

## Cifra de Hill

Uma aplicação ao estudo de Matrizes

Lucas Diego Antunes Barbosa<sup>1</sup>  
Mariana Garabini Cornelissen Hoyos<sup>2</sup>

**Resumo:** O aprendizado de um conteúdo matemático pode se tornar mais atrativo para o estudante se estiver associado a alguma aplicação. Partindo desse princípio, esse trabalho apresenta aos professores de matemática do ensino médio uma proposta de aplicação do conteúdo de matrizes à uma técnica criptográfica, ou seja, uma técnica para codificar e decodificar mensagens. A técnica escolhida é chamada Cifra de Hill em homenagem ao seu criador, o americano Lester S. Hill, que desenvolveu essa técnica em 1929. Além de mostrar uma aplicação de um conteúdo matemático, esse trabalho também apresenta uma possibilidade de trabalhar a interdisciplinaridade em sala de aula, já que fazemos uso de conhecimentos básicos de programação de computadores, conteúdo essencial para os estudantes no dia de hoje, na proposta de aula aqui apresentada.

**Palavras-chave:** cifra de Hill, criptografia, matrizes.

## 1 Introdução

O mundo em que vivemos está sofrendo várias transformações, mas, alguns aspectos permanecem iguais. Hoje, como no passado, para muitos jovens, aprender matemática na escola é uma experiência difícil e, às vezes, desestimulante, talvez devido à metodologia usada pelo professor, à falta de interesse do aluno ou também pelo alto nível de dificuldade que essa disciplina oferece, já que essa ciência exige uma maior capacidade de abstração por parte dos alunos.

Desde cedo, percebe-se a dificuldade de aprendizagem em diversas disciplinas como física, química, português, mas, no aprendizado da matemática essa dificuldade geralmente é maior. Uma possível explicação para essa situação é a forma com que os professores transmitem o conteúdo. Alguns alunos pensam que a matemática é simplesmente um amontoado de fórmulas e números, e é aí que eles se enganam, pois a matemática é uma ciência, ou melhor, a rainha das ciências, todas as outras ciências dependem da matemática. Quase todos os

---

<sup>1</sup>Aluno de Mestrado Profissional em Matemática, Turma 2013  
Instituição: Universidade Federal de São João del-Rei - Campus Alto Paraopeba - CAP/UFSJ  
E-mail: lucas.barbosa@ifnmg.edu.br

<sup>2</sup>Orientadora do Trabalho de Conclusão de Curso  
Departamento de Física e Matemática - DEFIM, CAP/UFSJ  
E-mail: mariana@ufs.edu.br

fatos decorrentes do dia-a-dia estão associados com a matemática. O aprendizado de um conteúdo matemático pode se tornar mais atrativo para o estudante se estiver associado a alguma aplicação, o que motiva e ajuda a relação ensino-aprendizado. Por isso, sempre que possível, sugere-se que o professor mostre essa aplicação com o objetivo de estimular e facilitar o aprendizado de um determinado conteúdo.

*”Um mundo onde as necessidades sociais, culturais e profissionais ganham novos contornos, todas as áreas requerem alguma competência em Matemática e a possibilidade de compreender conceitos e procedimentos matemáticos é necessária tanto para tirar conclusões e fazer argumentações, quanto para o cidadão agir como consumidor prudente ou tomar decisões em sua vida pessoal e profissional”. (PCN’s, p.40)*

Partindo desse princípio, esse trabalho apresenta aos professores de matemática uma proposta de aplicação do conteúdo de matrizes à uma técnica de criptografia, ou seja, uma técnica para codificar e decodificar mensagens. A técnica escolhida é chamada Cifra de Hill em homenagem ao seu criador, o americano Lester S. Hill, que desenvolveu essa técnica em 1929. Além de matrizes também pode ser explorado com esse método noções de aritmética modular. Dessa forma esse trabalho mostra uma aplicação de um conteúdo matemático, mostrando a possibilidade de trabalhar matrizes, criptografia e programação de computadores em sala de aula, mostrando assim uma possível relação entre teoria e prática matemática. Espera-se que esse trabalho instigue a curiosidade do professor e do aluno na relação de teoria e prática matemática, com o intuito de melhorar a relação de ensino aprendizagem.

## 2 Criptografia

Desde o surgimento da humanidade existe a necessidade de se obter maior segurança na transmissão de informações que são enviadas por diversos meios de comunicação. Em tempos passados de guerra se observou o uso de técnicas especiais para o envio de mensagens secretas para as tropas, como foi o caso de Júlio César, imperador de Roma, quando suas tropas estavam pela Europa em guerra. O imperador deslocava o alfabeto três casas adiante para codificar suas mensagens, como pode ser visualizado pela tabela abaixo.

letra → letra correspondente
A → D
B → E
C → F
D → G
E → H
F → I
e assim por diante

Tabela 1: Cifra de César

Neste caso, se a mensagem a ser enviada fosse: ACABEM COM O INIMIGO, as tropas receberiam a seguinte mensagem cifrada DFDEHPFRPRNQPNLR.

