Uma adaptação da Cifra de Hill para estudo de matrizes.

Edney Augusto Jesus de Oliveira edney.demat@gmail.com
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil

Mariana Martins Durães Brandão marianamartins431@hotmail.com
Universidade Federal de Ouro Preto, Ouro Preto, MG, Brazil

Resumo

Neste artigo serão apresentados alguns dos principais resultados matemáticos a respeito de Aritmética Modular, dando ênfase às relações de equivalência e classes residuais, além de alguns fatos sobre matrizes em $\mathbb{Z}_p$. Tais temas são abordados com o intuito de fundamentar os processos matemáticos aplicados para funcionamento da Cifra de Hill, que é um modelo de criptografia utilizado como inspiração para o desenvolvimento de uma atividade voltada para turmas de Ensino Médio.

Palavras-chave

Criptografia, Matrizes, Aritmética Modular

1 Introdução

Este presente trabalho é um fruto da dissertação de mestrado intitulada *Uma adaptação da Cifra de Hill para estudo de matrizes* (Veja [1]).

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. 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.

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* [1], 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 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.

2 Aritmética Modular

O campo da *Aritmética Modular*, (ou *Aritmética dos Restos*), 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.

Teorema 2.1 (Algoritmo de Divisão Euclidiana)**.** *Sejam a e m números inteiros, com $m \neq 0$. Então existem dois únicos números, q e r, tais que*

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

Uma demonstração para o teorema acima pode ser obtida em [2, cap. 3]. 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. *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. *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:*

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

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

2.1.1 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:

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

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, 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.

Observação 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, portanto, vamos apresentar um procedimento prático para tal tarefa:*
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:

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

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.*

Lema 2.1. *(Lema de Bézout) Dados* a *e* b *inteiros positivos, existem inteiros* x *e* y *tais que:*

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

Proposição 2.1. *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. □

2.2 Matrizes sobre $\mathbb{Z}_p$

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:

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

Sobre $\mathbb{Z}_p$, trabalhamos com as classes de congruência $\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{p-1}\}$. 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.

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 $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$,

2.2.1 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. 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 $\mathbb{Z}_7$,

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

Proposição 2.2. *A é inversível se, e somente se, $detA \neq 0$.*

Observação 2.2. *Ao trabalharmos sobre $\mathbb{Z}_p$, devemos considerar aqui 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:

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

Observação 2.3. *O inverso multiplicativo, sobre $\mathbb{Z}_p$, do determinante de A é denotado por $(det\ A)^{-1}$ e a matriz inversa da matriz dos cofatores de A, é denotada $adj(A)$.*

Para mais detalhes sobre a matriz adjunta, consulte por exemplo [3, cap. 8]

3 O jogo

O jogo proposto a seguir, baseado no jogo *War*[2], 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

[2] Detalhes do referido jogo em [4]

discutidas além de aspectos operacionais básicos da matemática.

3.1 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.
- Um instrumento de codificação.

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".

3.1.1 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.[3]

Observação 3.1. *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:

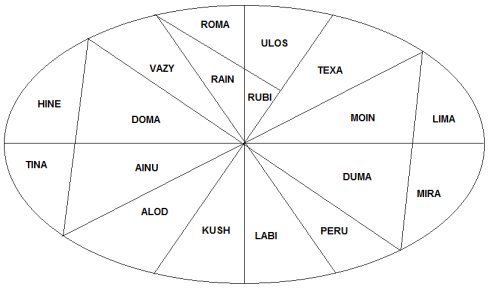
Tabela 1: Modelo de Tabela.

R1		I1	
R2		I2	
R3		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.

[3] Tal chave será apresentada na próxima seção.

Figura 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.

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 3.1.1. 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.

3.1.2 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.

3.1.3 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 2^{o} maior ponto atacante com o 2^{o} 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 3.1.

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:
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

Tabela 2: Lançamento Dados.

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

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.

3.1.4 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.

3.1.5 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.

3.1.6 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.

4 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.

4.1 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).

