UNIVERSIDADE ESTADUAL DO MARANHÃO - UEMA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO - PPG
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Katarine Araújo Baldez de Carvalho

A Criptografia no Ensino da Matemática: aplicações para a Educação Básica

São Luís - MA
2018

KATARINE ARAÚJO BALDEZ DE CARVALHO

A Criptografia no Ensino da Matemática: aplicações para a Educação Básica

Dissertação apresentada à Universidade Estadual do Maranhão – UEMA, como pré-requisito para obtenção do Título de Mestre em Matemática, através do Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT

Orientador: Professor Dr. João Coelho Silva Filho

São Luís - MA

2018

Carvalho, Katarine Araújo Baldez de.
A criptografia no ensino da matemática: aplicações para a educação básica / Katarine Araújo Baldez de Carvalho.– São Luís, 2018.

127 f

Dissertação (Mestrado) – Curso de Matemática em Rede Nacional, Universidade Estadual do Maranhão, 2018.

Orientador: Prof. Dr. João Coelho Silva Filho.

1.Criptografia. 2.Teoria dos números. 3.Aritmética modular. I.Título

CDU: 511:37

Katarine Araújo Baldez de Carvalho

A Criptografia no Ensino da Matemática: aplicações para a Educação Básica

Dissertação apresentada à Universidade Estadual do Maranhão – UEMA, como pré-requisito para obtenção do Título de Mestre em Matemática, através do Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT

Orientador: Professor Dr. João Coelho Silva Filho

Aprovado em: 31 de outubro de 2018

BANCA EXAMINADORA

Prof. Dr. João Coelho Silva Filho
(Universidade Estadual do Maranhão – UEMA)

Prof. Dr. Renato Fabrício Costa Lobato
(Universidade Federal do Pará – UFPA)

Prof. Drª. Valeska Martins de Souza
(Universidade Federal do Maranhão – UFMA)

São Luís
2018

Agradecimentos

Agradeço, primeiramente, a Deus pelo dom da vida e por me permitir vivenciar este momento que, por vezes, pensei que não alcançaria.

Agradeço às minhas filhas, Juliana e Camila, meus maiores tesouros e os amores da minha vida que, mesmo com tão pouca idade, conseguiram ser pacientes e compreensivas diante da minha ausência em determinados momentos, que me impediam de dar a atenção necessária e merecida, em função das aulas e dos momentos em que me dedicava aos estudos e à elaboração deste trabalho.

Agradeço a Pedro Barbosa de Carvalho Júnior, que me incentivou a fazer o curso e me deu o apoio necessário, durante o período em que estivemos casados, sendo compreensivo nos momentos em que precisava.

Agradeço a minha família, meu pai, Vital Magno, minha mãe, Terezinha de Jesus (in memorian), e meus irmãos Karine e Alexandre, que sempre acreditaram em mim e demonstraram orgulho com o meu cerescimento pessoal e profissional.

Agradeço aos meus tios, tias, primos e amigos que, direta ou indiretamente, estavam sempre me apoiando e me dando força para continuar crescendo e superando os obstáculos que precisei enfrentar nesse período.

Agardeço aos meus diretores, Cel. Anderson Fernando Holanda Maciel e Claudiana Pereira de Sousa, por terem me apoiado e proporcionado condições para que eu pudesse fazer o curso e desenvolver as atividades de pesquisa deste trabalho.

Agradeço aos meus alunos que souberam entender o momento que estava vivendo, demonstrando carinho e compreensão.

Agradeço aos colegas do Mestrado Profissonal - Profmat UEMA turma 2016, Aristoteles, Clessio, Darcio, Diwey, Enildo, Erivelton, José Alexandre, José Nazareno, Mario, Paulo, Valderlândio, Willanickson e, em especial, ao Vilson, por todos os momentos de união e colaboração da turma, pelas brincadeiras, pela amizade, pelo respeito e principalmente pelo conhecimento compartilhado entre todos.

Agradeço ao meu orientador, Profº. Drº. João Coelho Silva Filho, que foi fundamental na realização e conclusão deste trabalho, sendo compreensivo e me cobrando quando necessário.

"Motivação é o que faz você começar.
Hábito é o que mantém seguindo em frente."

Jim Rohn

RESUMO

O trabalho apresenta uma análise do uso da Criptografia no ensino da Matemática, despertando no estudante um maior interesse pela disciplina através da realização de atividades práticas, desenvolvidas dentro de um projeto intitulado "Desvendando Segredos", e fazendo-se uso de algumas das mais conhecidas cifras criptográficas, associadas a conteúdos matemáticos que são abordados no ensino fundamental e médio. A pesquisa foi desenvolvida sobre os principais conceitos aplicados em criptografia, fatos históricos relevantes que contribuíram para o desenvolvimento da criptografia e algumas cifras criptográficas utilizadas para cifrar e decifrar uma mensagem. O método motiva os estudantes no aprendizado da matemática e no aprofundamento dos conteúdos aplicados na sala de aula.

PALAVRAS-CHAVE: Criptografia. Teoria dos Números. Aritmética Modular.

ABSTRACT

The work presents an analysis of the use of Cryptography in the teaching of Mathematics, awakening in the student a greater interest in the discipline through the accomplishment of practical activities, developed within a project titled “Unraveling Secrets ”, and making use of some of the most The research was developed on the main concepts applied in cryptography, relevant historical facts that contributed to the development of cryptography and some cryptographic ciphers used to encrypt and decrypt a message. The method motivates students to learn mathematics and to deepen the content applied in the classroom.

KEYWORDS: Encryption. Theory of Numbers. Modular Arithmetic.

Lista de Figuras

Sumário

1 INTRODUÇÃO

A educação formal é parte fundamental da vida de cada pessoa, pois prepara o indivíduo para atuar de forma efetiva junto à sociedade. Assim, é possivel transformar o meio onde vive, em função das necessidades econômicas, sociais e políticas da coletividade, oferecendo-lhe o conhecimento científico necessário para isso.

Portanto, à medida que tais necessidades evoluem com o passar do tempo, se faz necessário que os educandos estejam preparados para lidar com essas mudanças e que consigam acompanhar os avanços da sociedade. A educação não deve ter apenas o papel de instruir, mas também de mostrar o quão prazeroso pode ser o ato de conhecer e de descobrir, nos fazendo crescer como indivíduos.

A matemática tem um papel essencial nesse processo educacional, pois é considerada uma ciência viva, ou seja, está em constante evolução. Sendo assim, é sempre possível rever conceitos, alterar pontos de vista sobre determinados assuntos e propor novas teorias, estando presente no cotidiano das pessoas, nas instituições de ensino superior e nos centros de pesquisas, onde novos conhecimentos são produzidos e utilizados na solução de problemas científicos e tecnológicos.

O professor de matemática é o elo entre o conhecimento formal da disciplina e a sociedade, sendo ele o responsável por mediar e gerenciar esse conhecimento, sempre atuando de forma a levar o educando a desenvolver um pensamento crítico diante dos conteúdos abordados em sala de aula. Dessa forma, é necessário que o professor de matemática, em especial o que atua na educação básica, consiga ministrar uma aula dinâmica, contextualizada e que considere a experiência de vida desse educando e seu conhecimento de mundo, de modo a despertar nele a vontade de aprofundar o conhecimento e de buscar diferentes caminhos para chegar a um mesmo resultado.

Contudo, essa não é uma tarefa fácil para muitos professores de matemática, em especial, aqueles que atuam nas escolas públicas municipais e estaduais. Os docentes dessas instituições de ensino enfrentam péssimas condiçoes de trabalho sendo, em grande parte, o quadro, o apagador e o pincel as únicas ferramentas de trabalho disponibilizadas a eles.

Deve-se ressaltar, também, a formação acadêmica do professor de matemática que, em sua maioria, tiveram uma formação tradicionalista o que leva muitos educadores a se tornarem meros reprodutores do conhecimento adquirido, ministrando aulas monótonas,

cansativas e sem conexão com a realidade do aluno, contribuindo assim, para que um grande número de estudantes sintam-se desmotivados e não tenham interesse pela disciplina.

É importante citar que a aprendizagem não depende, exclusivamente, do professor. O aluno tem um papel tão importante quanto o docente, pois é ele o objeto alvo nesse processo. Porém, muitas vezes, a reponsabilidade da não aprendizagem do aluno recai apenas sobre o educador, tornando o processo desigual e fazendo com que muitos se sintam desestimulados.

A partir dessas reflexões, surge uma pergunta: de que maneira os professores de matemática podem melhorar a sua prática de modo a desenvolver nos estudantes o interesse pela disciplina e o desejo de buscar novos conhecimentos, aprofundando aqueles que já lhes foram apresentados e lhes dando autonomia de investigar outros?

Acredita-se que transformar a matemática em uma disciplina prática, que associe os conteúdos trabalhados em sala de aula com situações reais vivenciadas pelo aluno e/ou que produza materiais concretos utilizando esse conteúdos na sua contrução ou no seu funcionamento seja uma forma de despertar o interesse pela matemática, levando-os a estar sempre em busca de adquirir novos conhecimentos.

Desse modo, desenvolveria uma característica pouco observada nesses estudantes: o desejo de investigar. Consequentemente, transformando-os em protagonistas na construção da sua aprendizagem. Ao mesmo tempo, desmistificando ideias, há muito difundidas, de que a matemática, por ser uma ciência exata, não exige a necessidade de pensar, pois tem sempre uma fórmula pronta para resolver todos os problemas, o que de fato é uma inverdade.

Assim, o professor de matemática deve pensar na investigação como uma estratégia de ensino a ser desenvolvida com o seu aluno e que, tal estratégia, não se resume em buscar informações prontas para que lhes sejam dados novos significados, reconstruindo um conhecimento pré-existente. A investigação deve ser pensada, acima de tudo, como a possibilidade de os estudantes realizarem suas próprias descobertas.

No ensino da matemática, tem-se buscado diferentes campos investigativos que ainda tenham sido pouco explorados na educação básica e que tenham potencial para despertar nos estudantes o interesse pela disciplina. Nesse contexto, a Criptografia foi escolhida como tema central da pesquisa por ter, como ferramenta principal, os recursos

matemáticos utilizados para transformar um texto compreensível em um texto secreto. Ao mesmo tempo, permite fazer o contrário, ou seja, desvendar um texto secreto tornando-o compreensível ao receptor da mensagem.

Atualmente, a criptografia é utilizada, principalmente, em ferramentas computacionais, que empregam a internet para transmissão de informações. Muitas dessas ferramentas são amplamente utilizadas pelos jovens, que em sua maioria, demonstram um grande fascínio pelo uso da tecnologia.

Considerando o fato de que esses jovens apresentam características frequentemente observadas nessa etapa da vida tais como a curiosidade, a impulsividade, a inquietação e o desejo de descobrir coisas novas, leva a acreditar que o mistério que envolve o conteúdo de mensagens secretas possa gerar nesses indivíduo uma ânsia cada vez maior em tentar descobri-lo, dando-lhes uma motivação a mais em buscar nos conteúdos matemáticos diferentes formas e métodos que os ajudem nessa tarefa.

A pesquisa contribui com o trabalho do professor de matemática que atua nos ensinos fundamental e médio, oferecendo-lhe um recurso que o ajude a estimular a curiosidade do estudante. À vista disso, o docente busca desenvolver o desejo investigativo do aluno, com base na observação, na manipulação de materiais, na exploração de conhecimentos e na verificação de resultados. Dessa maneira, o profissional contribui com o processo de desenvolvimento do senso crítico desse estudante e promove um novo significado ao estudo da matemática.

O trabalho analisa o uso da Criptografia no ensino da matemática por meio da proposição de atividades práticas e da resolução de situações problemas que abranjam conteúdo das séries finais do ensino fundamental e do ensino médio, verificando, assim, os resultados obtidos.

A contribuição principal do trabalho é a investigação da evolução histórica da criptografia, relacionando-a aos conteúdos matemáticos do ensino fundamental e do ensino médio, segundo o estudo das cifras criptográficas de maior relevância, o desenvolvimento de atividades práticas e a realização de experimentos com os alunos desses níveis de ensino, levando-os estabelecer uma conexão com o tema proposto e a avaliar o grau de compreensão e de interesse dos mesmos durante as atividades práticas.

No Capítulo 2, são estudadas algumas definições e resultados sobre Conjuntos, Relações e Funções, que servem de pré-requisito para o desenvolvimento de aplicações

apresentadas no trabalho. O referencial teórico utilizado na formulação deste capítulo é explorado no livro do Andrade.

No Capítulo 3, são apresentadas definições e resultados da Teoria dos Números e Aritméica Modular, que são utilizados no desenvolvimento deste trabalho. O referencial teórico utilizado na formulação deste capítulo é explorado nas obras de: Almeida, Coutinho, Galvão e Schlittler.

No Capítulo 4, descreve-se sobre a Criptografia, seus principais conceitos e evolução histórica, destacando-se alguns métodos criptográficos como a cifra de César, a cifra de Vigenère, a cifra de Hill e o sistema RSA. O referencial teórico utilizado na formulação deste capítulo é explorado nas obras de: Andrade, Bezerra, Cardoso, Coutinho, Dantas, Jansen, Singh e Souza.

No Capítulo 5, são apresentadas as atividades propostas e os resultados observados a partir de suas aplicações. Finalmente, no Capítulo 6, é realizada uma abordagem conclusiva.

2 CONJUNTOS, RELAÇÕES E FUNÇÕES

Neste capítulo, serão trabalhados conteúdos acerca de conjuntos e e de suas propriedades e das relações entre as grandezas, estudando as principais ideias relacionadas às funções e que estão associadas com o tema central do trabalho: a criptografia no ensino da matemática. Para tanto, serão abordados alguns tópicos trabalhados no ensino fundamental e médio. O referencial teórico utilizado na formulação deste capítulo é explorado no livro do Andrade, onde encontram-se demonstrados os teoremas apresentados.

2.1 Conjuntos

A noção de conjuntos é frequentemente usada quando se agrupa dois ou mais objetos de acordo com critérios de semelhança a eles atríbuídos. A ideia matemática de conjuntos segue este mesmo princípio, ou seja, agrupar elementos que obedeçam a um mesmo conjunto de regras e/ou propriedades bem definidas.

A teoria dos conjuntos é a estrutura para o pensamento da matemática abstrata, sendo tratado, neste trabalho, em uma abordagem formal e deliberadamente fundamentada no rigor puramente matemático.

Definição 2.1. *Um conjunto, também chamado de coleção, é composto por objetos bem definidos, sendo tais objetos chamados de elementos ou membros.*

Os conjuntos são usualmente designados (representados) por uma letra maiúscula do nosso alfabeto e os elementos por letras minúsculas.

Particularmente, emprega-se as seguintes notações:

I- $\mathbb{N}$ denota o conjunto de todos os números naturais $1, 2, 3, ...$

II- $\mathbb{Z}$ é o conjunto de todos os números inteiros $0, \pm 1, \pm 2, \pm 3, ...$

III- $\mathbb{Q}$ é o conjunto de todos os números racionais, isto é, frações $\frac{m}{n}$, onde m, n são números inteiros e $n \neq 0$.

IV- $\mathbb{R}$ é o conjunto de todos os números reais.

VI- $\mathbb{C}$ é o conjunto de todos os números complexos $a + bi$, onde a, b são números reais e $i^2 = -1$.

Se um elemento x é membro do conjunto A, diz-se que x pertence a A. Em símbolo, $x \in A$.

No caso contrário, isto é, se x não é membro do conjunto A, diz-se que x não pertence a A. Em símbolo, $x \notin A$.

Definição 2.2. *Seja A e B conjuntos. Diz-se que A e B são iguais, se os elementos que pertencem a A também pertencem a B e os elementos que pertence a B pertencem A, isto é, A e B consistem dos mesmos elementos. Em símbolo,*

$$A = B \Leftrightarrow x \in A \Rightarrow x \in B \; e \; x \in B \Rightarrow x \in A.$$

Os elementos de um conjunto com um número finito de elementos podem ser descritos com seus elementos entre chaves e separados por vírgula. A ordem em que os elementos aparecem não altera o conjunto e os elementos repetidos não tem efeito no conjunto.

Os conjuntos considerados são parte integrante de um conjunto U, denominado conjunto universo. Um conjunto é determinado por todos os elementos que satisfazem uma propriedade P, o qual denota-se

$$\{x \in U | P(x)\}.$$

Definição 2.3. *Seja A e B conjuntos. Diz-se que A é um subconjunto de B, se todo elemento de A é elemento de B. Em súmbolo,*

$$x \in A \Longrightarrow x \in B.$$

Se existe elemento que pertence A e não pertence a B. então A não é subconjunto de B e escreve-se A $\not\subset B$. Por exemplo,

$$N \subset Z \subset Q \subset R \subset C.$$

Existem propriedades que não satisfazem a qualquer elemento. Assim, o conjunto $\{x \in U | P(x)\}$ não possui elementos. Este conjunto é denominado conjunto vazio e denotado por $\emptyset$.

Teorema 2.1. *Sejam A, B e C subconjuntos de U. Então,*

1 **-** $A \subseteq A$ *e* $\emptyset \subseteq A, \forall A$;

2 **-** $A \subseteq \emptyset \Leftrightarrow A = \emptyset$;

3 **-** $A \subset B$ *e* $B \subset A \Leftrightarrow A = B$;

4 **-** $A \subseteq B$ *e* $B \subseteq C \Rightarrow A \subseteq C$.

Definição 2.4. *Sejam A, B e C subconjuntos de U:*
A união B é o conjunto dos elementos x que pertencem a A ou pertencem a B e é denotado por $A \cup B$. *Em símbolo,*

$$A \cup B = \{x | x \in A \text{ ou } x \in B\}.$$

A interseção B é o conjunto dos elementos x que pertencem a A e pertencem a B, simultaneamente, e denotado por $A \cap B$. *Em símbolo,*

$$A \cap B = \{x | x \in A \text{ e } x \in B\}.$$

A diferença de A e B é o conjunto dos elementos x que pertencem a A e não pertencem a B e denotado por $A - B$. *Em símbolo,*

$$A - B = \{x | x \in A \text{ e } x \notin B\}.$$

Teorema 2.2. *Sejam A, B e C subconjuntos de U. Então,*

1 **-** $A \subset A \cup B$ *e* $B \subset A \cup B$;

2 **-** $A \cap B \subset A$ *e* $A \cap B \subset B$;

3 **-** $A - B \subset A$;

4 **-** $A \cup B = (A \cap B) \cup (A - B) \cup (B - A)$.

Se $A \cap B = \emptyset$, diz-se que A e B são disjuntos.

Se $B \subset A$, a diferença $A - B$ é denominada de complementar de B em relação a A e denotado por

$$C_A(B).$$

2.2 Relações

Para iniciar o estudo das relações é necessário rever alguns conceitos que estão associados a esse estudo. Dessa forma, serão apresentados os conceitos de par ordenando e produto cartesiano.

