
(0,1)	(0,1)	(9,4)	$\mathcal{O}$	(8,6)	(6,4)	(8,5)	(9,7)	(6,7)	(7,7)	(7,4)	(0,10)
(0,10)	(0,10)	$\mathcal{O}$	(9,7)	(6,7)	(8,5)	(9,4)	(8,6)	(7,4)	(6,4)	(0,1)	(7,7)
(6,4)	(6,4)	(8,6)	(6,7)	(0,1)	$\mathcal{O}$	(9,7)	(7,4)	(0,10)	(9,4)	(7,7)	(8,5)
(6,7)	(6,7)	(6,4)	(8,5)	$\mathcal{O}$	(0,10)	(7,7)	(9,4)	(9,7)	(0,1)	(8,6)	(7,4)
(7,4)	(7,4)	(8,5)	(9,4)	(9,7)	(7,7)	(6,4)	$\mathcal{O}$	(8,6)	(0,10)	(6,7)	(0,1)
(7,7)	(7,7)	(9,7)	(8,6)	(7,4)	(9,4)	$\mathcal{O}$	(6,7)	(0,1)	(8,5)	(0,10)	(6,4)
(8,5)	(8,5)	(6,7)	(7,4)	(0,10)	(9,7)	(8,6)	(0,1)	(7,7)	$\mathcal{O}$	(6,4)	(9,4)
(8,6)	(8,6)	(7,7)	(6,4)	(9,4)	(0,1)	(0,10)	(8,5)	$\mathcal{O}$	(7,4)	(9,7)	(6,7)
(9,4)	(9,4)	(7,4)	(0,1)	(7,7)	(8,6)	(6,7)	(0,10)	(6,4)	(9,7)	(8,5)	$\mathcal{O}$
(9,7)	(9,7)	(0,10)	(7,7)	(8,5)	(7,4)	(0,1)	(6,4)	(9,4)	(6,7)	$\mathcal{O}$	(8,6)

Fonte: Próprio autor.

Veja agora um exemplo para uma outra Curva Elíptica:

Exemplo 5.4 *Considere a curva elíptica* $E(\mathbb{Z}_7)$ *de equação* $Y^2 = X^3 + 2X + 3$. *Vamos encontrar os pontos de* $E(\mathbb{Z}_7)$ *substituindo* X *por todos os valores possíveis e verificando para quais valores a quantidade* $X^3 + 2X + 3$ *é um quadrado módulo* 7. *Inicialmente faremos uma lista dos quadrados módulo* 7 :

$$\begin{aligned}
0^2 &\equiv 0 \mod 7;\\
1^2 &\equiv 1 \mod 7;\\
2^2 &\equiv 4 \mod 7;\\
3^2 &\equiv 9 \equiv 2 \mod 7;\\
4^2 &\equiv 16 \equiv 2 \mod 7;\\
5^2 &\equiv 25 \equiv 4 \mod 7;\\
6^2 &\equiv 36 \equiv 1 \mod 7.
\end{aligned}$$

Portanto, $0, 1, 2$ *e* 4 *são os quadrados módulo* 7.

Faremos agora uma lista com os valores módulo 7 *que obtemos ao substituirmos* X *por* $0, 1, 2, \ldots, 6$ *em* $X^3 + 2X + 3$:

- *Se* $X = 0$, *temos*

$$0^3 + 2 \cdot 0 + 3 \equiv 3 \equiv 3 \mod 7;$$

- *Se* $X = 1$, *temos*
$$1^3 + 2 \cdot 1 + 3 \equiv 6 \equiv 6 \mod 7;$$
- *Se* $X = 2$, *temos*
$$2^3 + 2 \cdot 2 + 3 \equiv 15 \equiv 1 \mod 7;$$
- *Se* $X = 3$, *temos*
$$3^3 + 2 \cdot 3 + 3 \equiv 36 \equiv 1 \mod 7;$$
- *Se* $X = 4$, *temos*
$$4^3 + 2 \cdot 4 + 3 \equiv 75 \equiv 5 \mod 7;$$
- *Se* $X = 5$, *temos*
$$5^3 + 2 \cdot 5 + 3 \equiv 138 \equiv 5 \mod 7;$$
- *Se* $X = 6$, *temos*
$$6^3 + 2 \cdot 6 + 3 \equiv 231 \equiv 0 \mod 7.$$

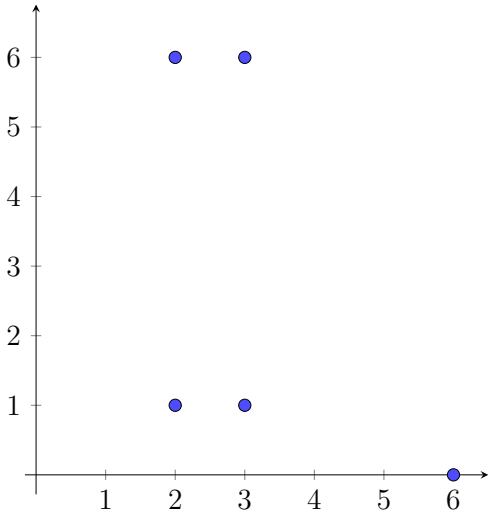
Com isso, temos que para $X = 2, 3, 6$, *obtemos valores módulo* 7 *ao calcularmos* $X^3 + 2X + 3$. *Observe que para* $X = 2$, *obtemos o valor* $1 \mod 7$ *que é o quadrado módulo* 7 *de* 1 *e de* 6. *Obtendo assim dois pontos em* $E(\mathbb{Z}_7)$, *são eles* $(2, 1)$ *e* $(2, 6)$. *Continuando assim, encontramos a lista completa:*

$$E(\mathbb{Z}_7) = \{\mathcal{O}, (2, 1), (2, 6), (3, 1), (3, 6), (6, 0)\}.$$

Portanto, $E(\mathbb{Z}_7)$ *consiste em 6 pontos.*

Vejamos a plotagem dos pontos dessa curva elíptica na Figura 24:

Figura 24 – Gráfico da curva $E(\mathbb{Z}_7) : \ Y^2 = X^3 + 2X + 3$.



Fonte: Próprio autor.

Utilizando o Teorema (5.2) para somar pontos dessa curva elíptica:

Exemplo 5.5 *Vamos realizar algumas somas de pontos da curva citada no Exemplo 5.4:*

- *Se* $P_1 = (2,1)$ *e* $P_2 = \mathcal{O}$, *então* $P_1 \oplus P_2 = P_3 = P_1 = (2,1)$;
- *Se* $P_1 = (2,1)$ *e* $P_2 = (2,6)$, *então* $P_1 \oplus P_2 = P_3 = \mathcal{O}$;
- *Se* $P_1 = (2,1)$ *e* $P_2 = (3,1)$, *fazemos*

$$\lambda = \frac{1-1}{3-2} = 0 \equiv 0 \mod 7.$$

Daí temos que

$$x_3 = 0^2 - 3 - 2 = -5 \equiv 2 \mod 7$$

e que

$$y_3 = 0 \cdot (2-2) - 1 = -1 \equiv 6 \mod 7.$$

Sendo assim, $P_1 \oplus P_2 = P_3 = (2,6)$.

