UFRRJ

INSTITUTO DE CIÊNCIAS EXATAS

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

DISSERTAÇÃO

CRIPTOGRAFIA: COMO PRESERVAR SUAS INFORMAÇÕES UTILIZANDO OS CONCEITOS BÁSICOS DE MATRIZES

Fábio Santos Celestino

2017

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

CRIPTOGRAFIA: COMO PRESERVAR SUAS INFORMAÇÕES UTILIZANDO OS CONCEITOS BÁSICOS DE MATRIZES

FÁBIO SANTOS CELESTINO

Sob a Orientação do Professor
Pedro Carlos Pereira

Dissertação submetida como requisito parcial como obtenção do grau de **Mestre**, no Curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, Área de Concentração em Matemática.

Seropédica, RJ

Agosto de 2017

Universidade Federal Rural do Rio de Janeiro
Biblioteca Central / Seção de Processamento Técnico

Ficha catalográfica elaborada
com os dados fornecidos pelo(a) autor(a)

C392c

Celestino, Fábio Santos, 1981-
Criptografia: como preservar suas informações utilizando os conceitos básicos de Matrizes / Fábio Santos Celestino. - 2017.
66 f.: il.

Orientador: Pedro Carlos Pereira.
Dissertação(Mestrado). -- Universidade Federal Rural do Rio de Janeiro, Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional PROFMAT, 2017.

1. Criptografia. 2. Matrizes. I. Pereira, Pedro Carlos, 1959-, orient. II Universidade Federal Rural do Rio de Janeiro. Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional PROFMAT III. Título.

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
CURSO DE PÓS-GRADUAÇÃO EM MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

FÁBIO SANTOS CELESTINO

Dissertação submetida como requisito parcial para obtenção do grau de **Mestre**, no curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, área de Concentração em Matemática.

DISSERTAÇÃO APROVADA EM 31/08/2017

_____
Pedro Carlos Pereira. Dr. UFRRJ
(Orientador)

_____
Orlando dos Santos Pereira. Dr. UFRRJ

_____
Gabriela dos Santos Barbosa. Dr.ª UERJ

AGRADECIMENTOS

Agradeço primeiramente a Deus por estar sempre ao meu lado, pela oportunidade de cursar este Mestrado.

À minha esposa por sempre incentivar meu crescimento profissional, que soube entender todos os momentos em que tive que me dedicar ao Mestrado.

A CAPES por financiar meus custos mensais para as aulas do PROFMAT, bem como os estudos para pesquisa.

Ao meu orientador Pedro pela dedicação, por cada conselho durante a pesquisa para esse trabalho.

Aos amigos da turma 2015 do PROFMAT, valeu galera pelo apoio nos momentos de dificuldade e pelas conversas descontraídas para aliviar a tensão das avaliações do curso.

Resumo

Nós professores, principalmente os de Matemática, somos o tempo todo questionados pelos alunos sobre “o porquê” e “para quê” estudamos determinado conteúdo. Perguntas estas que incomodam a maioria dos professores. A partir de uma interrogação durante uma das minhas aulas sobre Criptografia, é que passamos discutir em nossa pesquisa como relacionar os conceitos de Matrizes com os conceitos de Criptografia e como podem ser aplicados nos dias atuais. Podemos constatar que é um conceito que aparece frequentemente no dia-a-dia, por meio de filmes, séries, aplicativo de celular, e etc., ou seja, procuramos mostrar em nossa pesquisa que a Criptografia não é um conceito exclusivo dos filmes de espião, e sim algo ao alcance de todos.

Palavras-chave: Criptografia, Matrizes, Formação de Professores, Ensino de Matemática

Abstract

Summary teachers mainly Mathematics, we are all the time questioned from and to certain content. y the students about “the why” of the teachers from a questions these annoy most question during one of my classes about what we spend discussing in our how to relate the concepts of Matrices with the concepts of Criptography and how they can be applied in the present day. We can see that it is a concept that appears frequently in the day to Day, through movies, series, we try to show in our research that Cryptography is not a concept exclusive to spy films, but something within the reach of all.

Keywords: Cryptography, Matrices, Teacher Training, Mathematics Teaching

SUMÁRIO

1 Introdução

Ao longo dos anos, o homem sempre se preocupou com métodos exclusivos para enviar mensagens onde somente o destinatário seria capaz de revelar, ou seja, ocultar o real sentido das informações. No sentido de atender a essa necessidade, é que surgiu o estudo da Criptografia, que nada mais é que criar meios para que uma mensagem seja codificada/decodificada e a informação seja mantida em sigilo. Procuramos em nosso trabalho apresentar a Criptografia aos alunos do 3º ano do Ensino Médio, de uma escola pública, do município de Nova Iguaçu, Rio de Janeiro, que ela é um conceito comum no nosso dia-a-dia e que é possível elaborar um método de codificar mensagens, e que um desses métodos é através dos conceitos de Matrizes.

Em sala de aula e nos livros didáticos, o ensino de Matrizes sempre parte do modelo genérico da sua formação e de comparar matrizes com algumas situações diárias, como por exemplo: batalha naval, lotação de teatro, palavras cruzadas e etc. No momento em que nos livros se discute os tipos de matrizes (matriz linha, matriz coluna, matriz quadrada, inversa e transposta) e suas operações (adição, subtração multiplicação por um número e multiplicação entre matrizes) não há uma apresentação com relação aos fatos do nosso cotidiano. O mesmo ocorre com a apresentação dos conceitos sobre Determinante e Sistemas de Equações Lineares, bem como as suas respectivas propriedades. Tal fato nos deixa a impressão que após vários dias de aula falando sobre Matrizes, tudo se resume apenas em resolver Sistemas de Equações pelo método de Regra de Cramer, enquanto em nenhum momento no 2º ano do Ensino Médio se menciona a resolução de um Sistema pelo método do Escalonamento. Já no 3º ano, apresentamos aplicações de Matrizes nas aulas de Geometria Analítica, como por exemplo, em determinar a equação da reta e o valor da área de um triângulo. É do conhecimento de todos que no Curso de Matemática, seja Licenciatura ou Bacharel, nos é apresentado o conceito sobre Modelagem Matemática, onde podemos obter a resolução de algumas situações problemas utilizando os conceitos de Sistemas de Equações. Então, deixo aqui um questionamento: Por que no ensino de Matrizes no Ensino Médio, os autores dos livros didáticos não fazem essas aplicações?

É possível observar em filmes, séries e em programas de variedades, diversos comentários sobre criptografia e códigos de segurança de alguns sistemas computacionais de empresas, bancos e instituições. Ao analisarmos os livros didáticos de Matemática, somente o livro de Matemática, volume 2, 2º ano do Ensino Médio, no qual o autor Dante inicia o Capítulo de Matrizes falando sobre Criptografia e de forma superficial, retomando no final com mais uma aplicação, também sem nenhuma conexão com o conteúdo, deixando parecer como uma obrigação. Foi a partir dessas observações que procuramos em nossa pesquisa apresentar propostas de atividades envolvendo conceitos de Criptografia relacionado com o de Matrizes. Tais atividades foram aplicadas em sala de aula, em turmas do 3º ano do Ensino Médio.

No primeiro capítulo do nosso trabalho, apresentamos como a Aprendizagem Significativa pode contribuir para o ensino-aprendizagem da Matemática. Em seguida, no capítulo 2, fazemos um breve histórico do conceito de Matrizes e Determinantes. Já no terceiro capítulo discorremos sobre Criptografia e no quarto capítulo comentamos sobre Matrizes e Criptografia nos Livros Didáticos. Dando prosseguimento em nosso trabalho, apresentamos no 5º Capítulo a Criptografia na Sala de Aula, onde desenvolvemos cinco atividades em turmas do 3º ano do Ensino Médio. Para finalizar a pesquisa, expomos nossas conclusões e algumas sugestões para os professores.

2 A APRENDIZAGEM SIGNIFICATIVA E A MODELAGEM MATEMÁTICA E SUAS CONTRIBUIÇÕES PARA O ENSINO DA MATEMÁTICA

O psiquiatra norte-americano, David Paul Ausubel (1918-2008), destinou, aproximadamente, vinte e cinco anos de seus estudos à psicologia aplicada à educação. Durante todos esses anos Ausubel desenvolveu os seus estudos, denominado de “Teoria de Aprendizagem Significativa”, baseando-se no conhecimento a priori que os discentes possuem para que haja uma nova aprendizagem de conceitos, isto é, para que essas novas informações tenham significado e faça sentido para eles.

Segundo MOREIRA (2006, p.38): (...) “a aprendizagem significativa é o processo por meio do qual novas informações adquirem significado por interação (não associação) com aspectos relevantes preexistentes na estrutura cognitiva”. No momento que o aluno recebe uma nova informação ele deve incluí-la em algum conhecimento já existente, conhecimento este que Ausubel denomina de âncora, ou subsunçor, ou seja, o aluno deve relacionar a nova informação com as preexistentes em sua estrutura cognitiva. Essa estrutura é a parte fundamental para explicar a Aprendizagem Significativa.

Ela é, por hipótese, uma estrutura hierarquicamente organizada a partir dos termos conceituais mais importantes e menos diferenciados, isto é, ela é criada por uma diferenciação progressiva dos conceitos de maior para os de menor valor inclusivo. É importante ressaltar que a Aprendizagem Significativa se caracteriza pela interação entre conhecimentos prévios e conhecimentos novos. Nesse processo, os novos conhecimentos adquirem significado e sentido para o aluno e os conhecimentos prévios adquirem novos significados ou maior estabilidade cognitiva. De acordo com Antunes (2012, p.94), “atualmente, destaca-se que, ao construir um conceito, a pessoa não o memoriza, apenas transforma esse conceito em instrumento de ação para elaborar conexões mais elevadas e, dessa forma, resolver problemas”. Portanto, a ocorrência da aprendizagem significativa implica que as seguintes condições sejam satisfeitas:

- intenção do aluno para aprender significativamente, isto é, disposição de relacionar o novo material à sua estrutura cognitiva;
- disponibilidade de elementos relevantes na sua estrutura cognitiva com os quais o material a ser aprendido possa relacionar-se;

- que o material a ser aprendido seja potencialmente significativo para ele

e seja relacionável de um modo não arbitrário aos elementos relevantes da sua estrutura cognitiva.

Baseado nos estudos de Ausubel, quando a aprendizagem não é realizada o aluno de forma significativa, ele acaba utilizando a aprendizagem de forma mecânica. Este tipo de aprendizagem é a que o aluno “decora” os conteúdos para realizar suas tarefas e avaliações. Essas informações não tiveram nenhum significado para ele e elas são armazenadas de forma isolada, esquecidas e apagadas após um pequeno período de tempo. A aprendizagem mecanizada é a mais utilizada na maioria das escolas, é a que leva alunos, pais e educadores a acreditarem que o ensino se concretizou. Pois, esses alunos são capazes de decorar os conteúdos que lhe são apresentados em sala de aula e reproduzirem nas avaliações de forma eficaz e muitos deles acabam sendo promovidos sem terem aprendido realmente o conteúdo.

Ressaltamos que os dois tipos de aprendizagem citadas não são contrárias ou excludentes, elas podem fazer parte de um mesmo processo contínuo de ensino e aprendizagem de acordo com o momento e os devidos critérios. Outro fato que não podemos deixar de chamar a atenção, é que a Aprendizagem Significativa não é aquela que o aluno nunca esquece, já que esquecimento faz parte normal do funcionamento cognitivo. Se este tipo de aprendizagem realmente ocorre num determinado período, o processo de reaprendizagem é possível e relativamente rápida. O desafio que se estabelece para os educadores é despertar motivos para que a aprendizagem ocorra de maneira significativa, tornando as aulas mais interessantes de modo que os conteúdos possam ser compartilhados com outras experiências vivenciadas pelos alunos. Além disso, os professores devem atuar como pesquisadores da sua própria prática pedagógica e o aluno deverá ser tratado como sujeito que receberá o conhecimento e não como mero receptor de informações.

Essas ações devem ser constante em sala de aula e a todo o momento faz-se necessário que ao aluno seja apresentado alternativas para que o ensino da Matemática deixe de ser aplicado com o chamado método tradicional, onde a criatividade é sempre deixada de lado. Neste caso, as soluções das questões e as demonstrações são apresentadas aos alunos de tal modo que não passem por tentativas de novos caminhos. Assim sendo a Matemática acaba se constituindo

como um conjunto de técnicas aplicadas aos alunos de forma mecânica e acrítica, como um conhecimento pronto e acabado. No cenário brasileiro, a partir da década de 1970, destaca-se a Modelagem Matemática como um dos métodos de ensino que pode criar condições para o desenvolvimento de uma proposta interdisciplinar, constituiu-se inicialmente como um método de pesquisa. Já na década de 1980, na Universidade Estadual de Campinas – UNICAMP, um grupo de professores, em Biomatemática, coordenado pelo Professor Rodney Carlos Bassanezi, realizou estudos com Modelagem Matemática envolvendo crescimento de células cancerígenas. Porém o avanço significativo deu-se em 1983, na Faculdade de Filosofia Ciências e Letras de Guarapuava – FAFIG, hoje Universidade Estadual do Centro-Oeste – UNICENTRO, com os cursos de especialização para professores. Muitas vezes nós buscamos resolver situações da nossa realidade utilizando representações, ou seja, modelando ou utilizando modelos já definidos. Percebemos que o processo de modelagem está presente nas nossas vidas desde a nossa origem como ser humano. A noção de modelo se faz presente em todas as áreas e se constitui um conjunto simplificado de símbolos ou características criadas para representar aproximadamente uma determinada situação do mundo real de interesse do pesquisador. Essas representações podem aparecer de diversas formas: gráficos, leis matemáticas, desenhos, esquemas, etc, inclusive podemos citar o modelo criptográfico. “O modelo é o ponto de ligação entre as informações captadas pelo indivíduo e a sua ação sobre a realidade; situa-se no nível do indivíduo e é criado por ele como um instrumento de auxílio à compreensão da realidade através da reflexão”. (D'AMBRÓSIO, 1986, p.49). Modelagem é um ambiente de aprendizagem no qual os alunos são instigados a questionar situações oriundas de outras áreas de conhecimento utilizando como meio investigativo a Matemática. Um modelo matemático nada mais é do que uma representação aproximada na linguagem matemática de um fenômeno a um princípio não matemático; é a tradução de um fenômeno do mundo físico em uma equação ou sistemas de equações. Deve permitir fazer previsões, tomar decisões, explicar e entender o fenômeno a ser modelado. A modelagem matemática é um processo dinâmico utilizado para a obtenção e validação de modelos matemáticos. É uma forma de abstração e generalização com a finalidade de previsão de tendências. A modelagem consiste, essencialmente, na arte de transformar

situações da realidade em problemas matemáticos cujas soluções devem ser interpretadas na linguagem usual. (BASSANEZI, 2004, p. 24).

Pelo nosso olhar, o ambiente de Modelagem está associado à problematização e investigação. O primeiro refere-se ao ato de criar perguntas ou problemas, enquanto que, o segundo à busca, seleção, organização e manipulação de informações e reflexão sobre elas. Ambas as atividades não são separadas, mas articuladas no processo de envolvimento dos alunos para abordar a atividade proposta. Nela, podem-se levantar questões e realizar investigações que atingem o âmbito do conhecimento reflexivo. O trabalho que estamos propondo, que é o estudo da Criptografia, pode levar o aluno em uma situação problema, criar seu próprio código de mensagem, ou seja, uma linguagem idiossincrática, onde só o remetente e o destinatário conhecem o processo de codificação e decodificação.

Para que o aluno seja proativo, o professor deverá ser atuante, criativo, dinâmico, disposto a atuar como mediador na transição do conhecimento do senso comum para um conhecimento científico matemático, caminhando lado a lado com o aluno durante todo processo de construção do conceito a ser apresentado, visando fazer com que o ambiente de aprendizagem seja o mais agradável a todos os envolvidos. É importante que ele conheça as etapas da modelagem para que possa definir os responsáveis pelas atividades e adequar a sua aplicação à realidade da turma, considerando aspectos como: conhecimentos prévios dos alunos, conteúdo programático a ser desenvolvido, objetivos conceituais, atitudes, habilidades e o tempo para a aplicação de cada tarefa. Os resultados encontrados podem surpreender tanto o aluno quanto o professor, cabendo a este último a função de direcionar o estudo para que sejam atingidos os objetivos propostos e aí sim teremos atingido a Aprendizagem Significativa.

A primeira etapa do nosso trabalho nos remete a escolha do tema. É onde deve-se instigar o aluno a tratar de um tema presente no seu dia a dia, levando-o a coletar dados e informações. Na segunda parte levamos o aluno a interação com o tema, ou seja, é o momento em que propiciamos o aluno a formular e desenvolver problemas com os conteúdos curriculares pertinentes ao tema, Matrizes e Criptografia. A última, é a fase da representação, que é a formulação do problema e elaboração do modelo matemático, visando validar o modelo encontrado.

Com a Modelagem Matemática e Aprendizagem Significativa, o processo de ensino & aprendizagem não mais se dá no sentido único do professor para o aluno,

mas como resultado da interação do aluno com o seu ambiente natural. Segundo os Parâmetros Curriculares Nacionais do Ensino Médio (PCNEM - BRASIL, 1999), a Modelagem Matemática, na perspectiva da interdisciplinaridade, também contempla as competências sugeridas na medida em que permite identificar e relacionar os dados, interpretar informações relevantes em uma dada situação-problema, sendo apresentados em diferentes linguagens e representações. A passagem do modelo tradicional de ensino para os modelos propostos que visam o desenvolvimento do pensamento crítico do aluno não é algo tão simples assim, ela envolverá o abandono de posturas preestabelecidas e a consequente adoção de novas atitudes por parte de todos os envolvidos nesse processo. Logo, o objetivo de nosso trabalho é mostrar como a criptografia pode ser uma das aplicações dos conceitos de matrizes. Sendo assim, devemos ter claro de como introduzir a criptografia em sala de aula e, de como relacionar matrizes com codificação e decodificação de mensagens. Para atingir nossos objetivos, faremos uso da Modelagem Matemática e da Aprendizagem Significativa como parte metodológica aplicada no desenvolvimento das atividades propostas aos alunos em sala de aula.

3 MATRIZ E DETERMINANTE: NOÇÕES BÁSICAS

3.1 Um Pouco de História

Historicamente temos indícios de que os chineses resolveram alguns problemas cujos cálculos eram feitos em formas de tabelas. Em 1826, Augustin-Louis Cauchy (1789-1857) nomeou essas representações numéricas de tableau (tabela, em francês), e no ano de 1850, James Joseph Sylvester (1814-1897) chamou essa representação de matriz, nome utilizado até os dias atuais. Já em 1858, Arthur Cayley (1821-1895) ficou famoso quando demonstrou as aplicações das Matrizes em sua obra intitulada *Memoir on the Theory of Matrizes*. As aplicações eram basicamente para resolução de sistemas lineares, mas em 1790 Joseph Louis Lagrange (1736-1813) apresenta o primeiro uso da noção de matrizes. Ele utilizou matrizes para o estudo de máximos e mínimos de funções reais de várias variáveis.

Atualmente as Matrizes ganharam tamanha importância que não conseguimos imaginar a ideia do desenvolvimento dos computadores, das engenharias civil, elétrica e mecânica, meteorologia, oceanografia e outras inúmeras áreas sem o estudo das Matrizes.

3.2 Definição

Uma matriz é um conjunto de *m* linhas e *n* colunas de elementos numéricos organizadas em um retângulo. Em outras palavras, é uma tabela de informações codificadas em números.

Seja a matriz dada abaixo:

$$A_{mxn} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}$$

Os elementos da matriz A podem ser representados de maneira generalizada como $A_{mxn} = (a_{ij})$, onde *m* e *n* é a ordem da matriz entre linhas e colunas, respectivamente, *i* o número da linha e *j* o número da coluna do elemento dentro da

matriz. Assim, se quisermos o elemento da 4ª linha e 2º coluna, o escrevemos assim: $A_{mxn} = (a_{42})$

3.2.1 Tipos de Matrizes

- Quando n = 1, temos uma matriz chamada matriz coluna. Por exemplo:

$A_{3x1} = \begin{bmatrix} 5 \\ 0 \\ 3 \end{bmatrix}$, $B_{2x1} = \begin{bmatrix} 1 \\ -8 \end{bmatrix}$.

- Quando m = 1, temos uma matriz chamada matriz linha. Por exemplo:

$A_{1x2} = [10 \quad -5]$, $B_{1x3} = [2 \quad 6 \quad 0]$.

- Quando m = n, temos uma matriz chamada matriz quadrada. Por exemplo:

$A_{2x2} = \begin{bmatrix} 7 & 1 \\ -2 & 4 \end{bmatrix}$, $B_{3x3} = \begin{bmatrix} 2 & 3 & 4 \\ 0 & 5 & 7 \\ 1 & -2 & -3 \end{bmatrix}$.

Em uma matriz quadrada temos a diagonal principal que é representada pelos elementos cujo i =j, ou seja, $\{aij| \ i = j\} = \{a_{11}, a_{22}, a_{33}, ..., a_{nn}\}$

- Quando os elementos de diagonal principal de uma matriz quadrada são iguais a 1 e os demais iguais a zero, temos uma matriz chamada matriz identidade. Por exemplo:

$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

3.2.2 Operações com matrizes

i. Adição e Subtração

A (mxn) + B (mxn) = C (mxn)

Exemplo: Dadas as matrizes, $A = \begin{bmatrix} 2 & 4 \\ -2 & 5 \\ -4 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 3 & 1 \\ 1 & 0 \\ 10 & 2 \end{bmatrix}$ e $C = \begin{bmatrix} 5 & -4 \\ 0 & 3 \\ 1 & 1 \end{bmatrix}$, determine:

a) $A + B = \begin{bmatrix} 2 & 4 \\ -2 & 5 \\ -4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 1 \\ 1 & 0 \\ 10 & 2 \end{bmatrix} = \begin{bmatrix} 2+3 & 4+1 \\ -2+1 & 5+0 \\ -4+10 & 0+2 \end{bmatrix} = \begin{bmatrix} 5 & 5 \\ -1 & 5 \\ 6 & 2 \end{bmatrix}$

b) $C - A = \begin{bmatrix} 2 & 4 \\ -2 & 5 \\ -4 & 0 \end{bmatrix} - \begin{bmatrix} 5 & -4 \\ 0 & 3 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2-5 & 4-(-4) \\ -2-0 & 5-3 \\ -4-1 & 0-1 \end{bmatrix} = \begin{bmatrix} -3 & 8 \\ -2 & 2 \\ -5 & -1 \end{bmatrix}$

ii. Multiplicação de um número real por matriz

A (mxn) x B (nxp) = C (mxp)

Sejam as matrizes A_{mxn} e B_{nxp}, o produto da matriz A pela matriz B, é calculado multiplicando ordenadamente os elementos da linha da matriz A pelos elementos da coluna da matriz B, e somando-se os produtos obtidos. Note que, só podemos efetuar uma multiplicação de matrizes quando o número de colunas de A for igual ao número de linhas de B e que a matriz resultante de AB terá a dimensão igual a mxp.

Exemplo: Dados $A = \begin{bmatrix} 3 & 2 \\ 5 & 0 \\ -1 & 4 \end{bmatrix}$ e $B = \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix}$, determine AB.

Como a matriz A é 3x2 e a matriz B é 2x2, o número de colunas de A é igual ao número de linhas de B, logo AB existe e o produto será 3x2.

$$AB = \begin{bmatrix} 3 & 2 \\ 5 & 0 \\ -1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & 4 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 3 \bullet 2 + 2 \bullet 3 & 5 \bullet 2 + 0 \bullet 3 & (-1) \bullet 2 + 4 \bullet 3 \\ 3 \bullet 4 + 2 \bullet 1 & 5 \bullet 4 + 0 \bullet 1 & (-1) \bullet 4 + 4 \bullet 1 \end{bmatrix} = \begin{bmatrix} 12 & 10 & 10 \\ 14 & 20 & 0 \end{bmatrix}$$

3.3 Determinante

O estudo do Determinante data por volta do século 111a.C. Mas, somente em 1683, Takakazu Seki Kowa (1642-1708) utilizou a ideia de determinante na resolução de seus trabalhos envolvendo sistemas lineares. Dez anos depois, Gottfried Wilhelm Leibiniz (1646-1716) mostrou um trabalho envolvendo determinante na resolução de sistemas lineares. Em 1764, Étienne Bezout (1730-1783) estabeleceu o processo dos sinais dos termos do determinante. Mas a primeira abordagem da teoria dos determinantes foi com Alexandre Théophile Vandermonde (1735-1796). Em 1812, Cauchy apresentou um sobre o termo determinante, maneira essa utilizada até os dias atuais, mas a forma mais simples de apresentarmos os conceitos de determinante devem-se a Carl Gustav Jacob Jacobi(1804-1851).

3.3.1 Cálculo do Determinante

A. Matriz de ordem 2

Seja A = $\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, denotamos determinante de A da seguinte maneira: det(A) = $a_{11} \bullet a_{22} - a_{21} \bullet a_{12}$.

Exemplo: Seja A = $\begin{bmatrix} 5 & 6 \\ 2 & 7 \end{bmatrix}$, logo det(A) = 5•7 – 2•6 = 25

B. Matriz de ordem 3

Seja A = $\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$, utilizaremos a regra de Sarrus para calcular o determinante de A, fazendo o seguinte processo:

- Repetimos as duas primeiras colunas à direita de A, e efetuamos multiplicações em diagonal:

$$\left[\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{array}\right]$$

- Os produtos obtidos na direção da diagonal principal permanecem com o mesmo sinal;

- Os produtos obtidos na direção da diagonal secundária mudaram o sinal

- O determinante é a soma desses valores obtidos.

Logo, det (A) = a_{11}•a_{22}•a_{33} + a_{12}•a_{23}•a_{31} + a_{13}•a_{21}•a_{32} – a_{12}•a_{21}•a_{33} – a_{11}•a_{23}•a_{32} – a_{13}•a_{22}•a_{31}

Exemplo: Seja A = $\begin{bmatrix} 1 & 4 & 5 \\ 2 & 3 & 2 \\ 0 & -1 & 1 \end{bmatrix}$, determine det (A).

$$\det(A) = \left[\begin{array}{ccc|cc} 1 & 4 & 5 & 1 & 4 \\ 2 & 3 & 2 & 2 & 3 \\ 0 & -1 & 1 & 0 & -1 \end{array}\right] = 3 + 0 - 10 - 8 + 2 - 0 = -12$$

3.3.2 Determinante igual a zero

O determinante de uma matriz será igual a zero quando:

- Uma fila (ou linha ou coluna) em que todos os elementos são iguais a zero;

- Duas filas iguais ou múltiplas;

- Os elementos de uma fila formem uma combinação linear dos elementos de outras duas filas.

3.4 Matriz inversa

Dada uma matriz quadrada A de ordem n, se AB = I_n, então dizemos que B é a matriz inversa de A. Representamos matriz inversa de A por A^{-1}.

Quanto a matriz inversa de A existe, dizemos que A é invertível. E isso só acontece quando det (A) ≠ 0.

Exemplo: Dadas as matrizes A = $\begin{bmatrix} 1 & -1 \\ 2 & 0 \end{bmatrix}$ e B = $\begin{bmatrix} 1 & 2 & 0 \\ 2 & 4 & 1 \\ 3 & 6 & 3 \end{bmatrix}$, determine, se existir, A^{-1} e B^{-1}.

Temos que, det (A) = 0 + 2 = 2, logo A é invertível e A^{-1} = $\begin{bmatrix} 0 & \frac{1}{2} \\ -1 & \frac{1}{2} \end{bmatrix}$

E det (B) = $\begin{bmatrix} 1 & 2 & 0 & 1 & 2 \\ 2 & 4 & 1 & 2 & 4 \\ 3 & 6 & 3 & 3 & 6 \end{bmatrix}$ = 12 + 6 + 0 – 12 – 6 – 0 = 0, como det (B) = 0 temos que B^{-1} não existe.

4 CRIPTOGRAFIA: UM RECORTE HISTÓRICO

Criptografia é a ciência de escrever em códigos ou em cifras. Ela fornece técnicas que permitem a codificação ou decodificação dos dados; o objetivo da criptografia é permitir uma comunicação segura.

Desde a antiguidade, o homem tem a preocupação em manter seus segredos. Existem registros de criptografia do ano de 1900 a.C., no Egito, quando Khnumhotep II, arquiteto do faraó Amenemhet II, construiu monumentos que precisavam ser documentados, e essas informações não podiam ser de domínio público. O escriba teve a ideia de trocar algumas palavras do texto dos tabletes onde estão as informações dessas construções, pois em caso de roubo o ladrão não acharia o caminho do tesouro.

Na Mesopotâmia, em 1500 a.C., a Criptografia chegou a um nível mais moderno. O primeiro registro da utilização da Criptografia nessa região está em uma fórmula para fazer esmaltes para cerâmica. Essa fórmula foi encontrada em um tablete de 8x5 cm no Rio Tigre e usava símbolos especiais que podem ter vários significados.

Entre 600-500 a.C., as três cifras hebraicas mais conhecidas eram: Atbash, Albam e Atbash, sendo muito utilizadas em textos religiosos. Em 475 a.C. temos informação do sistema de criptografia militar mais antigo, o scytale ou bastão de Licurgo, utilizado por Tucídides para entregar ordens ao príncipe e general espartano Pasanius.

4.1 Esteganografia/Criptografia

Para manter em segredo suas informações sigilosas, o homem foi desenvolvendo diversos métodos. Um desses métodos consiste na Esteganografia (do grego “steganos”: coberto; “graphein”: escrever), essa foi uma dos primeiros métodos para ocultar mensagens usadas pelo homem. Esse método consiste em ocultar a existência da informação por algo meio químico ou físico.

A Esteganografia foi utilizada durante muitas épocas, mas sua fragilidade é um grande problema, pois uma vez descoberta à maneira de ocultar a mensagem seu conteúdo era exposto aos interceptadores.

Com relação a essa fragilidade da Esteganografia, citamos dois exemplos apresentados na dissertação de DE MELLO(2014):

> A técnica consistiu na raspagem da cabeça de um mensageiro e no registro da mensagem em seu couro cabeludo. Após o crescimento do cabelo, o mensageiro dirigiu-se ao destino sem sofrer qualquer tipo de interceptação, raspou novamente a cabeça e revelou o conteúdo da mensagem ao destinatário. No século XVI, o cientista italiano Giovanni Porta descreveu uma técnica estenográfica na qual era possível “esconder uma mensagem dentro de um ovo cozido fazendo uma tinta com uma onça de alume e um quartilho de vinagre e então escrevendo na casca do ovo. A solução penetra na casca porosa e deixa a mensagem sobre a clara endurecida do. Para ler basta retirar a casca do ovo”. (pág 9-10)

Durante a Segunda Guerra Mundial, os alemães usavam a esteganografia fazendo uso da técnica chamada de microponto. Essa técnica consiste em reduzir a fotografia de uma página de texto até obter uma imagem circular com o diâmetro menor que um milímetro. Logo depois, a imagem circular era ocultada sob o ponto final de uma suposta carta e enviada a seu destinatário. Até 1941 essa técnica teve sucesso, mas o FBI foi informado sobre a técnica utilizada pelos alemães e interceptou várias mensagens, decifrando a maioria de seus conteúdos.

Por causa de sua fragilidade a Esteganografia, obrigou o desenvolvimento de técnicas mais confiáveis. Assim surgiu a Criptografia (do grego” kriptos”: oculto; “graphein”: escrever). Diferente da Esteganografia, a Criptografia visa tornar a mensagem incompreensível caso seja interceptada aumentando assim o grau de segurança no transporte da mensagem.

4.2 Métodos de Criptografia

O processo de codificarmos uma mensagem começa a partir da cifragem da mensagem que será transmitida. Chamamos de cifra a técnica que faz uso da troca de letras ou caracteres da mensagem original por outras que são retiradas de um alfabeto cifrado. Obtemos o alfabeto cifrado quando reorganizamos o alfabeto original. Cada cifra é formada por um algoritmo, que envolve as técnicas de cifragem da mensagem, e por uma chave, que é o elemento ou o método específico que permite decifrar a mensagem.

4.2.1 Cifra de César

Esse método recebeu esse nome por ter sido utilizado pelo Imperador Júlio César. O método consiste em substituir cada letra da mensagem original por uma letra três casas a sua frente.

Ex:

a m i g o (Texto original)

D P L J R (Texto codificado)

Logo, as letras do alfabeto cifrado da Cifra de César ficam da seguinte forma:

Texto simples	a	b	c	d	e	f	g	h	i	j	k	l	m
Cifra	D	E	F	G	H	I	J	K	L	M	N	O	P
Texto simples	n	o	p	q	r	s	t	u	v	w	x	y	z
Cifra	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Figura 1 – Cifra de César

Disponível em:<https://www.google.com.br/search?q=cifra+de+cesar&client=firefox-b&biw=1024&bih=615&source=lnms&tbm=isch&sa=X&ved=0ahUKEwj4ta7l3szRAhWJGpAKHQWCAjc4ChD8BQgGKAE#imgrc=4QlK66d1xj_LqM%3A>. Acesso janeiro 2017

Por exemplo, ao utilizarmos a Cifra de César para a mensagem *"SÓ VITÓRIA IMPORTA"* teremos a sua codificação, a partir dos dados apresentados na Figura 1, como: *"VRYLWRULDLPSRUWD"*

4.2.2 Cifra de Vigenère

O Quadrado de Vigenère foi criado a partir de um alfabeto original de 26 letras relacionado a outros vinte e seis alfabetos cifrados distintos. Cada alfabeto cifrado foi formado a partir do seguinte critério: deslocamento de uma letra para esquerda em relação a uma letra do alfabeto anterior. A partir dessa condição as letras da Cifra de Vigenère ficam da seguinte forma:

	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 2 – Quadrado de Vigenère

Disponível em: <https://www.google.com.br/search?q=quadrado+de+vigenere&client=firefox-b&biw=1024&bih=615&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjX46Cf8czRAhXDEpAKHZnIA-4Q_AUIBigB#imgrc=vQy10r3rFmiiXM%3A>. Acesso janeiro de 2017

Por exemplo, quando utilizamos apenas as três primeiras linhas do Quadrado de Vigenère, para cifrar a mensagem: *AMIGO* obtemos: para a 1ª letra da mensagem original usaremos seu correspondente da 2ª linha; para a 2ª letra usaremos seu correspondente na 1ª linha; para a 3ª letra usaremos seu correspondente da 3ª

linha; para a 4ª letra usaremos o correspondente na 1ª linha e para a 5ª letra usaremos o correspondente na 3ª linha. Portanto, a mensagem cifrada será CNLHR.

Por conta do grande número de chaves que a Cifra de Vigenère possui, ela era conhecida como *le chiffre indechiffrable* (a cifra indecifrável), por mais que fosse difícil ser quebrado esse código, por conta da sua dificuldade em ser manuseado ela ficou esquecida por quase dois séculos.

4.2.3 Cifra de Hill

Foi criada em 1929 pelo matemático americano Lester Hill (1891-1961) e para utilizá-la devemos associar cada letra do alfabeto a um número. Para tanto, faz-se necessário o uso dos conceitos de matrizes, multiplicação de matrizes, matriz inversa e aritmética modular.

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

Figura 3: Tabela Cifra de Hill

Para cifrarmos uma palavra com o uso da tabela que associa as letras com os números, conforme mostra a figura 3, a Cifra de Hill, teremos que dividi-la em blocos com a mesma quantidade de letras. Caso a palavra tenha uma quantidade ímpar de letras, acrescentamos uma letra qualquer no final da palavra para garantirmos que os blocos tenham a mesma quantidade de letras. Cada bloco será parte de um vetor p e criaremos uma matriz K invertível para cifrarmos esse vetor p. Vejamos por exemplo como se dá a codificação da palavra ESCOLA.

- Dividiremos a palavra em blocos com duas letras;
- Associaremos cada letra a um número, ficando da seguinte forma:

  E S C O L A

  4 18 2 14 11 0

Assim, cada vetor p fica da seguinte maneira:

$p_1 = \begin{pmatrix} 4 \\ 18 \end{pmatrix}$, $p_2 = \begin{pmatrix} 2 \\ 14 \end{pmatrix}$, $p_3 = \begin{pmatrix} 11 \\ 0 \end{pmatrix}$.

- A matriz K escolhida para cifra o vetor p é: $\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$

- Cifrando o bloco ES, temos:

$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 4 \\ 18 \end{pmatrix} = \begin{pmatrix} 30 \\ 26 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 0 \end{pmatrix} \mod 26$

- Cifrando o bloco CO, temos:

$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 20 \\ 18 \end{pmatrix} \equiv \begin{pmatrix} 20 \\ 18 \end{pmatrix} \mod 26$

- Cifrando o bloco LA, temos:

$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 11 \\ 0 \end{pmatrix} = \begin{pmatrix} 33 \\ 22 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 22 \end{pmatrix} \mod 26$

- Utilizando a tabela da figura 3, a mensagem codificada será:
  EA US HW

Logo a mensagem a ser enviada é EAUSHW, sem espaços.

Fazendo o processo inverso, vamos agora decodificar essa mensagem. Novamente dividiremos a mensagem em blocos com duas letras e associá-las a números, ficando da seguinte forma:

E	A	U	S	H	W
4	0	20	18	7	22

E iremos multiplicar cada bloco pela matriz inversa de K, assim obteremos a mensagem original, logo, $K^{-1} = \begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$.

Decodificando os vetores cifrados:

$$\begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \bullet \begin{pmatrix} 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 4 \\ -8 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 18 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \bullet \begin{pmatrix} 20 \\ 18 \end{pmatrix} = \begin{pmatrix} 2 \\ 14 \end{pmatrix} \equiv \begin{pmatrix} 2 \\ 14 \end{pmatrix} \text{ mod } 26$$

$$\begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix} \bullet \begin{pmatrix} 7 \\ 22 \end{pmatrix} = \begin{pmatrix} -15 \\ 52 \end{pmatrix} \equiv \begin{pmatrix} 11 \\ 0 \end{pmatrix} \text{ mod } 26$$

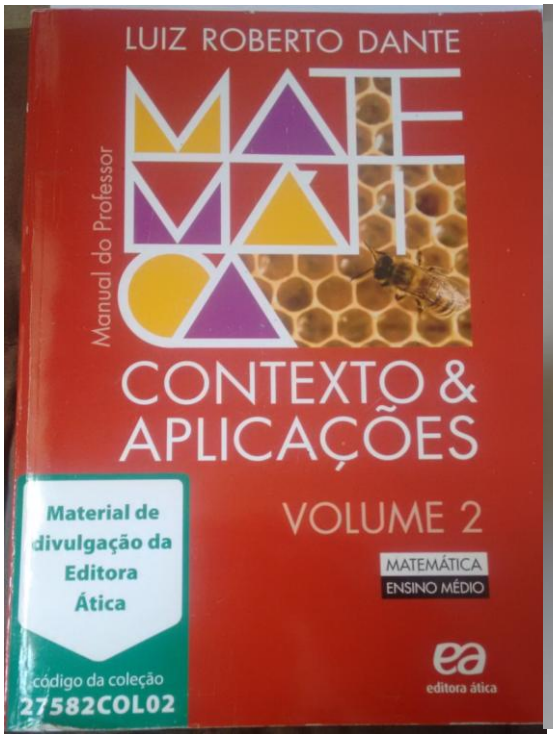
Notemos que cada vetor coluna corresponde aos vetores da mensagem original, logo a palavra decodificada é ESCOLA.

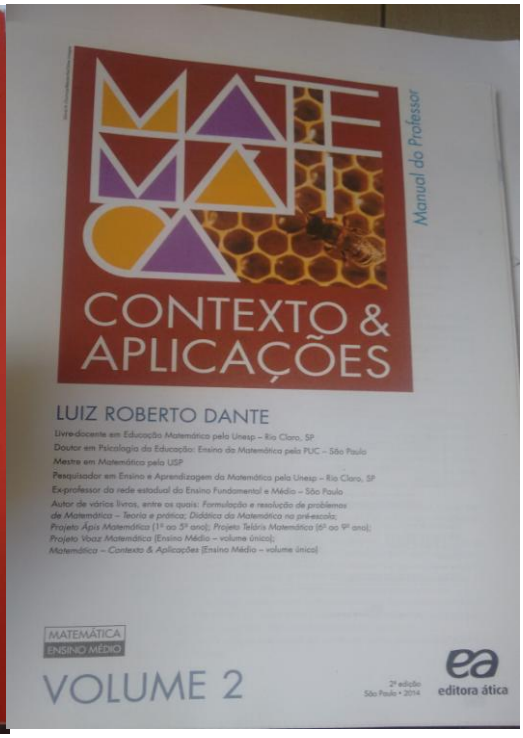
5 MATRIZES E CRIPTOGRAFIA NOS LIVROS DIDÁTICOS

Após analisarmos alguns livros do Ensino Médio, indicados pelo Programa Nacional de Livros Didáticos (PNLD), somente um livro do 2º ano do Ensino Médio fala sobre Criptografia. O autor, Dante, em seu livro faz a associação de Matrizes com Criptografia e de modo muito superficial. Ele coloca Criptografia como uma curiosidade, utilizando apenas um breve conceito de Criptografia como uma aplicação para Matrizes.

Os documentos oficiais apresentados pelo Ministério da Educação, os Parâmetros Curricular Nacional (PCN) e na Base Nacional Comum Curricular (BNCC), não falam explicitamente sobre Criptografia, mas falam a respeito do desenvolvimento de diversos tipos de raciocínios.

A seguir apresentaremos alguns livros do Ensino Médio que foram colocados como opção de escolha nas escolas públicas pelo Programa Nacional do Livro Didático para o Ensino Médio (PNLEM). O único livro que aborda a Criptografia como ferramenta para o ensino de Matrizes é o Volume 2, da Editora Ática, escrito por Luiz Roberto Dante.





CAPÍTULO 5

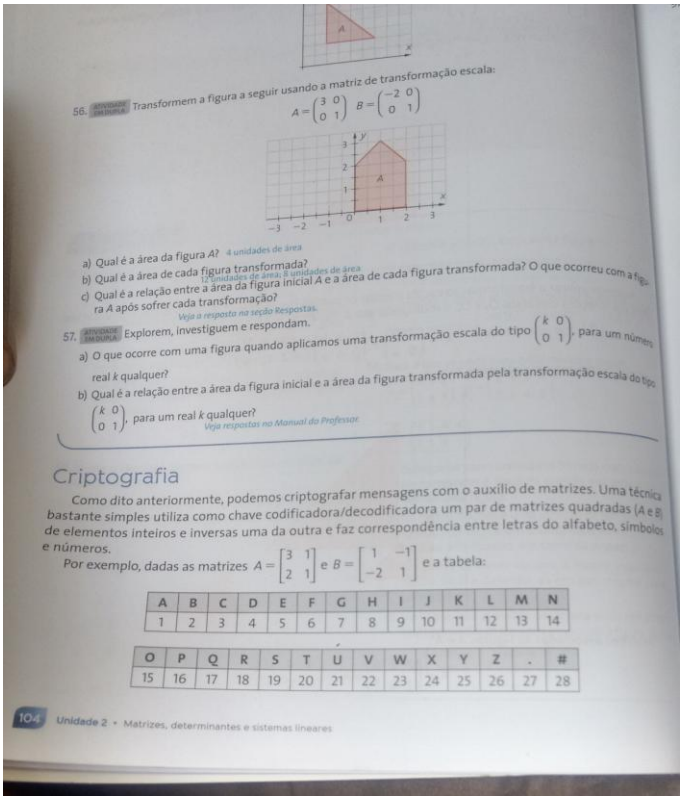
Matrizes e determinantes

A necessidade de se escrever mensagens sigilosas é muito antiga. Ao longo da história, reis, rainhas, generais, entre outros, buscaram meios eficientes de comunicação entre os seus aliados. O grande diferencial no tipo de comunicação que eles buscavam era o de não revelar segredos e estratégias aos inimigos. Esse contexto motivou o desenvolvimento de códigos e cifras, ou seja, técnicas para mascarar uma mensagem, de modo que apenas o destinatário consiga entender o conteúdo.

A criptografia – do grego *kryptós* (escondido) e *gráphein* (escrita) – tem por objetivo codificar mensagens para assegurar a integridade e o sigilo da informação. Em vários momentos da história essa técnica ajudou a decidir os resultados de batalhas.

Atualmente, as informações também são muito valiosas e o processo de codificação de mensagens tem um papel cada vez maior na sociedade, principalmente no que se refere à internet. Na rede mundial de computadores muitas informações são trocadas e o grande desafio é manter o sigilo das informações, por exemplo, instituições financeiras, lojas e *sites* precisam manter as informações dos seus clientes em sigilo.

A criptografia utilizada por grandes empresas e governos realiza cálculos complexos para obtenção de um modelo seguro e quase indecifrável. Mas é possível utilizarmos conceitos simples da álgebra matricial como "chave codificadora/decodificadora", tais como produto de matrizes, matriz identidade, matriz quadrada e matriz inversa, que devem ser do conhecimento tanto do remetente como do destinatário da mensagem. Neste capítulo você aprenderá essa técnica.



56. ATIVIDADE EM DUPLA Transformem a figura a seguir usando a matriz de transformação escala:

$A = \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}$ $B = \begin{pmatrix} -2 & 0 \\ 0 & 1 \end{pmatrix}$

a) Qual é a área da figura A? 4 unidades de área.

b) Qual é a área de cada figura transformada? 12 unidades de área; 8 unidades de área.

c) Qual é a relação entre a área da figura inicial A e a área de cada figura transformada? O que ocorreu com a figura A após sofrer cada transformação? Veja a resposta na seção Respostas.

57. ATIVIDADE EM DUPLA Explorem, investiguem e respondam.

a) O que ocorre com uma figura quando aplicamos uma transformação escala do tipo $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$, para um número real k qualquer?

b) Qual é a relação entre a área da figura inicial e a área da figura transformada pela transformação escala do tipo $\begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix}$, para um real k qualquer? Veja respostas no Manual do Professor.

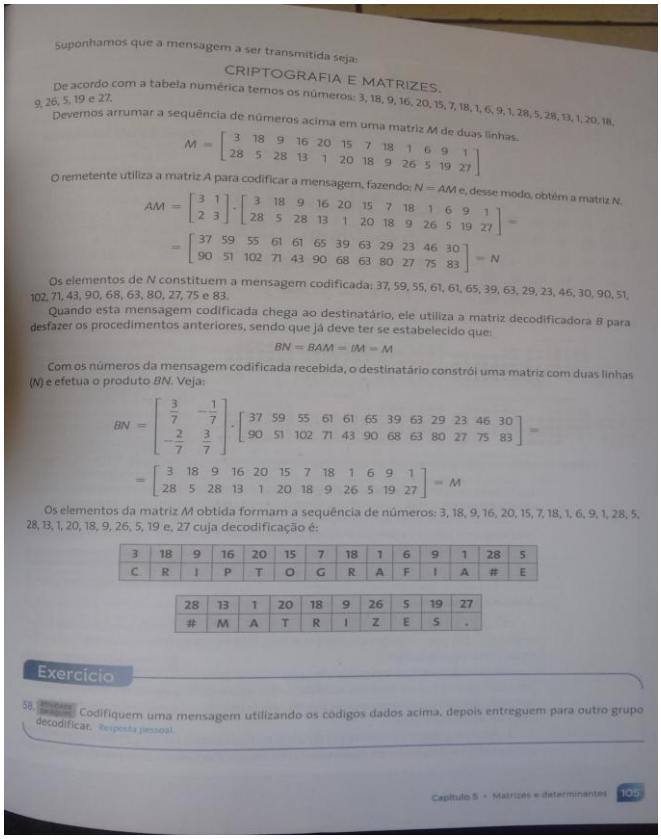
Criptografia

Como dito anteriormente, podemos criptografar mensagens com o auxílio de matrizes. Uma técnica bastante simples utiliza como chave codificadora/decodificadora um par de matrizes quadradas (A e B) de elementos inteiros e inversas uma da outra e faz correspondência entre letras do alfabeto, símbolos e números.

Por exemplo, dadas as matrizes $A = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix}$ e a tabela:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	2	3	4	5	6	7	8	9	10	11	12	13	14

O	P	Q	R	S	T	U	V	W	X	Y	Z	.	#
15	16	17	18	19	20	21	22	23	24	25	26	27	28



Suponhamos que a mensagem a ser transmitida seja:

CRIPTOGRAFIA E MATRIZES.

De acordo com a tabela numérica temos os números: 3, 18, 9, 16, 20, 15, 7, 18, 1, 6, 9, 1, 28, 5, 28, 13, 1, 20, 18, 9, 26, 5, 19 e 27.

Devemos arrumar a sequência de números acima em uma matriz M de duas linhas.

$$M = \begin{bmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{bmatrix}$$

O remetente utiliza a matriz A para codificar a mensagem, fazendo: $N = AM$ e, desse modo, obtém a matriz N.

$$AM = \begin{bmatrix} 3 & 1 \\ 2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{bmatrix} =$$

$$= \begin{bmatrix} 37 & 59 & 55 & 61 & 61 & 65 & 39 & 63 & 29 & 23 & 46 & 30 \\ 90 & 51 & 102 & 71 & 43 & 90 & 68 & 63 & 80 & 27 & 75 & 83 \end{bmatrix} = N$$

Os elementos de N constituem a mensagem codificada: 37, 59, 55, 61, 61, 65, 39, 63, 29, 23, 46, 30, 90, 51, 102, 71, 43, 90, 68, 63, 80, 27, 75 e 83.

Quando esta mensagem codificada chega ao destinatário, ele utiliza a matriz decodificadora B para desfazer os procedimentos anteriores, sendo que já deve ter se estabelecido que:

$$BN = BAM = IM = M$$

Com os números da mensagem codificada recebida, o destinatário constrói uma matriz com duas linhas (N) e efetua o produto BN. Veja:

$$BN = \begin{bmatrix} \frac{3}{7} & -\frac{1}{7} \\ -\frac{2}{7} & \frac{3}{7} \end{bmatrix} \cdot \begin{bmatrix} 37 & 59 & 55 & 61 & 61 & 65 & 39 & 63 & 29 & 23 & 46 & 30 \\ 90 & 51 & 102 & 71 & 43 & 90 & 68 & 63 & 80 & 27 & 75 & 83 \end{bmatrix} =$$

$$= \begin{bmatrix} 3 & 18 & 9 & 16 & 20 & 15 & 7 & 18 & 1 & 6 & 9 & 1 \\ 28 & 5 & 28 & 13 & 1 & 20 & 18 & 9 & 26 & 5 & 19 & 27 \end{bmatrix} = M$$

Os elementos da matriz M obtida formam a sequência de números: 3, 18, 9, 16, 20, 15, 7, 18, 1, 6, 9, 1, 28, 5, 28, 13, 1, 20, 18, 9, 26, 5, 19 e, 27 cuja decodificação é:

3	18	9	16	20	15	7	18	1	6	9	1	28	5
C	R	I	P	T	O	G	R	A	F	I	A	#	E

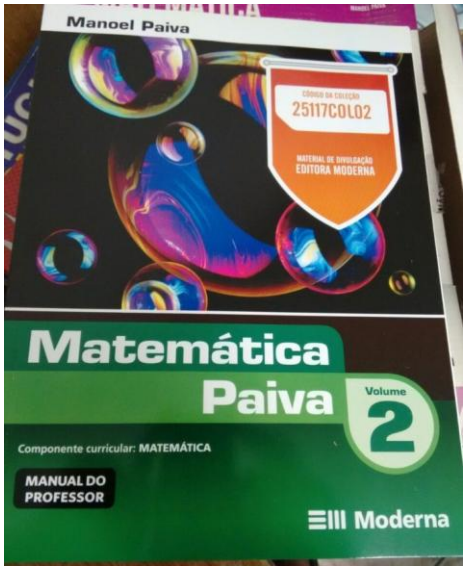
28	13	1	20	18	9	26	5	19	27
#	M	A	T	R	I	Z	E	S	.

Exercício

58. Codifiquem uma mensagem utilizando os códigos dados acima, depois entreguem para outro grupo decodificar. Resposta pessoal.

Capítulo 5 • Matrizes e determinantes 105

Os demais livros, por nós analisados, não relacionam Criptografia com Matrizes e nem comentam sobre o assunto. Apresentamos dois desses livros.



Dos livros analisados apenas do Dante fala sobre Criptografia e relaciona com os conceitos de Matrizes.

6 A CRIPTOGRAFIA NA SALA DE AULA

No sentido de verificarmos como os alunos do Ensino Médio venham compreender o conceito de Criptografia, passamos a elaborar algumas atividades para serem aplicadas em sala de aula.

As atividades foram aplicadas em três turmas do 3º ano do Ensino Médio, em uma escola pública estadual, situada no bairro de Comendador Soares, município de Nova Iguaçu, na baixada fluminense, estado Rio de Janeiro.

Foram aplicadas cinco atividades durante três dias. Em nosso trabalho cada turma foi denominada de T1, T2 e T3. Na turma T1 há 35 alunos, a turma T2, possui 40 alunos e, a T3 tem 35 alunos.

As atividades 1 e 2 foram aplicadas no 1º dia. As atividades 3 e 4 foram aplicadas no 2º dia e, por fim, no 3º dia aplicamos a atividade 5.

O período de aplicação das atividades foi na semana que antecedeu as festas carnavalescas, o que influenciou a baixa frequência nas turmas T1 e T3. O número de alunos presentes, por turma, foi:

TURMAS	1º DIA	2º DIA	3º DIA
T1	19	24	14
T2	30	31	31
T3	29	32	24
TOTAL	78	87	69

As tabelas a seguir apresentam a faixa etária e o gênero dos alunos presentes nos dias da aplicação de cada atividade. Podemos observar que a idade, da maioria dos alunos em todas as turmas, está compreendida entre 16 e 17 anos.

No primeiro dia de aplicação das atividades estiveram presente 78 alunos e dispostos da seguinte forma:

Tabela 1

Idades dos Alunos

Idades (em anos) / Turmas	15	16	17	18	19	20	21	Total
T1	0	5	11	3	0	0	0	19
T2	5	18	6	1	0	0	0	30
T3	0	6	12	7	2	1	1	29
Total	5	29	29	11	2	1	1	78

Fonte: Do Autor

Gráfico 1

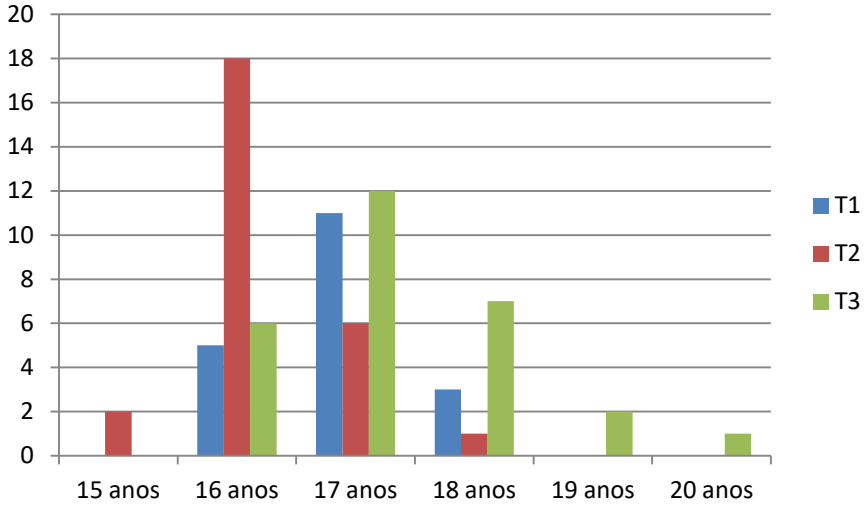


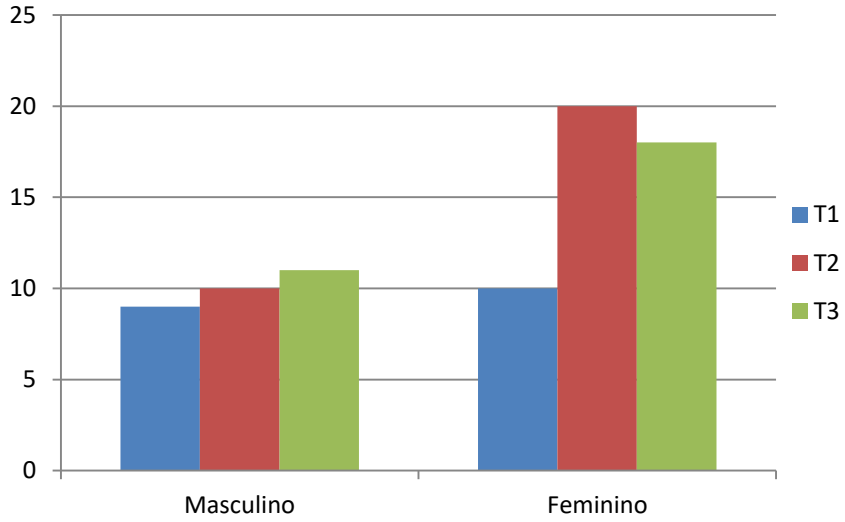
Tabela 2

Gênero dos Alunos

Gênero / Turmas	Masculino	Feminino	Total
T1	9	10	19
T2	10	20	30
T3	11	18	29
Total	30	48	78

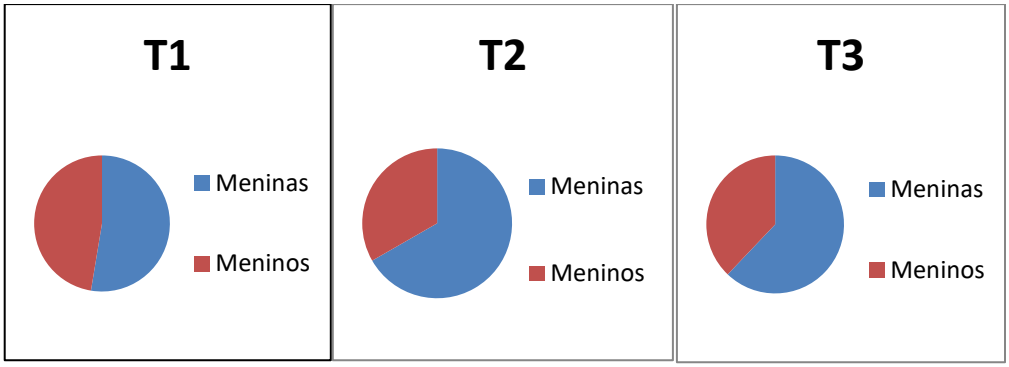
Fonte: Do Autor

Gráfico 2



O número de meninas foi maior durante a aplicação das atividades, representando 52,6% na turma T1, 66,7% na T2 e 62,1% na turma T3. O que podemos concluir que, em média, a frequência delas é de, aproximadamente, 60,5%.

Gráfico 3



Já no segundo dia de aplicação das atividades, 87 alunos estiveram presentes e estavam dispostos do seguinte modo:

Tabela 3

Tabela das idades dos alunos presentes

Idades / Turmas	15	16	17	18	19	20	21	Total
T1	0	6	14	3	1	0	0	24
T2	3	24	2	1	1	0	0	31
T3	0	7	13	10	0	1	1	32
Total	3	37	29	14	2	1	1	87

Fonte: Do Autor

Gráfico 4

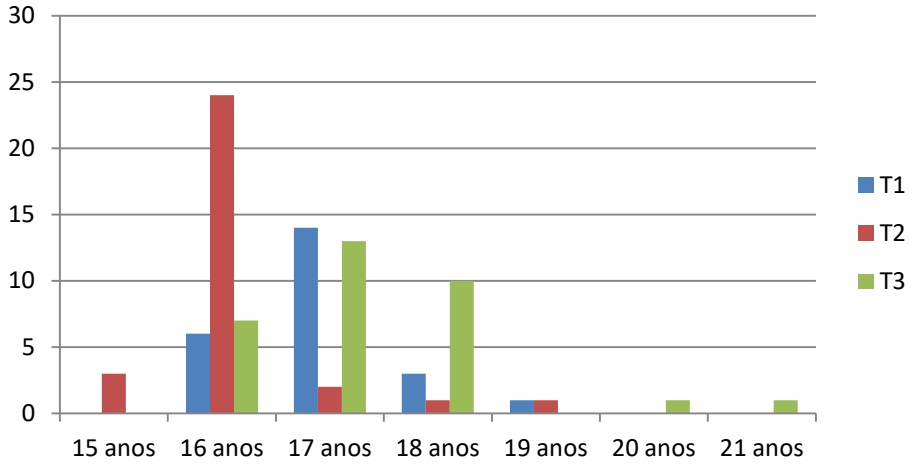


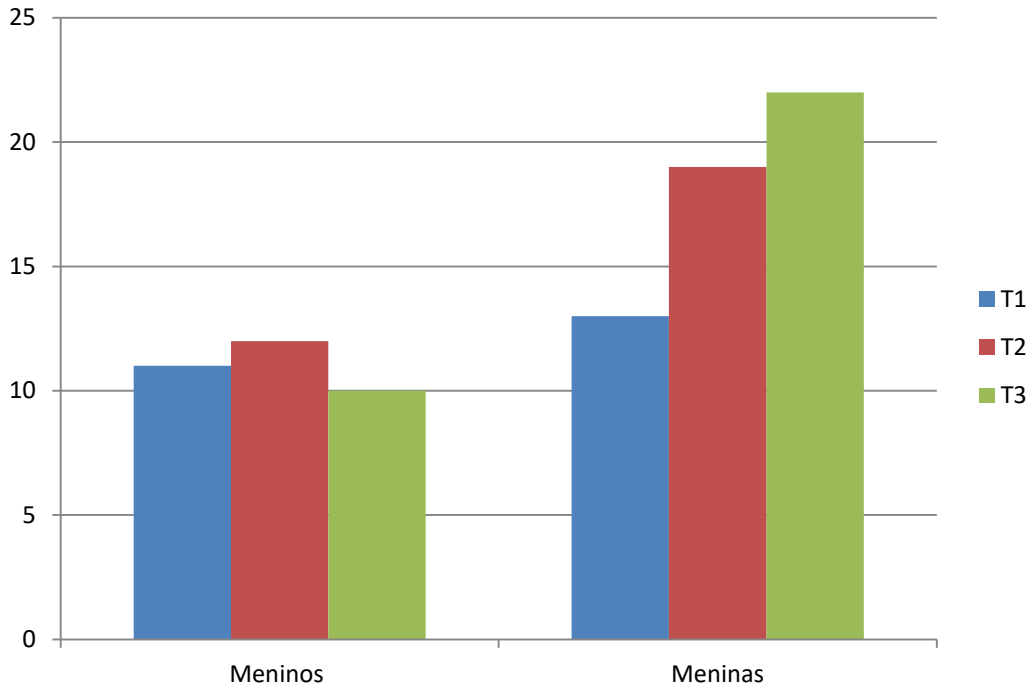
Tabela 4

Tabela representando o gênero dos alunos presentes

Gênero / Turmas	Masculino	Feminino	Total
T1	11	13	24
T2	12	19	31
T3	10	22	32
Total	33	56	87

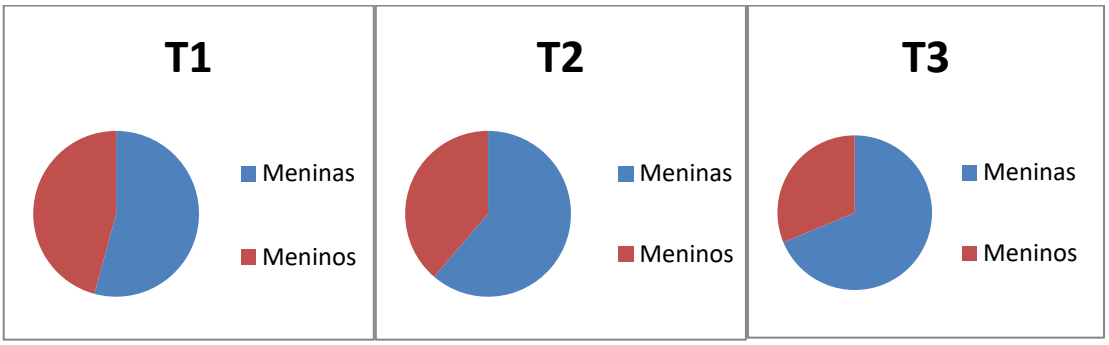
Fonte: Do Autor

Gráfico 5



Podemos observar que o número de meninas durante a aplicação das atividades permanece maior e foi de 54,2% na turma T1, 61,3% na T2 e 68,7% na turma T3. Implicando, em média, a frequência delas, aproximadamente, de 61,4%.

Gráfico 6



Por fim, no terceiro dia de aplicação das atividades estiveram presentes 69 alunos e dispostos da seguinte forma:

Tabela 5

Tabela das idades dos alunos presentes

Idades / Turmas	15	16	17	18	19	20	21	Total
T1	0	3	10	1	0	0	0	14
T2	3	21	7	0	0	0	0	31
T3	0	4	14	5	0	0	1	24
Total	3	28	31	6	0	0	1	69

Fonte: Do Autor

Gráfico 7

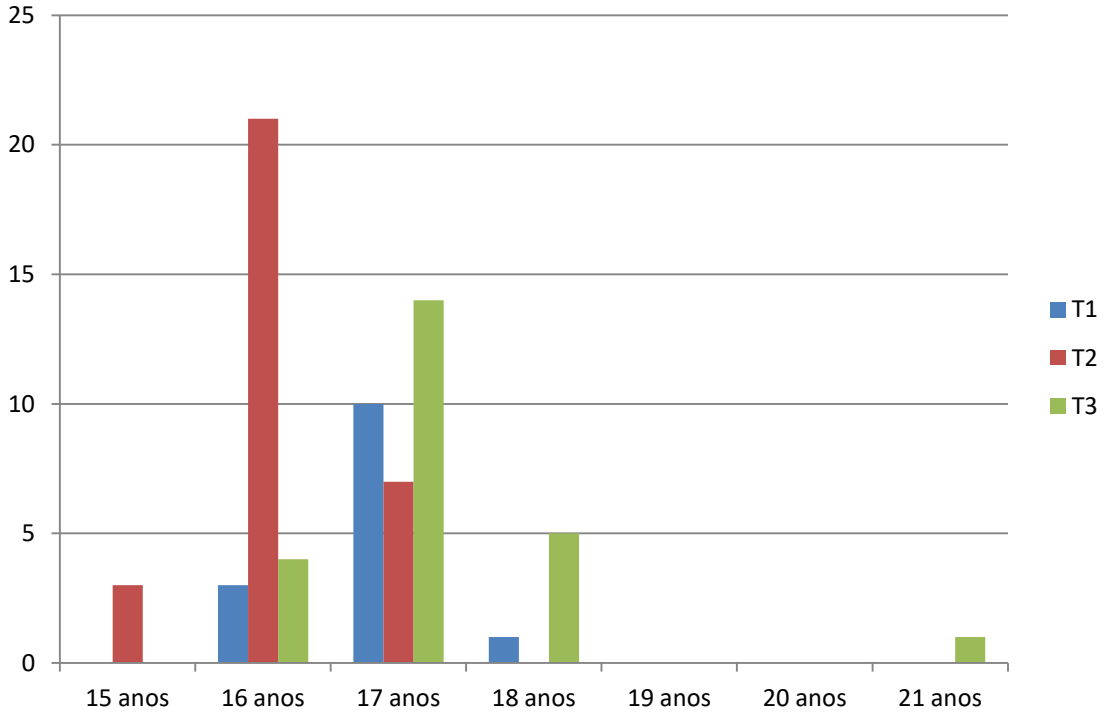


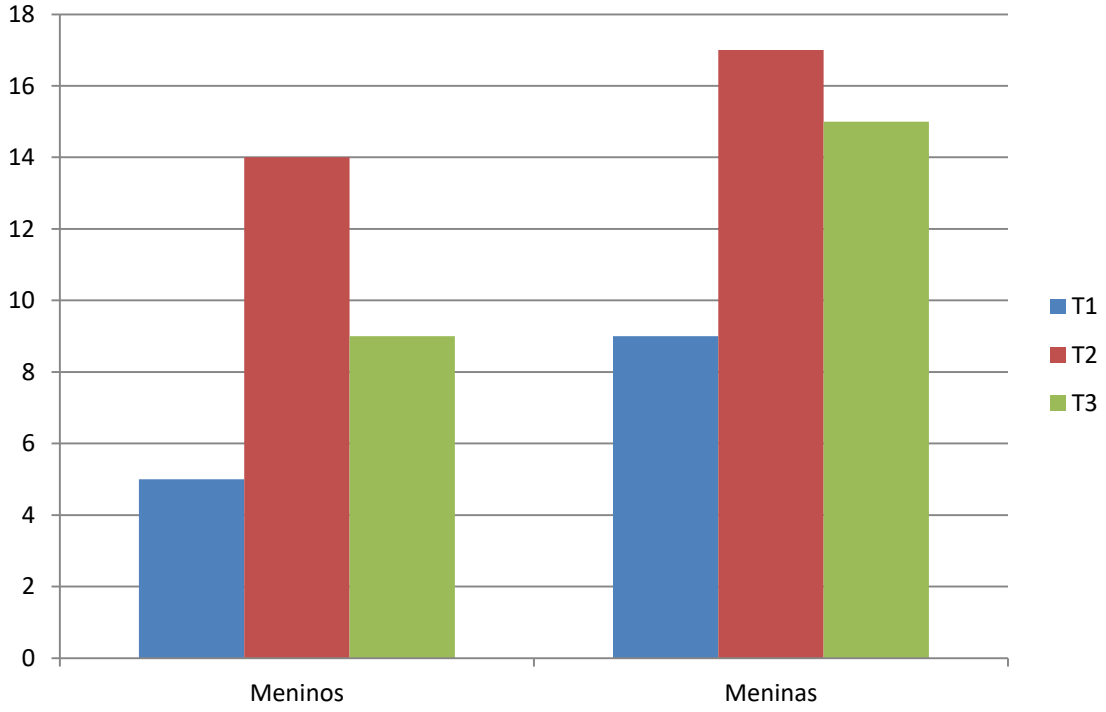
Tabela 6

Tabela representando o gênero dos alunos presentes

Gênero / Turmas	Masculino	Feminino	Total
T1	5	9	14
T2	14	17	31
T3	9	15	24
Total	28	41	69

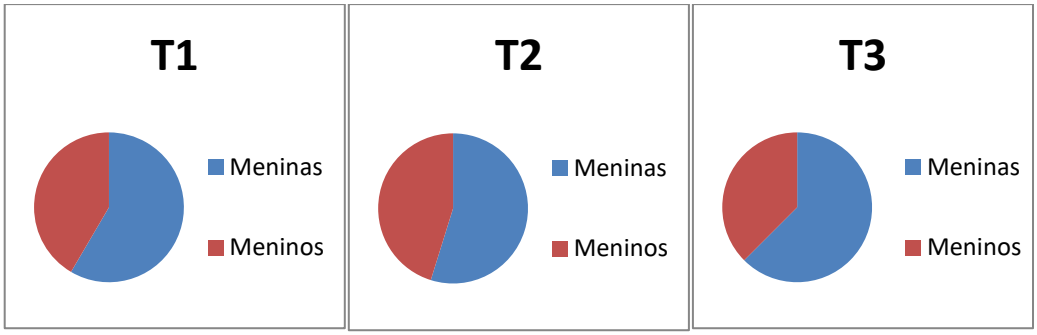
Fonte: Do Autor

Gráfico 8



Nos três dias de aplicação o número de meninas durante a aplicação das atividades foi 64,3% na turma T1, 54,8% na T2 e 62,5% na turma T3. Podemos concluir que, em média, a frequência delas é de aproximadamente, 60,5%.

Gráfico 9



6.1 Desenvolvimento das atividades

As atividades foram assim aplicadas: cada turma foi dividida em grupos, com 4 ou 5 alunos, exceto na T1, que por conta da baixa frequência, a turma foi dividida em duplas.

As quatro primeiras atividades foram aplicadas como parte introdutória do conceito de Criptografia. Nosso objetivo nessas atividades é verificar como os alunos compreendem a necessidade de criar códigos para emitir uma mensagem e que esses conceitos não estão distantes da realidade que os cercam.

Durante a aplicação, a dúvida comum apresentada por todos os alunos, independente da turma, era qual conteúdo a ser utilizado para resolver cada uma das atividades.

Após o debate sobre o conteúdo, os alunos concluíram que não havia um único modo específico de resolver cada atividade, pois cada uma apresentava mais de uma maneira de ser resolvida.

Vejamos a seguir como cada atividade foi desenvolvida.

6.1.1 Atividade 1 - Qual o peso das figuras?[1]

□ + □ + Δ + ○ = 17 kg

□ + Δ + Δ + ○ = 14 kg

□ + Δ + ○ + ○ = 13 kg

No desenho acima há três fileiras de figuras geométricas, que possuem cada uma delas, um determinado “peso”.

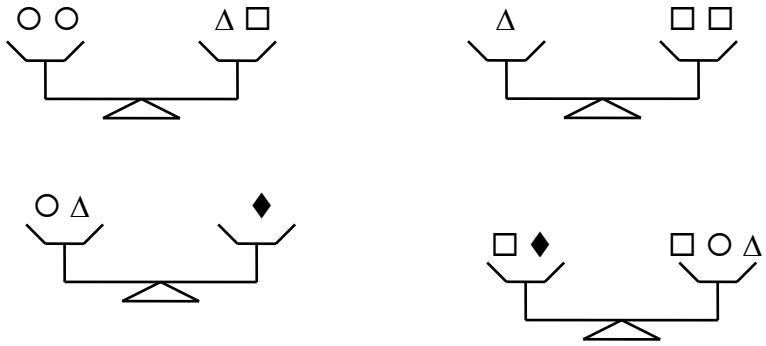
Descubra o “peso” exato da figura retangular, circular e triangular.

Nessa atividade foi estabelecido para cada figura geométrica um valor numérico. Portanto, nosso objetivo é saber como os alunos decodificaram esses valores e que conceito matemático foi utilizado. O nível de dificuldade dessa atividade foi considerado “médio” pelos alunos.

TURMAS	FÁCIL	MÉDIO	DIFÍCIL
T1	4	4	0
T2	2	4	1
T3	1	5	1
TOTAL	7	13	2

[1] Adaptação proposta por um aluno da Revista Globinho

6.1.2 Atividade 2 - Pesando as figuras[2]



Cada uma das figuras geométricas acima têm um “peso” e são colocadas nos pratos de uma balança que está em perfeito equilíbrio.

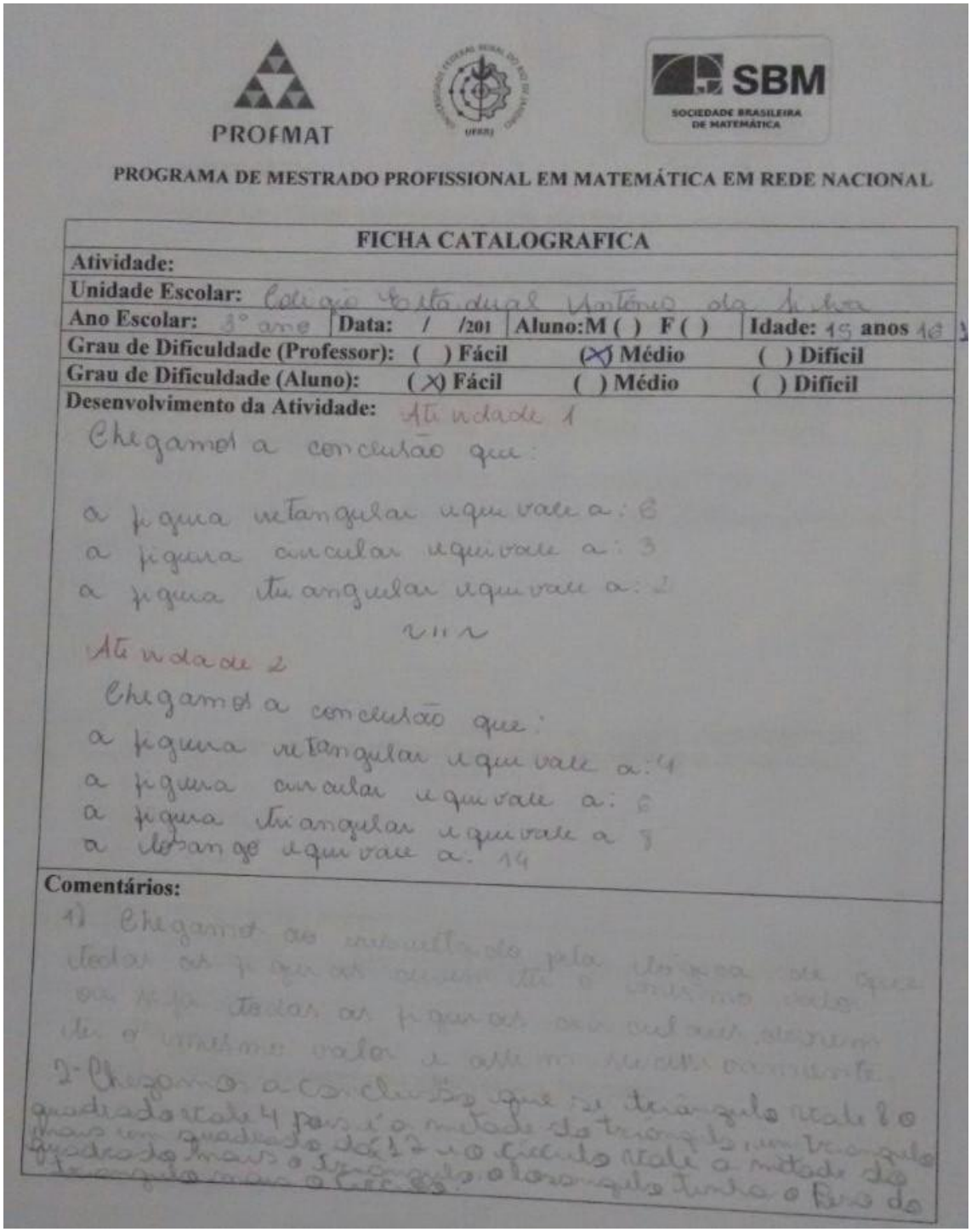
Sabendo que o triângulo “pesa” 8 g, calcule o “peso” de cada uma das outras figuras?

Esta atividade consiste em descobrir o valor das figuras geométricas de modo que as balanças fiquem equilibradas. Essa atividade foi de “fácil” aplicação pelo fato de sabermos o valor numérico do triângulo. A tabela a seguir representa a opinião dos grupos com relação ao grau de dificuldade desta atividade.

TURMAS	FÁCIL	MÉDIO	DIFÍCIL
T1	2	5	0
T2	2	4	1
T3	1	5	1
TOTAL	5	14	2

As duas atividades foram aplicadas no mesmo dia pela semelhança entre elas. A seguir temos algumas respostas apresentadas pelos alunos e os seus comentários.

[2] Adaptação do exercício criado pela professora Mariza Dela Laport Sanches



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FICHA CATALOGRAFICA

Atividade:			
Unidade Escolar: Colégio Estadual Antônio da Silva			
Ano Escolar: 3° ano	**Data:** / /201	**Aluno:** M ( ) F ( )	**Idade:** 15 anos 16
Grau de Dificuldade (Professor):	( ) Fácil	(X) Médio	( ) Difícil
Grau de Dificuldade (Aluno):	(X) Fácil	( ) Médio	( ) Difícil

Desenvolvimento da Atividade:

Atividade 1

Chegamos a conclusão que:

a figura retangular equivale a: 6
a figura circular equivale a: 3
a figura triangular equivale a: 2

2 + 1 = 2

Atividade 2

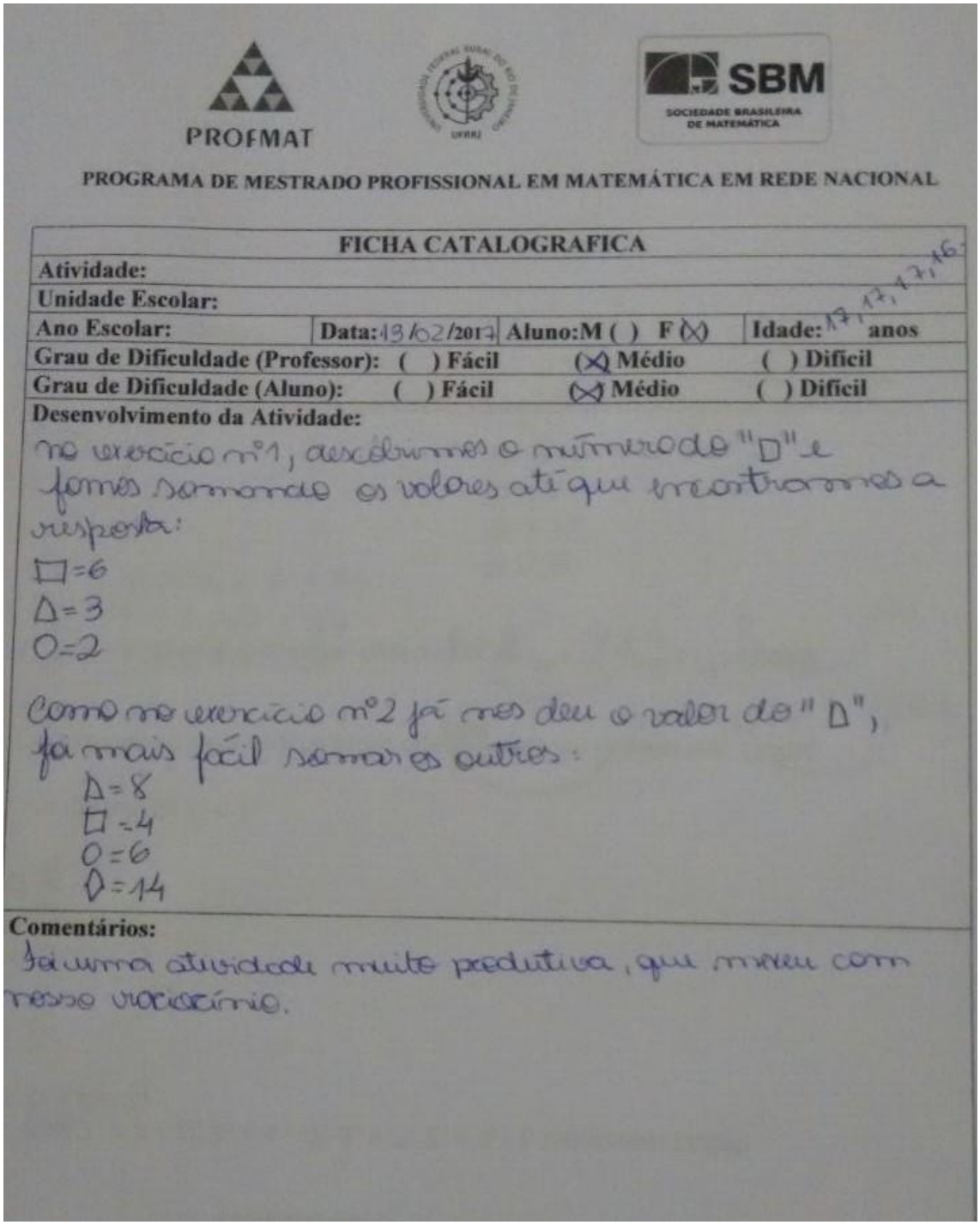
Chegamos a conclusão que:
a figura retangular equivale a: 4
a figura circular equivale a: 6
a figura triangular equivale a 3
a losango equivale a: 14

Comentários:

1) Chegamos ao resultado pela lógica as figuras de que todas as figuras devem ter o mesmo valor, ou seja, todas as figuras circulares devem ter o mesmo valor e assim sucessivamente.

2- Chegamos a conclusão que se o triângulo vale 8 o quadrado vale 4 pois é metade do triângulo, um triângulo mais um quadrado dá 12 e o círculo vale a metade do quadrado mais o triângulo, o losango tinha peso do triângulo mais o círculo.

Comentário do grupo com relação a atividade: "*1) Chegamos ao resultado pela lógica as figuras de que todas as figuras devem ter o mesmo valor, ou seja, todas as figuras circulares devem ter o mesmo valor e assim sucessivamente". "2) Chegamos a conclusão que se o triângulo vale 8 o quadrado vale 4 pois é metade do triângulo, um triângulo mais um quadrado dá 12 e o círculo vale a metade do quadrado mais o triângulo, o losango tinha peso do triângulo mais o círculo.*"



PROFMAT

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: | **Data:** 13/02/2017 | **Aluno:** M ( ) F (X) | **Idade:** 17 anos

Grau de Dificuldade (Professor): ( ) Fácil (X) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

No exercício nº1, descobrimos o número de "□" e fomos somando os valores até que encontrassemos a resposta:

□=6

Δ=3

O=2

Como no exercício nº2 já nos deu o valor de "Δ", foi mais fácil somar os outros:

Δ=8

□=4

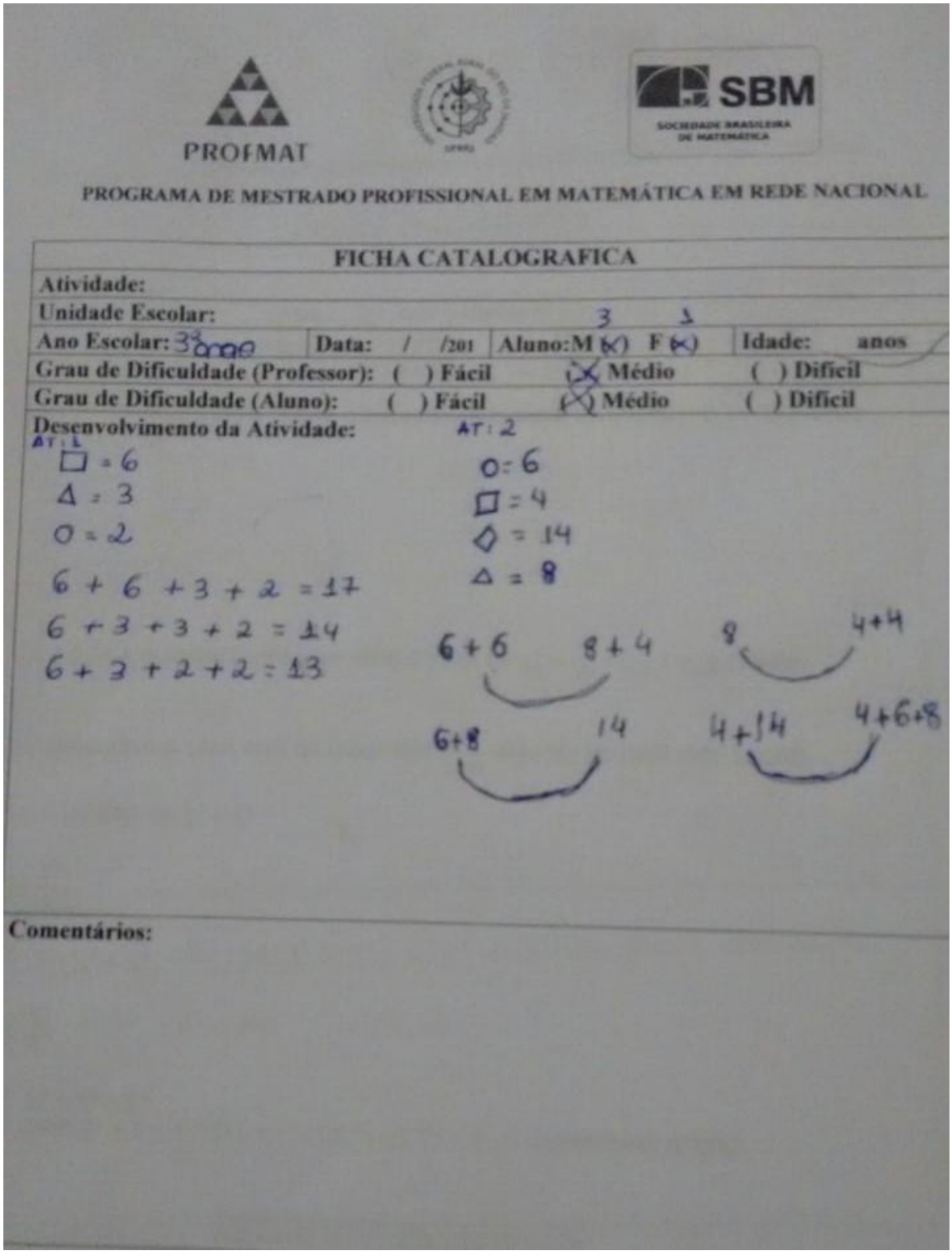
O=6

◊=14

Comentários:

Foi uma atividade muito produtiva, que mexeu com nosso raciocínio.

Comentário do grupo em relação a atividade: ”*Foi uma atividade muito produtiva, que mexeu com nosso raciocínio.*”



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: 3ºano | Data: / /201 | Aluno: M (3) F (1) | Idade: anos

Grau de Dificuldade (Professor): ( ) Fácil (X) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

AT: 1

□ = 6

Δ = 3

○ = 2

6 + 6 + 3 + 2 = 17

6 + 3 + 3 + 2 = 14

6 + 3 + 2 + 2 = 13

AT: 2

○ = 6

□ = 4

◇ = 14

Δ = 8

6+6 8+4

8 4+4

6+8 14

4+14 4+6+8

Comentários:

Durante a aplicação da atividade 1 alguns alunos, das três turmas, apresentaram uma dúvida bastante curiosa, eles perguntaram: *"As figuras tinham o mesmo valor em cada uma das equações?".* O que foi uma pergunta que me causou estranheza, afinal, por se tratar de turmas de terceiro ano do Ensino Médio, não imaginava que tal dúvida pudesse aparecer. Quando falei para tratar as figuras

geométricas como variáveis, todos entenderam que os seus valores teria de ser o mesmo nas três equações.

Com relação a atividade 2, os alunos não tiveram nenhuma dúvida em determinar o valor das figuras, pois já haviam resolvido a Atividade 1 que tratava figuras geométricas como variáveis.

Durante a resolução da segunda atividade todos os alunos utilizaram a quarta balança para descobrir o valor das figuras, sendo que a mesma não era necessária para resolver o problema. Mas precisávamos dela para verificar que os valores encontrados atendiam as quatro balanças.

No segundo dia aplicamos as atividades 3 e 4, conforme descrito abaixo.

6.1.3 Atividade 3 – Código de identificação[3]

Os números de identificação utilizados no cotidiano (de contas bancárias, de CPF, de Carteira de Identidade e etc.) usualmente possuem um dígito de verificação, normalmente representado após o hífen, como em 17326-9. Esse dígito adicional tem a finalidade de evitar erros no preenchimento ou digitação de documentos. Um dos métodos usados para gerar esse dígito utiliza os seguintes passos:

- multiplica-se o último algarismo do número por 1, o penúltimo por 2, o antepenúltimo por 1, e assim por diante, sempre alternando multiplicações por 1 e por 2.
- soma-se 1 a cada um dos resultados dessas multiplicações que for maior do que ou igual a 10.
- somam-se os resultados obtidos.
- calcula-se o resto da divisão dessa soma por 10, obtendo-se assim o dígito verificador.

Agora, você é capaz de saber qual o dígito verificador fornecido pelo processo acima para o número 24685?

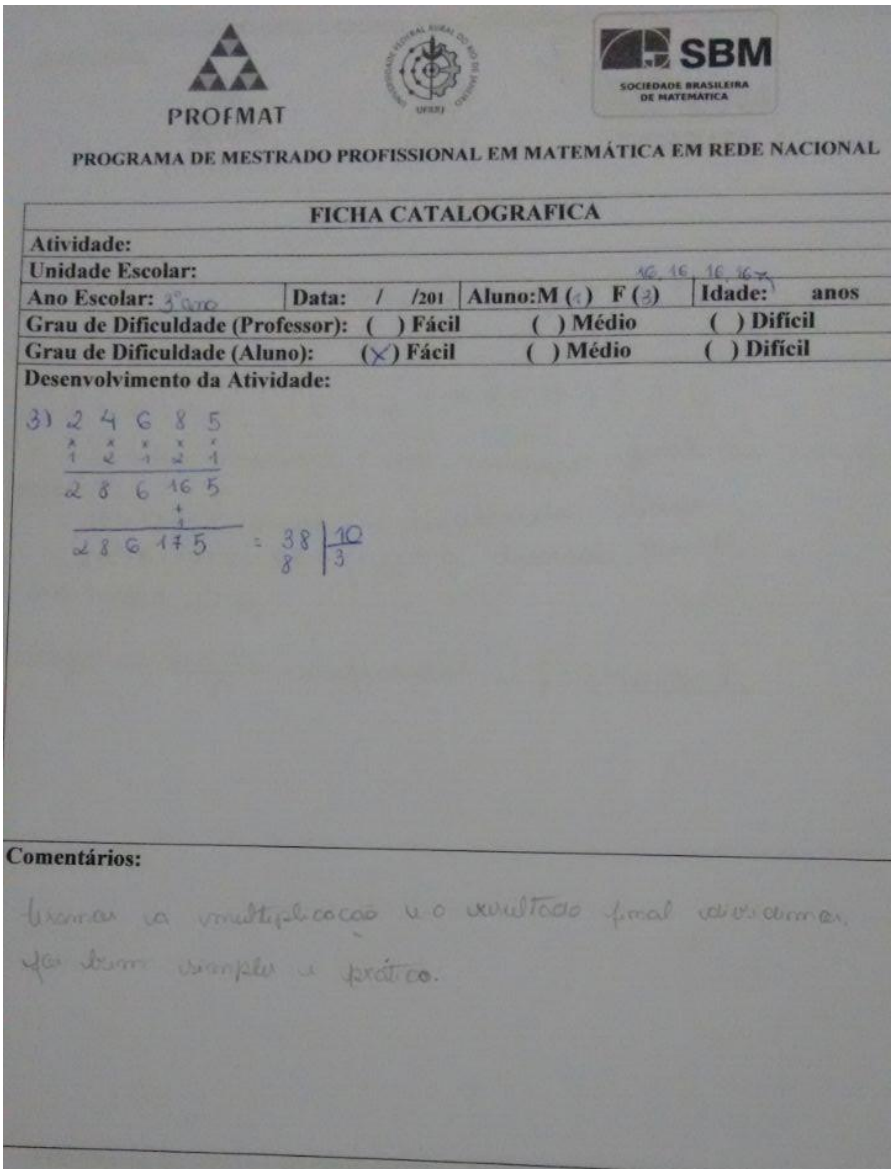
Para resolver esta atividade bastava que os alunos entendessem os métodos para descobrir o digito verificador de uma conta e trabalhar com o resto da

[3] Adaptação da Prova do ENEM 2005

divisão. A tabela a seguir representa a opinião dos grupos com relação ao grau de dificuldade da atividade.

TURMAS	FÁCIL	MÉDIO	DIFÍCIL
T1	5	5	2
T2	4	8	4
T3	5	9	0
TOTAL	14	22	6

Como essa atividade não exigia nenhum raciocínio bem elaborado, as respostas ficaram muito parecidas. Mesmo assim, encontramos respostas bem organizadas, como as que veremos a seguir.



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: 3°ano | **Data:** / /201 | **Aluno:** M (1) F (3) | **Idade:** 16, 16, 16, 16 anos

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): (X) Fácil ( ) Médio ( ) Difícil

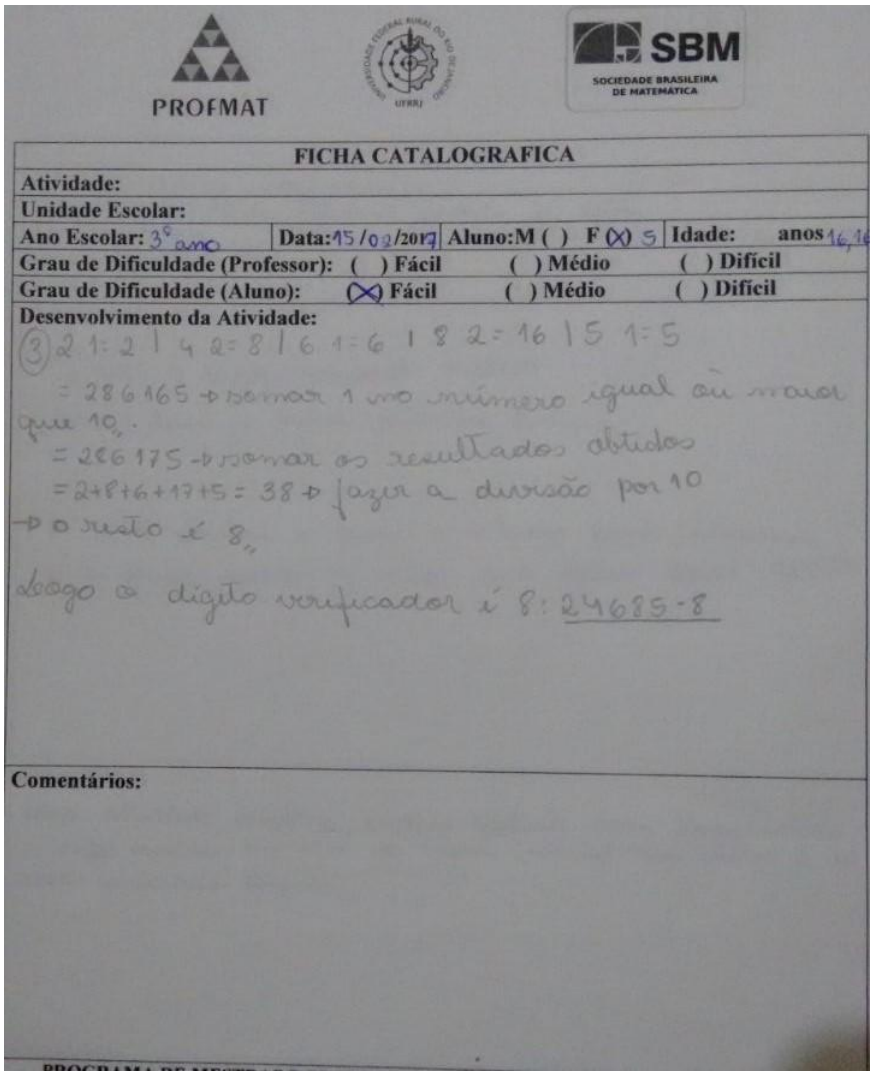
Desenvolvimento da Atividade:

3) 2 4 6 8 5
× 1 2 1 2 1
2 8 6 16 5
+ 1
2 8 6 17 5 = 38 | 10
8 | 3

Comentários:

Usamos a multiplicação e o resultado final dividimos, foi bem simples e prático.

Opinião do grupo sobre a atividade: “*Usamos a multiplicação e o resultado final dividimos foi bem simples a prática.*”



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: 3° ano | **Data:** 15/02/2017 | **Aluno:** M ( ) F (X) S | **Idade:** anos 16,16

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): (X) Fácil ( ) Médio ( ) Difícil

Desenvolvimento da Atividade:

③ 2 1:2 | 4 2=8 | 6 1=6 | 8 2=16 | 5 1=5

= 286165 → somar 1 no número igual ou maior que 10.

= 2861 75 → somar os resultados obtidos

= 2+8+6+17+5 = 38 → fazer a divisão por 10

→ o resto é 8.

Logo o dígito verificador é 8: 24685-8

Comentários:

A dúvida apresentada nesta atividade foi em relação ao resto da divisão. Afinal, os alunos estavam tentado descobrir o resto da divisão utilizando a calculadora, e não estavam acostumados a trabalhar com o resto da divisão para resolver situações envolvendo um problema matemático. Mas, após uma breve explicação essa dúvida foi esclarecida e todos os grupos conseguiram descobrir a solução.

6.1.4 Atividade 4 - CÓDIGO DOS METAIS[4]

Com a turma dividida em grupos, pedir que cada um descubra a regra do código.

Na lista, os numerais 24730; 4134; 63989; 50334 representam, em um determinado código, os nomes dos metais OURO; PRATA; COBRE; FERRO.

Se você decifrar este código, poderá usá-lo para escrever os nomes dos animais RATO; CABRA; FOCA; CARRAPATO; URUBU e dos vegetais: BATATA; CAFÉ; BETERRABA.

Poderá também traduzir uma mensagem escrita nesse código:

9393 9 80339 92933089 5938139

E, servir-se do código para transmitir uma outra mensagem:

O PORTO RECEBEU A FROTA E O BARCO PRETO ATRACOU.

Após esta descoberta, deixe que cada grupo crie seu *"código secreto"* e envie uma mensagem para outro grupo. Para tanto, cada letra do alfabeto terá seu valor numérico, ou seja: A = 1; B = 2; C = 3; D = 4; E = 5 e assim por diante.

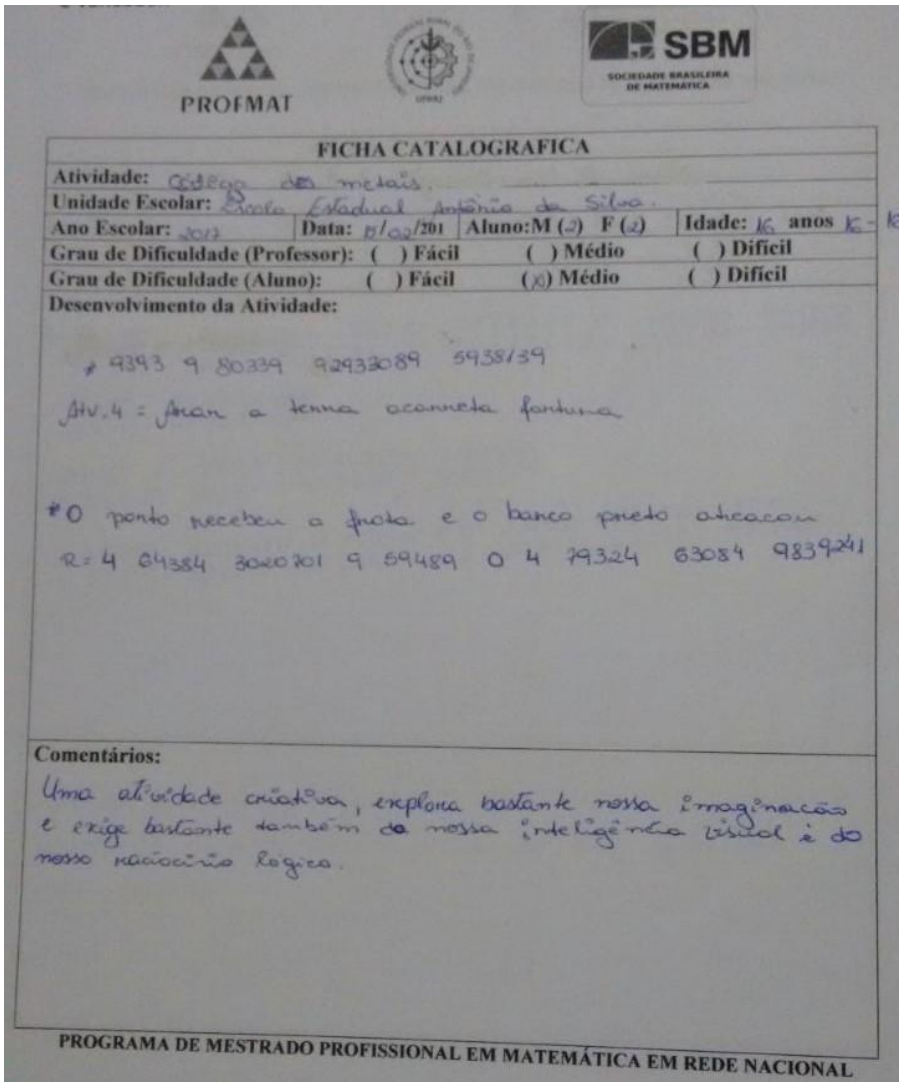
O grupo que decifrar a mensagem codificada com o maior valor numérico será o vencedor.

Para resolver esta atividade era necessário que os alunos compreendessem o enunciado e como funcionava o primeiro código e, depois, criar um código próprio para trocar informações entre eles. A tabela abaixo apresenta a opinião dos grupos com relação ao grau de dificuldade da atividade.

[4] Adaptação da atividade criada pela equipe de professores de Matemática do Centro de Ciências do Rio de Janeiro

TURMAS	FÁCIL	MÉDIO	DIFÍCIL
T1	5	5	2
T2	4	8	4
T3	5	11	0
TOTAL	14	24	6

Foi dificil encontrar um grupo que apresentasse uma resposta organizada para descoberta dos códigos. Após analisarmos cada ficha, consideramos as respostas a seguir como as mais significativas para apresentação do nosso trabalho.



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

FICHA CATALOGRAFICA

Atividade: Código de metais.

Unidade Escolar: Escola Estadual Antônio da Silva.

Ano Escolar: 2017 | **Data:** 15/02/201 | **Aluno:** M (✓) F (✓) | **Idade:** 16 anos

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

9393 9 80339 92933089 5938139

ATV.4 = Juan a terra acarreta fortuna

#O ponto recebeu a frota e o banco preto atacou

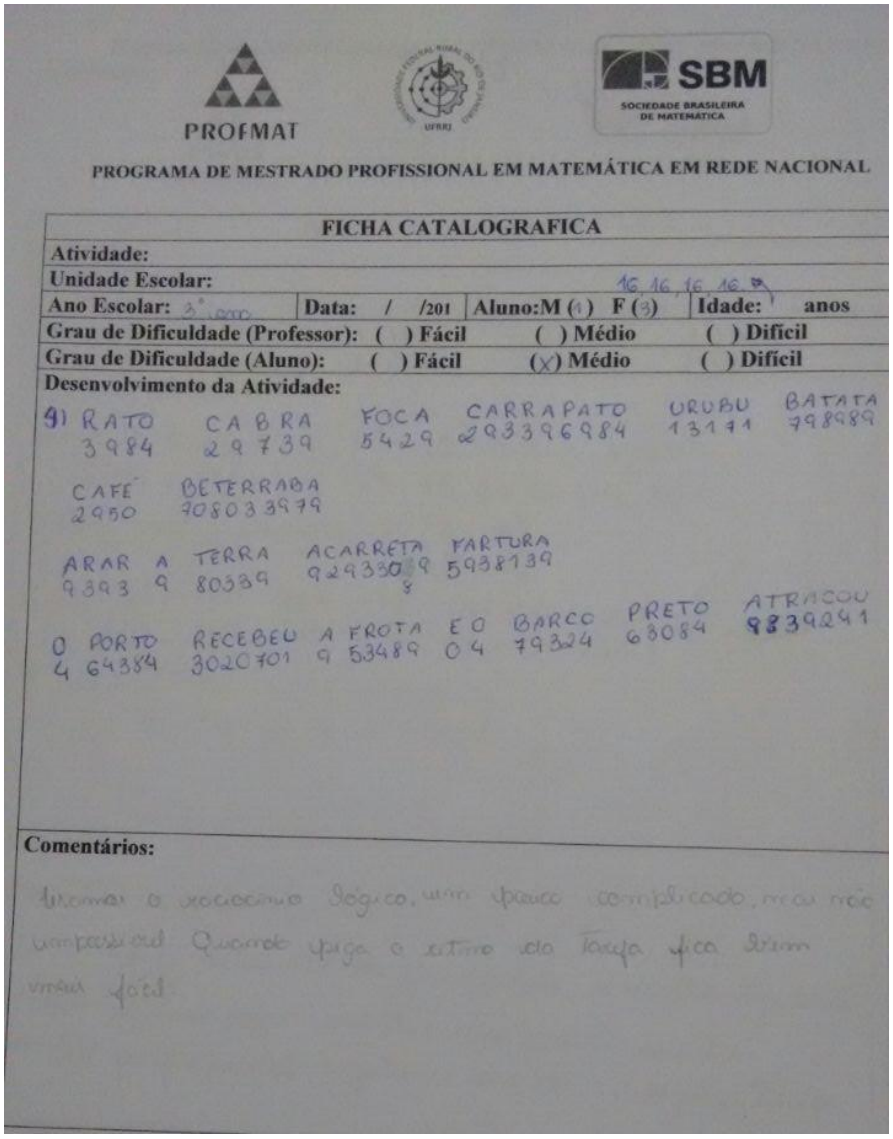
R= 4 64384 3020201 9 59489 0 4 79324 63084 9839241

Comentários:

Uma atividade criativa, explora bastante nossa imaginação e exige bastante também da nossa inteligência visual e do nosso raciocínio lógico.

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Comentário do grupo: "*Uma atividade criativa, explora bastante nossa imaginação e exige bastante também da nossa inteligência visual e do nosso raciocínio lógico.*"



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: 3° ano | **Data:** / /201 | **Aluno:M** (1) **F** (3) | **Idade:** 16, 16, 16, 16 anos

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

1) RATO 3984 CABRA 29739 FOCA 5429 CARRAPATO 293396984 URUBU 13141 BATATA 798989

CAFÉ 2950 BETERRABA 908033979

ARAR A TERRA 93939 80339 ACARRETA 92933089 FARTURA 5938139

O PORTO 4 64384 RECEBEU A FROTA 3020701 E O 9 53489 BARCO 04 79324 PRETO 63084 ATRACOU 98392491

Comentários:

Usamos o raciocínio lógico, um pouco complicado, mas não impossível Quando pega o ritmo da tarefa fica bem mais fácil.

Comentário do grupo: “*Usamos raciocínio lógico, um pouco complicado, mas não impossível quando pega o ritmo da tarefa fica bem mais fácil.*”

Durante a aplicação das atividades observamos que a grande dificuldade dos alunos foi interpretar o enunciado. Muitos deles ficaram confusos com o que era pedido e ficavam tentando descobrir qual conteúdo aprendido ao longo dos anos de estudo que teria que ser utilizado para obter a solução das atividades. Quando na verdade, não tinha uma única forma especifica de resolver essas atividades, o que causou grande estranheza por boa parte dos alunos. Mas, após uma discussão com eles, foi possível mostrar que todos tinham que ler, interpretar e compreender o que estava sendo pedido em cada atividade e, assim, procurar uma melhor solução.

No terceiro e último dia, aplicamos a quinta atividade. Nela relacionamos os conceitos de Criptografia com o de Matrizes, através de um aplicativo.

6.1.5 Atividade 5 - Criptografia utilizando Matrizes

Esta atividade tinha como proposta dar um significado ao ensino de Matrizes e seus conceitos. Para realizá-la é necessário que os alunos saibam os conceitos de Multiplicação de Matrizes e Matriz Inversa.

Segundo os alunos esta atividade foi considerada de médio para fácil.

TURMAS	FÁCIL	MÉDIO	DIFÍCIL
T1	4	0	0
T2	3	3	1
T3	2	3	1
TOTAL	9	6	2

Para resolver esta questão, fizemos uso de um aplicativo gratuito do celular, denominado *"Matrix Calculator"* ou *"Calculadora de Matrizes"*, que foi baixado em sala de aula durante a aplicação da atividade. Como o aplicativo é simples e de fácil manuseio, foi relativamente fácil para os alunos desenvolverem a atividade. Este fato causou muita estranheza por eles, pelo fato de estarmos utilizando o celular como ferramenta pedagógica para aprofundarmos o ensino de Matrizes.

De modo geral, a atividade foi bem recebida e mostrou para os alunos que a Criptografia não é algo que vemos apenas em filmes e programas de televisão, e que pode ser algo ao alcance de todos.

Como o conceito de Criptografia consiste em enviar mensagens utilizando códigos pré-estabelecidos entre as partes envolvidas, ou seja, entre o remetente e o destinatário. Essa atividade consiste em criar uma forma de trocarmos mensagens através de matrizes, onde uma delas é codificada com a mensagem e outra para decodificar a mensagem original.

Para maiores esclarecimentos dos alunos, fiz inicialmente uma exposição sobre o que é Criptografia e sua importância na atualidade. Como exemplo, citamos "código de barras", código Morse", "whatsapp". Em seguida, eles falaram que em filmes de espionagem este processo é muito utilizado.

O primeiro passo é estabelecer a relação entre os números e o alfabeto/caracteres:

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

A etapa posterior foi criamos as matrizes A e M, de modo que A seja uma matriz quadrada e inversível. Essa matriz é a que criará o código, ou seja, “matriz codificadora”. Teremos M como a matriz cujos elementos formam uma mensagem e, que A•M = C, sendo C a matriz com a mensagem decodificada. As matrizes A e C são conhecidas, logo usaremos a inversa de A para descobrir a mensagem original representada pela matriz M.

Temos que, $A \bullet M = C$ e $A^{-1} \bullet C = M$

Na Imagem 1 temos o layout do menu do celular antes de entrarmos no aplicativo Matrix Calculator.

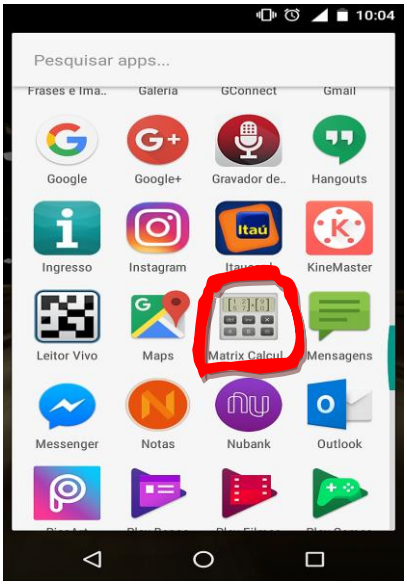


Imagem 1

Nas Imagens 2 e 3, respectivamente, temos como a tela do celular com o aplicativo quando está na horizontal e na vertical.

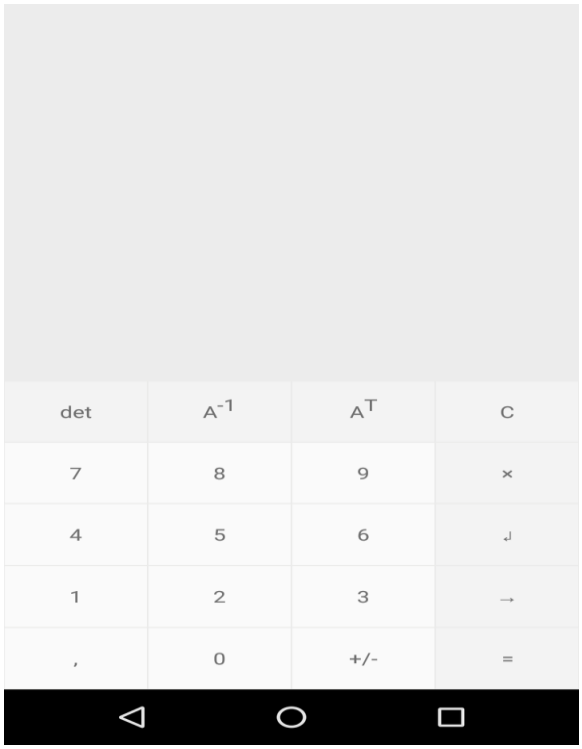


Imagem 2

Imagem 3

Entendendo a função de cada tecla:

- Det – calcula o determinante da matriz;
- A^{-1} – calcula a matriz inversa;
- A^{T} – calcula a matriz transposta;
- C – apaga os elementos da matriz;
- $\rightarrow$ - passa para o elemento seguinte da matriz;
- $\downarrow$ - acrescenta mais uma linha a matriz;
- LU – exibe uma matriz como o produto de duas matrizes;
- As demais teclas funcionam como em uma calculadora normal.

Para explicar o funcionamento do aplicativo, realizamos o seguinte exemplo: Mensagem: Oi, tudo bem?. Na forma matricial:

$$M = \begin{vmatrix} O & I & , & T & U & D & O \\ B & E & M & ? & \_ & \_ & \_ \end{vmatrix}$$

$$\text{Logo } M = \begin{vmatrix} 15 & 9 & 28 & 20 & 21 & 4 & 15 \\ 2 & 5 & 13 & 29 & 27 & 27 & 27 \end{vmatrix}$$

Seja $A = \begin{vmatrix} 2 & 3 \\ 4 & 5 \end{vmatrix}$, então $C = A \bullet M = \begin{vmatrix} 36 & 33 & 95 & 127 & 123 & 89 & 111 \\ 70 & 61 & 177 & 225 & 219 & 151 & 195 \end{vmatrix}$

Temos que $A^{-1} = \begin{vmatrix} -2{,}5 & 1{,}5 \\ 2 & -1 \end{vmatrix}$

Fazendo $A^{-1} \bullet C$, obtemos $\begin{vmatrix} 15 & 9 & 28 & 20 & 21 & 4 & 15 \\ 2 & 5 & 13 & 29 & 27 & 27 & 27 \end{vmatrix}$

Que é a matriz M, ou seja, a mensagem original: Oi, tudo bem?

Em seguida, demos início na aplicação da atividade e, para tanto, formamos grupos com, no máximo, quatro alunos. Cada grupo criou uma matriz M e após utilizar uma das codificadoras, passará para outro grupo a mensagem que precisará ser decodificada.

As Matrizes utilizadas para codificar as mensagens foram:

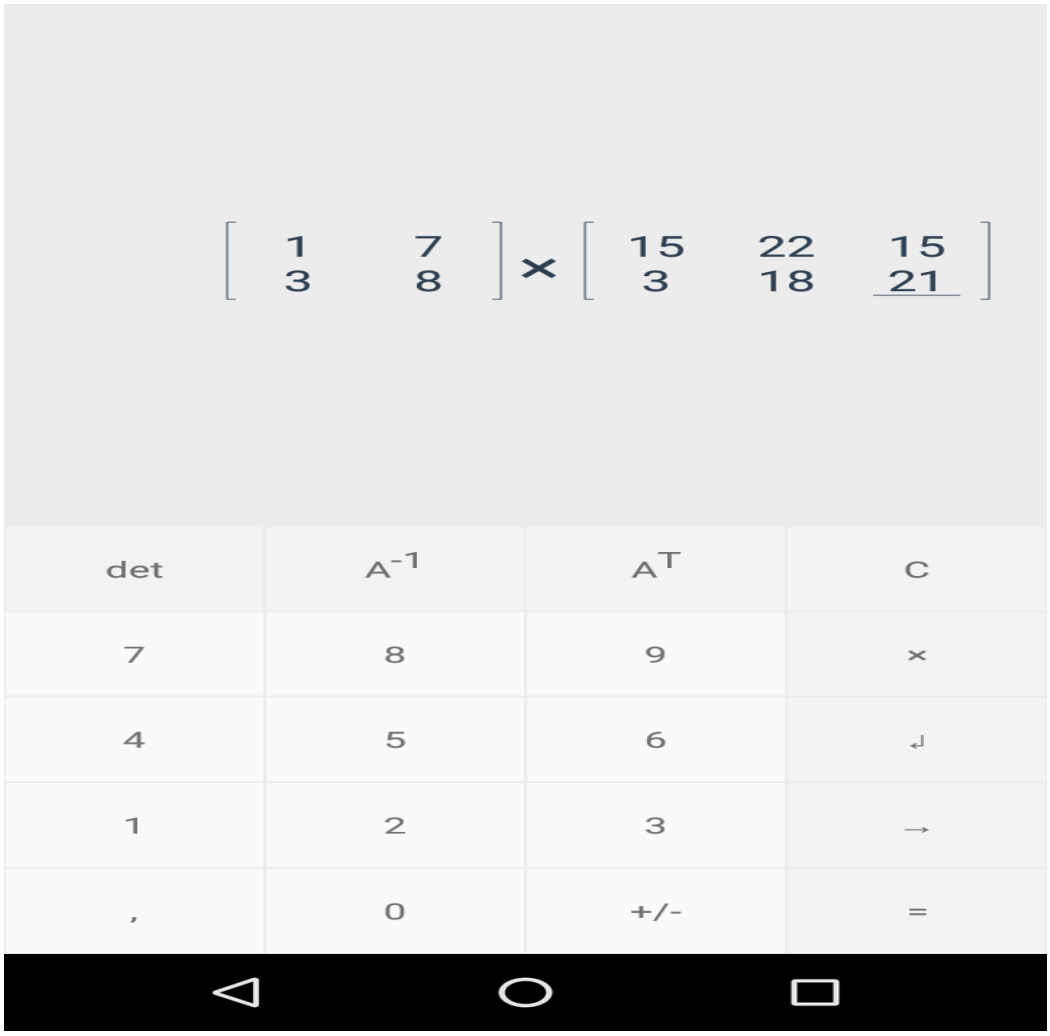
$$A = \begin{bmatrix} 1 & 7 \\ 3 & 8 \end{bmatrix},\ B = \begin{bmatrix} 1 & 0 \\ 4 & 6 \end{bmatrix},\ C = \begin{bmatrix} 5 & 1 \\ 1 & 6 \end{bmatrix},\ D = \begin{bmatrix} 3 & 4 \\ 10 & 0 \end{bmatrix}$$

No primeiro momento as matrizes codificadoras serão reveladas para os grupos que estão trocando mensagens. Aqui já foi apresentado o aplicativo para a turma e deixando-os familiarizados com o mesmo.

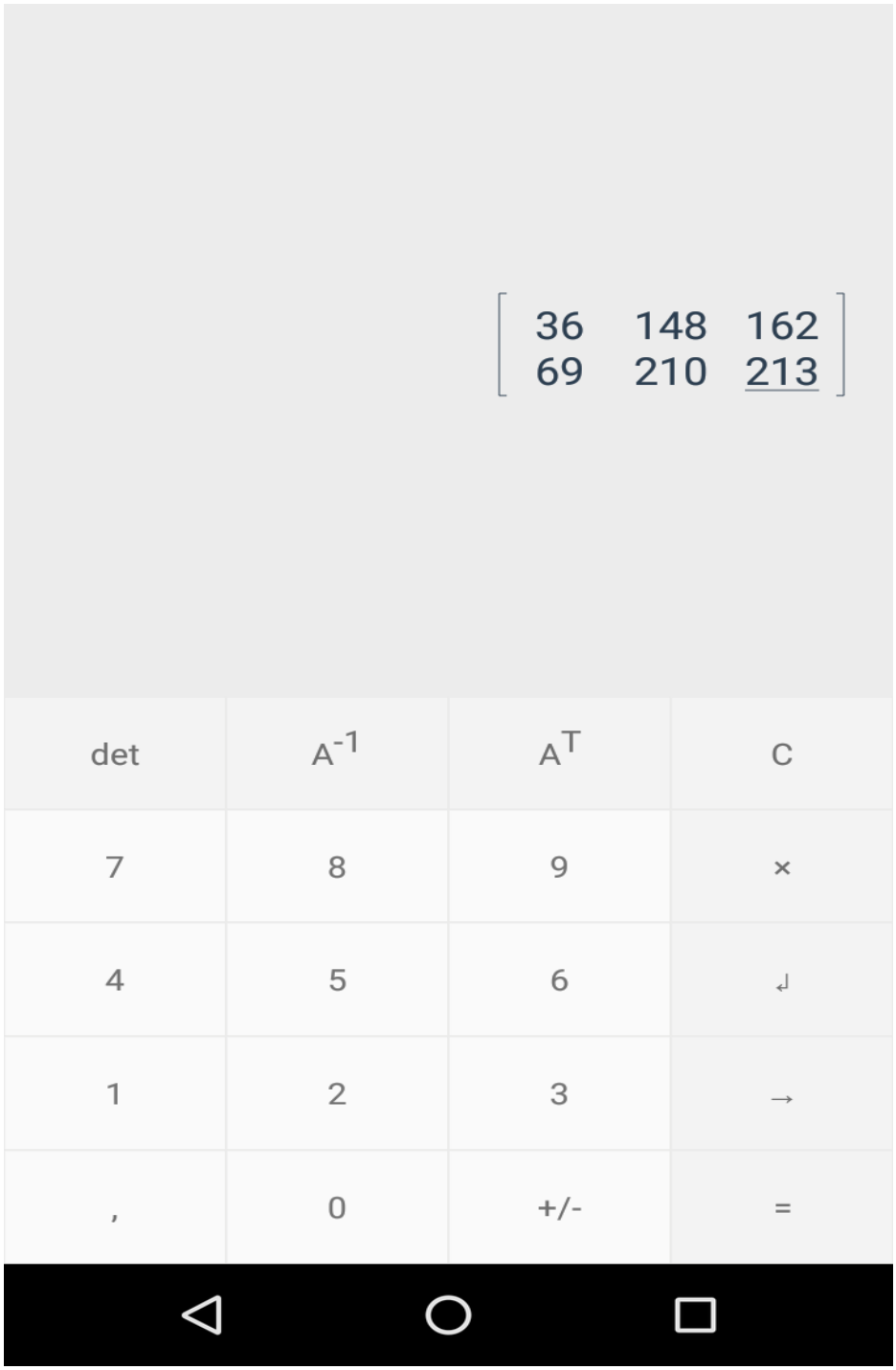
Em um segundo momento, uma nova mensagem será enviada entre os grupos. Para tanto, mantivemos as matrizes codificadoras, mas os grupos não devem revelar qual matriz codificadora foi usada. Este processo foi para mostrar as dificuldades que a Criptografia cria quando se deseja descobrir as mensagens trocadas entre os grupos.

Colocaremos imagens de como o aplicativo apresenta as operações com Matrizes. Temos a seguinte mensagem: $M = \begin{bmatrix} O & V & O \\ C & R & U \end{bmatrix} = \begin{bmatrix} 15 & 22 & 15 \\ 3 & 18 & 21 \end{bmatrix}$, para codificar a mensagem escolhemos a matriz A.

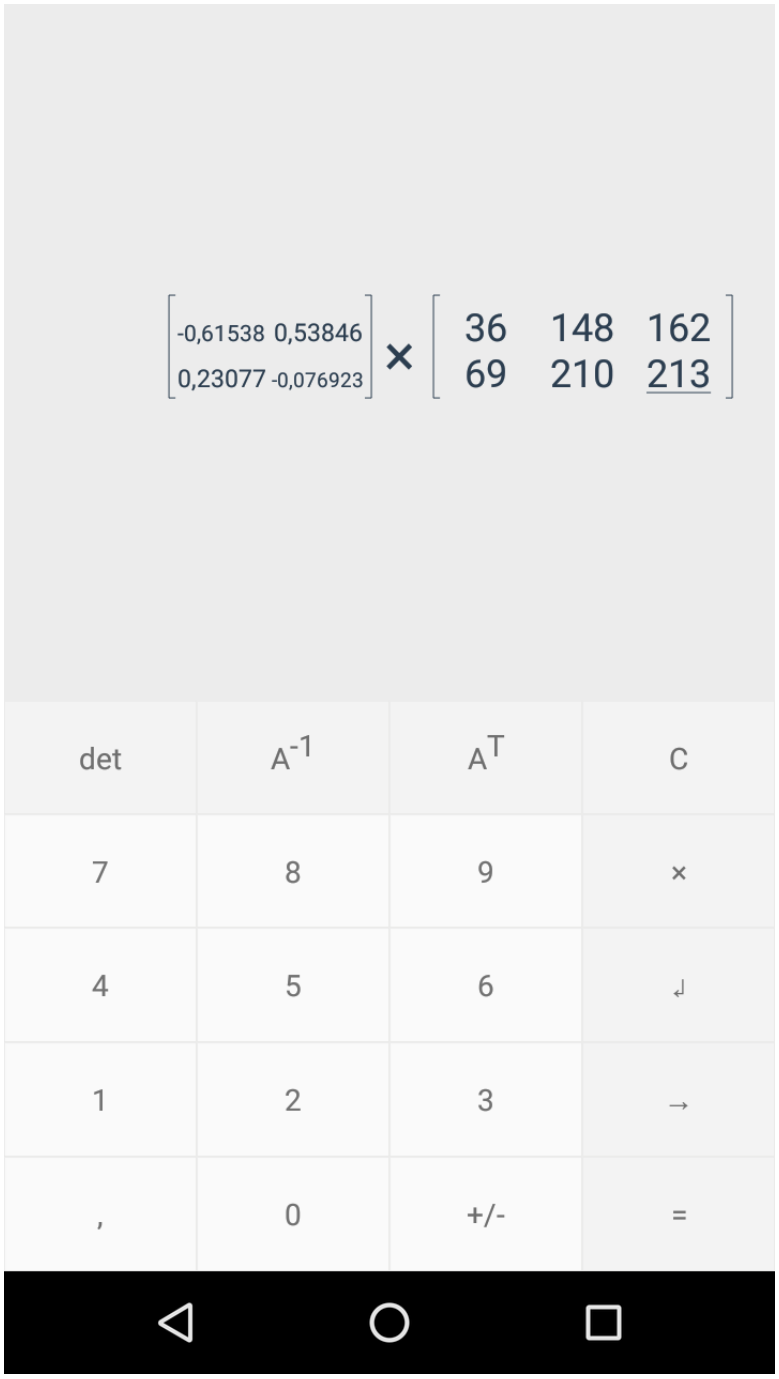
Na imagem temos A●M.



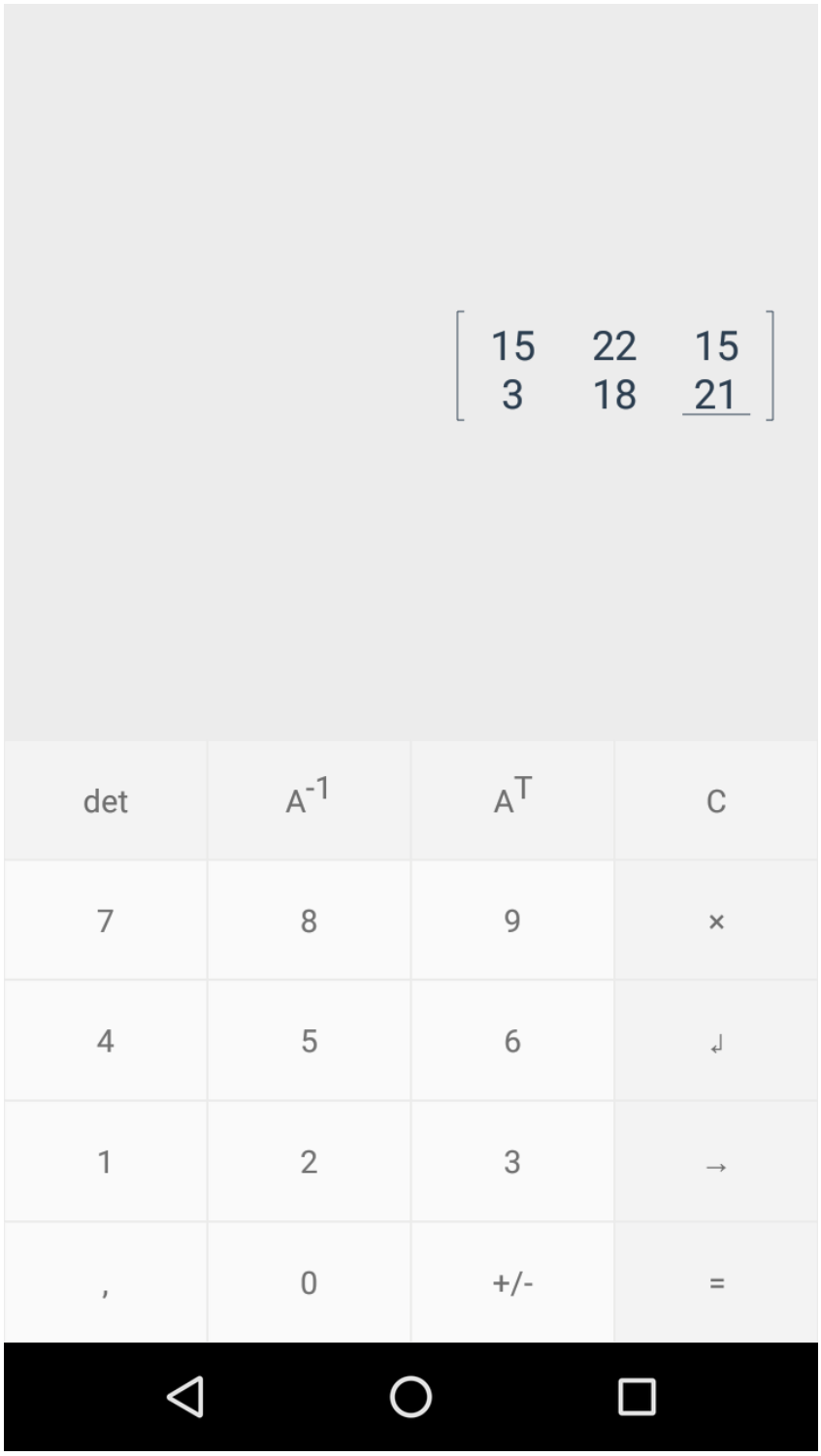
Na imagem seguinte temos o resultado de A●M = C



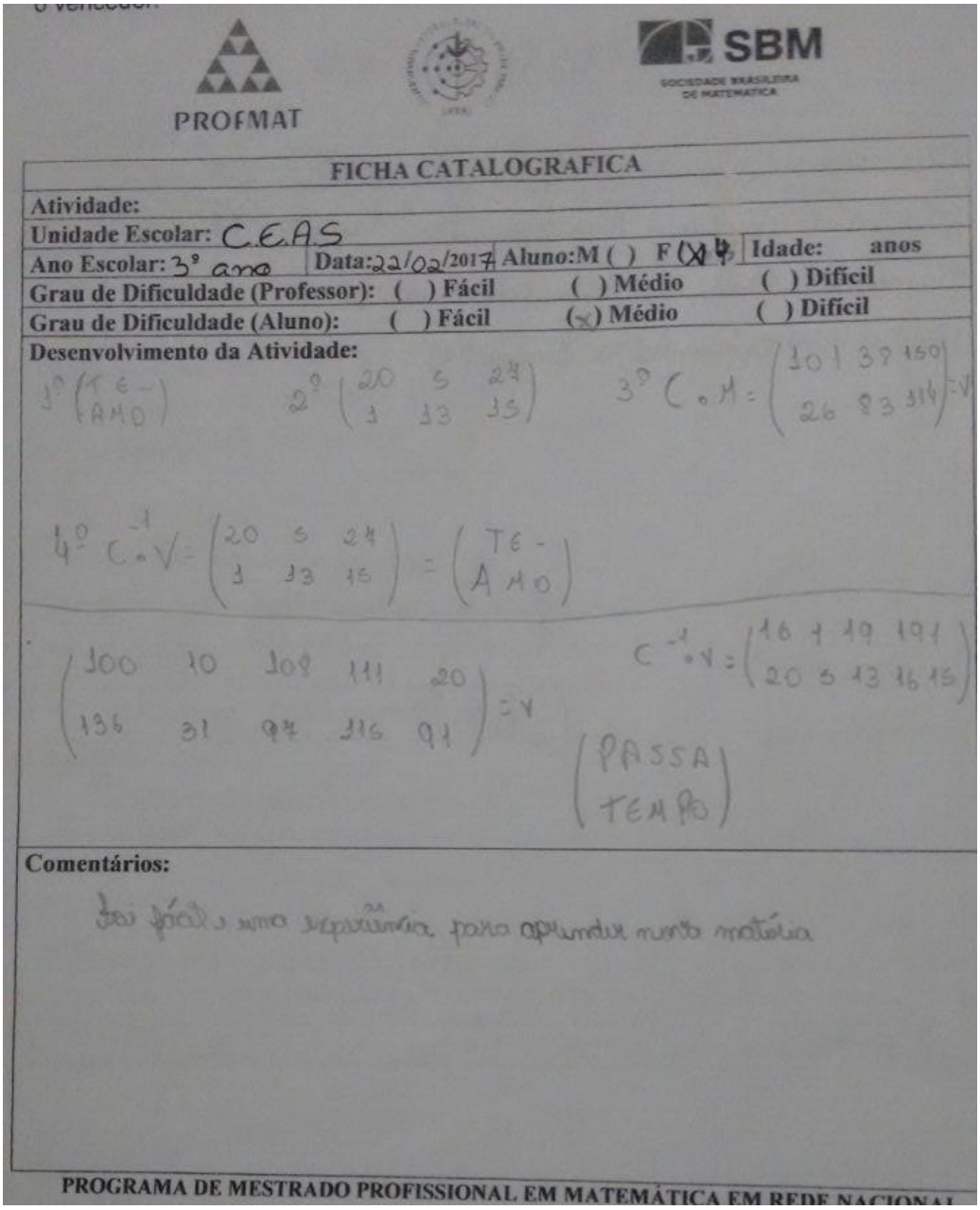
Nesta imagem temos $A^{-1} \bullet C$:



Resultado de $A^{-1} \bullet C = M$, sabemos que M representa a mensagem original $\begin{bmatrix} O & V & O \\ C & R & U \end{bmatrix}$.



Estas são algumas das respostas da atividade 5 apresentada pelos alunos:



PROFMAT

SBM
SOCIEDADE BRASILEIRA DE MATEMÁTICA

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar: C.E.A.S

Ano Escolar: 3° ano | **Data:** 22/02/2017 | **Aluno:** M ( ) F (X) | **Idade:** anos

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

1° (TE- / AMO) 2° $\begin{pmatrix} 20 & 5 & 24 \\ 1 & 13 & 15 \end{pmatrix}$ 3° C.M = $\begin{pmatrix} 101 & 37 & 150 \\ 26 & 83 & 316 \end{pmatrix}$ = V

4° $C^{-1}.V = \begin{pmatrix} 20 & 5 & 24 \\ 1 & 13 & 15 \end{pmatrix} = \begin{pmatrix} TE- \\ AMO \end{pmatrix}$

$\begin{pmatrix} 100 & 10 & 109 & 111 & 20 \\ 136 & 31 & 97 & 316 & 91 \end{pmatrix}$ = V

$C^{-1}.V = \begin{pmatrix} 16 & 1 & 19 & 191 \\ 20 & 5 & 13 & 16 & 15 \end{pmatrix}$

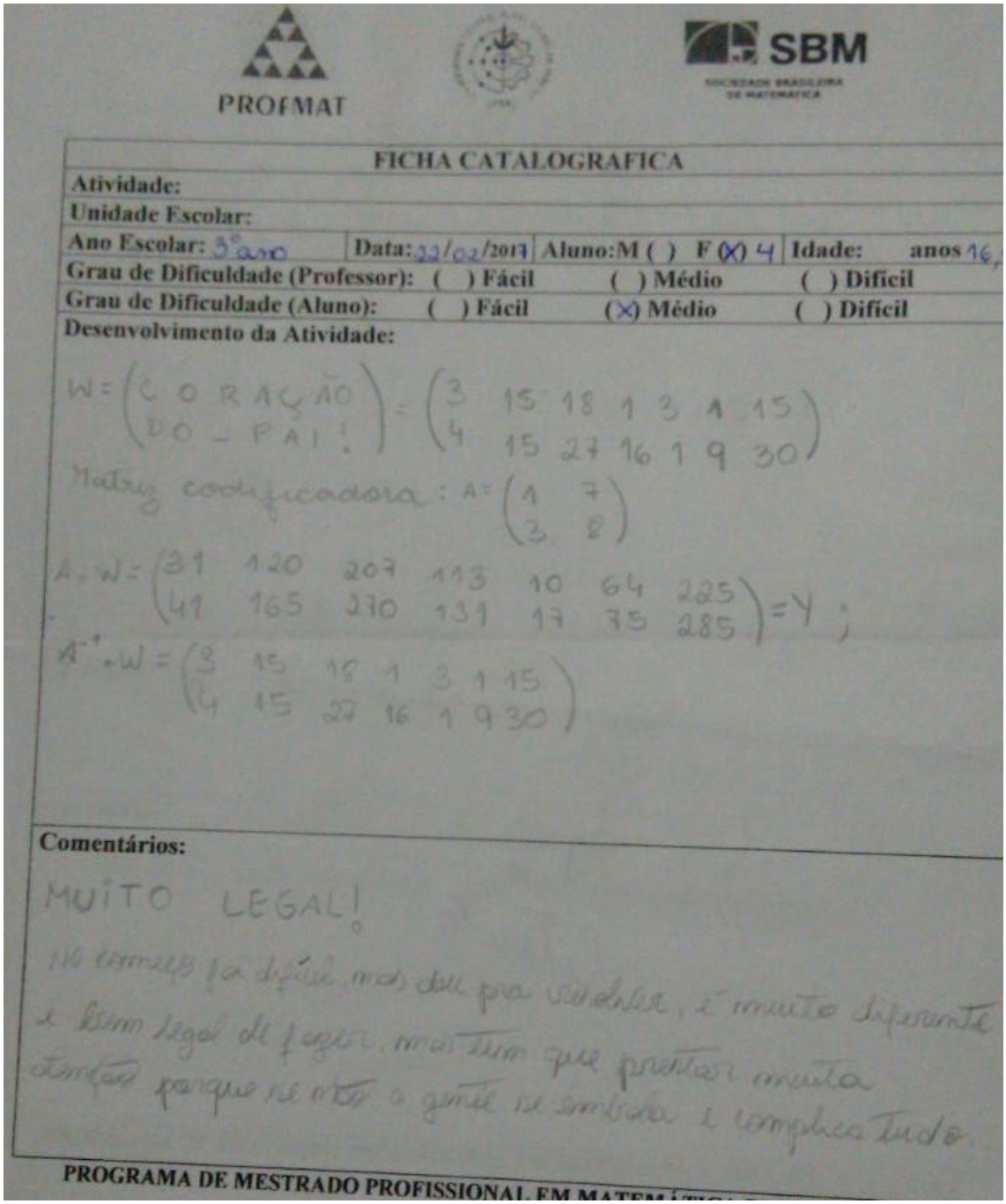
$\begin{pmatrix} PASSA \\ TEMPO \end{pmatrix}$

Comentários:

foi fácil e uma experiência para aprender nova matéria

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

Comentário do grupo: “*Foi fácil e uma experiência para aprender nova matéria*”.



PROFMAT

SBM

FICHA CATALOGRAFICA

Atividade:

Unidade Escolar:

Ano Escolar: 3° ano | Data: 22/02/2017 | Aluno: M ( ) F (X) 4 | Idade: anos 16

Grau de Dificuldade (Professor): ( ) Fácil ( ) Médio ( ) Difícil

Grau de Dificuldade (Aluno): ( ) Fácil (X) Médio ( ) Difícil

Desenvolvimento da Atividade:

$W = \begin{pmatrix} C & O & R & A & Ç & Ã & O \\ D & O & - & P & A & I & ! \end{pmatrix} = \begin{pmatrix} 3 & 15 & 18 & 1 & 3 & 1 & 15 \\ 4 & 15 & 27 & 16 & 1 & 9 & 30 \end{pmatrix}$

Matriz codificadora: $A = \begin{pmatrix} 1 & 7 \\ 3 & 8 \end{pmatrix}$

$A \cdot W = \begin{pmatrix} 31 & 120 & 207 & 113 & 10 & 64 & 225 \\ 41 & 165 & 270 & 131 & 17 & 75 & 285 \end{pmatrix} = Y$;

$A^{-1} \cdot W = \begin{pmatrix} 3 & 15 & 18 & 1 & 3 & 1 & 15 \\ 4 & 15 & 27 & 16 & 1 & 9 & 30 \end{pmatrix}$

Comentários:

MUITO LEGAL!

No começo foi difícil, mas deu pra resolver, é muito diferente e bem legal de fazer, mas tem que prestar muita atenção porque se não a gente se embola e complica tudo.

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEM

Comentário do grupo: "*MUITO LEGAL! No começo foi difícil, mas deu pra resolver, é muito diferente e bem legal de fazer, mas tem que prestar muita atenção porque se não a gente se embola e complica tudo.*"

Durante a aplicação, alguns grupos encontraram dificuldade em utilizar o aplicativo, mas depois de uma breve explicação conseguiram criar suas mensagens e codificá-las/decodificá-las.

Com esta atividade, podemos mostrar aos alunos como utilizar os conceitos aprendidos ao longo do ano letivo e como podem ser aplicados em algo do dia-a-dia

e como a Matemática tem seu caráter utilitário e, que vai além das paredes da sala de aula.

Acreditamos que esta atividade pode ser aplicada em turmas do 2º ano do Ensino Médio, quando estão estudando os conceitos de Matrizes, ou turmas do 3º ano do Ensino Médio, pois já estudaram Matrizes.

CONSIDERAÇÕES FINAIS

É impressionante como quando aplicamos uma atividade diferente durante a aula, os alunos agem com estranhamento. No início do ano letivo de 2017 aplicamos atividades diferenciadas para mostrar a importância de interpretar informações codificadas. Cada atividade tinha como objetivo estimular a interpretação e o que fazer diante de uma situação com códigos. Inicialmente, tínhamos a falta de interesse dos alunos achando que se tratava de mais do mesmo, mas conforme as atividades eram apresentadas cada uma com sua particularidade, eles iam mostrando interesse.

Com o entendimento de como seriam as aulas durante certo período, mostrarmos o conceito de Matrizes envolvendo Criptografia. Um assunto que faz parte do nosso dia-a-dia, mas que muitos só sabem que existe, mas não conhecem sua origem, “para quê foi criado?” e “onde podemos aplicar?”. Então, mostramos através das Matrizes que podemos criar uma Criptografia, dessa forma, esse conceito deixa de ser algo tão distante, que era apenas visto no cinema, ou programas de TV. Mas, que pessoas comuns podem criar seu próprio código, basta saber de qual maneira pode criá-lo.

Durante a aplicação da atividade nas turmas de 3º ano, alguns problemas apareceram, como o fato de não podermos escrever Matrizes muito grandes no aplicativo. Logo, não podemos enviar mensagens muito longas entre os grupos, o que não foi um problema, apenas tivemos que fazer pequenos ajustes na hora delas serem criadas.

Outro problema que surgiu durante a atividade, foi com relação aos resultados que não eram números inteiros após multiplicarmos pela Matriz Inversa. Mas, isso aconteceu por causa de problemas de arredondamento de resultados por parte do aplicativo. Também tivemos inicialmente o uso de uma matriz decodificadora que não era inversível, consequentemente não era possível descobrir a mensagem inicial, já que precisamos da Matriz Inversa.

Mesmo com esses imprevistos, os alunos entenderam a proposta, conseguiram enviar e codificar mensagens entre eles atividade e como possível criar seu próprio código. Gerando um resultado satisfatório, pois despertou o cuidado que

temos que ter ao ler as informações para podermos interpretá-las, o que tem ajudado bastante durante o restante do ano letivo.

Essa atividade não precisa ser apenas destinada para turmas de 3º ano, mas também para turmas de 2º ano, já que nessa série apresentamos os conceitos de Matrizes, Operações com Matrizes, Determinante e Matriz Inversa, conceitos necessários para aplicação dessa atividade relacionando Matrizes com Criptografia.

.

REFERÊNCIAS BIBLIOGRÁFICAS

BARBOSA, J. C. Modelagem Matemática: O que é? Por que? Como? Veriatati, n.4, p.73 – 80, 2004 http://www.uefs.br/nupemm/publicacoes.html

BASSANEZI, R. C. Ensino-aprendizagem com modelagem matemática: uma nova estratégia. 2 ed. São Paulo: Contexto, 2004.

_____. Modelagem Matemática: teoria e prática. São Paulo: Contexto, 2015.

BRASIL. Ministério da Educação. Parâmetros Curriculares Nacionais: matemática (1ª a 4ªséries). Brasília: MEC/SEF, 1997

_____ . Ministério da Educação. Parâmetros Curriculares Nacionais: Matemática (5ª a 8ª séries). Brasília, MEC/SEF, 1998.

_____. Ministério da Educação. Parâmetros Curriculares Nacionais: ensino médio: ciências da natureza, matemática e suas tecnologias. Brasília: MEC / SEMT, 1999.

CAMPOS, Carlos Eduardo de Souza. Musicalizando a escola: música, conhecimento e educação. São Paulo: Escrituras, 2008.

D' AMBRÓSIO, U. Da realidade à Ação: Reflexões sobre a Educação Matemática. Campinas: Editora da UNICAMP, 1986.

DANTE, Luiz Roberto, Matemática: Contexto & aplicações. 2ª ed. Ed Ática, 2014.

DE MELO, Clarissa Duarte Loureiro. Criptografia no Ensino Médio: uma proposta para o ensino de Matrizes. Universidade do Estado do Rio de Janeiro, 2014.

EVES, Howard, **Introdução à história da Matemática**. Ed. Unicamp, 2008.

FIARRESGA, Victor Manuel Calhabrês. Criptografia e Matemática, Lisboa [Mestrado em Matemática para Professores], Faculdade de Ciências da Universidade de Lisboa, 2010.

FIDELIS, Reginaldo; ALMEIDA, Lourdes M. W. Modelagem Matemática em sala de aula: contribuições para competência de refletir-na-ação. Disponível em:<http:/www.sbempaulista.org.br/epem/anais/Comunicacoes_Orais/co0080.doc> Acesso em: 24 mar 16

LOUREIRO, Flávio Ornellas. Tópicos de Criptografia para o ensino médio. Universidade Estadual do Norte Fluminense Darcy Ribeiro, 2014.

MOREIRA, M. A. A teoria da aprendizagem significativa e sua implementação em sala de aula. Brasília: Editora Universidade de Brasília, 2006

PAIVA, Manoel, Matemática. 1ª edição. Ed. Moderna, 2009.

SOUZA, Jaibis Freitas. Construindo uma aprendizagem significativa com história e contextualização da Matemática. Dissertação de mestrado em Ciências. Seropédica: Instituto de Agronomia, UFRRJ, 2009.

XAVIER, Cláudio, BARRETO, Benigno, Matemática: Aula por Aula. 2ª ed. Renovada, 2005.

http://www.mat.ufrgs.br/~portosil/passa3b.html 2/11/2016

http://wwwp.fc.unesp.br/~lfcruz/AL_CAP_01.pdf 09/01/2017

http://projetos.unioeste.br/cursos/cascavel/matematica/xxiisam/artigos/16.pdf 09/01/2017

https://www.ucb.br/sites/100/103/TCC/22005/WaldizarBorgesdeAraujoFranco.pdf
09/01/2017