4.1.1 Cubo

Os materiais utilizados para a construção do cubo, instrumento do processo de codificação foram: 27 palitos de churrasco, 27 bolas de isopor, 27 palitos de dente, 27 bandeirinhas de papel e cola quente.

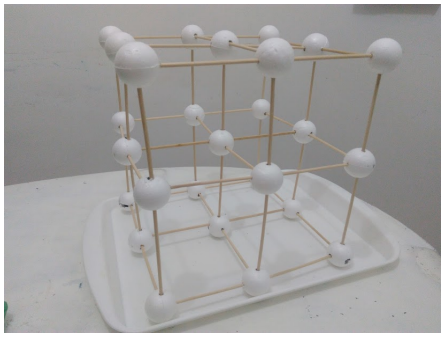


Figura 2: Cubo codificador.

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.

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.

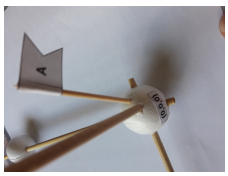


Figura 3: Associação entre símbolos e trincas ordenadas.

Observação 4.1. *As fotografias apresentadas nessa seção são de autoria dos autores do artigo.*

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

Tabela 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 $\begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}$.

4.1.2 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 $det\ C_r = 1$.

4.1.3 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:

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

4.2 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. 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 4.1. *Mensagem original: AMOR*

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

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

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

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

***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.*

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

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

Observação 4.2. *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.*

4.3 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 4.2. *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:*

$$D_r \cdot A = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}; \quad D_r \cdot M = \begin{bmatrix} 3 \\ 1 \\ 4 \end{bmatrix}; \quad D_r \cdot R = \begin{bmatrix} 8 \\ 1 \\ 10 \end{bmatrix}; \quad D_r \cdot Z = \begin{bmatrix} 8 \\ 2 \\ 10 \end{bmatrix}.$$

***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,*

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

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

4.3.1 Instrumento II de Codificação

Uma opção mais simplificada para o instrumento de codificação é a utilização de um tabuleiro de xadrez. As linhas e colunas do tabuleiro devem ser numerada, 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 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.

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 $\begin{bmatrix} 5 \\ 1 \end{bmatrix}$. O restante da atividade é desenvolvido de maneira análoga à utilização do cubo como instrumento de codificação.

6	β	θ	$\heartsuit$	∞	$\star$	$\spadesuit$	$\clubsuit$
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: Sugestão de distribuição dos símbolos.

5 Conclusão

Ao falar sobre criptografia, tínhamos como objetivos principal, mostrar de maneira simplificada um pouco sobre o conjunto dos números inteiros, para proporcionar um maior embasamento teórico ao professor de Ensino Básico.

Nossa ideia inicial era desenvolver a atividade proposta em sala de aula. Tal desenvolvimento foi inviável, porém, 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 assunto, para que possam realizar os cálculos exigidos no jogo.

Em contrapartida, apesar do interesse, acreditamos que a maior dificuldade da realização de tal atividade se dará pelo entendimento dos processos de Criptografar e Descriptografar uma mensagem, pois são procedimentos com sequências 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, analisando na perspectiva de professor, acreditamos que o artigo preenche possíveis lacunas referentes à aritmética modular básica. 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. [**?**]

Referências

[1] Mariana Martins Durães BRANDÃO. Uma adaptação da cifra de hill para estudo de matrizes. Master's thesis, Universidade Federal de Ouro Preto, 2017. Dissertação (mestrado em Matemática).

[2] Abramo HEFEZ. Aritmética. *Rio de Janeiro: SBM*, 2013. (Coleção PROFMAT).

[3] Abramo HEFEZ and Cecília de Souza FERNANDEZ. Introdução à álgebra linear. *Rio de Janeiro: SBM*, 2012. (Coleção PROFMAT).

[4] WAR. São Paulo: Grow, 1972. 1 jogo (1 tabuleiro, 6 conjuntos de peças de cores diferentes, 6 caixas plásticas, 14 cartas especiais , 44 cartas de jogo, 3 dados vermelhos, 3 dados amarelos).