De acordo com a pesquisa realizada por FIARRESGA (2010), o relato mais grotesco de transmissão de mensagens codificadas foi usado por Histieu ao transmitir uma mensagem a Aristágoras de Mileto. Histieu raspou a cabeça de um indivíduo, escreveu no seu couro cabeludo a mensagem que queria enviar, esperou que o cabelo do indivíduo voltasse a crescer e enviou-o em viagem até Aristágoras. O indivíduo quando chegou, raspou novamente a cabeça e mostrou a mensagem à Aristágoras de Mileto.

Essa transmissão de informações de forma oculta é conhecida por criptografia. Portanto, criptografia é a técnica de esconder uma escrita e o seu significado é de origem grega (*kripto* = escondido, oculto e *grápho* = grafia, escrita). Segundo EVARISTO e PERDIGÃO (2002) a criptografia pode ser entendida como a ação de reescrever um texto de modo que apenas as pessoas autorizadas pelo autor do texto sejam capazes de compreendê-lo. O texto normalmente é chamado de mensagem, uma pessoa autorizada a ler a mensagem é chamada destinatário e o autor da mensagem é chamado de remetente. Chamamos de chave criptográfica algo necessário para a codificação ou decodificação da mensagem. Dessa forma, podemos dizer que a criptografia estuda os métodos para codificar uma mensagem de modo que só o seu destinatário legítimo consiga interpreta-la.

Uma vez que a comunicação entre as pessoas é inevitável no atual momento de grande avanço tecnológico, percebemos o quão sério é a transmissão de informações sigilosas. Por exemplo, uma instituição financeira possui informações particulares e importantes de muitas pessoas e tais informações podem ser acessadas caso não haja um sistema de segurança eficaz. Informações secretas como senhas podem ser interceptadas por pessoas inescrupulosas e utilizadas de forma prejudicial aos proprietários, causando grande prejuízo a estes, pois, com a senha de uma conta bancária, podem ser realizados saques e empréstimos em favor de terceiros. Além do prejuízo com contas bancárias, como no exemplo das instituições financeiras, podemos também citar como exemplo a possibilidade de quebra de sigilo de e-mails, tratando-se de informações compartilhadas via internet, caso um sistema criptográfico não seja utilizado. A quebra do sigilo de e-mails pode provocar grandes danos, como a descoberta de endereço, telefone, local de trabalho, o que pode ser perigoso quando dados tão particulares forem parar na mão de pessoas maldosas. Neste sentido, a criptografia assume um importante papel.

Existem dois tipos de criptografia: simétrica e assimétrica. Na criptografia simétrica, a forma de codificar e decodificar uma mensagem é a mesma. Já na criptografia assimétrica a maneira de codificar não é a mesma de decodificar. No caso da criptografia assimétrica, a

chave de codificação é pública e no caso da criptografia simétrica essa chave é privada. São exemplos de métodos criptográficos simétricos: Cifra de César, Data Encryption Standard (DES), Advanced Encryption Standard (AES) e a RSA é exemplo de método assimétrico. Mais adiante, falaremos um pouco sobre cada um desses métodos.

*... Estes códigos foram criados para o uso em aplicações comerciais, e não na comunicação entre espíões. Por isso, os códigos modernos são todos de chave pública. Esta é uma ideia introduzida em 1976 por W. Diffie e M.E. Hellman da Universidade da Califórnia. No código usado por César, se você sabe codificar, então também sabe decodificar. Em um código de chave pública saber codificar não implica saber decodificar! Isto parece impossível: se sei codificar, para decodificar basta desfazer o que fiz. Desfazer o processo de codificação pode não ser tão simples quanto parece. (COUTINHO, 2014, p.3)*

O DES é um método criptográfico que foi designado, pelos Estados Unidos da América, como algoritmo padrão de criptografia em 1977 e foi amplamente utilizado internacionalmente. É um algoritmo de cifra em blocos, isto é, ele transforma um tamanho fixo de texto em um texto cifrado de mesmo tamanho, através de determinadas operações. Atualmente, o DES sozinho é considerado inseguro para muitas aplicações e, em 1997, foi substituído pelo AES, mas, ainda continuou a ser utilizado em larga escala até 2004 com algumas modificações. O AES tornou-se o algoritmo padrão em 2002 e em 2006 já era um dos algoritmos mais populares utilizados para criptografia simétrica. O AES também é um algoritmo de cifra em bloco, porém com um tamanho de chave maior que o DES. Uma descrição detalhada de tais algoritmos pode ser encontrada em [5]. A criptografia RSA foi desenvolvida em 1978 por R. L. Rivest, A. Shamir e L. Adleman (daí o nome RSA), pesquisadores na época do Instituto de Tecnologia de Massachussets. É um método de chave pública cuja codificação baseia-se em um determinado número que é o produto de dois números primos e a decodificação por esse método depende da fatoração desse número, ou seja, dos números primos que o originou. Portanto, sua segurança é garantida com a escolha de um par de números primos grandes. Ao leitor interessado nesse método criptográfico recomenda-se o livro [1]. A cifra de Hill será o assunto de uma próxima seção. Antes, precisaremos revisar alguns conceitos e resultados sobre matrizes e aritmética modular.

### 3 Preliminares

Apresentamos nesta seção algumas definições e resultados sobre matrizes e também sobre aritmética modular que serão necessários para o entendimento do método de Hill. Uma leitura mais detalhada sobre esses conteúdos pode ser encontrada em [13] e [8].