- *Se* $P_1 = P_2 = (2,1)$, *fazemos*

$$\lambda = \frac{3 \cdot 2^2 + 2}{2 \cdot 1} = 7 \equiv 0 \mod 7.$$

Daí temos que

$$x_3 = 0^2 - 2 - 2 = -4 \equiv 3 \mod 7$$

e que

$$y_3 = 0 \cdot (2-3) - 1 = -1 \equiv 6 \mod 7.$$

Sendo assim, $P_1 \oplus P_2 = 2P_1 = 2P_2 = P_3 = (3,6)$.

Efetuando o calculo das demais somas de pontos possíveis nessa curva elíptica obtemos a Tabela 9:

Tabela 9 – Somas de pontos da curva elíptica $E(\mathbb{Z}_7) : Y^2 = X^3 + 2X + 3$.

$\oplus$	$\mathcal{O}$	$(2,1)$	$(2,6)$	$(3,1)$	$(3,6)$	$(6,0)$
$\mathcal{O}$	$\mathcal{O}$	$(2,1)$	$(2,6)$	$(3,1)$	$(3,6)$	$(6,0)$
$(2,1)$	$(2,1)$	$(3,6)$	$\mathcal{O}$	$(2,6)$	$(6,0)$	$(3,1)$
$(2,6)$	$(2,6)$	$\mathcal{O}$	$(3,1)$	$(6,0)$	$(2,1)$	$(3,6)$
$(3,1)$	$(3,1)$	$(2,6)$	$(6,0)$	$(3,6)$	$\mathcal{O}$	$(2,1)$
$(3,6)$	$(3,6)$	$(6,0)$	$(2,1)$	$\mathcal{O}$	$(3,1)$	$(2,6)$
$(6,0)$	$(6,0)$	$(3,1)$	$(3,6)$	$(2,1)$	$(2,6)$	$\mathcal{O}$

Fonte: Proprio Autor

5.3 O PROBLEMA DO LOGARITMO DISCRETO SOBRE CURVAS ELÍPTICAS

Definiremos aqui o problema do logaritmo discreto sobre o conjunto formado pelos pontos de uma curva elíptica E definida sobre um corpo finito $\mathbb{Z}_p$.

Definição 5.3 *Seja* E *uma curva elíptica sobre* $\mathbb{Z}_p$ *e* P *um ponto de* E. *Se existe um*

inteiro k tal que $kP = Q$, tal que $Q \in E$, o problema do logaritmo discreto é encontrar k. Perceba que, seja $P = (2, 1)$ na curva elíptica exposta no exemplo (5.4), obtemos

$$\begin{aligned}
\text{Para } k = 2, \text{ temos} \quad & 2P = (2,1) \oplus (2,1) = (3,6) \\
\text{Para } k = 3, \text{ temos} \quad & 3P = 2P \oplus P = (3,6) \oplus (2,1) = (6,0) \\
\text{Para } k = 4, \text{ temos} \quad & 4P = 3P \oplus P = (6,0) \oplus (2,1) = (3,1) \\
\text{Para } k = 5, \text{ temos} \quad & 5P = 4P \oplus P = (3,1) \oplus (2,1) = (2,6) \\
\text{Para } k = 6, \text{ temos} \quad & 6P = 5P \oplus P = (2,6) \oplus (2,1) = \mathcal{O} \\
\text{Para } k = 7, \text{ temos} \quad & 7P = 6P \oplus P = \mathcal{O} \oplus (2,1) = (2,1) \\
\text{Para } k = 8, \text{ temos} \quad & 8P = 7P \oplus P = (2,1) \oplus (2,1) = (3,6) \\
\text{Para } k = 9, \text{ temos} \quad & 9P = 8P \oplus P = (3,6) \oplus (2,1) = (6,0) \\
\text{Para } k = 10, \text{ temos} \quad & 10P = 9P \oplus P = (6,0) \oplus (2,1) = (3,1) \\
\text{Para } k = 11, \text{ temos} \quad & 11P = 10P \oplus P = (3,1) \oplus (2,1) = (2,6) \\
\text{Para } k = 12, \text{ temos} \quad & 12P = 11P \oplus P = (2,6) \oplus (2,1) = \mathcal{O} \\
\text{Para } k = 13, \text{ temos} \quad & 13P = 12P \oplus P = \mathcal{O} \oplus (2,1) = (2,1) \\
& \vdots
\end{aligned}$$

Perceba que neste caso, estamos calculando os múltiplos de P, formando assim um grupo em que P é o seu gerador. Logo, pela Definição 2.14, o grupo de múltiplos de P é cíclico. Portanto, se existe k que satisfaz $kP = Q$, então existem infinitos valores para k. Devido a finitude de $E(\mathbb{Z}_p)$, sejam i e j inteiros distintos, existirão valores $iP = jP$. Veja que existe um valor s tal que $sP = \mathcal{O}$, podemos, sem perda de generalidade, definir $s = i - j$. A ordem do ponto P será o menor valor positivo possível para s.

De acordo com Hoffstein, Pipher e Silverman (2008), o Problema do logaritmo discreto sobre curvas elípticas é ainda mais difícil que o problema do logaritmo discreto e da fatoração de inteiros. Porém, algumas curvas devem ser evitadas, como por exemplo, as anômalas e as super-singulares . O motivo destas curvas serem evitadas é que Menezes, Okamoto e Vanstone (1993) e Smart (1999) conseguiram desenvolver algoritmos capazes de resolver o Problema do logaritmo discreto de forma relativamente rápida nesse tipo de curva. Porém, a quantidade desse tipo de curva é bem pequena em relação a todo o universo das curvas elípticas.

5.4 TROCA DE CHAVES DIFFIE-HELLMAN COM CURVAS ELÍPTICAS

Imagine que Alice e Bob vivem bem distantes um do outro, nunca estiveram juntos presencialmente e que pretendem trocar segredos. Além disso, existe Eva, uma detetive que vive procurando algo interessante sobre Alice e Bob. Portanto, é impraticável o envio de uma chave codificadora e/ou decodificadora por meio de terceiros, já que Eva

pode interceptá-la. Apresentaremos aqui um método análogo ao que Diffie e Hellman estabeleceram para troca de chaves, utilizando curvas elípticas. Vejamos:

1. Alice e Bob concordam na escolha de uma curva Elíptica E sobre um corpo $\mathbb{Z}_p$ e um ponto $P \in E(\mathbb{Z}_p)$. A curva E, o primo p e o ponto P são chaves públicas.
2. Alice e Bob, individualmente, escolhem uma chave secreta (um número inteiro).
3. Seja n a chave secreta escolhida por Alice e m a chave escolhida por Bob, eles calculam respectivamente os pontos $A = nP \in E(\mathbb{Z}_p)$ e $B = mP \in E(\mathbb{Z}_p)$ e enviam um ao outro.
4. Com os valores de A ou B em mãos, Alice e Bob calculam o ponto $S = nB$ ou $S = mA$.
5. Como $nB = n(mP) = m(nP) = mA$, então ambos encontram o mesmo valor para o ponto $S \in E(\mathbb{Z}_p)$. Esta é a chave secreta que eles dividem e usarão para codificar e decodificar uma mensagem.

