

UNIVERSIDADE FEDERAL DE SÃO CARLOS

REINALDO DONIZETE DE OLIVEIRA

**UTILIZAÇÃO DE MENSAGENS CRIPTOGRAFADAS NO ENSINO DE
MATRIZES**

São Carlos

2013

UNIVERSIDADE FEDERAL DE SÃO CARLOS

REINALDO DONIZETE DE OLIVEIRA

**UTILIZAÇÃO DE MENSAGENS CRIPTOGRAFADAS NO ENSINO DE
MATRIZES**

Dissertação de mestrado profissional apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Orientação:
Prof. Dr. Márcio de Jesus Soares

São Carlos

2013

**Ficha catalográfica elaborada pelo DePT da
Biblioteca Comunitária da UFSCar**

O48um Oliveira, Reinaldo Donizete de.
Utilização de mensagens criptografadas no ensino de matrizes / Reinaldo Donizete de Oliveira. -- São Carlos : UFSCar, 2013.
82 f.

Dissertação (Mestrado profissional) -- Universidade Federal de São Carlos, 2013.

1. Matrizes (Matemática). 2. Ensino médio. 3. Criptografia.
I. Título.

CDD: 512.9434 (20^a)

REINALDO DONIZETE DE OLIVEIRA

**UTILIZAÇÃO DE MENSAGENS CRIPTOGRAFADAS NO ENSINO DE
MATRIZES**

Dissertação de mestrado profissional apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da Universidade Federal de São Carlos, como parte dos requisitos para obtenção do título de Mestre em Matemática.
21 de março de 2013.

ORIENTADOR:



Prof. Dr. Márcio de Jesus Soares
Universidade Federal de São Carlos, UFSCar/São Carlos

EXAMINADORES:



Prof. Dr. Jamil Viana Pereira
Universidade Estadual de São Paulo, UNESP/Rio Claro



Prof. Dr. João Carlos Vieira Sampaio
Universidade Federal de São Carlos, UFSCar/São Carlos

*Dedico este trabalho à minha família,
por estarem comigo me apoiando e me
fortalecendo nos momentos de fraqueza e
nas vitórias alcançadas ao longo dessa
trajetória.*

“Escrevo para que o aprendiz possa sempre aperceber-se do fundamento interno das coisas que aprende, de tal forma que a origem da invenção possa aparecer e, portanto, de tal forma que o aprendiz possa aprender tudo como se o tivesse inventado por si próprio.”

(Gottfried Wilhelm von Leibniz)

AGRADECIMENTOS

A Deus, que me conduziu por estes caminhos surpreendentes e que, a cada dia de Profmat, renovou minhas forças para a conclusão dessa caminhada.

A toda minha família, que me apoiou em todos os momentos, sempre com a maior paciência do mundo, me confortando em todos os momentos.

A meus filhos Rafael, Melissa e Maria Fernanda, que mesmo com pouca idade entenderam minha dedicação a esse Mestrado e, com nobreza, souberam esperar e compreenderam minha ausência em momentos importantes de suas vidas.

Aos meus queridos professores do Profmat UFSCar, que, com toda sabedoria e disposição, contribuíram de maneira grandiosa para minha formação.

Ao meu orientador, Professor Doutor Márcio de Jesus Soares, que desde o primeiro momento me atendeu com presteza, humildade, paciência e conhecimento, conduzindo-me de maneira sólida e eficaz desde o início .

Aos meus amigos do mestrado, que dividiram comigo suas angústias, alegrias e seus conhecimentos, indispensáveis ao meu crescimento como professor e como pessoa.

À direção, coordenação, professores e alunos da Escola Estadual Esmeralda Soares Ferraz, que me apoiaram e me acompanharam em todas as fases desse curso.

RESUMO

O presente trabalho tem como objetivo mostrar a elaboração e realização de uma Engenharia Didática sobre o uso de mensagens criptografadas no ensino de matrizes com alunos do 2º ano do Ensino Médio da Escola Esmeralda Soares Ferraz na Cidade de Ourinhos-SP. Esse trabalho inicia-se com um questionamento sobre o desânimo e a apatia dos alunos em estudar Matemática e sugere, abordando o ensino de matrizes através de mensagens criptografadas por transposição de letras, uma abordagem diferente daquela aplicada no cotidiano, através da qual, o aluno, no anseio de solucioná-las, se empenhe e se interesse em aprender de forma simples os conceitos de matrizes e matrizes transpostas, sendo protagonista de sua busca pelo conhecimento.

Palavras-chave: Ensino Médio. Matrizes. Criptografia. Mensagens.

ABSTRACT

The present work aims at showing the development and implementation of a Didactic Engineering on the use of encrypted messages in teaching matrices to students who are attending the second high school year at Esmeralda Soares Ferraz School in the City of Ourinhos-SP. This work begins with a question related to the discouragement and apathy of students in studying mathematics and suggests, taking the teaching of matrices through encrypted messages by transposition of letters, a different approach from those commonly applied, through which, the student eager to solve them, will get engaged and interested in learning, in a simple way, the concepts of matrices and transposed matrices, being protagonist of his/her search for knowledge.

Key-words: High School. Matrices. Encrypted Messages.

TRAJETÓRIA

Minha jornada no magistério se iniciou no ano de 1995, com o Curso de Ciências Biológicas na Faculdade Estadual de Filosofia, Ciências e Letras de Jacarezinho. Posteriormente fiz Habilitação em Matemática, terminando esse curso no ano de 2002.

Em 2004, finalmente, ingressei na Profissão de Professor de Matemática, sendo efetivado na Secretaria de Educação do Estado de São Paulo, no ensino básico, na Escola Estadual Esmeralda Soares Ferraz, em Ourinhos-SP, onde leciono até hoje.

De 2005 a 2007, completei meus estudos na mesma faculdade fazendo uma pós graduação em Educação Matemática (Latu-senso).

A partir de 2006 comecei a trabalhar também em escolas particulares na cidade de Ourinhos, onde temos realidades diferentes do ambiente escolar das escolas estaduais.

Com o passar dos anos, veio a necessidade de mudanças, de algo que extrapolasse as barreiras escolares, visto que a motivação à prática do magistério estava diminuindo.

Na busca por algo diferente, mais avançado, descobri o Profmat, um curso novo que parecia atender aos meus anseios. Já na primeira tentativa, em 2011, ingressei no Profmat. Com o passar dos meses e o andamento do curso, pude verificar como estava aquém do ideal em relação ao conhecimento matemático e como a escola básica (ensino fundamental e médio) estava longe do praticado no Profmat, ou seja, haviam lacunas enormes entre os conteúdos acadêmicos e os praticados por mim na atividade docente.

Vários foram os assuntos estudados no decorrer desses dois anos de Profmat. Alguns já conhecidos, mas sem a profundidade adequada e outros novos e surpreendentes, como Geometria Analítica no espaço, Aritmética dos números inteiros, etc.

Finalmente, com a conclusão do Profmat, torna-se claro a ideia de que o conhecimento não tem limite, que o aperfeiçoamento faz-se necessário constantemente e que quanto mais estamos em contato com essa nobre ciência, mais temos a noção de sua beleza e de sua importância em nossas vidas.

LISTA DE FIGURAS

| | |
|--|----|
| Figura 1: Quadrado Mágico de Lo Shu..... | 32 |
| Figura 2: Quadrado Mágico de Lo Shu com cordas..... | 32 |
| Figura 3: Slide desafio inicial..... | 49 |
| Figura 4: Slide Transposição..... | 49 |
| Figura 5: Slide Definição e exemplo de matrizes..... | 50 |
| Figura 6: Slide Tabela com a mensagem original..... | 50 |
| Figura 7: Slide Matriz transformação..... | 51 |

LISTA DE TABELAS

| | |
|--------------------------------------|----|
| Tabela 1: Matriz 1×20 | 39 |
| Tabela 2: Matriz 20×1 | 40 |
| Tabela 3: Matriz 4×5 | 40 |
| Tabela 4: Mensagem inicial..... | 40 |
| Tabela 5: Matriz transformadora..... | 41 |
| Tabela 6: Matriz 2×10 | 41 |
| Tabela 7: Matriz 10×2 | 42 |
| Tabela 8: Matriz 5×4 | 42 |
| Tabela 9: Matriz reveladora..... | 43 |

LISTA DE FOTOGRAFIAS

| | |
|---|----|
| Fotografia 1: Decomposição numérica e mensagem revelada..... | 46 |
| Fotografia 2: Produtos..... | 47 |
| Fotografia 3: Utilização da matriz transposta..... | 47 |
| Fotografia 4: Mensagem criptografada proposta pelos alunos..... | 48 |
| Fotografia 5: Mensagem criptografada proposta pelos alunos..... | 48 |

SUMÁRIO

| | |
|--|----|
| INTRODUÇÃO | 25 |
| CAPÍTULO 1: APONTAMENTOS | 27 |
| 1.1 INÍCIO DOS TRABALHOS | 27 |
| 1.2 OBJETIVOS..... | 28 |
| 1.3 ENGENHARIA DIDÁTICA | 29 |
| CAPÍTULO 2: ANÁLISES PRÉVIAS | 31 |
| 2.1 ANÁLISE HISTÓRICA..... | 31 |
| 2.1.1 MATRIZES | 31 |
| 2.1.2 CRIPTOGRAFIA | 33 |
| 2.2 ANÁLISE DIDÁTICA..... | 34 |
| 2.2.1 IMPORTÂNCIA DO ESTUDO DE MATRIZES..... | 35 |
| 2.3 ANÁLISE COGNITIVA..... | 35 |
| CAPÍTULO 3: ANÁLISE A PRIORI | 37 |
| CAPÍTULO 4: EXPERIMENTAÇÃO | 45 |
| CAPÍTULO 5: ANÁLISE A POSTERIORI E VALIDAÇÃO | 53 |
| CONCLUSÃO | 55 |
| REFERÊNCIAS..... | 57 |
| APÊNDICE A : LISTA COM DITADOS POPULARES UTILIZADOS NA AULA..... | 59 |
| APÊNDICE B: MENSAGENS CRIPTOGRAFADAS PELOS ALUNOS | 61 |
| APÊNDICE C: RELATORIO REALIZADO PELOS ALUNOS NO FINAL DAS ATIVIDADES..... | 69 |
| APÊNDICE D SEQUÊNCIA DE SLIDES DA AULA | 73 |

INTRODUÇÃO

A dissertação aqui apresentada é uma aplicação da criptografia como recurso no ensino de matrizes, utilizando para isso uma prática de ensino embasada em princípios da Engenharia Didática.

Engenharia Didática é uma metodologia de pesquisa e teoria educacional criada na França nos anos 80, que é inspirada na atividade do engenheiro e é utilizada por educadores e profissionais de ensino. O trabalho de um pesquisador é baseado em um conhecimento sólido, mas o de um professor é fundamentado em sala de aula.

No capítulo 1 discorreremos sobre os objetivos desse trabalho, a Engenharia Didática e suas nuances, criptografia, transposição e matrizes.

No capítulo 2, nosso foco recai sobre as análises prévias do nosso trabalho, cujo objetivo é verificar o atual funcionamento do ensino e prática dos conteúdos para que, se necessário sejam propostas e efetivadas melhorias na transmissão e realização do conhecimento.

No capítulo 3, análise a priori, nosso raciocínio está voltado para as escolhas das variáveis locais e as características da aula a ser desenvolvida, a importância do tema para o aluno, prevendo os possíveis comportamentos, e as hipóteses do nosso trabalho.

No capítulo 4 ocorre a experimentação, fase na qual é relatada a aplicação da aula.

No capítulo 5, Análise a posteriori, verificaremos o funcionamento da aula, se houveram ou não resultados favoráveis. Ocorrerá a verificação das hipóteses e a sugestão das modificações. Também é descrito nesse capítulo a conclusão do trabalho.

Por fim temos o Apêndice, onde estão elencados os trabalhos realizados pelos alunos, a lista de ditados populares utilizados nas aulas, os relatórios produzidos pelos alunos e a aula aplicada em forma de slides no data show.

CAPÍTULO 1: APONTAMENTOS

Neste capítulo apresentaremos um breve relato de como escolhemos esse tema, sobre os objetivos do trabalho e sobre Engenharia Didática.