**Definição 3.1** *Seja  $k \in \mathbb{N} - \{0\}$ . Dizemos que dois números inteiros  $a$  e  $b$  são congruentes módulo  $k$  se os restos da divisão euclidiana de  $a$  e  $b$  por  $k$  são iguais. Neste caso, escrevemos  $a \equiv b \pmod{k}$ .*

Pode-se mostrar que  $\equiv$  é uma relação de equivalência em  $\mathbb{Z}$  cuja classe de equivalência módulo  $k$  de  $a \in \mathbb{Z}$  é dada por

$$[a] = \{x \in \mathbb{Z}; x \equiv a \pmod{k}\} = \{x = a + kq | q \in \mathbb{Z}\}$$

Além disso, para cada  $a \in \mathbb{Z}$  existe um e somente um  $r \in \mathbb{Z}, 0 \leq r < k$ , tal que  $[a] = [r]$ . Logo, existem exatamente  $k$  classes de equivalência módulo  $k$  distintas:

$$[0], [1], [2], \dots, [k-1]$$

O conjunto de todas essas classes módulo  $k$  será representado por  $\mathbb{Z}_k$ . O leitor interessado pode consultar esse conteúdo em [2].

**Definição 3.2** Um elemento  $[a] \in \mathbb{Z}_k$  será dito invertível, quando existir  $[b] \in \mathbb{Z}_k$  tal que  $[a][b] = [1]$ . O elemento  $[b] \in \mathbb{Z}_k$  é único (ver demonstração em [12]) e é dito o inverso de  $[a]$ .

**Proposição 3.1**  $[a] \in \mathbb{Z}_k$  é invertível se, e somente se,  $\text{mdc}(a, k) = 1$

**Demonstração:** Suponha que  $[a] \in \mathbb{Z}_k$  é invertível, logo, existe  $[b] \in \mathbb{Z}_k$  tal que:

$$[a].[b] = [1] \Leftrightarrow a.b \equiv 1 \pmod{k} \Leftrightarrow a.b - 1 \equiv 0 \pmod{k}$$

o que implica que existe  $q \in \mathbb{Z}$  tal que  $a.b - 1 = q.k$ . Logo,  $a.b - q.k = 1$  donde  $\text{mdc}(a, k) = 1$ .

Suponha agora que  $\text{mdc}(a, k) = 1$ . Então existem  $q, b \in \mathbb{Z}$  tais que:

$$a.b + q.k = 1.$$

Portanto,  $a.b \equiv 1 \pmod{k}$ , ou seja,  $[a][b] = [1]$ , como queríamos demonstrar. □

Veremos agora como encontrar o inverso de um número em  $\mathbb{Z}_k$ . Suponha  $a \in \mathbb{Z}_k$  invertível e seja  $a^{-1} \in \mathbb{Z}_k$  o seu inverso; então  $\text{mdc}(a, k) = 1$ , o que implica que existem  $b, q \in \mathbb{Z}$  tais que:

$$1 = a.b + k.q$$

donde

$$1 \equiv a.b \pmod{k}$$

Multiplicando os dois membros da igualdade por  $a^{-1}$ , obtemos:

$$a^{-1} \equiv b \pmod{k}$$

Precisamos portanto encontrar  $b$ . Os valores de  $b$  e  $q$  podem ser encontrados utilizando o algoritmo de Euclides, como pode ser visto no exemplo abaixo.

**Exemplo 3.1** Neste exemplo iremos encontrar o inverso de 55 em  $\mathbb{Z}_{26}$ . Como  $\text{mdc}(55, 26) = 1$ , sabemos que 55 é invertível em  $\mathbb{Z}_{26}$  e, além disso, existem  $b, q \in \mathbb{Z}$  tais que

$$55.b + 26.q = 1$$

Para encontrarmos  $b$  que, conforme dito anteriormente, será o inverso de 55 em  $\mathbb{Z}_{26}$ , devemos inicialmente dividir 55 por 26, através da divisão euclidiana, obtendo um quociente e um resto:

$$55 = 26.2 + 3$$

Agora, devemos dividir 26 pelo resto encontrado, no caso 3, e continuar esse processo, ou seja, de dividir o dividendo pelo resto, até encontrarmos resto nulo.

$$26 = 3.8 + 2$$

$$3 = 2.1 + 1$$

$$2 = 1.2 + 0$$

Observe que esse é o processo que utilizamos para determinar o máximo divisor comum (mdc) entre dois números. O último resto não nulo encontrado é o mdc entre 55 e 26. Agora, partindo da última equação cujo resto é não nulo, e utilizando as equações acima, conseguimos encontrar  $b$  e  $q$ . Vejamos:

$$1 = 3 - 2.1$$

Mas, das equações anteriores, temos que  $2 = 26 - 3.8$  e  $3 = 55 - 26.2$ , donde

$$1 = 3 - 2.1 = 3 - (26 - 3.8).1 = 3 - 26.1 + 3.8.1 = 3.9 - 26.1$$

$$1 = (55 - 26.2).9 - 26.1 = 55.9 - 26.2.9 - 26.1 = 55.9 - 26.19$$

donde

$$1 = 55.9 - 26.19$$

o que implica que 9 é o inverso de 55 em  $\mathbb{Z}_{26}$ .

