CRIPTOGRAFIA NO ENSINO MÉDIO: UMA PROPOSTA DE ATIVIDADE

Marcos Coutinho Mota
IF Sudeste MG – Câmpus Rio Pomba
marcoscm16@yahoo.com.br

Rafael Cazal Silva
IF Sudeste MG – Câmpus Rio Pomba
faelcazal@yahoo.com.br

Marcos Pavani de Carvalho
IF Sudeste MG – Câmpus Rio Pomba
marcos.pavani@ifsudestemg.edu.br

Resumo:
Este trabalho apresenta uma proposta de atividade para o ensino de matrizes envolvendo Criptografia na disciplina de Matemática do Ensino Médio. A escolha deste tema se deve pela sua importância no estudo da Matemática da Educação Básica e, de forma geral, pela dificuldade encontrada pelos alunos em seu entendimento e sua necessidade, importância e contribuição em estudos posteriores. No mundo em que vivemos, onde utilizamos diariamente senhas para inúmeras coisas, julgamos que a abordagem da Criptografia no ensino de matrizes pode ser muito bem recebido e motivador aos alunos. Como proposta de trabalho, sugerimos a utilização da Criptografia objetivando uma melhor fixação dos conceitos. Assim, esperamos promover uma reflexão nos futuros professores de Matemática para que estes criem condições para uma melhoria na aprendizagem dos alunos, preparando-os e tornando mais amplo o aprendizado dos conteúdos tentando assim, criar condições para que eles possam se aprofundar em estudos envolvendo esse assunto.

Palavras-chave: Ensino Médio; Matrizes; Criptografia.

1. Introdução

Este trabalho apresenta uma proposta de atividade voltada para o ensino de matrizes envolvendo Criptografia na disciplina de Matemática do Ensino Médio.

A escolha deste tema se deve pela sua importância no estudo da Matemática e, de uma forma geral, pela dificuldade encontrada pelos alunos no decorrer do Ensino Médio no seu entendimento e sua necessidade, importância e contribuição em estudos posteriores. Outro motivo que levou à escolha deste tema é o fato de se poder utilizar a Criptografia aplicando-se conceitos e operações com matrizes ao se trabalhar com mensagens criptografadas.

2. Objetivo

Propor uma atividade a uma turma de terceiro ano do Ensino Médio da rede pública da Zona da Mata Mineira que utilize o recurso da Criptografia e que promova uma maior habilidade com operações envolvendo matrizes, estimulando o interesse dos alunos, bem como levá-los a uma melhor fixação destes conceitos, visto que estes, ao cursarem o terceiro ano do Ensino Médio, já estudaram sobre matrizes no decorrer de sua vida acadêmica.

Propõe-se que esta atividade seja aplicada de forma que os alunos sejam divididos em grupos e que sejam utilizadas metodologias de ensino distintas para que se possa comparar o desenvolvimento dos mesmos conforme a metodologia empregada.

Assim, esta atividade poderá contribuir significativamente para os discentes possibilitando estudos posteriores envolvendo matrizes.

3. Referencial Teórico

No decorrer do Ensino Médio, geralmente todas as definições e propriedades de matrizes apresentadas são fortemente ligadas à técnica, ficando o aluno impossibilitado de perceber como poderia aplicar este conhecimento adquirido.

Segundo Carraher (1986 apud MENEZES e CARVALHO, 2010),

> os problemas de Matemática, em que o aluno tem que utilizar precisamente as fórmulas que acabou de estudar, não são verdadeiros problemas que exijam reflexão, mas sim, exercícios que exigem apenas memória; não lhe é exigida compreensão dos conceitos matemáticos, nem que faça relações entre o que já aprendeu e a possível solução do problema. Nesses casos, os problemas são tratados mecanicamente, sem que, muitas vezes, o aluno compreenda o que está fazendo. Esta abordagem não funciona para estimular o raciocínio do aluno. (CARRAHER, 1986 apud MENEZES e CARVALHO, 2010, p. 3).