1.1 Início dos trabalhos

Durante o tempo em que estou em sala de aula, aproximadamente 9 anos, foi verificado que a cada ano que passa, o interesse dos alunos pelas aulas diminui. Estamos diante de salas de aula compostas por muitos alunos apáticos, que não se interessam pelo que é proposto pelo professor. Isso gera um desgaste muito grande entre o corpo docente e discente, que se nega a pensar e, na maioria das vezes, no máximo copiam conteúdos da lousa, sem ao menos entenderem o que está escrito ali, ou para que servem. Também se negam a discutir e opinar, na maioria das vezes, sobre os temas e assuntos propostos por nós professores.

Incomodado com essa situação, após refletir muito sobre tais comportamentos, queria achar uma saída fácil que rompesse com essa apatia por parte dos alunos. Para um aluno que está cursando o 2º Ano do Ensino Médio, ele está pelo menos há dez anos na escola, assistindo e participando de seis aulas por dia, durante duzentos dias letivos por ano, ou seja, aproximadamente doze mil aulas ou 10000 horas. Esse tempo é necessário para o desenvolvimento intelectual do ser humano nos dias de hoje, mas verifica-se que uma parcela dos alunos não aproveitam esse tempo adequadamente.

O grande desafio era: como aplicar algum desses assuntos na sala de aula do Ensino Médio de maneira fácil, prazerosa e com uma abordagem diferente?

As ideias foram surgindo, até que no Módulo de Matemática e Atualidades, ministrado pelo Professor Pedro Malagutti no Profmat, fiz um trabalho sobre Criptografia, especificamente sobre a transposição de letras e a encriptação de mensagens.

Fiquei encantado com o tema. Conversando com os professores Pedro Malagutti e Márcio de Jesus Soares e com meus amigos de curso fui amadurecendo a ideia. Queria usar a transposição de letras no 2º Ano do Ensino Médio. De acordo com a Grade Curricular do Estado de São Paulo, trabalhamos no 2º ano do Ensino

Médio Matrizes, Determinantes, Probabilidade, Análise Combinatória, Geometria Espacial e Trigonometria. A Criptografia de Mensagens foi utilizada no ensino de Matrizes e Matrizes Transpostas, como veremos a seguir.

A construção deste trabalho teve origem no endereço eletrônico <http://www.cimt.plymouth.ac.uk/resources/codes/default.htm> que corresponde ao Bletcheley Park, um centro de códigos, uma antiga estação militar localizada em Bletcheley, na Inglaterra, na qual se realizavam os trabalhos de decifração de códigos alemães durante a Segunda Guerra Mundial. Utilizando-se das informações contidas nesse sítio, e de alguns outros materiais sobre criptografia e também livros didáticos de Ensino Médio, juntamente com o Currículo de Matemática praticado no Estado de São Paulo, montamos essa aula.

1.2 Objetivos

Um dos objetivos a ser alcançado na referida aula é o de mostrar que os alunos desinteressados, estão ali, alertas e esperando algo novo, diferente do que presenciaram até o momento, algo que chame a atenção e os coloque para trabalhar, para produzir.

Outro objetivo é mostrar que a Matemática não é desinteressante e evasiva, mas sim uma disciplina dinâmica, que pode ser trabalhada de forma interessante e diferente das apresentadas e que serve como ferramenta para a resolução de problemas de várias situações do nosso cotidiano.

Antes de iniciar a aula, foram verificados alguns dos objetivos do ensino de matemática no nível médio de acordo com os Parâmetros Curriculares Nacionais (PCN), que tem como finalidades levar os alunos a:

- compreender conceitos, procedimentos e estratégias matemáticas que permitam a ele desenvolver estudos posteriores e adquirir uma formação científica geral;
- aplicar seus conhecimentos matemáticos a situações diversas, utilizando-os na interpretação da ciência, na atividade tecnológica e nas atividades cotidianas;
- analisar e valorizar informações provenientes de diferentes fontes, utilizando ferramentas matemáticas para formar uma opinião própria que lhe permita

expressar-se criticamente sobre problemas da Matemática, das outras áreas do conhecimento e da atualidade;

- desenvolver as capacidades de raciocínio e resolução de problemas, de comunicação, bem como o espírito crítico e criativo;
- utilizar com confiança procedimentos de resolução de problemas para desenvolver a compreensão dos conceitos matemáticos;
- expressar-se oral, escrita e graficamente em situações matemáticas e valorizar a precisão da linguagem e as demonstrações em Matemática;
- estabelecer conexões entre diferentes temas matemáticos e entre esses temas e o conhecimento de outras áreas do currículo;
- reconhecer representações equivalentes de um mesmo conceito, relacionando procedimentos associados às diferentes representações;
- promover a realização pessoal mediante o sentimento de segurança em relação às suas capacidades matemáticas, o desenvolvimento de atitudes de autonomia e cooperação.

1.3 Engenharia Didática

Engenharia Didática é uma metodologia de pesquisa e teoria educacional criada na França nos anos 80, que é inspirada na atividade do engenheiro e é utilizada por educadores e profissionais de ensino. O trabalho de um pesquisador é semelhante ao de um engenheiro, que tem como base um conhecimento sólido, mas o de um professor é fundamentado em sala de aula.

Para ambos é necessária a junção da teoria e prática. Se não houver uma teoria que resolva o problema ocorrido devido à prática, faz-se necessário o desenvolvimento de uma nova teoria ou adequar uma já existente. É na união da prática à teoria que se constroem novos produtos e ferramentas didáticas.

Pode-se descrever a Engenharia Didática como uma metodologia de pesquisa com bases fundamentadas em experiências de sala de aula e também pode-se entender como proposta de ensino desenvolvida a partir de resultados de pesquisa realizada em sala de aula.

De acordo com ALMOULOU e COUTINHO (2008):

A Engenharia Didática, vista como metodologia de pesquisa, caracteriza-se, em primeiro lugar, por um esquema experimental baseado em "realizações didáticas" em sala de aula, isto é, na concepção, realização, observação e análise de sessões de ensino. Caracteriza também como pesquisa experimental pelo registro em que se situa e modo de validação que lhe são associados: a comparação entre análise a priori e análise a posteriori. Tal tipo de validação é uma das singularidades dessa metodologia, por ser feita internamente, sem a necessidade de aplicação de um pré-teste ou de um pós-teste.

Segundo ARTIGUE (1996), uma Engenharia Didática é composta pelas seguintes fases:

- 1) Análises Prévias;
- 2) Concepção e análise a priori de experiências didático-pedagógicas a serem desenvolvidas na sala de aula de matemática;
- 3) Implementação da experiência;
- 4) Análise a posteriori e validação da experiência.

Descreveremos no desenrolar dos capítulos os passos da Engenharia Didática.

CAPÍTULO 2: ANÁLISES PRÉVIAS

Como primeira parte da Engenharia Didática, o objetivo das análises prévias é verificar o atual funcionamento do ensino e prática dos conteúdos para que, se necessário sejam propostas e efetivadas melhorias na transmissão e realização do conhecimento. Segundo CARNEIRO (2005):

A análise é feita para esclarecer os efeitos do ensino tradicional, as concepções dos alunos e as dificuldades e obstáculos que marcam a evolução das concepções. A tradição é vista como um estado de equilíbrio do funcionamento de um sistema dinâmico, que tem falhas. A reflexão sobre essas falhas torna-se o ponto de partida para determinar condições possíveis de um ponto de funcionamento mais satisfatório.

2.1 Análise histórica

Verificaremos neste item das análises prévias, um pouco da história das matrizes e da criptografia.

2.1.1 Matrizes

Desde os tempos mais remotos o homem se utiliza dos recursos de matrizes para a resolução dos mais variados problemas. Um dos mais famosos problemas envolvendo matrizes é conhecido como Quadrado Mágico. É uma matriz quadrada de ordem 3 cujos elementos são organizados de modo que a soma dos elementos de cada linha, coluna ou diagonal sempre resultam numa constante.

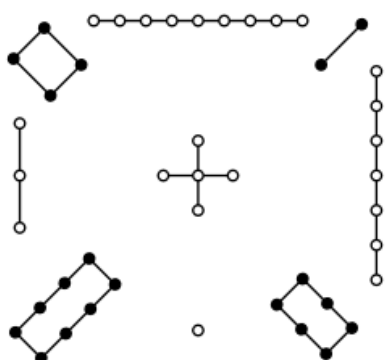
O exemplo abaixo é conhecido como Quadrado Mágico de Lo Shu, de origem chinesa, que satisfaz as condições acima. A soma dos elementos das linhas, colunas e diagonais resulta em 15.

Figura 1: Quadrado Mágico

| | | |
|---|---|---|
| 4 | 9 | 2 |
| 3 | 5 | 7 |
| 8 | 1 | 6 |

Fonte: http://en.wikipedia.org/wiki/Lo_Shu_Square

Figura 2: Quadrado Mágico com cordas e nós.



Fonte: http://en.wikipedia.org/wiki/Lo_Shu_Square

De acordo com EVES (2011):

“...é um arranjo quadrado de numerais expresso por nós em cordas; nós pretos para números pares e brancos para números ímpares”.

Por volta de 1700, Gottfried Wilhelm von Leibniz (1646-1716) utilizou tabelas numéricas para desenvolver métodos de resolução de sistemas lineares. Essas tabelas deram origem ao que chamamos de Matrizes.

Já no século XVIII, com a expansão comercial, se fazia uso de um grande número de tabelas, para a organização de dados comerciais. Gabriel Cramer (1704-1752) e Carl Friedrich Gauss (1777-1855) desenvolveram respectivamente a resolução de sistemas de equações lineares em termos de determinantes e multiplicação de matrizes.

O termo *matriz* foi introduzido por James Joseph Sylvester (1814-1897) no século XIX. Na mesma época, Arthur Cayley (1821-1895) aprofundou seus estudos em tabelas numéricas, sendo responsável por grande parte do desenvolvimento da teoria de matrizes.

Ainda de acordo com EVES (2011):

“...As matrizes surgiram para Cayley ligadas a transformações lineares do tipo $x'=ax+by$ e $y'=cx+dy$, onde a,b,c,d são números reais, e que podem ser imaginadas como aplicações que levam o ponto (x,y) no ponto (x',y') ...”.

Outros matemáticos também deram grande contribuição no desenvolvimento da teoria de matrizes, entre eles Alexandre Vandermonde, Pierre Simon Laplace, Carl Gustav Jacob Jacobi, Augustin Louis Cauchy, Leopold Kronecker, Saxon Frobenius.

2.1.2 Criptografia

O termo criptografia é de origem antiga, vem da fusão de duas palavras gregas: Kryptos que significa secreto, oculto e Gráphein que significa escrever. É a ciência que se dedica ao desenvolvimento de cifras e códigos para ocultar (tornar secreto) uma mensagem. Criptografar um texto significa transformá-lo em outro de maneira a ocultar o seu significado. Existem vários métodos para criptografar uma mensagem. Na maioria das vezes, só é possível a revelação de uma mensagem se o agente que trabalha para revelar o segredo conhece a chave, ou seja, o método utilizado na encriptação de tal transformação. Cada tipo de Criptografia tem uma determinada chave.

São exemplos de criptografias antigas:

- Cifrário de César
- Atbash Hebráico
- Cítala Espartana
- Transposição Colunar

Com o passar dos anos e séculos, chegamos aos modernos métodos de criptografia, que são utilizados em nossos sistemas de informação e segurança.

De acordo com SGARRO (1994):

“... A criptografia, hoje, é estudada ativamente e seriamente por matemáticos, cientistas da computação, especialistas em estatística, engenheiros da computação,...”.

O sistema de criptografia que utilizamos em nossa aula chama-se Criptografia por Transposição.

A Transposição é o método de codificação no qual se faz o deslocamento das letras de uma mensagem. As letras da mensagem original são trocadas de posição, alterando completamente o seu conteúdo, mas sem retirar e nem colocar uma nova letra. Verificaremos em nosso trabalho que a encriptação de mensagens por transposição faz permutações com as letras da mensagem, ou seja, cria anagramas da mensagem original. Com a transposição de letras podemos trabalhar os números primos e compostos, permutação e matrizes.

2.2 Análise didática

Verificamos agora, como é apresentado e desenvolvido o conteúdo de matrizes sob o ponto de vista de alguns autores no ensino médio.