**Definição 3.3** Dada uma matriz quadrada  $A$  de ordem  $n$ , chama-se de inversa de  $A$  à matriz quadrada  $B$  de ordem  $n$  tal que:

$$A.B = B.A = I_n$$

onde  $I_n$  é a matriz identidade de ordem  $n$ . Se uma matriz  $A$  possui inversa, então sua inversa é única (ver demonstração em [13]) e será denotada por  $A^{-1}$ .

**Definição 3.4** Seja  $A = (a_{ij})_{n \times n}$  uma matriz quadrada de ordem  $n$ . O determinante da matriz  $A$ , denotado por  $\det(A)$ , é o número real dado por:

$$\det(A) = \sum_{i=1}^n a_{ij} \cdot (-1)^{i+j} \det(A(i|j))$$

onde  $j$  é qualquer inteiro fixo entre 1 e  $n$  e  $A(i|j)$  é a matriz formada a partir da matriz  $A$  suprimindo sua  $i$ -ésima linha e sua  $j$ -ésima coluna.

Sabemos que uma matriz é invertível se, e somente se, seu determinante é não nulo. Uma demonstração desse fato pode ser encontrada em [7].

**Definição 3.5** *Define-se o cofator do elemento  $a_{ij}$  da matriz  $A$  como*

$$\Delta_{ij}(A) = (-1)^{i+j} \det(A(i|j)).$$

A matriz  $B = (\Delta_{ij}(A))_{n \times n}$  será chamada de matriz dos cofatores da matriz  $A$  e sua transposta será chamada de matriz adjunta de  $A$  e denotada por  $\text{adj}(A)$ .

**Lema 3.1** *Se  $A$  é uma matriz quadrada de ordem  $n$ , então*

$$a_{k1}\Delta_{i1} + a_{k2}\Delta_{i2} + \dots + a_{kn}\Delta_{in} = 0 \text{ se } k \neq i \quad (1)$$

$$a_{1k}\Delta_{1j} + a_{2k}\Delta_{2j} + \dots + a_{nk}\Delta_{nj} = 0 \text{ se } k \neq j \quad (2)$$

para  $i, j = 1, \dots, n$ .

**Demonstração:** Definimos a matriz  $A'$  como sendo a matriz obtida de  $A$  substituindo a  $i$ -ésima linha de  $A$  por sua  $k$ -ésima linha, ou seja,

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_i \\ \vdots \\ A_k \\ \vdots \\ A_n \end{pmatrix} \text{ e } A' = \begin{pmatrix} A_1 \\ \vdots \\ A_k \\ \vdots \\ A_i \\ \vdots \\ A_n \end{pmatrix}$$

Como a matriz  $A'$  possui duas linhas iguais, logo  $\det A' = 0$ . O desenvolvimento do determinante de  $A'$  segundo a  $i$ -ésima linha é exatamente a equação 1. De modo análogo prova-se a equação 2, ainda usando o fato que  $\det(A) = \det(A^t)$  onde  $A^t$  é matriz transposta de  $A$ .  $\square$

**Proposição 3.2** *Seja  $A$  um matriz quadrada de ordem  $n$ . Então:*

$$\text{adj}(A).A = \det(A).I_n$$

**Demonstração:** *O produto da matriz adjunta de  $A$  pela matriz  $A$  é dado por:*

$$\begin{pmatrix} \Delta_{11} & \cdots & \Delta_{n1} \\ \vdots & \vdots & \vdots \\ \Delta_{1i} & \cdots & \Delta_{ni} \\ \vdots & \vdots & \vdots \\ \Delta_{1n} & \cdots & \Delta_{nn} \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \cdots & a_{1j} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \cdots & a_{ij} & \cdots & a_{in} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n1} & \cdots & a_{nj} & \cdots & a_{nn} \end{pmatrix}$$

O elemento da posição  $i, j$  de  $\text{adj}(A).A$  é

$$(\text{adj}(A).A)_{ij} = \sum_{k=1}^n a_{ik}\Delta_{jk} = a_{i1}\Delta_{j1} + a_{i2}\Delta_{j2} + \dots + a_{in}\Delta_{jn}$$

Pelo lema 3.1, equação 2, e pela definição 3.4 temos que:

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

Assim,

$$\text{adj}(A).A = \begin{pmatrix} \det(A) & 0 & \dots & 0 \\ 0 & \det(A) & \dots & 0 \\ \vdots & \dots & \dots & \vdots \\ 0 & 0 & \dots & \det(A) \end{pmatrix} = \det(A).I_n$$

□

**Proposição 3.3** Se  $A$  é uma matriz invertível, então

$$A^{-1} = \frac{1}{\det A} \cdot \text{adj}(A)$$

**Demonstração:** Se  $A$  é invertível então  $\det(A) \neq 0$ . Logo, segue pela proposição 3.2 que

$$\left( \frac{1}{\det(A)} \text{adj}(A) \right) \cdot A = I_n$$

donde  $A^{-1} = \frac{1}{\det(A)} \text{adj}(A)$

□

**Corolário 3.1** Dada uma matriz  $A = (a_{ij})_{n \times n}$ , o determinante da matriz  $A$  será invertível em  $\mathbb{Z}_k$  se o  $\text{mdc}(\det A, k) = 1$ .

A demonstração desse corolário é direta pelo que foi visto na proposição 3.1. Com isso, estamos prontos para entender o método de Hill.