Motivados pela citação acima e objetivando uma maior reflexão e compreensão dos conceitos pelos alunos envolvendo matrizes, acreditamos que a utilização da Criptografia como um recurso didático possa contribuir ativamente no processo de ensino e aprendizagem de parte da disciplina de Matemática integrante da matriz curricular do Ensino Médio.

Buscando uma definição e aplicação para a Criptografia, deparamo-nos com a direta e simples frase de Terada (1988). Segundo este autor, a "Criptografia consiste em codificar informações, usando-se uma chave, antes que estas sejam transmitidas, e em decodificá-las, após a recepção". No mundo em que vivemos, onde utilizamos diariamente senhas para muitas coisas, julgamos assim, que a abordagem da Criptografia no ensino de matrizes pode ser muito bem recebido e motivador aos alunos.

Para Silva (2008 apud MENEZES e CARVALHO, 2010),

> A criptografia é tão antiga quanta a própria escrita, já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos utilizavam códigos secretos para comunicar planos de batalhas. O mais interessante é que a tecnologia de Criptografia não mudou muito até meados deste século. Depois da Segunda Guerra Mundial, com a invenção do computador, a área realmente floresceu incorporando complexos algoritmos matemáticos. Durante a guerra, os ingleses ficaram conhecidos por seus esforços para decifração de mensagens. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna. (SILVA, 2008 apud MENEZES e CARVALHO, 2010, p. 2).

Assim, a importância da Criptografia na sociedade e seu contexto histórico tornam-se também fatores motivadores para que os alunos se interessem pela sua utilização, em especial, trabalhando com matrizes.

Segundo Oliveira e Kripka (2011),

> Acredita-se que a inclusão de atividades que envolvam conceitos de criptografia pode ajudar a diminuir a existência de aulas mecânicas, onde o professor, através de atividades práticas, poderá mostrar a aplicabilidade dos conceitos trabalhados em sala de aula, relacionando-os a fatos importantes ocorridos na atualidade. (OLIVEIRA e KRIPKA, 2011, p. 11).

Nestas perspectivas, pretende-se utilizar a Criptografia como recurso no ensino de matrizes em uma turma de terceiro ano do Ensino Médio, objetivando uma melhor fixação dos conceitos e, consequentemente, criando condições para uma melhoria na aprendizagem.

4. Proposta de Trabalho

Para a aplicação da atividade, serão necessários uma sala de aula com carteiras e quadro branco, pincéis, apagador, projetor multimídia, notebook e folha de atividades. No final da atividade será aplicado um questionário objetivando um levantamento qualitativo e quantitativo das opiniões dos alunos sobre a atividade realizada.

A atividade será realizada em uma turma de terceiro ano do Ensino Médio.

Incialmente será aplicada uma avaliação diagnóstica com todos os alunos sobre conceitos de operações de matrizes tais como adição e multiplicação de matrizes, multiplicação de matriz por escalar e obtenção de uma matriz inversa.

Em seguida, serão ministradas duas aulas expositivas de cinquenta minutos cada de nivelamento sobre os tópicos matriciais supramencionados. Logo após, a turma será dividida em dois grupos, nos quais serão empregadas as seguintes metodologias: No grupo 1, em mais duas aulas, serão aplicadas algumas atividades envolvendo as operações de matrizes, as quais serão recolhidas após o tempo estabelecido, para análises posteriores das articulações dos

alunos perante as atividades propostas. Isto é, neste grupo será empregada uma metodologia de ensino tradicional.

Segundo Mizukami, (1986 apud TEODORO, 2008),

> na abordagem tradicional o professor em relação ao aluno ocupa uma posição vertical, aqui o mestre ocupa o centro de todo o processo educativo, cumprindo objetivos selecionados pela escola e pela sociedade. O professor comanda todas as ações da sala de aula e sua postura está intimamente ligada à transmissão de conteúdos. Ao aluno, neste contexto, era reservado o direito de aprender sem qualquer questionamento, através da repetição e automatização de forma racional. (MIZUKAMI, 1986 apud TEODORO, 2008, p. 8).