A Proposta Curricular da Secretaria de Educação do Estado de São Paulo (2010) aborda o tema Matrizes no caderno 2, que se inicia no segundo bimestre. Na situação de Aprendizagem 1, como vem apresentada na proposta, o conhecimento é construído com a utilização de gráficos e translação de polígonos, com tabelas de dupla entrada, inserindo aos poucos os conceitos iniciais de matrizes através da realização dessas atividades. Uma outra atividade ocorre nas situações de aprendizagem 3 e 4, nas quais aborda-se o conceito de *Pixel*, associando a ideia de matriz à da imagem fotografada em uma máquina digital, ou da imagem de um aparelho de televisão digital.

DANTE (2011) inicia o conceito de matrizes informando que matrizes são tabelas e faz uma ligação das mesmas com o advento da computação. Descreve a utilização de matrizes nos variados meios, assim como oferece ao leitor notas históricas sobre matrizes através dos tempos.

Após essa apresentação é sugerido ao aluno algumas atividades com tabelas envolvendo a taxa selic e tabelas de dupla entrada. A partir desse momento inicia-se

a definição, características e propriedades de matrizes, com exercícios sobre o tema.

IEZZI (2010) apresenta o assunto oferecendo ao leitor uma situação descrita pelo IBGE em forma de tabela de dados sobre empregos e outra sobre tolerância de álcool no sangue em alguns países. Apresenta um breve relato sobre a História das Matrizes, posteriormente abordando a definição, conceitos e propriedades de matrizes. Entre as definições e propriedades, encaixa exercícios relacionados ao tema.

Verificamos nessas abordagens acima, que o assunto matriz é apresentado de forma parecida, todas muito bem pensadas e interessantes, que conduzem o aluno ao conceito e uso de matrizes.

2.2.1 Importância do estudo de matrizes

Desde o seu aparecimento na China antiga as matrizes servem como ferramenta para a resolução de problemas que envolvem equações simultâneas lineares. Atualmente a aplicação de matrizes engloba os mais variados campos do conhecimento, são aplicadas diretamente na programação computacional, nas várias áreas da engenharia, na organização de informações nas empresas, em boletos, planilhas, softwares que necessitam de rotações e translações de fotos, construção de imagens, filmes, etc. É de grande utilidade quando se tem que organizar qualquer tipo de informações numéricas.

A aplicação de matrizes está diretamente ligada à nossa realidade, fazendo parte de nossas vidas nos mais variados momentos, justificando assim a escolha do nosso tema.

2.3 Análise cognitiva

Investigando as dificuldades e facilidades encontradas pelos alunos na aplicação do tema nos modos vistos acima, foi verificado que uma parte dos mesmos que se interessam por esse tipo de abordagem consegue entender, desenvolver, aplicar e completar as atividades propostas. Já, aos demais, o assunto

não causa interesse maior, pois não veem o assunto como novo, algo que impulse a vontade de aprender, visto que estão sem estímulos e cansados da rotina e programas parecidos, ou seja, não voltam seu olhar para a importância das atividades. Temos também uma grande parte dos alunos com dificuldades nas operações básicas e na interpretação de textos, gráficos e tabelas, os quais não conseguem interpretar o problema proposto, tomando para si tal situação como obstáculo e desistindo da atividade.

O problema para a construção do conhecimento não está nas atividades em si que são propostas de maneira clara, objetiva e de fácil entendimento. Estamos diante de uma situação nova, diferente, na qual competimos involuntariamente com outros interesses além classe, como aparelhos celulares, redes sociais, jogos eletrônicos e outras atividades que evoluem tecnologicamente mais rápido que nossos métodos de ensino, sendo natural o interesse dos alunos se voltar para tais atividades.

CAPÍTULO 3: ANÁLISE A PRIORI

Nessa etapa do nosso trabalho descreveremos nossa proposta didática, enfatizando os objetivos a serem alcançados, detalharemos os passos da aula a ser aplicada e as características das salas envolvidas.

Para idealizar essa aula, pensei e refleti sobre alguns tópicos:

- É necessário implementar na sala de aula algo diferente do cotidiano dos alunos, que em grande parte perderam o interesse pela Matemática, pela aula, pela escola, etc.
- Utilizar um tema de fácil compreensão e adequado aos alunos.
- Utilizar o currículo referente às séries às quais seria aplicada a aula.
- Fugir do tradicional, mas sempre ligado ao currículo.

Utilizaremos nessa aula a transposição de letras para a codificação de mensagens. Para a realização de codificação e decodificação das mensagens faz-se necessário o uso de matrizes e matrizes transpostas que é o tema de nosso trabalho.

Mas quais seriam as mensagens utilizadas na aula? Do que deveria falar?

Já de início veio a ideia de trabalhar com ditados populares, pois os mesmos são de conhecimento da grande maioria, são curiosos e possuem o tamanho ideal para que fossem criptografados e decifrados por eles.

A mensagem criptografada pelo método da transposição possui um grau relevante de dificuldade em ser decodificada do jeito natural, ou seja, ficar olhando para a mesma, analisando e tentar desembaralhar as letras formando a mensagem original, o sucesso quase nunca é obtido.

Com a utilização de matrizes como veremos, tal decodificação se torna uma brincadeira de criança, um truque de mágicas, que desvenda a mensagem quase que imediatamente. É claro que podemos colocar algumas travas para dificultar a decodificação, mas não estudaremos isso nesse trabalho.

Os alunos também farão uso dos números compostos para decifrar e criptografar as mensagens.

O tempo programado para a aplicação dessa aula é de 100 minutos. Caso ocorra a necessidade de reforçar o conceito de números primos e compostos,

utilizaremos mais uma aula de 50 minutos, pois tais conceitos são fundamentais para o sucesso de nossa empreitada.

A aula se inicia com a apresentação do tema Transposição e Criptografia e com um convite para decifrar as seguintes mensagens:

ASDQUNTEUNTADECERONA

e

AOFUFONARIZÇÃAA

Este é o desafio inicial que, em tese, deve atrair os alunos.

Podemos verificar que decifrar tais mensagens apenas tentando movimentar as letras na sequência não é tão fácil assim, mas também não é impossível. Os alunos terão alguns minutos para tentar decodificar tais mensagens. Ai está a oportunidade de envolver os alunos no ambiente matemático. Após o tempo determinado para decifrar o enigma, é feito um convite aos alunos a aprender um método simples e fácil para a decodificação desse modelo de mensagem criptografada: a utilização de matrizes e matrizes transpostas.

Espera-se que o aluno já ansioso por obter a resposta dos enigmas, se empenhe em saber como fazer para encontrar a solução. Faz-se necessário, nesse momento, a explanação do conceito de matriz, suas nuances, aplicações e modelos, enfatizando o conceito de matrizes transpostas.

Nossas mensagens são criptografadas ou decodificadas, se for o caso, com a utilização de “tabelas” ou matrizes. Necessitamos também do conceito de números primos e números compostos, que servirão para formar a matriz desejada.

Como funciona a codificação de mensagens pelo método da transposição de letras? Utilizaremos aqui uma das mensagens trabalhadas em sala: **Se cair, do chão não passa**. Para efeito didático, não utilizaremos a vírgula e nem o ponto final.

O primeiro passo é contar o número de letras da mensagem. **Se cair, do chão não passa** tem um total de 20 letras. Observamos que o número 20 pode ser escrito como o produto de dois números de várias formas:

$$20 = 1 \times 20 = 2 \times 10 = 4 \times 5 = 5 \times 4 = 10 \times 2 = 20 \times 1$$

Cada um desses produtos pode ser utilizado para compor a matriz onde codificaremos a mensagem. O primeiro número de cada produto representa a quantidade de linhas e o segundo número a quantidade de colunas de cada matriz $A=(a_{ij})_{m \times n}$, que pode ser formada com cada um desses produtos.

Observando os produtos, verificamos que **1x20 e 20x1** são produtos que não atendem ao nosso propósito pois o primeiro dá forma a uma matriz com uma linha e vinte colunas e o segundo da forma a uma matriz com 20 linhas e uma coluna. Com essas duas tabelas não é possível a realização da encriptação da mensagem pois temos apenas uma linha na primeira e apenas uma coluna na segunda.

O produto 20x1 forma a seguinte matriz:

| |
|---|
| S |
| E |
| C |
| A |
| I |
| R |
| D |
| O |
| C |
| H |
| Ã |
| O |
| N |
| Ã |
| O |
| P |
| A |
| S |
| S |
| A |

Tabela 1

Já o produto 1×20 gera a seguinte matriz:

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S | E | C | A | I | R | D | O | C | H | A | O | N | Ã | O | P | A | S | S | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Tabela 2

Podemos observar que em nenhuma dessas situações conseguiremos embaralhar as letras. Se observarmos melhor, uma é transposta da outra e, nas duas conseguimos ler a mensagem. Logo, trabalharemos com um dos produtos restantes. Escolhido um, 4×5 , façamos a encriptação da mensagem.

O produto 4×5 representa a matriz $A=(a_{ij})_{4 \times 5}$ que será formada contendo quatro linhas e cinco colunas, ou seja:

| | | | | |
|----------|----------|----------|----------|----------|
| a_{11} | a_{12} | a_{13} | a_{14} | a_{15} |
| a_{21} | a_{22} | a_{23} | a_{24} | a_{25} |
| a_{31} | a_{32} | a_{33} | a_{34} | a_{35} |
| a_{41} | a_{42} | a_{43} | a_{44} | a_{45} |

Tabela 3

Agora, preenchamos as células da matriz com as letras da mensagem na ordem em que aparecem. Poderemos fazer isso seguindo pelas linhas ou pelas colunas. Utilizaremos em nossa aula a escrita da mensagem original através das colunas para padronização.

| | | | | |
|---|---|---|---|---|
| S | I | C | N | A |
| E | R | H | Ã | S |
| C | D | Ã | O | S |
| A | O | O | P | A |

Tabela 4

Mas a partir daí, o que fazemos? Como codificamos a mensagem?

Agora vem a utilização das matrizes transpostas.

Como escrevemos a mensagem em colunas, agora embaralhamos as letras escrevendo a mensagem criptografada em linhas, ou seja, façamos a matriz

transposta da matriz $A = [a_{ij}]_{4 \times 5}$, a qual denominamos $A^t = [b_{ij}]_{5 \times 4}$, onde $b_{ij} = a_{ji}$. As colunas da matriz A agora são linhas na matriz A^t .

| | | | |
|--------------|----------------------|----------------------|--------------|
| $b_{11} = S$ | $b_{12} = E$ | $b_{13} = C$ | $b_{14} = A$ |
| $b_{21} = I$ | $b_{22} = R$ | $b_{23} = D$ | $b_{24} = O$ |
| $b_{31} = C$ | $b_{32} = H$ | $b_{33} = \tilde{A}$ | $b_{34} = O$ |
| $b_{41} = N$ | $b_{42} = \tilde{A}$ | $b_{43} = O$ | $b_{44} = P$ |
| $b_{51} = A$ | $b_{52} = S$ | $b_{53} = S$ | $b_{54} = A$ |

Tabela 5

Escrevemos a mensagem como apareceu nas colunas:

SICNAERHÃSCDÃOSAOPA

E assim temos a mensagem criptografada. De um modo prático, basta colocar a mensagem em uma tabela e, se for escrita em colunas, devemos embaralhar as letras escrevendo-as na ordem em que apareceram nas linhas. Para decifrar a mensagem, basta fazer o procedimento inverso.

Se não conhecemos a mensagem original, como no caso acima, podemos ter algum trabalho para decifrá-la. Vamos observar a mensagem criptografada:

SICNAERHÃSCDÃOSAOPA

É formada por 20 letras como já vimos. Suponhamos não saber a revelação. Observamos que $20 = 1 \times 20 = 2 \times 10 = 4 \times 5 = 5 \times 4 = 10 \times 2 = 20 \times 1$. Descartamos 20×1 e 1×20 pelos motivos já expostos acima.

Temos ainda quatro tipos de matrizes e apenas uma delas nos revelará o segredo da mensagem como veremos abaixo:

- Matriz $A_1 = (a_{ij})_{2 \times 10}$. Temos uma matriz com duas linhas e dez colunas.

Escrevamos a mensagem e observamos sua transposta.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| S | I | C | N | A | E | R | H | Ã | S |
| C | D | Ã | O | S | A | O | O | P | A |

Tabela 6

Lendo em colunas temos: SCIDCÃNOASEAROHOÃPSA, que em nossa língua materna não faz sentido algum.

