UNIVERSIDADE FEDERAL DE OURO PRETO
DEPARTAMENTO DE MATEMÁTICA

Mariana Martins Durães Brandão

Uma adaptação da Cifra de Hill para estudo de matrizes.

Ouro Preto

2017

MARIANA MARTINS DURÃES BRANDÃO

Uma adaptação da Cifra de Hill para estudo de matrizes.

Dissertação submetida ao Programa de Mestrado Profissional de Matemática em Rede Nacional - PROFMAT do Departamento de Matemática da Universidade Federal de Ouro Preto como requisito parcial para a obtenção do Grau de Mestre em Matemática.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira.

Ouro Preto
2017

B732a Brandão, Mariana Martins Durães.
Uma adaptação da Cifra de Hill para estudo de matrizes [manuscrito] / Mariana Martins Durães Brandão. - 2017.
91f.: il.: color; tabs.

Orientador: Prof. Dr. Edney Augusto Jesus de Oliveira.

Dissertação (Mestrado) - Universidade Federal de Ouro Preto. Instituto de Ciências Exatas e Biológicas. Departamento de Matemática. Programa de Pós-Graduação em Matemática em Rede Nacional.
Área de Concentração: Matemática com oferta nacional.

1. Criptografia. 2. Matrizes (Matemática). 3. Aritmética . I. Oliveira, Edney Augusto Jesus de . II. Universidade Federal de Ouro Preto. III. Titulo.

CDU: 519.142

Catalogação: www.sisbin.ufop.br

"Uma adaptação da Cifra de Hill para estudo de matrizes"

Autora: ***Mariana*** **Martins Durães Brandão**

Dissertação defendida e aprovada, em 15 de setembro de 2017, pela banca examinadora constituída pelos professores:

Edney Augusto Jesus de Oliveira (Orientador)
Universidade Federal de Ouro Preto

Thiago Morais Pinto
Universidade Federal de Ouro Preto

Gheyza Ferreira da Silva
Universidade Federal de São João Del-Rei

"Uma adaptação da Cifra de Hill para estudo de matrizes"

Autora: ***Mariana*** **Martins Durães Brandão**

Dissertação defendida e aprovada, em 15 de setembro de 2017, pela banca examinadora constituída pelos professores:

Edney Augusto Jesus de Oliveira (Orientador)
Universidade Federal de Ouro Preto

Thiago Morais Pinto
Universidade Federal de Ouro Preto

Gheyza Ferreira da Silva
Universidade Federal de São João Del-Rei

À minha família, por sempre acreditar em mim.
Em especial aos meus avós, Ediraldo e Marilena, aos meus pais, Guilherme e Andréa, e ao meu tio Leonardo.

Agradecimentos

> "Quem caminha sozinho pode até chegar mais rápido, mas aquele que vai acompanhado, com certeza vai mais longe." - Clarice Lispector.

Quero agradecer a todos que sempre confiaram em mim, me dando o necessário suporte para chegar até aqui.

À minha família, agradeço por serem tudo que eu preciso. Ao meu avô Ediraldo e minha avó Marilena, por serem as minhas maiores referências na vida. Ao meu pai Guilherme e a Ba, pela paciência e boa companhia. À minha mãe Andréa e ao Sérgio pela disposição em sempre me ajudar. Aos meus irmãos, Gabri, Duda, Branca, Cae e Dante, por a seu modo me completarem e sempre se orgulharem de mim. À minha irmã da vida, Ana, pela preocupação e lealdade. Aos meus tios pelo apoio, em especial ao Tio Leo, que não titubeou em me ajudar quando precisei. Às primas, Erika e Neca, pelas longas conversas e diversão. À Bete e a Má, por cuidarem de mim até quando não mereço.

Dos amigos que ganhei ao longo da vida, agradeço especialmente àqueles que compreenderam tantas vezes minha ausência e mesmo assim estiveram disponíveis quando necessário. Soraia, Iara, Fefe, Brei, Nádia, Aninha, Raquel, Arthur e Vini, obrigada por tudo! Das amizades inesperadas, agradeço à Maisa, pelo suporte e auxílio. Aos colegas do PROFMAT, muito obrigada pela ajuda em tantos momentos de desespero. Agradeço principalmente aos lindinhos, Dani, Dane, Livinha e Fabian, sem vocês a caminhada teria sido muito mais difícil. Às meninas da República Sonhos, agradeço pelo acolhimento, em especial à Afônica, por ter acompanhado de perto algumas das minhas dificuldades.

Aos meus alunos, agradeço por me motivarem a tentar ser melhor a cada dia. E por fim, não posso deixar de agradecer ao meu orientador, Professor Doutor Edney Augusto Jesus de Oliveira, por toda a paciência, empenho e sentido prático com que sempre me orientou neste trabalho. Muito obrigada por ter me corrigido quando necessário sem nunca me desmotivar.

A todos que torceram por mim, obrigada!

Resumo

Neste trabalho serão apresentados alguns dos principais resultados matemáticos a respeito de Aritmética Modular, dando ênfase às relações de equivalência e classes residuais. É feito também um estudo sobre matrizes e suas propriedades operacionais; a função determinante é construída e apresentada como instrumento para o cálculo de matrizes inversas. Tais temas são abordados com o intuito de fundamentar os processos matemáticos aplicados para funcionamento da Cifra de Hill. Essa cifra é um dos métodos de criptografia apresentados neste texto e ao qual daremos destaque. Para finalizar, foi desenvolvida uma atividade voltada para turmas do Ensino Médio e baseada na Cifra de Hill, cujo principal objetivo é despertar o interesse dos alunos para o estudo de matrizes.

Palavras-chave: Criptografia, Matrizes, Aritmética Modular.

Abstract

In this paper, some of the main mathematical results will be presented about Modular Arithmetic, emphasizing the relations of equivalence and residue classes. Besides, a study on matrices and their operational properties; the determinant function is constructed and presented as an instrument for the calculation of inverse matrices. These themes are approached in order to base the mathematical processes applied to the operation of the Hill Cipher. This cipher is one of the cryptographic methods presented in this text and we will highlight it. To conclude, an activity was developed, focused on high school classes and based on Hill Cipher, which main objective is to arouse students' interest in studying matrices.

Key words: Cryptography, Matrices, Modular Arithmetic.

Conteúdo

1 Introdução

Durante séculos, reis e rainhas buscaram maneiras seguras para se comunicarem com seus exércitos e transmitirem suas ordens aos seus subordinados. Acredita-se que a necessidade de não permitir que forças inimigas tivessem acesso a tais mensagens, tenha motivado a criação de códigos e cifras com o objetivo de alterar uma mensagem de forma que apenas o destinatário tivesse acesso ao conteúdo.

De acordo com [11], um dos primeiros registros de escrita oculta narra a utilização de um método para ocultar a mensagem em questão, que passou a ser chamado de *esteganografia*, do grego, *steganos*, que significa coberto, e *graphein*, que significa escrever. Para mais detalhes, recomendamos ao leitor que consulte [13]. Durante muito tempo a esteganografia foi utilizada, porém a interceptação da mensagem compromete toda sua segurança, uma vez que se a mesma for descoberta, seu conteúdo é imediatamente revelado.

Em paralelo ao desenvolvimento da esteganografia, houve o surgimento e evolução da *criptografia*, do grego, *kriptos* significa oculto. A criptografia tem como principal objeto ocultar o significado da mensagem, e não literalmente ocultar a mensagem em questão. Uma vantagem da criptografia em relação à esteganografia é que, se a mensagem for interceptada por um inimigo, ela estará, à princípio ilegível. O processo de criptografar uma mensagem, constitui-se em dois passos: codificá-la e decodificá-la. O responsável pelo primeiro passo é chamado de remetente, já o responsável pela decodificação pode ser chamado de receptor ou destinatário. Vale ressaltar aqui que, segundo Coutinho (2014), descriptografar uma mensagem é diferente de decifrá-la, uma vez que para o último não é necessário conhecer a chave de codificação. Isto impulsionou a criação de outro campo da *criptologia*[1], chamado *criptoanálise*, cujo principal objetivo é decifrar uma mensagem.

Apesar de a criptografia existir há anos, é ainda um assunto muito atual, já que está sempre em evolução. Isso acontece pois um código está, em boa parte do tempo, sofrendo ataques de *codebreakers* [2], e quando os *codebreakers* decifram tal código, ele se torna inútil. Então o código se extingue ou é aprimorado a outro mais forte. Novamente o código é utilizado

[1] Disciplina que estuda a escrita cifrada, reunindo técnicas da criptografia e da criptoanálise. (Fonte: Dicionário Aurélio)

[2] Termo utilizado por Singh (2002) para se referir àqueles que decifram uma mensagem.

até sofrer novo ataque de codebrakers, e o processo se repete. De acordo com Singh (2002), tal situação pode ser comparada à uma bactéria infecciosa. As bactérias prosperam e sobrevivem até que seja descoberto um antibiótico que expõe uma fraqueza da bactéria e a mata. Com isso, as bactérias são forçadas a evoluir, superando o antibiótico e, se houver sucesso, elas irão prosperar e se restabelecer.

Uma vez que o assunto é interessante e atual, existem várias dissertações do programa PROFMAT cujo tema central é criptografia, com desenvolvimento, em geral, voltado para números primos. Como exemplo, podemos citar [17], na qual é apresentado o histórico dos números primos e alguns conceitos sobre Teoria dos Números, com o objetivo de fundamentar e justificar a segurança do método RSA. Por outro lado, em [16] é apresentado um panorama sobre conjuntos, suas relações e operações, inclusive no que se trata de conjuntos numéricos. Também são apresentadas definições e conceitos sobre funções, os conceitos de divisibilidade, com o objetivo de introduzir o método RSA e a codificação por trinca americana. Já [13] apresenta uma linha entre a evolução da criptografia e o surgimento do código RSA, construindo uma proposta de aplicação dos fundamentos e funcionamentos deste código, de forma simplificada, para alunos da educação básica.

Nesta dissertação, optamos por uma vertente distinta das citadas anteriormente, dando ênfase a um outro modelo de criptografia: a Cifra de Hill. Para fundamentação matemática de tal Cifra, é realizada a apresentação e algumas demonstrações a respeito de Aritmética Modular e Matrizes. Por fim, é proposta uma atividade, envolvendo uma adaptação da Cifra de Hill, cujo público alvo são alunos do Ensino Médio.

No primeiro capítulo desse trabalho, apresentamos um estudo a respeito de Aritmética Modular, enfatizando a relação de congruência que pode ser estabelecida entre dois números inteiros. Além disso, apresentamos a caracterização de algumas estruturas algébricas e suas propriedades. No segundo capítulo, estudamos matrizes sobre corpos, apresentando de maneira formal algumas definições e demonstrações. Realizamos, também a construção da função determinante e apresentamos algumas de suas propriedades que serão úteis ao longo do texto. E, finalizamos este capítulo, apresentando a teoria de matrizes sobre corpos finitos. No quarto capítulo, faremos uma breve introdução à criptografia, suas vertentes e alguns dos tipos de criptografia mais conhecidos. Por exemplo, a cifra de César, Cifra de Vigenère (para mais informações sobre tais métodos consultar [13]). Também falaremos sobre o método RSA (como leitura complementar recomendamos a leitura de [15], [17], [16]). E por fim, apresentaremos a Cifra de Hill[3], que nos serviu de inspiração para a atividade proposta a ser realizada com alunos do Ensino Médio, apresentada no capítulo 5.

[3] Informações adicionais são encontradas em [14]

2 Aritmética Modular

De acordo com Hefez [7, pág. 192], o estudo sobre Aritmética Modular, ou simplesmente, Aritmética dos Restos, foi introduzido por Gauss em seu livro *Disquisitiones Arithmeticae*, de 1801. Tal ramo da matemática trata de realizar operações e obter resultados com os restos da divisão entre dois números inteiros.

Dados $a, m \in \mathbb{Z}$ é sempre possível efetuar a divisão de a por m e obter um resto r. Tal resultado é apresentado a seguir e a sua compreensão é fundamental para o desenvolvimento da aritmética modular. Para uma demonstração deste resultado, veja [4, Cap. 2].

Teorema 2.0.1 (Algoritmo de Euclides)**.** *Sejam a e m números inteiros, com $m \neq 0$. Então existem dois únicos números, q e r, tais que*

$$a = mq + r, \quad \textit{com } 0 \leq r < |m|.$$

Por serem únicos, chamaremos q de *quociente* e r de *resto* da divisão de a por m. Temos que o resto da divisão de a por m será igual a zero se, e somente se, m divide a, isto é, m é um divisor de a. Denotaremos essa relação por $m \mid a$. Caso contrário, escrevemos $m \nmid a$.

2.1. Congruências

Definição 2.1.1. *Dados $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}$, dizemos que a e b são congruentes módulo m se obtivermos o mesmo resto ao dividirmos a e b por m. Denotaremos tal relação da seguinte forma:*

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

Exemplo 2.1.1. *Tome os números 11 e 13. Ao dividirmos por 2, obtemos resto 1 em ambos os casos. Porém ao dividirmos por 3, encontramos como resto os números 2 e 1, respectivamente. Dessa forma, podemos escrever:*

$$11 \equiv 13 \ mod \ 2, \ \ 11 \not\equiv 13 \ mod \ 3.$$

Proposição 2.1.1. *Tomando $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, temos $a \equiv b \, mod \, m$ se, e somente se, $m \mid (b-a)$.*

Demonstração. Pelo Algoritmo de divisão de Euclides, existem quocientes $q_1, q_2 \in \mathbb{Z}$ e restos $r_1, r_2 \in \mathbb{Z}$ tais que $0 \leqslant r_1, r_2 < m$, $a = mq_1 + r_1$ e $b = mq_2 + r_2$. Assim,

$$b - a = m(q_2 - q_1) + (r_2 - r_1).$$

Uma vez que $a \equiv b \ mod \ m$, temos que o resto da divisão de a e b por m é o mesmo, isto é,

$$r_2 = r_1.$$

Daí,

$$r_2 - r_1 = 0,$$

o que significa que $b - a = m(q_2 - q_1)$ e portanto $m \mid (b-a)$.

Reciprocamente, suponha que $m \mid (b-a)$. Como $m \mid m$, segue que

$$m \mid m(q_2 - q_1),$$

e consequentemente

$$m \mid (b-a) - m(q_2 - q_1) \Rightarrow m \mid (r_2 - r_1).$$

Agora, como $0 \leqslant r_1, r_2 < m$, temos:

$$-(m-1) \leqslant r_2 - r_1 \leqslant (m-1).$$

No intervalo acima, somente 0 é divisível por m, e portanto, $r_2 = r_1$, logo:

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

□

Proposição 2.1.2. *Dados $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$ temos:*

1. $a \equiv a \, mod \, m$. *(Reflexividade)*
2. *Se* $a \equiv b \, mod \, m$, *então* $b \equiv a \, mod \, m$. *(Simetria)*
3. *Se* $a \equiv b \, mod \, m$ *e* $b \equiv c \, mod \, m$ *então* $a \equiv c \ mod \ m$. *(Transitividade)*

Demonstração.

Pela Proposição 2.1.1, temos que $a \equiv b \, mod \, m \Leftrightarrow m \mid (b-a)$.

1. $m \mid 0 \Rightarrow m \mid (a-a) \Rightarrow a \equiv a \, mod \, m$.
2. Se $a \equiv b \, mod \, m$, temos que $m \mid (b-a)$ e $m \mid -(b-a)$. Isto é,

$$m \mid (-b+a) \Rightarrow m \mid (a-b) \Rightarrow b \equiv a \, mod \, m.$$

3. Se $a \equiv b \ mod \ m$ e $b \equiv c \ mod \ m$ então $m|(b-a)$ e $m|(c-b)$. Daí, temos:

$$(b-a) = mq. \tag{2.1}$$
$$(c-b) = mq'. \tag{2.2}$$

Da equação (2.1), é possível concluir que $b = a + mq$. Substituindo em (2.2), temos:

$$\begin{aligned} c-(a+mq) = mq' \Rightarrow \quad & c-a = mq' + mq \\ \Rightarrow \quad & c-a = m(q'+q) \\ \Rightarrow \quad & c-a = mq''. \end{aligned}$$

Logo, $m \mid (c-a)$, ou seja, $a \equiv c \, mod \, m$.

□

Definição 2.1.2. *Chamamos de* relação binária *de A em B, qualquer subconjunto do produto cartesiano de A por B.*

Definição 2.1.3. *Chamamos de* relação de equivalência*, toda relação binária entre elementos de um dado conjunto que satisfaz as seguintes propriedades: reflexividade, simetria e transitividade.*

Corolário 2.1.0.1. *Toda congruência módulo m, $m \in \mathbb{N}$ é uma* relação de equivalência.

Proposição 2.1.3. *Dados $a,b,c,d \in \mathbb{Z}$ e $m > 1$, e se $a \equiv b \ mod \ m$ e $c \equiv d \ mod \ m$, então:*

1. $(a+c) \equiv (b+d) \, mod \, m;$ *2.* $ac \equiv bd \, mod \, m.$

Demonstração.

Suponha que $a \equiv b \, mod \, m$ e $c \equiv d \, mod \, m$. Então $m \mid (b-a)$ e $m \mid (d-c)$, isto é,

$$(b-a) = mq \text{ e } (d-c) = mq'.$$

1. Temos que $(b-a)+(d-c) = mq+mq'$, ou seja, $(b+d)-(a+c) = m(q+q') = mq''$. Daí, $m \mid (b+d)-(a+c)$, isto é, $(a+c) \equiv (b+d) \, mod \, m$.
2. Observe que $bd - ac = bd + ad - ad - ac = d(b-a) + a(d-c)$. Por hipótese, $m \mid (b-a)$ e $m \mid (d-c)$, isto é, $m \mid d(b-a) + a(d-c)$, ou seja, $m \mid bd - ac$. Daí, $ac \equiv bd \, mod \, m$.

□

2.2. Classes residuais

Ao dividirmos um número inteiro por $m > 1$, temos que $0 \leqslant r \leqslant m-1$, onde r é o resto de tal divisão. Podemos indexar todos os números inteiros que possuem o mesmo resto na divisão por um divisor fixado m definindo:

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \, mod \, m\}.$$

Dizemos que o conjunto $\overline{a}$ é a *classe residual módulo* m. O número $a \in \overline{a}$ é dito um *representante* da classe residual $\overline{a}$. Qualquer elemento pertencente ao conjunto $\overline{a}$ pode ser tomado como representante da mesma.

Dado $a \in \mathbb{Z}$, segue do Algoritmo de Divisão Euclidiana que existem $q, r \in \mathbb{Z}$ tais que $0 \leqslant r \leqslant m-1$ e $a = qm + r$. Por definição, obtemos que

$$a \equiv r \; mod \; m$$

e daí, conforme a Proposição 2.2.1 a seguir, a e r pertencem a uma mesma classe residual módulo m, e podemos escrever $\overline{a} = \overline{r}$.

É usual escolhermos como representantes principais para as classes residuais módulo m os números $0, 1, \ldots, m-1$, os quais são chamados de representantes principais. Note que

isso nos diz que existem exatamente m classes residuais distintas módulo m, fato que também será provado na Proposição 2.2.1.

Observação 2.2.1. *Para determinarmos qual o representante principal de uma classe residual módulo m de um número negativo, vale destacar que o processo apontado acima utilizando o Algoritmo de Divisão não é tão intuitivo, pois ao dividirmos um número a inteiro negativo por um número natural $b \neq 0$, não temos um procedimento direto como o ensinado para estudante do ensino básico para a divisão de um número inteiro positivo por outro.*

Vamos apresentar um procedimento prático para tal tarefa. Seja $a < 0$ um número inteiro. Então $-a > 0$, e para esse número positivo aplicamos o algoritmo de divisão Euclidiana através, por exemplo, da divisão por chave:

$$\begin{array}{r|l} -a & m \\ \hline \vdots & q \\ \hline r & \end{array} \quad \text{com } 0 \leqslant r < m. \qquad \Leftrightarrow \qquad \begin{array}{l} \text{Dados } -a, m \in \mathbb{Z}, m \neq 0, \text{ existem } q, r \in \mathbb{Z} \\ \text{com } 0 \leqslant r < m \text{ tais que } -a = qm + r. \end{array}$$

Ou seja, temos:

$$-a = qm + r \Rightarrow a = (-q)m + (-r). \tag{2.3}$$

Se $r = 0$, então $-r = 0$ e $\overline{a} = \overline{0}$. O problema é que se $r > 0$ o número $-r$ é menor do que 0, e portanto não serve como resto da divisão Euclidiana. Para contornar esse problema, note inicialmente que:

$$0 < r < m \Rightarrow -m < -r < 0 \Rightarrow -m + m < -r + m < 0 + m \Rightarrow 0 < m - r < m$$

ou seja, $m - r$ é um resto admissível na divisão Euclidiana por m. Assim, podemos reescrever (2.3) do seguinte modo:

$$a = (-q)m + (-r) = (-q)m + (-r) \pm m = (-1 - q)m + (m - r) \tag{2.4}$$

e portanto, na divisão do número inteiro negativo a por m, obtemos como quociente $-1 - q$ e resto $m - r$, onde q e r são os restos obtidos na divisão do número $-a$ por m.