Esta metodologia ainda prevalece, segundo Dullius et al, (2011), pois,

> Discute-se e observa-se o quanto é importante o uso de diferentes metodologias de ensino, mas a educação tradicional ainda apresenta uma certa resistência quanto à utilização de novas técnicas de ensino. (DULLIUS et al, 2011, p. 1).

Assim,

> A modernização do ensino da Matemática terá de ser feita não só quanto a programas, mas também quanto a métodos de ensino. O professor deve abandonar, tanto quanto possível, o método expositivo tradicional, em que o papel dos alunos é quase cem por cento passivo, e procurar, pelo contrário, seguir o método activo, estabelecendo diálogo com os alunos e estimulando a imaginação destes, de modo a conduzi-los, sempre que possível, à redescoberta. (PÓLYA, 1945 apud PONTE, 2002, p. 6).

Seguindo esta proposta, no segundo grupo inicialmente será aplicado um minicurso sobre a Criptografia, no qual serão abordados os seguintes tópicos: Introdução, Tipos e Aplicação da Criptografia. Segundo a literatura, há vários tipos de Criptografia: Bastão de Licurgo – Scytale, Código de César, Tabela Esparta, Cifra de Vigenere, a Grelha de Cardano e Cifra de Hill. Mas para aplicação do minicurso, focaremos neste último tipo, devido ao fato de se utilizar matrizes e, em especial, matrizes inversas. Neste processo, associa-se inicialmente a cada letra do alfabeto, a alguns sinais de pontuação e a alguns números, um número correspondente, conforme a representação no quadro abaixo:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Q	R	S	T	U	V	W	X	Y	Z	Á	É	1	2	3	.	!
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33

Logo após, divide-se o texto em blocos de tamanho *n*, que são considerados vetores de *n* dimensões. Escolhe-se uma matriz quadrada e inversível, isto é, com determinante não

nulo, de ordem *n* para servir de chave. A matriz chave é então multiplicada pelos vetores, um de cada vez, resultando nos chamados *vetores encriptados*. Por exemplo, vamos codificar a mensagem *XI ENEM* tendo como chave a matriz

$$A = \begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix}.$$

Consultando a tabela, temos os seguintes blocos de vetores para a mensagem selecionada:

24 9 0 5 14 5 13

Assim, como a matriz é de ordem 2, o texto será dividido em blocos de dimensão 2. Então, efetuando-se os produtos matriciais, temos:

$$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 24 \\ 9 \end{bmatrix} = \begin{bmatrix} 105 \\ 81 \end{bmatrix};$$

$$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 5 \end{bmatrix} = \begin{bmatrix} 5 \\ 5 \end{bmatrix};$$

$$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 5 \end{bmatrix} = \begin{bmatrix} 61 \\ 47 \end{bmatrix};$$

$$\begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 13 \\ 0 \end{bmatrix} = \begin{bmatrix} 52 \\ 39 \end{bmatrix}.$$

Observe que o acréscimo do 0 (zero) na última igualdade se justifica pelo fato de que este número representa apenas um espaço, isto é, não altera a mensagem e possibilita o cálculo do produto matricial.

Logo, obtemos os seguintes *vetores encriptados*:

105 81 5 5 61 47 52 39

Para descriptar a mensagem basta calcular a matriz inversa de *A* e multiplicá-la pelos *vetores encriptados*. Efetuando os cálculos necessários, encontramos:

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

Desta forma, multiplicando a matriz inversa A^{-1} pelos *vetores encriptados*, divididos em blocos de dimensão 2, temos:

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 105 \\ 81 \end{bmatrix} = \begin{bmatrix} 24 \\ 9 \end{bmatrix};$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 5 \\ 5 \end{bmatrix} = \begin{bmatrix} 0 \\ 5 \end{bmatrix};$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 61 \\ 47 \end{bmatrix} = \begin{bmatrix} 14 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 1 & -1 \\ -3 & 4 \end{bmatrix} \cdot \begin{bmatrix} 52 \\ 39 \end{bmatrix} = \begin{bmatrix} 13 \\ 0 \end{bmatrix}.$$

E obtemos os seguintes vetores: 24 9 0 5 14 5 13 0, que de acordo com o quadro significa: XI ENEM.