- Matriz $A_2 = (a_{ij})_{10 \times 2}$. Temos uma matriz com dez linhas e duas colunas. Escrevamos a mensagem e observamos sua transposta.

| | |
|---|---|
| S | I |
| C | N |
| A | E |
| R | H |
| Ã | S |
| C | D |
| Ã | O |
| S | A |
| O | O |
| P | A |

Tabela 7

Lendo em colunas temos: SCARÃCÃSOPINEHSDOAOA, que em nossa língua materna não faz sentido algum.

- Matriz $A_3 = (a_{ij})_{5 \times 4}$. Temos uma matriz com cinco linhas e quatro colunas. Escrevamos a mensagem e obsevamos sua transposta.

| | | | |
|---|---|---|---|
| S | I | C | N |
| A | E | R | H |
| Ã | S | C | D |
| Ã | O | S | A |
| O | O | P | A |

Tabela 8

Lendo em colunas temos: SAÃÃOIESOOCRCSPNHDA, que em nossa língua materna não faz sentido algum.

- Matriz $A_4 = (a_{ij})_{4 \times 5}$. Temos uma matriz com quatro linhas e cinco colunas. Escrevamos a mensagem e observamos sua transposta.

| | | | | |
|---|---|---|---|---|
| S | I | C | N | A |
| E | R | H | Ã | S |
| C | D | Ã | O | S |
| A | O | O | P | A |

Tabela 9

Lendo em colunas temos: SECAIRDOCHÃONÃOPASSA. Observando bem a mensagem, colocando espaços e vírgulas nos locais certos, temos o seguinte ditado popular: **Se cair, do chão não passa.**

Quanto maior for o número de produtos de dois números que resultam no total de letras contidas na mensagem, mais trabalhosa pode ser a decodificação da mesma.

Não há sentido em trabalhar mensagens com números primos, pois assim não teremos alternativas de tabelas para a codificação. Se a mensagem escolhida possuir uma quantidade de letras que seja um número primo, devemos acrescentar um símbolo no final da mensagem e certamente teremos um número composto. (descartamos a mensagem formada por duas letras apenas).

Essa aula foi construída para ser aplicada em duas salas, 2º B e 2º C do Ensino Médio da Escola Estadual Esmeralda Soares Ferraz, localizada em Ourinhos, SP. Foi preparada em forma de slides para melhor desenvolvimento e visualização.

Perfil das salas:

2ºB: sala no período da manhã, com 27 alunos, participativos em sua grande maioria, porém com vícios e costumes como esperar a resolução de exercícios feita pelo professor sem ao menos tentar resolver, não estudar em casa, não realizarem tarefas de casa, não estudarem para avaliações e não se preocuparem com notas.

Temos alguns alunos nessa sala com dificuldades no trato das operações básicas da matemática.

2ºC: sala do período da manhã, com 23 alunos, na sua maioria apáticos, com dificuldades no trato das operações básicas matemáticas, sem estímulo e iniciativa para resolver qualquer problema sozinhos. Temos também alguns alunos faltosos nessa sala.

Espera-se, nessas aulas, que o aluno desperte o interesse em fazer uso das ferramentas matemáticas (aplicação de matrizes) para solucionar o problema proposto, no caso a resolução de mensagens criptografadas; que ele se posicione na sala como protagonista que deve ser, construindo seu conhecimento através de situações e ferramentas propostas pelo professor, que servirá como guia nesse caminho a ser percorrido.

A aula de 100 minutos será dividida basicamente:

- Apresentação do tema Criptografia e Transposição de Letras;
- Convite aos alunos a decodificar algumas mensagens criptografadas;
- Oferecimento da ferramenta matrizes e matrizes transpostas para a resolução das mensagens criptografadas;
- Explicação do conceito de matrizes, alguns tipos de matrizes importantes, aplicação de matrizes e matrizes transpostas;
- Revisão (se necessário) sobre números primos e compostos;
- Decodificação das mensagens propostas com o uso das matrizes;
- Proposta de codificação de mensagens (será oferecido aos alunos uma lista com ditados populares);
- Troca entre os grupos de alunos das mensagens criptografadas para decodificação das mesmas;
- Discussão entre todos sobre a aplicação da atividade proposta;
- Produção de um relatório por grupo sobre a aula realizada.

CAPÍTULO 4: EXPERIMENTAÇÃO

Nesta etapa, descreveremos a aplicação da proposta, como ocorreu, alguns detalhes da prática, da interação dos alunos, qual o material coletado para análise.

A aplicação da aula programada deu-se primeiro no 2º ano B, nos dias 5 e 6 de novembro de 2012. A aula foi programada para ser apresentada como slide, mas o aparelho que reproduz slides da escola estava quebrado e não havia previsão para arrumá-lo. Decidi realizar o projeto na lousa.

A aula foi iniciada com uma conversa com os alunos para levantar os conhecimentos prévios sobre matrizes e tabelas, criptografia e decodificação de mensagens. Ao falar de criptografia, surgiram assuntos em nossa conversa como criptografia de bancos, códigos de internet, segurança de informações, etc.

Falamos de transposição de letras e fiz aos mesmos uma proposta em decifrar a seguinte mensagem: **ASDQUUNTEUNTADECERONA**. E foi como esperado. Os alunos ficaram obsecados em resolver o enigma. Mas nenhum dos presentes conseguiu.

Para ficar melhor ainda, fiz uma nova proposta: decifrar uma mensagem aparentemente mais fácil: **AOFUFONARIZÇÃAA**. Após alguns minutos, como a solução não aparecia, os alunos perambularam pela escola para oferecerem o enigma a outras pessoas, mas sem sucesso. Consegui, finalmente, mexer com os alunos, incomodá-los intelectualmente, pois algo parecido tão fácil e que “*não precisava de equações e cálculos*” não tinha solução. Ninguém da escola, do período da manhã, conseguiu decodificar tais mensagens.

Como já tinha alcançado o objetivo do momento que era incomodá-los, atizar a curiosidade dos mesmos, fiz uma nova proposta, que era encontrar a solução das mensagens utilizando números compostos, matrizes e matrizes transpostas. De imediato a proposta foi aceita pois não se conformavam com o fracasso em decifrar a mensagem. Nesse momento, os alunos que estavam organizados em fileiras individuais se organizaram em grupos e entreguei aos mesmos algumas folhas quadriculadas, nos quais realizariam a codificação e a decodificação dos ditados populares.

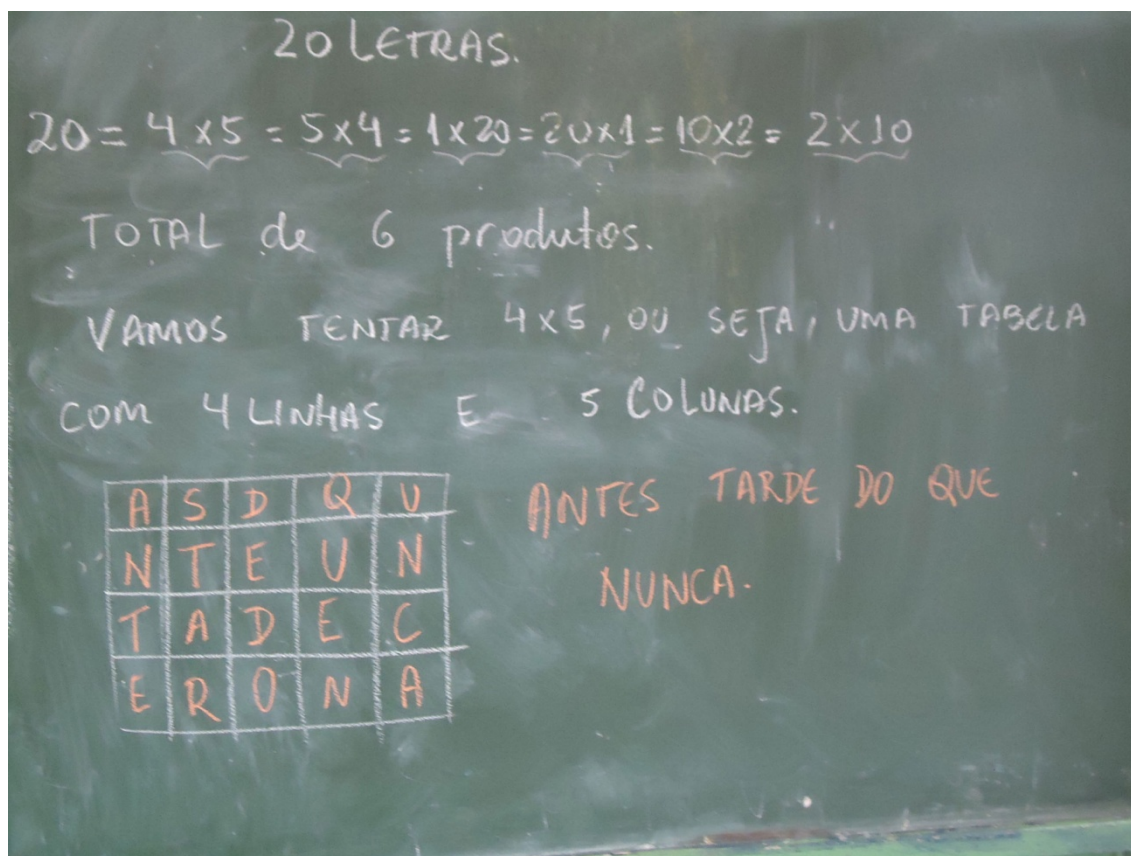
Escrevi na lousa a definição de matrizes, tipos de matrizes e matrizes transpostas, assim como foi necessário revisar o conceito de números primos e

compostos. Discutimos sobre o assunto proposto, que era de fácil compreensão e enfim, chegamos à primeira mensagem: **ASDQUNTEUNTADECERONA.**

A primeira ligação com a mensagem foi a contagem das letras. Como já vimos, um total de 20 letras. Aproveitei a oportunidade para explicar sobre a decomposição de números, divisores de um número e pedi que encontrassem os números cujo produto de dois deles resultava 20.

Após a explicação de que apenas uma das matrizes é aquela que funcionará para esse tipo de situação, foi revelada a matriz abaixo e a decodificação da mensagem:

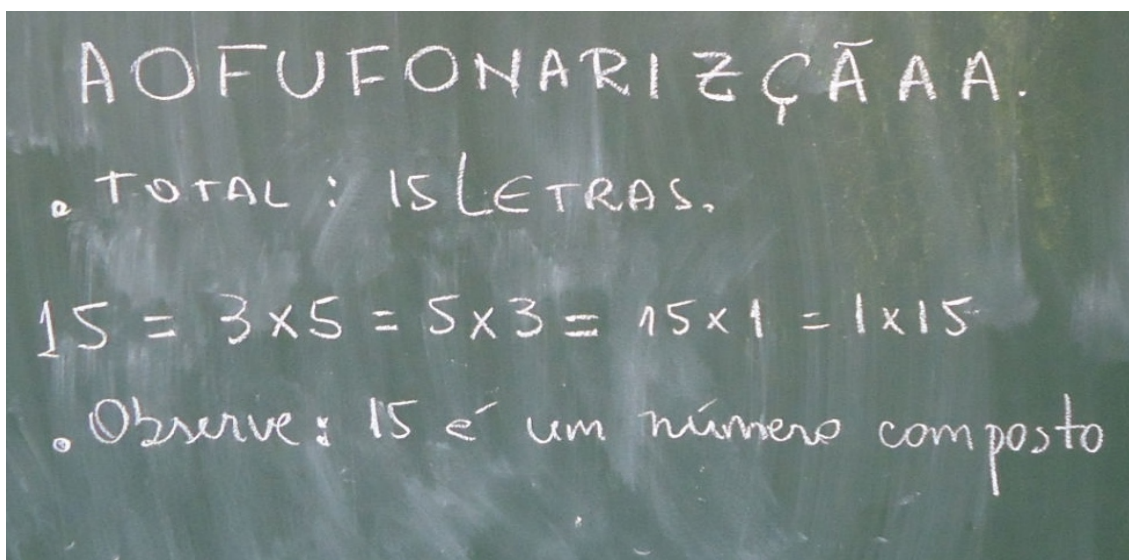
Fotografia 1



Decomposição e mensagem revelada.