## 4 Cifra de Hill

A cifra de Hill é um método de criptografia inventado pelo americano Lester S. Hill, por volta de 1929. Esse método faz parte da época das cifras com papel e lápis, ele é inseguro contra ataque via computador e pode ser decodificado facilmente. Abaixo, segue um roteiro detalhando passo a passo desse algoritmo de codificação e decodificação, assim como um exemplo.

1. Inicialmente devemos converter as letras da mensagem a ser criptografada em números. Isso pode ser feito de diversas maneiras, dependendo de qual número será associado a cada letra. Aqui neste trabalho, usaremos a tabela ASCII (American Standard Code for Interchange Information) na base decimal para essa conversão, que é a tabela mais utilizada na área computacional. Sem perda de generalidade, podemos trabalhar somente com as letras maiúsculas. No anexo 1 desse trabalho terá a tabela ASCII completa na base decimal, binária e hexadecimal.

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Tabela 2: Alfabeto maiúsculo na base decimal segundo a tabela ASCII

2. Agora devemos agrupar a sequência numérica obtida em vetores coluna de tamanho  $n$  onde  $n$  pode ser qualquer número natural não nulo. Caso o último vetor tenha tamanho menor que  $n$ , repita o último número do vetor até completar o tamanho  $n$ .
3. O terceiro passo é escolher uma matriz  $A = (a_{ij})_{n \times n}$  que será a chave de codificação. O determinante da matriz  $A$  deve ser invertível em  $\mathbb{Z}_k$ , isto é, de acordo com o corolário 3.1, devemos escolher  $A$  de forma que  $\text{mdc}(\det A, k) = 1$ . Aqui  $k$  é o número de símbolos possíveis de acordo com a tabela utilizada. No nosso caso, que estamos trabalhando só com as letras maiúsculas,  $k = 26$ .
4. Em seguida, iniciamos a codificação que consiste simplesmente em multiplicar à esquerda a matriz chave  $A$  por uma matriz  $B$  cujas colunas são formadas pelos vetores coluna do passo 2 com cada entrada subtraída de 65. Deve-se subtrair o número 65, pois assim tem-se a classe residual módulo 26.

$$A.B = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{n1} \\ a_{21} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ b_{21} & \cdots & b_{n2} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix}$$

5. Após efetuar o produto das matrizes, caso alguma entrada da matriz final seja maior ou igual a 26, devemos trocar esse número pelo seu resto na divisão por 26.
6. Finalmente some 65 a cada uma das entradas dessa matriz obtida e transforme seus vetores coluna em letras de acordo com a tabela 2. Essa mensagem formada é a codificação da mensagem original.

Faremos agora um exemplo desse algoritmo de codificação. Como estamos utilizando a tabela 2, só utilizamos as letras maiúsculas sem os espaços e os acentos.

### Exemplo 1

Mensagem original: CIFRADEHILL

C	I	F	R	A	D	E	H	I	L	L
67	73	70	82	65	68	69	72	73	76	76

Passo 1: Conversão da mensagem de acordo com a tabela 2

Passo 2: Agrupando a sequência numérica em vetores coluna de tamanho  $n = 3$  e repetindo o último número do vetor coluna:

$$\begin{pmatrix} 67 \\ 73 \\ 70 \end{pmatrix}, \begin{pmatrix} 82 \\ 65 \\ 68 \end{pmatrix}, \begin{pmatrix} 69 \\ 72 \\ 73 \end{pmatrix}, \begin{pmatrix} 76 \\ 76 \\ 76 \end{pmatrix}$$

Passo 3: Escolha da chave de codificação. Neste caso, uma matriz  $A$  de ordem 3 dada por

$$A = \begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix}$$

Observe que  $\det A = 55$  e  $\text{mdc}(55, 26) = 1$ .

Passo 4: Multiplicando a matriz  $A$  à esquerda pela matriz formada pelos vetores coluna com cada entrada subtraída de 65, obtemos:

$$\begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix} \cdot \begin{pmatrix} 2 & 17 & 4 & 11 \\ 8 & 0 & 7 & 11 \\ 5 & 3 & 8 & 11 \end{pmatrix} = \begin{pmatrix} 64 & 35 & 80 & 121 \\ 33 & 15 & 47 & 66 \\ 38 & 75 & 69 & 110 \end{pmatrix}$$

Passos 5: Agora devemos determinar os restos da divisão euclidiana de cada entrada por 26, obtendo:

$$\begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

Passo 6: E finalmente, somando 65 a cada entrada da matriz anterior, chegamos à matriz abaixo

$$\begin{pmatrix} 77 & 74 & 67 & 82 \\ 72 & 80 & 86 & 79 \\ 77 & 88 & 82 & 71 \end{pmatrix}$$

Fazendo a conversão dos números obtidos em letras de acordo com a tabela 2 concluímos que o destinatário receberá a seguinte mensagem codificada: MHMJPCVRRROG  
Agora, passaremos ao processo de decodificação. Segue abaixo um roteiro detalhando passo a passo o que deve ser feito para decodificar uma mensagem codificada utilizando o processo de Hill.