Por exemplo, se Alice e Bob concordam em utilizar o ponto $P = (0, 1)$ da Curva Elíptica $E(\mathbb{Z}_{11}) : \ Y^2 = X^3 + 5X + 1$, descrita no Exemplo 5.2, cuja soma de seus pontos pode ser visualizada na Tabela 23, caso Alice escolha sua chave secreta $n = 2$ e Bob escolha como sua chave secreta $m = 3$, eles precisam calcular, respectivamente, os valores $A = nP$ e $B = mP$. Nesse caso, eles encontram

$$A = 2P = (0, 1) \oplus (0, 1) = (9, 4)$$

e

$$B = 3P = 2P \oplus P = (9, 4) \oplus (0, 1) = (7, 4).$$

Alice envia A para Bob, que por sua vez, envia B para Alice. Com os valores de A e B em mãos, Alice calcula

$$S = nB = 2B = (7, 4) \oplus (7, 4) = (6, 4),$$

e Bob calcula

$$S = mA = 3(9, 4) = ((9, 4) \oplus (9, 4)) \oplus (9, 4) = (8, 5) \oplus (9, 4) = (6, 4).$$

Portanto, ambos encontram a mesma chave pública S.

Caso Eva intercepte todas as mensagens enviadas por Alice e Bob, ela obterá as informações E, p, P, A e B. Sendo assim, como $A = nP$ e $B = mP$, para encontrar S, Eva terá de resolver o problema do logaritmo discreto caso queira descobrir a chave.

5.5 O SISTEMA ELGAMAL EM CURVAS ELÍPTICAS

Imaginemos aqui que Bob queira enviar uma mensagem para Alice. Para isso, Alice cria sua chave pública da seguinte forma: Ela escolhe uma curva elíptica E sobre um corpo $\mathbb{Z}_p$ e um ponto P desta curva. Alice escolhe ainda um inteiro m e calcula $B = mP$. Com isso, Alice torna público E, $\mathbb{Z}_p$, P e B, que fazem parte da sua chave pública, sendo sua chave privada apenas o inteiro m. Bob, que quer enviar a mensagem a Alice, por sua vez, procura a chave pública que ela disponibilizou por algum meio, e faz os seguintes passos:

1. Expressa sua mensagem na forma de um ponto $M \in E(\mathbb{Z}_p)$;
2. Escolhe um inteiro aleatório n e calcula $M_1 = nP$;
3. Em seguida, calcula $M_2 = M + nB$, e envia M_1 e M_2 para Alice.

Alice decifra a mensagem enviada por Bob calculando $M_2 - mM_1$. O que funciona, pois

$$M_2 - mM_1 = (M + nB) - m(nP) = M + n(mP) - m(nP) = M.$$

Caso Eva tenha acesso a todas as mensagens enviadas por Bob, Eva conhecerá a chave pública de Alice, ou seja, E, $\mathbb{Z}_p$, P e B, além da mensagem $M_2 - mM_1$, interceptada. Sendo assim, para encontrar M, Eva terá de resolver o problema do logaritmo discreto e os pontos P e B para encontrar o valor de m, além de usar P e M_1 para encontrar o valor de n.

5.6 MAPEANDO UMA MENSAGEM EM UMA CURVA ELÍPTICA

Existem várias formas de expressar uma mensagem na forma de pontos de uma curva elíptica, como a apresentada em Chandravathi, Prapoorna e Padma (2010), mas a que vamos apresentar aqui foi proposta por Reyad (2018).

A ideia consiste em encontrar um ponto G de ordem maior ou igual a 128 em uma curva elíptica de modo que cada símbolo da tabela ASCII seja representado pelo produto de um inteiro k com um ponto G. O inteiro k em questão é o sucessor imediato da representação decimal do símbolo da tabela ASCII a ser mapeado. Por exemplo, se quisermos mapear a letra "A" em uma curva elíptica, escolhemos o ponto G da curva e o multiplicamos por $k = 66$, já que a representação decimal do símbolo "A" na tabela ASCII é 65.

Exemplo 5.6 *Mapeie os caracteres 65 a 90 da tabela ASCII que representam as letras do alfabeto maiúsculo na curva elíptica* $E(\mathbb{Z}_{1459}) : \ Y^2 = X^3 + 805X + 1100$.

Solução: Escolhemos o ponto $G = (301, 22)$, calculamos seus múltiplos e apresentamos os pontos $P_{\mathcal{M}}$'s que representam cada letra do alfabeto maiúsculo mapeada na Tabela 10 a seguir:

Tabela 10 – Alfabeto maiúsculo mapeado na curva elíptica $E(\mathbb{Z}_{1459}) : Y^2 = X^3 + 805X + 1100$.

Símbolo	Código ASCII	kG	$P_{\mathcal{M}}$
A	65	$66G$	$(1305, 1003)$
B	66	$67G$	$(1373, 500)$
C	67	$68G$	$(530, 619)$
D	68	$69G$	$(1291, 245)$
E	69	$70G$	$(5, 307)$
F	70	$71G$	$(398, 1141)$
G	71	$72G$	$(1059, 845)$
H	72	$73G$	$(403, 872)$
I	73	$74G$	$(176, 47)$
J	74	$75G$	$(165, 1118)$
K	75	$76G$	$(230, 779)$
L	76	$77G$	$(677, 1110)$
M	77	$78G$	$(31, 1287)$
N	78	$79G$	$(491, 598)$
O	79	$80G$	$(1393, 722)$
P	80	$81G$	$(81, 755)$
Q	81	$82G$	$(52, 362)$
R	82	$83G$	$(156, 489)$
S	83	$84G$	$(801, 884)$
T	84	$85G$	$(78, 1197)$
U	85	$86G$	$(941, 1093)$
V	86	$87G$	$(659, 1344)$
W	87	$88G$	$(999, 131)$
X	88	$89G$	$(1430, 573)$
Y	89	$90G$	$(995, 226)$
Z	90	$91G$	$(818, 894)$

Fonte: Proprio Autor

■

5.7 ENCRIPTANDO UMA MENSAGEM NO SISTEMA ELGAMAL

Agora Bob vai utilizar o Sistema Elgamal em Curvas elípticas para encriptar a palavra BRASIL e enviá-la a Alice. Vejamos:

Primeiramente Alice cria sua chave pública escolhendo a curva elíptica $E(\mathbb{Z}_{1459}) : Y^2 = X^3 + 805X + 1100$, e o ponto $P = (301, 22)$. Alice escolhe também o inteiro $m = 5$ e calcula $B = mP \Rightarrow B = 5(301, 22) = (247, 249)$. Em seguida, ela torna público a curva, o corpo e os pontos P e B.