2.2.1 Par Ordenado

Um *par* é um conjunto formado por dois elementos. Assim, $\{1, 2\}$, $\{-2, 3\}$ e $\{a, b\}$ são exemplos de pares.
Sabe-se que a ordem dos elementos dentro do conjunto não gera um novo conjunto, portanto:

$$\{1, 2\} = \{2, 1\}, \{-2, 3\} = \{3, -2\}, \{a, b\} = \{b, a\}$$

Mas alguns problemas em matemática necessitam que seja feita uma distinção entre pares considerando-se a ordem dos elementos dentro do conjunto.

Definição 2.5. *Sejam x e y elementos de um conjunto A. Então o conjunto $\{\{x\}, \{x, y\}\}$ é chamado par ordenado, em símbolos (x, y); x é chamada a primeira componente (ou coordenada) e y a segunda componente (ou coordenada).*

De acordo com a definição dada, será chamado de *par ordenando* o conjunto de dois elementos em que para cada elemento a e cada elemnto b, existe um terceiro elemento (a, b), de modo que:

$$(a, b) = (x, y) \iff a = x \text{ e } b = y.$$

2.2.2 Produto Cartesiano

Definição 2.6. *Dados dois conjuntos A e B não vazios, denomina-se produto cartesiano de A por B, indicado por $A \times B$, o conjunto cujos elementos são todos os pares ordenados (x, y), em que a 1^a coordenada pertence a A e a 2^a, a B:*

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

Quando $A = B$, tem-se o produto cartesiano $A^2 = A \times A$. O subconjunto

$$D = \{(a, b) \in A^2 : a = b\}$$

é chamado a diagonal de A^2.

Exemplo 2.1. *Dados os conjuntos* $A = \{0, 1\}$ *e* $B = \{1, 2, 3\}$*, os produto cartesianos* $A \times B$ *e* $B \times A$ *são:*

$$A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3)\}$$

e

$$B \times A = \{(1, 0), (1, 1), (2, 0), (2, 1), (3, 0), (3, 1)\}.$$

2.2.3 Relações

Definição 2.7. *Sejam* A*,* B *conjuntos e* R *um subconjunto de* $A \times B$*. Então* R *é chamado uma relação de* A *para* B*. Se* $(x, y) \in R$*, então diz-se que* x *está relacionado com* y*, em símbolos* $x \ R \ y$*. Quando* $A = B$ *diz-se que* R *é uma relação em* A*.*

Em outras palavras, dado um produto cartesiano $A \times B$, denomina-se relação de A em B qualquer subconjunto de $A \times B$.

2.2.4 Relação Inversa

Definição 2.8. *Seja* R *uma relação de* A *em* B*, então* R^{-1} *definida por*

$$R^{-1} = \{(y, x) \in B \times A : x \ R \ y\}$$

é uma relação de B *para* A*, chamada relação inversa de* R*.*

Exemplo 2.2. *Sejam* $A = \{1, 2, 3\}$ *e* $B = \{2, 3, 4, 5\}$*. E seja* $y = x + 2$ *a lei que defini uma relação* R *de* A *para* B*, tem-se:*

$$R = \{(1, 3), (2, 4), (3, 5)\}$$

e

$$R^{-1} = \{(3, 1), (4, 2), (5, 3)\}.$$

2.2.5 Relação Composta

Definição 2.9. *Sejam R uma relação de A em B e S uma relação de B em C. Então a relação composta de A em C, em símbolos $S \circ R$, é dada por*

$$S \circ R = \{(x, z) \in A \times C : \exists\ y \in B \text{ tal que } xRy \text{ e } ySz\}.$$

Exemplo 2.3. *Seja $A = \{0, 1, 2, 3\}$. Se $R = \{(1, 1), (1, 2), (2, 2), (2, 3)\}$ e $S = \{(1, 0), (2, 1), (3, 2)\}$ são duas relações em A, então*

$$S \circ R = \{(1, 0), (1, 1), (2, 1), (2, 2)\} \text{ e } R \circ S = \{(2, 1), (2, 2), (3, 2), (3, 3)\}.$$

Teorema 2.3. *Sejam R uma relação de A em B, S uma relação de B em C e T uma relação de C em D. Então as seguintes condições são satisfeitas:*

1. $(R^{-1})^{-1} = R$.
2. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.
3. $(T \circ S) \circ R = T \circ (S \circ R)$.

Demonstração. Será provado apenas o item (1).

$$(x, y) \in (R^{-1})^{-1} \Leftrightarrow (y, x) \in R^{-1} \Leftrightarrow (x, y) \in R.$$

□

2.2.6 Domínio, Imagem e Contradomínio de uma relação

Seja R uma relação de A para B. Então o domínio de R, em símbolos $DomR$, é o conjunto

$$DomR = \{x \in A : \exists\ y \in B \text{ tal que } xRy\}$$

e a imagem de R, em símbolos ImR, é o conjunto

$$ImR = \{x \in B : \exists\ y \in A \text{ tal que } xRy\}.$$

Exemplo 2.4. *Sejam* $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$ *e* $R = \{(1, 3), (2, 4), (3, 5)\}$, *tem-se:*

$$DomR = \{1, 2, 3\} \text{ e } ImR = \{3, 4, 5\}.$$

Veja que o domínio da relação ($DomR$) está contido ou é igual ao conjunto A e a imagem (ImR), está contida ou é igual ao conjunto B.

O conjunto B é chamado contradomínio da relação R.

Teorema 2.4. *Sejam* R *uma relação de* A *em* B *e* S *uma relação de* B *em* C. *Então:*

1. $DomR = ImR^{-1}$.
2. $ImR = DomR^{-1}$.
3. $Dom(S \circ R) \subseteq DomR$.
4. $Im(S \circ R) \subseteq ImS$.

Demonstração. Serão provados apenas os itens (1) e (3).

$$\begin{array}{rcc} x \in DomR & \Leftrightarrow & \exists\ y \in B \text{ tal que } (x, y) \in R \\ & \Leftrightarrow & \exists\ y \in B \text{ tal que } (y, x) \in R^{-1} \\ & \Leftrightarrow & x \in ImR^{-1}. \end{array}$$

e

$$\begin{array}{rcc} x \in Dom(S \circ R) & \Rightarrow & \exists\ z \in C \text{ tal que } (x, z) \in S \circ R \\ & \Rightarrow & \exists\ y \in B \text{ tal que } (x, y) \in R \text{ e } (y, z) \in S \\ & \Rightarrow & x \in DomR. \end{array}$$

□

2.3 Funções

Dados dois conjuntos A e B, uma função é uma regra ou um conjunto de instruções que indica como associar a cada elemento $x \in A$ um único elemento $y \in B$.

Simbolicamente representa-se a função como

$$f : A \to B.$$

Se f é uma função de A em B, então o gráfico de f é o conjunto de todos os pares ordenados (x, y) tais que $y = f(x)$, isto é,

$$graf(f) = \{(x, y) \in A \times B : y = f(x)\}.$$

Definição 2.10. *Uma função ou aplicação de A em B é uma relação f de A em B tal que se $(x, y_1) \in f$ e $(x, y_2) \in f$, então $y_1 = y_2$.*

Escreve-se $f : A \to B$ para indicar que f é uma função com domínio A e contra-domínio B. Se $(x, y) \in f$ dizemos que y é o valor ou a imagem de x com respeito a f , em símbolos $y = f(x)$, também dizemos que x é a pré-imagem de y com respeito a f . Assim, a definição acima é equivalente a: para cada elemento $x \in A$ corresponde a uma única imagem $y \in B$. Note que, se $y_1 = f(x_1)$, $y_2 = f(x_2)$ e $x_1 = x_2$, então $y_1 = y_2$; dize-se que a função f está bem definida, isto é, se $x_1 = x_2$, então $f(x_1) = f(x_2)$.

Seja $f : A \to B$ uma função. Então $Imf \subseteq B$. Se $Imf = B$ dizemos que f aplica A sobre B ou que f é sobrejetora, isto é, dado qualquer $y \in B$ existe pelo menos um $x \in A$ tal que $y = f(x)$.

Uma função $f : A \to B$ é chamada injetora se f satisfaz a seguinte condição:

$$(x_1, y) \in f \text{ e } (x_2, y) \in f \Rightarrow x_1 = x_2, \forall x_1, x_2 \in A$$

ou, equivalentemente,

$$f(x_1) = f(x_2) \Rightarrow x_1 = x_2, \forall x_1, x_2 \in A.$$

Uma função$f : A \to B$ é chamada bijetora se f é sobrejetora e injetora.

Note que, se $f : A \to B$ é bijetora, então todo elemento de A tem exatamente uma imagem em B e todo elemento de B tem exatamente uma pré-imagem em A. Assim, todos os elementos de A e todos os elementos de B são associados aos pares. Por essa razão, se $f : A \to B$ é bijetora, dizemos, às vezes, que f é uma correspondência biunívoca entre A e B. Em particular, se $f : A \to A$ é bijetora, dizemos que f é uma permutação de A.

Seja A um conjunto não-vazio. A função $I_A : A \to A$ dada por

$$I_A(x) = x, \forall x \in A$$

é chamada a *função identidade*. Note que I_A é sempre bijetora.

Sejam A, B dois conjuntos e $b \in B$. A função $k : A \to B$ dada por

$$k(x) = b, \forall x \in A$$

é chamada a *função constante*. Note que, se A tem pelo menos dois elementos, então k não é injetora e se B tem pelo menos dois elementos, então k não é sobrejetora.

Sejam A um conjunto e $X \subseteq A$. A função $i : X \to A$ dada por

$$i(x) = x, \forall x \in X$$

é chamada a *função inclusão*. Note que, i é sempre injetora, portanto, se $X \neq A$, então i não é sobrejetora.

Sejam $f : A \to B$ uma função e $X \subseteq A$. Então f induz uma função $f_X : X \to B$ dada por

$$f_X(x) = f(x), \forall x \in X,$$

a qual é chamada a *restrição* de f para X, em símbolos $f_X = f \mid X$. Por outro lado, se $A \subseteq C$, então a função $F : C \to B$ dada por

$$F(x) = f(x), \forall x \in A$$

é chamada a *extensão* de f para C. Note que, $f = F \mid A$.

Sejam $f : A \to A$ uma função e $X \subseteq A$. Dizemos que X é invariante sob f se $f(x) \in X$, para cada $x \in X$, isto é, $f(X) \subseteq X$. Assim, se X é invariante sob f, então a f_X é uma função de X em X. O conjunto

$$A_f = \{x \in A : f(x) = x\}$$

é o conjunto de pontos fixos de f e é claramente invariante sob f.

Teorema 2.5. *Sejam $f : A \to B$ e $g : B \to C$ duas funções. Então $g \circ f : A \to C$ é uma função.*

A função $g \circ f$ é chamada a composição de f com g. Assim, para obter o valor da composição de f com g em x primeiro encontramos o valor de f em x para depois encontrarmos o valor de g em $f(x)$.

Uma função $f : A \to B$ é chamada inversível se $f^{-1} : B \to A$ for uma função. Seja $f : A \to B$ uma função inversível. Então

$$y = f(x) \Leftrightarrow (x, y) \in f \Leftrightarrow (y, x) \in f^{-1} \Leftrightarrow x = f^{-1}(y).$$

Teorema 2.6. *Se $f : A \to B$ é uma função bijetora, então $f^{-1} : B \to A$ é uma função bijetora.*

Demonstração. Pelo Teorema 2.4, tem-se que

$$Imf^{-1} = Domf = A \; e \; Domf{-}1 = Imf = B.$$

Agora, será mostrado que f^{-1} é uma função.

$$(y, x_1) \in f^{-1} \; e \; (y, x_2) \in f^{-1} \Rightarrow (x_1, y) \in f \; e \; (x_2, y) \in f \Rightarrow x_1 = x_2,$$

pois f é injetora. Como Im $f^{-1} = A$ tem-se que f^{-1} é sobrejetora. Finalmente, dados $y_1, y_2 \in B$,

$$\begin{aligned} x = f^{-1}(y_1) = f^{-1}(y_2) \quad &\Rightarrow \quad (y_1, x) \in f^{-1} \; e \; (y_2, x) \in f^{-1} \\ &\Rightarrow \qquad (x, y_1) \in f \; e \; (x, y_2) \in f \\ &\Rightarrow \qquad\qquad y_1 = y_2, \end{aligned}$$

pois f é uma função. Logo, f^{-1} é injetora. □

Teorema 2.7. *Se $f : A \to B$ é uma função inversível, então $f : A \to B$ é uma função bijetora.*

Demonstração. Como, por hipótese $f : A \to B$ é uma função inversível, tem-se que $f^{-1} : B \to A$ é uma função. Assim, pelo Teorema 2.4, tem-se que $Imf = Domf^{-1} = B$. Como $Imf = B$ tem-se que f é sobrejetora. Finalmente, dados $x_1,\ x_2 \in A$,

$$\begin{aligned} y = f(x_1) = f(x_2) \quad &\Rightarrow \quad (x_1, y) \in f \text{ e } (x_2, y) \in f \\ &\Rightarrow \quad (y, x_1) \in f^{-1} \text{ e } (y, x_2) \in f^{-1} \\ &\Rightarrow \quad x_1 = x_2, \end{aligned}$$

pois f^{-1} é uma função. Logo, f é injetora. □

Teorema 2.8. *Seja $f : A \to B$ uma função inversível. Então:*

1. $f^{-1} \circ f = I_A$
2. $f \circ f^{-1} = I_B$.

Demonstração. Será provado apenas o item (1). Dado $x \in A = Domf$. Então existe $y \in B$ tal que $y = f(x)$. Como f é inversível temos que $x = f^{-1}(y)$. Logo,

$$(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = I_A(x), \ \forall x \in A,$$

isto é, $f^{-1} \circ f = I_A$. □

Teorema 2.9. *Sejam $f : A \to B$ e $g : B \to A$ duas funções. Se $g \circ f = I_A$ e $f \circ g = I_B$, então $f : A \to B$ é bijetora e $g = f^{-1}$.*

Sejam $f : A \to B$ uma função e $X \subseteq A$. A imagem direta de X sob f , em símbolos $f(X)$, é o seguinte subconjunto de B:

$$f(X) = y \in B : \exists\ x \in X \text{ tal que } y = f(x) = f(x) : x \in X \subseteq Imf.$$

Sejam $f : A \to B$ uma função e $Y \subseteq B$. A pré-imagem ou imagem inversa de Y sob f , em símbolos $f^{-1}(Y)$, é o seguinte subconjunto de A:

$$f^{-1}(Y) = x \in A : f(x) \in Y.$$

Teorema 2.10. *Seja $f : A \to B$ uma função. Então:*

1. $f(f^{-1}(Y)) \subseteq Y$, *para todo* $Y \subseteq B$.
2. $X \subseteq f^{-1}(f(X))$, *para todo* $X \subseteq A$.
3. $f(f^{-1}(Y)) = Y$, *para todo* $Y \subseteq B \Leftrightarrow f$ *é sobrejetora.*

4. $X = f^{-1}(f(X))$*, para todo* $X \subseteq A \Leftrightarrow f$ *é injetora.*

Demonstração. Será provado apenas o item (3). Supondo que $f(f^{-1}(Y)) = Y$, para todo $Y \subseteq B$. Dado $y \in B = f(f^{-1}(B))$, temos que $y = f(x)$, para algum $x \in f^{-1}(B) \subseteq A$; logo, $y = f(x)$, para algum $x \in A$, isto é, f é sobrejetora.
Reciprocamente, pelo item (1), $f(f^{-1}(Y)) \subseteq Y$, para todo $Y \subseteq B$. Por outro lado, se $y \in Y \subseteq B$, então existe, por hipótese, $x \in A$ tal que $y = f(x)$ e, portanto, para algum $x \in f^{-1}(Y)$, pois $f(x) \in Y$; assim,

$$y = f(x) \in f(f^{-1}(Y)).$$

Logo, $Y \subseteq f(f^{-1}(Y))$. □

O produto cartesiano de dois subconjuntos A e B de U foi definido como o conjunto $A \times B = (x, y) : x \in A, y \in B$.

Definição 2.11. *Sejam* $\{A_i\}i \in I$ *uma família indexada de subconjuntos de* U *e* $A = \bigcup_{i \in I} A_i$*. O produto cartesiano dos subconjuntos* A_i *é*

$$\prod_{i \in I} A_i = \{f : I \to A : f \text{ e uma funcao e } f(i) \in A_i, \forall i \in I\}.$$

2.3.1 Função Afim

Definição 2.12. *Uma função* $f : R \to R$ *chama-se função afim quando existem dois números reais* a *e* b *, com* $a \neq 0$*, tal que*

$$f(x) = ax + b$$

para todo x *real, onde a constante* a *é chamada de coefciente de* x*, e a constante* b *é chamada de termo independente da função.*

Casos particulares importantes de função afim:

1. *Função identidade*

   $f : R \to R$ definida por $f(x) = x$ para todo $x \in R$. Nesse caso, $a = 1$ e $b = 0$.

2. *Função linear*

   $f : R \to R$ definida por $f(x) = ax$ para todo $x \in R$. Nesse caso, $b = 0$.

3. *Função contante*

   $f : R \to R$ definida por $f(x) = b$ para todo $x \in R$. Nesse caso, $a = 0$.

3. *Função translação*

   $f : R \to R$ definida por $f(x) = x + b$ para todo $x \in R$ e $b \neq 0$. Nesse caso, $a = 1$.

O valor da função afim $f(x) = ax + b$ para $x = x_0$ é dado por $f(x_0) = ax_0 + b$.

Uma função afim $f(x) = ax + b$ fica inteiramente determinada quando conhecemos dois dos seus valores $f(x_1)$ e $f(x_2)$ para quaisquer x_1, $x_2 \in R$, com $x_1 \neq x_2$. De modo geral, conhecendo $y_1 = f(x_1)$ e $y_2 = f(x_2)$ para x_1, $x_2 \in R$, com $x_1 \neq x_2$, pode-se explicar os valores a e b da função $f(x) = ax + b$, determinando-a assim:

$$y_1 = f(x_1) = ax_1 + b \quad (1)$$

$$y_2 = f(x_2) = ax_2 + b \quad (2)$$

Fazendo $(2) - (1)$, tem-se

$$y_2 - y_1 = (ax_2 + b) - (ax_1 + b) = ax_2 - ax_1 = a(x_2 - x_1) \Rightarrow a = \frac{y_2 - y_1}{x_2 - x_1}, x_1 \neq x_2.$$

Substituindo a em (1), obtém-se o valor de b, assim:

$$y_1 = (\frac{y_2 - y_1}{x_2 - x_1})x_1 + b \Rightarrow y_1(x_2 - x_1) = y_2x_1 - y_1x_1 + b(x_2 - x_1) \Rightarrow$$

$$\Rightarrow y_1x_2 - y_1x_1 - y_2x_1 + y_1x_1 = b(x_2 - x_1) \Rightarrow b = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, x_1 \neq x_2.$$

3 TEORIA DOS NÚMEROS E ARITMÉTICA MODULAR

A teoria dos números se dedica ao estudo das propriedades dos números inteiros $\mathbb{Z}$. Neste capítulo, serão apresentadas algumas definições e resultados sobre a teoria dos números necessários para estudos posteriores. O referencial teórico utilizado na formulação deste capítulo é explorado nas obras de: Almeida, Coutinho, Galvão e Schlittler, onde encontram-se demonstrados os teoremas apresentados.

3.1 Números

Quando olhamos a nossa volta, percebemos o quanto é difícil encontrar uma situação que, de uma forma ou de outra, não esteja direta ou indiretamente relacionada aos números. Eles são usados para ordenar coisas ou pessoas, para medir algo, para codifirca ou ainda para quando fazemos a mais primitiva função dos números: contar. O processo de contagem não é algo instintivo ou inato. Tal método teve início quando o homem desenvolveu a capacidade de comparar conjuntos de objetos e estabelecer entre eles uma correspondência um a um.

Contamos e registramos os números através de símbolos a partir de regras preestabelecidas. Mas nem sempre eles foram escritos da forma como os conhecemos hoje. Segundo a história, quando o homem primitivo deixou de ser nômade e passou a desenvolver atividades como a agricultura e a pecuária, a partir de então, a necessidade de registrar quantidades, para, por exemplo, marcar os dias passados após um certo evento, como os períodos de chuva ou controlar a quantidade de animais de um rebanho.

Acredita-se que, inicialmente, tais registros foram feitos associando-se os dedos das mãos e/ou dos pés, pedras, gravetos, conchas e grãos.

O homem primitivo tinha uma percepção de quantidade basicamente intuitiva, isto é, comparável à percepção dos animais. Contavam grupos pequenos de até duas unidades. Grupos com três ou mais unidades eram contadas assim: um, dois e muitos.

Com a evolução do homem, surgiu a necessidade de guardar esses registros, foi então que essa noção intuitiva de quantidade deu lugar à numerção escrita, uma vez que essa era uma forma mais prática e confiável, diante da dificuldade em registrar números muito grandes, guardar e carregar um amontoado de pedras. A numeração escrita era

feita com marcas em qualquer objeto que possibilitasse o traçado, como madeiras e osssos por exemplo.

O osso de Ishango, mostrado na Figura 3.1, é um dos mais antigos objetos com indícios de registro de caráter numérico. É um osso petrificado, medindo cerca de 10 cm de comprimento, que foi encontrado na África e tem cerca de 30.000 anos. Possui três colunas de traços entalhados, que correspondem às suas três faces. As marcas sugerem uma tentativa de contagem.

Figura 3.1: Faces frontal e posterior do osso de Ishango

Fonte: Rogério S. Mol (2013)

3.1.1 Sistemas de Numeração

Um **sistema de numeração** é um conjunto de símbolos e regras de escrita numérica. Muitas civilizações da Antiguidade, como os povos babilônios, egípcios, gregos, chineses e hindus, criaram seus próprios sistemas de numeração. As sociedades da Europa, Oriente e Oriente Médio não trocavam apenas mercadorias, como tamém conhecimento.

> O intercâmbio cultural, que também envolveu os conhecimentos matemáticos daqueles povos, refletiu-se nas formas de contar e de escrever os números. Assim a matemática, enquanto atividade humana há já algumas centenas de anos, (Davis, 1995), deve ser olhada fundamentalmente como um produto da sociedade (ALMEIDA, 2007, p.1).

Os mais antigos registros escritos, que trazem informações sobre a evolução dos sistemas de numeração, são originários da Mesopotâmia e do Egito e datam de, aproximadamente, 3500 a.C. A Figura 3.2 mostra a representação do númeral 7 escrito por diferentes povos.

Figura 3.2: Numeral 7 em diferentes escritas numéricas

Fonte: Bezerra (2016)

3.1.2 Sistema de Numeração Babilônico

A representação escrita dos povos da Mesopotâmia, frequentemente chamados de Babilônios, é a escrita cuneiforme, pois seus caracteres eram grafados em forma de cunha, produzidos, através da impressão, em tabletes de argila, com um tipo de estilete. Nesses tabletes, foram registrados quantidades e totais, tabelas e cálculos de áreas, tendo em si uma matemática bastante desenvolvida e data de, aproximadamente, 2000 a.C (Galvão, 2014).

No sistema de numeração babilônico, a unidade era indicada por uma cunha vertical, e a dezena por uma cunha horizontal, mostrado na Figura 3.3. A posição e o tamanho das cunhas ou de seus grupos indicavam a ordem de grandeza.

Figura 3.3: Representação na Escrita Cuneiforme

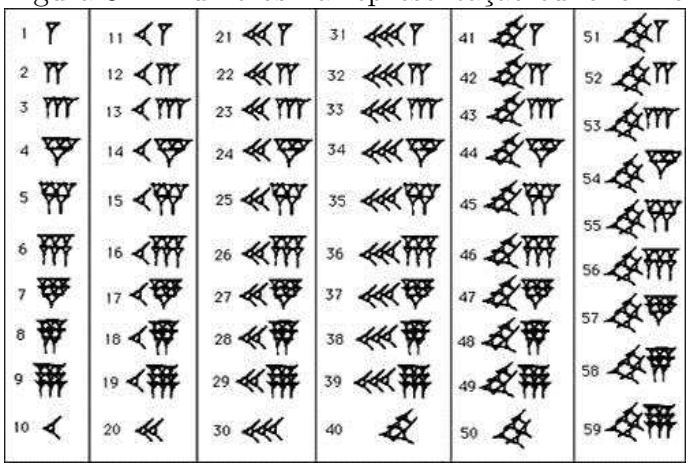
Fonte: Próprio autor (2018)

Por volta de 200 a 300 a.C., surgiu uma representação para o zero, na escrita cuneiforme, simbolizado por uma cunha inclinada, passando assim a facilitar a interpretação numérica dos sistemas que utilizavam essa escrita, dado que originalmente, não havia símbolo para o zero, usava-se apenas um espaço em branco o que tornava a interpretação um pouco difícil.

Com o surgimento do algarismo zero o sistema de numeração babilônico passa a ter 60 algarismos distintos e por isso também é chamado de sistema de numeração sexagesimal, quer dizer que, utiliza a base 60 para a formação de seus numerais.

Ainda hoje, o sistema de numeração babilônico ou sexagesimal é utilizado. A divisão de uma hora em 60 minutos e de um minuto em 60 segundos é uma herança dos babilônicos. A figura 3.4 mostra a representação cuneiforme de alguns desses números.

Figura 3.4: Números na representação cuneiforme



Fonte: Miranda (c2018)

3.1.3 Sistema de Numeração Egípcio

O Egito, localizado no nordeste de África no vale do Nilo, foi uma das primeiras e grandes civilizações da antiguidade. Seu povo, os egípcios, criou um elaborado sistema de numeração que tinha como principais características ser aditivo, não posicional, não existir um símbolo para o zero e utilizar a base 10. A representação escrita dos números, no sistema de numeração egípcio, era hieroglífica, ou melhor, cada símbolo era a imagem de um objeto ou de um ser.

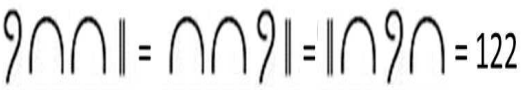
O sistema de numeração egípcio ser aditivo, quer dizer, que os valores dos símbolos são somados uns aos outros para representar as quantidades, como mostrado na Figura 3.5.

Figura 3.5: Princípio aditivo

Fonte: Próprio Autor (2018)

Ser não posicional significa que o valor de cada símbolo não depende de sua posição na representação numérica, como mostra a Figura 3.6.

Figura 3.6: Não Posicional



Fonte: Próprio Autor (2018)

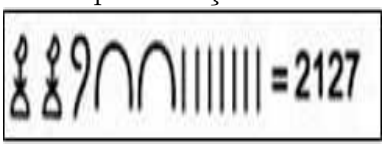
Nesse sistema de numeração, a cada grupo de 10 símbolos iguai,s tem-se um outro símbolo. Assim, a base do sistema de numeração egípcia é 10, como se observa na Figura 3.7. Na Figura 3.8, tem-se um exemplo da representação do número 2.127 pelo sitema de numeração egípcio.

Figura 3.7: Símbolos do Sistema de Numeração Egípcio

Símbolo egípcio	descrição	nosso número
	bastão	1
	calcanhar	10
	rolo de corda	100
	flor de lótus	1000
	dedo apontando	10000
	peixe	100000
	homem	1000000

Fonte: Miranda (c2018)

Figura 3.8: Representação numérica egípcia



Fonte: Almeida (2007, p. 84)

3.1.4 Sistema de Numeração Indo-Arábico

O sistema de numeração utilizado atualmente, em grande parte das culturas contemporâneas, é o denominado sistema indo-arábico. Criado por matemáticos e astrônomos, pertencentes à civilização hindu, esse sistema se desenvolveu no vale do rio Indo, região que hoje pertence ao Paquistão.

O sistema de numeração indo-arábico é também conhecido como sistema de numeração decimal, por se tratar de um sistema de base dez, ou seja, os agrupamentos são feitos de dez em dez unidades. Acredita-se que esse agrupamento teve origem, provavelmente, pelo fato de o homem ter dez dedos e usar as mãos para contar.

A nomenclatura indo-arábico para este sistema de numeração deve-se ao fato de seus símbolos e suas regras terem sido inventadas pelo antigo povo indiano e divulgados pelos árabes.

Os símbolos do sistema indo-arábico nem sempre tiveram a forma que se conhece hoje, como foi um sistema criado na Índia, adotado pelos árabes e passado aos europeus, é natural que sua escrita sofresse alterações ao longo dos séculos, a Figura 3.9 mostra a evolução da escrita deste sistema de numeração.

Figura 3.9: Evolução da escrita no sistema de numeração indo-arábico

Fonte: Schlittler (2008)

3.2 Algoritmo da Divisão Euclidiana

Sabe-se que no processo de dividir um inteiro positivo a por um inteiro positivo b, obtém-se um quociente q e um resto r. Formalmente escreve-se:

Teorema 3.1. *Sejam $a, b \in \mathbb{Z}$ com $b > 0$. Então, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = qb + r \text{ onde } 0 \leq r < b$$

Demonstração. **Prova da Existência.** Suponha que $a \geq 0$, pois se $a \leq 0$ basta substituir a por $-a \geq 0$. Quando $a = 0$, tem-se $q = r = 0$; quando $a = b$, tem-se $q = 1$ e $r = 0$; quando $a \leq b$, tem-se $q = 0$ e $r = a$. Assim, deve-se supor $a > b$ e $a \geq 1$. Seja

$$X = \{a \in \mathbb{N} \mid a = b + r, \text{ onde } 0 \leq r < b\}.$$

Então,

- (i) $1 \in X$, pois $1 = 1 \cdot 1 + 0$;
- (ii) Suponha por hipótese de indução que o resultado é válido para todo k, $1 \leq k \leq a - 1$, isto é, $\{1, 2, ..., a - 1\} \subseteq X$. Como $a > b > 0$, tem-se que $0 < a - b < a$. Pela hipótese de indução, existem $q_1, r \in \mathbb{Z}$, tais que

  $$a - b = q_1 b + r, \text{ onde } 0 \leq r < b.$$

  Fazendo, $q = q_1 + r$, obtém-se que

  $$a = qb + r, \text{ onde } 0 \leq r < b.$$

Prova da Unicidade. Suponha que existe $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que

$$a = q_1 b + r_1, \text{ onde } 0 \leq r_1 < b$$

e

$$a = q_2 b + r_2, \text{ onde } 0 \leq r_2 < b.$$

Assim,

$$q_1 b + r_1 = q_2 b + r_2 \Longleftrightarrow (q_1 - q_2)b = r_2 - r_1.$$

Além disso,

$$0 \leq r_2 < b \; e \; -b < -r_1 \leq 0 \Longrightarrow 0 \leq \mid r_2 - r_1 \mid < b.$$

Logo,

$$\mid q_1 - q_2 \mid b = \mid r_2 - r_1 \mid < b \Longrightarrow 0 \leq \mid q_1 - q_2 \mid < 1.$$

Portanto, tem-se que $\mid q_1 - q_2 \mid = 0$, isto é, $q_1 = q_2$ e assim, $r_1 = r_2$. □

Exemplo 3.1. *Sejam* $a = -52$ *e* $b = 7$*. Determinar a divisão de a por b. Solução*

$$-52 = (-8) \cdot 7 + 4.$$

Assim, $q = -8$ *e* $r = 4$*.*

Corolário 3.1. *Sejam* $a, b \in \mathbb{Z}$ *com* $b \neq 0$*. Então, existem únicos* $q, r \in \mathbb{Z}$ *tais que*

$$a = qb + r, \text{ onde } 0 \leq r < b.$$

Exemplo 3.2. *Sejam* $a = 85$ *e* $b = -11$*. Determinar a divisão de a por b. Solução*

$$85 = (-7) \cdot 11 + 2 = -224 \cdot (-11) + 8.$$

Assim, $q = -7$ *e* $r = 8$*.*

Definição 3.1. *Sejam* $a, b \in \mathbb{Z}$ *com* $b \neq 0$*. Diz-se que b divide a ou b é divisor de a ou que a é um múltiplo de a, em símbolos* $b|a$*, se existe* $c \in \mathbb{Z}$ *tal que* $a = bc$*. Caso contrário, diz-se que b não divide a, e denota-se* $b \nmid a$*. Além disso,* $a \in \mathbb{Z}$ *é um número par se* $2|a$ *e ímpar se* $2 \nmid a$*.*

Observação 3.1. *O inteiro c tal que* $a = bc$ *é único, pois se* $c' \in \mathbb{Z}$ *satisfaz* $a = bc'$*, então*

$$a - a = bc - bc' = b(c - c') \Longrightarrow c - c' = 0 \Longrightarrow c = c'.$$

Teorema 3.2. *Sejam* $a, b, c \in \mathbb{Z}^*$*. Então as seguintes condições são satisfeitas:*

1. $\pm 1|a, \pm a|a$;
2. $\pm b|1 \Leftrightarrow b = \pm 1$;
3. $b|a \text{ e } a > 0 \Rightarrow \pm b \leq a$;
4. $b|a \Leftrightarrow bc|ac$;
5. $b|a \text{ e } a|c \Rightarrow b|c$;
6. $b|a \text{ e } a|b \Rightarrow a = \pm b$;
7. $c|a \text{ e } c|b \Rightarrow c|(ax + by), \forall x, \ y \in \mathbb{Z}$.

Demonstração. Somente os ítens 2 e 6 serão demonstrados.

- 2. $b|1 \Leftrightarrow \exists\ d \in \mathbb{Z}$ tal que $bd = 1 \Leftrightarrow |bd| = |b||d| = 1$. Como $b, d \in \mathbb{Z}^*$, tem-se que $|b| \geq 1$ e $|d| \geq 1$. Assim, se $|b| > 1$, então

$$|bd| = |b||d| > |d| \geq 1,$$

  o que é uma contradição. Logo, $|b| = 1$. Portanto, $a = \pm b$.

- 6. Se $a|b$ e $b|a$, então existem $d, e \in \mathbb{Z}$, tais que $a = bd$ e $b = ae$. Assim,

$$b = ae = bde \Longrightarrow de = \pm 1.$$

  indent Logo, $d = e = \pm 1$. Portanto, $a = \pm b$.

□

Teorema 3.3. *Seja $b \in \mathbb{Z}$ com $b > 1$. Então para todo $a \in \mathbb{N}$ existem únicos $n, r_i \in \mathbb{Z}$ tais que*

$$a = r_n b^n + r_{n-1} b^{n-1} + ... + r_1 b^1 + r_0 b^0 = (r_n r_{n-1} ... r_1 r_0)_b,$$

onde $r_i \in \{0, 1, ..., b-1\}, \forall i = 0, 1, ..., n$ e $n = \lfloor \log_b a \rfloor$.

A prova do Teorema fornece um algoritmo prático para representar um inteiro a em uma base $b > 1$, através das seguintes relações:

$$\begin{array}{rcll} a & = & q_0 b + r_0, & 0 \leq r_0 < b \\ q_0 & = & q_1 b + r_1, & 0 \leq r_1 < b \\ \vdots & & \vdots & \vdots \\ q_{n-2} & = & q_{n-1} b + r_{n-1}, & 0 \leq r_n - 1 < b \text{ e } q_n - 1 < b. \end{array}$$

Considerando,$r_n = q_n - 1$, obtém-se

$$a = r_n b^n + r_n - 1 b^n - 1 + ... + r_1 b^1 + r_0.$$

Exemplo 3.3. *Considere $(142)_{10}, (153)_{10}$. Note que:*

$$142 = 35 \cdot 4 + 2$$

$$35 = 8 \cdot 4 + 3$$

$$8 = 2 \cdot 4 + 0$$

$$2 = 0 \cdot 4 + 2.$$

Assim,

$$(142)_{10} = 2 \cdot 4^3 + 0 \cdot 4^2 + 3 \cdot 4 + 2 = (2032)_4.$$

Analogamente,

$$(153)_{10} = 2 \cdot 4^3 + 1 \cdot 4^2 + 2 \cdot 4 + 1 = (2121)_4.$$

3.3 Máximo Divisor Comum

Nesta seção são mostrados os conceitos de máximo divisor comum e de mínimo múltiplo comum de qualquer dois inteiros não nulos, os quais podem ser estendidos para um número finito de inteiros não nulos.

Definição 3.2. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. O máximo divisor comum de a e b, em símbolo $mdc(a, b)$, é um inteiro positivo d tal que*

1. *$d|a$ e $d|b$;*

2. *Se $c|a$ e $c|b$, então $c|d$.*

Note que a condição 1 afirma que d é um divisor comum de a e b, e 2 assegura que d é o maior divisor comum de a e b. Além disso, se $a, b \in \mathbb{Z}$ e $mdc(a, b)$ existe, então o $mdc(a, b)$ é único.

Teorema 3.4. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Então $d = mdc(a, b)$ existe. Além disso, existem $x, y \in \mathbb{Z}$ tais que*

$$d = ax + by.$$

Demonstração.

$$X = \{ar + bs \mid r, s \in \mathbb{Z} \text{ e } ar + bs > 0\}.$$

Então $X \neq \emptyset$, pois se $a \neq 0$, então $|a| = a1 + b \cdot 0$ ou $\mid a \mid = a(-1) + b \cdot 0$. Assim, $\mid a \mid \in X$ e $X \subseteq \mathbb{N}$. Logo, X contém um menor elemento $d > 0$, isto é, existem $x, y \in \mathbb{Z}$ tais que

$d = ax + by$. Para mostrar que $d = mdc(a, b)$, utiliza-se o Teorema 3.1, pelo qual existem $q \cdot r \in \mathbb{Z}$ tais que

$$a = qd + r, \ onde \ 0 \leq r < d.$$

Então

$$r = a - qd = a(1 - qx) + b(-qy) \Rightarrow r = 0,$$

pois se $r > 0$, então $r \in X$, o que é uma contradição na escolha de d. Assim, $a = qd$ ou $d \mid a$. Analogamente, mostra-se que $d \mid b$. Finalmente, se $c \mid a$ e $c \mid b$, então, pelo Teorema 3.2, $c \mid (ax + by)$, isto é, $c \mid d$. □

Sejam $a, b \in \mathbb{Z}^*$. Diz-se que a e b são relativamente primos ou primos entre si quando $mdc(a, b) = 1$.

Teorema 3.5. *Sejam $a, b \in \mathbb{Z}^*$. Então a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que*

$$ax + by = 1.$$

Demonstração. Suponha que existam $x, y \in \mathbb{Z}$ tais que $ax + by = 1$ e $d = mdc(a, b)$. Então, pelo Teorema 5.2, ítem 7 , $d|1$. Portanto, $d = 1$. A recíproca é imediata. □

Lema 3.1. *Sejam $a, b, c \in \mathbb{Z}^*$. Então $mdc(ac, bc) = |c| \ mdc(a, b)$.*

O fato de $c|ab$ não implica que $c|a$ ou $c|b$. Para verificar, veja que

$$6|3 \cdot 4 \ onde, \ 6 \not| 3 \text{ e } 6 \not| 4.$$

Afirmação: Sejam $a, b, c \in \mathbb{Z}^*$. Se $c|ab$ e $mdc(a, c) = 1$, então $c|b$.
Prova: Se $mdc(a, c) = 1$, então existem $x, y \in \mathbb{Z}$ tais que $ax + cy = 1$. Assim,

$$abx + bcy = b.$$

Como $c|ab \ ec|c$, tem-se que $c|(abx + bcy)$, isto é, $c|b$.

Lema 3.2. *Sejam $a, b, c \in \mathbb{Z}^*$. Se $a = qb+r$, onde $0 \leq r < b$, então $mdc(a, b) = mdc(b, r)$.*

Tabela 3.1: Algorítmo de Euclides

	q_1	q_2	q_3	$\cdots$	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-1}	r_n
r_1	r_2	r_3	$\cdots$	r_n	0	

O Teorema 3.5 mostra a existência do $mdc(a, b)$, mas não mostra como encontrar o valor. Para determinar o máximo divisor comum entre dois inteiros a e b, é utilizado o Algoritmo de Euclides.

Supondo que $a \geq b > 0$, pois $mdc(a, b) = mdc(|a|, |b|)$. Então existem $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = q_1 b + r_1, \ \textit{onde}\ 0 \leq r_1 < b.$$

Se $r_1 = 0$, então $b|a$ e $mdc(a, b) = b$. Se $r_1 \neq 0$, então existem $q_2, r_2 \in \mathbb{Z}$ tais que

$$b = q_2 r_1 + r_2, \ \textit{onde}\ 0 \leq r_2 < r_1.$$

Se $r_2 = 0$, então $r_1|b$ e $mdc(a, b) = mdc(b, r_1) = r_1$. Se $r_2 \notin 0$, então existem $q_3, r_3 \in \mathbb{Z}$ tais que

$$r_1 = q_3 r_2 + r_3, \ \textit{onde}\ 0 \leq r_3 < r_2$$

e assim por diante até que algum resto seja nulo, isto é, $rn + 1 = 0$. Obtendo assim as seguintes relações:

$$\begin{aligned}
a &= q_1 b + r_1, && \textit{onde} && 0 \leq r_1 < b \\
b &= q_2 r_1 + r_2, && \textit{onde} && 0 \leq r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, && \textit{onde} && 0 \leq r_3 < r_2 \\
&\vdots && \vdots && \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n, && \textit{onde} && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n. &&
\end{aligned}$$

Portanto, $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_{n-1}, r_n) = r_n$. Estas relações podem ser representadas pela Tabela 3.1.

Exemplo 3.4. *Determinar o máximo divisor comum entre 132 e 56.*

Solução

Considere o Algorítmo de Euclides,

	2	2	1	4
132	56	20	16	4
20	16	4	0	

Assim, mdc(132, 56) = 4.

Observação 3.2. *O Algoritmo de Euclides também é utilizado para representar o* $mdc(a, b)$ *na forma* $ax + by$. *Observe que da penúltima equação tem-se*

$$r_n = r_{n-2} + (-q_n)r_{n-2}.$$

Substituindo o resto r_{n-1} *da equação anterior, obtém-se*

$$r_n = (-q_n)r_{n-3} + (1 + q_n q_{n-1})r_{n-2}.$$

Com esse procedimento são eliminados sucessivamente os restos

$$r_{n-1}, r_{n-2}, \cdots, r_2, r_1$$

e r_n *é determinado em termos de* a *e* b, *isto é, encontra-se* $x, y \in \mathbb{Z}$ *tais que*

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

3.4 Números Primos

Um número $P \in \mathbb{Z}$ é denominado primo se as seguintes afirmações são satisfeitas:

1. p não inversível ($p \neq \pm 1$);
2. Se $p = ab$, onde $a, b \in \mathbb{Z}^*$, então $a = \pm 1$ ou $b = \pm 1$.

Um número $n \in \mathbb{Z}$ é denominado composto se as seguintes condições são satisfeitas:

1. n é não inversível ($p \neq \pm 1$);
2. Se $p = ab$, onde $a, b \in \mathbb{Z}^*$, então $a > \pm 1$ ou $b > \pm 1$.

Como $-p$ é primo se, e somente se, p é primo, as investigações serão restritas aos primos positivos. Por exemplo, $2, 3, 5, 7, 11, 13$ e 17 são os primeiros números primos, enquanto $4, 6, 8, 9, 10, 12, 14$ e 15 são os primeiros compostos.

Teorema 3.6. *Se $a \in \mathbb{Z}^*$, com $|a| > 1$, então existe um número primo p que divide a.*

Teorema 3.7. *Seja $a \in \mathbb{Z}^*$, com$|a| > 1$ um número composto. Então a contém um divisor primo p tal que $p \leq p|a|$.*

Exemplo 3.5. *Seja $a = 1998$. Então $\lfloor\sqrt{1998}\rfloor = 44$. Assim, para encontrar um divisor primo de a é preciso testar com os primos menores ou iguais a 44.*
Verificando, tem-se

$$1998 = 2 \cdot 33 \cdot 37$$

Teorema 3.8. *Seja $a \in \mathbb{Z}^*$, com $|a| > 1$ um número composto. Então a contém um divisor primo p tal que $p \leq p|a|$.*

Teorema 3.9. *(**Teorema Fundamental da Aritmética**) Dado um inteiro positivo $n > 1$ pode-se se escrever, de modo único, a menos da ordem dos fatores, na forma*

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k},$$

em que os p_i são primos distintos e positivos $p_1 \leq p_2 \leq ... \leq p_k$ e os e_i são inteiros $e_1, e_2, ..., e_k$.

Lema 3.3. *Se p é um número primo e $p|p_1 p_2 \cdots p_n$, onde $p_1 p_2 \cdots p_n$ são números primos, então $p = p_i$ para algum $i = 1, 2, \cdots, n$.*

A demonstração a seguir tem duas partes: a primeira mostra que existe fatoração em números primos, e a segunda mostra a unicidade da fatoração.

Demonstração. (1) **Existência:** Suponha a negação da tese, ou seja, que existe pelo menos um inteiro maior do que 1 que não possa ser representado por fatores primos. Seja A o conjunto de todos esses números. Como A é um subconjunto dos inteiros, pelo Princípio da Boa Ordenação existe um elemento mínimo. Seja x esse elemento. Como x é maior do que 2 (já que 2 é primo, e tem fatoração em fatores primos), tem-se que existem a e b, tais que $x = ab$, com $a < x$ e $b < x$, e $a \notin A$ e $b \notin A$, possuindo fatoração e, assim, $x = ab$, o que é uma contradição, pois $x \in A$. Logo, A não pode ter elemento mínimo, e, portanto, $A =$, o que demonstra a existncia.

(2) **Unicidade:** Para demonstrar a unicidade, utiliza-se o Lema 5.3. Sejam

$$x = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_n$$

duas fatorações de x. Observe que os $p_i's$ não são necessariamente distintos, assim como os $q_i's$. Da igualdade, e da definição de divisibilidade, verifica-se que $p_1 | q_1 q_2 \cdots q_s$ e portanto, pelo lema, existe k tal que,

$$p_1 | q_k \Longrightarrow p_1 = q_k,$$

pois ambos são primos. Por extensão, para qualquer $j < k$, existe um $i < n$ tal que $p_j | q_i \Longrightarrow p_j = q_i$. Por fim, basta provar que $n = k$, que é trivial, já que, se $n > k$, teria-se que

$$q_1 q_2 \cdots q_k \cdots q_n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_k,$$

o que é absurdo, já que $q > 1$. Ou seja, o conjunto de q_i deve ser idêntico ao de p_j, finalizando a demonstração da unicidade.

Por (1) e (2), está demonstrado o Teorema Fundamental da Aritmética. □

Teorema 3.10. *Se $a \in \mathbb{N}$ com $a > 2$, então entre a e $a!$ existe pelo menos um número primo.*

Demonstração. Seja $b = a! - 1$. Então $b > 1$ e existe um número p tal que $p|b$. Claramente, $p \leq b < a!$. Suponhamos que $p \leq a$. Então p é um dos fatores do produto $1 \cdot 2 \cdot 3a = a!$ e, assim, $p|a!$. Logo, $p|(a! - b)$, isto é, $p|1$, o que é impossível. Portanto, $a < p < a!$. □

Teorema 3.11. *Existem infinitos números primos.*

A demonstração apresentada em seguida por contradição é dada por Euclides.

Demonstração. Suponhamos, por absurdo, que exista um número finito de primos, digamos

$$p_1, p_2, ..., p_m.$$

Seja $a = p_1, p_2, \cdots, p_{m+1}$. Então $a > 2$, existe um número p tal que $p > a$. Portanto,

$$p \neq p_i, \forall i = 1, 2, \cdots, m,$$

o que é uma contradição. □

3.5 Congruência

Definição 3.3. *Sejam $a, b \in \mathbb{Z}$ e $n \in N$. Diz-se que a e b são congruentes módulo n se os restos de a e b quando dividido por n forem iguais. Se a e b são congruentes módulo n, escreve-se $a \equiv b \ mod \ n$.*

Exemplo 3.6. $24 \equiv 59 \ mod \ 7$. *Pois,* $24 = 3 \cdot 7 + 3$ *e* $59 = 8 \cdot 7 + 3$.

Exemplo 3.7. $17 \equiv -13 \ mod \ 6$. *Pois,* $17 = 2 \cdot 6 + 5$ *e* $-13 = -3 \cdot 6 + 5$.

Exemplo 3.8. *Note que* $94 \equiv 1 \ mod \ 5$. *Pois, se* $a \equiv 0 \ mod \ n$, *então* $a = n \cdot k$ *e*

$$94 - 1 = (92 - 1)(92 + 1) = 80 \cdot 82 = 5 \cdot 16 \cdot 82.$$

Teorema 3.12. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Então, $a \equiv b \ mod \ n$ se, e somente se, n divide $a - b$.*

Demonstração. ($\Rightarrow$) Se $a, b \in \mathbb{Z}$, então existem r, q_1 e q_2 tais que $a = n \cdot q_1 + r$ e $b = n \cdot q_2 + r$. Assim, $(a - b) = n(q_1 - q_2)$. Logo,

$$n|(a - b).$$

($\Leftarrow$) Supondo que $n|(a - b)$. Pela divisão Euclidiana, tem-se que

$$a = n \cdot q_1 + r_1 \ e \ b = n \cdot q_2 + r_2, \ com \ 0 \leq r_1 \leq ne0 \leq r_2 \leq n.$$

Assim,

$$(a - b) = n(q_1 - q_2) + (r_1 - r_2).$$

Como $n|n(q_1 - q_2)$, tem-se que $n|(r_1 - r_2)$. Logo, $r_1 = r_2$, pois $|r_1 - r_2| < n$. Portanto,

$$a \equiv b \ mod \ n.$$

□

Teorema 3.13. *Sejam $a, b, c, d, k, n \in \mathbb{Z}$ com $n > 1$ e $k \geq 1$. Então as condições seguintes são satisfeitas:*

1. $a \equiv a \ mod \ n$;

2. $a \equiv b \ mod \ n \Rightarrow b \equiv a \ mod \ n$;

3. $a \equiv b \ mod \ n \ e \ b \equiv c \ mod \ n \Rightarrow a \equiv c \ mod \ n$;

4. $a \equiv b \ mod \ n \ e \ c \equiv d \ mod \ n \Rightarrow (a + c) \equiv (b + d) \ mod \ n$;

5. $a \equiv b \ mod \ n \ e \ c \equiv d \ mod \ n \Rightarrow a \cdot c \equiv b \cdot d \ mod \ n$;

6. $a \equiv b \ mod \ n \Rightarrow ak \equiv bk \ mod \ n$.

3.6 Divisibilidade

Nesta subseção, são utilizados os conceitos e propriedades das congruências para definir os principais critérios de divisibilidade e mostrar um modelo para definir os demais critérios.

Definição 3.4. *Sejam a, b$\in \mathbb{Z}$, com $a \neq 0$. Diz-se que a divide b, denota-se $a|b$, se existir $c \in \mathbb{Z}$ tal que $b = ac$, onde o inteiro c é único.*

Propriedades fundamentais:

1. $a|a$, para todo $a \in \mathbb{Z}$.

2. Se $a|b$ e $b|c$, então $a|c$, para todo a, b $\in \mathbb{Z}$.

3. Se $a|b$ e $c|d$, então $ac|bd$.

4. Se $a|b$, então $a|mb$, para todo $m \in \mathbb{Z}$.

5. Se $a|b$ e $a|c$, então $a|(bx + cy)$, $\forall x, y \in \mathbb{Z}$.

6. Se $a|b$ e $b|a$, então $a = \pm b$.

Propriedade 3.1. ***Propriedade de Arquimedes***
Dados a, b $\in \mathbb{Z}$, com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, ou seja,

(i) se $b > 0$, tem-se $qb \leq a < (q + 1)b$,

(ii) e se $b < 0$, tem-se $qb \leq a < (q - 1)b$, onde $q \in \mathbb{Z}$.

3.7 Classes Residuais

Um inteiro $n > 1$ determina uma Classe Residual módulo n do elemento a em $\mathbb{Z}$ e a classe do $\overline{a}$ é o conjunto

$$\overline{a} = \{x \in Z | x \equiv a \ mod \ n\}.$$

Proposição 3.1. *Seja $n > 1$ um inteiro. Então*

1. *$\overline{a} = \overline{b}$ se, e somente se, $a \equiv b \ mod \ n$;*
2. *Se $\overline{a} \cap \overline{b} \neq \emptyset$, então $\overline{a} = \overline{b}$;*
3. $\bigcup_{a \in \mathbb{Z}} \overline{a} = \mathbb{Z}$.

Um inteiro qualquer b tal que $\overline{b} = \overline{a}$ é denominado representante da classe residual $\overline{a}$.

Proposição 3.2. *Para cada $a \in \mathbb{Z}$, existe um e somente um $r \in \mathbb{Z}$ com $0 \leq r < n$ tal que $\overline{a} = \overline{r}$.*

Corolário 3.2. *Existem exatamente n classes residuais módulo n distintas, a saber $\overline{0}, \overline{1}, ..., \overline{m-1}$.*

Um conjunto $\{a_1, a_2, ..., a_m\}$ é chamado de sistema completo de resíduo módulo n se para todo $a \in \mathbb{Z}$ existir um i com $i = 0, 1, ..., m$ tal que $a = a_i \ mod \ n$.

O conjunto de todas as classes residuais módulo n é representado por $\mathbb{Z}_n$, onde $\mathbb{Z}_n$ possui n elementos representados por $\overline{0}, \overline{1}, ..., \overline{m-1}$, na classe residual a congruência $a \equiv b \ mod \ n$ é substituída pela igualdade $\overline{a} = \overline{b}$.

As operações em $\mathbb{Z}_n$ são definidas por:

Adição: $\overline{a} + \overline{b} = \overline{a+b}$;

Multiplicação: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Propriedades Operatórias:

Para todos $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, tem-se

A_1 (Associativa) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

A_2 (Comutativa) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

A_3 (Elemento Neutro) $\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$ *para todo* $\overline{a} \in \mathbb{Z}_n$;

A_4 (Elemento Simétrico) $\overline{a} + (\overline{-a}) = (\overline{-a}) + \overline{a} = \overline{0}$ *para todo* $\overline{a} \in \mathbb{Z}_n$;

M_1 (Associativa) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;

M_2 (Comutativa) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;

M_3 (Unidade) $\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$;

AM (Distributiva) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Proposição 3.3. *Um elemento $\overline{a} \in \mathbb{Z}$ é inversível se, e somente se, $mdc(a, n) = 1$.*

Observação 3.3. *Todo $x \in \mathbb{Z}_p$, p primo, é inversível. Em símbolo*

$$\overline{x} \in \mathbb{Z}_p^* \Longrightarrow \exists\ \overline{y}\ tal\ que\ \overline{xy} = \overline{yx} = \overline{1}.$$

4 CRIPTOGRAFIA

O ser humano, de modo geral, sente a necessidade de buscar métodos cada vez mais modernos, que lhe permita transmitir ou guardar informações de forma segura e muitas vezes sigilosas. Essa necessidade impulsionou o homem a vencer os desafios que surgiram ao longo dos tempos, principalmente com o advento da tecnologia, para que pudesse garantir a segurança e o sigilo dessas informações. "Quando se pensou em compartilhar uma mensagem sem que ela fosse lida pela pessoa errada, estava lançado o desafio do desenvolvimento de uma forma de escrever a mensagem de forma oculta. Nasciam assim as raízes da criptografia" (DANTAS, 2016, p.11).

Em grego, cryptos significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de maneira que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos".

Chama-se encriptação ao processo de transformar um texto legível em um texto ilegível, processo também conhecido como cifragem. O processo usado para reverter a encriptação é chamado de decriptação, ou decifragem. Para cifrar e decifrar uma mensagem é necessário que se tenha, além do método, uma informação sigilosa, chamada chave criptográfica, que deve ser de conhecimento exclusivo das partes envolvidas na troca da mensagem.

Existem dois tipos de chaves criptográficas: a chave simétrica e a chave assimétrica. A chave simétrica é um tipo de chave mais simples, na qual o emissor e o receptor fazem uso da mesma chave, isto é, uma única chave é usada na codificação e na decodificação da informação.

A chave assimétrica, também conhecida como chave pública, é na verdade um conjunto de duas chaves: uma denominada privada e outra denominada pública. Nesse caso, o emissor da mensagem deve criar uma chave de codificação e enviá-la ao receptor, essa é a chave pública. Uma outra chave será criada para decodificar a mensagem que é chamada chave privada, essa deve ser secreta.

4.1 Criptografia no Tempo

Atualmente, a Criptografia tem papel fundamental no sigilo das informações transmitidas, principalmente, através da internet, tais como: uma mensagem enviada via

Whatsapp, e-mail, dados de compras online, senha bancária, a chave de segurança do smartphone, do computador, emfim são muitas as informações que queremos guardar ou impedir que pessoas não autorizadas tenham acesso.

> Hoje em dia a tecnologia da criptografia, após anos de aprimoramento, é amplamente utilizada na proteção de dados sigilosos, seja de cunho pessoal ou profissional, através da ciência da computação e de seus recursos, onde é possível transmitir uma grande quantidade de dados de maneira extremamente rápida e segura, tendo em vista o conforto e segurança pra pessoas que se utilizam de tais recursos (OLIVEIRA, 2011, p.2).

No entanto, não é de hoje que se faz uso desse recurso para tal objetivo. Existem registros antigos que comprovam o uso da criptografia desde a antiguidade. Os romanos, durante séculos, também fizeram uso de mensagens secretas que permitiram a comunicação segura entre seus exércitos, transmitindo seus planos e estratégias de guerra, e impedindo, dessa forma, que fossem descobertos por seus inimigos.

No século V, a.C., os espartanos, fizeram uso de um dos mais sofisticados métodos de cifrar mensagens da época, o Citale espartano, mostrado na Figura 4.1. A técnica consistia em escrever uma mensagem em uma tira de couro enrolada em um bastão de madeira na forma de um cilindro (citale). Em seguida a tira de couro era desenrolada e usada pelo mensageiro como um cinto com as letras no verso. A mensagem, a princípio, parecia uma série de letras sem nenhum sentido. Só faria sentido novamente se a tira de couro fosse enrolada pelo receptor em um citale idêntico àquele em que foi utilizado para cifrar. A técnica do citale consiste em uma cifra chamada cifra de transposição, ou seja, as letras do texto são misturadas como um anagrama.

Figura 4.1: Citale Espartano

Fonte: Medeiros (2013)

Outro tipo de cifra, considerada uma das mais simples formas de cifrar uma mensagem, é a chamada cifra de substituição monoalfabética, ela consiste em usar a troca de

uma letra da mensagem original por outra letra do alfabeto de acordo com um critério pré-estabelecido. A exemplo tem-se o Código de César ou Cifra de César, nome dado em homenagem ao imperador romano Júlio César, a quem atribuí-se a criação deste método de criptografar mensagens. O método consiste em substituir a letra da mensagem por outra letra do mesmo alfabeto que esteja três casas à frente da letra original. A quantidade de casas ou letras do alfabeto que se pula é a chave criptográfica.

No entanto, tais cifras que substituem uma letra por outra, como a de César, são muito fáceis de se "quebrar", quer dizer, desvendar o conteúdo da mensagem mesmo não sendo o destinatário legítimo.

> Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante (COUTINHO, 2016, p.2).

Dada a fragilidade demonstrada pelas cifras de substituição monoalfabéticas, o italiano Leon Alberti, por volta de 1940, sugeriu o uso de dois ou mais alfabetos, de modo que fossem usados alternadamente. Assim, tinha origem a cifra de substituição polialfabética. A partir desse princípio, o francês Blaise de Vigenère passou a cifrar mensagens usando 26 alfabetos distintos, criando então uma cifra que leva seu nome. Para decifrar a mensagem, é necessário que o destinatário saiba qual alfabeto usar para cada letra da mensagem, e ainda deve ter conhecimento da palavra-chave que foi usada para cifrar a mensagem e que será a mesma para decifrar. A vantagem da cifra de Vigenère, em relação às cifras de substituição monoalfabéticas, é que não pode ser feita a análise de frequências. Por isso, durante quase dois séculos, ficou conhecida como a "cifra indecifrável" (MACHADO, 2012, p.4).

No ano de 1929, Lester S. Hill introduziu um sistema de substituição polialfabética que ficou conhecido como a Cifra de Hill. A cifra de Hill é um cipto-sistema, que utiliza a transformação matricial para substituição de letras do texto original, aplicando alguns conceitos de álgebra e álgebra linear. Porém, rapidamente, um método de decifragem para essa cifra foi desenvolvido, tornando-a insegura.

Um dos grandes marcos da história da criptografia moderna deve-se ao alemão Arthur Scherbius, com a criação da sua máquina criptográfica conhecida como Enigma, conforme mostrado na Figura 4.2.

Figura 4.2: Máquina Enigma

Fonte: Bezerra (2017)

Criada em 1918, era composta por um teclado pelo qual dava-se entrada em cada letra do texto original, uma unidade misturadora, responsável por cifrar cada letra inserida por meio do teclado, e um mostrador, que iluminava a letra cifrada.

> [...] a Enigma fornecia dez quatrilhões de possibilidades de cifrar uma mensagem. Com tantas possibilidades de codificação, esse foi por muito tempo o trunfo dos alemães durante a Segunda Guerra Mundial. Contudo, em 1943, o matemático inglês Alan Turing (1912-1954) juntamente com sua equipe deu início ao projeto Colossus. Financiado pelo governo britânico, Turing criou o primeiro computador da história que foi utilizado para decodificar as mensagens codificadas pela Enigma. Com isso, todo o desfecho da Segunda Guerra Mundial foi modificado (DANTAS, 2016, p.16).

Após a Segunda Guerra Mundial, deu-se início ao desenvolvimento de computadores muito mais poderosos que o Colossus, bem como, a criação de códigos mais complexos do que aqueles da Enigma. Surgia, assim, a Era da Informática (BEZERRA, 2016, p.80).

Um dos maiores problemas dos códigos, utilizados até então, estava no fato de ter que se transmitir, ao destinatário da mensagem, a chave que havia sido usada para cifrá-la e que seria a mesma a ser usada para decifrar a mensagem.

Diante desse problema, dois grupos de matemáticos analisaram a questão e chegaram a uma mesma conclusão: a chave para cifrar deveria ser pública e livremente transmitida e a chave para decifrar deveria ser privada, de conhecimento exclusivo do destinatário da mensagem. Assim a ideia era que a mensagem fosse cifrada por uma função matemática de "mão única", isto é, de fácil aplicação, mas de difícil reversão (MACHADO, 2012, p.5).

Em 1977, três pesquisadores do M.I.T. (Massachusetts Institute of Technology), R. L. Rivest, A. Shamir e L. Adleman, foram os responsáveis por criar o mais conhecido dos métodos de criptografia de chave pública, o RSA. A sigla RSA é formada pelas letras iniciais dos nomes dos seus inventores.

O RSA tem suas raízes em teoremas clássicos da Teoria dos Números e se baseia num antigo problema matemático que era o de obter os fatores primos de um determinado número. E é na dificuldade em se fatorar números muito grandes que está a segurança desse sistema.

> O método de criptografia RSA baseia-se neste sistema de chaves duplas e na impossibilidade prática de se obter a chave secreta a partir da chave pública. Isto se deve ao fato de não se conhecer atualmente algoritmos para decompor números grandes em fatores primos em um tempo razoável – uma impossibilidade tecnológica (BEZERRA, 2016, p.108).

A evolução da criptografia tem sido contínua. Até hoje vários algoritmos têm sido criados e testados, a fim de se encontrar métodos cada vez mais prático e eficientes de criptografar uma mensagem. Os avanços tecnológicos e os estudos matemáticos relacionados com a criptografia vem crescendo com o passar do tempo, sempre na busca de encontrar soluções que tragam segurança na transmissão de informações onde possam existir situações de perigo (OLIVEIRA, 2011, p.4).

Para tanto, diversos conceitos matemáticos tem sido utilizados como recursos nesse processo, a exemplo: divisibilidade, máximo divisor comum, números primos, fatoração de números inteiros, conjuntos, funções, matrizes. Esses princípios quase sempre são estudados de forma abstrata e descontextualizada, fazendo com que o aluno não perceba uma aplicação prática desses conteúdo.

4.2 Cifras Criptográficas

A cifra é um ou mais algoritmos (conjunto de regras e procedimentos que levam à solução de um problema em um número finito de etapas) que cifram e decifram um texto. A execução do algoritmo tem como critério o uso de uma chave criptográfica que deve ser de conhecimento restrito àqueles que estão envolvidos no processo de comunicação. A cifra pode ser de conhecimento público, mas a chave deve ser privada.

Em uma linguagem informal, cifra e código tem o mesmo significado. Porém,

em uma linguagem técnica, especializada, essas palavras tem significados bem diferentes. Formalmente, o código funciona manipulando o significado, o que normalmente acontece através da substituição de palavras ou frases do texto, enquanto a cifra manipula a forma da representação da mensagem, como mudar as letras ou grupos de letras do texto.

1. **Código:** Substituir frases. "Guerra declarada"⇒ "Bandeira Branca".

2. **Cifra:** Substituir letras. "Guerra declarada"⇒ "jxhuud ghfodudgd".

De forma simplificada, os códigos não dependem de chave criptográfica e sim de tabelas de substituição ou outro mecanismo parecido, enquanto as cifras dependem da chave criptográfica para cifrar e decifrar uma mensagem.

As cifras criptograficas podem ser divididas em *cifras de transposição* e *cifras de substituição*. Na transposição, as letras da mensagem da mensagem original são rearranjadas, gerando um anagrama, enquanto na substituição cada letra na mensagem original é trocada por outra letra do alfabeto ou por um símbolo.

A transposição faz com que cada letra mantenha sua identidade, mas muda sua posição, em contrapartida, a substituição faz com que as letras mudem de identidade, retendo a posição.

4.2.1 Cifras de Transposição

As cifras de transposição utilizam como processo de cifragem a mudança de posição das letras, números ou símbolos do texto original, ou seja, é feita uma alteração na ordem das letras, números ou símbolos, como em um anagrama. A decifração da mensagem ocorre utilizando-se o processo inverso.

Matematicamente, trata-se da aplicação de uma função bijectiva, utilizada para cifrar a mensagem e da sua respectiva função inversa utilizada para decifrar essa mensagem.

Para mensagens muito curtas, de uma palavra, por exemplo, a transposição é um método inseguro, pois existe uma quantidade finita de de maneiras que se pode reordenar as letras de uma palavra, como mostrado no exemplo 4.1, cinfrando-se a mensagem: EVA.

Exemplo 4.1. ***EVA*** *- EAV - AVE - AEV - VEA - VAE*

Por outro lado, à medida que a quantidade de letras da mensagem aumenta o número de anagramas possíveis cresce exponencialmente tornando impossível decifrar a

mensagem sem que se conheça de maneira precisa o método pelo qual as letras foram misturadas.

> Uma transposição ao acaso das letras oferece um nível muito alto de segurança, porque não será possível que o interceptador inimigo consiga recompor até mesmo uma frase curta. Mas há uma desvantagem. A transposição efetivamente gera um anagrama incrivelmente difícil e, se as letras forem misturadas ao acaso, sem rima ou fundamento, a decodificação do anagrama se tornará impossível, tanto para o destinatário quanto para o interceptador inimigo (SINGH, 2007, p.23).

Assim, para que uma mensagem cifrada usando o métoda da transposição possa ser decifrada de maneira segura e eficaz, é necessário que o reordenamento das letras tenha seguido um sistema direto e tenha sido previamente acertado, exclusivamente, entre o emissor e o receptor da mensagem.

Apesar de existirem muitas maneiras de aplicar a cifra de transposição, serão mostradas duas das mais importantes: a Transposição de Colunas e a Cifra em Rail Fence (Cerca).

Transposição de Colunas

A utilização dessa cifra consiste inicialmente na escolha de uma palavra que funcionará como chave criptográfica e que será usada como cabeçalho da grelha na qual serão distribuídas as letras do texto que se deseja cifrar. A palavra chave não pode conter letras iguais.

Em seguida, escreve-se a mensagem que deseja-se cifrar, distribuindo cada letra da mensagem original abaixo de uma letra da chave criptográfica, de modo que todas as letras da mensagem a ser cifrada sejam organizadas em colunas que serão encabeçadas pelas letras da palavra chave. Caso todas as colunas na última linha não tenham sido preenchidas por letras do texto a ser cifrado deve-se, acrescentar letras (caracteres) sem significado apenas com o intuíto de completar todas as colunas, de acordo com a Tabela 4.1.

Concluída a etapa inicial, a mensagem que será transmitida, deverá ser escrita por colunas, de modo que a ordem das colunas a serem colocadas no texto cifrado deve obedecer a ordem alfabética das letras no cabeçalho, como mostra a Tabela 4.2.

Exemplo 4.2. *A forma cifrada da mensagem: O SOL JÁ VAI RAIAR E A LUA SE*

RETIRAR, utilizando-se o método da tranposição de colunas e considerando-se a chave criptográfica: CAMELO, é:

Tabela 4.1: Grelha 1

C	**A**	**M**	**E**	**L**	**O**
O	S	O	L	J	A
V	A	I	R	A	I
A	R	E	A	L	U
A	S	E	R	E	T
I	R	A	R	B	T

A palavra chave em ordem alfabética: ACELMO.

Tabela 4.2: Grelha 2

A	**C**	**E**	**L**	**M**	**O**
SARSR	OVAAI	LRARR	JALEB	OIEEA	AIUTT

Portanto a mensagem cifrada é: SARSROVAAILRARRJALEBOIEEAAIUTT.

Para decifrá-la, o receptor da mensagem deve dividir o comprimento da mensagem, que corresponde à quantidade de letras da mensagem cifrada (30) pelo da chave (6), e ler as colunas pela ordem das letras da chave.

Cifra Rail Fence ou Cerca de Trilhos

A cifra Rail Fence, também conhecida como Cerca de Trilhos, tem como algoritmo a distribuição dos caracteres sobre uma "cerca"virtual fazendo-se um movimento de zig-zag.

O processo inicia removendo-se, da mensagem que será cifrada, todos os espaços em branco e definindo a quantidade de rails (ou trilhas) que se quer usar para cifrar a mensagem, essa quantidade será a chave criptográfica. Em seguida, cria-se uma tabela que contenha a quantidade de linhas coincidindo com a cifra criptográfica e a quantidade de colunas de acordo com o número total de caracteres da mensagem a ser cifrada.

Com a tabela pronta, inicia-se o seu preenchimento distribuindo os carcteres de cima para baixo e depois de baixo pra cima, preenchendo, inicialmente, a primeira linha (trilha) e a primeira coluna com o primeiro caracter. Para cada novo caracter preenche-se a

próxima coluna na linha abaixo do caracter anterior até chegar à última linha. Chegando à última trilha, começa-se a subir preenchendo a próxima coluna na linha acima. Ao chegar na primeira trilha, novamente o processo repetirá até todos os carcteres da mensagem terem sido colocados na tabela.

Com a tabela preenchida, a cifragem é feita extraindo-se da tabela os carcteres por linha, começando da primeira. O Exemplo 4.3 mostra uma aplicação da cifra.

Exemplo 4.3. *Considere a mensagem DESVENDANDO SEGREDOS e a chave criptográfica 4. Escreva a forma cifrada da mensagem utilizando-se a cifra Rail Fence.*

I. Inicialmente, tira-se os espaços entre as palavras da mensagem a ser cifrada, assim tem-se: DESVENDANDOSEGREDOS.

II. Constrói-se uma tabela contendo 4 linhas, isto é, 4 trilhas, que corresponde à chave criptográfica 4. Já o número de colunas é 19, que corresponde à quantidade de caracteres da mensagem que será cifrada.

III Distribui-se os caracteres da mensagem na tabela.

IV Finalizando-se o processo, a mensagem cifrada será retirada da tabela, linha a linha, na ordem em que os caracteres aparecem.

O resultado é mostrado na Tabela 4.3.

Tabela 4.3: Cerca de Trilhos

D						D						E						S
	E				N		A				S		G				O	
		S		E				N		O				R		D		
			V						D						E			

A mensagem cifrada é DDESENASGOSENORDVDE.

Uma forma de decifrar essa mensagem é construindo a tabela de acordo com a chave criptográfica, que determina o número de linhas e a quantidade de carcteres da mensagem cifrada, que determina a quantidade de coluna. Depois, é só preencher a tabela colocando o primeiro caractere do primeiro bloco na primeira linha e na primeira coluna. Em seguida, coloca-se o primeiro caractere, do segundo bloco, na linha logo abaixo e na segunda coluna, repetindo até terminar todos os primeiros caracteres de cada

bloco.Posteriormente, inicia-se colocando o segundo caractere de cada bloco, depois, o terceiro até que todos os caracteres tenham sidos preenchidos. Então, a mensagem decifrada estará distribuída nas colunas.

4.2.2 Cifras de Substituição

Uma cifra de substituição tem como principal característica a manutenção da posição dos caracteres do texto original. Eles são trocados por outros caracteres (letra, número ou símbolo) de um conjunto previamente escolhido, chamado de alfabeto de substituição ou alfabeto de cifra, de acordo com um sistema predefinido e fazendo uso de uma chave criptográfica, dando origem aos chamados criptogramas. Além da substituição de caracteres de maneira isolada, pode-se também substituir palavras ou até mesmo frases inteiras.
Existem algumas classificações dadas para as cifras de substituição, trataremos neste trabalho apenas duas destas classificações a monoalfabética e a polialfabética.

Substituição simples ou monoalfabética é aquela em que para cada caracter do texto original associa-se um caracter de um único alfabeto de substituição, enquanto a substituição polialfabética utiliza mais de um alfabeto de substituição para cifrar um texto.

Os alfabetos não precisam ter origens diferentes. Dessa forma, por exemplo, um alfabeto grego e o outro latino, basta mudar a ordem na sequência das letras de um alfabeto que já se obtém um "novo"alfabeto. Assim por exemplo, um novo alfabeto criado a partir do alfabeto latino pode ser *b-c-d-e-...-w-y-z-a*, enquanto *c-d-e-f-...-w-y-z-a-b* já seria um alfabeto diferente.

Neste trabalho, serão abordadas três das mais conhecidas cifras de substituição, a Cifra de César, que é uma cifra de substituição monoalfabética, a Cifra de Vigenère e a Cifra de Hill que são de substituição polialfabética.

Cifra de César

O primeiro documento que usou uma cifra de substituição para propósitos militares aparece nas *Guerras da Gália* de Júlio César. Nos registros, ele descreve como substituiu

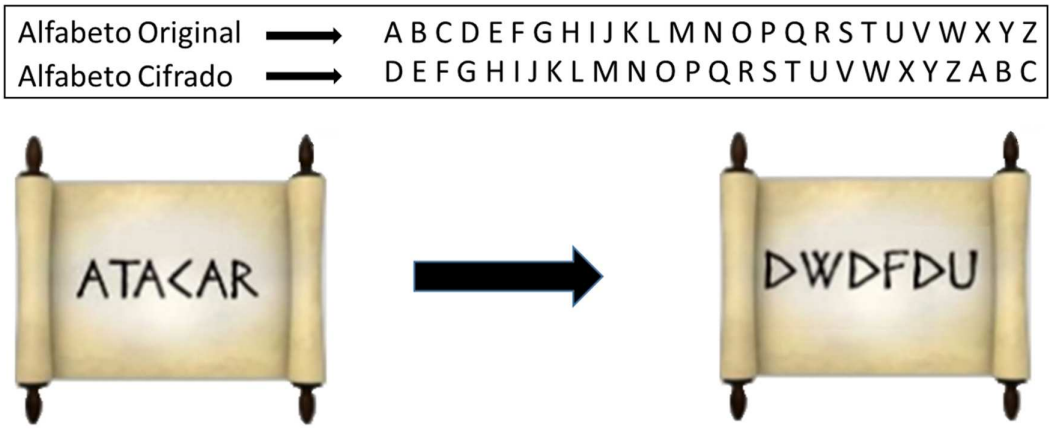
as letras do alfabeto romano por letras gregas, o que tornou a mensagem intelegível aos seus inimigos (SINGH, 2007, p.26).

Júlio César usava frequentemente a *criptografia* em suas mensagens. Uma de suas técnicas mais conhecidas foi detalhadamente descrita em *As vidas dos Césares*, escrito no século II por Suetônio. Essa técnica substituía cada letra na mensagem original por uma outra que estivesse três posições à frente no alfabeto. Este tipo de substituição é conhecido como *cifra de deslocamento de César* ou, simplesmente, *cifra de César*.

Portanto, o método que troca a letra original na mensagem por outra letra que está a uma certa quantidade de casas depois dela é o chamado *algoritmo* e a quantidade de casas que se desloca é a *chave*. Em particular, no caso da *cifra de César*, como o deslocamento das letras é de 3 casas, a chave é 3.

Assim, ao se colocar o alfabeto original acima do alfabeto cifrado vê-se, claramente, que as letras do código foram deslocadas três posições, como mostra a Figura 4.3.

Figura 4.3: Cifra de César



Fonte: Adaptado do Slideshare: Criptografia redes de computadores (2018)

Exemplo 4.4. *Cifre a mensagem A MINHA COR PREFERIDA É O VERMELHO, usando-se a cifra de César.*

Mensagem original	A	M	I	N	H	A	C	O	R	P	R	E	F	E	R	I	D	A	E	O	V	E	R	M	E	L	H	O
Mensagem cifrada	D	P	L	Q	K	D	F	R	U	S	U	H	I	H	U	I	G	D	H	R	Y	H	U	P	H	O	K	R

Logo a mensagem cifrada é DPLQKDFRUSUHIHUIGDHRYHUPHOKR.

A *cifra de César* tem ao todo 25 chaves possíveis, considerando-se qualquer deslocamento entre uma e 25 casas, o que a torna uma cifra extremamente frágil do ponto de

vista da criptoanálise, já que facilmente pode-se testar cada uma das 25 possibilidades. No entanto, considerando-se não apenas o deslocamento das letras, como também qualquer rearranjo do alfabeto original, poderão ser geradas mais de $4 \cdot 10^{26}$ cifras distintas. Em termos de um método geral de codificação conhecido como *algoritmo* e uma *chave*, que especifica os detalhes exatos de uma codificação em particular (SINGH, 2007, p.27).

A ideia é que mesmo se o inimigo conseguir interceptar uma mensagem cifrada, ainda que ele conheça o *algoritmo* usado para codificar a mensagem, ou seja, ele pode até saber que cada letra do texto original foi substituída por outra de um alfabeto cifrado, mas se ele não conhecer a *chave* não poderá decifrar a mensagem. Desse modo, percebe-se que a segurança de um código depende, exclusivamente, de manter a chave em segredo.

Para que se tenha um sistema de código seguro, é necessário que este possua um grande número de *chaves*. A *cifra de César*, por ter apenas 25 chaves, é considerada um sistema de codificação fraco, porém, considerando-se um algoritmo de substituição mais geral, ou seja, um rearranjo qualquer do alfabeto. Então, existe $4 \cdot 10^{26}$ chaves possíveis. Fazendo-se uso da força bruta seríam necessários, aproximadamente, um bilhão de vezes o tempo de existência do universo para se testar todas as chaves e decifrar a mensagem, o que a torna uma cifra fácil de executar mas, que oferece um alto nivel de segurança.

Uma opção para se obter um alfabeto cifrado de forma simples, sem precisar rearranjar ao acaso o alfabeto original, é escolher uma *palavra-chave* ou uma *frase-chave* que será usada como o início do alfabeto. Removendo-se os espaço e as letras repetidas, o restante do alfabeto começa onde a palavra cifrada ou frase cifrada termina, excluindo-se as letras que já foram usadas na palavra-chave.

Exemplo 4.5. *O alfabeto gerado a partir da frase- chave CIFRA DE CÉSAR é obtido inicialmente retirando-se os espaços e as letras repetidas da frase-chave. Dessa forma ,tem-se a palavra CIFRADES, que será usada como o início do alfabeto seguido das outras letras que não estão presentes nessa palavra. A Tabela 4.4 mostra o alfabeto cifrado.*

Tabela 4.4: Alfabeto gerado pela frase-chave CIFRA DE CÉSAR

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m	$\cdots$
Alfabeto cifrado	C	I	F	R	A	D	E	S	T	U	V	W	X	$\cdots$

$\cdots$	n	o	p	q	r	s	t	u	v	w	x	y	z
$\cdots$	Y	Z	B	G	H	J	K	L	M	N	O	P	Q

Cifra de Vigenère

A *cifra de Vigenère*, também conhecida como "*a cifra indecifrável*", é um tipo de cifra polialfabética, pois emprega mais de um alfabeto cifrado para codificar uma mensagem. A natureza polialfabética da *cifra de Vigenère* é responsável por sua força e a faz mais complexa do que uma cifra monoalfabética.

Essa cifra ficou conhecida como a *cifra de Vigenère* em homenagem ao diplomata francês Blaise de Vigenère reponsável por desenvolvê-la na sua forma final, visto que os estudos que se precederam ao surgimento dessa cifra tiveram início no século XV, quando o arquiteto Leon Battista Alberti propôs o uso de dois ou mais alfabetos cifrados, que deveriam ser usados alternadamente para codificar uma mensagem, na tentativa de confundir os criptoanalistas que quisessem decifrar aquela mensagem. Embora esse tivesse sido o avanço mais significativo das cifras num período de mil anos, Alberti não conseguiu concluir sua idéia a ponto de desenvolver um sistema completo (SINGH, 2007).

Posteriormente aos estudos iniciados por Alberti, outros intelectuais como o abade alemão Johannes Trithemius e o cientista italiano Giovanni Porta deram prosseguimento aos trabalhos de Alberti na tentativa de desenvolver um sistema completo de cifragem, mas não tiveram sucesso.

Somente por volta do ano de 1562, Blaise de Vigenére, começou a examinar em detalhes os trabalhos de Alberti, Trithemius e Porta, misturando as ideias e desenvolvendo uma nova e poderosa cifra, que culminou em seu *Traicté des Chiffres*, um tratado sobre a Escrita Secreta, publicado em 1586.

A *cifra de Vigenére* utiliza 26 alfabetos cifrados possíveis para codificar uma mensagem. Para isso, inicialmente, deve-se construir um quadrado, chamado de quadrado de Vigenère, que é obtido montando uma tabela na qual na primeira linha é colocado, em letra minúscula, o alfabeto normal e abaixo dessa linha, com letra maiúscula, escreve-se o alfabeto da linha anterior deslocando-se uma letra de posição.

Assim a linha 1 representa um alfabeto cifrado com a cifra de César na chave 1, a linha 2 representa um alfabeto cifrado na cifra de César na chave 2 e assim por diante até a última linha, quando retorna-se ao alfabeto original, coincidindo com a linha que está no topo do quadrado. A Tabela 4.5 mostra o *quadro de Vigenère*.

Na *cifra de Vigenère*, cada letra da mensagem a ser cifrada será codificada por um alfabeto cifrado diferente do quadrado, contudo, para que seja possível a codificação,

Tabela 4.5: *Quadro de Vigenère*

Alfabeto correto	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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

inicialmente, escolhe-se uma palavra-chave ou frase-chave, de modo que, se houver espaços ou letras repetidas, deve-se excluí-los antes de iniciar o processo. É importante observar que quanto maior a palavra-chave, mais difícil será quebrar essa cifra.

Caso o remetente da mensagem use apenas um dos alfabetos cifrados, ou seja, use uma chave única numérica ao invés da palavra-chave, isso resultaria em uma cifra de César simples, que poderia se facilmente decifrada por um interceptador inimigo.

A palavra-chave escolhida é escrita acima da mensagem original e repetida até que cada letra da mensagem esteja associada a uma letra da palavra-chave. As letras da palavra-chave são substituídas por números correspondentes a elas que variam de 1 a 26. Então, para cada símbolo do texto original, um substituto é colocado, localizado na linha, começando com o número que está associado a uma letra correspondente da

palavra chave e na coluna começando com a letra do texto original. Uma aplicação do código é mostrada no Exemplo 4.6.

Exemplo 4.6. *Usando-se a palvra-chave VENTILADOR codifique a mensagem O CAMINHO É LONGO, fazendo uso da cifra de Vigenère.*

1. *Primeiro escreve-se a palavra-chave acima do texto original, repetindo-a até que todas as letras da mensagem original estejam associadas a uma letra da palavra-chave, como mostrado na Tabela 4.6.*

Tabela 4.6: 1º Passo

Palavra-chave	V	E	N	T	I	L	A	D	O	R	V	E	N	T
Mansagem original	O	C	A	M	I	N	H	O	E	L	O	N	G	O

2. *Em seguida, associa-se cada letra da palvra-chave a um número variando de 1 a 26, como indicado na Tabela 4.7.*

Tabela 4.7: 2º Passo

Palavra-chave	V	E	N	T	I	L	A	D	O	R	V	E	N	T
Número	22	5	14	20	9	12	1	4	15	18	22	5	14	20

3. *Por fim, substitui-se cada letra da mensagem original pela letra do quadro de Vigenère que está localizada na intesecção entre a linha indicada pelo número da palavra-chave e pela coluna representada por cada letra da mensagem original, o resultado é o mostrado na Tabela 4.8.*

Tabela 4.8: 3º Passo

Número	22	5	14	20	9	12	1	4	15	18	22	5	14	20
Mansagem original	O	C	A	M	I	N	H	O	E	L	O	N	G	O
Mensagem cifrada	K	C	O	G	R	Z	I	S	T	D	K	S	U	I

Logo a mensagem cifrada é KCOGRZISTDKSUI.

A grande vantagem dessa cifra é que ela é imune à análide de frequência das letras, usada por muitos criptoanalistas para decifrar um texto criptografado, com padrões que se repetem constantemente, o que pode indicar a ocorrêcia de letras de uso frequente, como a vogal “a”, ou até palavras corriqueiras como“sim”ou “não”.

Para decifrar a mensagem, deve-se, inicialmente, escrever a palavra-chave acima da mensagem cifrada. Depois, verifica-se qual número está associado a cada letra desta palavra. Na linha indicada pelo número, busca-se a letra da mensagem cifrada e verifica-se qual é a letra do alfabeto original, localizada no topo do quadro, que foi associado a ela. Substituindo-se assim, cada uma das letras da mensagem cifrada e desvendando-se a mensagem original.

Cifra de Hill

A cifra de Hill foi desenvolvida por Lester S. Hill e é caracterizada como um cripto-sistema de substituição polialfabética. É um sistema criptográfico baseado em transformações lineares para a substituição de uma mensagem original por uma mensagem criptografada, fazendo uso de conceitos estudados em Álgebra Linear, para codificar e decodificar uma mensagem através da multiplicação de matrizes.

A cifra baseia-se em codificar uma mensagen a partir de uma matriz quadrada, isto é, NxN, que servirá como chave criptográfica e, portanto, deverá ser matida em segredo, sendo revelada apenas ao receptor da mensagem, que irá decifrar o conteúdo secreto fazendo uso da inversa dessa matriz. Logo, nesse processo só é possível usar matrizes inversíveis.

Uma mensagem codificada com uma matriz nxn recebe o nome de"N-Cifra de Hill". Assim, ao se codificar uma mensagem com uma matriz 2x2, esta será chamada "2-Cifra de Hill".

O procedimento se dá, inicialmente, substituindo-se as letras da mensagem original por números, depois, agrupando-se os números n a n e multiplicando-se cada grupo por uma matriz quadrada de ordem n inversível, ou seja, que tenha determinante diferente de 0. Os números resultantes são novamente passados para letras, e, dessa forma, obtém-se a mensagem criptografada.

Se o resultado de alguma das multiplicações, obtidas nesse processo, for um número maior que o número de letras do alfabeto utilizado para cifrar a mensagem, então deve-se utilizar o resto desse número pelo número de letras do alfabeto.

Para fins deste trabalho, será adotada a Tabela 4.9 de correspondência que associa cada letra do alfabeto aos números indicados.

O Exemplo 4.7 mostra uma aplicação de como codificar uma mensagem usando a

Tabela 4.9: Correspondência entre letras e números

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

cifra de Hill.

Exemplo 4.7. *O método será demonstrado codificando-se a mensagem "O PODER DA MENTE", usando-se como chave criptográfica a matriz* $A = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix}$.

1. *Primeiramente agrupa-se a mensagem de acordo com a ordem (n) da matriz escolhida, se necessário acrescentam-se letras que não tenham sentido na mensagem, para completar o último grupo. Neste caso, como n = 2, tem-se*

$$OP\ \text{-}\ OD\ \text{-}\ ER\ \text{-}\ DA\ \text{-}\ ME\ \text{-}\ NT\ \text{-}\ EK$$

2. *Substitui-se as letras pelos seus respectivos valores, de acordo com a tabela 4.9, assim tem-se*

O	*P*	-	*O*	*D*	-	*E*	*R*	-	*D*	*A*	-	*M*	*E*	-	*N*	*T*	-	*E*	*K*
↓	↓		↓	↓		↓	↓		↓	↓		↓	↓		↓	↓		↓	↓
14	*15*	-	*14*	*3*	-	*4*	*17*	-	*3*	*0*	-	*12*	*4*	-	*13*	*19*	-	*4*	*10*

3. *Posteriormente cada par de números irá constituir um vector coluna p, que será multiplicado pela matriz A, dando origem a um novo par (c) cifrado, tal que c = Ap. Assim,*

$$OP \rightarrow \begin{bmatrix} 14 \\ 15 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 14 \\ 15 \end{bmatrix} = \begin{bmatrix} 73 \\ 89 \end{bmatrix} = \begin{bmatrix} 21 \\ 11 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 21 \\ 11 \end{bmatrix} \rightarrow VL.$$

$$OD \rightarrow \begin{bmatrix} 14 \\ 3 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 14 \\ 3 \end{bmatrix} = \begin{bmatrix} 37 \\ 29 \end{bmatrix} = \begin{bmatrix} 11 \\ 3 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 11 \\ 3 \end{bmatrix} \rightarrow LD.$$

$$ER \rightarrow \begin{bmatrix} 4 \\ 17 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} = \begin{bmatrix} 59 \\ 89 \end{bmatrix} = \begin{bmatrix} 7 \\ 11 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 7 \\ 11 \end{bmatrix} \rightarrow HL.$$

$$DA \rightarrow \begin{bmatrix} 3 \\ 0 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 3 \\ 0 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 6 \\ 3 \end{bmatrix} \rightarrow GD.$$

$$ME \rightarrow \begin{bmatrix} 12 \\ 4 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 12 \\ 4 \end{bmatrix} = \begin{bmatrix} 36 \\ 32 \end{bmatrix} = \begin{bmatrix} 10 \\ 6 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 10 \\ 6 \end{bmatrix} \rightarrow KG.$$

$$NT \rightarrow \begin{bmatrix} 13 \\ 19 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 13 \\ 19 \end{bmatrix} = \begin{bmatrix} 83 \\ 108 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 5 \\ 4 \end{bmatrix} \rightarrow FE.$$

$$EK \rightarrow \begin{bmatrix} 4 \\ 10 \end{bmatrix},\ então\ Ap = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} 4 \\ 10 \end{bmatrix} = \begin{bmatrix} 38 \\ 54 \end{bmatrix} = \begin{bmatrix} 12 \\ 2 \end{bmatrix} = c,\ logo\ \begin{bmatrix} 12 \\ 2 \end{bmatrix} \rightarrow MC.$$

Portanto a mensagem codifidaca é VLLDHLGDKGFEMC.

Para decifrar a mensagem utiliza-se o mesmo processo, no entanto, a matriz utilizada será a matriz inversa.

Em aritmética euclidiana, cada número não-nulo a, tem um inverso multiplicativo, denotado por a^{-1}, tal que

$$aa^{-1} = a^{-1}a = 1.$$

Em aritmética modular, tem-se que dado um número a em $\mathbb{Z}_m$, existe um número a^{-1} que é inverso multiplicativo de a módulo m se

$$aa^{-1} = a^{-1}a \equiv 1(mod\ m).$$

Tem-se também que, se a e m não têm fatores primos comuns. Então a tem um único inverso multiplicativo módulo m; analogamente, se a e m têm fator primo comum, então a não tem inverso multiplicativo módulo m.

Ainda em aritmética modular, uma matriz A com entradas em $\mathbb{Z}_m$ é inversível módulo m se houver uma matriz A^{-1} tal que

$$A \cdot A^{-1} = A^{-1} \cdot A \equiv I(mod\ m).$$

De acordo com a Tabela 4.9, o alfabeto utilizado é composto por 26 letras, logo, $m = 26$. Daí tem-se que se $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ é inversível módulo 26 e se $p = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ é um vetor, então $c = A \cdot p$ é o correspondente vetor cifrado e $p = A^{-1} \cdot c$.

Portanto, cada vetor pode ser recuperado do correspondente vetor cifrado pela multiplicação à esquerda por $A^{-1}(mod 26)$.

Como em aritmética modular, uma matriz quadrada é inversível se, e somente se, $detA \neq 0$. A inversa de $detA$ $(mod\ 26)$ é dada por:

$$A^{-1} = (detA)^{-1}. \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} (mod 26).$$

Para uma referência futura, fornece-se a seguinte Tabela 4.10 de inversos módulo 26.

Tabela 4.10: Inversos Módulo 26

a	1	3	5	7	9	11	15	17	19	21	23	25
a^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

O Exemplo 4.8, mostra uma aplicação de como decifrar uma mensagem usando da cifra de Hill.

Exemplo 4.8. *Para ilustrar o processo de descriptografia, será utilizada a mensagem, VLLDHLGDKGFEMC, cifrada no Exemplo 4.7.*

1. *Para decifrar a mensagem, é preciso encontrar a inversa da matriz* $A = \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix}$ *que foi usada como chave criptográfica no Exemplo 4.7. Para tanto, primeiramente, será encontrado do detA, portanto*

$$detA = (a_{11}a_{22} - a_{12}a_{21}) \Longrightarrow detA = (2 \cdot 5 - 3 \cdot 1) \Longrightarrow detA = 7.$$

2. *Em seguida, determina-se o* $(detA)^{-1}$*, nesse caso, o inverso multiplicativo de 7 módulo 26, que pela Tabela 4.10 o* $(detA)^{-1}$ *é 15.*

3. *Calculando-se a inversa da matriz A tem-se*

$$A^{-1} = (detA)^{-1} \cdot \begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix} (mod 26) \Rightarrow A^{-1} = 15 \cdot \begin{bmatrix} 5 & -3 \\ -1 & 2 \end{bmatrix} (mod 26) \Rightarrow$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 75 & -45 \\ -15 & 30 \end{bmatrix} (mod 26) \Rightarrow A^{-1} = \begin{bmatrix} 23 & 7 \\ 11 & 4 \end{bmatrix} (mod 26)$$

4. *Posteriormente, agrupa-se a mensagem de acordo com a ordem (n) da matriz inversa.*

VL - LD - HL - GD - KG - FE - MC

5. *Substitui-se as letras da mensagem cifrada pelos seus respectivos valores, de acordo com a Tabela 4.9.*

V	*L*	-	*L*	*D*	-	*H*	*L*	-	*G*	*D*	-	*K*	*G*	-	*F*	*E*	-	*M*	*C*
↓	↓		↓	↓		↓	↓		↓	↓		↓	↓		↓	↓		↓	↓
21	*11*	-	*11*	*3*	-	*7*	*11*	-	*6*	*3*	-	*10*	*6*	-	*5*	*4*	-	*12*	*2*

6. *Finalmente, cada par de números irá constituir um vetor coluna , que será multiplicado pela matriz A^{-1}, dando origem a um par decifrado. Assim,*

$$VL \rightarrow \begin{bmatrix} 21 \\ 11 \end{bmatrix}, \text{ então } \begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \cdot \begin{bmatrix} 21 \\ 11 \end{bmatrix} = \begin{bmatrix} 560 \\ 275 \end{bmatrix} = \begin{bmatrix} 14 \\ 15 \end{bmatrix} \rightarrow OP.$$

O processo se repete até que todos os vetores sejam multiplicados pela inversa de A, retornando-se à mensagem original que nesse caso é "O PODER DA MENTE".

4.3 Cripto-sistema

A mensagem a ser enviada é chamada de texto-original (plaintext) e a mensagem codificada é chamada de texto-cifrado (ciphertext). O texto-original e o texto-cifrado são escritos em algum alfabeto $\mathbb{F}$ consistindo de um certo número n de símbolos; isto é,

$$\#(\mathbb{F}) = n.$$

O texto-original e texto-cifrado são divididos em mensagens unitárias. Uma mensagen unitária poder ser um bloco de k símbolos do alfabeto $\mathbb{F}$. O processo de codificação é uma função que associa cada mensagem unitária u do texto-original a uma mensagem unitária c do texto-cifrado. Mais precisamente, sejam $\mathcal{P}$ o conjunto de todas as possíveis mensagens unitárias u do texto-original e $\mathcal{C}$ o conjunto de todas as possíveis mensagens unitárias c do texto-cifrado. Então a correspondência biunívoca

$$f : \mathcal{P} \rightarrow \mathcal{C} \text{ tal que } f(u) = c$$

é o processo de codificação. A correspondência biunívoca

$$f^{-1} : \mathcal{C} \to \mathcal{P} \text{ tal que } f^{-1}(c) = u$$

é o processo de decodificação. Assim, temos o seguinte diagrama

$$\begin{array}{ccccc} & & f & & f^{-1} & \\ \mathcal{P} & \longrightarrow & \mathcal{C} & \longrightarrow & P \end{array}$$

Cripto-sistema

Portanto, um Cripo-sistema é qualquer bijeção de $\mathcal{P}$ sobre $\mathcal{C}$.

É útil substituir os símbolos de um alfabeto $\mathbb{F}$ por números inteiros 0, 1, 2, . . ., para tornar mais fácil a construção do cripto-sistema f. Uma correspondência natural entre o alfabeto

$$\mathbb{F} = \{A, B, C, ..., K, ..., X, Y, Z, \text{espaço} = \sqcup\}$$

e o conjunto de números inteiros

$$Z_{27} = 0, 1, 2, ..., 10, ..., 23, 24, 25, 26$$

é dada pela tabela:

$$\begin{array}{cccccccccc} \text{A} & \text{B} & \text{C} & \ldots & \text{K} & \ldots & \text{X} & \text{Y} & \text{Z} & \sqcup \\ \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow & \cdots & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 0 & 1 & 2 & \ldots & 10 & \ldots & 23 & 24 & 25 & 26. \end{array}$$

Teorema 4.1. *Sejam $n \in \mathbb{N}$ e $a, b \in \mathbb{Z}_n$ fixados. Se $mdc(a, n) = 1$, então a função $f : Z_n \to Z_n$ dada por $f(x) = ax + b$ é um cripto-sistema.*

Demonstração. Como $mdc(a, n) = 1$ temos que existe $a^{'} = a^{-1} \in \mathbb{Z}_n^{\bullet}$ tal que $a \cdot a^{'} = 1$. Assim,

$$f^{-1}(x) = a^{'}x + b^{'},$$

onde $b^{'} = -a^{'}b$, é tal que

$$f \circ f^{-1} = f^{-1} \circ f = I_{\mathbb{Z}_n};$$

isto é, f^{-1} é a função inversa de f . □

Observação 4.1. *O cripto-sistema*

$$f(x) = ax + b$$

é chamado de transformação afim. O par (a, b) *é chamado de chave de codificação ou chave secreta. Quando* $n = 27$, $a = 1$ *e* $b \in \mathbb{Z}_{27}$ *o cripto-sistema*

$$f(x) = x + b$$

é chamado de Cifra de César, pois Júlio César a utilizava. Quando $b = 0$ *o cripto-sistema* $f(x) = ax$ *é uma transformação linear.*

4.4 Criptografia RSA

O entendimento do funcionamento do RSA está atrelado ao estudo de idéias e técnicas construídas sobre uma das áreas mais clássicas da matemática, a Teoria dos Números.

Considerado um dos mais seguros sistemas de criptografia, o RSA é um sistema de chaves assimétricas, pois utiliza duas chaves criptográficas, uma chave pública e uma privada. A chave pública é usada para cifrar a mensagem e a chave privada para decifrar. A chave pública n é gerada a partir da multiplicação de dois números primos p e q, enquanto a chave privada é obtida pela decomposição desse produto. Portanto, o RSA é basicamente o resultado de dois cálculos matemáticos até certo pontomuito simples, pois um é o produto de dois números conhecidos e o outro é a fatoração de um número composto.

A dificuldade em quebrar esse sistema é que os números primos, p e q, usados para obter o produto **n**, são muito grandes. Na prática uma chave segura de RSA é gerada a partir de números primos de cerca de 100 algarismos cada, de forma que **n**, que é o produto desses primos, terá cerca de 200 algarismos. Sendo necessários cerca de zilhões de anos para fatorar um número deste tamanho e achar seus fatores primos, ainda que se faça uso dos mais poderosos computadores da atualidade (COUTINHO, 2016, p.10). Em resumo tem-se:

- para implementar o RSA, escolhemos dois primos distintos muito grandes p e q, e

calculamos o produto $n = p \cdot q$;

- para codificar uma mensagem usamos n;
- para decodificar uma mensagem usamos p e q;
- n pode ser tornado público;
- p e q precisam ser mantidos em segredo;
- quebrar o RSA consiste em fatorar n, que leva muito tempo se n for grande.

4.4.1 Descrição do método RSA

Os sistemas criptográficos de chave pública funcionam do seguinte modo: um usuário A desejando se comunicar com um usuário B, de maneira secreta, envia uma solicitação para início de comunicação. O usuário A determina um par de chaves (n, e) e (n, d) tais que

$$(n, e) \circ (n, d)(b) = b \; e \; (n, d) \circ (n, e)(b) = b,$$

no qual a chave (n, d) é mantida secreta e usada para a decodificação, enquanto a chave (n, e) é tornada pública e usada para codificação. O usuário A obtém a chave pública (n, e) e, assim, passa a codificar mensagens unitárias para o usuário B, pois só este conhece a chave secreta (n, d). Esses processos de codificação e decodificação deverão satisfazer as seguintes condições:

1. O cálculo das chaves (n, e) e (n, d) deve ser simples;
2. O usuário (transmissor) A deve realizar a operação de codificação facilmente, isto é,
$$c = (n, e)(b);$$
3. O usuário (receptor) B deve realizar a operação de decodificação facilmente, isto é,
$$b = (n, d)(c);$$
4. É praticamente impossível descobrir (n, d) a partir de (n, e). É claro que dada (n, e) tem-se uma maneira de descobrir $(n, d)(c)$, basta codificar toda mensagem unitária b e quando $c = (n, e)(b)$, tem-se que $b = (n, d)(c)$, mas isso torna-se inviável.

Em um sitema de criptografia de chave pública RSA, cada usuário A escolhe dois números primos extremamente grandes p e q (com aproximadamente 100 dígitos cada), donde tem-se $n = p \cdot q$, e aleatoriamente um inteiro e de forma que $mdc(\phi(n); e) = 1$ e $1 < e < \phi(n)$. Agora o usuário A torna pública a chave de codificação (n, e) e mantém secreta a chave de decodificação (n, d).

O processo de codificação é dado pela função

$$f : \mathbb{Z}_n \to \mathbb{Z}_n,\ f(b) = b^e$$

O processo de decodificação é dado pela função

$$f^{-1} : \mathbb{Z}_n \to \mathbb{Z}_n,\ f^{-1}(b) = b^d$$

Seja $\mathbb{F}$ um alfabeto com n símbolos. Cada letra do alfabeto é colocada em correspondência biunívoca com um número de dois algarismos, inclusive, o espaço entre as palavras, que é identificado pelo número 99, como mostra a Tabela 4.11.

Tabela 4.11: Correspondência biunívoca entre letra e número

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
10	11	12	13	14	15	16	17	18	19	20	21	22	23

O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	⊔
24	25	26	27	28	29	30	31	32	33	34	35	99

Após a pré-codificação, é obtida uma sequência de números, a qual é preciso separar em blocos apropriadamente.

Neste exemplo, os blocos foram denotados por b. Para cada inteiro b, relativamente primo com n, tem-se:

$$b\phi(n) \equiv 1(mod\ n). \tag{3}$$

Como para cada primo p, tem-se $\phi(p) = p - 1$, segue, das propriedades da *função totiente de Euler*, que

$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1).$$

O bloco codificado é o resto da divisão b^e por n. Assim, deve-se calcular $C(b)$, de

forma que:

$$b^e \equiv C(b)(mod\ n). \tag{4}$$

Para decifrar a mensagem é necessário encontrar um número d tal que

$$ed \equiv 1(mod\ (p-1)(q-1)). \tag{5}$$

Para isso, basta resolver, através do Algoritmo Euclidiano, a equação

$$ed + y\phi(n) = 1.$$

Após determinar d, encontra-se o resto da divisão de $C(b)^d$ por n. Assim, de 4.1,4.2 e 4.3 segue que

$$C(b)^d \equiv (b^e)^d \equiv b^{1+\phi(n)t} \equiv b(b^{\phi(n)})^t \equiv b(1^t) \equiv b(mod\ n).$$

Exemplo 4.9. *Usando os parâmetros $p = 11$ e $q = 13$, codifique a mensagem*

HOJE ACORDEI CEDO.

1. *A primeira etapa do processo é a chamada pré-codificação, na qual faz-se a substituição das letras da mensagem original por números associados a elas de acordo com a Tabela 4.11. Assim, obtém-se a sequência:*

   $$17241914991012242713141899121413 24;$$

2. *Como etapa final do processo de pré-codificação, quebra-se a mensagem em blocos menores que n, em que $n = p \cdot q$. Como $p = 11$ e $q = 13$, tem-se que $n = 11 \cdot 13$, logo $n = 143$. Assim a mensagem convertida pode ser quebrada nos seguintes blocos:*

   $$17 - 24 - 19 - 14 - 99 - 101 - 22 - 42 - 71 - 31 - 41 - 89 - 91 - 21 - 41 - 32 - 4;$$

3. *Em seguida determina-se $e \in \mathbb{Z}_+$, que seja inversível módulo $\phi(n)$. Ou seja, $mdc(e, \phi(n)) = 1$. Para o cáculo de $\phi(n)$ faz-se*

   $$\phi(n) = (p-1)(q-1).$$

Dessa forma, tem-se $\phi(143) = (11-1)(13-1) = 10 \cdot 12 = 120$. *Para* e, *escolhe-se* $e = 7$ *por ser o menor número primo com 120, tal que* $mdc(7, 120) = 1$. *Logo, o par* (n, e) *é chamado de chave de codificação do sistema RSA. Neste caso achave pública é o par* $(143, 7)$.

4. *Por fim, codifica-se os blocos obtidos, separadamente. Cada bloco denotado* b *é codificado de acordo com a expressão*

$$b^e \equiv C(b)(mod\ n).$$

Em termos de aritmética modular, $C(b)$ *é a forma reduzida de* b^e *módulo* n. *Assim, tem-se*

$Bloco17 \Rightarrow (17)^7 \equiv (51)^2 \cdot 17 \equiv 27 \cdot 17 \equiv 30(mod\ 143)$

$Bloco24 \Rightarrow (24)^7 \equiv (96)^2 \cdot 24 \equiv 64 \cdot 24 \equiv 106(mod\ 143)$

$Bloco19 \Rightarrow (19)^7 \equiv (138)^2 \cdot 19 \equiv 25 \cdot 1 \equiv 46(mod\ 143)$

$Bloco14 \Rightarrow (14)^7 \equiv (27)^2 \cdot 14 \equiv 14 \cdot 14 \equiv 53(mod\ 143)$

$Bloco99 \Rightarrow (99)^7 \equiv (44)^2 \cdot 99 \equiv 77 \cdot 99 \equiv 44(mod\ 143)$

$Bloco101 \Rightarrow (101)^7 \equiv (129)^2 \cdot 101 \equiv 53 \cdot 21 \equiv 62(mod\ 143)$

$Bloco22 \Rightarrow (22)^7 \equiv (66)^2 \cdot 22 \equiv 66 \cdot 22 \equiv 22(mod\ 143)$

$Bloco42 \Rightarrow (42)^7 \equiv (14)^2 \cdot 42 \equiv 53 \cdot 42 \equiv 81(mod\ 143)$

$Bloco71 \Rightarrow (71)^7 \equiv (18)^2 \cdot 71 \equiv 38 \cdot 71 \equiv 124(mod\ 143)$

$Bloco31 \Rightarrow (31)^7 \equiv (47)^2 \cdot 31 \equiv 64 \cdot 31 \equiv 125(mod\ 143)$

$Bloco41 \Rightarrow (41)^7 \equiv (138)^2 \cdot 41 \equiv 25 \cdot 41 \equiv 24(mod\ 143)$

$Bloco89 \Rightarrow (89)^7 \equiv (122)^2 \cdot 89 \equiv 12 \cdot 89 \equiv 67(mod\ 143)$

$Bloco91 \Rightarrow (91)^7 \equiv (104)^2 \cdot 91 \equiv 91 \cdot 91 \equiv 130(mod\ 143)$

$Bloco21 \Rightarrow (21)^7 \equiv (109)^2 \cdot 21 \equiv 12 \cdot 21 \equiv 109(mod\ 143)$

$Bloco41 \Rightarrow (41)^7 \equiv (138)^2 \cdot 41 \equiv 25 \cdot 41 \equiv 24(mod\ 143)$

$Bloco32 \Rightarrow (32)^7 \equiv (21)^2 \cdot 32 \equiv 12 \cdot 32 \equiv 98(mod\ 143)$

$Bloco4 \Rightarrow (4)^7 \equiv 82(mod\ 143)$

Logo, a mensagem codificada é

$$30106465344622281124125246713010924 98.$$

Exemplo 4.10. *Decifre a mensagem codificada no Exemplo 4.9*

$$30106465344622281124125246713010924 98.$$

1. *Para decodificar a mensagem é necessário encontrar o número inteiro positivo d, a partir da equação diofantina* $7d + 120y = 1$. *O par* (n, d) *é chamado de chave de decodificação.*

   Seja $C(b)$ *um bloco da mensagem codificada, denota-se por* $C(b)^d$ *o bloco decodificado, tal que*

   $$C(b)^d \equiv b(mod\ n).$$

   Para calcular d, determina-se inicialmente o $mdc(120, 7)$ *através do algoritmo de Euclides, portanto*

   $$120 = 17 \cdot 7 + 1$$

   $$7 = 1 \cdot 7.$$

   Sendo assim, o $mdc(120, 7) = 1$ *e a equação dada tem solução.*

   Para expressar, 1 como combinação linear de 120 e 7, basta eliminar o resto 1 na primeira igualdade, obtendo-se

   $$1 = 120 - 17 \cdot 7 = 7 \cdot (-17) + 120.$$

   Portanto, $d = -17$. *Porém d é um inteiro positivo, mas como* $-17 \equiv 103\ mod 120$, *tem-se então, que* $d = 103$.

   Logo a chave de decodificação é $(143, 103)$.

2. *Em seguida divide-se a mensagem cifrada em blocos menores que n, sendo* $n = 143$, *tem-se*

   $$30 - 106 - 46 - 53 - 44 - 62 - 22 - 81 - 124 - 125 - 24 - 67 - 130 - 109 - 24 - 98.$$

3. *Por fim decodifica-se os blocos codificados. Cada bloco denotado* $C(b)$ *é decodificado*

de acordo com a expressão

$$C(b)^d \equiv b(mod\ n).$$

Decodificando o primeiro bloco tem-se

$$Bloco\ 30 \Rightarrow (30)^{103} \equiv (133)^5(116) \equiv (100)(116) \equiv 17(mod\ 143)$$

De acordo com a Tabela 4.11, o número 17 corresponde à letra H.
Analogamente faz-se o mesmo procedimento para cada um dos blocos obtendo-se, como resultado, a mensagem decifrada.

5 APLICAÇÕES E RESULTADOS

Neste capítulo, são apresentadas as aplicações das atividades propostas, os procedimentos metodológicos adotados para desenvolver o trabalho e os resultados obtidos na realização das atividades.

Após a realização das atividades propostas, foram feitas avaliações para mostrar que os objetivos traçados foram alcançados.

O trabalho refere-se a uma pesquisa com abordagem qualitativa e quantitativa.

Na análise qualitativa, foi verificado o caráter subjetivo do objeto analisado, onde foram estudadas as particularidades e experiências individuais obseravdas ao longo do processo, elaborado através da coleta de dados narrativos e através da observção. Os alunos entrevistados estavam livres para apontar os seus pontos de vista sobre os assuntos relacionados com o objeto do estudo, assim como o seu comportamento e suas reações diante das atividades propostas.

A análise quantitativa objetiva retratar os resultados da pesquisa a partir de índices numéricos que apontam preferências, comportamentos, dificuldades e as principais necessidades dos estudantes pesquisados. Os dados apresentados foram coletados apartir da análise de questionários aplicados aos estudantes alvo da pesquisa, bem como na realização de atividades propostas nas quais foram associados conteúdos matemáticos ao uso da criptografia.

Para validar qualitativamente as atividades da pesquisa, foi lançado, no Colégio Militar Tiradentes VI - Escola Municipal Parque Vitória, localizada no bairro Parque Vitória, município de São José de Ribamar, o projeto "Desvendando Segredos", que tinha como objetivo principal atrair estudantes com conhecimentos mínimos suficientes para realização das atividades propostas, mas com pouco interesse em se aprofundar na disciplina de Matemática.

Para tanto, optou-se por abrir inscrições de forma voluntária para que apenas os alunos interessados em participar da pesquisa fizessem a avaliação diagnóstica que seria aplicada posteiormente. Nessa etapa, foi apresentado, em cada sala de aula, o tema e o objetivo geral da pesquisa, bem como os horários e o período de duração do projeto. A fase de inscrição ocorreu do dia 29 a 31 de janeiro de 2018.

No total 324 estudantes, do 6º ao 9º ano do ensino fundamental do Colégio Militar Tiradentes VI, increveram-se para participar do projeto, esse número corresponde a 72%,

dos alunos regularmente matriculados no turno vespertino da instituição.

Como segunda etapa de seleção, foi aplicado, no dia 05 de fevereiro de 2018, um teste diagnóstico, contendo cinco questões de conhecimentos matemáticos e uma pergunta de cunho pessoal sobre o grau de interesse desses alunos pela disciplina. O objetivo dessa etapa era selecionar 10 alunos de cada série. O resultado da seleção foi divulgado no dia 16 de fevereiro de 2018. A Figura 5.1 mostra um registro do grupo de alunos que participaram do projeto.

Figura 5.1: Registro Fotográfico dos Estudantes do Projeto "Desvendando Segredos"

Fonte: Próprio autor (2018)

Após selecionar os alunos, seguiu-se como terceira e última etapa, antes do início das atividades do projeto, que se deu através do encaminhamento de um documento, aos pais e/ou responsáveis, solicitando a autorização para que os alunos pudessem participar do projeto em vista da divulgação de suas imagens, do período e dos horários de realização dos trabalhos. Das 40 solicitações encaminhadas, quatro estudantes não foram autorizados a participar, o que levou a uma nova escolha de quatro alunos que haviam participado da seleção, e o encaminhamento das novas solicitações. Dos novos encaminhamentos todos foram autorizados.

Como os alunos selecionados realizam suas atividades escolares no turno vepertino, optou-se em realizar as atividades do projeto no contraturno, quer dizer, no turno matutino. Por indisponibilidade de uma sala livre, que que comportasse os 40 alunos ao mesmo tempo, optou-se por desenvolver os trabalhos por série, dividindo-os em quatro grupos

de dez alunos e trabalhando uma semana para cada série, com duas horas de atividades diárias, totalizando uma carga-horária de 10 horas semanais para cada grupo.

A abertura do projeto aconteceu no dia 26 de fevereiro de 2018 e as atividades finalizaram-se no dia 23 de março de 2018.

No primeiro dia de atividades de cada grupo, foi abordado o significado da palavra criptografia, definindo conceitos, histórico, destacando as principais cifras criptográficas, até chegar aos dias atuais, sempre buscando de maneira simples relacionar o tema abordado ao dia a dia desses estudantes. Nessa etapa, fez-se uso de uma apresentação de slides em data show. Na sequência, os alunos assitiram a um documentário entitulado "O que é Criptografia?", produzido por estudantes do sétimo semestre do curso de Comunicação Social - Jornalismo, do Instituto Superior de Ciências Aplicadas - ISCA Faculdades e publicado em 2016, com duração de 11m 24s.

Ao final, foi aplicado o Quetionário 1 que tinha como principais objetivos investigar a vivência de cada estudante com atividades práticas e ou lúdicas associadas à resolução de exercícios que abordam conteúdos matemáticos e o avaliar o grau de interesse desses estudantes pela matemática antes da participação no projeto "Desvendando Segredos".

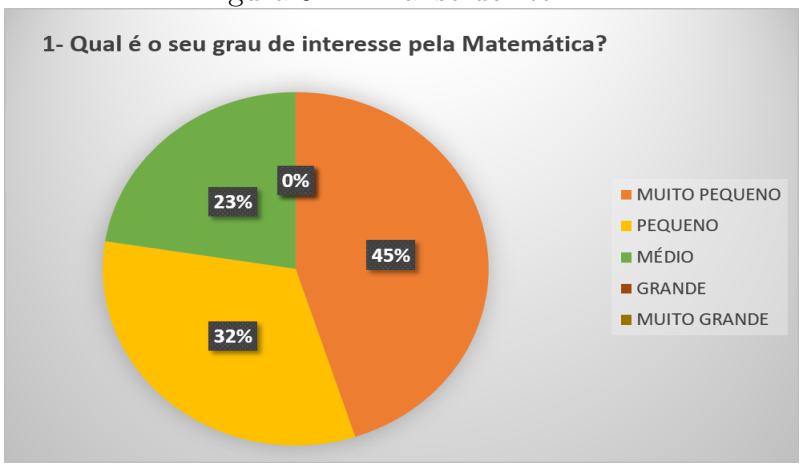
Posteriormente, os alunos desenvolveram atividades práticas elaborando alguns materiais concretos, que seríam utilizados na resolução das atividades propostas. À medida que os alunos confeccionavam um determinado material em seguida fazia-se a atividade a ele relacionada e assim sucedeu-se até o último dia de atividades quando os estudantes foram submetidos a um segundo questionário. Esse questionário, objetivava avaliar o projeto de maneira geral, mas priorizando questões que avaliassem se houve ou não aprendizagem significativa com a metodologia adotada e se o uso da Criptografia associada a conteúdos matemáticos despertou nesses estudantes um desejo maoir em buscar se aprofundar na disciplina.

5.1 Análise do Questionário 1

A aplicação do Questionário 1 objetivava investigar a vivência dos estudante em atividades práticas e/ou lúdicas, associadas a resolução de exercícios que abordam conteúdos matemáticos, e verificar o grau de interesse desses estudantes pela matemática, antes da participação no projeto. A Figura 5.2 mostra a análise das respostas dadas pelos alunos ao primeiro item do questionário. Conforme dados apresentados, concluiu-se que nenhum

aluno considerava-se interessado ou muito interessado por matemática, enquanto 45% dos alunos afirmaram ter um interesse muito pequeno pela disciplina.

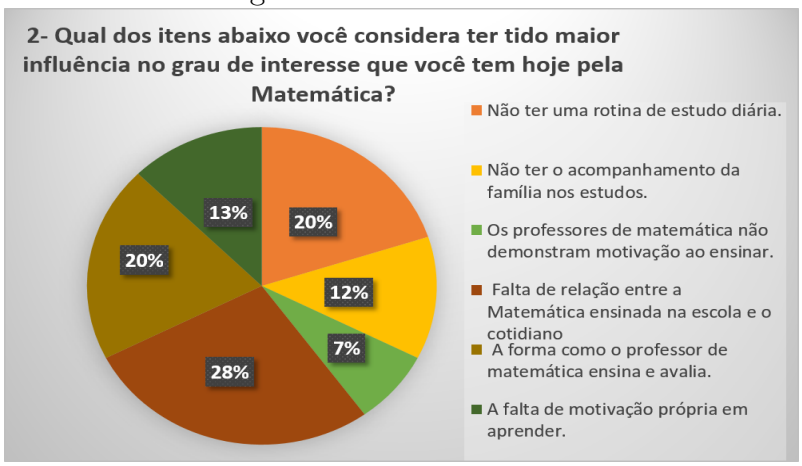
Figura 5.2: Análise do Item 1



Fonte: Dados obtidos na análise do Questionário 1

Por meio da análise do gráfico, mostrado na Figura 5.3, concluiu-se que 28% dos alunos consideraram a falta de relação entre a Matemática ensinada na escola e o cotidiano ser o fator que mais influencia no grau de interesse que eles têm pela disciplina. Em segundo lugar, com 20% cada, os entrevistados afirmaram que não ter uma rotina diária de estudo e a forma como o professor de matemática ensina e avalia são fatores que contribuem para o desinteresse pela disciplina.

Figura 5.3: Análise Item 2

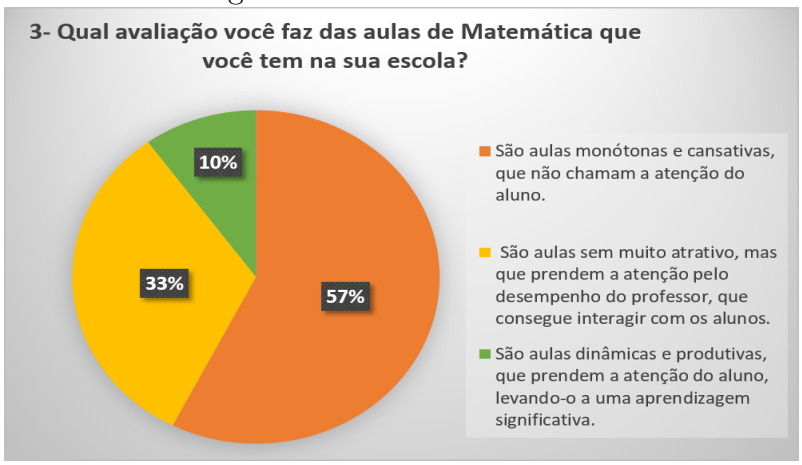


Fonte: Dados obtidos na análise do Questionário 1

O gráfico que analisa o item 3, como visto na Figura 5.4, revelou que, 57% dos alunos entrevistados, consideram suas aulas monótonas e cansativas, não sendo capaz de lhes chamar atenção ou depertar algum interesse pela disciplina. Apenas 10% dos alunos

disseram que suas aulas são diâmicas e produtivas. Essa análise permite concluir que, o grande número de alunos desmotivados em sala de aula, tem influência na metodologia adotada pelos professores de matemática, existindo uma necessidade desses docentes reverem suas práticas.

Figura 5.4: Análise do Item 3



Fonte: Dados obtidos na análise do Questionário 1

O resultado da análise do item 4, mostrado na Figura 5.5, revelou que 72% dos alunos entrevistados nunca realizaram atividades práticas e/ou lúdicas nas aulas de matemática e que 28% afirmou que, às vezes, essas atividades são desenvolvidas em sala de aula. Nenhum aluno afirmou ter aulas práticas frequentemente.

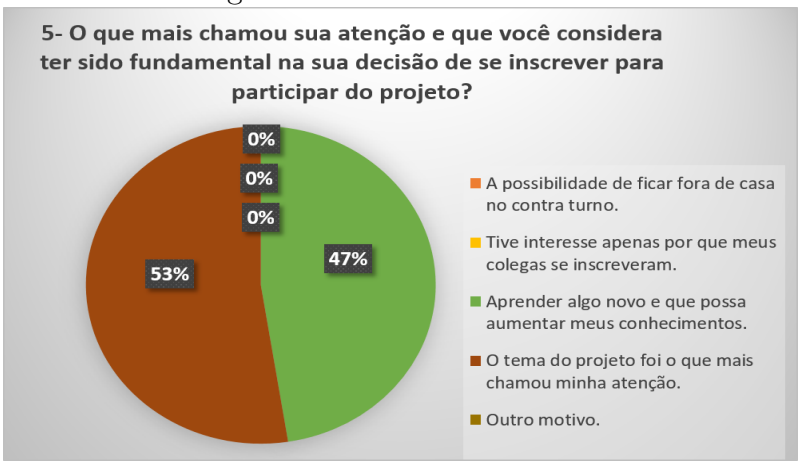
Figura 5.5: Análise do Item 4

Fonte: Dados obtidos na análise do Questionário 1

No último item do questionário, buscava-se avaliar o que mais chamou a atenção, desses alunos, levando-os a se inscreverem para participar do projeto "Desvendando Segredos". Os dados apresentados no gráfico, mostrado na Figura 5.6, revelaram que

53% dos alunos inscreveram-se no projeto por causa do tema, que lhes chamou atenção, despertando-lhes interesse e curiosidade em aprender Criptografia. Ao passo que, 47% dos alunos desejavam aprender algo novo que lhes permitisse aumantar seus conhecimentos. As outras alternativas desse item não foram marcadas por nenhum aluno.

Figura 5.6: Análise do Item 5



Fonte: Dados obtidos na análise do Questionário 1

5.2 Aplicações e Resultados

O objetivo desta seção é apresentar algumas atividades lúdicas que envolvam criptografia e que foram desenvolvidas utilizando-se instrumentos confeccionados com materiais simples, permitindo aos alunos colocar em prática, nessas construções, alguns conteúdos matemáticos previamente estudados. Os conteúdos abordados são trabalhados no Ensino Fundamental (6º ao 9º anos) e no Ensino Médio. As atividades 1, 2, 3 e 5 foram desenvolvidas pela autora deste trabalho e a atividade 4 foi uma aplicação da segunda etapa da prova da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP, do ano de 2007.

5.2.1 Atividade 1: O Segredo da Pirâmide.

Nível: Ensino Fundamental

Conteúdos Matemáticos Relacionados: Sistema de Numeração, Operações com Números Naturais

Recurso: Tabela de Substituição Egípcia

Descrição da atividade: cada aluno recebeu uma Tabela de Substituição Egípcia que

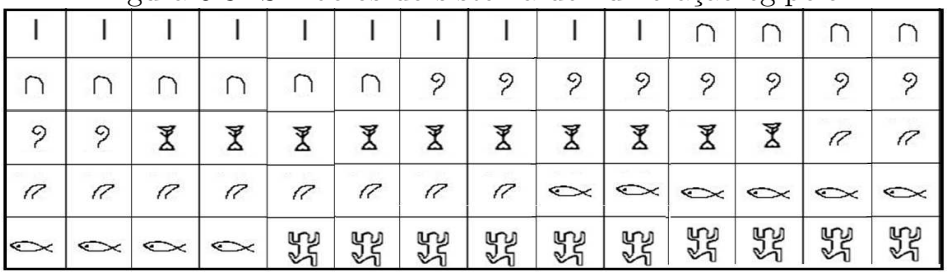
estarava incompleta, como mostra a Figura 5.7. Como primeira atividade, os alunos completaram a tabela substituindo os espaços em branco pelos símbolos do Sistema de Numeração Egípcio, que foram impressos e disponibilizados a eles, segundo modelo da Figura 5.8, os símbolos foram cortados e colados na tabela.

Figura 5.7: Tabela de Substituição Egípcia Incompleta

	1	10	100	1.000	10.000	100.000	1.000.000
0							
1							
2							
3							
4							
5							
6							

Fonte: Próprio Autor (2018)

Figura 5.8: Símbolos do sistema de numeração egípcio.



Fonte: Próprio Autor (2018)

O procedimento a ser usado para preencher a tabela é baseado no princípio da *cifra de Vigenère*, no qual cada linha da tabela é representada por um algarismo, variando de 0 a 6. Esses números indicam a chave criptográfica a ser utilizada para cifrar e decifrar mensagens, e as colunas correspondem aos valores numéricos que cada símbolo egípcio representa, de acordo com a chave que está sendo utilizada.

Na linha indicada pelo algarismo 0, é colocado para cada valor numérico o seu símbolo original, quer dizer, não há mudança no valor dos símbolos com a chave zero. Como mostra a Figura 5.9.

Figura 5.9: Chave zero

	1	10	100	1.000	10.000	100.000	1.000.000
0							

Fonte: Próprio Autor (2018)

A partir da linha 1, os símbolos devem seguir a sequência da linha 0, porém na primeira casa deve-se colocar o símbolo que está uma posição do símbolo original e assim, cada um dos símbolos a serem colocados na sequência sofrerá alteração, de uma posição, em relação a linha 0. Como pulou-se um símbolo ao se colocar o primeiro, o símbolo que sobrou será colocado na última casa completando assim o preenchimento desta linha. A Figura 5.10 mostra essa etapa do processo.

Figura 5.10: Chave 1

	1	10	100	1.000	10.000	100.000	1.000.000
0							
1							

Fonte: Próprio Autor (2018)

O preenchimento das linhas seguintes segue o mesmo raciocínio da linha 1, porém, na linha 2 o aluno pula dois símbolos em relação a linha 0 para colocar o primeiro símbolo. Na linha 3, o estudantes pulará três símbolos , e assim, sucessivamente, até que a tabela esteja completa.

De posse da Tabela de Substituição Egípcia Completa, mostrada na Figura 5.11, os alunos receberam um texto informativo sobre as pirâmides de Gizé e abaixo do texto algumas atividades que foram desenvolvidas com o uso da tabela.

Todos os números que aparecem no texto estão criptografados por símbolos do sistema de numeração egípcia, como mostrado na Figura 5.12, de acordo com uma chave criptográfica escolhida pelo autor. Essa chave criptogáfica corresponde ao critério usado para codificar as informações e que também serve para decodificá-las. A linha indicada pelo algarismo 0 mostra que cada símbolo está relacionado ao seu valor original. A linha indicada pelo algarismo 1, corresponde a chave 1, no qual pulou-se uma posição em relação aos símbolos da posição original, passando cada símbolo a assumir novos valores. A linha

Figura 5.11: Tabela de Substituição Egípcia Completa

	1	10	100	1.000	10.000	100.000	1.000.000
0							
1							
2							
3							
4							
5							
6							

Fonte: Próprio Autor (2018)

indicada pelo algarismo 2, corresponde a chave 2, pulando-se duas posições em relação a posição original e assim sucessivamente, até a última linha da tabela.

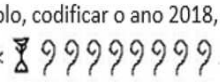
Figura 5.12: Texto: As pirâmides de Gisé

"As pirâmides de Gizé estão localizadas na cidade de Gizé, que integra o Cairo, no Egito. Elas são as únicas das antigas maravilhas que sobreviveram ao tempo. São pirâmides. Cada uma serviu de tumba para um dos faraós Quéops, Quéfren e Miquerinos. A maior das pirâmides é a do faraó Quéops com metros de altura, e cobre, aproximadamente, metros quadrados de superfície. Ela é conhecida como a "Grande Pirâmide". Acredita-se que mais de homens, na maioria escravos, foram utilizados para a construção da pirâmide de Quéops. Levou, aproximadamente, anos para ser finalizada. Nelas está escondido um segredo guardado a mais de anos. Vamos tentar descobrir?"

Fonte: Próprio Autor (2018)

Logo após o texto sobre as pirâmides de Gisé, segue um texto complementar, mostrado na Figura 5.13, que serviu para explicar aos alunos de que modo foi feita a substituição dos números pelos símbolos para, então, desenvolver o restante da atividade. