Universidade Federal do Oeste da Bahia

Centro das Ciências Exatas e da Tecnologia

Criptografia: aplicação de funções, matrizes e aritmética modular

por

Adilson Oliveira da Silva

Barreiras

2021

Adilson Oliveira da Silva

Criptografia: aplicação de funções, matrizes e aritmética modular

Dissertação apresentada ao Programa de Pós-Graduação em Nível de Mestrado Profissional em Matemática- PROFMAT da Universidade Federal do Oeste da Bahia, como requisito parcial para a obtenção do título de mestre.
Orientador: Prof. Dr. Bruno Trindade Reis

Barreiras
2021

Adilson Oliveira da Silva

Criptografia: aplicação de funções, matrizes e aritmética modular

Dissertação como requisito para a obtenção do grau de Mestre Profissional em Matemática da Universidade Federal do Oeste da Bahia.

Aprovada em 26 de novembro de 2021.

Banca Examinadora

Prof. Dr. Bruno Trindade Reis- Orientador (UFOB)

Prof. Dr. Edvaldo Elias de Almeida Batista (UFOB)

Prof. Dr. Alex Carrazedo Dantas (UNB)

FICHA CATALOGRÁFICA

S586 Silva, Adilson Oliveira da

Criptografia: aplicação de funções, matrizes e aritmética modular. / Adilson Oliveira da Silva. – 2021.

45f.:

Orientador: Prof. Dr. Bruno Trindade Reis

Dissertação – PROFMAT – Mestrado Profissional em Matemática em Rede Nacional, Universidade Federal do Oeste da Bahia. Centro das Ciências Exatas e das Tecnologias - Barreiras, BA, 2021.

1. Matemática – Estudo e Ensino. I. Reis, Bruno Trindade. II. Universidade Federal do Oeste da Bahia – Centro das Ciências Exatas e das Tecnologias. III. Título.

CDD 510.07

Biblioteca Universitária de Barreiras – UFOB

Agradecimentos

Agradeço a Deus por essa vitória alcançada, à minha amada esposa Ywane V. Guimarães Santana Oliveira, ao meu querido filho Jaaziel Guimarães Oliveira, aos meus familiares, aos meus amigos e aos meus colegas.

Resumo

O presente trabalho mostra a importância da criptografia em nossas vidas, principalmente nos dias atuais com o advento dos computadores e da internet. Apresentamos a criptografia como mecanismo para o professor de matemática da educação básica ensinar funções, matrizes, aritmética modular e relação de equivalência. Foi apresentado um pouco da história da criptografia, assim como sua importância em nossas vidas. Mostramos uma aplicação destes conteúdos na criptografia para que houvesse um interesse em estudar tais conteúdos. Apresentamos alguns conceitos de funções e de matrizes que são utilizados na criptografia como função afim, função injetora, sobrejetora e bijetora, composição de função e função inversa, apresentamos também alguns tipos especiais de matrizes, determinante de uma matriz e matriz inversível. Para aplicar esses conteúdos na criptografia apresentamos alguns métodos para cifrar e decifrar textos. Finalizamos o presente trabalho mostrando algumas sugestões para os professores do ensino fundamental e médio trabalhar estes conteúdos.

Palavras-chave: Criptografia, Aritmética modular, Funções, Matrizes.

Abstract

The present work shows the importance of encryption in our lives, especially in today with the advent of computers and the Internet. We present cryptography as a mechanism for the mathematics teacher of basic education to teach functions, matrices, modular archethretics and equivalence ratio. It was presented some of the history of cryptography, as well as its importance in our lives. We showed an application of these contents in cryptography so that there was an interest in studying such content. We present some concepts of functions and matrices that are used in cryptography as a function, injector function, injector and bijeor, function composition and inverse function, we also present some special types of matrices, determinant of a matrix and inverter matrix. To apply these contents in cryptography we present some methods for encrypting and deciphering texts. We conclude the present work by showing some suggestions for elementary and high school teachers to work on these contents.

Keywords: Encryption, Modular Aritmetics, Functions, Matrices.

Conteúdo

Capítulo 1

Introdução

Neste presente trabalho falaremos sobre a aplicação de alguns conteúdos da matemática básica aplicados na criptografia, tais como: funções, matrizes, relações de equivalência, congruência módulo m e algumas técnicas de contagem. A palavra criptografia é de origem grega, derivada da palavra *kriptos* que significa oculto, portanto, criptogrfia significa escrita oculta. Na prática, a criptografia tem o papel de ocultar um texto de terceiros, de forma que somente o emissor e o recptor possa ler o texto. Todos nós temos algo importante que não pode ser descorberto por pessoas que não fazem parte da nossa vida, principalmente pessoas que são mal intencionadas, por isso a criptografia faz parte da nossa vida. Muitos já utilizam a criptografia desde os tempos de criança, muitas crianças para conversarem na frente dos adultos ou até mesmo diante de outras crianças que não entendem seus códigos e não serem entendidas por estas pessoas, criam seus métodos de codificar suas mensagens. Por exemplo, um método bastante conhecido e utilizado por crianças e adolescente é a lingua do "p", que consite em acrescentar depois de cada vogal a letra p e a própria vogal, assim por exemplo, a palavra GATO ficaria GAPATOPO. Esta é uma brincadeira de criança, mas serve para proteger suas mensagens, ainda que esse sigilo pode ser quebrado facilmente.

Um método de criptografia bem famoso e muito antigo é a cifra de César. Este método foi utilizado pelo Imperador Júlio César na Roma Antiga para se comunicar com seu exército durante as batalhas de maneira que se as mensagens fossem vistas pelo exército inimigo, ainda assim não descobriam seu segredo de batalha. E dessa forma seu exército vencia e conquistava mais territórios. A cifra de César consiste em mudar uma letra do alfabeto por outra, seguindo o padrão, como no exemplo a seguir:

$$\begin{array}{cccccc} a & b & c & \cdots & y & z \\ D & E & F & \cdots & B & C \end{array}$$

Assim, devemos iniciar a segunda linha com a letra D. Esse método era simples e podia ser quebrado por alguém que tivesse muito conhecimento da língua, observando a frequência

de algumas letras. A utilização desse método custou a vida da rainha da Escócia Maria Stuart ($1542 - 1587$), por tramar o assassinato de sua prima a rainha Elizabeth I da Inglaterra, por meio de mensagens cifradas. A quebra deste segredo trouxe provas contra Maria, que foi condenada à morte por decapitação.

Ter uma mensagem decifrada por um exército inimigo no meio de uma batalha poderia custar o fim da guerra e a derrota seria certa. Da mesma forma, se nossos dados bancários caírem nas mãos de hackers pode nos causar um grande prejuízo. Portanto, muitas mensagens devem ser bem protegidas, mas muitos métodos de criptografias eram simples e fáceis de serem quebrados. Ao longo da história muitos estudiosos criaram métodos de criptografia mais seguros e difíceis de serem quebrados. Um exemplo disso foram os alemães que utilizaram a máquina ENIGMA para criptografar suas mensagens durante a segunda guerra mundial. Essa máquina tinha como função embaralhar as letras seguindo um padrão e para dificultar ainda mais de ser quebrada a criptografia os alemães mudavam todos os dias o padrão. Entretanto, os britânicos conseguiram quebrar esta criptografia graças a uma das mentes brilhantes do século XX, Alan Turing que ficou conhecido como o pai da computação. A quebra dessa criptografia significou a antecipação do final da segunda guerra mundial.

Desde os tempos mais remotos a criptografia foi utilizada em guerras. Pois se um exército inimigo tivesse acesso a uma informação importante, como uma estratégia de ataque ou de defesa, o exército inimigo poderia se preparar melhor para se defender e atacar. Porém, atualmente, com o avanço da tecnologia e da internet, temos muitas informações que devem ser protegidas, tais como: nossas conversas em redes sociais, nossos dados bancários, nossos dados pessoais, segredos de negócios, entre outros. Dessa maneira a criptografia se tornou indispensável em nossa vida.

Diante da importância da criptografia para a nossa vida e, sabendo que o ensino de matemática se torna mais atraente e eficaz quando o aluno percebe uma aplicação, do conteúdo estudado, na vida cotidiana. Então buscamos apresentar a aplicação de funções, de matrizes e de relações de equivalência na criptografia para que o professor de matemática do ensino fundamental e médio faça o uso desses mecanismos para ter uma aula mais proveitosa e um melhor aprendizado por parte dos alunos.

No capítulo 2 apresentamos os conteúdos de funções que serão necessários para a aplicação na criptografia e que são estudados no final do ensino fundamental e no ensino médio. Já no capítulo 3 apresentamos os conteúdos de matrizes que também são utilizados na criptografia e que são estudados no ensino médio. No capítulo 4 apresentamos os conteúdos de relação de equivalência e congruência módulo m que são aplicados na criptografia, pois, como o nosso alfabeto possui 26 letras então devemos trabalhar com o conjunto $\mathbb{Z}_{26}$, esse conteúdo pode ser estudado no ensino fundamental e no ensino médio. No capítulo 5 falamos de criptografia e mostramos como aplicar os conteúdos de funções, de matrizes e de relação de equivalência para criptografar e decifrar textos e

mostramos alguns métodos de criptografia e mostramos como podemos verificar quantas chaves possíveis existem em alguns métodos de criptografia utilizando algumas técnicas de contagens. No capítulo 6 mostramos algumas sugestões para o professor do ensino fundamental e do ensino médio trabalhar com os alunos na sala de aula e fizemos as considerações finais.

Capítulo 2

Funções

Neste capítulo apresentaremos um breve estudo sobre funções, que será importante para a aplicação na criptografia. Podemos encontrar estes conteúdos em [7], [10], [14] e [15].

Definição 2.1. *Dados dois conjuntos X e Y definimos uma função f de X em Y, denotado por $f : X \longrightarrow Y$, uma regra que associa a cada $x \in X$ um único $y \in Y$.*

O $y \in Y$ que é associado ao $x \in X$ é chamado de $f(x)$, assim $f(x) = y$, ou seja, y é o valor que a função f assume em x. Neste caso, dizemos que y é a imagem de x.

Em uma função $f : X \longrightarrow Y$, chamamos o conjunto X de domínio de f e indicamos por Df. O conjunto Y é chamado de contradomínio de f. O conjunto formado por todos os elementos $y \in Y$ tais que $y = f(x)$ para algum $x \in X$, formam o conjunto imagem de f e indicamos por Imf,

$$Imf = \{f(x) \mid x \in X\}.$$

Veja alguns exemplos a seguir:

Exemplo 2.1. *Dados os conjuntos $X = \{2, 4, 7\}$ e $Y = \{5, 7, 10, 12\}$. A regra definida por $f(x) = x + 3$ é uma função $f : X \longrightarrow Y$, pois, temos:*

$$f(2) = 2 + 3 = 5,$$

$$f(4) = 4 + 3 = 7$$

e

$$f(7) = 7 + 3 = 10,$$

ou seja, cada $x \in X$ é associado a um único $y \in Y$.

Exemplo 2.2. *Dados os conjuntos $X = \{1, 3, 4\}$ e $Y = \{2, 4, 6\}$. A regra definida por $f(x) = x + 1$ não é uma função de X em Y, pois,*

$$f(4) = 4 + 1 = 5 \notin Y.$$

Definição 2.2. *Uma função $f : X \longrightarrow Y$ é dita injetora se, para todo $y \in Y$, existir no máximo um $x \in X$ tal que $f(x) = y$. É dita sobrejetora se $Imf = Y$. Isto é, para todo $y \in Y$, existe pelo menos um $x \in X$ tal que $y = f(x)$. E é dita bijetora se for simultaneamente injetora e sobrejetora.*

Para mostrar que uma função $f : X \longrightarrow Y$ é injetora devemos mostrar que

$$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$$

para todos $x_1, x_2 \in X$. Equivalentemente

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2.$$

Exemplo 2.3. *Seja $\mathbb{R}$ o conjunto dos números reais. A função Afim $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = ax + b$ com $a \neq 0$ é injetora. Para provarmos, basta fazer:*

$$f(x_1) = f(x_2) \Rightarrow ax_1 + b = ax_2 + b \Rightarrow a(x_1 - x_2) = 0 \Rightarrow x_1 = x_2$$

.

Exemplo 2.4. *A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$ não é injetora. Note que,*

$$-1 \neq 1$$

mas

$$f(-1) = f(1) = 1.$$

Exemplo 2.5. *A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = ax + b$ com $a \neq 0$ é sobrejetora, pois, para cada $y \in \mathbb{R}$,*

$$y = f(\frac{y-b}{a}).$$

De fato,

$$f(\frac{y-b}{a}) = a(\frac{y-b}{a}) + b = y - b + b = y$$

Exemplo 2.6. *A função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = x^2$ não é sobrejetora, pois se tomarmos $y = -a$, com $a > 0$, não existe $x \in \mathbb{R}$ tal que $f(x) = -a$.*

Note que, a função $f : \mathbb{R} \longrightarrow \mathbb{R}$ definida por $f(x) = ax + b$ com $a \neq 0$ é bijetora, pois, de acordo com os exemplos 2.3 e 2.5, ela é injetora e sobrejetora.

Definição 2.3. *Considere as funções $f : X \longrightarrow Y$ e $g : Y \longrightarrow Z$ tais que $Imf \subset Dg$.*

Denominamos função composta de g e f a função $f : X \longrightarrow Z$ definida por:

$$y = g(f(x)),\ x \in Df.$$

Geralmente para indicar a composta de g e f usamos a notação $g \circ f$. Dessa forma, temos:

$$(g \circ f)(x) = g(f(x)),\ x \in Df.$$

A composição de funções é associativa, ou seja, dadas as funções f, g e h, temos:

$$(f \circ g) \circ h = f \circ (g \circ h).$$

Exemplo 2.7. *Considere as funções $f : \mathbb{R} \longrightarrow \mathbb{R}$ e $g : \mathbb{R} \longrightarrow \mathbb{R}$ definidas por $f(x) = 4x + 3$ e $g(x) = x^2 + 2x$, temos:*

$$(g \circ f)(x) = g(f(x)) = [f(x)]^2 + 2[f(x)] = (4x + 3)^2 + 2(4x + 3) = 16x^2 + 32x + 15.$$

Chamamos de **função identidade** a função $f : X \longrightarrow X$ definida por $f(x) = x$ e denotamos por Id_x.

Seja $f : X \longrightarrow Y$. Uma função $g : Y \longrightarrow X$ é dita inversa à esquerda para f se,

$$(g \circ f) = Id_x$$

isto é,

$$g(f(x)) = x \text{ para todo } x \in X.$$

Por exemplo, considere o conjunto $X = \{x \in \mathbb{R};\ x \geq 0\}$. Seja a função $f : X \longrightarrow \mathbb{R}$ definida por $f(x) = 9x^2$. A função $g : \mathbb{R} \longrightarrow X$ definida por

$$g(y) = \begin{cases} 0, & \text{se} \quad y < 0 \\ \frac{\sqrt{y}}{3}, & \text{se} \quad y \geq 0 \end{cases}$$

é uma inversa à esquerda para f, pois,

$$(g \circ f)(x) = g(f(x)) = g(9x^2) = \frac{\sqrt{9x^2}}{3} = \frac{3x}{3} = x.$$

Note que a inversa à esquerda não é única, pois para qualquer $x_0 \in \mathbb{R}$, podemos definir $g(y) = x_0, \text{com } x_0 \in X$ para cada $y < 0$.

Teorema 2.1. *Uma função $f : X \longrightarrow Y$ possui inversa à esquerda se, e somente se, é injetora.*

Demonstração. Primeiro, suponha que f é injetora. Assim, para cada $y \in Imf$, existe

um único $x \in X$ tal que $f(x) = y$. Defina $g(y) = x$, para $y \in Y - Imf$. Teremos

$$(g \circ f)(x) = g(f(x)) = g(y) = x.$$

Reciprocamente, se existe $g : Y \longrightarrow X$ tal que $(g \circ f)(x) = x$ então, sendo $x_1, x_2 \in X,\ f(x_1) = f(x_2) \Rightarrow x_1 = g(f(x_1)) = g(f(x_2)) = x_2$. Portanto f é injetora. □

Seja uma função $f : X \longrightarrow Y$ chamamos a função $g : Y \longrightarrow X$ de inversa à direita de f se,

$$(f \circ g)(y) = Id_y$$

isto é,

$$f(g(y)) = y.$$

Por exemplo, considere o conjunto $Y = \{y \in \mathbb{R};\ y \geq 0\}$, dada a função $f : \mathbb{R} \longrightarrow Y$ definida por

$$f(x) = \begin{cases} 0, & \text{se} \quad x < 0 \\ \sqrt{x}, & \text{se} \quad x \geq 0 \end{cases}$$

A função $g : Y \longrightarrow \mathbb{R}$ definida por $g(y) = y^2$ é inversa à direita de f, pois,

$$(f \circ g)(y) = f(g(y)) = f(y^2) = \sqrt{y^2} = y.$$

Veja que, a inversa à direita também não é única, pois, podemos definir $f(x) = y_0$, com $y_0 \in Y$ para cada $x < 0$, sem tornar $(f \circ g)(y) \neq y$.

Teorema 2.2. *Uma função $f : X \longrightarrow Y$ possui inversa à direita se, e somente se, é sobrejetora.*

Demonstração. Suponha que f é sobrejetora. Escolhendo para cada $y \in Y$, um $x \in X$ tal que $f(x) = y$ e pondo $g(y) = x$. Definimos uma função $g : Y \longrightarrow X$ tal que

$$(f \circ g)(y) = f(g(y)) = y.$$

Logo g é uma inversa à direta de f. Reciprocamente, se existe $g : Y \longrightarrow X$ com $(f \circ g)(y) = y$ então, para cada $y \in Y$, pondo $x = g(y)$, temos

$$f(x) = f(g(y)) = y.$$

Portanto, f é sobrejetora. □

Definição 2.4. *Seja a função $f : X \longrightarrow Y$. Dizemos que $g : Y \longrightarrow X$ é uma inversa de f se,*

$$(g \circ f)(x) = Id_x$$

e

$$(f \circ g)(y) = Id_y$$

Dada uma função $f : X \longrightarrow Y$ denotaremos sua inversa por $f^{-1} : Y \longrightarrow X$.

A inversa da função $f : \mathbb{R} \longrightarrow \mathbb{R}$, definida por $f(x) = ax + b$, com $a,\ b \in \mathbb{R}$ e $a \neq 0$, é a função $g(x) = \dfrac{x-b}{a}$. Veja que,

$$(g \circ f)(x) = \frac{ax+b}{a} - \frac{b}{a} = \frac{ax+b-b}{a} = x.$$

e

$$(f \circ g)(x) = a(\frac{x-b}{a}) + b = (x-b) + b = x$$

Ao contrário da inversa à esquerda ou à direita, se uma função $f : X \longrightarrow Y$ possui inversa, essa inversa é única. De fato, suponha que $g : Y \longrightarrow X$ e $h : Y \longrightarrow X$ são ambas inversas de f. Temos:

$$h \ = \ h \circ Id = h \circ (f \circ g) = (h \circ f) \circ g = Id \circ g = g.$$

Pelos teoremas 2.1 e 2.2 uma função $f : X \longrightarrow Y$ possui uma função inversa se, e somente se, f é bijetora.

Capítulo 3

Matrizes

Neste capítulo apresentaremos os conteúdos de matrizes que serão utilizados na criptografia, tais conteúdos podem ser vistos em [4], [5] e [11].

Definimos matriz, como sendo uma tabela com m linhas e n colunas (indicamos por $m \times n$), com m e n números inteiros positivos . Veja um exemplo de matriz:

Exemplo 3.1.

$$A = \begin{pmatrix} 2 & 4 & 0 \\ 3 & 8 & 100 \\ 0 & 5 & 7 \end{pmatrix}$$

Dizemos que A é uma matriz 3×3, pois, possui 3 linhas e 3 colunas.

Em uma matriz A, indicamos cada elemento por a_{ij}. Onde o índice i indica a linha e o índice j a coluna às quais o elemento pertence. Veja como podemos representar uma matriz com m linhas e n colunas:

$$A = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Chamamos de matriz quadrada de ordem n toda matriz do tipo $n \times n$, isto é, toda matriz que possui n linhas e n colunas e representamos assim:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

Uma matriz A_n é dita nula se $a_{ij} = 0$ para todo i e todo j.

Chamamos de diagonal principal de uma matriz quadrada de ordem n o conjunto formado pelos elementos que possui os dois índices iguais, isto é:

$$\{a_{ij}; i = j\} = \{a_{11}, a_{22}, a_{33}, \cdots, a_{nn}\}$$

Uma matriz quadrada é dita matriz diagonal se os elementos que não pertencem à diagonal principal são iguais a zero. Veja alguns exemplos:

Exemplo 3.2.

$$A = \begin{pmatrix} 0 & 0 \\ 0 & 3 \end{pmatrix}$$

e

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{pmatrix}$$

Matriz identidade de ordem n (indica-se I_n) é toda matriz quadrada tal que

$$I_n = (a_{ij})_n = \begin{cases} 1, & \text{se} \quad i = j \\ 0, & \text{se} \quad i \neq j \end{cases}$$

Veja alguns exemplos:

Exemplo 3.3.

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Dada uma matriz $M = (a_{ij})_{m \times n}$, chamamos de matriz transposta de M a matriz $A = (a_{ji})_{n \times m}$ obtida quando se troca as linhas pelas colunas de M e denotamos por M^T.

Sejam A e B matrizes $m \times n$. Definimos $A + B$ a matriz C também $m \times n$ tal que:

$$A + B = B + A = C$$

onde ,

$$c_{ij} = a_{ij} + b_{ij}$$

A soma de matrizes satisfaz as propriedades a seguir. Dadas as matrizes A, B e C $m \times n$, a soma é associativa, ou seja:

$$A + (B + C) = (A + B) + C.$$

A soma é comutativa, isto é:

$$A + B = B + A$$

Existe o elemento neutro da soma, para qualquer matriz $A_{m\times n}$ existe a matriz nula do tipo $m \times n$, chamaremos de 0, tal que

$$A + 0 = 0 + A = A.$$

Veja como podemos efetuar o produto de um escalar por uma matriz qualquer. Dado um número real k e uma matriz $A_{m\times n}$ qualquer, o produto kA será a matriz $B_{m\times n}$ tal que $b_{ij} = ka_{ij}$. Veja um exemplo a seguir:

$$3 \cdot \begin{pmatrix} 2 & 8 \\ 1 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 24 \\ 3 & 9 \end{pmatrix}$$

O produto de um número por uma matriz apresenta as seguintes propriedades:
i) $x \cdot (y \cdot A) = (xy) \cdot A$
ii) $x \cdot (A + B) = x \cdot A + x \cdot B$
iii) $(x + y) \cdot A = x \cdot A + y \cdot A$
iv) $1 \cdot A = A$
em que A e B são matrizes e x e y são números reais quaisquer.

Veja como efetuamos o produto entre duas matrizes. Considere duas matrizes $A = (a_{ij})_{m\times n}$ e $B = (b_{jk})_{n\times p}$, chamamos de produto AB a matriz $C = (c_{ik})_{m\times p}$ tal que

$$c_{ik} = a_{i1} \cdot b_{1k} + a_{i2} \cdot b_{2k} + a_{i3} \cdot b_{3k} + \cdots + a_{in} \cdot b_{nk} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

para todo $i \in \{1, 2, \cdots, m\}$ e todo $k \in \{1, 2, \cdots, p\}$. Veja a seguir, duas observações importantes:

1^a) Dadas duas matrizes A e B, só podemos efetuar o produto AB se o número de colunas de A for igual ao número de linhas de B.

2^a) Dadas as matrizes $A_{m\times n}$ e $B_{n\times p}$ produto AB será do tipo $m \times p$.

Exemplo 3.4. *Seja as matrizes*

$$A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 1 & 4 \end{pmatrix}$$

e

$$B = \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix},$$

como A é do tipo 2×3 e B é do tipo 3×1, então o produto AB existe, pois o número de colunas de A é igual ao número de linhas de B. E AB é do tipo 2×1, pois o número de linhas de A é igual a 2 e número de colunas de B é igual a 1.

Temos, então,

$$AB = \begin{pmatrix} c_{11} \\ c_{21} \end{pmatrix},$$

calculando c_{11} e c_{21}, temos:

$$c_{11} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31} = 1 \cdot 7 + 2 \cdot 8 + 5 \cdot 9 = 7 + 16 + 45 = 68$$

e

$$c_{21} = a_{21} \cdot b_{11} + a22 \cdot b_{21} + a_{23} \cdot b_{31} = 3 \cdot 7 + 1 \cdot 8 + 4 \cdot 9 = 21 + 8 + 36 = 65$$

logo

$$AB = \begin{pmatrix} 68 \\ 65 \end{pmatrix}.$$

Dadas as matrizes A, B e C, temos as seguintes propriedades:

$$A(BC) = (AB)C$$

(associatividade da multiplicação), e

$$A(B + C) = AB + AC,$$

distributividade. Mas, nem sempre teremos

$$AB = BA,$$

ou seja, o produto não é comutativo. Temos ainda

$$A_n I_n = I_n A_n = A_n.$$

Logo, de acordo com a definição abaixo, o conjunto das matrizes de ordem n é um anel não comutativo com unidade.

Um conjunto W não vazio e um par de operações sobre W, uma soma $(x, y) \longmapsto x + y$ e uma multiplicação $(x, y) \longmapsto xy$ $(ou\ x \cdot y)$, é chamado de anel e indicamos por $(W, +, \cdot)$ se satisfazem as seguintes propriedades:

i) se $a, b, c \in W$, então $a + (b + c) = (a + b) + c$ (associatividade);

ii) se $a, b \in W$, então $a + b = b + a$ (cumutatividade);

iii) existe um elemento $0_W \in W$ tal que, para todo $a \in W$, $a + 0_W = a$ (existência do elemento neutro);

iv) para todo $a \in W$, existe um elemento em W, geralmente indicado por $-a$, tal que $a + (-a) = 0_W$ (existência do oposto);

v) se $a, b, c \in W$, então $a(bc) = (ab)c$, ou seja, a multiplicação goza da propriedade associativa;

vi) se $a, b, c \in W$, então $a(b+c) = ab+ac$ e $(a+b)c = ac+bc$, ou seja, a multiplicação é distributiva em relação à adição

Se o anel $(W, +, \cdot)$ satisfaz a propriedade:

vii) se $a \in W$ então, existe $1_W \in W$ com $1_W \neq 0_W$ tal que $a \cdot 1_W = 1_W \cdot a = a$, (existência do elemento neutro da multiplicação) dizemos que $W, +, \cdot)($ é um anel com unidade.

Se o anel $(W, +, \cdot)$ satisfaz a propriedade:

viii) se $a, b \in W$ então, $ab = ba$ (comutatividade da multiplicação) dizemos que $(W, +, \cdot)$ é um anel comutativo.

Se o anel $(W, +, \cdot)$ satisfaz a propriedade:

ix) se $a, b \in W$ então, $ab = 0 \Rightarrow a = 0_W$ *ou* $b = 0_W$, dizemos que $(W, +, \cdot)$ é um anel sem divisores de zero.

Definição 3.1. *Uma matriz $A_{n\times n}$ é dita invertível, se existe uma matriz $B_{n\times n}$ tal que:*

$$AB = BA = I_n.$$

Neste caso, dizemos que B é a matriz inversa de A e denotamos por A^{-1}.

Exemplo 3.5. *A iversa da matriz* $A = \begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix}$ *é a matriz* $B = \begin{pmatrix} \frac{-1}{10} & \frac{2}{5} \\ \frac{3}{10} & \frac{-1}{5} \end{pmatrix}$ *pois,* $AB = BA = I_2$.

Teorema 3.1. *Dada uma matriz A_n, se existir a inversa de A_n, ela é única.*

Demonstração. Suponha que as matrizes B e C são inversas de A, onde A é de ordem n. Assim,

$$B = BI_n = B(AC) = (BA)C = I_nC = C \Rightarrow B = C.$$

□

Seja uma matriz A_n. Se $n = 1$, então,

$$A_1 = \begin{pmatrix} a_{11} \end{pmatrix},$$

definiremos o determinante de A por a_{11}. Denotaremos o determinante por, $detA$ ou $|a_{11}|$. Se $n = 2$, temos:

$$A_2 = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

e definiremos o determinante de A_2 por $detA =\mid M_2 \mid= a_{11}a_{22} - a_{21}a_{12}$.

Dada uma matriz $A_{m\times n}$, definiremos o cofator do elemento $a_{ij} \in A$ e denotamos por A_{ij}, como sendo o produto $(-1)^{i+j} \cdot D_{ij}$, onde D_{ij} é o determinante da matriz formada pelos elementos de A suprimindo a linha i e a coluna j.

Exemplo 3.6. *Sendo a matriz*

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 3 & 4 & 2 \\ 2 & 1 & 2 \end{pmatrix},$$

o cofator do elemento a_{31} *será* $A_{31} = (-1)^{3+1} \cdot D_{31}$*, onde* D_{31} *é o determinante da matriz*

$$\begin{pmatrix} 3 & 5 \\ 4 & 2 \end{pmatrix},$$

logo,

$$A_{31} = (-1)^{3+1} \cdot (3 \cdot 2 - 4 \cdot 5) = 1 \cdot (6 - 20) = -14.$$

Para $n \geq 2$ definiremos o determinante de A_n, como sendo a soma dos produtos dos elementos de uma linha ou de uma coluna pelos respectivos cofatores, assim, por exemplo, se escolhermos a coluna j da matriz A, teremos:

$$detA =\mid A_n \mid= a_{1j}A_{1j} + a_{2j}A_{2j} + ... + a_{nj}A_{nj} = \sum_{i=1}^{n} a_{ij}A_{ij}$$

Veja algumas propriedades dos determinantes:

i) seja $A = (a_{ij})_n$ e $A^T = (b_{ij})_n$, onde $b_{ij} = a_{ji}$, então $detA^T = detA$

ii) dada uma matriz A_n se para uma linha t, tivermos $a_{tj} = 0$ ou para uma coluna k, tivermos $a_{ik} = 0$, então:

$$detA = 0$$

iii) seja as matrizes A_n e N_n, temos:

$$det(A \cdot N) = det(N \cdot A) = detA \cdot detN$$

iv) dada uma matriz A_n se $a_{ij} = a_{kj}$, com $i \neq k$ ou $a_{it} = a_{iy}$, com $t \neq y$, então $detA = 0$.

v) dada uma matriz A_n, escolhendo as linha i e k com $i \neq k$, temos:

$$\begin{aligned} a_{i1} \cdot A_{k1} + a_{i2} \cdot A_{k2} + \cdots + a_{in} \cdot A_{kn} &= \sum_{j=1}^{n} a_{ij} A_{kj} \\ &= 0. \end{aligned}$$

De maneira análoga, se tomarmos as coluna j e t com $j \neq t$, teremos:

$$\begin{aligned} a_{1j} \cdot A_{1t} + a_{2j} \cdot A_{2t} + \cdots + a_{nj} \cdot A_{nt} &= \sum_{i=1}^{n} a_{ij} A_{it} \\ &= 0. \end{aligned}$$

Dada uma matriz $A = (a_{ij})_n$, chamamos de matriz dos cofatores de A, a matriz $A' = (A_{ij})_n$. Chamaremos de matriz adjunta de A a matriz transposta de A' e denotaremos por $\overline{A}$.

Teorema 3.2. *Dada uma matriz A_n, temos*

$$\begin{aligned} A \cdot \overline{A} &= \overline{A} \cdot A \\ &= detA \cdot I_n. \end{aligned}$$

Demonstração. Temos:

$$A \cdot \overline{A} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1j} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2j} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ii} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \cdots & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} A_{11} & A_{21} & \cdots & A_{j1} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{j2} & \cdots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots & \cdots & \vdots \\ A_{1i} & \cdots & \vdots & A_{ii} & \vdots & A_{ni} \\ \vdots & \vdots & \cdots & \cdots & \ddots & \vdots \\ A_{1n} & \cdots & \cdots & A_{jn} & \cdots & A_{nn} \end{pmatrix}$$

Considere o produto

$$A \cdot \overline{A} = (b_{ij})_{n \times n}.$$

Veja por exemplo, que

$$b_{11} = a_{11} \cdot A_{11} + a_{12} \cdot A_{12} + \cdots + a_{1n} \cdot A_{1n} = detA$$

e

$$b_{12} = a_{11} \cdot A_{21} + a_{12} \cdot A_{22} + \cdots + a_{1n} \cdot A_{2n}$$

então, pela propriedade iv

$$b_{12} = 0.$$

De modo geral, se $i = j$, então

$$b_{ij} = b_{ii} = a_{i1} \cdot A_{i1} + a_{i2} \cdot A_{i2} + a_{in} \cdot A_{in} = detA,$$

e se $i \neq j$, então teremos

$$b_{ij} = a_{i1} \cdot A_{j1} + a_{i2} \cdot A_{j2} + \cdots + a_{in} \cdot A_{jn} = 0.$$

Portanto,

$$A \cdot \overline{A} = \begin{pmatrix} detA & 0 & \cdots & 0 & 0 & 0 \\ 0 & detA & 0 & 0 & \vdots & 0 \\ \vdots & 0 & \ddots & \cdots & 0 & 0 \\ 0 & 0 & \cdots & detA & \cdots & \vdots \\ \vdots & \cdots & \cdots & 0 & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 & detA \end{pmatrix} = detA \cdot I_n.$$

De maneira análoga, $\overline{A} \cdot A = detA \cdot I_n$.

□

Teorema 3.3. *Seja A_n uma matriz com $det(A) \neq 0$. Então,*

$$A^{-1} = \frac{1}{det(A)} \cdot \overline{A}.$$

Demonstração. Pelo teorema 3.2, temos:

$$A \cdot (\frac{1}{det(A)} \cdot \overline{A}) = \frac{1}{det(A)} \cdot (A \cdot \overline{A}) = \frac{det(A)}{det(A)} \cdot I_n = I_n$$

$$(\frac{1}{det(A)} \cdot \overline{A}) \cdot A = \frac{1}{det(A)} \cdot (\overline{A} \cdot A) = \frac{det(A)}{det(A)} \cdot I_n = I_n$$

Portanto,

$$A^{-1} = \frac{1}{det(A)} \cdot \overline{A}.$$

□

Teorema 3.4. *Se uma matriz quadrada A_n possui inversa, então $det(A) \neq 0$.*

Demonstração. Seja A^{-1} a inversa de A, pela propriedade (iii) temos:

$$detA \cdot detA^{-1} = det(A \cdot A^{-1}) = det(I_n) = 1.$$

Logo $det(A) \neq 0$. $\square$

Pelos teoremas anteriores, temos que uma matriz A possui inversa se, e somente se, $det(A) \neq 0$.

Capítulo 4

Relações de Equivalência

Neste capítulo estudaremos as classes de equivalência módulo m no conjunto dos números inteiros. Essas classes são fundamentais para a criptografia, visto que, o nosso alfabeto possui apenas 26 letras. Logo para criptografar textos será necessário efetuarmos cálculos usando um conjunto finito de números. Os conteúdos abordados neste capítulo podem ser vistos em [1], [2], [8] e [13]. Iniciaremos definindo relação de equivalência em um conjunto. Dado um conjunto A e elementos $x, y \in A$, se x se relaciona com y, usaremos a notação $x \sim y$, se x não se relaciona com y usaremos a notação $x \not\sim y$.

Definição 4.1. *Seja um conjunto A e os elementos $x, y, z \in A$. Diremos que a relação $\sim$ é uma relação de equivalência se as 3 propriedades a seguir são satisfeitas:*

i) $x \sim x$ $(reflexiva)$

ii) $Se\ x \sim y,\ então\ y \sim x$ $(simétrica)$

iii) $Se\ x \sim y\ e\ y \sim z,\ então\ x \sim z$ $(transitiva)$

Exemplo 4.1. *Dado um conjunto não vazio A, então a relação de igualdade sobre o conjunto A é uma relação de equivalência, de fato:*

$$\begin{aligned} x \in A &\Rightarrow x = x,\ \textit{para todo } x \\ x = y &\Rightarrow y = x,\ \textit{para todos } x, y \in A \\ x = y \ e\ y = z &\Rightarrow x = z,\ \textit{para todos } x, y, z \in A \end{aligned}$$

A congruência módulo m é outro exemplo de relação de equivalência. Dados $a, b, m \in \mathbb{Z}$ diremos que a é congruente a b módulo m, e denotamos por $a \equiv b \pmod{m}$, se m divide $(a - b)$, notação $m \mid (a - b)$. Veja que:

$$x, m \in \mathbb{Z} \Rightarrow x \equiv x \pmod{m},$$

pois, $x - x = 0$ e $m \mid 0$.

$$x, y, m \in \mathbb{Z}\ se\ x \equiv y \pmod{m} \Rightarrow y \equiv x \pmod{m},$$

observe que, se $m \mid (x-y)$ então $m \mid q(x-y)$, para todo $q \in \mathbb{Z}$. Portanto, $m \mid (-1)(x-y) \Rightarrow m \mid (y-x)$.

$$x, y, z \in \mathbb{Z} \text{ se } x \equiv y \pmod{m} \text{ e } y \equiv z \pmod{m} \;\Rightarrow\; x \equiv z \pmod{m}$$

Se $m \mid (x-y)$ e $m \mid (y-z)$, então $m \mid (x-y)+(y-z)$, logo $m \mid (x-z)$.

Definição 4.2. *Considere um conjunto A com uma relação de equivalência $\sim$. Para cada $a \in A$, chamamos de classe de equivalência de a o conjunto $\overline{a} \subset A$ formado pelos elementos que se relacionam com a. Assim:*

$$\overline{a} = \{x \in A \mid a \sim x\}.$$

Sendo $a, b \in A$, se $a \sim b$ então $\overline{a} = \overline{b}$. De fato, suponha que $s \in \overline{a}$, assim $a \sim s$. Sabemos que $a \sim b$ e que $\sim$ é simétrica então $b \sim a$ e como $\sim$ é transitiva, $b \sim s$. Logo $s \in \overline{b}$, portanto $\overline{a} \subset \overline{b}$. De maneira análoga, $\overline{b} \subset \overline{a}$.

Exemplo 4.2. *Considere o conjunto $\mathbb{Z}$ com a relação de congruência módulo m. Seja $a \in \mathbb{Z}$, pela divisão euclidiana podemos escrever $a = m \cdot q + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < m$, então*

$$a \equiv r \ (mod \ \ m),$$

portanto a e r se relacionam. A classe de equivalência de a será o conjunto formado por todos os elementos $x \in \mathbb{Z}$ tal que

$$a \equiv x \equiv r \ (mod\ m)$$

ou seja,

$$\overline{a} = \{x \in \mathbb{Z} \mid x = mt + r, \ \ com\ t \in \mathbb{Z}\}.$$

Indicaremos o conjunto das classes de equivalência de um conjunto A por $A/\sim$ e chamaremos de conjunto quociente de A por $\sim$.

Já vimos que a relação de congruência módulo m é uma relação de equivalência em $\mathbb{Z}$. Veja como será o conjunto quociente $\mathbb{Z}/\sim$, que é o conjunto $\mathbb{Z}_m$.

Se $a \in \mathbb{Z}$, pela divisão euclidiana de a por m, temos

$$a = mq + r, \text{ com } 0 \leq r < m$$

logo,

$$a \ \equiv \ r \pmod{\ m},$$

então

$$\overline{a} \;=\; \overline{r}$$

Portanto,

$$\overline{a} \in \{\overline{0}, \overline{1}, ..., \overline{m-1}\}.$$

Suponhamos que $\overline{r} = \overline{t}$ em $\mathbb{Z}_m$ com $r < t$. Logo

$$\overline{r} = \overline{t} \text{ e } 0 \leq r < t < m,$$

portanto,

$$r \equiv t \pmod{m},$$

mas isso é absurdo, pois significa dizer que $m \mid t - r$ e sabemos que $0 < t - r < m$. Portanto, o conjunto

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

é formado por m elementos distintos dois a dois.

Definição 4.3. *Dado um conjunto não vazio A. Definiremos partição de A, a classe $\mathcal{P}$ dos subconjuntos não vazios de A que satisfaz as três propriedades abaixo:*

i) $\mathcal{P} \neq \emptyset$.

ii) Se X *e* $Y \in \mathcal{P}$ *e* $X \neq Y$*, então* $X \cap Y = \emptyset$.

iii) a união dos membros de $\mathcal{P}$ *é igual a* A.

Assim, dados os conjuntos $A = \{x \in \mathbb{R} \mid x < 0\}$ e $B = \{x \in \mathbb{R} \mid x > 0\}$ e $C = \{0\}$, então $\mathcal{P} = \{A, B, C\}$ é uma partição de $\mathbb{R}$.

Teorema 4.1. *Dado $\sim$ uma relação de equivalência no conjunto A. O conjunto quociente $A/\sim$ é uma partição de A.*

Demonstração. Devemos mostrar que as 3 propriedades de partição são satisfeitas.

a) Considere $\overline{a} \in A/\sim$ então $a \sim a$, logo $a \in \overline{a}$ e, portanto $\overline{a} \neq \emptyset$ para todo $\overline{a} \in A/\sim$.

b) Considere $\overline{a}$, $\overline{b} \in A/\sim$, tais que $\overline{a} \cap \overline{b} \neq \emptyset$. Então existe $x \in \overline{a} \cap \overline{b}$. Logo $x \in \overline{a}$ e $x \in \overline{b}$ portanto $x \sim \overline{a}$ e $x \sim \overline{b}$, logo $b \sim x$ e $x \sim a$ daí concluimos que $b \sim a \Rightarrow \overline{b} = \overline{a}$

c) Devemos mostrar que, sendo $\overline{a}_1, \overline{a}_2, ..., \overline{a}_n$ todos os elementos de $A/\sim$, então, $\overline{a}_1 \cup \overline{a}_2 \cup ... \cup \overline{a}_n = A$.

i) Para todo $a \in A$, temos $\overline{a} \subset A$, então $\overline{a}_1 \cup \overline{a}_2 \cup ... \cup \overline{a}_n \subset A$.

ii) Considere $y \in A$, então $y \sim y$, logo $y \in \overline{y}$, portanto $y \in \overline{a}_1 \cup \overline{a}_2 \cup ... \cup \overline{a}_n$, logo $A \subset \overline{a}_1 \cup \overline{a}_2 \cup ... \cup \overline{a}_n$. Portanto, de *i)* e *ii)* conclui-se que $A = \overline{a}_1 \cup \overline{a}_2 \cup ... \cup \overline{a}_n$ □

Dados $\overline{a}, \overline{b} \in \mathbb{Z}_m$ definiremos a soma no conjunto $\mathbb{Z}_m$ como sendo:

$$\overline{a} + \overline{b} = \overline{(a+b)}.$$

No conjunto $\mathbb{Z}_m$ a soma admite as seguintes propriedades:

i) Dados $\overline{a},\ \overline{b}\ \in\ \mathbb{Z}_m$, temos:

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

ii) Sejam $\overline{a},\ \overline{b},\ \overline{c}\ \in \mathbb{Z}_m$, temos:

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

iii) Para todo $\overline{a}\ \in\ \mathbb{Z}_m$,

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$$

iv) Para todo $\overline{a}\ \in\ \mathbb{Z}_m$ existe um $\overline{-a}\ \in\ \mathbb{Z}_m$, tal que

$$\overline{a} + \overline{-a} = \overline{-a} + \overline{a} = \overline{0}$$

neste caso

$$\overline{-a} = \overline{m-a}$$

Sendo $\overline{a}, \overline{b} \in \mathbb{Z}_m$ definiremos o produto por:

$$\overline{a} \cdot \overline{b} = \overline{(a \cdot b)}.$$

O produto em $\overline{Z}_m$ admite as propriedades a seguir:

i) Dados $\overline{a},\ \overline{b}\ \in\ \mathbb{Z}_m$, temos:

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

ii) Sejam $\overline{a},\ \overline{b},\ \overline{c}\ \in \mathbb{Z}_m$, temos:

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

iii) Dados $\overline{a},\ \overline{b},\ \overline{c}\ \in \mathbb{Z}_m$, temos:

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

iv) Para todo $\overline{a}\ \in\ \mathbb{Z}_m$, existe $\overline{1}\ \in\ \mathbb{Z}_m$, tal que

$$\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}.$$

Portanto $\mathbb{Z}_m$ é um anel comutativo com unidade.

Dado um $\overline{a} \in \mathbb{Z}_m$, se existir um elemento $\overline{b} \in \mathbb{Z}_m$, tal que

$$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a} = \overline{1},$$

chamaremos $\overline{b}$ de inverso multiplicativo de $\overline{a}$ e denotaremos por $\overline{b} = (\overline{a})^{-1}$.

Dadas as classes $\overline{a},\ \overline{b} \in \mathbb{Z}_m$, para resolvermos a equação

$$\overline{a} \cdot \overline{x} = \overline{b},$$

é importante sabermos se $\overline{a}$ possui um inverso multiplicativo, pois a solução para esta equação seria

$$\begin{aligned} (\overline{a})^{-1} \cdot \overline{a} \cdot \overline{x} &= (\overline{a})^{-1} \cdot \overline{b} \\ (\overline{a})^{-1} \cdot a) \cdot \overline{x} &= (\overline{a})^{-1} \cdot \overline{b} \\ \overline{1} \cdot \overline{x} &= (\overline{a})^{-1} \cdot \overline{b} \\ \overline{x} &= (\overline{a})^{-1} \cdot \overline{b}. \end{aligned}$$

Logo, a equação teria uma única solução e, portanto o inverso multiplicativo, se existir, é único.

Como vimos que é importante sabermos se uma classe $\overline{a} \in \mathbb{Z}_m$ possui ou não um inverso multiplicativo, faremos essa investigação de quando $\overline{a} \in \mathbb{Z}_m$ terá um inverso em $\mathbb{Z}_m$.

Considere $\overline{a} \in \mathbb{Z}_m$, $(\overline{a})^{-1}$ será a solução da equação

$$\overline{a} \cdot \overline{x} = \overline{1},$$

mas essa equação pode ser reescrita como

$$ax \equiv 1 (\text{mod } m) \Rightarrow ax = qm + 1, \text{com } \ q \in \mathbb{Z} \Rightarrow ax - qm = 1$$

fazendo $y = -q$, teremos:

$$ax + my = 1.$$

Dessa maneira $\overline{a} \in \mathbb{Z}_m$ terá um inverso multiplicativo só se existirem $x, y \in \mathbb{Z}$, tais que:

$$ax + my = 1.$$

Agora considere $mdc(a, m) = b$ então, temos:

$$a = tb, \text{para algum } t \in \mathbb{Z}$$

e

$$m = sb, \text{para algum } s \in \mathbb{Z},$$

substituindo, teremos:

$$ax + my = tbx + sby = b(tx + sy) = 1 \Rightarrow b \quad | \quad 1$$

Logo, $b = 1$ ou $b = -1$, portanto $mdc(a, m) = 1$. Então $\overline{a} \in \mathbb{Z}_m$ possui inverso multiplicativo implica que $mdc(a, m) = 1$.

Agora, considere $mdc(a, m) = 1$, pelo algoritmo de Euclides para encontrar o $mdc(a, b)$, com $a, b \in \mathbb{Z}$ podemos escrever

$$mdc(a, b) = ax_0 + by_0$$

logo, se

$$mdc(a, m) = 1,$$

então existem $x_1, y_1 \in \mathbb{Z}$, tais que

$$mdc(a, m) = 1 = ax_1 + my_1.$$

Logo, se $mdc(a, m) = 1$, então existe um inverso multiplicativo para $\overline{a} \in \mathbb{Z}_m$. Agora, note que em $\mathbb{Z}_m$,

$$\overline{m} \cdot \overline{y_1} = \overline{my_1} = \overline{0}$$

daí temos:

$$1 = \overline{ax_1} + \overline{my_1} = \overline{ax_1} + \overline{0} = \overline{ax_1} \Rightarrow \overline{a^{-1}} \quad = \quad \overline{x_1}.$$

Portanto, podemos concluir que $\overline{a} \in \mathbb{Z}_m$ possui inverso multiplicativo se, e somente se, $mdc(a, m) = 1$.

Logo, as classes que possuem inversos multiplicativos em $\mathbb{Z}_{26}$ são:

$$\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{15}, \overline{17}, \overline{19}, \overline{21}, \overline{23}, \overline{25}\}.$$

Capítulo 5

Criptografia

A criptografia atualmente é indispensável na nossa vida, pois, muitas coisas que iremos fazer, desde a troca de uma mensagem nas redes sociais até uma transação bancaria, necessita de sigilo. Teríamos um prejuízo muito grande se nossos dados bancários, assim como muitas outras informações caíssem em mãos de pessoas desconhecidas e mal intencionadas. Com o advento dos computadores e da internet a única maneira de estarmos seguros é protegendo essas informações. Acontece que com o advento dos computadores e da internet fica difícil impedir que alguém tenha acesso aos nossos dados. Então a única saída de manter esse sigilo é usar a criptografia, de maneira que mesmo que nossas conversas ou nossos dados importantes caiam nas mãos de outras pessoas não sejam entendidos por estas pessoas. O papel da criptografia é, por exemplo, fazer com que duas pessoas possam trocar mensagens sem a preocupação de terem suas mensagens lidas por outras pessoas, como, por exemplo, Pedro e Ana podem trocar mensagens, através de cartas, de celular ou de qualquer outra maneira, sem a preocupação de suas mensagens serem lidas por Raimundo. Para isso, eles devem criptografar suas mensagens de forma que apenas eles mesmos possam ler, decifrando-as.

Diante disso, veremos a seguir algumas operações matemáticas que são aplicadas na criptografia. Estes resultados podem serem vistos em [12] e [16].

Definição 5.1. *Definiremos um criptosistema, como sendo uma* 5*-tupla*

$$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$$

onde $\mathcal{P}$ *é um conjunto finito de palavras não cifradas,* $\mathcal{C}$ *é um conjunto finito de palavras cifradas,* $\mathcal{K}$ *é um conjunto de chaves. Para cada* $k \in \mathcal{K}$*, existe uma regra de criptografia* $e_k \in \mathcal{E}$ *e uma regra para decifrar correspondente* $d_k \in \mathcal{D}$*. Onde*

$$e_k : \mathcal{P} \longrightarrow \mathcal{C}$$

e

$$d_k : \mathcal{C} \longrightarrow \mathcal{P},$$

são funções tais que,

$$d_k(e_k(x)) = x, \textit{para } x \in \mathcal{P}$$

ou seja, d_k é uma inversa à esquerda de e_k, portanto e_k deve ser injetora.

Assim, duas pessoas podem se comunicar sem correr o risco de alguém ficar sabendo o conteúdo da conversa, basta usar um criptosistema onde o texto do emissor é cifrado, para se cair nas mãos de terceiros não ser entendido por eles e o receptor possui a chave para decifrar o texto.

Veja a seguir alguns criptosistemas nos quais serão usados as operações soma e produto em $\mathbb{Z}_m$, funções e matrizes.

5.1 Cifra de mudança

A cifra de mudança é uma cifra fácil de ser quebrada por alguém que tenha um bom conhecimento da lingua, basta verificar quais são as letras que aparecem com mais frequência. Como podemos observar na defição a seguir, quando tivermos chave $\overline{k} = \overline{3}$ teremos exatamente a cifra de Cesar. Por isso, esse método não é recomendado para criptografar uma mensagem importante atualmente.

Definição 5.2. *Seja $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. Para $\overline{k} \in \mathbb{Z}_{26}$, define*

$$e_k(\overline{x}) = (\overline{x} + \overline{k})$$

e

$$d_k(\overline{y}) = (\overline{y} - \overline{k}) \textit{ para } \overline{x}, \overline{y} \in \mathbb{Z}_{26}$$

Usaremos a correspondência entre o alfabeto e o conjunto $\mathbb{Z}_{26}$:

A	B	C	D	$\cdots$	Z
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\cdots$	$\overline{25}$

Exemplo 5.1. *Suponha que a chave é $\overline{k} = \overline{20}$, temos:*

$$e_k(x) = (\overline{x} + \overline{20})$$

para criptografar nosso texto. Se quisermos criptografar a palavra "CIFRA"basta fazermos assim:

$$C = \overline{2} \Rightarrow e_k(\overline{2}) = (\overline{2} + \overline{20}) = \overline{22} = X$$

$$I = \overline{8} \Rightarrow e_k(\overline{8}) = (\overline{8} + \overline{20}) = \overline{28} = \overline{2} = C$$

$$F = \overline{5} \Rightarrow e_k(\overline{5}) = (\overline{5} + \overline{20}) = \overline{25} = Z$$

$$R = \overline{17} \Rightarrow e_k(\overline{17}) = (\overline{17} + \overline{20}) = \overline{37} = \overline{11} = L$$

$$A = \overline{0} \Rightarrow e_k(\overline{0}) = (\overline{0} + \overline{20}) = \overline{20} = U$$

Assim, a palavra "CIFRA"fica "XCZLU".
Para decifrar a palavra "XCZLU"usaremos a chave

$$d_k(\overline{y}) = (\overline{y} - \overline{20})$$

e faremos assim:

$$d_k(\overline{22}) = \overline{22} - \overline{20} = \overline{2} = C$$

$$d_k(\overline{2}) = \overline{2} - \overline{20} = \overline{-18} = \overline{8} = I$$

$$d_k(\overline{25}) = \overline{25} - \overline{20} = \overline{5} = F$$

$$d_k(\overline{11}) = \overline{11} - \overline{20} = \overline{-9} = \overline{17} = R$$

$$d_k(\overline{20}) = \overline{20} - \overline{20} = \overline{0} = A$$

A palavra "XCZLU"foi decifrada de maneira correta e encontamos novamente a palavra "CIFRA".

É fácil verificar que temos exatamente 26 chaves possíveis na cifra de mudança, pois $\overline{k}$ varia entre 0 e 25.

5.2 Cifra de Substituição

Outro criptossistema muito conhecido e utilizado por muitos anos é a cifra de substituição. Diferente da cifra de mudança que eram feitas operações algébricas em $\mathbb{Z}_{26}$ para cifrar e decifrar textos, na cifra de substituição nós ciframos e deciframos textos utili-

zando a permutação das letras do nosso alfabeto. Veja como definiremos a seguir esse criptossistema.

Definição 5.3. *Seja $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$. $\mathcal{K}$ consiste em todas as permutações possíveis dos símbolos $\overline{0}, \overline{1}, \overline{2}, ..., \overline{25}$. Para cada permutação $\pi \in \mathcal{K}$, definimos*

$$e_\pi(x) = \pi(x),$$

e

$$d_\pi(y) = \pi^{-1}(y)$$

onde π^{-1} é a permutação inversa de π.

Veja um exemplo a seguir de uma permutação aleatória π, que será a nossa função de criptografia. Vamos escrever as letras do texto simples minúsculas e as letras do texto cifrado maiúsculas:

a	b	c	d	e	f	g	h	i	j	k	l	m
X	N	Y	A	H	P	O	G	Z	Q	W	B	T

n	o	p	q	r	s	t	u	v	w	x	y	z
S	F	L	R	C	V	M	U	E	K	J	D	I

E para decifrar o texto, o receptor ficará com o alfabeto do texto cifrado em ordem alfabética, como veremos a seguir:

A	B	C	D	E	F	G	H	I	J	K	L	M
d	l	r	y	v	o	h	e	z	x	w	p	t

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
b	g	f	j	q	n	m	u	s	k	a	c	i

Exemplo 5.2. *Usando o exemplo acima para criptografar a frase "CIFRA DE SUBSTITUICAO", teremos a frase "YZPCX AH VUNVMZMUZYXF". Para decifrar esta mensagem basta o destinatário usar corretamente o alfabeto com a permutação aleatória verificando cada letra.*

Para cifrar os textos devemos ter uma bijeção do alfabeto nele mesmo, ou seja, para cada letra do alfabeto usado para o texto simples teremos somente uma letra do alfabeto usado para criptografar. Caso contrário teríamos confusão para decifrar o texto. Dessa maneira temos 26 opções para a letra "a", 25 opções para a letra "b", 24 opções para a letra "c"e assim, sucessivamente, até termos 1 opção para a letra "z", logo, pelo princípio multiplicativo o número de permutações aleatórias possíveis são 26!. Portanto, para ficar mais difícil de se quebrar esse sistema de criptografia pode se usar uma chave diferente a dia.

5.3 Cifra Afim

Vejamos a seguir a aplicação de função afim para criptografar mensagens, como podemos observar a seguir, este método é mais sofisticado do que o método de mudança e mais difífil de ser quebrado.

Definição 5.4. *Seja* $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$ *e* $\mathcal{K} = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26},\ mdc(a,26) = 1\}$. *Para* $k = (a,b) \in \mathcal{K}$, *definiremos*

$$e_k(\overline{x}) = \overline{a} \cdot \overline{x} + \overline{b},$$

e

$$d_k(y) = (\overline{a})^{-1}(\overline{y} - \overline{b})$$

com $\overline{x}, \overline{y} \in \mathbb{Z}_{26}$.

Note que se $mdc(\overline{a}, 26) = 1$ então

$$e_k(\overline{x}) = (\overline{a} \cdot \overline{x} + \overline{b})$$

é injetora. De fato, tomando $e_k(\overline{x_1}) = e_k(\overline{x_2})$ temos:

$$\overline{a} \cdot \overline{x_1} + \overline{b} = \overline{a} \cdot \overline{x_2} + \overline{b} \Rightarrow \overline{a} \cdot (\overline{x_1} - \overline{x_2}) = \overline{0} \Rightarrow x_1 = x_2.$$

A condição $mdc(\overline{a}, 26) = 1$ é importante. Considere $K = (\overline{12}, \overline{13})$, isto é

$$e_k(\overline{x}) = \overline{12} \cdot \overline{x} + \overline{13},$$

Então

$$M = \overline{13} \Rightarrow e_k(\overline{13}) = \overline{12} \cdot \overline{13} + \overline{13} = \overline{156} + \overline{13} = \overline{0} + \overline{13} = \overline{13} = M$$

e

$$A = (\overline{0}) \Rightarrow e_k(\overline{0}) = \overline{12} \cdot \overline{0} + \overline{13} = \overline{0} + \overline{13} = \overline{13} = M.$$

Logo e_k não é injetora. Portanto, é necessário que a equação

$$\overline{a} \cdot \overline{x} + \overline{b} = \overline{y}$$

possua uma única solução para $\overline{x} \in \mathbb{Z}_{26}$.

Observe que $\overline{0} \leq \overline{y} \leq \overline{25}$, então $\overline{0} \leq \overline{y} - \overline{b} \leq \overline{25}$, fazendo

$$\overline{y} - \overline{b} = \overline{y_0},\ \text{com}\ \ \overline{y_0} \in \mathbb{Z}_{26}$$

teremos a equação

$$\overline{a} \cdot \overline{x} = \overline{y_0}.$$

Para que seja possível cifrar e decifrar um texto usando função afim é necessário que a equação

$$\overline{a} \cdot \overline{x} = \overline{y_0}$$

possua uma única solução para $\overline{x} \in \mathbb{Z}_{26}$ para qualquer valor que $\overline{y_0}$ assumir em $\mathbb{Z}_{26}$. Mas, como vimos no capítulo 4 essa equação possuirá uma única solução se, e somente se, $mdc(\overline{a}, 26) = 1$.

Exemplo 5.3. *Assim, podemos usar a chave* $K = (\overline{3}, \overline{12})$*, isto é*

$$e_k(\overline{x}) = (\overline{3x} + \overline{12})$$

para criptografar, pois, $mdc(3, 26) = 1$*. Dessa maneira, a palavra "HOJE será criptografada assim:*

$$H = \overline{7} \Rightarrow e_k(\overline{7}) = (\overline{3} \cdot \overline{7} + \overline{12}) = \overline{33} = \overline{7} \Rightarrow H = H$$

$$O = \overline{14} \Rightarrow e_k(\overline{14}) = (\overline{3} \cdot \overline{14} + \overline{12}) = \overline{54} = \overline{2} \Rightarrow O = C$$

$$J = \overline{9} \Rightarrow e_k(\overline{9}) = (\overline{3} \cdot \overline{9} + \overline{12}) = \overline{39} = \overline{13} \Rightarrow J = N$$

$$E = \overline{4} \Rightarrow e_k(\overline{4}) = (\overline{3} \cdot \overline{4} + \overline{12}) = \overline{24} \Rightarrow E = Y$$

A palavra "HOJE"fica criptografada dessa forma "HCNY".
Para decifrar a palavra "HCNY"usaremos a chave

$$d_k(\overline{y}) = (\overline{3})^{-1}(\overline{y} - \overline{12}) = \overline{9}(\overline{y} - \overline{12}),$$

pois

$$d_k(e_k(x)) = d_k(\overline{3}x + \overline{12}) = \overline{9}((\overline{3}x + \overline{12}) - 12)) = \overline{9}(\overline{3}x + \overline{0}) = \overline{27}x = \overline{1}x = x$$

e efetuaremos os cálculos a seguir:

$$H = \overline{7} \Rightarrow d_k(\overline{7}) = \overline{9}(\overline{7 - 12}) = \overline{9}(\overline{-5}) = \overline{9} \cdot \overline{21} = 189 = \overline{7} = H$$

$$C = \overline{2} \Rightarrow d_k(\overline{2}) = \overline{9}(\overline{2 - 12}) = \overline{9}(\overline{-10}) = \overline{9} \cdot \overline{16} = 144 = \overline{14} = O$$

$$N = \overline{13} \Rightarrow d_k(\overline{13}) = \overline{9}(\overline{13 - 12}) = \overline{9} \cdot \overline{1} = \overline{9} = J$$

$$Y = \overline{24} \Rightarrow d_k(\overline{24}) = \overline{9}(\overline{24 - 12}) = \overline{9} \cdot \overline{12} = 108 = \overline{4} = E$$

Então a palavra "HCNY"foi decifrada corretamente e, obtivemos novamente a palavra "HOJE".

O número de classes de equivalência em $\mathbb{Z}_m$ que possuem inverso multiplicativo é calculado através de $\phi(m)$, essa função é chamada de função "fi"de Euler. Se m for um número primo, então

$$\phi(m) = m - 1,$$

caso contrário, podemos escrever m como o produto de números primos assim teremos $m = p_1^{r_1} \cdot p_2^{r_2} \cdots p_n^{r_n}$ e faremos

$$\phi(m) = (p_1^{r_1} - p_1^{r_1 - 1}) \cdot (p_2^{r_2} - p_2^{r_2 - 1}) \cdots (p_n^{r_n} - p_n^{r_n - 1}).$$

Exemplo 5.4. *O número de classes de equivalência em $\mathbb{Z}_{26}$ que possui inverso multiplicativo é dado por*

$$\phi(26) = (2^1 - 2^{1-1}) \cdot (13^1 - 13^{1-1}) = 12.$$

Observe que na Cifra Afim as chaves possíveis são $K = (\overline{a}, \overline{b})$, com $\overline{a}$ sendo inversível em $\mathbb{Z}_{26}$ e $\overline{0} \leq \overline{b} \leq \overline{25}$. Assim teremos 12 opções para $\overline{a}$ e para cada uma delas teremos 26 opções para $\overline{b}$. Portanto, o número de chaves possíveis será $12 \cdot 26 = 312$.

5.4 Cifra de Hill

Agora mostraremos alguns conceitos de matrizes em $\mathbb{Z}_{26}$ aplicados na criptografia. No ano de 1929 Lester Hill criou uma maneira de criptografar mensagens utilizando matrizes, esta maneira ficou conhecida como cifra de Hill. Como podemos observar a seguir a cifra Hill é difícil de ser quebrada.

Definição 5.5. *Considere um número natural $n \geq 2$. Seja $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^n$ e seja $\mathcal{K} = \{M_n$ matrizes invertíveis sobre $\mathbb{Z}_{26}\}$. Para criptografar o texto usaremos a chave*

$$e_k(x) = M \cdot x$$

e para decifrar usaremos

$$d_k(y) = M^{-1} \cdot y.$$

Aqui x e y são vistos como vetores colunas. Todas essas operações são realizadas em $\mathbb{Z}_{26}$.

Observe que tudo que foi dito sobre matrizes continua sendo válido para matrizes

sobre $\mathbb{Z}_{26}$, pois $\mathbb{Z}_{26}$ é um anel comutativo com unidade. A única alteração que teremos é o teorema a seguir.

Teorema 5.1. *Seja M_n uma matriz em $\mathbb{Z}_{26}$, M_n possui inversa em $\mathbb{Z}_{26}$ se, e somente se, $det(M)$ é inversível em $\mathbb{Z}_{26}$.*

Demonstração. Considere M^{-1} a matriz inversa de M em $\mathbb{Z}_{26}$, então teremos:

$$1 = det(I_n) = det(M \cdot M^{-1}) = det(M) \cdot det(M^{-1}),$$

mas como vimos no capítulo 4 isso só é possível se $mdc(detM, 26) = 1$.

Suponha que $det(M) = \overline{x}$ possui inverso multiplicativo, pelo teorema 3.2, sendo $\overline{M}$ a matriz adjunta de M, temos:

$$M \cdot \overline{M} = \overline{M} \cdot M = detM \cdot I_n$$

pelas propriedades de produto de matrizes por um escalar e pelas propriedades de produto em $\mathbb{Z}_{26}$ temos:

$$(\overline{x})^{-1} \cdot (M \cdot \overline{M}) = ((\overline{x})^{-1} \cdot M)\overline{M} = ((\overline{x})^{-1} \cdot \overline{M}) \cdot M \quad =$$
$$(\overline{x})^{-1} \cdot (detM \cdot I_n) = ((\overline{x})^{-1} \cdot detM) \cdot I_n = \overline{1} \cdot I_n = I_n$$

logo

$$M^{-1} = (\overline{x})^{-1} \cdot \overline{M}.$$

□

Exemplo 5.5. *Vamos usar a matriz*

$$M_2 = \begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix}$$

para criptografar nosso texto, pois $det(M) = \overline{5}$ é inversível.

Veja como fazemos para criptografar a palavra "CRIPTOGRAFIA", separamos as letras de duas em duas, se precisar acrescente uma letra qualquer no final da palavra sem mudar o significado da palavra, pois estamos trabalhando com matriz quadrada de ordem 2. Assim, começamos com o par "CR", temos a matriz coluna

$$\begin{pmatrix} C \\ R \end{pmatrix} = \begin{pmatrix} \overline{2} \\ \overline{17} \end{pmatrix}$$

agora efetuamos o cálculo,

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{2} \\ \overline{17} \end{pmatrix} = \begin{pmatrix} \overline{89} \\ \overline{87} \end{pmatrix} = \begin{pmatrix} \overline{11} \\ \overline{9} \end{pmatrix} = \begin{pmatrix} L \\ J \end{pmatrix},$$

agora faremos o mesmo com o par "IP"

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{8} \\ \overline{15} \end{pmatrix} = \begin{pmatrix} \overline{91} \\ \overline{83} \end{pmatrix} = \begin{pmatrix} \overline{13} \\ \overline{5} \end{pmatrix} = \begin{pmatrix} N \\ F \end{pmatrix},$$

agora o par "TO"

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{19} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} \overline{108} \\ \overline{89} \end{pmatrix} = \begin{pmatrix} \overline{4} \\ \overline{11} \end{pmatrix} = \begin{pmatrix} E \\ L \end{pmatrix},$$

é a vez de efetuarmos o cálculo com o par "GR"

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{7} \\ \overline{17} \end{pmatrix} = \begin{pmatrix} \overline{99} \\ \overline{92} \end{pmatrix} = \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} V \\ O \end{pmatrix},$$

efetuando os cáculos com "AF", temos

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{0} \\ \overline{5} \end{pmatrix} = \begin{pmatrix} \overline{25} \\ \overline{25} \end{pmatrix} = \begin{pmatrix} Z \\ Z \end{pmatrix},$$

e por último, o par "IA"

$$\begin{pmatrix} \overline{2} & \overline{5} \\ \overline{1} & \overline{5} \end{pmatrix} \cdot \begin{pmatrix} \overline{8} \\ \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{16} \\ \overline{8} \end{pmatrix} = \begin{pmatrix} Q \\ I \end{pmatrix},$$

Assim, a palavra "CRIPTOGRAFIA"ficou "LJNFELVOZZQI". Para decifrar o texto será usada a matriz inversa de M em $\mathbb{Z}_{26}$. Como vimos no capítulo 3*,*

$$\begin{aligned} M^{-1} &= (detM)^{-1} \cdot \overline{M} \\ &= \overline{(5)}^{-1} \cdot \overline{M}, \end{aligned}$$

onde $\overline{M}$ é a matriz adjunta de M, logo,

$$\overline{M} = \begin{pmatrix} \overline{5} & \overline{-5} \\ \overline{-1} & \overline{2} \end{pmatrix}.$$

A classe inversa de $\overline{5} \in \mathbb{Z}_{26}$ *é* $\overline{21}$*, pois,* $\overline{5} \cdot \overline{21} = 105 = \overline{1}$*, então:*

$$M^{-1} = \overline{21} \cdot \begin{pmatrix} \overline{5} & \overline{-5} \\ \overline{-1} & \overline{2} \end{pmatrix} = \begin{pmatrix} \overline{105} & \overline{-105} \\ \overline{-21} & \overline{42} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix}$$

Para decifrar a palavra "LJNFELVOZZQI"basta separar as letras em pares e efetuar os cálculos, observando corretamente a letra e a sua classe de equivalência. Assim teremos:

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{11} \\ \overline{9} \end{pmatrix} = \begin{pmatrix} \overline{2} \\ \overline{17} \end{pmatrix} = \begin{pmatrix} C \\ R \end{pmatrix}$$

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{13} \\ \overline{5} \end{pmatrix} = \begin{pmatrix} \overline{8} \\ \overline{15} \end{pmatrix} = \begin{pmatrix} I \\ P \end{pmatrix}$$

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{4} \\ \overline{11} \end{pmatrix} = \begin{pmatrix} \overline{-7} \\ \overline{196} \end{pmatrix} = \begin{pmatrix} \overline{19} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} T \\ O \end{pmatrix}$$

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{21} \\ \overline{14} \end{pmatrix} = \begin{pmatrix} \overline{7} \\ \overline{329} \end{pmatrix} = \begin{pmatrix} \overline{7} \\ \overline{17} \end{pmatrix} = \begin{pmatrix} G \\ R \end{pmatrix}$$

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{25} \\ \overline{25} \end{pmatrix} = \begin{pmatrix} \overline{0} \\ \overline{525} \end{pmatrix} = \begin{pmatrix} \overline{0} \\ \overline{5} \end{pmatrix} = \begin{pmatrix} A \\ F \end{pmatrix}$$

$$\begin{pmatrix} \overline{1} & \overline{-1} \\ \overline{5} & \overline{16} \end{pmatrix} \cdot \begin{pmatrix} \overline{16} \\ \overline{8} \end{pmatrix} = \begin{pmatrix} \overline{8} \\ \overline{208} \end{pmatrix} = \begin{pmatrix} \overline{8} \\ \overline{0} \end{pmatrix} = \begin{pmatrix} I \\ A \end{pmatrix}.$$

Dessa maneira, basta juntar os pares de letras decifrados e perceber que a palavra "LJNFELVOZZQI"foi decifrada corretamente.

5.5 Cifra de Vigenère

A seguir veremos um método bastante difícil de ser quebrado, a ideia é parecida com a do método de mudança, inclusive, se escolhermos uma palavra-chave de apenas uma letra teremos exatamente a cifra de mudança. Porém podemos utilizar uma palavra-chave com mais de uma letra, como veremos a seguir.

Definição 5.6. *Seja* m *um inteiro positivo. Definimos* $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$*. Por uma chave* $K = (\overline{k_1}, \overline{k_2}, ..., \overline{k_m})$*, definimos*

$$e_k(\overline{x_1}, \overline{x_2}, ..., \overline{x_m}) = (\overline{x_1 + k_1}, \overline{x_2 + k_2}, ..., \overline{x_m + k_m})$$

e

$$d_k(\overline{y_1}, \overline{y_2}, ..., \overline{y_m}) = (\overline{y_1 - k_1}, \overline{y_2 - k_2}, ..., \overline{y_m - k_m}).$$

Assim, para criptografar um texto utilizando a cifra de Vigenère nós usamos uma palavra-chave, se a palavra-chave possuir menos letras que o texto, então repetiremos a palavra-chave seguindo um padrão como no exemplo abaixo.

Exemplo 5.6. *Veja como podemos criptografar a frase 'CIFRA DE VIGENERE' usando como chave a palavra 'FACE'. Associando cada letra à sua classe de equivalência em* $\mathbb{Z}_{26}$*, temos:* $CIFRA\,DE\,VIGENERE = \overline{2}\,\overline{8}\,\overline{5}\,\overline{17}\,\overline{0}\;\;\overline{3}\,\overline{4}\;\;\overline{21}\,\overline{8}\,\overline{6}\,\overline{4}\,\overline{13}\,\overline{4}\,\overline{17}\,\overline{4}$ *e* $FACE = \overline{5}\,\overline{0}\,\overline{2}\,\overline{4}$*. Como a chave usada tem menos caracteres que o texto então vamos repetir os caracteres seguindo o padrão abaixo e efetuar a soma corretamente,*

$$\begin{array}{cccccccccccccc} \overline{2} & \overline{8} & \overline{5} & \overline{17} & \overline{0} & \overline{3} & \overline{4} & \overline{21} & \overline{8} & \overline{6} & \overline{4} & \overline{13} & \overline{4} & \overline{17} & \overline{4} \\ \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} \end{array}$$

assim teremos:

$$\overline{7}\;\;\overline{8}\;\;\overline{7}\;\;\overline{21}\;\;\overline{5}\;\;\overline{3}\;\;\overline{6}\;\;\overline{25}\;\;\overline{13}\;\;\overline{6}\;\;\overline{6}\;\;\overline{17}\;\;\overline{9}\;\;\overline{17}\;\;\overline{6}$$

Dessa maneira, a frase ficou 'HIHVF DG ZNGGRJRC'. Para decifrar a frase basta subtrair corretamente as classes de equivalência abaixo,

$$\begin{array}{cccccccccccccc} \overline{7} & \overline{8} & \overline{7} & \overline{21} & \overline{5} & \overline{3} & \overline{6} & \overline{25} & \overline{13} & \overline{6} & \overline{6} & \overline{17} & \overline{9} & \overline{17} & \overline{6} \\ \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} & \overline{4} & \overline{5} & \overline{0} & \overline{2} \end{array}$$

note que obtemos novamente as classes de equivalência

$$\overline{2}\,\overline{8}\,\overline{5}\,\overline{17}\,\overline{0}\;\;\overline{3}\,\overline{4}\;\;\overline{21}\,\overline{8}\,\overline{6}\,\overline{4}\,\overline{13}\,\overline{4}\,\overline{17}\,\overline{4}$$

Assim, a frase 'HIHVF DG ZNGGRJRC' foi decifrada corretamente e agora temos a frase 'CIFRA DE VIGENERE'.

Sendo $K = (\overline{k_1}, \overline{k_2}, ..., \overline{k_m})$ com $m \geq 1$, uma chave usada para criptografar um texto usando a cifra de Vigenère. Então, para escolhermos uma palavra-chave que possua m letras, nós temos exatamente 26 opções para k_1, 26 opções para k_2, 26 opções para k_3, e assim sucessivamente. Portanto, temos 26^m chaves possíveis.

Capítulo 6

Considerações Finais

A presente dissertação teve como objetivo apresentar a importância que a criptografia sempre teve em nossas vidas, sobretudo na atualidade com o advento da tecnologia. E utilizar deste fato para mostrar a importância de estudar funções, matrizes, relações de equivalência e congruência modular mostrando a aplicabilidade desses conteúdos na criptografia.

No estudo de funções foi apresentado o conteúdo que seria fundamental para o uso na criptografia, definições, exemplos e teoremas com suas demonstrações, para dar fundamentos ao professor para aplicar em suas aulas. O conteúdo de funções é trabalhado no final do ensino fundamental e no ensino médio e, o professor pode ir utilizando a aplicação de funções na criptografia no momento que estiver trabalhado os conceitos fundamentais para a aplicação.

No ensino médio, muitas vezes, é ensinado o conteúdo de matrizes sem que seja mostrado ao aluno alguma aplicação para este conteúdo, tornando-o pouco atrativo ao aluno, muito cansativo e difícil de ser entendido. Por isso, foi mostrado a aplicação de matrizes na criptografia. Assim que o professor trabalhar os conteúdos de matrizes indispensáveis para a aplicação na criptografia, pode mostrar aos alunos esta aplicabilidade. Desta maneira os alunos perceberão a importância do estudo de matrizes e a aula será mais proveitosa.

Apesar da aritmética modular não ser um conteúdo estudado no ensino fundamental e no ensino médio, apresentamos um breve estudo sobre a congruência módulo m e o conjunto $\mathbb{Z}_m$, com alguns exemplos, definições e teoremas demonstrados, para que os professores de matemática dos anos finais do ensino fundamental e do ensino médio pudessem usar em suas aulas aplicando-os na criptografia.

Deixamos como sugestão aos professores de matemática do ensino fundamental e médio mostrar a importância da criptografia em nossas vidas e aplicar esses conteúdos na criptografia, à medida que forem ministrando em suas aulas. Para que se tenha a atenção e participação dos alunos em suas aulas e desta forma sua aula seja mais dinâmica e atraente. Ou seja feito um estudo teórico mostrando aos alunos a aplicabilidade desses

conteúdos na criptografia, para que possa despertar no aluno um iteresse em estudar esses conteúdos. Outra possibilidade para se trabalhar esses conteúdos, é aplicando um minicurso de criptografia na escola se houver tempo suficiente, assim outros alunos que tenham interesse podem participar.

Bibliografia

[1] CALLIOLI, C. A.; DOMINGUES, H. H.; COSTA, R. C. F. **Álgebra Linear e Aplicações**, 6 ed., São Paulo: Atual, 1990.

[2] COUTINHO, S. C. **Criptografia**, Rio de Janeiro: IMPA, 2015.

[3] DELGADO, J.; FRENSEL, K.; CRISSAFF, L. **Geometria Analítica (coleção PROFMAT)**, 2 ed., Rio de Janeiro: SBM, 2017.

[4] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**, 4 ed. São Paulo: Atual, 2003.

[5] GARCIA, A.; LEQUAIN, Y. **Elementos de Álgebra**, 1 ed. Rio de Janeiro: IMPA, 2014.

[6] GONÇALVES, A. **Introdução à Álgebra**, 5 ed. Rio de Janeiro: IMPA, 2008.

[7] GUIDORIZZI, H. L. **Um Curso de Cálculo**, vol. 1, 5 ed. Rio de Janeiro: LTC, 2001.

[8] HEFEZ, A. **Iniciação à Aritmética**, Rio de Janeiro: IMPA, 2015.

[9] HERSTEIN, I. N. **Topics in Algebra**, Blaisdell Publishing Company, 1964.

[10] IEZZI, G. **Fundamentos de matemática elementar 1**, vol. 1, 7 ed. São Paulo: Atual, 1993.

[11] IEZZI, G. **Fundamentos de matemática elementar 4**, vol. 4, 6 ed. São Paulo: Atual, 1993.

[12] JACOBSON, N. **Basic Algebra**, vol. 1, 2 ed. , New York: Dover, 2009.

[13] LEMOS, M. **Criptografia, Números Primos e Algoritmos**, 4 ed. Rio de Janeiro: IMPA, 2010.

[14] LIMA, E. L. **Curso de Análise**, vol. 1, 6 ed. , Rio de Janeiro: IMPA, 1980.

[15] LIMA, E. L. **Números e Funções Reais**, 1 ed., Rio de Janeiro: SBM, 2013.

[16] STINSON, D. R. **CRYPTOGRAPHY Theory and Practice**, Third Edition. Ontario, Canada.