Bob encontra os dados públicos disponibilizados por Alice e expressa sua mensagem na forma de pontos $P_{\mathcal{M}}$'s. Observe que a curva escolhida por Alice é a mesma do Exemplo 5.6 e o ponto P é o mesmo ponto G utilizado para construir a Tabela 10. Logo, as letras do alfabeto já estão mapeadas. Sendo assim, os pontos que Bob irá utilizar são

$P_B = (1373, 500)$, $P_R = (156, 489)$, $P_A = (1305, 1003)$, $P_S = (801, 884)$, $P_I = (176, 47)$ e $P_L = (677, 1110)$.

- Para encriptar $P_B = (1373, 500)$, Bob escolhe um inteiro aleatório $n = 8$ e calcula o ponto $M_1 = nP = 8(301, 22)$.

$$\begin{aligned} 2P &= P \oplus P = (301, 22) \oplus (301, 22) = (1321, 419); \\ 4P &= 2P \oplus 2P = (1321, 419) \oplus (1321, 419) = (1395, 757); \\ 8P &= 4P \oplus 4P = (1395, 757) \oplus (1395, 757) = (796, 633). \end{aligned}$$

  Sendo assim, $M_1 = (796, 633)$.
  Em seguida Bob calcula $M_2 = P_B \oplus nB = (1373, 500) \oplus 8B$. Temos que

$$\begin{aligned} 2B &= B \oplus B = (247, 249) \oplus (247, 249) = (67, 137); \\ 4B &= 2B \oplus 2B = (67, 137) \oplus (67, 137) = (1131, 1428); \\ 8B &= 4B \oplus 4B = (1131, 1428) \oplus (1131, 1428) = (1051, 471). \end{aligned}$$

  Portanto, $M_2 = (1373, 500) \oplus (1051, 471) = (595, 1165)$.
- Para encriptar $P_R = (156, 489)$, Bob escolhe um inteiro aleatório $n = 6$ e calcula o ponto $M_1 = nP = 6(301, 22)$. Sabemos que $4P = (1395, 757)$ e $2P = (1321, 419)$. Como $6P = 4P \oplus 2P$, então

$$M_1 = (1395, 757) \oplus (1321, 419) = (679, 108).$$

  Em seguida Bob calcula $M_2 = P_R \oplus nB = (156, 489) \oplus 6B$. Temos que $4B$ e $2B$ são, respectivamente, $(67, 137)$ e $(1131, 1428)$. Temos ainda que $6B = 4B \oplus 2B$, portanto,

$$6B = (67, 137) \oplus (1131, 1428) = (1134, 569).$$

  Logo, $M_2 = (156, 489) \oplus (1134, 569) = (394, 318)$.
- Para encriptar $P_A = (1305, 1003)$, Bob escolhe um inteiro aleatório $n = 10$ e calcula o ponto $M_1 = nP = 10(301, 22)$. Sabemos que $8P = (796, 633)$ e $2P = (1321, 419)$. Como $10P = 8P \oplus 2P$, então

$$M_1 = (796, 633) \oplus (1321, 419) = (67, 137).$$

  Em seguida Bob calcula $M_2 = P_A \oplus nB = (1305, 1003) \oplus 10B$. Temos que $8B$ e $2B$ são, respectivamente, $(1051, 471)$ e $(1131, 1428)$. Temos ainda que $10B = 8B \oplus 2B$, portanto,

$$10B = (1051, 471) \oplus (1131, 1428) = (1260, 493).$$

  Logo, $M_2 = (1305, 1003) \oplus (1260, 493) = (1292, 117)$.

- Para encriptar $P_S = (801, 884)$, Bob escolhe um inteiro aleatório $n = 4$ e calcula o ponto $M_1 = nP = 4(301, 22) = (1395, 757)$.
  Em seguida Bob calcula $M_2 = P_S \oplus nB = (801, 884) \oplus 4B$. Portanto,

$$M_2 = (801, 884) \oplus (1131, 1428) = (225, 39).$$

- Para encriptar $P_I = (176, 47)$, Bob escolhe como inteiro aleatório o $n = 2$ e calcula o ponto $M_1 = nP = 2(301, 22) = (1321, 419)$.
  Em seguida Bob calcula $M_2 = P_I \oplus nB = (176, 47) \oplus 2B$. Portanto,

$$M_2 = (176, 47) \oplus (67, 137) = (801, 884).$$

- Para encriptar $P_L = (677, 1110)$, Bob escolhe um inteiro aleatório $n = 16$ e calcula o ponto $M_1 = nP = 16(301, 22)$. Sabemos que $8P = (796, 633)$. Como $16P = 8P \oplus 8P$, então

$$M_1 = (796, 633) \oplus (796, 633) = (126, 550).$$

  Em seguida Bob calcula $M_2 = P_L \oplus nB = (677, 1110) \oplus 16B$. Temos que $8B = (1051, 471)$ e que $16B = 8B \oplus 8B$, portanto,

$$16B = (1051, 471) \oplus (1051, 471) = (1393, 722).$$

  Logo, $M_2 = (677, 1110) \oplus (1393, 722) = (171, 572)$.

Com isso, Bob envia a Alice o conjunto de pares (M_1, M_2), que por sua vez, precisa decodificá-los para que possa entender a mensagem enviada por Bob. Para isso, para cada par (M_1, M_2), Alice deve calcular $M = M_2 - mM_1$.

Lembremos que o ponto $-mM_1$ é o simétrico do ponto mM_1. Logo, Alice calcula primeiramente mM_1 para então identificar seu simétrico.

- Para decodificar o par $M_1 = (796, 633)$ e $M_2 = (595, 1165)$, como $m = 5$, temos que encontrar $5M_1$.

$$\begin{aligned} 2M_1 &= M_1 \oplus M_1 = (796, 633) \oplus (796, 633) = (126, 550); \\ 4M_1 &= 2M_1 \oplus 2M_1 = (126, 550) \oplus (126, 550) = (512, 867); \\ 5M_1 &= 4M_1 \oplus M_1 = (512, 867) \oplus (796, 633) = (1051, 471). \end{aligned}$$

  Sendo assim, $-5M_1 = (1051, -471)$.
  Portanto, $M = M_2 - mM_1 = (595, 1165) \oplus (1051, -471) = (1373, 500)$.
- Para decodificar o par $M_1 = (679, 108)$ e $M_2 = (394, 318)$, precisamos encontrar $5M_1$.

$$2M_1 = M_1 \oplus M_1 = (679, 108) \oplus (679, 108) = (1456, 514);$$

$$\begin{aligned} 4M_1 &= 2M_1 \oplus 2M_1 = (1456, 514) \oplus (1456, 514) = (1323, 519); \\ 5M_1 &= 4M_1 \oplus M_1 = (1323, 519) \oplus (679, 108) = (1134, 569). \end{aligned}$$

Sendo assim, $-5M_1 = (1134, -569)$.
Portanto, $M = M_2 - mM_1 = (394, 318) \oplus (1134, -569) = (156, 489)$.