Então, o processo de divisão de um número inteiro negativo a por um número inteiro $m > 0$ pode ser descrito do seguinte modo:

1. *Desconsidere o sinal de negativo de a, e obtenha o quociente q e o resto r.*
2. *Ao reconsiderar o sinal de negativo, o novo quociente será $-1 - q$ e o resto será $m - r$ ou 0.*

Agora, se o objetivo é apenas obter o resto da divisão de $a < 0$ por $m > 0$, e consequentemente o representante principal de $\overline{a}$, basta somarmos, sucessivamente, m a esse número até que o mesmo se torne positivo pela primeira vez, ou se torne zero.

Para ilustrar a observação acima, considere o exemplo:

Exemplo 2.2.1. *Considerando $m = 3$, para determinarmos a classe residual de -7 módulo 3, iremos determinar o resto da divisão de -7 por 3. Para isso, iremos fazer a divisão Euclidiana de $7 = -(-7)$ por 3:*

$$\begin{array}{r|l} 7 & 3 \\ \hline -6 & 2 \\ \hline 1 & \end{array}$$

ou seja,

$$7 = 2 \cdot 3 + 1 \Rightarrow -7 = (-2) \cdot 3 + (-1) \Rightarrow -7 = (-3) \cdot 3 + 2.$$

De outro modo, podemos ir somando a -7 o valor 3 sucessivamente até obter o primeiro valor não-negativo. Assim,

$$\begin{aligned} -7 &+ 3 = -4; \\ -4 &+ 3 = -1; \\ -1 &+ 3 = 2. \end{aligned}$$

Portanto, temos $-7 \in \overline{2}$, módulo 3.

Proposição 2.2.1. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$, então:*

1. *$a \equiv b \ mod \ m$ se, e somente se, $\overline{a} = \overline{b}$;*
2. *Se $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$;*
3. *$\bigcup_{a \in \mathbb{N}} \overline{a} = \mathbb{Z}$.*

Demonstração.

1. Seja $x \in \overline{a}$, temos, por definição de classe de congruência que $x \equiv a \ mod \ m$. Por hipótese, $a \equiv b \ mod \ m$, aplicando a transitividade, teremos $x \equiv b \ mod \ m$, o que implica que $x \in \overline{b}$ e daí podemos concluir que $\overline{a} \subset \overline{b}$. Procedendo de maneira análoga, concluímos que $\overline{b} \subset \overline{a}$. Portanto $\overline{a} = \overline{b}$.
   Por outro lado, se $\overline{a} = \overline{b}$, então, por exemplo $x \in \overline{a} = \overline{b}$, o implica que, $x \equiv a \ mod \ m$ e $x \equiv b \ mod \ m$, daí, por transitividade, $a \equiv b \ mod \ m$.

2. Se $\overline{a} \cap \overline{b} \neq \emptyset$, então existe pelo menos um elemento x tal que $x \equiv a \ mod \ m$ e $x \equiv b \ mod \ m$. Daí, por transitividade, $a \equiv b \ mod \ m$, e pelo item (a), $\overline{a} = \overline{b}$.
3. Por definição, $\overline{a} \subset \mathbb{Z}, \forall a \in \mathbb{N}$. Logo, $\bigcup_{a \in \mathbb{N}} \overline{a} \subset \mathbb{Z}$.

   Por outro lado, dado $x \in \mathbb{Z}$, se $x \geq 0$, então $x \in \mathbb{N}$ e disso temos que $x \in \overline{x} \subset \bigcup_{a \in \mathbb{N}} \overline{a}$.

   Se $x < 0$, então temos que $-x > 0$, e como $m > 0$ pela propriedade Arquimediana do inteiros, existe $k \in \mathbb{N}$ tal que $-x < mk$, ou seja $mk + x > 0$. Note também que $x \equiv (mk + x) \bmod m$, e pelo item 1 desta Proposição, temos que $\overline{x} = \overline{mk + x}$. Como $mk + x \in \mathbb{N}$, segue que $x \in \overline{x} = \overline{mk + x} \subset \bigcup_{a \in \mathbb{N}} \overline{a}$.

   Portanto, $\mathbb{Z} \subset \bigcup_{a \in \mathbb{N}} \overline{a}$.

□

Uma consequência da proposição acima é que existem exatamente m classes residuais módulo m, e portanto, podemos escolher os números $0, 1 \ldots, m-1$ como os representantes principais e se $i, j \in \{0, 1 \ldots, m-1\}$ então $(i \not\equiv j \mod m)$ pois seus restos na divisão por m são distintos e consequentemente $\overline{i} \neq \overline{j}$.

O conjunto de todas as m classes residuais módulo m distintas será denotado $\mathbb{Z}_m$, podendo ser representado por $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$.

Observação 2.2.2. *Não é errado escrever, por exemplo,* $\mathbb{Z}_5 = \{\overline{25}, \overline{51}, \overline{-78}, \overline{128}, \overline{-996}\}$.

2.3. O anel $\mathbb{Z}_m$

Iremos agora "arimetizar" o conjunto $\mathbb{Z}_m$ construído na seção anterior, munindo-o com duas operações cujas propriedades sejam "parecidas" com as operações que utilizamos em $\mathbb{Z}$.

Podemos definir as operações *adição* e *multiplicação* da seguinte forma:

Definição 2.3.1. *Dadas duas classes* $\overline{a}, \overline{b} \in \mathbb{Z}_m$

1. *Chamaremos de soma* $\overline{a} + \overline{b}$*, a classe* $\overline{a + b}$*, ou seja,*

$$\begin{aligned} + := \quad \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (\overline{a}, \overline{b}) &\longmapsto \overline{a} + \overline{b} := \overline{a + b}. \end{aligned}$$

2. *Chamaremos de produto $\overline{a}\cdot\overline{b}$, a classe $\overline{a\cdot b}$, ou seja,*

$$\begin{aligned}\cdot := \quad \mathbb{Z}_m \times \mathbb{Z}_m \quad &\longrightarrow \mathbb{Z}_m \\ (\overline{a},\overline{b}) \quad &\longmapsto \overline{a}\cdot\overline{b} := \overline{a\cdot b}.\end{aligned}$$

Em tais operações, tomamos a como representante da classe $\overline{a}$ e b como representante de $\overline{b}$. Ao mudarmos os representantes das classes, o valor das operações definidas acima serão conservados. Para observamos com mais clareza esse fato, recorremos à Proposição 2.1.3, que nos diz que, se $a \equiv a_1 \ mod \ m$ e $b \equiv b_1 \ mod \ m$, então $(a+b) \equiv (a_1+b_1) \ mod \ m$ e $ab \equiv a_1 b_1 \ mod \ m$, isto é, $\overline{a+b} = \overline{a_1+b_1}$ e $\overline{a\cdot b} = \overline{a_1\cdot b_1}$.

Podemos classificar $\mathbb{Z}_m$ como um *anel*, uma vez que é uma estrutura algébrica constituída de um conjunto não vazio e de duas operações binárias, que usufrui das seguintes propriedades:

- Em relação à adição:
  Sejam $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}_m$, então:
  - $\overline{a}+(\overline{b}+\overline{c}) = (\overline{a}+\overline{b})+\overline{c}$ (Associativa);
  - $\overline{a}+\overline{b} = \overline{b}+\overline{a}$ (Comutativa);
  - Existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}+\overline{b} = \overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$ (Elemento neutro);
  - Existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}+\overline{b} = \overline{0}$, para todo $\overline{a} \in \mathbb{Z}_m$ (Simétrico aditivo).
- Em relação à multiplicação:
  Sejam $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}_m$, então:
  - $\overline{a}\cdot(\overline{b}\cdot\overline{c}) = (\overline{a}\cdot\overline{b})\cdot\overline{c}$ (Associativa);
  - $\overline{a}\cdot\overline{b} = \overline{b}\cdot\overline{a}$ (Comutativa);
  - Existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\cdot\overline{b} = \overline{a}$, para todo $\overline{a} \in \mathbb{Z}_m$ (Identidade).
- Em relação à interação entre multiplicação e adição:
  Sejam $\overline{a},\overline{b},\overline{c} \in \mathbb{Z}_m$, então:
  - $\overline{a}\cdot(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$ (Distributiva)

Observação 2.3.1. *Mostraremos aqui que os elementos classificados como elemento neutro, simétrico aditivo e identidade são únicos e portanto recebem uma notação especial.*

- *Suponhamos que $\overline{b}$ e $\overline{b'}$ sejam elementos neutros. Então*

$$\overline{b} \ \underset{\uparrow}{=} \ \overline{b}+\overline{b'} \ \underset{\downarrow}{=} \ \overline{b'}.$$

($\overline{b}$ é o elemento neutro) — ($\overline{b'}$ é o elemento neutro)

Pela unicidade do elemento neutro, representaremos o mesmo por $\overline{0}$.

- *Suponha que $\overline{b'}$ e $\overline{b''}$ sejam simétricos aditivos de $\overline{a}$. Então, temos:*

$$\overline{b'} = \overline{b'}+\overline{0} \underset{\uparrow}{=} \overline{b'}+\left(\overline{a}+\overline{b''}\right) = \left(\overline{b'}+\overline{a}\right)+\overline{b''} \overset{\downarrow}{=} \overline{0}+\overline{b''} = \overline{b''}.$$

($\overline{b''}$ é o elemento simétrico de $\overline{a}$)

($\overline{b'}$ é o elemento simétrico de $\overline{a}$)

Portanto, o simétrico aditivo será tomado como o simétrico do elemento, $\overline{a}$, isto é, $-\overline{a}$.

- *Suponhamos que $\overline{b}$ e $\overline{b'}$ sejam identidades. Segue que:*

$$\overline{b} \underset{\uparrow}{=} \overline{b}\cdot\overline{b'} \overset{\downarrow}{=} \overline{b'}.$$

($\overline{b'}$ é o elemento identidade)

($\overline{b}$ é elemento identidade)

Desse modo, indicaremos a identidade por $\overline{1}$.

Para efeito de ilustração, tomaremos o caso em que $m = 4$. Portanto trabalhamos com as seguintes classes: $\overline{0}, \overline{1}, \overline{2}$ e $\overline{3}$. Podemos então, construir as seguintes tabelas:

Tabela 2.1.: Adição em $\mathbb{Z}_4$.

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Tabela 2.2.: Multiplicação em $\mathbb{Z}_4$.

·	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observe que, diferente da aritmética entre números inteiros, temos que $\overline{2}\cdot\overline{2} = \overline{0}$, mas $\overline{2} \neq \overline{0}$.

Definição 2.3.2. *Seja K um anel, dado $a \in K, a \neq 0$, dizemos que a é um divisor de zero se existe $b \in K, b \neq 0$ tal que $ab = 0$.*

Exemplo 2.3.1. *Note que $2 \cdot 3 \equiv 0 \bmod 6$. Isto é, em $\mathbb{Z}_6$, 2 e 3 são divisores de zero.*

Definição 2.3.3. *Um elemento $\overline{a}$ em $\mathbb{Z}_m$ é dito invertível se existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a}\cdot\overline{b} = \overline{1}$.*

Exemplo 2.3.2. *Em $\mathbb{Z}_{26}$, temos que $\overline{9}$ é invertível, e seu inverso é $\overline{3}$, uma vez que $\overline{9}\cdot\overline{3} = \overline{1}$.*

Proposição 2.3.1. *Um divisor de zero nunca possui inverso multiplicativo.*

Demonstração. Suponha que a seja um divisor de zero e que possua inverso multiplicativo, isto é, $a \cdot a^{-1} = 1$. Pela Definição 2.3.2, temos que $ab = 0$ tal que $a, b \neq 0$. Daí,

$$0 = 0a^{-1} = (ab)a^{-1} = (ba)a^{-1} = b(aa^{-1}) = b1 = b,$$

o que contradiz a hipótese. Portanto, a não possui inverso multiplicativo. □

Definição 2.3.4. *Um anel comutativo com unidade D em que nenhum divisor de zero é não nulo, é chamado* domínio de integridade.

Proposição 2.3.2. *Se D é domínio de integridade, então a lei do cancelamento na multiplicação é válida. Isto é,*

$$\forall a, b, c \in D, \forall c \neq 0, a = b \Longleftrightarrow ac = bc.$$

Demonstração.

$(\Rightarrow)$ Se $a = b$, podemos concluir imediatamente do fato de, em K, a multiplicação ser bem definida, que $ac = bc$.

$(\Leftarrow)$ $ac = bc \Rightarrow ac - bc = 0 \Rightarrow (a-b)c = 0$. Como D é um domínio de integridade, temos $a - b = 0$ ou $c = 0$. Mas, por hipótese, $c \neq 0$, ou seja, $a - b = 0$, o que implica em $a = b$. □

Teorema 2.3.1. *(Teorema de Bézout) Dados a e b inteiros positivos, existem inteiros x e y tais que:*

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

Demonstração. O Algoritimo de Euclides, apresentado no apêndice, usado de trás pra frente, nos fornece as seguintes igualdades:

$$\begin{aligned}
r_2 &= a - q_1 \cdot b && (2.1)\\
r_3 &= b - q_2 \cdot r_2 && (2.2)\\
&\vdots \quad \vdots &&\\
r_{n-2} &= r_{n-4} - q_{n-3} \cdot r_{n-3} && (2.3)\\
r_{n-1} &= r_{n-3} - q_{n-2} \cdot r_{n-2} && (2.4)\\
r_n &= r_{n-2} - q_{n-1} \cdot r_{n-1} && (2.5)
\end{aligned}$$

Substituindo o valor de r_{n-1} dado na $(n-1)$-ésima equação na (n)-ésima, teremos:

$$r_n = (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-2} - q_{n-1} \cdot r_{n-3} = x_{n-2} \cdot r_{n-2} + y_{n-2} \cdot r_{n-3}.$$

A $(n-2)$-ésima, nos fornece o valor de r_{n-2}, substituindo na igualdade anterior, obtemos:

$$r_n = -(q_{n-3} + q_{n-1} \cdot q_{n-2} \cdot q_{n-3} + q_{n-1}) \cdot r_{n-3} + (1 + q_{n-1} \cdot q_{n-2}) \cdot r_{n-4} = x_{n-3} \cdot r_{n-3} + y_{n-3} \cdot r_{n-4}.$$

Procedemos assim, indutivamente, até encontrarmos x_3 e y_3 tais que:

$$x_3 \cdot r_3 + y_3 \cdot r_2 = r_n.$$

Agora, note que as equações (2.1) e (2.2) nos fornecem os valores de r_3 e r_2. Substituindo na equação encontrada, teremos:

$$\begin{aligned} r_n &= x_3 \cdot r_3 + y_3 \cdot r_2 \\ &= x_3 \cdot (b - q_2 \cdot r_2) + y_3 \cdot (a - q_1 \cdot b) \\ &= a(y_3 - q_2 \cdot x_3) + b(-q_1 \cdot y_3 + q_1 \cdot q_2 \cdot x_3 + x_3) \\ &= ax + by. \end{aligned}$$

Assim, temos $ax + by = r_n$, isto é, $ax + by = mdc(a,b)$, onde x e y são números inteiros. □

Proposição 2.3.3. *Um elemento $\overline{a} \in Z_m$ é invertível se, e somente se, a e m são coprimos.*

Demonstração. Se $\overline{a}$ é invertível, então existe $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{1}$, ou seja, $ab \equiv 1 \ mod \ m$, isto é, $ab - 1 = mq \Rightarrow ab + m(-q) = 1$. Daí, pelo Teorema de Bézout, 1 é o máximo divisor comum entre a e m, o que implica que a e m são primos entre si.

Por outro lado, se a e m são primos entre si, temos $mdc(a,m) = 1$, isto é, existem inteiros b e p tais que $ab + mp = 1$, ou seja, $\overline{1} = \overline{ab} + \overline{mp} \Rightarrow \overline{1} = \overline{ab} = \overline{a}\overline{b}$, ou seja, $\overline{a}$ é invertível. □

Pela proposição acima, podemos concluir que ao trabalharmos com $\mathbb{Z}_p$, p primo, toda classe não nula apresentará inverso multiplicativo. Portanto, podemos classificar $\mathbb{Z}_p$ como um *corpo finito*. Doravante, nosso estudo será voltado para a análise de matrizes sobre $\mathbb{Z}_p$.

3 Matrizes

Dados m e n números naturais, uma matriz de ordem m por n com entradas em um corpo F é uma tabela com m linhas e n colunas onde cada célula desta tabela contém um elemento de F. O conjunto de todas as matrizes $m \times n$ é denotado por:

$$M_{m\times n}(F).$$

Em Álgebra Linear usualmente nos referimos ao corpo F como sendo o *corpo de escalares*, ou simplesmente *conjunto de escalares*. Uma matriz em $M_{m\times n}(F)$ será denotada utilizando letras maiúsculas com o índice $m \times n$, como por exemplo $A_{m\times n}$ ou $B_{m\times n}$ – quando não houver risco de confusão com relação as dimensões da matriz estudada, iremos representá-las apenas por suas letras maiúsculas A ou B.

A fim de facilitar a identificação de cada entrada de uma matriz, as colunas serão enumeradas da esquerda para a direita e as linhas, de cima para baixo. Por exemplo, a matriz

$$A = \begin{bmatrix} 1 & -10 & 49 & 8 \\ 3 & 19 & 13 & -5 \\ 0 & 98 & 9 & -1 \end{bmatrix}$$

é uma matriz 3×4 na qual o valor -10 se encontra na primeira linha, segunda coluna.

Podemos generalizar a escrita dos elementos de uma matriz utilizando a notação a_{ij}, onde i indica a i-ésima linha e j, a j-ésima coluna da matriz A. Dessa forma, uma matriz $A_{m\times n}$ pode ser escrita da seguinte forma:

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn} \end{bmatrix} = \left[a_{ij}\right]_{m\times n}.$$

Toda matriz formada por apenas uma coluna, ou seja, do tipo $M_{m\times 1}(F)$ recebe o nome de *matriz coluna* $m \times 1$ ou simplesmente *vetor* com m coordenadas.

Tabela 3.1.: Vetor com 4 coordenadas.

$$\begin{bmatrix} 7 \\ 5 \\ -8 \\ 19 \end{bmatrix}.$$

Definição 3.0.1. *Dada uma matriz $A_{m\times n} = A$, chamamos de* transposta *de A, e denotamos por A^t, a matriz $B_{n\times m}$, onde $b_{ij} = a_{ji}$, para todo $1 \leqslant i \leqslant m$ e para todo $1 \leqslant j \leqslant n$.*

Exemplo 3.0.1. *Se* $A = \begin{bmatrix} 10 & 1 & 13 \\ 0 & -6 & 5 \end{bmatrix}$, *então* $B = A^t = \begin{bmatrix} 10 & 0 \\ 1 & -6 \\ 13 & 5 \end{bmatrix}$.

Definição 3.0.2. *Dada uma matriz $A_{m\times n}$, chamamos de oposta de A, e denotamos por $-A$, a matriz $B_{m\times n}$, tal que $b_{ij} = -a_{ij}$, para todo $1 \leqslant i \leqslant m$ e para todo $1 \leqslant j \leqslant n$.*

Exemplo 3.0.2. *Se* $A = \begin{bmatrix} 54 & 1 & -13 \\ -7 & 6 & 0 \end{bmatrix}$, *então* $B = -A = \begin{bmatrix} -54 & -1 & 13 \\ 7 & -6 & 0 \end{bmatrix}$.

3.1. Operações entre matrizes

Nesta seção veremos o conjunto das matrizes como uma estrutura algébrica. Para tal, iremos definir operações de soma e produto por escalar sobre esse conjunto.

Definição 3.1.1. *Sejam $A = \left[a_{ij}\right], B = \left[b_{ij}\right] \in M_{m\times n}(F)$. Definimos:*

$$A + B := C$$

onde $C \in M_{m\times n}(F)$ definida por $c_{ij} = a_{ij} + b_{ij}$ para todo $i = 1,\ldots,m$ e $j = 1,\ldots,n$, ou seja:

$$C = \left[a_{ij} + b_{ij}\right].$$

A adição entre matrizes A e B é bem definida quando as matrizes apresentam mesma ordem. Tal operação consiste em somar as entradas correspondentes.

Observação 3.1.1. *A soma das matrizes A e $-B$, na qual $-B$ representa a matriz oposta de B, $A + (-B)$ será denotada, simplesmente, por $A - B$.*

Exemplo 3.1.1.

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \\ -4 & 10 \end{bmatrix} + \begin{bmatrix} 3 & -3 \\ 5 & 1 \\ 0 & 20 \end{bmatrix} = \begin{bmatrix} 1+3 & 0+(-3) \\ 2+5 & 3+1 \\ -4+0 & 10+20 \end{bmatrix} = \begin{bmatrix} 4 & -3 \\ 7 & 4 \\ -4 & 30 \end{bmatrix}.$$

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \\ -4 & 10 \end{bmatrix} - \begin{bmatrix} 3 & -3 \\ 5 & 1 \\ 0 & 20 \end{bmatrix} = \begin{bmatrix} 1-3 & 0-(-3) \\ 2-5 & 3-1 \\ -4-0 & 10-20 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ -3 & 2 \\ -4 & -10 \end{bmatrix}.$$

Proposição 3.1.1. *Sejam $A, B, C \in M_{m\times n}(F)$. Então:*

1. *$A+(B+C) = (A+B)+C$; (Associatividade da soma)*
2. *$A+B = B+A$; (Comutatividade da soma)*
3. *Existe uma matriz $N \in M_{m\times n}(F)$ tal que $A+N = N+A = A$, para toda matriz A; (Existência do Elemento Neutro)*
4. *Existe uma matriz $A' \in M_{m\times n}(F)$ tal que $A+A' = A'+A = N$, para toda matriz A e toda matriz neutra aditiva N – tal matriz A' é dita ser uma matriz simétrica aditiva de A. (Existência do Elemento Simétrico Aditivo)*

Demonstração. Tomaremos $A = \left[a_{ij}\right], B = \left[b_{ij}\right]$ e $C = \left[c_{ij}\right]$, onde a_{ij}, b_{ij} e c_{ij} representam as entradas das matrizes, que são elementos de F, e consequentemente, herdam as propriedades operatórias do corpo F. Assim,

1. $$\begin{aligned} A+(B+C) &= \left[a_{ij}\right] + \left[b_{ij}+c_{ij}\right] = \left[a_{ij}+\left(b_{ij}+c_{ij}\right)\right] = \left[\left(a_{ij}+b_{ij}\right)+c_{ij}\right] \\ &= \left[a_{ij}+b_{ij}\right] + \left[c_{ij}\right] = (A+B)+C. \end{aligned}$$
2. $A+B = [a_{ij}+b_{ij}] = [b_{ij}+a_{ij}] = B+A.$
3. Considere a matriz $N = \left[x_{ij}\right]$ tal que $x_{ij} = 0$ para todo $i, j \in \{1,\ldots,n\}$. Deste modo, $A+N = [a_{ij}+x_{ij}] = [a_{ij}+0] = [a_{ij}] = A.$
4. Considere a matriz $A' = \left[y_{ij}\right]$ tal que $y_{ij} = -a_{ij}$ para todo $i, j \in \{1,\ldots,n\}$. Deste modo, $A+A' = [a_{ij}+(-a_{ij})] = [a_{ij}-a_{ij}] = [0] = N.$

□

Um conjunto X munido de uma operação que satisfaça todas as propriedades apontadas na Proposição 3.1.1 é dito ser um *grupo aditivo abeliano*[1], ou seja, $M_{m\times n}(F)$ munido da operação usual de soma de matrizes é um grupo aditivo abeliano.

[1] Para mais detalhes sobre esta estrutura algébrica, consulte por exemplo [3].

Agora suponha que N e N' sejam duas matrizes nulas, temos:

$$N \underset{\uparrow}{=} N+N' \underset{\downarrow}{=} N'.$$

(N é matriz nula) acima do segundo $=$; (N' é matriz nula) abaixo do primeiro $=$.

Ou seja, quaisquer duas matrizes nulas são iguais, e portanto provamos a unicidade do elemento neutro aditivo de $M_{m\times n}(F)$, o qual, a partir de agora denotaremos por $\overline{0}$ (ou simplesmente 0 quando não houver risco de confusão entre a matriz nula e o número zero.)

Também, suponha que A' e A'' sejam duas matrizes simétricas aditivas de uma dada matriz A, temos:

$$A' = A'+\overline{0} \underset{\uparrow}{=} A'+\big(A+A''\big) = \big(A'+A\big)+A'' \underset{\downarrow}{=} \overline{0}+A'' = A''.$$

(A'' é uma matriz simétrica de A) abaixo do primeiro $=$; (A' é uma matriz simétrica de A) acima do segundo $=$.

Ou seja, quaisquer duas matrizes simétricas aditivas de uma dada matriz A são iguais, e portanto provamos a sua unicidade em $M_{m\times n}(F)$. Note que a matriz oposta de A é tal que

$$A+(-A) = [a_{ij}+(-a_{ij})] = [a_{ij}-a_{ij}] = [0] = \overline{0}.$$

Logo, toda matriz simétrica aditiva de A é igual a matriz oposta de A, ou seja, $-A$.

Também podemos definir a multiplicação de uma matriz por um escalar de F. Isto é, se $A = [a_{ij}]_{m\times n}$ e $\alpha \in F$, então

$$\alpha \cdot A = [\alpha \cdot a_{ij}]_{m\times n}.$$

Por simplicidade usaremos a notação por justa posição omitindo o símbolo de produto "$\cdot$", escrevendo $\alpha A = [\alpha a_{ij}]$ ao invés de $\alpha \cdot A = [\alpha \cdot a_{ij}]$. Por exemplo,

$$5\cdot\begin{bmatrix} -2 & 3 \\ -3 & 2 \\ -4 & -10 \end{bmatrix} = 5\begin{bmatrix} -2 & 3 \\ -3 & 2 \\ -4 & -10 \end{bmatrix} = \begin{bmatrix} 5(-2) & 5(3) \\ 5(-3) & 5(2) \\ 5(-4) & 5(-10) \end{bmatrix} = \begin{bmatrix} -10 & 15 \\ -15 & 10 \\ -20 & -50 \end{bmatrix}$$

Proposição 3.1.2. *Sejam A, B matrizes $m\times n$ e $\alpha, \alpha' \in \mathbb{R}$. Então:*

(i) $\alpha(A+B) = \alpha A + \alpha B$. *(Propriedade distributiva do escalar em relação à adição de matrizes)*

(ii) $(\alpha+\alpha')A = \alpha A + \alpha' A$. *(Propriedade distributiva da matriz em relação à adição de escalares)*

(iii) $\alpha(\alpha' A) = (\alpha\alpha')A$. *(Propriedade da multiplicação por escalar)*

(iv) $1A = A$. *(Propriedade da ação da unidade de F em matrizes)*

Demonstração. Tomamos $A = [a_{ij}]$ e $B = [b_{ij}]$ duas matrizes em $M_{m\times n}(F)$, daí a_{ij}, b_{ij}, α, $\alpha' \in F$. Temos:

(i) $$\begin{aligned}\alpha(A+B) &= \alpha[a_{ij}+b_{ij}] = [\alpha\left(a_{ij}+b_{ij}\right)] = [\alpha a_{ij}+\alpha b_{ij}] = [\alpha a_{ij}] + [\alpha b_{ij}] = \alpha[a_{ij}] + \alpha[b_{ij}] \\ &= \alpha\cdot A + \alpha\cdot B.\end{aligned}$$

(ii) $$\begin{aligned}(\alpha+\alpha')A &= (\alpha+\alpha')[a_{ij}] = [(\alpha+\alpha')a_{ij}] = [\alpha a_{ij}+\alpha' a_{ij}] = [\alpha a_{ij}] + [\alpha' a_{ij}] \\ &= \alpha[a_{ij}] + \alpha'[a_{ij}] = \alpha A + \alpha' A.\end{aligned}$$

(iii) $\alpha(\alpha' A) = \alpha[\alpha' a_{ij}] = [\alpha(\alpha' a_{ij})] = [(\alpha\alpha')a_{ij}] = (\alpha\alpha')[a_{ij}] = (\alpha\alpha')A.$

(iv) $1A = 1[a_{ij}] = [1a_{ij}] = [a_{ij}] = A.$

□

A multiplicação usual entre matrizes não é bem definida em geral, para ser possível determinar o produto AB é necessário que o número de colunas de A coincida com o número de linhas de B. Além disso, tal operação apresenta uma definição formal e pouco intuitiva. De acordo com Hefez e Fernandez (2012, pág. 18), a definição do produto entre matrizes foi apresentada por Arthur Cayley (Inglaterra, 1821-1895) e pode ser descrito da seguinte forma:

Sejam $A = [a_{ij}]_{m\times n}$ e $B = [b_{ij}]_{n\times p}$ duas matrizes. O produto AB de A por B, é definido como a matriz $C = [c_{ij}]_{m\times p}$ tal que:

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + ... + a_{in}b_{nj},$$

para todo $1 \leqslant i \leqslant m$ e para todo $1 \leqslant j \leqslant p$.

Por exemplo,

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & -3 & 4 \\ 5 & 1 & -5 \end{bmatrix} = \begin{bmatrix} 1(3)+0(5) & 1(-3)+0(1) & 1(4)+0(-5) \\ 2(3)+3(5) & 2(-3)+3(1) & 2(4)+3(-5) \end{bmatrix}$$

$$= \begin{bmatrix} 3 & -3 & 4 \\ 21 & -3 & -7 \end{bmatrix}.$$

Devemos destacar que, mesmo que o produto entre as matrizes esteja definido para AB e para BA, em geral, teremos que $AB \neq BA$.

Exemplo 3.1.2. *Sejam:*

$$A = \begin{bmatrix} 1 & 2 \\ 4 & 1 \end{bmatrix} \quad e \quad B = \begin{bmatrix} 0 & -1 \\ 1 & 2 \end{bmatrix}.$$

Realizando os cálculos necessários obtemos:

$$AB = \begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix} \neq BA = \begin{bmatrix} -4 & -1 \\ 9 & 4 \end{bmatrix}.$$

3.2. Matrizes quadradas

Chamamos de matriz quadrada de orden n, ou simplesmente de matriz quadrada, toda matriz cujo número de linhas é igual ao número de colunas, isto é, uma matriz do conjunto $M_{n\times n}(F)$. Toda *matriz quadrada* de ordem n apresenta duas diagonais: a diagonal principal que é formada pelos elementos do tipo a_{ii}, com $1 \leqslant i \leqslant n$, já a outra diagonal é chamada de diagonal secundária e seus elementos são expressos por $a_{i(n+1-i)}$, com $1 \leqslant i \leqslant n$. Abaixo, um exemplo de matriz quadrada de ordem 3:

$$\begin{bmatrix} 0 & 76 & -10 \\ 15 & 47 & 99 \\ 89 & -23 & 812 \end{bmatrix}.$$

Na matriz acima, por exemplo, os elementos que compõe a diagonal principal são os números $0, 47$ e 812, que correspondem, sucessivamente, às entradas a_{11}, a_{22} e a_{33}. Já os elementos da diagonal secundária são os números $-10, 47$ e 89, que se encontram, sucessivamente, nas posições a_{13}, a_{22} e a_{31}.

A matriz cujos elementos da diagonal principal são iguais a 1 e os demais elementos são iguais a zero, é dita *matriz identidade de ordem n* e será denotada por Id_n. Por exemplo, se $n = 4$, temos:

$$\mathrm{Id}_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Todas as propriedades citadas anteriormente, continuam valendo para matrizes quadradas. Além disto, como a multiplicação está sempre bem definida entre matrizes quadradas, podemos verificar a veracidade de tais propriedades:

Proposição 3.2.1. *Considerando as matrizes A, B e C* $\in M_{n\times n}(F)$ *e* $\lambda \in \mathbb{R}$*:*

(i) $A(B+C) = AB+AC.$
(ii) $(A+B)C = AC+BC.$
(iii) $(AB)C = A(BC).$
(iv) $A\mathrm{Id}_n = \mathrm{Id}_n A = A.$
(v) $\lambda(AB) = (\lambda A)B$

Demonstração. Sejam A, B, C matrizes de ordem m.

(i) $A(B+C) = \sum_{k=1}^{n} A_{ik}(B+C)_{kj} = \sum_{k=1}^{n} a_{ik}(b_{kj}+c_{kj}) = \sum_{k=1}^{n}(a_{ik}b_{kj}+a_{ik}c_{kj}) =$
$= \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj} = AB+AC.$

(ii) $(A+B)C = \sum_{k=1}^{n}(A+B)_{ik}C_{kj} = \sum_{k=1}^{n}(a_{ik}+b_{ik})c_{kj} = \sum_{k=1}^{n}(a_{ik}c_{kj}+b_{ik}c_{kj}) =$
$= \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj} = AC+BC.$

(iii) $((AB)C)_{ij} = \sum_{k=1}^{n}(AB)_{ik}C_{kj} = \sum_{k=1}^{n}\left(\sum_{l=1}^{n} a_{il}b_{lk}\right)c_{kj} = \sum_{l=1}^{n} a_{il}\left(\sum_{k=1}^{n} b_{lk}c_{kj}\right) =$
$= \sum_{l=1}^{n} a_{il}(BC)_{ij} = (A(BC))_{ij}.$

(iv) Seja $\mathrm{Id}_n = [b_{ij}]$, sabemos que se $i = j$, então $b_{ij} = 1$, caso contrário, $b_{ij} = 0$. Então,

$A\mathrm{Id}_n = c_{ij} = \sum_{k=1}^{n}(A\mathrm{Id}_n)ij = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n} a_{ij}b_{jj} = \sum_{k=1}^{n} a_{ij} = A.$
$\mathrm{Id}_n A = d_{ij} = \sum_{k=1}^{n}(\mathrm{Id}_n A)ij = \sum_{k=1}^{n} b_{ik}a_{kj} = \sum_{k=1}^{n} b_{ii}a_{ij} = \sum_{k=1}^{n} a_{ij} = A.$

Logo, $A\mathrm{Id}_n = \mathrm{Id}_n A = A.$

(v) $\lambda(AB)_{ij} = \lambda\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{n}\lambda(a_{ik}b_{kj}) = \sum_{k=1}^{n}(\lambda a_{ik})b_{kj} = ((\lambda A)B)_{ij}.$

□

3.3. Determinantes

Dada uma matriz quadrada $A \in M_{n\times n}(F)$, podemos associar a ela um elemento de F, o qual chamaremos de *determinante*. Tal número é obtido através de uma função que satisfaz as propriedades apresentadas a seguir. Para mais detalhes, vide [1, Cap. 4].

Definição 3.3.1. *Seja $A \in M_{n\times n}(F)$, na qual $c_1, c_2, ..., c_n$ representam seus vetores colunas, isto é, $c_1, c_2, ..., c_n \in F^n$. Chamamos de **função determinante** e representamos por $D(c_1, c_2, ..., c_n)$ uma função:*

$$\begin{aligned} D(A) := \quad & F^n \times \cdots \times F^n \quad \longrightarrow F \\ & (c_1, \ldots, c_n) \quad \longmapsto D(c_1, \ldots, c_n) \end{aligned}$$

que satisfaça as seguintes propriedades:

1. *D é multilinear, ou seja, D é linear em cada coluna separadamente. Isto é, se $c_j = c'_j + \lambda c''_j$, onde $c'_j, c''_j \in F^n$ e $\lambda \in F$, então:*

$$D(c_1, \cdots, c'_j + \lambda c''_j, \cdots, c_n) = D(c_1, \cdots, c'_j, \cdots, c_n) + \lambda D(c_1, \cdots, c''_j, \cdots, c_n).$$

2. *Se c_j e c_{j+1} são colunas adjacentes e iguais, então:*

$$D(c_1, \cdots, c_j, c_{j+1}, c_n) = 0.$$

3. *Se Id_n representa a matriz identidade de $M_{n\times n}(F)$, então:*

$$D(\mathrm{Id}_n) = 1.$$

3.3.1. Consequências da definição

Proposição 3.3.1. *Seja $j \in \mathbb{N}$, com $1 \leqslant j \leqslant n-1$. Se $A' \in M_{n\times n}(F)$ é a matriz obtida trocando de posição duas colunas adjacentes de $A \in M_{n\times n}(F)$, isto é, $c_j \longleftrightarrow c_{j+1}$, então:*

$$D(A') = -D(A).$$

Demonstração. Sejam $A = [c_1\ c_2\ \cdots\ c_n]$ e $B = [b_1\ b_2\ \cdots\ b_n]$ matrizes em $M_{n\times n}(F)$ representadas através de seus vetores colunas, tais que $b_i = c_i$, se $i \neq j$ e $i \neq j+1$, e com $b_j = b_{j+1} = c_j + c_{j+1}$.

Uma vez que $b_j = b_{j+1}$, temos $D(B) = D(c_1, \cdots, b_j, b_{j+1}, \cdots, c_n) = 0$. Então:

$$\begin{aligned} 0 &= D(c_1, \cdots, c_j + c_{j+1}, c_j + c_{j+1}, \cdots, c_n) \\ &= D(c_1, \cdots, c_j, c_j, \cdots, c_n) + D(c_1, \cdots, c_j, c_{j+1}, \cdots, c_n) \\ &+ D(c_1, \cdots, c_{j+1}, c_j, \cdots, c_n) + D(c_1, \cdots, c_{j+1}, c_{j+1}, \cdots, c_n). \end{aligned}$$

Mas, pela propriedade 2 de determinante, temos:

$$D(c_1, \cdots, c_j, c_j, \cdots, c_n) = D(c_1, \cdots, c_{j+1}, c_{j+1}, \cdots, c_n) = 0$$

Isto é:

$$\begin{aligned} 0 &= D(c_1, \cdots, c_j, c_{j+1}, \cdots, c_n) + D(c_1, \cdots, c_{j+1}, c_j, \cdots, c_n) \\ &\Leftrightarrow D(c_1, \cdots, c_{j+1}, c_j, \cdots, c_n) = -D(c_1, \cdots, c_j, c_{j+1}, \cdots, c_n) \\ &\Leftrightarrow D(A') = -D(A). \end{aligned}$$

□

Corolário 3.3.0.1. *Se $A \in M_{n\times n}(F)$ apresenta quaisquer duas colunas iguais, então $D(A) = 0$.*

Demonstração. Dada uma matriz com colunas iguais, podemos trocar as colunas de posição até que as colunas coincidentes sejam também adjacentes. Segue da proposição acima e da propriedade 2 do determinante que:

$$D(A) = \pm D(A') = 0.$$

□

Corolário 3.3.0.2. *Seja A' uma matriz obtida ao trocarmos quaisquer duas colunas de $A \in M_{n\times n}(F)$, isto é, $c_i \longleftrightarrow c_j$, com $i \neq j$, então $D(A') = -D(A)$.*

Demonstração. Sejam c_k, com $k = 1, \ldots, n$ as n colunas de A, e A' a matriz quadrada de ordem n obtida a partir da matriz A onde trocamos de posição as colunas c_i e c_j. Defina a matriz $B = [b_{ij}] \in M_{n\times n}(F)$ cujas colunas b_k são definidas como segue:

$$b_k = \begin{cases} c_i + c_j, & \text{se } k = i \text{ ou } k = j, \\ c_k, & \text{se } k \neq i \text{ e } k \neq j. \end{cases}$$

Uma vez que $b_i = b_j$, temos $D(B) = D(c_1, \cdots, b_i, \cdots, b_j, \cdots, c_n) = 0$. Daí:

$$\begin{aligned} 0 &= D(c_1,\cdots,c_i+c_j,\cdots,c_i+c_j,\cdots,c_n) \\ &= D(c_1,\cdots,c_i,\cdots,c_i,\cdots,c_n)+D(c_1,\cdots,c_i,\cdots,c_j,\cdots,c_n) \\ &+ D(c_1,\cdots,c_j,\cdots,c_i,\cdots,c_n)+D(c_1,\cdots,c_j,\cdots,c_{j+1},\cdots,c_n). \end{aligned}$$

Mas, pelo Corolário 3.3.0.1:

$$D(c_1,\cdots,c_i,\cdots,c_i,\cdots,c_n) = D(c_1,\cdots,c_j,\cdots,c_j,\cdots,c_n) = 0.$$

E portanto:

$$\begin{aligned} & 0 = D(c_1,\cdots,c_i,\cdots,c_j,\cdots,c_n)+D(c_1,\cdots,c_j,\cdots,c_i,\cdots,c_n) \\ \Leftrightarrow\ & D(c_1,\cdots,c_j,\cdots,c_i,\cdots,c_n) = -D(c_1,\cdots,c_i,\cdots,c_j,\cdots,c_n) \\ \Leftrightarrow\ & D(A') = -D(A). \end{aligned}$$

□

Doravante, assumiremos a existência e unicidade da função determinante[2] e nos referiremos ao determinante de uma matriz $A \in M_{n\times n}(F)$, escrevendo $det\ A$, ou ainda $|A|$ e cujo valor é obtido utilizando a seguinte expressão:

$$detA = |A| = \sum_{\pi\in S_n} \varepsilon(\pi) a_{1\pi(1)} a_{2\pi(2)} a_{3\pi(3)} ... a_{n\pi(n)},$$

na qual π representa uma das permutações entre os elementos de um conjunto finito do tipo $\{1,2,\cdots,n\}$ e $\varepsilon(\pi)$ indica o sinal de tal permutação. A derivação desta expressão para o determinante é apresentada no Apêndice A.

Como casos particulares da definição de determinante dada acima, segue que:

- Se $A = [a_{11}]$, $det\ A = a_{11}$.
- Se $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $det\ A = a_{11}a_{22} - a_{12}a_{21}$.

  Tal relação também é conhecida como a diferença entre os produtos dos elementos da diagonal principal e o produto dos elementos da diagonal secundária.
- Se $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, então

$$det\ A = a_{11}a_{22}a_{33} + a_{13}a_{21}a_{32} + a_{12}a_{23}a_{31} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

[2] Veja [1, Capítulo 4] para mais detalhes.

A expressão acima também pode ser obtida após aplicarmos a Regra de Sarrus.

- Para matrizes de ordens maiores, apresentaremos o cálculo através de cofatores. Serão apresentadas também algumas propriedades do determinante que serão úteis ao longo do texto.

Observação 3.3.1. *A matriz que possui todos os elementos acima ou abaixo da diagonal principal iguais a zero é dita triangular inferior ou superior, respectivamente, e seu determinante é expresso por:*

$$det\ A = a_{11}a_{22} \cdot \ldots \cdot a_{nn}.$$

Exemplo 3.3.1. *Para ilustrar a relação acima, considere as matrizes A e B dadas abaixo:*

a) $A = \begin{bmatrix} 1 & 3 & 2 & 1 \\ 0 & 6 & 5 & 24 \\ 0 & 0 & -3 & 3 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow det\ A = 1 \cdot 6 \cdot (-3) \cdot 1 = -18.$

b) $B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 11 & 2 & 0 & 0 \\ 7 & 12 & -3 & 0 \\ 1 & 1 & 4 & 1 \end{bmatrix} \Rightarrow det\ B = 1 \cdot 2 \cdot (-3) \cdot 1 = -6.$

Proposição 3.3.2. *Sejam A e B matrizes de ordem n e $\lambda \in F$:*

1. $det(A \cdot B) = det\ A \cdot det\ B.$
2. $det\ A = det\ A^t.$
3. $det(\lambda A) = \lambda^n det\ A.$

Para uma demonstração da proposição acima, vide [1].

3.3.2. Cofator e determinante

Para o cálculo do determinantes de matrizes com ordem superior a três, os métodos usualmente conhecidos como: diferença entre os produtos das diagonais, no caso 2×2 e a Regra de Sarrus, no caso 3×3, não se aplicam. Para tal, utilizaremos o desenvolvimento por cofatores.

Definição 3.3.2. *Seja A uma matriz quadrada, o cofator de um elemento $a_{ij} \in A$ é definido pela expressão:*

$$cof(a_{ij}) = (-1)^{i+j} det\ A_{ij},$$

onde a matriz A_{ij} é obtida retirando-so a i-ésima e a j-ésima coluna da matriz A.

Teorema 3.3.1. *A partir da definição de cofator, o determinante de A será expresso por:*

$$det\ A = \sum_{i=1}^{n} a_{ij} cof(a_{ij}),$$

onde j, $1 \leqslant j \leqslant n$, *representa uma coluna qualquer de* A.

O resultado acima é conhecido como *Teorema de Laplace* e sua demonstração encontra-se no Apêndice A deste texto.

Exemplo 3.3.2. *Seja* $A = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 0 & 2 \\ 1 & 2 & 1 \end{bmatrix}$, *teremos:*

- $cof(a_{11}) = (-1)^{1+1} \begin{vmatrix} 0 & 2 \\ 2 & 1 \end{vmatrix} = -4.$
- $cof(a_{12}) = (-1)^{1+2} \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = 1.$
- $cof(a_{13}) = (-1)^{1+3} \begin{vmatrix} 1 & 0 \\ 1 & 2 \end{vmatrix} = 2.$

Procedendo da mesma forma com o restante dos elementos, obtemos:

$$\begin{array}{lll} cof(a_{21}) = 0, & cof(a_{22}) = 2, & cof(a_{23}) = -4, \\ cof(a_{31}) = 0, & cof(a_{32}) = -4, & cof(a_{33}) = 0. \end{array}$$

Para o cálculo do determinante, fixando, por exemplo, a coluna 2, temos:

$$det\ A = \sum_{i=1}^{n} a_{i2} cof(a_{i2}) = a_{12} cof(a_{12}) + a_{22} cof(a_{22}) + a_{32} cof(a_{32}).$$

Utilizando os resultados obtidos anteriormente, segue que:

$$det\ A = 0.1 + 0.2 + 2.(-4) = -8.$$

3.3.3. Matriz inversa

Dadas duas matrizes $A, B \in M_{n\times n}(F)$ tais que $A, B \neq 0$. Dizemos que A (ou B) é inversível se $AB = BA = \mathrm{Id}_n$. Quando uma matriz é inversível, isto é, quanto possui inversa, então a inversa

é única. De fato, suponhamos que B e B' são inversas de A. Daí, por definição, $AB = BA = \mathrm{Id}_n$ e $AB' = B'A = \mathrm{Id}_n$. Utilizando os itens (c) e (d) da Proposição 3.2.1, temos:

$$B = B\mathrm{Id}_n = B(AB') = (BA)B' = \mathrm{Id}_n B' = B'.$$

Devido a unicidade da inversa da matriz A, a denotaremos por A^{-1}.

Podemos calcular a inversa de uma matriz, caso ela exista, por meio da resolução de um sistema linear. Como ilustra o exemplo a seguir:

Exemplo 3.3.3. *Considere a matriz:*

$$A = \begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix},$$

se sua inversa existir, esta será uma matriz de ordem 2, que satisfaz a seguinte equação:

$$\begin{bmatrix} 2 & 3 \\ 0 & 4 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Ou seja:

$$\begin{bmatrix} 2a+3c & 2b+3d \\ 0a+4c & 0b+4d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Acima temos uma igualdade entre matrizes. Isso ocorre se, dadas duas matrizes A e B de mesmo ordem, temos $a_{ij} = b_{ij}$ para todo $1 \leqslant i \leqslant m$ e $1 \leqslant j \leqslant n$. Portanto, temos:

$$\begin{cases} 2a+3c = 1 \\ 4c = 0 \\ 2b+3d = 0 \\ 4d = 1 \end{cases}.$$

Realizando os cálculos necessários, encontramos que

$$A^{-1} = \begin{bmatrix} 1/2 & 3/8 \\ 0 & 1/4 \end{bmatrix}.$$

Em alguns casos, o sistema linear obtido não apresenta solução, isso implica que a matriz em questão não possui inversa.

Exemplo 3.3.4. *Seja a matriz:*

$$B = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix},$$

se sua inversa existir, esta será uma matriz de ordem 2, tal que:

$$\begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix} \cdot \begin{bmatrix} x & z \\ y & w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Daí:

$$\begin{bmatrix} 2x+3y & 2z+3w \\ 4x+6y & 4z+6w \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Portanto,

$$\begin{cases} 2x+3y=1 \\ 4x+6y=0 \\ 2z+3w=0 \\ 4z+6w=1 \end{cases}.$$

Note que a primeira e a segunda equações são incompatíveis. Isso significa que o sistema não apresenta solução, ou, equivalente, a matriz B não possui inversa.

O método apresentado é simples, mas trabalhoso quando aumentamos a ordem da matriz da qual queremos determinar a inversa. Felizmente, existe uma maneira alternativa de determinar a inversa de uma matriz, quando a mesma existe. Na próxima seção apresentaremos tal método em conjunto com a condição necessária e suficiente para garantir a existência da inversa.

3.3.4. Cofatores no cálculo da inversa

Já vimos como determinar a inversa de uma matriz quadrada através de sistemas lineares. Apresentaremos agora como tal cálculo pode ser realizado utilizando cofatores e o determinante da matriz.

Tomaremos agora a matriz formada pelos cofatores de A, onde cada cofator ocupará a posição do seu elemento de referência, por exemplo, o $cof(a_{11})$ ocupará a posição na linha 1 e coluna 1, tal matriz será chamada de C.

Exemplo 3.3.5. *A matriz dos cofatores correspondente à matriz A apresentada no Exemplo 3.3.2, será expressa por:*

$$C = \begin{bmatrix} -4 & 1 & 2 \\ 0 & 2 & -4 \\ 0 & -2 & 0 \end{bmatrix}.$$

Definição 3.3.3. *Ao tomarmos a transposta da matriz dos cofatores, obtemos a matriz adjunta, isto é,*

$$adj(A) = \left([cof(a_{ij})]\right)^t.$$

Exemplo 3.3.6. *Tomando a matriz dos cofatores C obtida no Exemplo 3.3.5, temos que a matriz adjunta será:*

$$adj(A) = \begin{bmatrix} -4 & 0 & 0 \\ 1 & 2 & -2 \\ 2 & -4 & 0 \end{bmatrix}.$$

É possível estabelecer uma expressão que relacione uma matriz quadrada, sua adjunta e seu determinante. Para ilustrar tal relação, considere A uma matriz 3×3 qualquer e defina $B = adj(A) \cdot A$. Vamos mostrar que:

$$b_{ij} = \begin{cases} det(A), \text{se } \ i = j; \\ 0, \text{se } \ i \neq j. \end{cases}$$

onde b_{ij} são as entradas da matriz B.

Escreva

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \quad \text{e} \quad adj(A) = \begin{bmatrix} cof(a_{11}) & cof(a_{21}) & cof(a_{31}) \\ cof(a_{12}) & cof(a_{22}) & cof(a_{32}) \\ cof(a_{13}) & cof(a_{23}) & cof(a_{33}) \end{bmatrix}$$

Vamos analisar separadamente os casos em que $i = j$ e $i \neq j$.

No caso particular em que $i = j = 1$, temos:

$$b_{11} = a_{11}cof(a_{11}) + a_{12}cof(a_{12}) + a_{13}cof(a_{13}).$$

Situação análoga acontece nos casos em que $i = j = 2$ e $i = j = 3$. De maneira que, podemos escrever:

$$b_{jj} = \sum_{k=1}^{3} (cof(a_{kj}))a_{kj}.$$

De acordo com a Definição 3.3.1, a expressão acima representa o determinante da matriz A. Portanto, $b_{jj} = det(A)$.

Agora, se $i \neq j$, temos:

$$b_{ij} = \sum_{k=1}^{3} (cof(a_{ki}))a_{kj} = (cof(a_{1i}))a_{1j} + (cof(a_{2i}))a_{2j} + (cof(a_{3i}))a_{3j}.$$

Fixando, por exemplo, $i = 1$ e $j = 3$, encontramos:

$$b_{13} = (cof(a_{11}))a_{13} + (cof(a_{21}))a_{23} + (cof(a_{31}))a_{33}.$$

Tal expressão pode ser reescrita como:

$$b_{13} = (-1)^2 \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} a_{13} + (-1)^3 \begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} a_{23} + (-1)^4 \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} a_{33}.$$

Observe que b_{13} é equivalente ao determinante de uma matriz, a qual denotaremos por C, de ordem 3, fixada a primeira coluna:

$$C = \begin{bmatrix} a_{13} & a_{12} & a_{13} \\ a_{23} & a_{22} & a_{23} \\ a_{33} & a_{32} & a_{33} \end{bmatrix}.$$

Note que, temos duas colunas iguais em C, o que implica que $det\ C = 0$. Ao tomarmos os demais b_{ij}, com $i \neq j$, encontraremos situações análogas. Portanto, se $i \neq j$, teremos $b_{ij} = 0$.

Por fim, podemos concluir que, ao multiplicarmos a adjunta de uma matriz de ordem 3 pela própria matriz, nessa ordem, iremos obter uma matriz diagonal, na qual os elementos da diagonal principal são iguais ao determinante da matriz A e os demais elementos são iguais a 0, isto é:

$$adj(A) \cdot A = det(A)\mathrm{Id}_3.$$

A expressão obtida acima é válida para qualquer matriz quadrada. Tal fato é apresentado na proposição a seguir.

Proposição 3.3.3. *Se A é uma matriz quadrada de ordem n, então:*

$$adj(A) \cdot A = det(A)\mathrm{Id}_n. \tag{3.1}$$

A prova de tal proposição é análoga ao caso aqui apresentado e é encontrada com mais detalhes em [6, pág. 235].

Proposição 3.3.4. *A é inversível se, e somente se, $detA \neq 0$.*

Demonstração.

($\Rightarrow$) Seja A uma matriz inversível de ordem m, então:

$$A \cdot A^{-1} = \mathrm{Id}_n \Rightarrow det(A \cdot A^{-1}) = det(\mathrm{Id}_n) \Rightarrow det(A) \cdot det(A^{-1}) = 1.$$

$det\ A$ e $det\ A^{-1}$ são números reais, portanto, para que seu produto seja 1, é necessário que $det\ A \neq 0$.

($\Leftarrow$) Se $det\ A \neq 0$, podemos reescrever a equação 3.1 como:

$$\frac{1}{det\ A}(adj(A) \cdot A) = \mathrm{Id}_n.$$

Pela proposição 3.2.1, tal expressão é equivalente a

$$\left(\frac{1}{det\ A} adj(A)\right) \cdot A = \mathrm{Id}_n.$$

Seja $\left(\frac{1}{det\ A} adj(A)\right) = B$, temos então

$$BA = \mathrm{Id}_n.$$

Podemos concluir que A é inversível, uma vez que o Teorema 2.5 de [8], nos garante que se A e B são matriz quadradas de ordem n tais que $BA = Id_n$, então B é a inversa de A. □

Corolário 3.3.1.1. *Se A é inversível, então:*

$$A^{-1} = (det\ A)^{-1} adj(A).$$

Demonstração. Se A é inversível, então $detA \neq 0$ e segue que:

$$adj(A) \cdot A = det(A)\mathrm{Id}_n \Rightarrow adj(A) = det(A)\mathrm{Id}_n \cdot A^{-1} \Rightarrow adj(A).(det(A))^{-1} = A^{-1}.$$

□

Exemplo 3.3.7. *Determine a inversa da matriz:*

$$A = \begin{bmatrix} 2 & -1 & 2 \\ 1 & 0 & 1 \\ 0 & 1 & 3 \end{bmatrix}.$$

Realizando os cálculo necessário, encontramos $det\ A = 3 \Rightarrow (det\ A)^{-1} = 3^{-1}$ *e* $adj(A) = \begin{bmatrix} -1 & 5 & -1 \\ -3 & 6 & 0 \\ 1 & -2 & 1 \end{bmatrix}$*, pelo Corolário 3.3.0.3, teremos:*

$$A^{-1} = 3^{-1} \begin{bmatrix} -1 & 5 & -1 \\ -3 & 6 & 0 \\ 1 & -2 & 1 \end{bmatrix} = \begin{bmatrix} -3^{-1} & 5.3^{-1} & -3^{-1} \\ -1 & 2 & 0 \\ 3^{-1} & -2.3^{-1} & 3^{-1} \end{bmatrix}.$$

3.4. Matrizes sobre $\mathbb{Z}_p$, onde p é um número primo

Nesta seção iremos voltar nosso foco para o estudo de matrizes com entradas em $\mathbb{Z}_p$, observando que todo estudo feito antes continuará válido aqui. Destacaremos as peculiaridades do estudo de matrizes sobre corpos finitos.

Sobre $\mathbb{Z}_p$, trabalhamos com as classes de congruência $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\}$. Como tais classes são as únicas que compõe $\mathbb{Z}_p$, por abuso de notação, iremos considerar que $\mathbb{Z}_p = \{0, 1, 2, ..., p-1\}$. Além disso, trataremos como iguais e não equivalentes, elementos que ocupam a mesma classe de congruência. Por exemplo, sabemos que os números 9 e 16 deixam resto 2 ao serem divididos por 7. Daí, escreveremos simplesmente 9 = 16 = 2, deixando claro o corpo sobre o qual estamos efetuando os cálculos.

Uma matriz $m \times n$ sobre $\mathbb{Z}_p$ é uma tabela de m linhas e n colunas de modo que seus elementos a_{ij} são tais que $0 \leq a_{ij} \leq p-1$.

Por exemplo, a matriz $A = \begin{bmatrix} 7 & 24 & -1 \\ 0 & -5 & 10 \\ 1 & 5 & 81 \end{bmatrix}$ em $\mathbb{Z}_2$ é igual a $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$,

enquanto em $\mathbb{Z}_3$ teremos $A = \begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 1 \\ 1 & 2 & 0 \end{bmatrix}$.

3.4.1. Operações entre matrizes sobre $\mathbb{Z}_p$

As operações de matrizes $M_{n\times n}(\mathbb{Z}_p)$, são idênticas às exibidas na seção 3.1. Aqui, só temos que levar em consideração as classes de $\mathbb{Z}_p$. Vejamos alguns exemplos:

1. Em $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \\ 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 2 \\ 5 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1+3 & 0+2 \\ 2+5 & 3+1 \\ 4+2 & 0+0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 7 & 4 \\ 6 & 0 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 2 & 4 \\ 1 & 0 \end{bmatrix}.$$

2. Em $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \\ 4 & 0 \end{bmatrix} - \begin{bmatrix} 3 & 2 \\ 5 & 1 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 1-3 & 0-2 \\ 2-5 & 3-1 \\ 4-2 & 0-0 \end{bmatrix} = \begin{bmatrix} -2 & -2 \\ -3 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 2 & 2 \\ 2 & 0 \end{bmatrix}.$$

3. Em $\mathbb{Z}_7$:

$$5 \cdot \begin{bmatrix} 2 & 3 \\ 3 & 1 \\ 4 & 6 \end{bmatrix} = \begin{bmatrix} 10 & 15 \\ 15 & 5 \\ 20 & 30 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 1 & 5 \\ 6 & 2 \end{bmatrix}.$$

4. Em $\mathbb{Z}_7$:

$$\begin{bmatrix} 1 & 0 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 2 & 4 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1(3)+0(0) & 1(2)+0(1) & 1(4)+0(0) \\ 2(3)+3(0) & 2(2)+3(1) & 2(4)+3(0) \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 2 & 4 \\ 6 & 7 & 8 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 4 \\ 6 & 0 & 1 \end{bmatrix}.$$

3.5. Determinantes:

Para o cálculo do determinante de uma matriz A sobre $\mathbb{Z}_p$, usaremos os métodos previamente apresentados. Porém, vale ressaltar que o resultado obtido ao realizarmos os cálculos devem

pertencer a $\mathbb{Z}_p$, de modo que $0 \leqslant det\ A \leqslant p-1$, e para isso, em alguns momentos será necessário encontrar o representante principal da classe de congruência do resultado obtido.

Por exemplo, em $\mathbb{Z}_7$,

$$detA = \begin{vmatrix} 3 & 1 \\ 2 & 6 \end{vmatrix} = 16 = 2.$$

3.5.1. Cofator e determinante

O cálculo de cofatores também segue a definição já apresentada. Isto é, dada uma matriz $A_{m\times n}$ sobre $\mathbb{Z}_p$,

$$cof(a_{ij}) = (-1)^{i+j} det\ A_{ij},$$

onde a matriz A_{ij} é obtida retirando-so a i-ésima linha e a j-ésima coluna da matriz A, e $0 \leq cof(a_{ij}) \leq p-1$.

Assim, o determinante de A será expresso por:

$$det\ A = \sum_{i=1}^{n} a_{ij} cof(a_{ij}),$$

fixando j como uma coluna qualquer da matriz A.

Exemplo 3.5.1. *Em* $\mathbb{Z}_3$, *se* $A = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 0 & 2 \\ 1 & 2 & 1 \end{bmatrix}$, *teremos:*

- $cof(a_{11}) = (-1)^{1+1} \begin{vmatrix} 0 & 2 \\ 2 & 1 \end{vmatrix} = -4 = 2.$
- $cof(a_{12}) = (-1)^{1+2} \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = 1.$
- $cof(a_{13}) = (-1)^{1+3} \begin{vmatrix} 1 & 0 \\ 1 & 2 \end{vmatrix} = 2.$

Procedendo da mesma forma com o restante dos elementos, obtemos:

$$\begin{array}{lll} cof(a_{21}) = 0, & cof(a_{22}) = 2, & cof(a_{23}) = -4 = 2, \\ cof(a_{31}) = 0, & cof(a_{32}) = -4 = 2, & cof(a_{33}) = 0. \end{array}$$

Para o cálculo do determinante, fixaremos, por exemplo, a coluna 2. Daí:

$$det\ A = \sum_{i=1}^{n} a_{i2} cof(a_{i2}) = a_{12} cof(a_{12}) + a_{22} cof(a_{22}) + a_{32} cof(a_{32}).$$

Utilizando os resultados obtidos anteriormente, teremos

$$det\ A = 0.1 + 0.2 + 2.2 = 4 = 1.$$

3.6. Cofatores no cálculo da inversa

Ao trabalharmos sobre $\mathbb{Z}_p$ o cálculo de inversas por meio de sistemas lineares não é o mais adequado, uma vez que os elementos encontrados podem, eventualmente, serem números fracionários. Dessa forma, utilizaremos o cálculo através de cofatores.

Por exemplo, se tomarmos a matriz formada pelos cofatores da matriz A do exemplo anterior, teremos:

$$C = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 2 & 2 \\ 0 & 2 & 0 \end{bmatrix}.$$

A partir dessa matriz, obtemos a *matriz adjunta*:

$$adj(A) = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 2 & 2 \\ 2 & 2 & 0 \end{bmatrix}.$$

Proposição 3.6.1. *A é inversível se, e somente se, $detA \neq 0$.*

Observe que tal proposição continua sendo válida uma vez que, o elemento 0 ocupa a classe de equivalência $\overline{0}$, para todo $\mathbb{Z}_p$. A novidade aqui é que matrizes cujo determinante é um número inteiro múltiplo de p (matrizes que são inversíveis sobre $\mathbb{Q}$, por exemplo) aqui não são inversíveis, uma vez que $p \in \overline{0}$. Se a inversa de A existe, então:

$$A^{-1} = (det\ A)^{-1} adj(A).$$

Nesse ponto, denotamos o inverso multiplicativo, sobre $\mathbb{Z}_p$, do determinante de A por

$$(det\ A)^{-1}.$$

Exemplo 3.6.1. *Seja $A \in M_{n\times n}(\mathbb{Z})$ uma matriz com coeficientes inteiros tal que seu determinante seja o número inteiro 2. Então, a imersão da matriz A em $M_{n\times n}(\mathbb{Z}_p)$, temos $det\, A = 2$,*

(a) em $\mathbb{Z}_5$ temos $(det\ A)^{-1} = 3$, uma vez que $2 \cdot 3 = 6 = 1$.
(b) em $\mathbb{Z}_7$, temos que $(det\ A)^{-1} = 4$, já que $2 \cdot 4 = 8 = 1$.

Observação 3.6.1. *Em $\mathbb{Z}_4$, o 2 não possui inverso multiplicativo pois é um divisor de zero, uma vez que $2 \cdot 2 = 4 = 0$.*

Exemplo 3.6.2. *Determine, em $\mathbb{Z}_5$ a inversa da matriz $A \in \mathbb{Z}_5$:*

$$A = \begin{bmatrix} 3 & 1 & 2 \\ 1 & 1 & 2 \\ 0 & 1 & 3 \end{bmatrix}.$$

Realizando os cálculos necessários, encontramos $det\ A = 2$, e disso obtemos pelo exemplo 3.6.1 que $(det\ A)^{-1} = 3$. Além disso,

$$adj(A) = \begin{bmatrix} 1 & 4 & 0 \\ 2 & 4 & 1 \\ 1 & 2 & 2 \end{bmatrix},$$

logo:

$$A^{-1} = 3 \begin{bmatrix} 1 & 4 & 0 \\ 2 & 4 & 1 \\ 1 & 2 & 2 \end{bmatrix} = \begin{bmatrix} 3 & 12 & 0 \\ 6 & 12 & 3 \\ 3 & 6 & 6 \end{bmatrix} = \begin{bmatrix} 3 & 2 & 0 \\ 1 & 2 & 3 \\ 3 & 1 & 1 \end{bmatrix}.$$

4 Um pouco sobre Criptografia

A cada dia, a segurança de acesso a informação torna-se uma mercadoria cada vez mais valiosa, fazendo com que os processos de codificação estejam cada vez mais presentes no cotidiano, mesmo que utilizados sem o nosso conhecimento. Sites de banco, sites de compra online, por exemplo, utilizam protocolos que, por meio da criptografia, garantem a segurança do cliente. Mas nem sempre foi assim, até a década de 1970, a criptografia segura era utilizada com o principal objetivo de proteger segredos de Estado. A história é repleta de códigos, que auxiliaram na decisão de importantes batalhas, levando inclusive, à morte alguns reis e rainhas. Faremos uma breve descrição e um apanhado histórico sobre os tipos mais famosos de criptografia clássica, isto é, aqueles que utilizam de papel e caneta.

O processo de criptografia, consiste nas seguintes etapas:

- O remetente transforma a mensagem original em um texto criptografado utilizando uma *chave criptografadora*.
- O destinatário recebe o texto criptografado, e utilizando uma *chave descriptografadora*, a descriptografa, recuperando assim a mensagem original.

Método de criptografar

O processo de criptografar funciona em geral, de duas maneiras: por transposição ou por substituição.

O processo de **transposição** consiste em trocarmos os caracteres do texto de posição, entre si, seguindo uma determinada regra previamente combinada entre remetente e destinatário. Ao se tratar de palavras curtas, é simples descobrir a palavra original. Mas, ao se tratar de textos longos, torna-se mais trabalhosa a sua decifragem.

Exemplo 4.0.1. *A palavra LUA pode ser criptografada como AUL.*

Já no processo de **substituição**, os caracteres do texto são mantidos em suas posições originais, mas são substituídos por outro símbolo de um conjunto pré-determinado, tal conjunto é chamado de *alfabeto de substituição*.

Exemplo 4.0.2. *Ao tomarmos a tabela abaixo como referência para o alfabeto de substituição, temos que a palavra LUA, ao ser criptografada, se torna MVB.*

Tabela 4.1.: Alfabeto de substituição

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

Observação 4.0.1. *A criptografia por substituição funciona com caracteres isolados, palavras ou até mesmo frases.*

Observação 4.0.2. *A substituição pode ser monoalfabética, nesse caso cada caracter do texto original corresponde a um só caracter do alfabeto de substituição, ou ainda polialfabéticas, nesse caso são utilizados mais de um alfabeto de substituição para o alfabeto normal.*

Métodos de Chave

A chave utilizada para criptografia pode ser uma *chave simétrica* ou uma *chave pública*.

No método que utiliza a *chave simétrica*, as chaves para criptografar e descriptografar mensagens são conhecidas pelo emissário e receptor, podendo ser a mesma.

Já no método que utiliza a *chave pública*, a chave de encriptação é pública, mas apenas o destinatário possui informações capazes de descriptografar a mensagem, sendo computacionalmente impossível encontrar a chave de descriptação sem tais informações. Para ilustrar tal método, imagine a seguinte situação: Ana pretende enviar uma mensagem secreta para Gabriela que está do outro lado do país. Ana escreve a mensagem, a tranca numa caixa de ferro com um cadeado e a manda pelo correio. No entanto, Gabriela não consegue abrir a caixa pois não tem a chave do cadeado. Tal problema não é simples de ser solucionado, uma vez que Ana não confia nos correios e acha que o carteiro pode fazer uma cópia da chave, revelando assim o conteúdo da mensagem. Isso impede que a chave seja enviada pelo mesmo caminho que a mensagem. Para resolver esse problema, Gabriela recebe a mensagem, e sem ter como abri-la, coloca seu próprio cadeado e a manda de volta pra Ana. Ana recebe a mensagem, retira seu cadeado e remete a mensagem novamente a Gabriela, que recebe seu cadeado e finalmente lê a mensagem. Observe que tal método é eficiente, uma vez que a caixa nunca fica destrancada e as chaves não saem do poder de seus donos. Tal ideia motivou a criação das chaves públicas.[1]

[1] Tal fato é narrado de maneira semelhante em [11].

Cifras

As mensagens que utilizam *chaves simétricas* para serem criptografadas, podem ser enviadas em blocos ou de forma contínua. Chamamos de *cifra contínua* o processo no qual as informações são enviadas em pequenas partes para o processo de criptografia e a saída também é produzida em pequenas partes. Já uma *cifra em bloco* é àquela na qual as informações são previamente agrupadas para serem criptografadas, e a saída também é produzida da mesma forma.

4.1. Modelos famosos de Criptografia

4.1.1. Cítala Espartana

A *cítala espartana* consiste em um método de enviar mensagem usando a transposição, de chave simétrica. Esse, segundo Singh (2002), foi o primeiro dispositivo criptográfico militar, datado no século V a.C. e consiste em um bastão de madeira com um pergaminho, ou tira de couro, enrolado. O remetente enrola o pergaminho, escreve a mensagem e em seguida o desenrola, de modo que obtém uma lista de letras sem sentido. Ao receber a mensagem cifrada, o destinatário deve voltar a enrolá-la no bastão, de modo a obter a mensagem original.

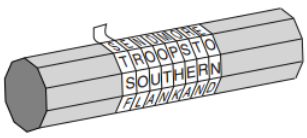


Figura 4.1.: Cítala Espartana.
(Fonte: Singh, 2002, pág. 12)

4.1.2. Cifra de César

A cifra de César consiste em um modelo de substituição, de chave simétrica, onde cada letra da mensagem original é trocada por outra letra do alfabeto.

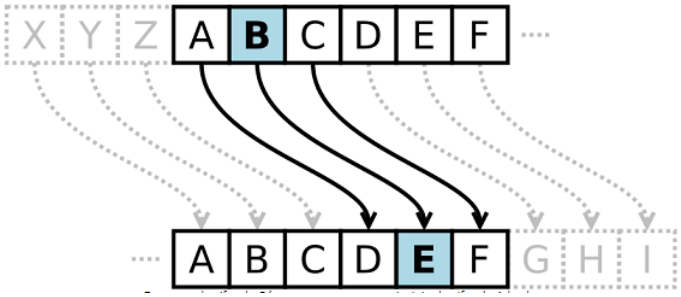


Figura 4.2.: Modelo Cifra de César.
(Fonte:
$http://www.dsc.ufcg.edu.br/pet/jornal/abril2014/materias/historia_da_computacao.html$
- Acesso em $26/07/2017$)

Tal modelo foi muito utilizado na Roma antiga, por Júlio César. César utilizava sempre o deslocamento de 3 posições no alfabeto para cifrar suas mensagens, mas o padrão pode ser alterado.

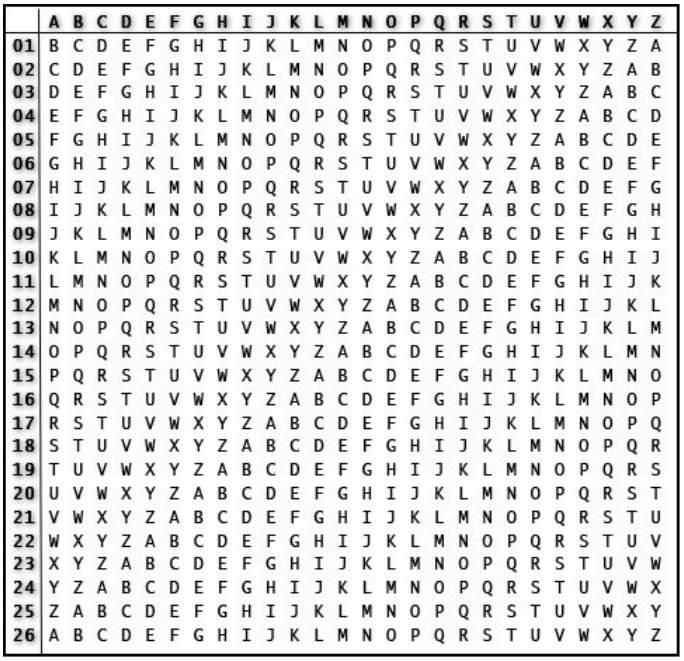
Exemplo 4.1.1. *Utilizando a Cifra de César convencional, a palavra LUA se transformaria em OXD.*

4.1.3. Cifra de Vingenère

A Cifra de Vingenère consiste na utilização de várias Cifras de César, baseando-se em letras de uma senha. Tal método é considerado de substituição polialfabética e representa uma versão simplificada da Cifra de Albertini.[2]

Para criptografar uma mensagem utilizando a Cifra de Vingenère, o primeiro passo é montar a grelha de Vigenère, um alfabeto normal seguido de 26 alfabetos cifrados, cada um deslocando uma letra em relação ao alfabeto anterior. O remetente da mensagem pode, por exemplo, cifrar a primeira letra de acordo com a linha 5, a segunda de acordo com a linha 14 e a terceira de acordo com a linha 21, e assim por diante. Esse sistema deve ser previamente combinado entre remetente e destinatário.

[2]Para informações sobre a Cifra de Albertini, recomendamos a leitura de [13].



	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
01	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
02	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
03	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
04	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
05	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
06	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
07	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
08	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
09	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

Figura 4.3.: Grelha de Vingenère.
(Fonte: $https://danieldonda.wordpress.com/2007/10/31/cifra-de-vigenere-le-chiffre-indechiffrable/$ - Acesso em $26/07/2017$)

Um dos métodos utilizados era a escolha de uma palavra-chave. Por exemplo, na mensagem "Amigos, obrigada", podemos considerar a primeira palavra como palavra-chave, o que significa que toda a mensagem será codificada usando seis dos vinte e seis alfabetos disponíveis. De maneira mais clara, a primeira letra deve ser codificada com o alfabeto que tem início em A, a segunda com o alfabeto que tem início em M, a terceira com o alfabeto que se inicia em I e assim sucessivamente. Ao fechar o ciclo dos 6 alfabetos, repetimos o processo começando do primeiro alfabeto utilizado.

Exemplo 4.1.2. *De acordo com o sistema apresentado, a frase "Amigos, obrigada" ao ser codificada se transformaria em AYQMCKONZOUSDM. Nessa cifra acentos, sinais de pontuação e espaços são desconsiderados.*

4.1.4. O método RSA

Desenvolvido por Ron Rivest, Leonard Adleman e Adi Shamir, o método RSA é um dos principais modelos de criptografia que utilizam a chave pública. Tal modelo veio a se tornar a cifra mais influente da criptografia moderna, isto é, criptografias que usam artifícios digitais.

Figura 4.4.: Ronald Rivest, Adi Shamir e Leonard Adleman.
(Fonte: Singh, 2002, pág. 204)

O RSA, como já citado, é uma criptografia de chave pública, onde parte desta chave é um número N, obtido através da multiplicação de dois números primos. O valor de N pode ser divulgado sem comprometer a mensagem em questão, pois os números primos escolhidos são números muito grandes, de modo que nem os computadores mais modernos conseguem obtê-los. [3]

4.2. Cifra de Hill

Uma das cifrais conhecidas mais populares, é a Cifra de Hill, segundo [18], tal cifra foi desenvolvida por Lester S. Hill em 1929.

A Cifra de Hill consiste em um sistema de criptografia por substituição polialfabética, baseado em transformações matriciais. Para a aplicação de tal cifra, é necessário criar uma relação biunívoca entre as letras do alfabeto e um subconjunto dos números inteiros, uma das possibilidades é mostrada na tabela abaixo.

Tabela 4.2.: Correspondência entre letras e números.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

4.2.1. Criptografando uma mensagem

Para aplicação da cifra de Hill é necessário que a mensagem seja escrita em letras maiúsculas e que sejam ignorados acentos e possíveis espaços. Por exemplo, a frase "Eu amo matemática",

[3] Para mais informações sobre o RSA consultar [15], [16] e [17].

para ser criptografada deve se transformar em "EUAMOMATEMATICA". Em seguida, a nova "palavra" é divida em blocos de n letras. O valor de n pode variar de acordo com o interesse do remetente.

Exemplo 4.2.1. *Vamos criptografar a palavra* AMOR *utilizando uma criptografia de Hill, com $n = 2$, e para isso, organizamos o processo em 4 passos com o objetivo de torna-lo claro:*

***Passo 1**: Escolher uma matriz quadrada, de ordem igual a n, nesse caso, uma matriz quadrada de ordem 2. Tal matriz deve ser formada por números inteiros e possuir inversa em $\mathbb{Z}_{26}$, o que pode ser verificado de acordo com a Corolário 3.6.0.1.*
Com base nessas especificações, tomamos a matriz quadrada abaixo, cujo determinante é 3. Tal matriz será chamada de chave criptografadora.

$$A = \begin{bmatrix} 5 & 4 \\ 3 & 3 \end{bmatrix}.$$

***Passo 2**: Agrupamos as letras da mensagem em pares, como definido previamente. Em seguida, deve-se substituir cada letra pelo número correspondente, encontrado na Tabela 4.2.*

$$\text{AMOR} \longrightarrow \text{AM OR} \longrightarrow 1\ 13 \quad 15\ 18$$

Observação 4.2.1. *Caso a quantidade de letras da mensagem original seja um número ímpar, nesse caso onde $n = 2$, deve-se adicionar uma letra qualquer ao final da palavra com o intuito de completar os pares. Por exemplo, se estivéssemos trabalhando com a palavra LUA, seria necessário acrescentar uma quarta letra a fim de obtermos os blocos com 2 letras, como foi determinado. A escolha da letra fica a critério do remetente uma vez que não interfere de maneira significativa o significado da mensagem.*

***Passo 3**: Colocar capa par de letras formado em um vetor coluna, os quais chamaremos de E_1 e E_2. Em seguida determinar os produtos AE_1 e AE_2, a fim de obtermos os vetores cifrados.*

$$E_1 = \begin{bmatrix} 1 \\ 13 \end{bmatrix} \quad \text{e} \quad E_2 = \begin{bmatrix} 15 \\ 18 \end{bmatrix}.$$

Daí,

$$AE_1 = \begin{bmatrix} 57 \\ 16 \end{bmatrix} \quad \text{e} \quad AE_2 = \begin{bmatrix} 147 \\ 99 \end{bmatrix}.$$

***Passo 4**: Para os vetores cifrados no passo 3, devemos encontrar seus correspondentes em $\mathbb{Z}_{26}$ para associarmos cada um a seu equivalente alfabético.*

Daí,

$$AE_1 = \begin{bmatrix} 5 \\ 16 \end{bmatrix} \quad e \quad AE_2 = \begin{bmatrix} 17 \\ 21 \end{bmatrix}.$$

E, portanto, ao criptografarmos a palavra AMOR, obtemos EPQU.

4.2.2. Descriptografando uma mensagem

A criptografia pela Cifra de Hill utiliza uma chave simétrica, isto é, ao conhecer a chave criptografadora utilizada pelo remetente, o destinatário tem condições de, por meio de operações matriciais e pelo Algoritmo de Euclides, de determinar a chave descriptografadora e assim ter acesso à mensagem enviada.

Exemplo 4.2.2. *Para ilustrar o processo de descriptografia, vamos utilizar o Exemplo 4.2.1, onde obtivemos a mensagem EPQU. O objetivo aqui é exibir como recuperar a mensagem original AMOR. Para tal, devemos seguir os seguintes passos:*

***Passo 1**: Para descriptografar uma mensagem criptografada pela cifra de Hill, é necessário conhecer a chave criptografadora e determinar a sua inversa. Do exemplo anterior temos:*

$$A = \begin{bmatrix} 5 & 4 \\ 3 & 3 \end{bmatrix}.$$

E fazendo os cálculos necessários, obtemos:

$$A^{-1} = (det\ A)^{-1} \cdot adj(A) = (det\ A)^{-1} \cdot \begin{bmatrix} 3 & -4 \\ -3 & 5 \end{bmatrix}.$$

***Passo 2**: Devemos encontrar o inverso multiplicativo em $\mathbb{Z}_{26}$ do determinante da matriz chave. Sabemos que $det A = 3$, daí, o $(det A)^{-1} = 9$. Daí:*

$$A^{-1} = \begin{bmatrix} 27 & -36 \\ -27 & 45 \end{bmatrix}.$$

***Passo 3**: A matriz de decodificação inversa será dada pela equivalente em $\mathbb{Z}_{26}$ à matriz encontrada no passo 2. Teremos:*

$$A^{-1} = \begin{bmatrix} 1 & 16 \\ 25 & 19 \end{bmatrix}.$$

Passo 4: *Analogamente ao processo utilizado para criptografar, tomamos a palavra ou frase criptografada, dividindo suas letras em duplas. Encontramos os números correspondentes e transformamos cada dupla em um vetor, que chamaremos de D_1 e D_2.*

$$EPQU \longrightarrow EP \quad QU \longrightarrow 5 \;\; 16 \quad 17 \;\; 21$$

$$D_1 = \begin{bmatrix} 5 \\ 16 \end{bmatrix} \text{ e } D_2 = \begin{bmatrix} 17 \\ 21 \end{bmatrix}.$$

Passo 5: *Tomamos o produto da matriz inversa por cada um dos vetores obtidos e em seguida, encontramos seu equivalente em $\mathbb{Z}_{26}$. Fazendo os cálculos necessários, por fim obtemos:*

$$A^{-1}D_1 = \begin{bmatrix} 1 \\ 13 \end{bmatrix} \text{ e } A^{-1}D_2 = \begin{bmatrix} 15 \\ 18 \end{bmatrix}.$$

Obtendo a palavra AMOR.

No próximo capítulo será apresentada uma atividade envolvendo duas possíveis adaptações da Cifra de Hill. Tal atividade pode ser utilizada em turmas do Ensino Médio, com o intuito de estimular o estudo de matrizes por parte dos alunos, além de reforçar fundamentos de divisibilidade e o Algoritmo de Euclides.

5 Desenvolvimento da atividade

Um jogo pode ser entendido de diversas maneiras e pretender atingir objetivos distintos. Quando trabalhado em sala de aula, o papel primordial dessas atividades é despertar interesse e prazer, uma vez que representam um desafio. De acordo com os Parâmetros Curriculares Nacionais (1998):

> Os jogos constituem uma forma interessante de propor problemas, pois permitem que estes sejam apresentados de modo atrativo e favorecem a criatividade na elaboração de estratégias de resolução e busca de soluções. Propiciam a simulação de situações problema que exigem soluções vivas e imediatas, o que estimula o planejamento das ações; possibilitam a construção de uma atitude positiva perante os erros, uma vez que as situações sucedem-se rapidamente e podem ser corrigidas de forma natural, no decorrer da ação, sem deixar marcas negativas.

O jogo proposto a seguir, pretende estimular o trabalho em grupo, permitindo que o professor avalie alguns aspectos importantes corriqueiros da sala de aula, como a capacidade dos alunos trabalharem em grupos, a facilidade para compreender o mecanismo do jogo, a construção de uma estratégia vencedora, a capacidade de analisar as hipóteses previamente discutidas além de aspectos operacionais básicos da matemática.

Nosso principal objetivo na proposta desse jogo, é que os estudantes “brinquem” de espionagem. À princípio, a turma deve ser divida em grupos, tais grupos serão organizados em duas grandes alianças. Cada grupo deve enviar mensagens de maneira segura para seus aliados, de modo que os opositores tenham acesso à essas mensagens, mas não consigam decifrá-las.

5.1. O jogo - Crip War

Para realização do jogo são necessários os seguintes materias:

- Seis dados (Três de ataque e três de defesa);

- Fichas contendo os objetivos;
- Pincéis/giz de duas cores para simbolizar os exércitos de cada aliança.

A aplicação do jogo pode variar de acordo com o interesse do professor, mas propomos a seguinte execução, que é uma adaptação do jogo "War".

Organização do Jogo

Suponha uma turma na qual seja possível formar 6 grupos, com em média, 4 alunos por grupo; de modo que $R1$, $R2$ e $R3$ compondo a aliança REPÚBLICA, e $I1$, $I2$ e $I3$, a aliança IMPÉRIO. Cada uma das aliança deverá criar sua própria chave criptografadora, a qual os opositores não devem ter acesso.[1]

Observação 5.1.1. *A quantidade dos grupos pode variar, desde que seja um número par.*

Feita a divisão, o professor deve fazer uma tabela no quadro, contendo duas colunas e o número de linhas igual ao número de grupos. Na hipótese em questão, teríamos a seguinte situação:

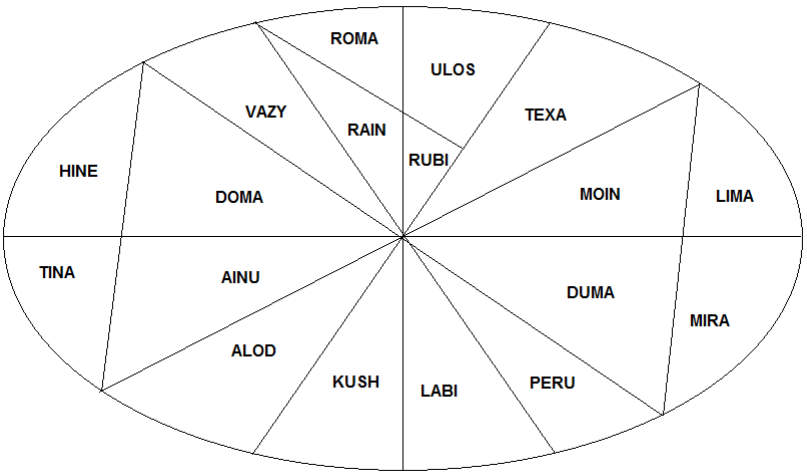
Tabela 5.1.: Modelo de Tabela.

R1	
R2	
R3	
I1	
I2	
I3	

Também deve ser desenhado uma região aleatória, a qual será dividida em pequenas regiões, as quais chamaremos de países. O número de países deve ser igual ao triplo do número de grupos. Em seguida, os países devem ser nomeados, com nomes que possuam a mesma quantidade de letras. Sugerimos a utilização de 4 letras a fim de simplificar os cálculos.

[1] Tal chave será apresentada na próxima seção.

Figura 5.1.: Sugestão de mapa para 6 grupos.



Em seguida, cada grupo receberá um objetivo entre os 12 existentes, evitando revelá-lo aos seus adversários. Os objetivos do jogo são, por exemplo:

- Conquiste os países ROMA, KUSH e MIRA.
- Conquiste os países RUBI, TEXA e HINE.
- Conquiste os países ALOD, VAZY e MOIN.
- Conquiste os países LABI, TINA e ULOS.
- Conquiste os países AINU, DUMA e VAZY.
- Conquiste os países RAIN, DOMA e LIMA.
- Conquiste os países LIMA, DUMA e KUSH.
- Conquiste os países VAZY, TEXA e MIRA.
- Conquiste os países ALOD, HINE e LABI.
- Conquiste os países ULOS, ROMA e MOIN.
- Conquiste os países MIRA, RUBI e TINA.
- Conquiste os países AINU, ALOD e HINE.

Após receberem a carta de objetivo, cada grupo deve criptografar os países ali presentes, utilizando um dos instrumentos propostos nas próximas seções e a chave pré determinada. Feito isso, um integrante de cada grupo deve ir até o quadro e escrever o nome dos países que devem ser conquistados por aquela equipe, de maneira criptografada, na linha referente ao seu grupo na Tabela 5.1. Em seguida, as equipes de cada aliança, devem descriptografar a carta objetivo de seus aliados de modo à criarem uma estratégia vitoriosa.

Feito isso, deve ser estabelecida, por meio de sorteio, uma ordem de jogada, tal ordem deve alternar um grupo de cada aliança. Suponhamos que a ordem sorteada seja $R1 - I1 -$

$R2 - I2 - R3 - I3$. Após o sorteio e seguindo a ordem estabelecida, cada grupo deve dirigir-se ao mapa e posicionar dois exércitos, da maneira que desejar, em territórios vazios ou em territórios já ocupados por exércitos aliados.

Nas rodadas seguintes, cada grupo passa pelas seguintes etapas:

1. recebe um novo exército e o coloca de acordo com a sua estratégia;
2. se desejar, atacar uma vez os seus adversários e
3. remanejar seus exércitos, se houver conveniência.

Para as rodadas seguintes, o grupo recebe um exército, que deve ser disposto em algum país que já contenha algum exército de sua aliança, ou em um país vazio, conforme estratégia, não podendo em hipótese alguma colocar um exército onde haja tropas rivais.

Feito isso, o grupo pode optar por atacar os exércitos oponentes. Para atacar a partir de um território, é necessário que haja pelo menos 2 exércitos da mesma aliança neste mesmo território, uma vez que um único exército é chamado de "exército de ocupação", e não tem o direito de ataque.

Regras de ataque:

1. O ataque, a partir de um território qualquer possuído, só pode ser dirigido a um território adversário que tenha fronteiras em comum.
2. O número de exércitos que poderá participar de um ataque será igual ao número de exércitos situados no território atacante menos um, que é o exército de ocupação.
3. O número máximo de exércitos participantes em cada ataque é de 3, mesmo que o número de exércitos possuídos no território seja superior a 4.
4. Um jogador pode atacar tantas vezes quantas quiser para conquistar um território adversário, até ficar só um exército no seu território ou, ainda, até quando achar conveniente não atacar.
5. O número de exércitos que a defesa pode usar, em cada batalha, é de no máximo 3 e no mínimo 1 (podendo utilizar inclusive o exército de ocupação).
6. O jogador atacante jogará o dado quantas vezes for o número de seus exércitos participantes da batalha, o mesmo ocorrendo com o jogador da defesa. Assim, se o atacante usar 3 exércitos contra um da defesa, ele jogará o dado 3 vezes contra um lançamento do defensor.

Contagem dos dados

Após uma batalha, a decisão de quem ganha e quem perde exércitos é feita da seguinte forma: compara-se o maior ponto do lançamento atacante com o maior ponto do lançamento defensor e o maior deles ganha, sendo que o empate é sempre da defesa. Em seguida, compara-se o 2º maior ponto atacante com o 2º maior do defensor, e a decisão de vitória é como no caso anterior. Por fim, comparam os menores valores, baseando-se na mesma regra.

Exemplo 5.1.1.

a) *No caso do atacante possuir 4 exércitos no seu território e o defensor 3, ambos poderiam jogar com 3 dados. Supondo-se que o atacante tivesse tirado 5, 4 e 1 e o defensor 6, 3 e 1 a comparação seria feita da seguinte forma:*

Tabela 5.2.: Lançamento Dados.

	Ataque	Defesa	Vencedor
Maior	5	6	Defesa
2º	4	3	Ataque
Menor	1	1	Defesa

Observe que nesse caso, o atacante teria vencido uma jogada e perdido duas, o que significa que ele perde 2 exércitos enquanto o defensor perde 1 exército. Assim, o território do atacante, que tinha 4 exércitos, passou a ficar com 2 e do defensor que tinha 3, ficou com 2. Se houvesse interesse, o atacante poderia continuar o ataque com 1 exército contra 2 da defesa.

b) *Atacante : 3 exércitos – Defesa : 1 exército. O atacante pode jogar 2 dados contra 1 da defesa. Supondo-se que os pontos tenham sido : ataque 3 e 2; defesa 6, compararia-se o maior ponto do ataque (3), com o maior ponto da defesa (no caso só um único valor 6). A vitória caberia à defesa, retirando do ataque um de seus exércitos.*

Conquista de Territórios

Se após a batalha o atacante destruir todos os exércitos do território do defensor, terá então conquistado o território e deverá, após a conquista, deslocar um de seus exércitos atacantes para o território conquistado.

Remanejamentos

Ao finalizar seus ataques o jogador poderá, de acordo com a sua estratégia, efetuar deslocamentos de exércitos entre os seus territórios que fazem fronteira, lembrando-se que em cada território deve permanecer sempre pelo menos um exército (de ocupação) que nunca pode ser deslocado. Além disso um exército pode ser deslocado uma única vez, isto é, não se pode deslocar um exército para um território vizinho e deste para outro, também vizinho, numa mesma jogada.

Em suma, em cada rodada, um grupo deve, nessa ordem:

1. Receber novo exército;
2. Colocar este exército de acordo com sua estratégia;
3. Efetuar um ataque, se possível e desejável e
4. Remanejar seus exércitos, se possível e desejável.

Final do jogo

O jogo termina quando uma das alianças conquistar todo seu objetivo, isto é, dominar todos as regiões designadas a cada um dos grupos que a compõe. Nesse momento as fichas "objetivo" de cada um dos grupos da mesma devem ser exibidas, comprovando a vitória.

5.2. Instrumento I de Codificação

O material proposto a seguir tem como objetivo servir de instrumento para que as palavras do Crip War sejam criptografadas, impedindo o conhecimento da equipe rival a respeito das mesmas.

1. Construção dos materiais;
2. Criptografando uma mensagem;
3. Descriptografando uma mensagem.

5.2.1. Construção dos materiais

O primeiro passo do jogo é a construção dos instrumentos a serem utilizados, e para isso, será necessário que a turma seja dividida em grupos de 3 a 5 alunos, que desponham dos seguintes materiais:

- Um cubo no qual seja possível nomear os vértices, os pontos médios das arestas e os pontos médios onde as diagonais das faces e as diagonais do cubo se cruzam;
- Uma matriz que será a chave criptografadora (C_r);
- Uma matriz que será a chave descriptografadora (D_r).

Cubo

Para construir o cubo, sugerimos a utilização dos seguintes materiais:

- 27 Palitos de churrasco;
- 27 Bolas de isopor;
- 27 Palitos de dente;
- Papel

Para iniciar, devemos conectar dois palitos de churrasco em uma bola de isopor formando um ângulo de 90° entre eles. Para melhor acabamento é recomendada a utilização de cola quente no palito após a fixação.

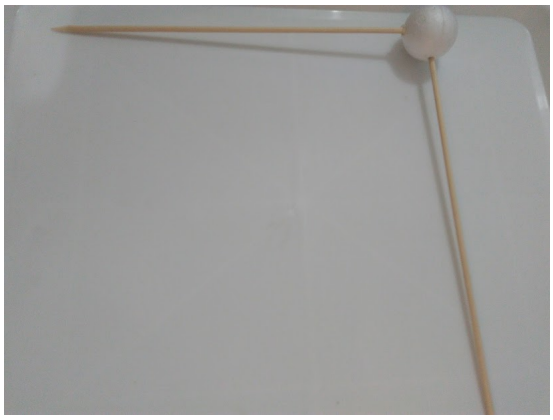


Figura 5.2.: Passo 1.

Feito isso, fixamos uma bola de isopor no ponto médio de cada um dos palitos já posicionados.

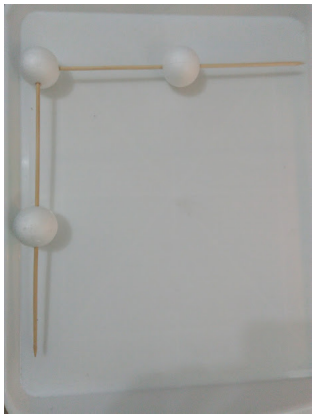
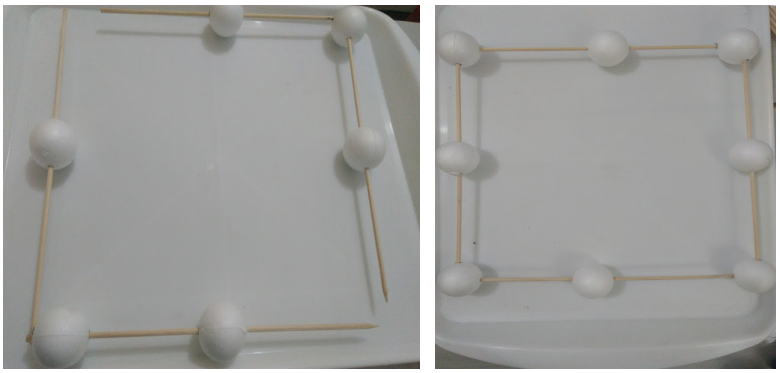


Figura 5.3.: Passo 2.

Repetimos o precedimento e conectamos as duas estruturas obtidas utilizando bolinhas de isopor nas pontas soltas.



(a) (b)

Figura 5.4.: Passo 3.

Devemos repetir todo o processo até obtermos 3 estruturas iguais à obtida no passo 3.

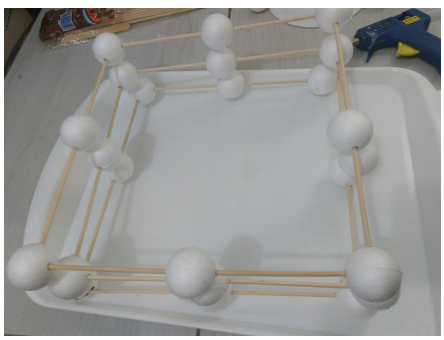
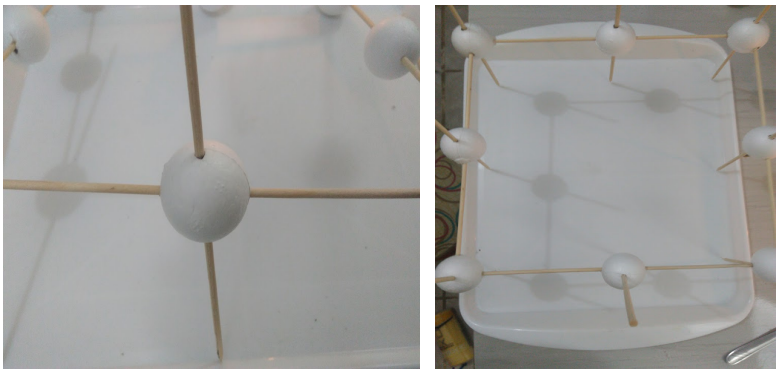


Figura 5.5.: Passo 4.

Pegamos uma das estruturas acima e fixamos, em cada uma das bolas, um palito perpendicular ao já fixado.



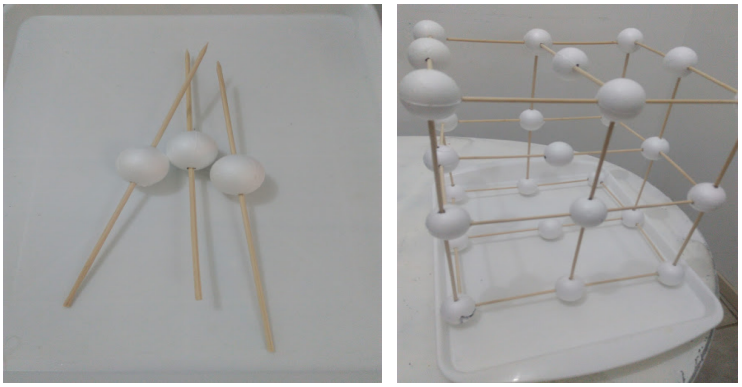
(a) (b)

Figura 5.6.: Passo 5.

Unimos então as estruturas obtidas em 5.5

Figura 5.7.: Passo 6.

Para finalizar, fixamos uma bola no ponto médio de um novo palito. Repetimos esse procedimento três vezes e os encaixamos na estrutura obtida em 5.7.



(a) (b)

Figura 5.8.: Passo 7.

Para reforçar a estrutura construída, sugerimos que sejam acrescentados palitos perpendiculares aos últimos palitos acrescentados em 5.8(b).

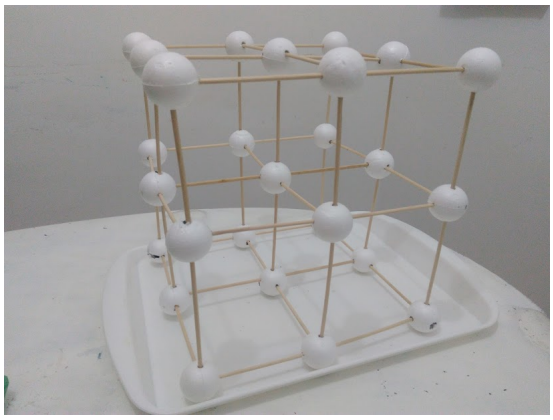


Figura 5.9.: Cubo codificador.

Feita a estrutura, devemos associar cada isopor a uma trinca ordenada do tipo (x, y, z). Para fazer tal enumeração, deve-se levar em conta o sistema de coordenadas tridimensional no qual um dos vértices do cubo representa a origem do sistema.

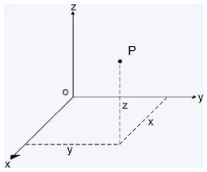


Figura 5.10.: Sistema Cartesiano Tridimensional
(Fonte: $http://efisica.if.usp.br/mecanica/universitario/cinematica/pos_coord_cartes/$ - Acesso em $24/07/2017$)

A partir daí, os 27 símbolos pré determinados devem ser associados, um a um, a uma bolinha de isopor, e portanto a uma única trinca ordenada. Tal distribuição pode ser feita de maneira aleatória.

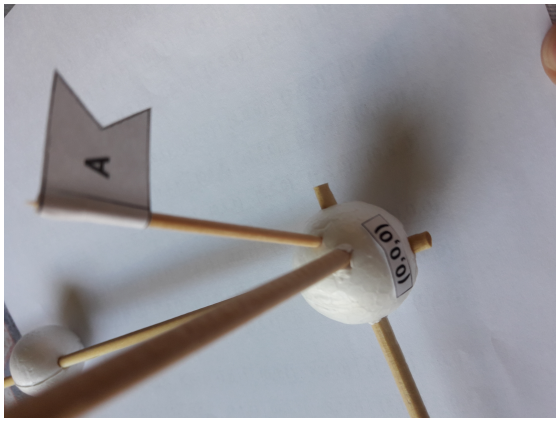


Figura 5.11.: Associação entre símbolos e trincas ordenadas.

Observação 5.2.1. *As fotografias apresentadas nessa seção foram retiradas pela autora da dissertação.*

Sugerimos que tal associação, por questão de praticidade, seja associada a uma tabela, como mostraremos a seguir.

Tabela 5.3.: Correspondência entre trincas e símbolos

(0,0,0) $\longrightarrow$ A	(1,0,0) $\longrightarrow$ B	(2,0,0) $\longrightarrow$ C
(0,1,0) $\longrightarrow$ D	(1,1,0) $\longrightarrow$ E	(2,1,0) $\longrightarrow$ F
(0,2,0) $\longrightarrow$ G	(1,2,0) $\longrightarrow$ H	(2,2,0) $\longrightarrow$ I
(0,0,1) $\longrightarrow$ J	(1,0,1) $\longrightarrow$ K	(2,0,1) $\longrightarrow$ L
(0,1,1) $\longrightarrow$ M	(1,1,1) $\longrightarrow$ N	(2,1,1) $\longrightarrow$ O
(0,2,1) $\longrightarrow$ P	(1,2,1) $\longrightarrow$ Q	(2,2,1) $\longrightarrow$ R
(0,0,2) $\longrightarrow$ S	(1,0,2) $\longrightarrow$ T	(2,0,2) $\longrightarrow$ U
(0,1,2) $\longrightarrow$ V	(1,1,2) $\longrightarrow$ W	(2,1,2) $\longrightarrow$ X
(0,2,2) $\longrightarrow$ Y	(1,2,2) $\longrightarrow$ Z	(2,2,2) $\longrightarrow$?

Observe que cada símbolo está associado a uma trinca ordenada (x,y,z), a qual tomaremos como uma matriz coluna do tipo $\begin{bmatrix} x \\ y \\ z \end{bmatrix}$. A letra M, por exemplo, será representada pela matriz $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$.

Chave Criptografadora

O próximo passo pode ser feito em conjunto com a turma, ou apenas apresentado pelo professor. É necessário que seja construída uma matriz quadrada, de ordem 3, com entradas variando de 0 à 2 cujo determinante não seja múltiplo de 3. Tal matriz será chamada de *matriz chave*. Para ilustrar, vamos utilizar a seguinte matriz:

$$C_r = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix},$$

a qual atende os requisitos levantados acima: $c_{i,j} \in \{0,1,2\}$ e $det\ C_r = 1$.

Chave Descriptografadora

Uma vez dada a matriz chave, precisamos de uma outra matriz, a qual será chamada matriz *Chave Descriptografadora*, a qual denotaremos por D_r. Inicialmente, determinamos a matriz adjunta de C_r. Em nosso exemplo,

$$adj(C_r) = \begin{bmatrix} -1 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & -1 & -4 \end{bmatrix}.$$

Agora, devemos encontrar algum número natural, cujo produto pelo valor de $det\ C_r$ deixe resto 1 quando dividido por 3. Sabemos que $det\ C_r = 1$, Note que $1 \times 1 = 1$, cujo resto na

divisão por 3 é 1. Feito isso, tomamos o produto do número encontrado como $(det\ C_r)^{-1}$ pela matriz $adj(C_r)$. Então:

$$(C')_r^{-1} = 1 \cdot adj(C_r) = \begin{bmatrix} -1 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & -1 & -4 \end{bmatrix} = D'_r.$$

Para finalmente encontrarmos a chave descriptografadora, precisamos determinar a matriz D_r, correspondente à D'_r, com entradas d_{ij} tais que $0 \leqslant d_{ij} \leqslant 2$. Cada elemento de D_r será o resto obtido na divisão de cada um dos elementos de D'_r por 3. Caso o número seja negativo, somamos, sucessivamente, 3 a ele até que se torne positivo. Durante todo o processo utilizaremos esse fato, caso encontremos alguma matriz com entradas que não variem de 0 à 2. Daí, obtemos a matriz:

$$D_r = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & 2 & 2 \end{bmatrix}.$$

5.2.2. Criptografando uma mensagem

Para iniciar o processo de criptografar uma mensagem, criptografamos cada letra de maneira independente, depois, ordenadamente, as juntamos a fim de obter a palavra criptografada. Já vimos que cada letra está associada a uma única trinca ordenada, de maneira que, a representaremos por uma matriz coluna do tipo:

$$\begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}.$$

Em seguida, obtemos o produto entre a matriz chave e as matrizes correspondentes a cada letra. Encontraremos assim, novas matrizes colunas, e ao tomarmos a condição de que suas entradas devem variar de 0 à 2, encontramos trincas correspondentes na Tabela 5.3 e teremos a palavra criptografada.

Observe tal processo de maneira prática:

Exemplo 5.2.1. *Mensagem original: AMOR*

***Passo 1**: Encontrar as matrizes correspondentes a cada letra:*

$$\text{A} \longrightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad \text{M} \longrightarrow \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}; \quad \text{O} \longrightarrow \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}; \quad \text{R} \longrightarrow \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}.$$

***Passo 2**: Tomamos o produto da matriz C_r, determinada anteriormente, pelas matrizes encontradas no Passo 1.*

- $C_r \cdot A = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$;
- $C_r \cdot M = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 1 \end{bmatrix}$;
- $C_r \cdot 0 = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \\ 1 \end{bmatrix}$;
- $C_r \cdot R = \begin{bmatrix} 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ 5 \\ 2 \end{bmatrix}$.

***Passo 3**: Devemos encontras as matrizes com entradas variando de 0 à 2. Para a construção de tais matrizes, consideramos, novamente, o resto da divisão de cada um dos elemento por 3. Daí:*

$$C_r \cdot A = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad C_r \cdot M = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}; \quad C_r \cdot O = \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}; \quad C_r \cdot R = \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}.$$

***Passo 4**: Finalmente, para obter a mensagem criptografada, determinamos os símbolos correspondentes às matrizes criptografadas.*

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \longrightarrow \text{A}; \quad \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \longrightarrow \text{M}; \quad \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix} \longrightarrow \text{R}; \quad \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} \longrightarrow \text{Z}.$$

Daí ao criptografar a palavra AMOR*, obtemos a sequência* AMRZ.

Observação 5.2.2. *Para criptografar uma mensagem podemos optar por criptografar grupos de letras ou letra a letra. Escolhemos a segunda opção pelo fato de que a medida que aumentamos a quantidade de letras por grupo, a ordem das matrizes C_r e D_r crescem consideravelmente. O processo em agrupamentos se dá de maneira análoga, se o agrupamento é feito considerando grupos de n letras, as matrizes C_r e D_r devem ter ordem igual a $3n$. Isto é, ao optarmos por trabalhar com o agrupamento em duplas, trabalharemos com matrizes de ordem 6. É interessante*

que esse fato seja discutido com a turma mas ao optar pelo trabalho com matrizes de ordem 6, acreditamos que o jogo pode ficar exaustivo e deixar de ser interessante para o estudante.

5.2.3. Descriptografando uma mensagem

Para descriptografar uma mensagem, devem ser conhecidas a chave descriptografadora (D_r) e a tabela utilizada como referência de símbolos tabela. O processo inicial é análogo ao realizado para criptografar, devemos identificar as matrizes coluna referentes a cada uma das letras da sequência criptografada.

Tomamos então, o produto de D_r pelas matrizes criptografados. Ao tomarmos as matrizes com entradas de 0 à 2, correspondentes ao produto, considerando os restos da divisão por 3, teremos descriptografado as matrizes, obtendo assim, a mensagem original.

De maneira prática:

Exemplo 5.2.2. *Mensagem original: AMRZ*

***Passo 1**: Determinamos então as matrizes coluna correspondentes a cada dupla. Teremos:*

$$\mathrm{A} \longrightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad \mathrm{M} \longrightarrow \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}; \quad \mathrm{R} \longrightarrow \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}; \quad \mathrm{Z} \longrightarrow \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix}.$$

***Passo 2**: Tomamos o produto de D_r pelas matrizes obtidas no Passo 1. Teremos:*

$$D_r \cdot A = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix};$$

$$D_r \cdot M = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix};$$

$$D_r \cdot R = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \\ 1 \\ 10 \end{bmatrix};$$

$$D_r \cdot Z = \begin{bmatrix} 2 & 1 & 2 \\ 0 & 0 & 1 \\ 2 & 2 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ 2 \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \\ 10 \end{bmatrix}.$$

***Passo 3**: Encontramos matrizes correspondentes às anteriores, considerando o resto da divisão de cada um dos elementos por 3. Daí:*

$$D_r \cdot A = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad D_r \cdot M = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}; \quad D_r \cdot R = \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix}; \quad D_r \cdot Z = \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix}.$$

***Passo 4**: Finalmente, basta encontrar na Tabela 2 os símbolos referentes às matrizes descriptografadas. Portanto,*

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \longrightarrow \text{A}; \quad \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \longrightarrow \text{M}; \quad \begin{bmatrix} 2 \\ 1 \\ 1 \end{bmatrix} \longrightarrow \text{O}; \quad \begin{bmatrix} 2 \\ 2 \\ 1 \end{bmatrix} \longrightarrow \text{R}.$$

Daí, ao descriptografarmos a sequência AMRZ*, obtemos a palavra* AMOR*.*

5.3. Instrumento II de Codificação

O instrumento apresentado a seguir, funciona como uma simplificação do instrumento anterior, mantendo o objetivo de servir de instrumento para que as palavras do Crip War sejam criptografadas, impedindo o conhecimento da equipe rival a respeito das mesmas.

1. Construção dos materiais;
2. Criptografando uma mensagem;
3. Descriptografando uma mensagem.

5.3.1. Construção dos materiais

O primeiro passo do jogo é a construção dos instrumentos a serem utilizados, e para isso, será necessário que a turma seja dividida em grupos de 3 a 5 alunos, que desponham dos seguintes materiais:

- Um tabuleiro de xadrez, podendo ser substituído por um quadrado de cartolina - que será o instrumento de codificação;
- Uma matriz que será a chave criptografadora (C_r);
- Uma matriz que será a chave descriptografadora (D_r).

Tabuleiro

Inicialmente, o professor deverá solicitar que cada grupo numere as linhas e colunas do tabuleiro de acordo com o número de símbolos pretendidos para criptografar uma mensagem. Sugerimos que sejam consideradas 7 linhas e 7 colunas, possibilitando assim a utilização de todas as letras do alfabeto e alguns símbolos extras. É importante que o número escolhido para colunas e linhas seja o mesmo número primo.

As linhas e colunas devem ser numeradas, de 0 a 6, de maneira ordenada. Assim como no plano cartesiano, as linhas devem crescer da esquerda para a direita e as colunas de baixo para cima, dessa forma cada quadrado do tabuleiro estará associado a um único par ordenado do tipo (x,y), onde x indica a posição horizontal e y a posição vertical, como na figura a seguir.

6	$(0,6)$	$(1,6)$	$(2,6)$	$(3,6)$	$(4,6)$	$(5,6)$	$(6,6)$
5	$(0,5)$	$(1,5)$	$(2,5)$	$(3,5)$	$(4,5)$	$(5,5)$	$(6,5)$
4	$(0,4)$	$(1,4)$	$(2,4)$	$(3,4)$	$(4,4)$	$(5,4)$	$(6,4)$
3	$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$(4,3)$	$(5,3)$	$(6,3)$
2	$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
1	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
0	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$
	0	1	2	3	4	5	6

Tabela 5.4.: Pares ordenados e as casa do tabuleiro.

Feito isso, o professor deve solicitar que os alunos distribuam algumas das letras e símbolos da maneira que acharem adequada. Uma distribuição possível é apresentada na tabela a seguir.

6	β	θ	♡	∞	⋆	♠	♣
5	9	?	!	,	·	...	α
4	2	3	4	5	6	7	8
3	*V*	*W*	*X*	*Y*	*Z*	0	1
2	*O*	*P*	*Q*	*R*	*S*	*T*	*U*
1	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	*A*	*B*	*C*	*D*	*E*	*F*	*G*
	0	1	2	3	4	5	6

Tabela 5.5.: Sugestão de distribuição dos símbolos.

Observe que cada símbolo está associado a um par ordenado (x,y) que tomaremos como uma matriz coluna do tipo $\begin{bmatrix} x \\ y \end{bmatrix}$. A letra M, por exemplo, será representada pela matriz $\begin{bmatrix} 5 \\ 1 \end{bmatrix}$.

Chave Criptografadora

O próximo passo pode ser feito em conjunto com a turma, ou apenas apresentado pelo professor. É necessário que seja construída uma matriz quadrada, de ordem 4, com entradas variando de 0 à 6 cujo determinante não seja múltiplo de 7. Tal matriz será chamada de *matriz chave*. Para ilustrar, vamos utilizar a seguinte matriz:

$$C_r = \begin{bmatrix} 2 & 1 & 2 & 1 \\ 1 & 0 & 2 & 1 \\ 2 & 0 & 1 & 2 \\ 1 & 1 & 0 & 1 \end{bmatrix},$$

a qual atende os requisitos levantados acima: $c_{i,j} \in \{0,1,2,3,4,5,6\}$ e $det\ C_r = 3$.

Chave Descriptografadora

Tal matriz, D_r será obtida através da matriz C_r apresentada anteriormente. Inicialmente, determinamos a matriz adjunta de C_r. Em nosso exemplo, obtemos:

$$adj(C_r) = \begin{bmatrix} 3 & -4 & 2 & -3 \\ 0 & 1 & -2 & 3 \\ 0 & 2 & -1 & 0 \\ -3 & 3 & 0 & 3 \end{bmatrix}.$$

Agora, devemos encontrar um número natural, cujo produto pelo valor de $det\ C_r$ deixe resto 1 quando dividido por 7. Sabemos que $det\ C_r = 3$, Note que $3 \times 5 = 15$, cujo resto na divisão por 7 é 1. Ou seja, $(det\ C_r)^{-1} = 5$. Feito isso, tomamos o produto do número encontrado pela matriz $adj(C_r)$.

$$C_r^{-1} = 15 \cdot adj(C_r) = \begin{bmatrix} 15 & -20 & 10 & -15 \\ 0 & 5 & -10 & 15 \\ 0 & 10 & -5 & 0 \\ -15 & 15 & 0 & 15 \end{bmatrix} = D_r'.$$

Para finalmente encontrarmos a chave descriptografadora, precisamos determinar a matriz D_r, correspondente a D_r', com entradas d_{ij} tais que $0 \leqslant d_{ij} \leqslant 6$. Cada elemento de D_r será o resto obtido na divisão de cada um dos elementos de D_r' por 7. Caso o número seja negativo, somamos, sucessivamente, 7 a ele até que se torne positivo. Durante todo o processo utilizaremos esse fato, caso encontremos alguma matriz com entradas que não variem de 0 à 6. Daí, obtemos a matriz:

$$D_r = \begin{bmatrix} 1 & 1 & 3 & 6 \\ 0 & 5 & 4 & 1 \\ 0 & 3 & 2 & 0 \\ 6 & 1 & 0 & 1 \end{bmatrix}.$$

5.3.2. Criptografando uma mensagem

Para iniciar o processo de criptografar uma mensagem, é necessário agrupar, em duplas, as letras da palavra. Por exemplo, para criptografar a palavra MATRIZ, teremos $MA\ \ TR\ \ IZ$. Caso faltem letras para completar as duplas, devemos repetir a última letra da palavra. Por exemplo, ao agruparmos as letras da palavra LUA, teremos $LU\ \ AA$.

Em seguida, devemos encontrar as matrizes colunas correspondentes a cada agrupamento. As matrizes deverão ser do tipo

$$\begin{bmatrix} x_1 \\ y_1 \\ x_2 \\ y_2 \end{bmatrix},$$

onde (x_1, y_1) e (x_2, y_2) são, respectivamente, as coordenadas da primeira e segunda letra do agrupamento. Feito isso, devemos obter o produto entre a matriz chave e as matrizes correspondentes ao agrupamento das letras. Encontraremos novas matrizes colunas, e ao tomarmos a condição de que suas entradas devem variar de 0 à 6, encontramos seus correspondentes na Tabela 2. Feito isso, temos a palavra inicial criptografada.

Daqui em diante, o processo é análogo ao apresentado na seção anterior, razão pela qual, não descreveremos a parte numérica do mesmo.

Exemplo 5.3.1. *Mensagem original: AMOR*

***Passo 1**: Agrupar as letras e encontrar as matrizes correspondentes*

$$\text{AMOR} \longrightarrow \text{AM} \quad \text{OR} \longrightarrow \begin{bmatrix} 0 \\ 0 \\ 5 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 2 \\ 3 \\ 2 \end{bmatrix}$$

***Passo 2**: Tomamos o produto da matriz C_r, determinada anteriormente, pelas matrizes encontradas no Passo 2.*

***Passo 3**: Devemos encontrar as matrizes com entradas variando de 0 à 6, equivalentes às anteriores, considerando, novamente, o resto da divisão de cada elemento por 7.*

***Passo 4**: Finalmente, para obter a mensagem criptografada, determinamos os símbolos correspondentes às matrizes criptografadas.*
Realizando corretamente os passos anteriores, concluímos que, ao criptografar a palavra AMOR*, obtemos a sequência* 6HK2.

Observação 5.3.1. *Para iniciar o processo de criptografar uma mensagem, é necessário agrupar, de maneira fixa, as letras da palavra. No exemplo em questão, optamos pelo agrupamento em duplas, mas o processo é análogo independente do agrupamento escolhido. Por exemplo, se for escolhido um agrupamento em trios, a palavra MATRIZ nos fornecerá os grupos, $MAT \quad RIZ$. Caso faltem letras para completar os grupos, devemos repetir a última letra da palavra até que cada grupo seja composto pelo mesmo número de letras.*

Apesar da escolha de tal agrupamento ser aleatória, a medida que aumentamos o tamanho do grupo, a ordem das matrizes C_r e D_r também é alterada, aumentando a quantidade

de cálculos envolvidos no processo. Se o agrupamento é feito considerando grupos com n letras, as matrizes C_r e D_r devem ter ordem igual a $2n$. Isto é, ao optarmos por agrupamento em trios, trabalharemos com matrizes de ordem 6. É interessante que esse fato seja discutido com a turma.

5.3.3. Descriptografando uma mensagem

Para descriptografar uma mensagem, devem ser conhecidas a chave descriptografadora (D_r) e a tabela (5.5) utilizada como referência de símbolos. O processo então, se torna análogo ao realizado para criptografar. A seguir, observe tal procedimento explicitado passo a passo, desconsiderando a parte numérica:

Exemplo 5.3.2. *Mensagem original: 6HK2*

***Passo 1**: Tomamos a palavra criptografada em pares e determinamos então as matrizes coluna correspondentes a cada dupla.*

$$6\mathrm{HK2} \longrightarrow 6\mathrm{H} \quad \mathrm{K2} \longrightarrow \begin{bmatrix} 4 \\ 4 \\ 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 3 \\ 1 \\ 0 \\ 4 \end{bmatrix}$$

***Passo 2**: Tomamos o produto de D_r pelas matrizes obtidas no Passo 2.*

***Passo 3**: Encontramos matrizes correspondentes às anteriores, considerando o resto da divisão de cada um dos elementos por 7.*

***Passo 4**: Finalmente, basta encontrar na Tabela 2 os símbolos referentes às matrizes descriptografadas. Daí, encontramos que a sequência simbólica $6\mathrm{HK2}$, que quando descriptografada, corresponde a palavra AMOR.*

6 Conclusão

Existem inúmeros temas para se dissertar na área de criptografia. Tínhamos como objetivos principal, mostrar de maneira simplificada a complexidade do conjunto dos números inteiros. Realizamos também um estudo aprofundando a respeito de matrizes, sendo incluídas demonstrações de alguns fatos que são rotineiramente utilizados em aulas no Ensino Médio sobre esse tema. Abordamos esses dois temas com o objetivo de proporcionar um embasamento teórico mais profundo ao professor de Ensino Básico, o que certamente tornará as aulas relacionadas a esses temas mais claras.

Nesse trabalho, também apresentamos métodos de criptografia clássicos. Demos ênfase à Cifra de Hill, pois os tópicos abordados permitem fundamentar e esclarecer o funcionamento da mesma, uma vez que para a compreensão dessa Cifra é necessário ter conhecimento sobre operações matriciais e sobre congruências módulo um número inteiro. Por fim, propomos uma atividade envolvendo uma adaptação da Cifra de Hill, cujo público alvo são alunos do Ensino Médio. Com tal atividade, pretendemos motivar e estimular o estudo de matrizes, já que muitas vezes o mesmo é feito de forma tradicional, baseando-se na explicação oral do professor, em exemplos e exercícios de fixação. Além disso, almejamos incentivar o professor de matemática ao estudo do tema "criptografia", introduzindo conceitos ligados à ele em sala de aula.

Nossa ideia inicial era desenvolver a atividade proposta em sala de aula, para observar os pontos que funcionaram e àqueles que deveriam ser adaptados. Tal desenvolvimento foi inviável, mas apesar disso, acreditamos que a atividade será funcional, uma vez que sua proposta é estimular a curiosidade e o interesse dos alunos desde o primeiro momento, onde é realizada a construção dos instrumentos de codificação. Para o desenvolvimento da atividade, é necessário conhecimento sobre matrizes, com isso, pretendemos que os alunos se interessem em compreender o necessário sobre o assunto, para que possam realizar os cálculos exigidos no jogo, que incluem determinar a matriz inversa, utilizando o determinante de uma matriz e sua adjunta. Ao apresentarmos a atividade, esperamos que os alunos vejam uma das diversas aplicações de matrizes e com isso deem mais importância ao estudo do assunto.

Em contrapartida, apesar do interesse, acreditamos que a maior dificuldade da realização de tal atividade se dê pelo entendimento dos processos de Criptografar e Descriptografar

uma mensagem, pois são procedimentos com um número considerável de etapas envolvendo contas que podem se tornar grandes, tirando um pouco do interesse inicial. Além disso, é importante enfatizar que tais contas devem ser realizadas com cautela, uma vez que, qualquer erro comprometerá o bom funcionamento da atividade. Outro possível obstáculo, é em relação ao tempo, uma vez que a mesma demanda certa dedicação para a construção dos instrumentos e a realização da mesma pode se alongar mais do que o esperado.

Apesar dos possíveis empecilhos, acreditamos que o trabalho cumpriu com sua proposta inicial, pois, analisando na perspectiva de professor, o mesmo preenche possíveis lacunas referentes à aritmética modular e ao estudo de matrizes. Por outro lado, voltando a análise para o aluno, acreditamos que a atividade proposta estimule a curiosidade, se tornando um produto valioso para o estudo de matrizes e um ponto de partida para o estudo de aritmética modular.

A Determinantes e Permutações

Seja F um corpo. A cada matriz quadrada A com coeficientes em F podemos definir um elemento $a \in F$, o qual chamaremos de *determinante* de A. Neste apêndice, mostraremos uma forma de definir o determinante. Para tal, iremos introduzir alguns conceitos.

Definição A.0.1. $I_n := \{1, \ldots, n\}$.

Definição A.0.2. *Dado um conjunto X finito, toda função bijetora de X nele mesmo será chamada de permutação.*

No caso em que $X = I_n$, podemos representar cada uma das possíveis permutações do seguinte modo:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

onde tal notação nos diz que a permutação π atribui a 1 o valor de $\pi(1)$, a 2 o valor de $\pi(2)$, a 3 o valor de $\pi(3)$ e assim por diante.

Por exemplo, uma permutação de I_6 pode ser representada como:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 2 \end{pmatrix}.$$

Definição A.0.3. *O conjunto de todas as permutações no conjunto I_n é chamado de* Grupo de Permutações[1] *e será representado por S_n.*

Vale ressaltar que a situação acima representa apenas uma possibilidade de permutação dos elementos de I_6. Em geral, o calculo do número de permutações de I_n é um exercício de contagem, no qual obtemos como resposta $n!$, ou seja, para o exemplo acima, basta tomarmos $6!$. Isso significa que são 720 possíveis permutações distintas 2 a 2 que compõe o conjunto S_6.

Podemos ainda representar uma permutação de acordo com a maneira que os elementos do conjunto mudam quando tal permutação é aplicada, como ilustra o exemplo a seguir.

[1] Em realidade tal nome deve-se ao fato desse conjunto munido da operação conjugação ter a estrutura algébrica de um grupo. Para mais detalhes, veja [2, Cap. 7].

Exemplo A.0.1. *Seja* $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$*, podemos representa* π *por (1 4 3 2), significando que a permutação atribui a 1 o valor 4, que recebe o valor 3, que recebe o valor 2, que recebe o valor 1, completando o que chamaremos de ciclo. A escrita de ciclos não é única, o ciclo apresentado pode reescrito, por exemplo, como (2 1 4 3). Além disso, tal ciclo, é dito ciclo de comprimento 4, ou simplesmente um 4-ciclo.*

Observe que um ciclo deve ser encerrado quando o último elemento evidenciado, tiver valor atribuído ao primeiro elemento apresentado. Por conta disso, nem toda permutação é um ciclo. Por exemplo,

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix},$$

uma vez que 1 vai em 4, 4 vai em 3 e 3 vai em 1, deixando de fora 2, 5 e 6.

A seguir um resultado que nos permite sempre relacionar uma permutação com ciclos.

Teorema A.0.1. *Toda permutação é um produto*[2] *finito entre ciclos.*

Demonstração. Veja por exemplo, [2, Teorema 1.1, pág. 129]. □

No exemplo acima, temos

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 2 & 5 \end{pmatrix} = (1\,4\,3)(2\,6\,5),$$

ou seja, tal permutação é o produto de dois ciclos (disjuntos – isto é, não apresentam nenhum valor em comum) de comprimento três.

Quando um ciclo apresentar comprimento dois, iremos chamá-lo de *transposição* e quando for um 1-ciclo, podemos omiti-lo. Por exemplo, a permutação $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ pode ser representada por $(13)(2)$ ou apenas pela transposição (13).

A ordem da escrita entre os ciclos disjuntos que compõe uma permutação é irrelevante, pois é fácil verificar que:

$$(143)(265) = (265)(143),$$

[2] O produto aqui é a a operação usual de composição de funções.

mas o mesmo não se aplica para a ordem dos elementos dentro de um ciclo, ou seja,

$$(143)(265) \neq (134)(265).$$

Teorema A.0.2. *Toda permutação pode ser decomposta como um produto de transposições. Tal decomposição não é única, mas a quantidade de fatores de qualquer decomposição de uma dada permutação tem mesma paridade.*

Para uma prova do Teorema A.0.2, vide [3, Proposição V.10.8, Porposição V.10.10].

Podemos portanto, sempre escrever permutações em produto de transposições. Por exemplo, seja uma permutação de S_7 escrita como $(1532)(67)$, a qual pode ser escrita como $(12)(13)(15)(67)$, portanto, tal permutação é obtida através do produto entre quatro transposições.

Definição A.0.4. *Definimos* $\varepsilon : S_n \to \{-1, 1\}$ *dada por:*

$$\varepsilon(\pi) = \begin{cases} 1, & \text{se } \pi \text{ tiver uma quantidade par de transposições.} \\ -1, & \text{se } \pi \text{ tiver uma quantidade ímpar de transposições.} \end{cases}$$

Note que o Teorema A.0.2 nos garante que a função ε está bem definida e é fácil verificar que:

$$\varepsilon(\pi\alpha) = \varepsilon(\pi)\varepsilon(\alpha) \quad \forall \pi, \alpha \in S_n.$$

Se $\pi \in S_n$ é tal que $\varepsilon(\pi) = 1$ dizemos que π é uma permutação *par*, caso contrário dizemos que π é uma permutação *ímpar*.

Definição A.0.5. *Dada uma matriz* A *de ordem* n*, seu determinante será definido por:*

$$detA = |A| = \sum_{\pi \in S_n} \varepsilon(\pi) a_{1\pi(1)} a_{2\pi(2)} a_{3\pi(3)} ... a_{n\pi(n)}.$$

Temos, portanto, uma parcela para cada possível permutação. Daí, como já citado anteriormente, teremos $n!$ parcelas para o cálculo do determinante de uma matriz de ordem n.

Exemplo A.0.2. *Calcule o determinante da matriz* $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$.

Inicialmente iremos determinar todas as permutações em S_3 *e suas respectivas decomposições em produto de transposições, determinando assim, a sua imagem por* ε*.*

As possíveis permutações serão denotadas por π_m*, com* $1 \leqslant m \leqslant 6$ *e são apresentadas a seguir.*

- $\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
  $\Rightarrow \quad \varepsilon(\pi_1) = 1;$

- $\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3)$
  $\Rightarrow \quad \varepsilon(\pi_2) = -1;$

- $\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)$
  $\Rightarrow \quad \varepsilon(\pi_3) = -1;$

- $\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 3)(1\ 2)$
  $\Rightarrow \quad \varepsilon(\pi_4) = 1;$

- $\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 2)(1\ 3)$
  $\Rightarrow \quad \varepsilon(\pi) = 1;$

- $\pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)$
  $\Rightarrow \quad \varepsilon(\pi_1) = -1.$

Substituindo no somatório, teremos:

$$\begin{aligned} det\,A = & \sum_{m=1}^{6} \varepsilon(\pi_m) a_{1\pi_m(1)} a_{2\pi_m(2)} a_{3\pi_m(3)} \\ = & \ \varepsilon(\pi_1) a_{11}a_{22}a_{33} + \varepsilon(\pi_2) a_{11}a_{23}a_{32} + \varepsilon(\pi_3) a_{12}a_{21}a_{33} \\ & + \varepsilon(\pi_4) a_{12}a_{23}a_{31} + \varepsilon(\pi_5) a_{13}a_{21}a_{32} + \varepsilon(\pi_6) a_{13}a_{22}a_{31} \\ = & \ a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}. \end{aligned}$$

Note que a resposta obtida acima é precisamente a Regra de Sarrus*.*

É fácil perceber que a quantidade de parcelas no cálculo do determinante aumenta consideravelmente à medida que aumentarmos a ordem da matriz A. Porém, como já mencionamos anteriormente, tal método sempre funciona, mas nem sempre é viável – basta observar que calcular um determinante de uma matriz 6×6 nos obriga a obter 720 permutações explicitamente.

A.1. Teorema de Laplace - Demonstração

No *Capítulo 3*, apresentamos o Teorema de Laplace para o cálculo de determinantes de matrizes quadradas de ordem n, com $n \geqslant 4$. Tal método é uma alternativa para o cálculo de determinantes uma vez que o cálculo através da definição se torna trabalhoso, à medida que aumentamos a ordem da matriz.

A seguir, vamos demonstrar o Teorema 3.3.1:

Demonstração do Teorema 3.3.1. Seja A uma matriz quadrada de ordem n com entradas no corpo F e seja também $a_{ij} \in F$ a (i, j)-ésima entrada de A.

Fixando a j-ésima coluna, queremos demonstrar a seguinte expressão:

$$det\ A = a_{1j}cof(a_{1j}) + a_{2j}cof(a_{2j}) + \cdots + a_{nj}cof(a_{nj}). \tag{A.1}$$

Faremos a demonstração para as colunas de uma matriz A, por indução[3] sobre n.

Inicialmente, tomemos o caso inicial, em que A é uma matriz de ordem 2, isto é,

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

Fixando a primeira coluna e aplicando a Definição A.0.5, temos:

$$\begin{aligned} det\ A &= a_{11}a_{22} - a_{21}a_{12} \\ det\ A &= a_{11}cof(a_{11}) + a_{21}cof(a_{21}) \\ &= a_{11}(-1)^{1+1}det\ A_{11} + a_{21}(-1)^{2+1}det\ A_{21}. \end{aligned}$$

E segue que a expressão (A.1) é válida para $n = 2$.

Suponhamos agora, que a expressão (A.1) é valida para toda matriz de ordem $n-1$ e mostraremos que também é verdadeira para uma matriz de ordem n.

Para tanto, iremos desenvolver o lado direito da igualdade (A.1) fixando a k-ésima coluna, a qual denotaremos por D,

$$D := \sum_{i=1}^{n} a_{ik}cof(a_ik) = a_{1k}cof(a_{1k}) + a_{2k}cof(a_{2k}) + \cdots + a_{nk}cof(a_{nk}).$$

A definição de cofator nos permite reescrever D como

$$D = a_{1k}(-1)^{1+k}det\ A_{1k} + a_{2k}(-1)^{2+k}det\ A_{2k} + \cdots + a_{nk}(-1)^{n+k}det\ A_{nk}. \tag{A.2}$$

[3] Para mais detalhes sobre essa técnica consulte, por exemplo, [5, Cap. 2].

Note que as matrizes $A_{1k}, A_{2k}, \cdots, A_{nk}$ são de ordem $n-1$ e portanto, pela hipótese de indução, podemos calcular esses determinantes utilizando a expressão (A.1). Sem perda de generalidade, fixaremos sempre a primeira coluna para o cálculo de cada um dos determinantes.

Observação A.1.1. *Denotaremos por A_{ij}^{kl} a matriz de ordem $n-2$ obtida ao retirarmos as linhas i,k e as colunas j,l de A.*

Denotando $I_n^j = I_n \backslash \{j\} = \{1,\ldots,j-1,j+1,\ldots,n\}$ com $j = 1,\ldots,n$, temos

$$\begin{aligned}
det\ A_{1k} &= a_{21}(-1)^{2+1} det\ A_{1k}^{21} + a_{31}(-1)^{3+1} det\ A_{1k}^{31} + \ldots + a_{n1}(-1)^{n+1} det\ A_{1k}^{n1} \\
&= \sum_{i \in I_n^1} a_{i1}(-1)^{i+1} det A_{1k}^{i1}. \qquad \text{(A.3)} \\
det\ A_{2k} &= a_{11}(-1)^{1+1} det\ A_{2k}^{11} + a_{31}(-1)^{2+1} det\ A_{2k}^{31} + \ldots + a_{n1}(-1)^{n+1} det\ A_{2k}^{n1} \\
&= \sum_{i \in I_n^2} a_{i1}(-1)^{i+1} det\ A_{2k}^{i1}. \qquad \text{(A.4)} \\
&\vdots \\
det\ A_{nk} &= a_{11}(-1)^{1+1} det\ A_{nk}^{11} + a_{21}(-1)^{2+1} det\ A_{nk}^{21} + \ldots + a_{n-1;1}(-1)^{n-1+1} det\ A_{nk}^{n-1;1} \\
&= \sum_{i \in I_n^n} a_{i1}(-1)^{i+1} det\ A_{nk}^{i1}. \qquad \text{(A.5)}
\end{aligned}$$

Substituindo as sentenças (A.3), (A.4) e (A.5) em (A.2), teremos:

$$\begin{aligned}
D = a_{1k}(-1)^{1+k} \left[\sum_{i \in I_n^1} a_{i1}(-1)^{i+1} det A_{1k}^{i1} \right] + a_{2k}(-1)^{2+k} \left[\sum_{i \in I_n^2} a_{i1}(-1)^{i+1} det\ A_{2k}^{i1} \right] \\
+ \ldots\ + a_{nk}(-1)^{n+k} \left[\sum_{i \in I_n^n} a_{i1}(-1)^{i+1} det\ A_{nk}^{i1} \right].
\end{aligned}$$

Em D, agruparemos todas as sentenças em que o termo a_{11} aparece a fim de o colocarmos em evidência, temos:

$$a_{11}(-1)^{1+1} \left[a_{2k}(-1)^{2+k} det A_{2k}^{11} + a_{3k}(-1)^{3+k} det A_{3k}^{11} + \ldots + a_{nk}(-1)^{n+k} det A_{nk}^{11} \right] = a_{11} det A_{11}.$$

Repetindo o processo com as parcelas em que a_{21} aparece:

$$a_{21}(-1)^{2+1} \left[a_{1k}(-1)^{1+k} det A_{1k}^{21} + a_{3k}(-1)^{3+k} det A_{3k}^{21} + \ldots + a_{nk}(-1)^{n+k} det A_{nk}^{21} \right] = -a_{21} det A_{21}.$$

Analogamente, se tomarmos as parcelas nas quais o termo a_{n1} aparece:

$$a_{n1}(-1)^{n+1}\left[a_{1k}(-1)^{1+k}detA^{n1}_{1k}+\ldots+a_{n-1;k}(-1)^{n-1+k}detA^{n1}_{n-1;k}\right]=a_{n1}(-1)^{n+1}det\ A_{n1}.$$

Assim podemos reescrever D como:

$$D=a_{11}(-1)^{1+1}det\ A_{11}+a_{21}(-1)^{2+1}det\ A_{21}+\ldots a_{n1}(-1)^{n+1}det\ A_{n1},$$

ou seja:

$$D=a_{11}cof(a_{11})+a_{21}cof(a_{21})+\ldots+a_{n1}cof(a_{n1}). \tag{A.6}$$

Para finalizar a demonstração, basta mostrarmos que o determinante de A, definido por A.0.5 é expresso pela sentença obtida em (A.6).

Pela definição $A.0.5$, temos:

$$detA=|A|=\sum_{\pi\in S_n}\varepsilon(\pi)a_{1\pi(1)}a_{2\pi(2)}a_{3\pi(3)}...a_{n\pi(n)}.$$

Então, segue que:

$$\begin{aligned}detA=\ & a_{11}\sum_{\pi\in S^1_n}\varepsilon(\pi)a_{2\pi(2)}a_{3\pi(3)}...a_{n\pi(n)}+a_{21}\sum_{\pi\in S^2_n}\varepsilon(\pi)a_{1\pi(1)}a_{3\pi(3)}...a_{n\pi(n)}\\ &+\ \ldots\ +a_{n1}\sum_{\pi\in S^n_n}\varepsilon(\pi)a_{1\pi(1)}a_{2\pi(2)}...a_{n-1\pi(n-1)},\end{aligned}$$

onde S^j_n denota o conjunto das permutações de I^j_n, com $j=1,\ldots,n$.[4]

Note que, por definição, $\sum_{\pi\in S^1_n}a_{2\pi(2)}a_{3\pi(3)}...a_{n\pi(n)}$ representa o determinante da matriz A após serem retiradas a primeira linha e primeira coluna. Daí:

$$\sum_{\pi\in S^1_n}\varepsilon(\pi)a_{2\pi(2)}a_{3\pi(3)}...a_{n\pi(n)}=(-1)^{1+1}det\ A_{11}=cof(a_{11}).$$

Analogamente, $\sum_{\pi\in S^2_n}a_{1\pi(1)}a_{3\pi(3)}...a_{n\pi(n)}$, representa o determinante da matriz A, retiradas a segunda linha e primeira coluna. Isto é:

$$\sum_{\pi\in S^2_n}\varepsilon(\pi)a_{1\pi(1)}a_{3\pi(3)}...a_{n\pi(n)}=(-1)^{2+1}det\ A_{21}=cof(a_{21}).$$

[4] Para maiores detalhes, vide [9].

Assim, indutivamente, podemos concluir que:

$$\sum_{\pi \in S_n^n} \varepsilon(\pi) a_{1\pi(1)} a_{2\pi(2)} \ldots a_{n-1\pi(n-1)} = cof(a_{n1}).$$

E portanto:

$$detA = a_{11}cof(a_{11}) + a_{21}cof(a_{21}) + \ldots + a_{n1}cof(a_{n1})$$

E segue que o Teorema de Laplace é válido para uma matriz quadrada de ordem n, fixando-se a primeira coluna. Uma vez que a escolha da coluna é arbitrária e que $det\ A = det\ A^t$, concluímos a prova do Teorema de Laplace. □

B Algorítmo de Euclides

O Algoritimo de Euclides é um dos métodos mais antigos conhecidos, destacando-se por sua simplicidade e eficácia no cálculo do máximo divisor comum entre dois números inteiros não nulos.

Proposição B.0.1. *Sejam a e b inteiros positivos não nulos, e m um inteiro qualquer. Então $mdc(a,b) = mdc(a,b+am)$ e $mdc(a,b) = mdc(a+bm,b)$.*

Demonstração. Sejam $d = mdc(a,b)$ e $d' = mdc(a,b+am)$.

Por hipótese, $d \mid a$ e $d \mid b$. Como $d \mid a$, podemos concluir que $d \mid am$, o que implica que $d \mid (b+am)$. Como $d' = mdc(a,b+am)$, podemos concluir que $d \mid d'$.

Por outro lado, uma vez que $d' = mdc(a,b+am)$, temos que $d' \mid a$ e $d' \mid (b+am)$. Ou seja, $d' \mid a$, $d' \mid b$ e $d' \mid am$. Por hipótese $d = mdc(a,b)$. Daí, $d' \mid d$, e portanto $d = d'$, isto é, $mdc(a,b) = mdc(a,b+am)$.

De maneira análoga, temos $mdc(a,b) = mdc(a+bm,b)$. □

Observe que as igualdades encontradas acima podem ser escritas como $mdc(a,b) = mdc(a,b-am)$ e $mdc(a,b) = mdc(a-bm,b)$, uma vez que m é um inteiro qualquer.

O Algorítmo de Euclides

Considere dois inteiros, a e b, não nulos. Para determinar o mdc entre a e b, se $a \neq b$, podemos optar pelo método de divisões sucessivas. Sem perda de generalidade, suponhamos que $a > b > 0$.

Pela divisão euclidiana, teremos que:

$$a = b \cdot q_1 + r_1.$$

Do lema anterior, podemos concluir que:

$$mdc(a,b) = mdc(a - b \cdot q_1, b) = mdc(r_1, b) = mdc(b, r_1).$$

Se $r_1 = 0$, teremos o caso trivial, no qual,

$$mdc(a,b) = mdc(b, r_1) = mdc(b, 0) = b.$$

Por outro lado, se $r_1 \neq 0$, efetuamos novamente a divisão euclidiana, obtendo assim:

$$b = r_1 \cdot q_2 + r_2.$$

Usando o mesmo argumento anterior, teremos:

$$mdc(a,b) = mdc(b, r_1) = mdc(b - r_1 \cdot q_2, r_1) = mdc(r_2, r_1) = mdc(r_1, r_2).$$

Novamente, podemos ter $r_2 = 0$ ou $r_2 \neq 0$. Se $r_2 \neq 0$, repetimos o processo e encontramos $mdc(a,b) = mdc(r_2, r_3)$, e assim sucessivamente.

Agora, vamos verificar que o processo iniciado acima termina após um número finito de passos. Note que em cada passo, obtemos um novo resto r_k, para algum $k \in \mathbb{N}$. Seja X o conjunto formado por todos os possíveis tais restos. Primeiro notamos que $r_k \geq 0$ para todo k, pela definição de resto. Como em cada passo, o novo divisor é o resto do passo anterior, temos que:

$$r_k > r_{k+1} \ \forall k \in \mathbb{N}$$

e assim, concluímos que $r_k < r_1$ para todo $k \in K$. Portanto:

$$X \subset I_{r_1} \cup \{0\} \subset \mathbb{Z},$$

com $I_{r_1} = \{1, 2, 3, \ldots, r_1 - 1, r_1\}$. Seja:

$$X' = \{x \in X \mid x \neq 0\}.$$

Assim, como $r_1 \in X'$, temos que $X' \neq \varnothing$, e temos também que X' é limitado inferiormente por 0. Logo, pelo Princípio da Boa Ordenação, X' possui um menor elemento, digamos r_m, ou seja, temos

$$r_m \neq 0 \quad \text{e } r_{m+1} = 0.$$

Mais ainda, note que:

$$X' \subset I_{r_1},$$

o que mostra que tal conjunto é finito.

Daí,

$$mdc(a,b) = mdc(r_m, r_{m+1}) = mdc(r_m, 0) = r_m.$$

Esse resultado nos diz que, o último resto não nulo, r_m, nos fornecerá o $mdc(a,b)$.

Podemos indicar as divisões sucessivas do Algoritimo de Euclides de maneira mais prática, como no diagrama a seguir:

	q_1	q_2	q_3	$\ldots$	q_{m-2}	q_{m-1}	q_m
a	b	r_1	r_2	$\ldots$	r_{m-3}	r_{m-2}	r_{m-1}
r_1	r_2	r_3	r_4	$\ldots$	r_{m-1}	0	

.

Bibliografia

[1] BUENO, H. P.. *Álgebra Linear, um segundo curso*. 1ªed., SBM: Rio de Janeiro, 2006.

[2] BHATTACHARYA, P. B., JAIN, S.K., NAGPAUL,S.R.. *Basic Abstract Algebra*. 2ªed., Cambrigde: New York, 1994.

[3] GARCIA, A. e LEQUAIN, Y.. *Elementos de Álgebra*. 4ªed., IMPA: Rio de Janeiro, 2006.

[4] GONÇALVES, A.. *Introdução à Álgebra*. 4ªed., IMPA: Rio de Janeiro, 2006.

[5] MORGADO, A. C. e CARVALHO, P. C. P.. *Matemática Discreta*. 1ªed., SBM: Rio de Janeiro, 2014.

[6] HEFEZ, A. e FERNANDEZ, C. S.. *Introdução à Álgebra Linear*. 1ªed., SBM: Rio de Janeiro, 2012.

[7] HEFEZ, A.. *Aritmética*. 1ª ed., SBM: Rio de Janeiro, 2014.

[8] SANTOS, R. J.. *Introdução à Álgebra Linear*. 1ªed., Imprensa Universitária da UFMG: Belo Horizonte, 2013.

[9] SÁ, F. L.. *Estudo dos determinantes, Caderno Dá Licença*. v.5, Ano 6, p. 70 - 84., Rio de Janeiro, Dez. 2004.

[10] BRASIL, *Parâmetros Curriculares Nacionais: Matemática*. Secretaria de Educação Fundamental. Brasília : MEC / SEF, 1998.

[11] SINGH, S.. *The Code Book*. v. 1, Delacorte Press: New York, 2002.

[12] COUTINHO, S. C.. *Números inteiros e Criptografia RSA*. 2ª ed., IMPA: Rio de Janeiro, 2014.

[13] SILVA, I. N.. *Criptografia na educação básica: das escritas ocultas ao código RSA*. PROFMAT - PUCRJ: Rio de Janeiro, 2016.

[14] TENANI, G. A.. *Criptografia Clássica, Matrizes e Tecnologia*. PROFMAT - UEM: Maringá, 2016.

[15] MOLINARI, J. R. A.. *Números Primos e a Criptografia RSA*. PROFMAT - UEPG: Ponta Grossa, 2016.

[16] RODRIGUES, M. A.. *Tópicos de criptografia para ensino médio*. PROFMAT - USP: São Carlos, 2016.

[17] SOUZA, L. P.. *Criptografia RSA: A teoria dos números posta em prática*. PROFMAT - UFC: Fortaleza, 2015.

[18] GODINHO, D. da S., CESARIO, G. de L., REIS, N. dos., SARAIVA, R. S.. v.II, nº 2, *Criptografia: A Importância da Álgebra Linear para Decifrá-la* Faculdade Cenecista de Osório (FACOS): Osório, Julho 2011.