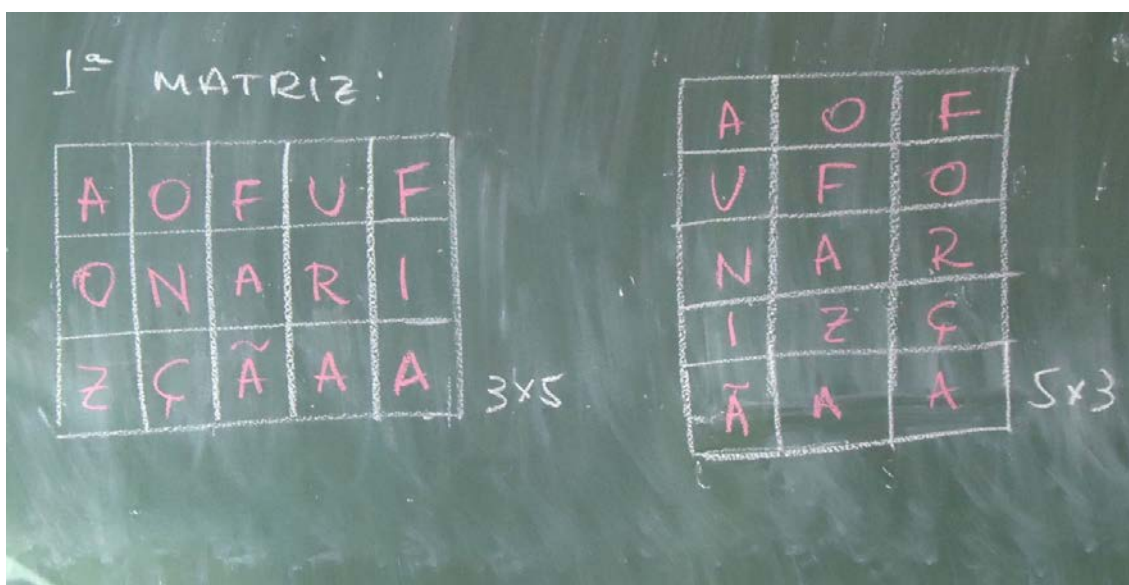
Após a decodificação dessa mensagem, foi dado alguns minutos para que decodificassem a outra mensagem apresentada **AOFUFONARIZÇÃAA.**

Fotografia 2



Decomposição em produtos

Fotografia 3



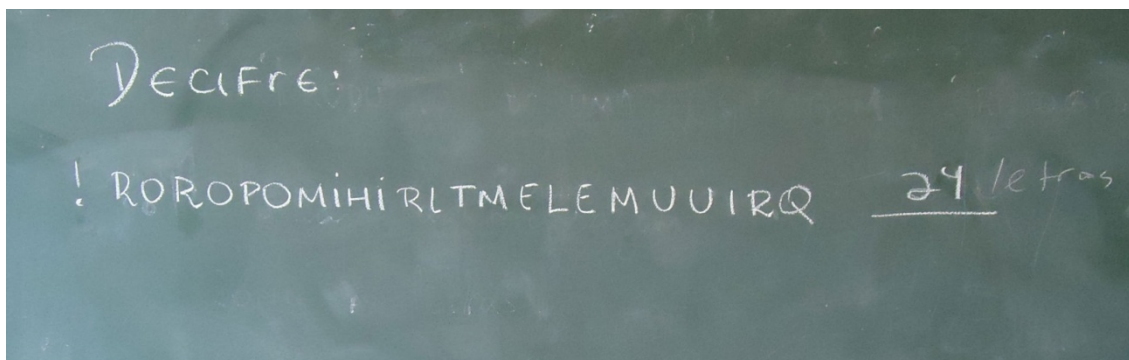
Utilização da transposta.

Observando a segunda matriz: **A união faz a força.**

A proposta agora foi a seguinte: de posse de uma lista de ditados populares, os alunos ficaram encarregados de no primeiro momento, encontrar o seu ditado preferido e codificá-lo de acordo com as regras explicitadas.

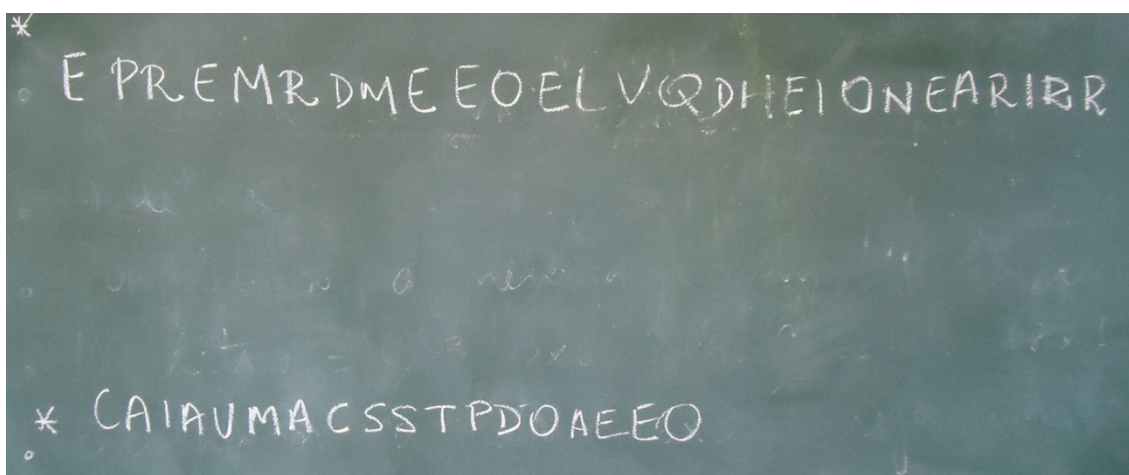
Após essa atividade, algumas das mensagens criptografadas pelos alunos foram escritas na lousa, para que os demais conseguissem descobrir.

Fotografia 4



Mensagem criptografada proposta pelos alunos.

Fotografia 5



Mensagens criptografadas proposta pelos alunos.

São os seguintes ditados:

Escrito de traz para frente: **Quem ri por último ri melhor.**

Na escrita normal: **É melhor prevenir do que remediar e cada coisa a seu tempo.**

Além dessas, outras também foram realizadas e trocadas entre os grupos.

Ao final da aula, os alunos foram orientados a confeccionar um relatório sobre as atividades realizadas.

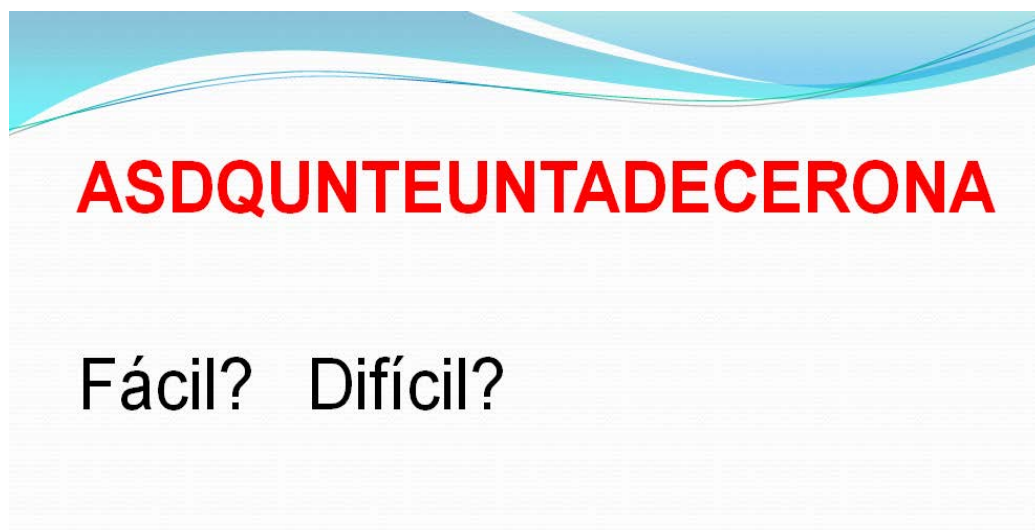
Na semana seguinte, no dia 12 de novembro, a aplicação da aula ocorreu na sala do 2ºC. No transcorrer da semana entre as aplicações das aulas nas duas salas, o tema Criptografia percorreu várias rodas de conversa na escola, e alguns alunos da outra sala já estavam sabendo algo sobre o assunto, assim como a

equipe pedagógica conseguiu colocar o aparelho data show em funcionamento, pois o mesmo estava danificado na semana anterior.

As estratégias para o andamento da aula foram as mesmas citadas acima, diferenciando no ponto em que foi apresentada em forma de slides e não em lousa. O transcorrer da aula deu-se de maneira parecida com a aula ministrada na outra sala, com a mesma dinâmica. O tempo de 100 minutos foi suficiente para a realização completa da aula, devido ao conteúdo ser apresentado no data show.

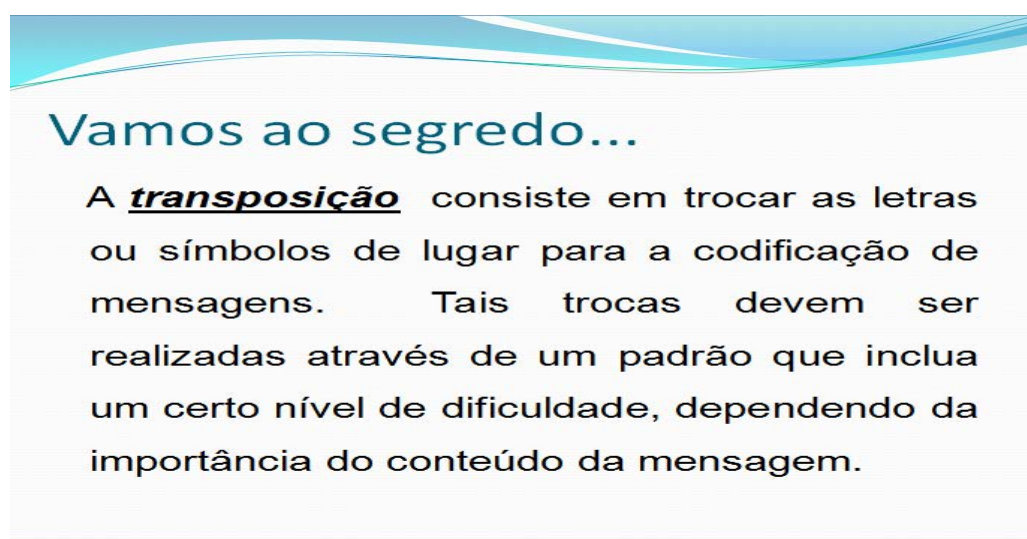
Momentos da aula:

Slide 1



Desafio Inicial

Slide 2



Transposição

Slide 3

Matriz

Chama-se matriz do tipo $m \times n$ (lê-se m por n) toda tabela de números dispostos em m linhas e n colunas. Tal tabela deve ser representada entre parênteses $()$, entre colchetes $[]$ ou entre barras duplas $\| \downarrow \|$.

Exemplos:

$$a) A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2 \times 3} \quad \text{lê-se: matriz } A \text{ de ordem } 2 \text{ por } 3$$

$$b) B = \begin{bmatrix} 0 & 0 & 1 \\ 5 & 6 & 0 \\ 2 & 2 & 2 \end{bmatrix}_{3 \times 3} \quad \text{lê-se: matriz } B \text{ de ordem } 3$$

Definição e exemplos de matrizes

Slide 4

Vamos preencher a tabela com a mensagem.
Cada letra na sua gaveta.

| | | | | |
|----------|----------|----------|----------|----------|
| S | I | C | N | A |
| E | R | H | Ã | S |
| C | D | Ã | O | S |
| A | O | O | P | A |

Tabela com a mensagem original

Slide 5

Como escrevemos a mensagem em colunas, agora embaralhamos as letras escrevendo a mensagem criptografada em linhas, ou seja, fazemos a matriz transposta da matriz $A = [a_{ij}]_{4 \times 5}$, a qual denominamos $A^t = [b_{ij}]_{5 \times 4}$, onde $b_{ij} = a_{ji}$. As colunas da matriz A agora são linhas na matriz A^t .

| | | | |
|--------------|----------------------|----------------------|--------------|
| $b_{11} = S$ | $b_{12} = E$ | $b_{13} = C$ | $b_{14} = A$ |
| $b_{21} = I$ | $b_{22} = R$ | $b_{23} = D$ | $b_{24} = O$ |
| $b_{31} = C$ | $b_{32} = H$ | $b_{33} = \tilde{A}$ | $b_{34} = O$ |
| $b_{41} = N$ | $b_{42} = \tilde{A}$ | $b_{43} = O$ | $b_{44} = P$ |
| $b_{51} = A$ | $b_{52} = S$ | $b_{53} = S$ | $b_{54} = A$ |

Matriz transformação

Em ambas as salas foram coletadas folhas quadriculadas que os alunos utilizaram para fazer as codificações e as decodificações das mensagens.