- Para decodificar o par $M_1 = (67, 137)$ e $M_2 = (1292, 117)$, precisamos encontrar $5M_1$.

$$\begin{aligned} 2M_1 &= M_1 \oplus M_1 = (67, 137) \oplus (67, 137) = (1131, 1428); \\ 4M_1 &= 2M_1 \oplus 2M_1 = (1131, 1428) \oplus (1131, 1428) = (1051, 471); \\ 5M_1 &= 4M_1 \oplus M_1 = (1051, 471) \oplus (67, 137) = (1260, 493). \end{aligned}$$

Sendo assim, $-5M_1 = (1260, -493)$.
Portanto, $M = M_2 - mM_1 = (1292, 117) \oplus (1260, -493) = (1305, 1003)$.

- Para decodificar o par $M_1 = (1395, 757)$ e $M_2 = (225, 39)$, precisamos encontrar $5M_1$.

$$\begin{aligned} 2M_1 &= M_1 \oplus M_1 = (1395, 757) \oplus (1395, 757) = (796, 633); \\ 4M_1 &= 2M_1 \oplus 2M_1 = (796, 633) \oplus (796, 633) = (126, 550); \\ 5M_1 &= 4M_1 \oplus M_1 = (126, 550) \oplus (1395, 757) = (1131, 1428). \end{aligned}$$

Sendo assim, $-5M_1 = (1131, -1428)$.
Portanto, $M = M_2 - mM_1 = (225, 39) \oplus (1131, -1428) = (801, 884)$.

- Para decodificar o par $M_1 = (1321, 419)$ e $M_2 = (801, 884)$, precisamos encontrar $5M_1$.

$$\begin{aligned} 2M_1 &= M_1 \oplus M_1 = (1321, 419) \oplus (1321, 419) = (1395, 757); \\ 4M_1 &= 2M_1 \oplus 2M_1 = (1395, 757) \oplus (1395, 757) = (796, 633); \\ 5M_1 &= 4M_1 \oplus M_1 = (796, 633) \oplus (1321, 419) = (67, 137). \end{aligned}$$

Sendo assim, $-5M_1 = (67, -137)$.
Portanto, $M = M_2 - mM_1 = (801, 884) \oplus (67, -137) = (176, 47)$.

- Para decodificar o par $M_1 = (126, 550)$ e $M_2 = (171, 572)$, precisamos encontrar $5M_1$.

$$\begin{aligned} 2M_1 &= M_1 \oplus M_1 = (126, 550) \oplus (126, 550) = (512, 867); \\ 4M_1 &= 2M_1 \oplus 2M_1 = (512, 867) \oplus (512, 867) = (645, 888); \\ 5M_1 &= 4M_1 \oplus M_1 = (645, 888) \oplus (126, 550) = (1393, 722). \end{aligned}$$

Sendo assim, $-5M_1 = (1393, -722)$.

Portanto, $M = M_2 - mM_1 = (171, 572) \oplus (1393, -722) = (677, 1110)$.

Encontrados os valores dos M's, Alice então consegue fazer a leitura da mensagem "BRASIL" após associar cada ponto M com sua letra correspondente através da Tabela 10.

As situações citadas abaixo são alguns dos motivos da criptografia por curvas elípticas, ou em inglês, *Elliptic Curve Cryptography (ECC)* não ter sido tão difundida.

> As operações matemáticas contidas no modelo de curvas elípticas são consideralvelmente mais sofisticadas do que as operações do RSA. Um problema em relação ao criptossistema ECC é o fato de se definir alguns parâmetros antes de executar o algoritmo de cifragem/decifragem, sendo estes parâmetros não comuns em outros criptossistemas. Devemos definir inicialmente um corpo finito e, em seguida, definir a curva elíptica para que possamos gerar o grupo elíptico sobre o qual as operações serão definidas. A questão de se definir estes parâmetros já é um empecilho para a adoção do criptossistema ECC, pois são questões matemáticas de certa complexidade e fundamentais para a segurança do criptossistema, o que acarreta em maior complexidade para implementação. Uma possível consequência de uma má escolha de parâmetros é um baixo desempenho do criptossistema, o que torna a sua utilização inviável ou insegura. (HENRIQUES, SANGALLI e TARAPANOFF, 2012, p. 112).

Mais informações sobre Criptografia por Curvas Elípticas podem ser encontradas em Silverman (1992) e em Koblitz, Menezes e Vanstone (2000).

6 CONCLUSÃO

A criptografia evoluiu bastante com o passar do tempo e a isso muito se deve o fato de que sempre existiram curiosos afim de descobrir o segredo alheio. À medida que os criptossistemas foram quebrados, houve a necessidade de ser criado um novo criptossistema mais seguro. Portanto, a guerra entre os criadores de criptossistemas e os criptólogos existe a muito tempo e foi essencial para que a criptografia evoluísse para o que é hoje.

A cifra de César, uma cifra de substituição monoalfabética pode ser facilmente quebrada com a utilização da análise de frequências, já a cifra "indecifrável" de Vigenère, que também é de substituição, porém, polialfabética, também pode ser decifrada através da análise de frequências. Ou seja, a matemática já se fazia presente na quebra dessas cifras de substituição.

O rumo da primeira guerra mundial mudou após a descoberta do conteúdo escrito no Telegrama Zimmermann, já a segunda guerra foi encurtada muito devido a Enigma ser decifrada.

Por trás da criptografia RSA existe muita teoria dos números, principalmente aritmética modular. Esse sistema criptográfico é muito eficaz pois além de não haver necessidade de emissor e receptor de uma mensagem se encontrarem para definir uma chave para encriptar e decriptar uma mensagem, também não existe a necessidade de esconder uma determinada chave, podendo torná-la pública. Porém existe uma chave secreta que é usada na criação da chave pública. O mesmo ocorre na criptografia por curvas elípticas onde alguns parâmetros são públicos.

A criptografia por curvas elípticas sobre um corpo $\mathbb{Z}_p$ é possível devido a possibilidade de "somar" dois pontos de uma curva elíptica. Tal operação gera um grupo abeliano devido a existência de um ponto no infinito $\mathcal{O}$ que é usado como elemento neutro da adição, onde usamos a Geometria Descritiva para justificá-lo.