1. Além da mensagem codificada, o remetente também deve enviar para o destinatário a matriz chave de codificação,  $A = (a_{ij})_{n \times n}$  utilizada. O destinatário ao receber a mensagem codificada precisará converter as letras em números conforme a tabela utilizada pelo remetente, subtrair 65 de cada um desses números e formar uma matriz  $C = (c_{ij})_{n \times m}$ , ou seja, ele deve agrupar a sequência numérica obtida em vetores coluna de tamanho  $n$ .
2. Agora, o destinatário precisa determinar o inverso do determinante da matriz  $A$  em  $\mathbb{Z}_{26}$  e, em seguida, determinar a matriz adjunta de  $A$ .
3. O próximo passo é multiplicar o inverso do determinante em  $\mathbb{Z}_{26}$  e a matriz adjunta de  $A$  encontrados no passo anterior pela matriz  $C$ . Observe que aqui estamos simplesmente fazendo o produto  $A^{-1} \cdot C$ .
4. Em seguida, encontre o resto da divisão euclidiana de cada uma das entradas dessa matriz por 26.
5. E finalmente, some 65 a cada uma das entradas.

Dessa forma, o destinatário descobrirá a mensagem original enviada. Após a apresentação dos processos de codificação e decodificação do método da Cifra de Hill, podemos perceber que, de fato, o método é bastante inseguro, já que através da codificação e por alguns cálculos matemáticos simples, a decodificação é descoberta de forma fácil. Agora, como na codificação, vamos aplicar o algoritmo de decodificação visto acima para recuperar a mensagem do exemplo 1.

## Exemplo 2

Passo 1: Suponha que o destinatário recebeu a matriz chave de ordem 3 e a mensagem abaixo:

MHMJPCVRRROG

$$A = \begin{pmatrix} 1 & 4 & 6 \\ 0 & 1 & 5 \\ 3 & -1 & 8 \end{pmatrix}$$

Tomando como referência a tabela 2, o destinatário pode transformar esse bloco de letras na seguinte matriz:

$$B = \begin{pmatrix} 77 & 74 & 67 & 82 \\ 72 & 80 & 86 & 79 \\ 77 & 88 & 82 & 71 \end{pmatrix}$$

Subtraindo 65 de cada entrada da matriz anterior obtém-se a matriz:

$$C = \begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix}$$

Passo 2 : Como o determinante da matriz chave é 55, precisamos encontrar o inverso de 55 em  $\mathbb{Z}_{26}$ . Pelo exemplo 3.1, temos que o inverso de 55 em  $\mathbb{Z}_{26}$  é 9.

Obtendo a matriz adjunta de A, tem-se a matriz:

$$\text{adj}(A) = \begin{pmatrix} 13 & -38 & 14 \\ 15 & -10 & -5 \\ -3 & 13 & 1 \end{pmatrix}$$

Passo 3: O próximo passo agora é multiplicar  $9 \cdot \text{adj}(A) \cdot C$ :

$$\begin{aligned} & 9 \cdot \begin{pmatrix} 13 & -38 & 14 \\ 15 & -10 & -5 \\ -3 & 13 & 1 \end{pmatrix} \cdot \begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 117 & -342 & 126 \\ 135 & -90 & -45 \\ -27 & 117 & 9 \end{pmatrix} \cdot \begin{pmatrix} 12 & 9 & 2 & 17 \\ 7 & 15 & 21 & 14 \\ 12 & 23 & 17 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 522 & -1179 & -4806 & -2043 \\ 450 & -1170 & -2385 & 765 \\ 603 & 1719 & 2556 & 1233 \end{pmatrix} \end{aligned}$$

Passo 4: Em seguida, encontre o resto da divisão euclidiana de cada uma das entradas dessa matriz por 26

$$= \begin{pmatrix} 2 & 17 & 4 & 11 \\ 8 & 0 & 7 & 11 \\ 5 & 3 & 8 & 11 \end{pmatrix}$$

Passo 5: Somando 65 a cada entrada da matriz acima e consultando a tabela 2, obtém-se a mensagem codificada.

$$\begin{aligned} &= \begin{pmatrix} 67 & 82 & 69 & 76 \\ 73 & 65 & 72 & 76 \\ 70 & 68 & 73 & 76 \end{pmatrix} \\ &= \begin{pmatrix} C & R & E & L \\ I & A & H & L \\ F & D & I & L \end{pmatrix} \end{aligned}$$

Portanto o destinatário encontrará a seguinte mensagem original: CIFRADEHILLL

## 5 Proposta de Aula

Essa proposta de aula pode ser aplicada no ensino médio, curso técnico em Informática, no curso de licenciatura em matemática ou em qualquer outro curso em que são ministrados os conteúdos de matrizes e programação de computadores. A proposta tem os seguintes objetivos:

- Despertar o interesse dos alunos para o aprendizado da matemática.
- Associar teoria e prática matemática.
- Desenvolver a interdisciplinaridade.
- Aprender a trabalhar em equipe.
- Mostrar aplicações de conteúdos matemáticos no dia-a-dia.