Assim, serão propostas atividades experimentais mostrando a Matemática de uma forma interessante e que possibilite ao aluno aplicar o conhecimento adquirido.

Para tanto, serão distribuídas duas mensagens, sendo uma *normal* e outra codificada, onde os grupos deverão codificar e descodificar as mensagens, usando a Cifra de Hill, conforme foi explicado no exemplo acima. Posteriormente será aplicada uma atividade de fixação dos conceitos vistos no minicurso. Prevemos que o trabalho com o grupo 2 tenha duração mínima de duas aulas.

Finalizando, será aplicada ao grupo 2 a mesma atividade aplicada para o grupo 1, objetivando uma comparação entre o desempenho dos mesmos de acordo com a metodologia empregada, após as análise da folhas de atividades. Pretende-se realizar toda a atividade proposta e utilizando as metodologias mencionadas em um período de seis aulas.

5. Resultados Esperados

Devido à dificuldade encontrada pelos alunos no decorrer do Ensino Médio com os conceitos de matrizes, e sabendo de sua necessidade e importância, espera-se com a atividade proposta e descrita neste trabalho, preparar e tornar mais amplo o aprendizado destes conteúdos, criando condições para que os mesmos possam se aprofundar em estudos posteriores envolvendo estes importantes conceitos da Matemática.

Para tanto, sugere-se que a escolha da chave seja uma matriz cuja respectiva inversa possua como elementos números inteiros, para que os alunos não se confundam nos cálculos com números fracionários. Além disso, as mensagens devem ser preferencialmente curtas e é indicado a utilização de matrizes de ordem 2 como chaves para que os cálculos não se tornem árduos, especialmente, no cálculo da matriz inversa.

Por fim, indica-se aos futuros professores de Matemática da Educação Básica que estes reflitam sobre sua futura prática pedagógica para que, quando estiverem em exercício docente, sempre busquem metodologias alternativas de ensino e, consequentemente,

contribuam em uma sólida formação dos conceitos matemáticos dos estudantes do Ensino Médio.

6. Referências

DULLIUS, M. M. et al. **Metodologias para o Ensino de Ciências Exatas**. 2011. p. 8. Disponível em: <www.projetos.unijui.edu.br/matematica/cnem/cnem/principal/re/PDF/RE12.pdf>. Acesso em: 12 mar. 2013.

MENEZES, L. A.; CARVALHO, M. P. Criptografia na Sala de Aula. In: **X Encontro Nacional de Educação Matemática**. 2010, Salvador - Bahia. Anais do X Encontro Nacional de Educação Matemática. Sociedade Brasileira de Educação Matemática. Ilheus, Bahia: Via Litterarum, 2010.

OLIVEIRA, D.; KRIPKA, R. M. L. **O Uso da Criptografia no Ensino de Matemática**. 2011. Disponível em: <www.cimm.ucr.ac.cr/ocs/index.php/xiii_ciaem/xiii_ciaem/paper/viewFile/1817/630>. Acesso em: 12/11/12.

PONTE, J. P. **O ensino da matemática em Portugal:** Uma prioridade educativa? 2002. Disponível em: <*www.educ.fc.ul.pt/docentes/jponte/docs-pt/02-Ponte(cne).pdf* >. Acesso em: 12 mar. 2013.

TEODORO, N. M. **Metodologia de ensino:** Uma contribuição pedagógica para o processo de aprendizagem da diferenciação. 2008. p. 6. Disponível em: <*www.diaadiaeducacao.pr.gov.br/portals/pde/arquivos/2234-8.pdf* >. Acesso em: 12 mar. 2013.

TERADA, R. **Criptografia e a Importância de suas Aplicações**. Revista do Professor de Matemática 12. SBM: 1988.