Podemos perceber que nem a criptografia RSA nem a criptografia por curvas elípticas é indecifrável, pelo contrário, sabe-se bem a forma necessária de decifrar uma mensagem encriptada com elas. No caso da RSA, fatorar o número inteiro $N = pq$ é o problema a ser resolvido. Já no caso das curvas elípticas, encontrar o logaritmo discreto significa encontrar a chave utilizada naquela encriptação. Porém, em ambos os casos essa tarefa pode ser impraticável por conta do número muito grande de possibilidades. A solução para a quebra dessas cifras serem efetivas seria encontrar um método que sirva para todas as mensagens encriptadas com uma determinada cifra, ou até mesmo um método que consiga decifrar qualquer criptossistema usado.

A guerra entre aqueles que buscam guardar segredos e aqueles que buscam decifrá-los aparentemente ainda não acabou. Dizemos "aparentemente" pois desconhecemos qualquer método que resolva o problema da fatoração de inteiros ou do logaritmo

discreto de forma rápida, porém, o fato de desconhecermos tal método não significa que este não existe, pois aquele que por ventura tenha encontrado tal método muito provavelmente não irá divulga-lo facilmente, afinal, estaríamos lidando com alguém capaz de desvendar segredos de todo o mundo. Perceba que apesar de Bletchley Park ter vencido a Enigma, durante muito tempo esta vitória ficou em segredo, afinal, não adianta vencer um criptossistema e não obter vantagem com isso.

Nem mesmo a criação de um criptossistema perfeito, indecifrável, ou de um método capaz de decifrar qualquer criptossistema seria o fim da guerra entre criptoanalistas e criptólogos, uma vez que durante a história imaginou-se ter sido criado sistemas indecifráveis e mesmo assim os criptólogos continuaram tentando vencer esses criptossistemas. Acreditamos que hoje não seria diferente.

A matemática que faz os sistemas de assinatura digital funcionar é muito semelhante à da criptografia RSA ou por curvas elípticas, por isso resolvemos incluir este assunto que está cada vez mais necessário no Apêndice deste trabalho. Imagine não precisar mais ir fisicamente a qualquer local apenas para assinar um documento, ou até mesmo escapar de um golpe devido a não autenticação de uma assinatura falsa. A assinatura digital já é uma realidade, e a menos que se consiga burlar esses sistemas matematicamente tão seguros, a assinatura digital passará a ser cada vez mais utilizada.

Por fim, acreditamos que este trabalho traz consigo um vasto material sobre criptografia possibilitando que o leitor construa uma visão mais integrada da Matemática, na perspectiva de sua aplicação à realidade, como pede a própria BNCC (BRASIL, 2018). Por si só, a criptografia é um assunto muito atraente, mas não é só na proteção de dados que a matemática pode ser aplicada, mas também na música, nos negócios, nas engenharias e em várias outras áreas. A matemática vai muito além de uma simples disciplina do currículo da educação básica.

REFERÊNCIAS

ANDRADE, P. F. A.; BARROS, A. A. **Introdução à Geometria Projetiva**. Rio de Janeiro: Coleção textos universitários SBM, 2010.

BRASIL. Base Nacional Comum Curricular. Brasília: Ministério da Educação, 2018.

CHANDRAVATHI, D.; ROJA, P.Prapoorna; Bh, PADMA. Encoding And Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz's Method. **(IJCSE) International Journal on Computer Science and Engineering**, v. 2, n. 5, p. 1904–1907, 2010.

CORON, Jean S.; LEFRAN, David; POUPARD, Guillaume. A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis. **Cryptographic hardware and embedded systems - CHES 2005 (Edinburgh, 29 August - 1 September 2005),** Berlim : Springer, v. 3659, p. 47–60, 2005.

COUTINHO, S. C. **Números inteiros e criptografia RSA.** 2. ed. Rio de Janeiro: IMPA, 2011.

COUTINHO, Severino. **Criptografia**. Rio de Janeiro: IMPA, 2016.

DOMINGUES, Hygino H.; IEZZI, Gelson. **Álgebra moderna**. 4.ed. Reform. São Paulo: Atual, 2003.

FERNANDES, Cláudio. **Máquina Enigma.** Brasil Escola, 2013. Disponível em: <https://brasilescola.uol.com.br/historiag/maquina-enigma.htm.>. Acesso em: 05 dez. 2021.

FISCHER, Eric. **The Evolution of Character Codes, 1874-1968**. Autoedición, 2015.

GONÇALVES, Tiago da Silva. **Uma Introdução à Geometria Projetiva para o Ensino Fundamental.** Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal do Rio Grande, Rio Grande do Sul, 2013.

GUIDORIZZI, Hamilton. **Um curso de Cálculo. Volume 1.** 5.ed. São Paulo: LTC, 1995.

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

HENRIQUES, M.A.A.; SANGALLI, L. A.; TARAPANOFF, K. Criptossistemas Baseados em Curvas Elpticas e seus Desafios, 04/2012, Científico Nacional, **V Encontro dos Alunos e Docentes do Departamento de Engenharia de Computação (EADCA)**, Vol. 1, pp.110-113, Campinas., 2012.

HOFFSTEIN, Jeffrey; PIPHER, Jill; SILVERMAN, Joseph H. **An Introduction to Mathematical Cryptography.** New York: Springer, 2008.

KOBLITZ, Neal; MENEZES, Alfred; VANSTONE, Scott. The State of Elliptic Curve Cryptography. **Designs, Codes and Cryptography**, v. 19, p. 173–193, 2000.

MAHTO, D.; K., YADAV D. Rsa and ECC: A comparative analysis. **International Journal of Applied Engineering Research**, v. 12, n. 19, p. 9053–9061, 2017.

MENEZES, A. J.; OKOMOTO, T.; VANSTONE, S. A. Reducing elliptic curve logarithms in a finite field. **IEEE Transaction on Information Theory**, v. 39, n. 5, p. 1639–1646, 1993.

MORIMOTO, Carlos Hitoshi; HASHIMOTO, Ronaldo Fumio. **Introdução à Ciência da Computação Usando a Linguagem C**. Compilação de notas de aulas utilizadas em disciplinas introdutórias do Departamento de Ciência da Computação do Instituto de Matemática e Estatística da Universidade de São Paulo, 2010.

OBMEP, CLUBE DE MATEMÁTICA DA. **Fatorando de um jeito diferente.**, 2010. Disponível em: <http://clubes.obmep.org.br/blog/fatorando-de-um-jeito-diferente/>. Acesso em: 27 nov. 2021.

OLIVEIRA, Francisco Erilson Freire de. **Sobre Várias Demonstrações do Pequeno Teorema de Fermat e as Inter-relações entre as Áreas da Matemática**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal do Ceará, Fortaleza, 2019.

REINHOLD, C. **Criptografia.**, 2020. Disponível em: <https://cgreinhold.dev/2020/03/13/criptografia/>. Acesso em: 09 set. 2021.

REYAD, Omar. "Text Message Encoding Based on Elliptic Curve Cryptography and a Mapping Methodology. **Information Sciences Letters :**Vol. 7, 2018.

SANTOS, J.P. de O. **Introdução à Teoria dos Números.** Rio de Janeiro: Coleção Matemática Universitária, IMPA, 2000.

SAUTOY, Marcus Du. **A música dos números primos:** a história de um problema não resolvido na matemática. Rio de Janeiro: ZAHAR, 2007.

SILVERMAN, J.H. **The Arithmetic of Elliptic Curves**. 2. ed. New York: Springer, 1992.

SINGH, Simon. **O livro dos códigos**. 11. ed. Rio de Janeiro: Record, 2020.

SMART, N. The Discrete Logarithm Problem on Elliptic Curves of Trace One. **Journal**

of Cryptology, New York: Springer-Verlag , v. 12, p. 193–196, 1999.

WASHINGTON, Lawrence C. **Elliptic Curves:**number theory and criptography. 2. ed. Boca Raton: Chapman e Hall, 2008.

APÊNDICE A – ASSINATURA DIGITAL

Sabemos que a internet nos possibilita realizar diversas tarefas de forma ágil. Uma destas tarefas é a assinatura de documentos de forma digital. Acordos e negócios podem ser feitos sem que haja necessidade de um encontro entre as partes, tudo pode ser feito de forma digital. A assinatura digital pode facilitar a autenticidade de pedidos em comércio eletrônico, identificação de sites da internet, acompanhamento e aditamento de processos judiciais, bem como a assinatura de documentos em geral. Por exemplo, seu computador reconhece se uma determinada atualização veio ou não do fabricante através de uma assinatura digital. A segurança de um sistema de assinatura digital tem muito da matemática utilizada na criptografia de chave pública. Vamos expor aqui os algoritmos padrões de assinatura digital, o *Digital Standard Algorithm (DSA)* e o *Elliptic Curve Digital Standard Algorithm (ECDSA)*.

I – ALGORITMO PADRÃO DE ASSINATURA DIGITAL.

O DSA é um sistema de assinatura digital que se utiliza da dificuldade de resolver o Problema do Logaritmo discreto. Vejamos o algoritmo a seguir:

Primeiramente é necessário criar os parâmetros públicos:

1. Escolher primos p e q de modo que $p \equiv 1 \mod p$;

2. Escolher um inteiro g de ordem $q \mod p$.

Em seguida, cria-se uma chave:

3. Escolher um inteiro secreto a, tal que $1 < a < q - 1$;

4. Calcular $A = g^a \mod p$;

5. Publicar a chave de verificação A.

O processo de assinatura funciona da seguinte forma:

6. Seja D um documento a ser assinado, calcula-se $D \mod q$; 7. Escolhe-se um inteiro aleatório k, tal que $1 < k < q$; 8. A assinatura de D são os valores S_1 e S_2 tais que

$$\begin{cases} S_1 \equiv (g^k \mod p) \mod q \\ S_2 \equiv (D + aS_1)k^{-1} \mod q \end{cases}$$

Para verificar a assinatura, é necessário calcular V_1 e V_2 tais que

$$\begin{cases} V_1 \equiv DS_2^{-1} \mod q \\ V_2 \equiv S_1 S_2^{-1} \mod q \end{cases}$$

e verificar se

$$(g^{V_1} A^{V_2} \mod p) \mod q = S_1.$$

Se for, a assinatura é verdadeira.

É fácil ver que a verificação funciona, pois como

$$V_1 \equiv DS_2^{-1} \mod q,\ V_2 \equiv S_1 S_2^{-1} \mod q \text{ e } A = g^a \mod p,$$

então

$$(g^{V_1} A^{V_2} \mod p) \mod q \equiv (g^{DS_2^{-1}} g^{a \cdot S_1 S_2^{-1}} \mod p) \mod q \Rightarrow$$

$$\Rightarrow (g^{V_1} A^{V_2} \mod p) \mod q \equiv (g^{S_2^{-1}(D+aS_1)} \mod p) \mod q. \tag{36}$$

Como $S_2 \equiv (D + aS_1)k^{-1} \mod q$, então $S_2^{-1} \equiv k \cdot (D + aS_1)^{-1} \mod q$. Dessa forma, a congruência (36) pode ser reescrita como

$$(g^{V_1} A^{V_2} \mod p) \mod q \equiv (g^{k \cdot (D+aS_1)^{-1}(D+aS_1)} \mod p) \mod q \Rightarrow$$

$$\Rightarrow (g^{V_1} A^{V_2} \mod p) \mod q \equiv (g^k \mod p) \mod q = S_1.$$

Exemplo 1. Escolhemos o inteiro secreto $a = 5$ para assinar o documento $D = 8$ com

os parâmetros a seguir:

$$\begin{cases} p = 23 \\ q = 11 \\ g = 2. \end{cases}$$

Calculamos $A = 2^5 \mod 23 \Rightarrow A = 9$, que será a chave de verificação a ser publicada.

Para assinar um documento $D = 8 \mod q$, escolhe-se um inteiro aleatório k tal que $1 < k < q$. Escolhendo $k = 3$, calculamos a chave (S_1, S_2).

$$\begin{cases} S_1 \equiv (g^k \mod p) \mod q \\ S_2 \equiv (D + aS_1)k^{-1} \mod q \end{cases} \Rightarrow \begin{cases} S_1 \equiv (2^3 \mod 23) \mod 11 \\ S_2 \equiv (8 + 5 \cdot 8) \cdot 4 \mod 11 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} S_1 \equiv 8 \mod 11 \\ S_2 \equiv 192 \mod 11 \end{cases} \Rightarrow \begin{cases} S_1 = 8 \\ S_2 = 5 \end{cases}$$

O verificador vai calcular os valores V_1 e V_2. Vejamos:

$$\begin{cases} V_1 \equiv DS_2^{-1} \mod q \\ V_2 \equiv S_1 S_2^{-1} \mod q \end{cases} \Rightarrow \begin{cases} V_1 \equiv 8 \cdot 9 \mod 11 \\ V_2 \equiv 8 \cdot 9 \mod 11 \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} V_1 = 6 \\ V_2 = 6 \end{cases}$$

O próximo passo é verificar se $S_1 \equiv (g^{V_1} A^{V_2} \mod p) \mod q$.

Temos que

$$(g^{V_1} A^{V_2} \mod p) \mod q = (2^6 \cdot 9^6 \mod 23) \mod 11 \Rightarrow$$

$$\Rightarrow (18 \cdot 3 \mod 23) \mod 11 \Rightarrow (54 \mod 23) \mod 11 \equiv 8 \mod 11 = S_1.$$

Portanto, a assinatura é verdadeira.

O DSA pode ser adaptado para o uso de curvas elípticas, onde o Problema do logaritmo discreto é ainda mais difícil de ser resolvido. Essa adaptação é o que veremos na seção a seguir, o *Curve Digital Signature Algorithm (ECDSA).*

II – O ALGORITMO PADRÃO DE ASSINATURA DIGITAL POR CURVAS ELÍPTICAS.

Para a criação de uma chave é necessário escolher uma curva E sobre um corpo $\mathbb{Z}_p$, um ponto $G \in E(\mathbb{Z}_p)$ de ordem n. Define-se também um inteiro secreto d, tal que $1 \leqslant d < p$. Calcula-se o ponto $Q = dG$. E torna público a curva E, o corpo $\mathbb{Z}_p$ e os pontos G e Q.

Para assinar um documento D, escolhe um inteiro aleatório k, tal que $1 \leqslant k < p$ e calcula-se o ponto $kG = (x_1, y_1)$. Os valores r e s tais que

$$\begin{cases} r \equiv x_1 \mod n \\ s \equiv k^{-1}(D + dr) \mod n \end{cases}$$

é a assinatura de D.

Para checar a veracidade da assinatura, considere $w \equiv s^{-1} \mod p$ e calcule os valores U_1 e U_2 tais que

$$\begin{cases} U_1 \equiv Dw \mod n \\ U_2 \equiv rw \mod n \end{cases}$$

Calcula-se então o ponto $(x_2, y_2) = U_1G \oplus U_2Q$. Seja $v \equiv x_2 \mod n$, se $v = r$, então a assinatura é verdadeira.

Vejamos porque a verificação funciona: Desde que $s \equiv k^{-1}(D + dr) \mod n$, temos que

$$s \equiv k^{-1}(D + dr) \mod n \Rightarrow k \equiv (s^{-1}D + s^{-1}dr) \mod n \Rightarrow$$

$$\Rightarrow k \equiv (wD + wdr) \mod n. \tag{37}$$

Como $U_1 = Dw \mod n$ e $U_2 = rw \mod n$, podemos reescrever a congruência 37 como

$$\Rightarrow k \equiv (U_1 + U_2 d) \mod n. \tag{38}$$

Observe que devido o fato de que $Q = dG$, temos que

$$U_1G \oplus U_2Q \equiv U_1G \oplus U_2dG \mod n \Rightarrow U_1G \oplus U_2Q \equiv (U_1 + U_2d)G \mod n,$$

e aplicando isso em 38, obtemos

$$kG \equiv U_1G \oplus U_2Q \mod n. \tag{39}$$

Porém, $kG = (x_1, y_1)$ e $U_1G \oplus U_2Q = (x_2, y_2)$. Com isso, a congruência 39 nos diz que $x_1 \equiv x_2 \mod n \Rightarrow r \equiv v \mod n$.

Exemplo 2. Escolhemos o inteiro secreto $d = 5$ para assinarmos o documento $D = 10$ com os parâmetros a seguir:

$$\begin{cases} E(\mathbb{Z}_{11}): \ Y^2 = X^3 + 5X + 1 \\ \qquad\qquad\qquad\qquad G = (0, 10). \end{cases}$$

Primeiramente calcula-se o ponto $Q = dG \Rightarrow Q = 5(0, 10)$.

Observe que a curva elíptica em questão é a mesma utilizada no Exemplo 5.2, cuja soma de seus pontos foi expressa na Tabela 23. Sendo assim, temos que

$$\begin{aligned} 2G &= G \oplus G = (0, 10) \oplus (0, 10) = (9, 7) \\ 4G &= 2G \oplus 2G = (9, 7) \oplus (9, 7) = (8, 6) \\ 5G &= 4G \oplus G = (8, 6) \oplus (0, 10) = (6, 4). \end{aligned}$$

Logo, $Q = 5G = (6, 4)$. Com isso, torna-se público a curva $E(\mathbb{Z}_{11}): \ Y^2 = X^3 + 5X + 1$ e os ponto $G = (0, 10)$ e $Q = (6, 4)$.

Para fazermos a assinatura é necessário escolher um inteiro positivo menor que 11. Seja tal inteiro o número $k = 8$, devemos agora calcular o ponto $kG = (x_1, y_1)$. Sabemos que $4G = (8, 6)$, então

$$8G = 4G \oplus 4G = (8, 6) \oplus (8, 6) = (7, 4).$$

Dessa forma temos que $x_1 = 7$ e $y_1 = 4$. Precisamos agora calcular os valores r e s tais que

$$\begin{cases} r \equiv x_1 \mod n \\ s \equiv k^{-1}(D + dr) \mod n \end{cases}$$

que é a assinatura de D. Fazendo as devidas substituições, temos que

$$\begin{cases} r \equiv 7 \mod 11 \Rightarrow r = 7 \\ s \equiv 8^{-1}(10 + 5r) \mod 11 \end{cases} \Rightarrow s \equiv 7(10 + 5 \cdot 7) \mod 11 \Rightarrow s \equiv 315 \mod 11 \Rightarrow s = 7.$$

Logo, a assinatura de D é o par $r = 7$ e $s = 7$.

Para checar esta assinatura, devemos considerar $w \equiv s^{-1} \mod p$. Sendo assim, temos que $w \equiv 7^{-1} \mod 11 \Rightarrow w = 8$. Agora devemos calcular os valores U_1 e U_2 tais que

$$\begin{cases} U_1 \equiv Dw \mod n \\ U_2 \equiv rw \mod n \end{cases}$$

Fazendo as devidas substituições, obtemos

$$\begin{cases} U_1 \equiv 10 \cdot 8 \mod 11 \\ U_2 \equiv 7 \cdot 8 \mod 11 \end{cases} \Rightarrow \begin{cases} U_1 \equiv 80 \mod 11 \\ U_2 \equiv 56 \mod 11 \end{cases} \Rightarrow \begin{cases} U_1 = 3 \\ U_2 = 1. \end{cases}$$

Calcula-se então o ponto $(x_2, y_2) = U_1G + U_2Q$. Seja $v \equiv x_2 \mod 11$, se $v = r$, então a assinatura é verdadeira. Neste caso, $(x_2, y_2) = U_1G + U_2Q = 3(0, 10) + 1(6, 4)$. Sabemos que $2G = (9, 7)$ e que $3G = 2G \oplus G = (9, 7) \oplus (0, 10) = (7, 7)$. Portanto,

$$(x_2, y_2) = (7, 7) \oplus (6, 4) = (7, 4).$$

Logo, temos que $x_2 = 7$ e $y_2 = 4$. Como $v \equiv x_2 \mod 11$, então $v \equiv 7 \mod 11 \Rightarrow v = 7$. Como $v = r = 7$, então temos uma assinatura verdadeira.