Conforme apêndice os alunos destas salas realizaram a encriptação e a decodificação de mensagens em folhas quadriculadas e no final do nosso encontro foram convidados a escreverem um relatório sobre a aula e as atividades propostas.

CAPÍTULO 5: ANÁLISE A POSTERIORI E VALIDAÇÃO

Na análise a posteriori, verificamos se nossa proposta, nossas hipóteses funcionaram, confrontamos o que idealizamos na análise a priori com o que realmente aconteceu. É o momento de comparação.

Após a aplicação da aula sobre matrizes e criptografia, alguns itens merecem destaque:

Ao escrever a mensagem criptografada na lousa, no início das aulas, notou-se que os alunos que estavam acomodados pela rotina começaram a pensar na solução do enigma e como não conseguiram, começaram a se incomodar, e a se movimentar no sentido de encontrar a solução. Esse foi o ponto de partida para atraí-los ao universo das matrizes.

Notou-se também, que existe, por parte de alguns alunos, principalmente na sala 2°C, uma grande resistência em se envolver com o assunto proposto em sala, mesmo sendo algo diferente. Ainda que fazendo o convite aluno a aluno, negaram-se a realizar as atividades. Conversando com eles sobre os motivos que os levaram a não realizá-las, alegaram falta de vontade em estudar, que alguns estavam ali obrigados pelas mães, falta de perspectiva em relação ao futuro e também, falta de credibilidade no sistema educacional atual.

Verificou-se também que em determinado grupo de alunos que estavam desanimados e cansados e já haviam abandonado a rotina escolar, ou seja, estavam na escola com outros objetivos diferentes do aprender nas aulas, desenvolveram de forma prazerosa e dinâmica as atividades em sala, como podemos verificar nos relatórios anexos no Apêndice.

Em relação aos alunos que se esforçam e tem objetivos direcionados para o pós ensino médio, ou seja, querem entrar em uma universidade, foram além e tentaram dificultar a encriptação de mensagem, oferecendo o desafio aos demais, como é o caso da aluna M. B. e do aluno G.T.

A apresentação no slide fica mais limpa, clara e ágil em relação à apresentação na lousa de giz, motivo esse que na sala do 2ºB (lousa) utilizei 150 minutos de aula e no 2°C (projektor) apenas 100 minutos.

Como esperado e previsto, foi muito fácil atrair os alunos a resolverem os enigmas, devido à curiosidade, natural em qualquer ser humano em querer saber dos segredos. Após tentativas frustradas, a saída proposta que era através da aplicação de matrizes, foi prontamente aceita pela maioria. As atividades ocorreram conforme o planejado. A boa receptividade da maioria dos alunos com relação ao assunto pode ser comprovada pelas leituras dos relatórios e também nas folhas quadriculadas.

Alguns fatos interessantes surgiram durante a aplicação, como por exemplo a saída da sala de aula em busca de ajuda para resolver os enigmas. Imaginemos se esta situação ocorresse para todos os problemas que apresentamos na lousa.

Conseguimos, com essa atividade, resgatar alguns alunos que estavam desgostosos, desanimados com a escola e com o ambiente escolar. Revivemos o aluno protagonista que estava adormecido em alguns e desafiamos aqueles que acompanham o ensino de maneira responsável e eficiente.

Em uma minoria, principalmente na sala do 2ºC, a proposta de decifrar as mensagens criptografadas sem utilizar nenhum conceito de matrizes surtiu efeito, mas como não acharam a solução do enigma, desanimaram e desistiram da atividade, esperando que os demais encontrassem o resultado.

De maneira geral, a aplicação da referida aula foi de bom grado, pois conseguimos comprovar que os alunos esperam por algo diferente da escola, que estão prontos, mas cansados da forma tradicional e repetitiva da nossa aplicação em relação aos conteúdos aplicados. A atividade realizada comprovou que o fato de o aluno querer ou não participar de determinada aula está sobretudo relacionado à questão de a situação de aprendizagem ser significativa, isto é, o conhecimento só ocorre de fato quando o aluno participa do processo de sua construção.

CONCLUSÃO

Ao iniciar o Profmat, não tinha a mínima ideia de onde essa história chegaria. Percorri, juntamente com meus amigos de curso, os mais variados caminhos enlaçados pelas disciplinas que frequentamos. Os professores que nos ofereceram sua sabedoria e experiência aliadas ao nosso esforço e persistência, nos transformaram, provocando-nos inquietações características daquelas crianças que ganham um brinquedo novo e não veem a hora de se divertirem com ele.

E foi assim. Ao campo de batalha. Tínhamos, como tarefa, que aplicar algo diferente do usual em nossas salas de aula. Escolhido o tema, embasado na Engenharia Didática, foi oferecido aos alunos uma maneira diferente de utilizar um conceito matemático (matrizes), aplicado em resolução de enigmas (mensagens criptografadas).

Segundo Dante (1995):

“...As rápidas mudanças sociais e o aprimoramento cada vez maior e mais rápido da tecnologia impedem que se faça uma previsão exata de quais habilidades, conceitos e algoritmos matemáticos seriam úteis hoje para preparar um aluno para sua vida futura. Ensinar apenas conceitos e algoritmos que atualmente são relevantes parece não ser o caminho, pois eles poderão tornar-se obsoletos daqui a quinze ou vinte anos, quando a criança de hoje estará no auge de sua vida produtiva. ...E para isso, é fundamental desenvolver nela iniciativa, espírito explorador, criatividade e independência...”.

Precisamos inovar. Urgentemente. Os alunos da escola pública estão esperando por isso. A aplicação dessa aula foi uma pequena experiência que demonstrou o quanto eles estão prontos para interagir e absorver os conteúdos propostos. A maneira pela qual conduzimos tal aprendizado faz a diferença no resultado final. Muitas nuances devem ser levadas em consideração, como a vida social e econômica do aluno, a organização da escola em si, enquanto empresa que tem seu funcionamento voltado para o aprendizado e o conhecimento do aluno. Faz-se necessária também a adequação constante da escola em relação aos meios tecnológicos utilizados pela sociedade. Vivemos em intensa interação com estes recursos e esta dependência também se faz necessária na escola.

Na escola básica, os alunos veem os professores como pessoas sábias e capazes de realizar transformações. Nosso papel é conduzi-los, através de

estratégias e articulações ao mais profundo conhecimento possível, o qual nos propomos a transmiti-los. Que esta aula sirva para discussões, inspirações e difusão do conhecimento e cultura matemática, pois reforça o valor da pesquisa, quando está a serviço da sociedade, abrindo caminhos para a prática docente e reafirmando a importância das teorias para o cotidiano das pessoas.

REFERÊNCIAS

ALMOULOU, S.A.; COUTINHO, C. Q. S. Engenharia didática: Características e seus usos em trabalhos apresentados no GT-19 / ANPEd. **Revemat**, Florianópolis, v3.6, p62-77, UFSC: 2008. Disponível em: <<http://www.periodicos.ufsc.br/index.php/revemat/issue/view/1883>>. Acesso em: 3 dez. 2012.

ARTIGUE, M. Engenharia didática. In: BRUN, J. (Ed.). **Didáctica das matemáticas**. Lisboa: Instituto Piaget, Horizontes Pedagógicos, 1996. p. 193-217.

BRASIL, Secretaria da Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais: Ensino Médio**. Brasília: Ministério da Educação, 1999.

CARNEIRO, V. C. G. Engenharia Didática: referencial para a ação investigativa e para formação de professores de matemática. **Zetetiké**, Campinas, v. 13, n. 23., p.87-119, 2005. Disponível em: <<http://www.fe.unicamp.br/zetetike/viewarticle.php?id=6>>. Acesso em: 5 jan. 2013.

DANTE: L.R. **Didática Da Resolução De Problemas De Matemática**. São Paulo: Ática, 1995.

DANTE: L. R. **Matemática**: contexto e aplicações. São Paulo: Ática, 2011.

EVES, H. **Introdução à história da matemática**. tradução Higino H. Domingues. 5ª ed. – Campinas,SP: Unicamp, 2011.

FALABONITO. **Provérbios e ditados populares**. Disponível em: <<http://falabonito.wordpress.com/2007/03/14/proverbios-e-ditos-populares/>>. Acesso em: 2 out. 2012.

FALEIROS, A. C. **Criptografia**. Criptografia - São Carlos, SP : SBMAC, 2011, 138 p., (Notas em Matemática Aplicada; v. 52). Disponível em: <http://www.sbmec.org.br/arquivos/notas/livro_52.pdf>. Acesso em: 10 out, 2012.

HEFEZ, A.; FERNANDEZ, C. S. **Introdução à Álgebra Linear**. Rio de Janeiro: SBM, Coleção PROFMAT, 2012.

IEEZI, G; DOLCE, O; DEGENSZAJN, D; PÉRIGO, R; ALMEIDA, N. **Matemática: Ciências e Aplicações**, 2. São Paulo: Saraiva, 2010.

KELEN, L. C. Ensino de Combinatória: Problemas de Divisão, Teoria de Vergnaud e Metodologia da Engenharia Didática, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2008. Disponível em:
<http://euler.mat.ufrgs.br/~comgradmat/tccs/monos_0802/TCC_Kelen.pdf>. Acesso em: 6 jan. 2013.

SÃO PAULO, Secretaria da Educação. **Caderno do Aluno**: Matemática, Ensino Médio- 2ª série. São Paulo: SEE, v. 1, 2009.

SÃO PAULO, Secretaria da Educação. **Caderno do Professor**: Matemática, Ensino Médio- 2ª série. São Paulo: SEE, v.1, 2009.

SÃO PAULO, Secretaria da Educação. Currículo do Estado de São Paulo: Matemática e suas Tecnologias. São Paulo: SEE, 2010.

SÃO PAULO, Secretaria da Educação. **Proposta Curricular para o Ensino de Matemática: 2º Grau**. 3.ed. São Paulo: SE/CENP, 1992.

SGARRO, A. **Códigos Secretos**. São Paulo: Companhia Melhoramentos, 1994.

O quadrado mágico de Lo Shu. Disponível em:
<http://en.wikipedia.org/wiki/Lo_Sh_Square>. Acesso em: 7 jan. 2013.

Codes and Ciphers Teaching Resources Website. Transposition. Disponível em :
<<http://www.cimt.plymouth.ac.uk/resources/codes/default.htm>>. Acesso em: 18 set. 2012.

APÊNDICE A : Lista com ditados populares utilizados na aula

- À noite todos os gatos são pardos.
- A união faz a força.
- Agora, Inês é morta.
- Água mole em pedra dura, tanto bate até que fura.
- Antes tarde do que nunca.
- Aprenda todas as regras e transgrida algumas.
- Aproveite a sorte enquanto ela está a seu favor.
- Aquele que só pensa em trabalho torna-se maçante.
- Aqui se faz, aqui se paga.
- As aparências enganam.
- Cada cabeça, uma sentença.
- Cada coisa a seu tempo.
- Cada macaco no seu galho.
- Cão que ladra não morde.
- Cautela nunca é demais.
- De grão em grão, a galinha enche o papo.
- De moeda em moeda se faz uma fortuna.
- Depois da tormenta, sempre vem a bonança.
- Desgraça pouco é bobagem.
- Devagar se vai longe.
- Dia de muito, véspera de pouco.
- Dizei-me com quem andas e eu te direi quem és.
- É melhor não cutucar a onça com vara curta.
- É melhor prevenir do que remediar.
- É na necessidade que se conhece o amigo.
- Em boca fechada não entra mosca.
- Em casa de ferreiro, espeto de pau.
- Em rio que tem piranha, jacaré nada de costas.
- Em terra de cego, quem tem um olho é rei.
- Falar é prata, calar é ouro.

- Gato escaldado tem medo de água fria.
- Mais vale um pássaro na mão do que cem voando.
- Melhor um pardal na mão do que um pombo no telhado.
- Na cama que farás, nela te deitarás.
- Nada como um dia após o outro.
- Não adianta chorar sobre o leite derramado.
- Não confie na sorte. O triunfo nasce da luta.
- Não conte com o ovo na barriga da galinha.
- Não há bem que sempre dure, nem mal que nunca se acabe.
- Não há marcas que o tempo não apague.
- Nem tudo que reluz é ouro.
- Nunca puxe o tapete dos outros, afinal você também pode estar em cima dele.
- Os melhores homens são os que as mulheres julgam melhores.
- Os últimos serão os primeiros.
- Papagaio come milho, periquito leva fama.
- Pense duas vezes antes de agir.
- Pense rápido, fale devagar.
- Pequenos riachos formam grandes rios.
- Quem desdenha quer comprar.
- Quem espera sempre alcança.
- Quem não tem cão caça com gato.
- Quem ri por último ri melhor.
- Quem semeia ventos, colhe tempestades.
- Quem tem boca vai a Roma.
- Quem tem pressa come cru.
- Quem tem telhado de vidro não atira pedra ao vizinho.
- Quem tudo quer, tudo perde.
- Santo de casa não faz milagre.
- Se cair, do chão não passa.
- Um homem prevenido vale por dois.
- Uma andorinha só não faz verão.

APÊNDICE B: Mensagens criptografadas pelos alunos

• As ocorrências enganam.
 • 19 letras.
 • Completamos a mensagem com "!"
 • $20 \text{ letras} = 2 \times 10 = 10 \times 2 = 5 \times 4 = 4 \times 5 = 20 \times 1 = 1 \times 20$.
 • Escolhemos a matriz 5×4 , ou seja, uma tabela com 5 linhas e 3 colunas.

| | | | |
|---|---|---|---|
| A | R | A | A |
| S | Ê | S | N |
| A | N | E | A |
| P | C | N | M |
| A | I | G | ! |

A R A A S Ê S N A N E A P C N M A I G !

• Aqui se faz, aqui se paga.
 • 19 letras.
 • Completamos a mensagem com "!"
 • $20 \text{ letras} = 2 \times 10 = 10 \times 2 = 5 \times 4 = 4 \times 5 = 20 \times 1 = 1 \times 20$.
 • Escolhemos a matriz 4×5 , ou seja, uma tabela com 4 linhas e 5 colunas.

| | | | | |
|---|---|---|---|---|
| A | S | Z | I | A |
| Q | E | A | S | G |
| V | F | Q | E | A |
| I | A | U | P | ! |

A S Z I A Q E A S G V F Q E A I A U P !

• Cada coisa a seu tempo.
 • 18 letras.
 • $18 \text{ letras} = 6 \times 3 = 3 \times 6 = 2 \times 9 = 9 \times 2 = 1 \times 18 = 18 \times 1$.
 • Escolhemos a matriz 6×3 , ou seja, uma tabela com 6 linhas e 3 colunas.

| | | |
|---|---|---|
| C | I | U |
| A | S | T |
| D | A | E |
| A | A | M |
| C | S | P |
| O | E | O |

C I U A S T D A E A A M C S P O E O

MENSAGEM

QUEM ri POR ULTIMO
ri MELHOR!

- 23 LETRAS
- COMPLETAMOS A MENSAGEM COM "!"
- 24 LETRAS = $3 \times 8 = 8 \times 3 = 2 \times 12 = 12 \times 2 = 1 \times 24 = 24 \times 1$
 $4 \times 6 = 6 \times 4$
- ESCOLHEMOS A MATRIZ 8×3 OU SEJA
UMA MATRIZ BELA COM 8 LINHAS E 3 COLUNAS

MATRIZ A (A15) 8×3

| O1 | O2 | |
|-----|------|--|
| QRI | !R0 | <ul style="list-style-type: none"> • O1 FOI MONTADA DO MODO TRADICIONAL SENDO ESCRITA NAS COLUNAS FICANDO TRAVADA DA SEGUINTE MANEIRA: • QRIUUMELLEMLRILHIMOPORO |
| UBM | ROP | |
| ELG | OMI | |
| MTL | HIR | |
| R1H | LTM | |
| 1MO | ELG | |
| POR | MUU | |
| OR! | IRAQ | |

• O2 FOI MONTADA DO MODO TRADICIONAL SENDO ESCRITA NAS COLUNAS MAS AO CONTRARIO, FICANDO TRAVADA DA SEGUINTE MANEIRA:

• 1. ROROPOMIHIRELMELEMUUR
Q"

1. MELHOR PREVENIR DO QUE REMEDIAR

E P R C
M R D M
C E O E
L V Q D
H E U I
O N E A
R I R R

E P R E M R D M E E O E L V Q D H E U I O N E A R I R R

2. CADA COISA A SEU TEMPO

C A I A U M
A C S S T P
D O A C E O

C A I A U M A C S S T P D O A C E O

3. DE MOEDA EM MOEDA SE FAZ UMA FORTUNA!

D A D Z R
E S A U T
M M S M U
D M C A N
E D E F A
D E A O !

D A D Z R E E A U T M M S M U O M G A N C O F F A D E A O !

| | | | | | | | | | | | | | | | | | |
|---------------|---|---|---|---|---|-------|---|---|---|---|---|---|---|---|---|---|---|
| A | R | R | B | E | D | S | E | E | E | Ç | O | M | S | S | M | | |
| A | C | A | T | T | C | R | H | I | O | A | O | A | Ã | R | M | M | C |
| 36 Juntas 6x6 | | | | | | | | | | | | | | | | | |
| A | R | R | B | E | D | | | | | | | | | | | | |
| S | E | E | E | Ç | O | | | | | | | | | | | | |
| m | S | S | M | A | C | | | | | | | | | | | | |
| A | T | T | C | R | H | | | | | | | | | | | | |
| i | O | A | O | A | Ã | | | | | | | | | | | | |
| O | R | m | m | m | O | 6 x 6 | | | | | | | | | | | |

"AS MAIORES TORRES TAMBÉM COMEÇARAM
DO CHÃO"

CADA COISA A SEU TEMPO

CAIAUM

18 LETRAS

ACSSTP

3x6

DOAEEEO

CAIAUMACSSTPDOAEEEO

QUEM SEMEIA VENTOS COLHE TEMPESTADES

QSINCEPA

32 LETRAS

VEATOTED

EMVOLESE

MEESHMTS

4x8

QSINCEPAVEATOTEDEMVOLESEMEESHMTS

ANTES TARDE DO QUE NUNCA

ASDBU

20 LETRAS

NTEUN

TADEC

ERONA

4x5

ASDBUNTEUNTADECERONA

A NOITE TODOS GATOS SÃO PARDOS

ATDASA

NEOTAR

OTSOOD

POGSPD

4x6

ATDASANEOTAROTSOODIOSPO

| | | |
|---------------------|-----------------------------|---|
| O S M E L H O R E S | H O M E S S A O O S | Q U E A S M U L H E R G S J U L G A M M E |
| L H O A E S | | |
| 4 B L E T R A S | N U M E R O M P O A | L I S T A |
| 4 B = 1 x 4 B | 4 B X 1 | 4 X 1 2 |
| 3 x 1 6 | 1 6 X 3 | 4 X 2 |
| | | 2 X 2 4 |
| | | 2 4 X 2 |
| | | 4 X 1 2 |
| | | 1 2 X 4 |
| O E S A E M | | |
| S S A S S E | | |
| M H O M S L | | |
| E O O U U H | | |
| L M S L L O | | |
| H E Q H G R | | |
| O N U G A E | | |
| R S E R M S | | |
| O E S A E M S | S A S S E M H O M S L E O O | V U X L M S L L O H E G H 6 R O M U E A E |
| R S E R M S | | |

• QUEM TEM PRESSA
COME CRU

• 20 Letras

• 20 Letras = $4 \times 5 = 5 \times 4 = 2 \times 10 = 10 \times 2 = 1 \times 20 = 20 \times 1$

• Escolhemos a matriz 5×4 , ou seja uma tabela
(com 5 linhas e 4 colunas)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Q | E | S | M | Q | E | S | M | U | M | S |
| U | M | S | E | E | E | P | A | C | M | P |
| E | P | A | C | E | R | T | E | O | U | |
| M | P | C | R | | | | | | | |
| T | E | O | U | | | | | | | |

2012

MENSAGEM

NÃO há MARCAS QUE O TEMPO NÃO APAGUE!
COMPLETAMOS A MENSAGEM COM "!"

30 LETRAS

MONTAREMOS UMA TABELA COM 5x6

| | | | | | |
|---|---|---|---|---|---|
| N | M | S | T | N | A |
| Ã | A | Q | E | Ã | G |
| O | R | U | M | O | U |
| H | C | E | P | A | E |
| Ã | A | O | O | P | ! |

NmstNAÃAQEÃGORUMOUHCEPAEÃAOPP!

APÊNDICE C: Relatório realizado pelos alunos no final das atividadesRelatório de Matemática

Como aprendemos desde sempre, a matemática é um estudo que só aprimoramos com o passar do tempo, porque é consideravelmente um ser obscuro, e de difícil total compreensão.

Com o passar dos anos, subimos um patamar da escada para o aprendizado da matemática, um nível por vez; soma, subtração, divisão e multiplicação; fração; logaritmo e hoje atualmente utilizamos a matriz para resolvermos a criptografia.

E falando sério, funcionou mesmo, e hoje ainda estou em degraus baixos, comparando com o que existe neste mundo.

Relatório Matemática

A matéria desenvolvida hoje em sala de aula foi melhor do que nos outros dias; pois foi produzida em trio com os colegas, que desenvolveram um bom trabalho.

O trabalho que fizemos foi fácil com os conhecimentos que o professor nos passou nas aulas anteriores, tivemos uma boa aptidão para resolver os exercícios.

Na minha opinião trabalhar em sala de aula desse modo, é muito melhor pois todas interagem umas com as outras, e também não tem aquela pressão de como se fosse um prova, então achamos que é muito melhor a aula dessa maneira

O Trabalho de criptografia foi muito legal pois essa aula que tivemos foi diferente do que as outras aulas foi uma aula descontraída

Na aula de matemática do Prof^o Rinaldo do dia 22/11/12 fizemos uma atividade bem criativa, onde cada um dos alunos presente na aula, pode se juntar em grupo para resolver uma atividade proporcionado pelo professor. Assim podemos discutir entre as grupos, resolvendo em equipe, até chegar a um certo resultado final.

As atividades proporcionado ia nós alunos criptografia, um assunto prático e fácil para ser resolvido em equipe!

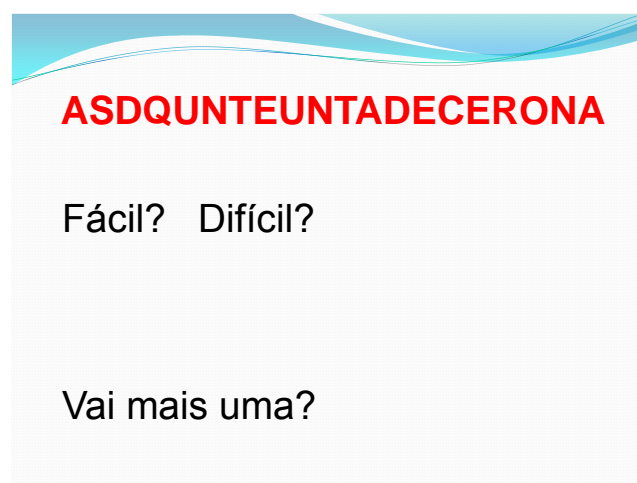
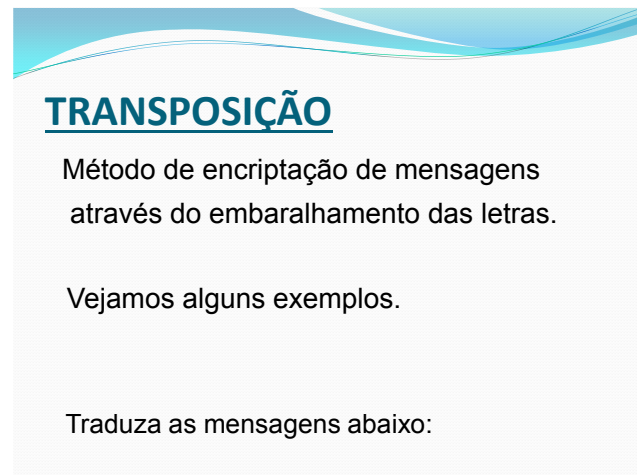
A matemática em sua forma prática, se revela como algo bem mais divertido e profundo do que sua forma teórica, que é a mais usada no universo da matemática.

Todas as atividades que nos são oferecidas na forma prática são melhores e cuidadosamente mais trabalhadas, pois, nos proporcionam trabalhos com coisas realmente interessantes de forma simplificada e divertida.

Um exemplo, é a produção de mensagens criptografadas, um modo de "ocultar" frases, utilizando o clássico sistema de matrizes. Outro exemplo foi a realização de um trabalho pedido pelo professor Renaldo, sobre o esquema de construção das colmeias utilizadas pelas abelhas. Neste trabalho, foram utilizadas diferentes formas geométricas com as mesmas medidas, e depois, com cálculos precisos, chegamos à conclusão de qual forma mais proporcionaria benefícios às abelhas.

Com isto, podemos concluir que a matemática é divertida, ao contrário do que a maioria das pessoas pensam, ela é apenas mal explorada.

APÊNDICE D Sequência de Slides da aula



AOFUFONARIZÇÃAA.

E aí? Mais fácil?

Ainda não?

Vamos ao segredo...

A **transposição** consiste em trocar as letras ou símbolos de lugar para a codificação de mensagens. Tais trocas devem ser realizadas através de um padrão que inclua um certo nível de dificuldade, dependendo da importância do conteúdo da mensagem.

Nosso método consiste em embaralhar as letras através de **tabelas**. Mas como? Primeiro vamos entender um pouco sobre tabelas.

Façamos um breve estudo sobre tabelas(matrizes) para utilizar os conceitos sobre matriz transposta na solução das mensagens.

Matriz

Chama-se matriz do tipo $m \times n$ (lê-se m por n) toda tabela de números dispostos em m linhas e n colunas. Tal tabela deve ser representada entre parênteses $()$, entre colchetes $[]$ ou entre barras duplas $|| \ ||$.

Exemplos:

$$a) A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}_{2 \times 3} \quad \text{lê-se: matriz } A \text{ de ordem } 2 \text{ por } 3$$

$$b) B = \begin{bmatrix} 0 & 0 & 1 \\ 5 & 6 & 0 \\ 2 & 2 & 2 \end{bmatrix}_{3 \times 3} \quad \text{lê-se: matriz } B \text{ de ordem } 3$$

Representação Genérica de uma matriz

Podemos representar genericamente uma matriz A do tipo $m \times n$ da seguinte maneira:

$$A_{m \times n} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{pmatrix}$$

Essa matriz representa uma matriz de qualquer ordem $m \times n$.

Um modo simplificado de fazer a representação é:

$$A = [a_{ij}]_{m \times n}, \text{ sendo } m, n \in \mathbb{N}^*.$$

Onde:

- a_{ij} : é o elemento da matriz, sendo os índices i e j indicadores da posição do elemento na matriz
- o índice i indica linha, $1 \leq i \leq m$
- o índice j indica a coluna, $1 \leq j \leq n$

Exemplo:

O elemento a_{13} (lê-se: a um três) ocupa a primeira linha e a terceira coluna da tabela.

Tipos de matrizes

As matrizes são classificadas de acordo com seu formato e com os números que as compõe.

Como exemplo, temos a matriz quadrada, matriz identidade, matriz linha, matriz coluna, matriz diagonal, entre outras.

Nosso estudo será realizado em um desses modelos, a matriz transposta.

Dada a matriz A de ordem $m \times n$, chama-se matriz transposta de A indicada por A^t a matriz cuja ordem é $n \times m$, sendo as suas linhas ordenadamente iguais às colunas da matriz A .

Exemplos

$$a) \text{ Se } A = \begin{bmatrix} 1 & -3 \\ 2 & 4 \end{bmatrix}, \text{ então } A^t = \begin{bmatrix} 1 & 2 \\ -3 & 4 \end{bmatrix}$$

$$b) \text{ Se } B = \begin{bmatrix} 1 & 0 & 4 & 9 \\ 2 & -4 & 3 & 5 \end{bmatrix}, \text{ então } B^t = \begin{bmatrix} 1 & 2 \\ 0 & -4 \\ 4 & 3 \\ 9 & 5 \end{bmatrix}$$

Bom, agora que já sabemos um pouco mais sobre tabelas ou matrizes, vamos aprender como decifrar as mensagens.

Primeiro vamos escolher a mensagem.

SE CAIR, DO CHÃO NÃO PASSA.

Contamos as letras.

Um total de 20 letras.

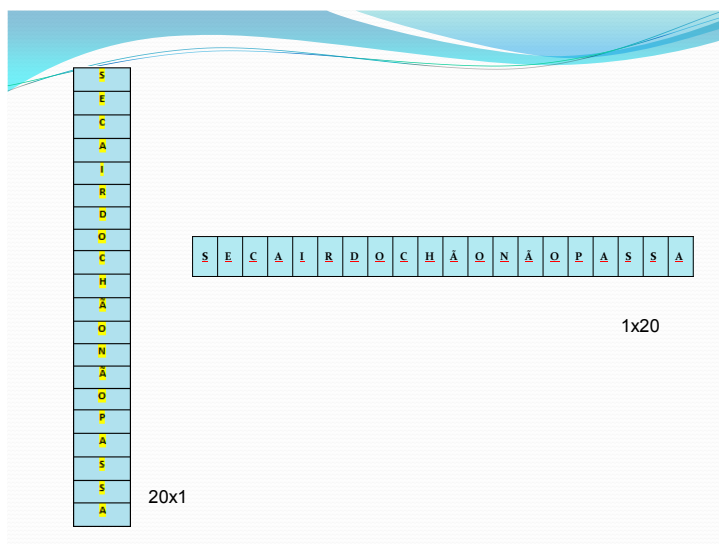
Vejamos:

$$20 = 1 \times 20 = 2 \times 10 = 4 \times 5 = 5 \times 4 = 10 \times 2 = 20 \times 1.$$

Temos um total de 6 produtos que resultam 20, obtendo assim 6 tipos diferentes de matrizes que podemos formar com os produtos acima.

Dos 6 produtos, descartamos 20×1 e 1×20 , pois não servirão ao nosso propósito.

Com o produto 20×1 , teremos uma tabela com 20 linhas e uma coluna apenas, assim as letras não são embaralhadas como queremos. Já no produto 1×20 , teremos uma tabela com uma linha e 20 colunas, que também não embaralha as letras. Nas duas configurações não obteremos sucesso na encriptação da mensagem proposta.



Restaram 4 produtos dos quais escolhemos um.

4x5

Façamos então uma matriz com 4 linhas e cinco colunas

$$\text{Matriz } A = [a_{ij}]_{4 \times 5}$$

| | | | | |
|--|--|--|--|--|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Vamos preencher a tabela com a mensagem.
Cada letra na sua gaveta.

| | | | | |
|----------|----------|----------|----------|----------|
| S | I | C | N | A |
| E | R | H | Ã | S |
| C | D | Ã | O | S |
| A | O | O | P | A |

Observe que cada letra corresponde a um elemento A_{ij} da matriz escolhida.

| | | | | |
|---------------------|---------------------|---------------------|---------------------|---------------------|
| $a_{11} = \text{S}$ | $a_{12} = \text{I}$ | $a_{13} = \text{C}$ | $a_{14} = \text{N}$ | $a_{15} = \text{A}$ |
| $a_{21} = \text{E}$ | $a_{22} = \text{R}$ | $a_{23} = \text{H}$ | $a_{24} = \text{Ã}$ | $a_{25} = \text{S}$ |
| $a_{31} = \text{C}$ | $a_{32} = \text{D}$ | $a_{33} = \text{Ã}$ | $a_{34} = \text{O}$ | $a_{35} = \text{S}$ |
| $a_{41} = \text{A}$ | $a_{42} = \text{O}$ | $a_{43} = \text{O}$ | $a_{44} = \text{P}$ | $a_{45} = \text{A}$ |

Como escrevemos a mensagem em colunas, agora embaralhamos as letras escrevendo a mensagem criptografada em linhas, ou seja, façamos a matriz transposta da matriz $A = [a_{ij}]_{4 \times 5}$, a qual denominamos $A^t = [b_{ij}]_{5 \times 4}$, onde $b_{ij} = a_{ji}$. As colunas da matriz A agora são linhas na matriz A^t .

| | | | |
|---------------------|---------------------|---------------------|---------------------|
| $b_{11} = \text{S}$ | $b_{12} = \text{E}$ | $b_{13} = \text{C}$ | $b_{14} = \text{A}$ |
| $b_{21} = \text{I}$ | $b_{22} = \text{R}$ | $b_{23} = \text{D}$ | $b_{24} = \text{O}$ |
| $b_{31} = \text{C}$ | $b_{32} = \text{H}$ | $b_{33} = \text{Ã}$ | $b_{34} = \text{O}$ |
| $b_{41} = \text{N}$ | $b_{42} = \text{Ã}$ | $b_{43} = \text{O}$ | $b_{44} = \text{P}$ |
| $b_{51} = \text{A}$ | $b_{52} = \text{S}$ | $b_{53} = \text{S}$ | $b_{54} = \text{A}$ |

Escrevemos a mensagem como apareceu nas colunas:

SICNAERHÃSCDÃOSAOPA

Pronto. Temos aí o nosso segredo.

De um modo prático, basta colocar a mensagem em uma tabela e, se for escrita em colunas, devemos embaralhar as letras escrevendo-as na ordem em que apareceram nas linhas.

Para decifrar a mensagem, basta fazer o procedimento inverso.

Mas não é só isso não.

Escolhemos a mensagem observando a quantidade de letras contidas nela.

Tal quantidade não pode ser um número primo, pois assim não teremos alternativas para as tabelas.

Quanto maior for a decomposição do número que totaliza a quantidade de letras da frase, mais difícil fica a revelação da mensagem, pois teremos um maior número de tabelas.

Vejam os:

O número 24 é igual a $2^3 \cdot 3$. Temos para 24 os seguintes divisores: 1, 2, 3, 4, 6, 8, 12 e 24. Assim:

$$24 = 1 \times 24 = 2 \times 12 = 3 \times 8 = 4 \times 6 = 6 \times 4 = 8 \times 3 = 12 \times 2 = 24 \times 1$$

Oito produtos que resultam em 24, ou seja, oito tabelas, das quais podemos utilizar com segurança, pelo menos 4:

$$4 \times 6; 3 \times 8; 8 \times 3; 6 \times 4$$

O primeiro número de cada produto resulta na quantidade de linhas e o seguinte na quantidade de colunas da matriz escolhida.

Para terminar...

ASDQUNTEUNTADECERONA

20 letras. Possivelmente deve ser 4×5 ou 5×4 . Caso contrário tentaremos 2×10 ou 10×2 .

Tentaremos 4×5 . 4 linhas e 5 colunas.

| | | | | |
|---|---|---|---|---|
| A | S | D | Q | U |
| N | T | E | U | N |
| T | A | D | E | C |
| E | R | O | N | A |

ANTES TARDE DO QUE NUNCA

AOFUFONARIZÇÃAA

15 letras. Tentaremos 3x5 OU 5x3.

Utilizaremos 3 linhas e 5 colunas.

| | | | | |
|---|---|---|---|---|
| A | O | F | U | F |
| O | N | A | R | I |
| Z | Ç | Ã | A | A |

Não fez sentido. Vamos fazer então uma tabela com três colunas e cinco linhas.

| | | |
|---|---|---|
| A | O | F |
| U | F | O |
| N | A | R |
| I | Z | Ç |
| Ã | A | A |

A UNIÃO FAZ A FORÇA.

Ainda poderíamos embaralhar as linhas e colunas, assim o grau de dificuldade aumentaria.

Nesta aula, utilizamos a transposição de letras para trabalhar uma aplicação de matriz transposta. Podemos relacionar a transposição de letras com números primos e compostos, fatoração e decomposição assim como apresentar a Matemática de maneira interessante aos alunos.

Observação

Se a frase desejada contiver uma quantidade de letras que seja número primo, podemos encaixar nessa frase um outro símbolo que denominamos “coringa”. Pode ser um @, um #, um \$, etc. Assim teremos um número composto como quantidade de letras.

Prof. Reinaldo