A proposta consiste em pedir aos alunos que construam um algoritmo para codificar e decodificar mensagens através do método de Hill. Inicialmente o professor de matemática deve desenvolver com esses alunos os seguintes conteúdos matemáticos: matrizes, determinante, MDC e noções de aritmética modular. Em seguida, será explicado para os alunos o histórico da criptografia e o método aplicável em sala de aula, a cifra de Hill. Após o ensino dos conteúdos teóricos necessários, o professor pedirá que os alunos formem grupos de 5 membros e construam um algoritmo, em qualquer linguagem de programação, para codificar e decodificar uma mensagem utilizando o método de Hill. Essa proposta de aula deve ser aplicada com o auxílio do laboratório de informática e, preferencialmente, com a participação dos professores de informática da escola.

Segue abaixo um cronograma com o tempo estimado de aula e o conteúdo a ser trabalhado. O tempo de uso do laboratório de informática fica a critério do professor envolvido com essa proposta de aula.

Tempo estimado	Conteúdo
4h/a	Divisão euclidiana, MDC, noções de aritmética modular.
1h/a	Números inversíveis em $\mathbb{Z}_k$ .
1h/a	Matrizes: exemplos e operações.
4h/a	Determinante e Matriz Inversa.
3h/a	Criptografia e Cifra de Hill.

Tabela 3: Cronograma

## 6 Aplicação e resultados

Nos meses de outubro e novembro de 2014, essa proposta de aula foi aplicada para os alunos do 3º ano do curso técnico em informática do ensino integrado do Instituto Federal do Norte de Minas Gerais-IFNMG/Campus: Arinos. No primeiro momento, os alunos tomaram um susto quando ouviram as palavras algoritmo e programação dentro de um trabalho de matemática. Eles haviam estudado a disciplina de programação no 1º ano, ou seja, há dois anos atrás.

Apesar disso, muitos alunos mostraram um grande interesse em participar do trabalho, já que cada integrante do grupo seria contemplado com 10 pontos dos 35 pontos distribuídos naquela etapa.

O primeiro passo foi explicar os conteúdos teóricos necessários. Noções de aritmética modular e números inversíveis foram novidade para os alunos, pois os mesmos nunca tinham visto esses temas. Os alunos mostraram grande dificuldade em efetuar divisões usando o algoritmo de divisão euclidiana. Uma situação que pode justificar essa dificuldade, é o fato dos alunos estarem acostumados a efetuar operações básicas de matemática em aparelhos eletrônicos. No conteúdo matrizes e determinantes, os alunos não tiveram muita dificuldade, pois muitos deles já tinham estudado o conteúdo no 2º ano do curso. Quando foram citados os métodos de criptografia existentes e a importância da criptografia no contexto atual, foi o momento que os alunos mais prestaram atenção na aula, pois naquele momento eles estavam estudando conteúdos matemáticos associados à uma aplicação. Nesse momento percebe-se a importância de mostrar conteúdos matemáticos associados com fatos decorrentes do dia-a-dia.

O segundo passo foi dividir a turma em grupos de 5 membros, aleatoriamente, para que os alunos pudessem ter interação entre eles. Em seguida, foi agendado o laboratório de informática para que os alunos pudessem todos os dias após as aulas regulares, se reunirem e confeccionarem o trabalho proposto. Os alunos mostraram grande dificuldade em traduzir as expressões matemáticas para a linguagem em que o seu algoritmo estava sendo construído. Nesse momento, a presença do professor de matemática é fundamental. As dificuldades de programação que iam surgindo eram encaminhadas aos professores de informática, que participaram desses encontros que os alunos realizaram durante uma semana no laboratório.

O terceiro passo, após terem criado o algoritmo de codificação pela cifra de Hill, foi apresentar o trabalho em sala de aula. Os alunos criaram uma interface, entregaram os códigos dos trabalhos feitos na linguagem C++ e PHP, e ainda hospedaram o mesmo no servidor. Segue o link de um dos trabalhos apresentados: <http://www.criptexmatrix.esy.es>. Ao final da apresentação dos trabalhos, alguns alunos julgaram o algoritmo como trabalhoso, mas afirmaram que puderam lembrar códigos de programação e ainda aprenderam matemática.

Neste trabalho, os alunos utilizaram a tabela 4 abaixo, dos caracteres minúsculos (ao invés dos maiúsculos como fizemos na seção anterior) para fazerem a conversão das letras em números e ainda limitaram o tamanho da mensagem para apenas 9 caracteres.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 4: Alfabeto minúsculo

## 7 Considerações Finais

Existem vários tópicos da matemática que podem ser trabalhados com aplicações como o que foi proposto acima. Isso ajudaria a responder a pergunta clássica de uma aula de matemática: "Para que isso servirá em minha vida?". O algoritmo construído pelos alunos teve um aspecto positivo, pois, contribuiu para o desenvolvimento dos alunos no estudo de matrizes e

na programação, auxiliando o aprendizado dessas disciplinas. Esse trabalho não esgotará o estudo sobre aplicações na matemática, espera-se que a partir dele possam surgir novas ideias para associar a teoria à prática em sala de aula, podendo assim melhorar o aprendizado em matemática.

## 8 Agradecimentos

Agradeço à minha família, amigos e alunos pelas palavras de apoio e incentivo. Também sou grato à equipe de professores do DEFIM/CAP-UFSJ que acreditaram no programa PROFMAT, em especial à coordenadora Professora Dra. Mariana Garabini Cornelissen Hoyos pela competência e paciência. Aos companheiros do PROFMAT-2013/2015, que sempre foram dispostos a ajudar quando surgiam as dificuldades. Agradeço ainda a CAPES pelo apoio financeiro.

## Referências

- [1] COUTINHO, S.C.: *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, 2014.
- [2] DOMINGUES, Higino H.; IEZZI, Gelson.: *Álgebra Moderna*. São Paulo: Atual, 2003.
- [3] LIMA, Elon Lages.: *Álgebra linear*. Rio de Janeiro: SBM, 2003.
- [4] EVARISTO, Jaime; PERDIGÃO, Eduardo.: *Introdução à Álgebra Abstrata*. Maceió: EDUFAL, 2002.
- [5] FALEIROS, Antônio Cândido.: *Criptografia*. São Carlos-SP: SBMAC, 2011.
- [6] FIARRESGA, Victor Manuel Calhabrês.: *CRIPTOGRAFIA E MATEMÁTICA*. (Dissertação do Mestrado em Matemática para Professores). Departamento de Matemática, Universidade Federal de Lisboa, 2010. Disponível em: <http://repositorio.ul.pt>. Acessado: 10/01/2015.
- [7] HEFEZ, Abramo; FERNANDEZ, Cecília de Souza.: *Introdução à Álgebra Linear*. Rio de Janeiro: SBM, 2012.
- [8] HEFEZ, Abramo.: *Aritmética*. Rio de Janeiro: SBM, 2013.
- [9] BRASIL, Ministério da Educação, Secretaria de Educação Média e Tecnológica.: *Parâmetros Curriculares Nacionais: ensino médio*. Brasília: 1999.
- [10] RIBENBOIM, Paulo.: *Números Primos: Velhos Mistérios e Novos Recordes*. Rio de Janeiro: IMPA, 2012.
- [11] SANTOS, Reginaldo J.: *Introdução a Álgebra Linear*. Departamento de Matemática-ICEX. Universidade Federal de Minas Gerais, 2010.
- [12] SHOKRANIAN, Salahoddin.: *Uma introdução à Teoria dos números*. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

- [13] SEYMOUR, Lipschutz.: *Álgebra Linear: teorema e problemas*. São Paulo: Pearson Makron Books, 1994.- (Coleção Schaum)

# Anexo 1

Binário	Decimal	Hexa	Glifo	Binário	Decimal	Hexa	Glifo	Binário	Decimal	Hexa	Glifo
0010 0000	32	20		0100 0000	64	40	@	0110 0000	96	60	`
0010 0001	33	21	!	0100 0001	65	41	A	0110 0001	97	61	a
0010 0010	34	22	"	0100 0010	66	42	B	0110 0010	98	62	b
0010 0011	35	23	#	0100 0011	67	43	C	0110 0011	99	63	c
0010 0100	36	24	\$	0100 0100	68	44	D	0110 0100	100	64	d
0010 0101	37	25	%	0100 0101	69	45	E	0110 0101	101	65	e
0010 0110	38	26	&	0100 0110	70	46	F	0110 0110	102	66	f
0010 0111	39	27	'	0100 0111	71	47	G	0110 0111	103	67	g
0010 1000	40	28	(	0100 1000	72	48	H	0110 1000	104	68	h
0010 1001	41	29	)	0100 1001	73	49	I	0110 1001	105	69	i
0010 1010	42	2A	*	0100 1010	74	4A	J	0110 1010	106	6A	j
0010 1011	43	2B	+	0100 1011	75	4B	K	0110 1011	107	6B	k
0010 1100	44	2C	,	0100 1100	76	4C	L	0110 1100	108	6C	l
0010 1101	45	2D	-	0100 1101	77	4D	M	0110 1101	109	6D	m
0010 1110	46	2E	.	0100 1110	78	4E	N	0110 1110	110	6E	n
0010 1111	47	2F	/	0100 1111	79	4F	O	0110 1111	111	6F	o
0011 0000	48	30	0	0101 0000	80	50	P	0111 0000	112	70	p
0011 0001	49	31	1	0101 0001	81	51	Q	0111 0001	113	71	q
0011 0010	50	32	2	0101 0010	82	52	R	0111 0010	114	72	r
0011 0011	51	33	3	0101 0011	83	53	S	0111 0011	115	73	s
0011 0100	52	34	4	0101 0100	84	54	T	0111 0100	116	74	t
0011 0101	53	35	5	0101 0101	85	55	U	0111 0101	117	75	u
0011 0110	54	36	6	0101 0110	86	56	V	0111 0110	118	76	v
0011 0111	55	37	7	0101 0111	87	57	W	0111 0111	119	77	w
0011 1000	56	38	8	0101 1000	88	58	X	0111 1000	120	78	x
0011 1001	57	39	9	0101 1001	89	59	Y	0111 1001	121	79	y
0011 1010	58	3A	:	0101 1010	90	5A	Z	0111 1010	122	7A	z
0011 1011	59	3B	;	0101 1011	91	5B	[	0111 1011	123	7B	{
0011 1100	60	3C	<	0101 1100	92	5C	\	0111 1100	124	7C	
0011 1101	61	3D	=	0101 1101	93	5D	]	0111 1101	125	7D	}
0011 1110	62	3E	>	0101 1110	94	5E	^	0111 1110	126	7E	~
0011 1111	63	3F	?	0101 1111	95	5F	_				

Figura 1: Tabela ASCII completa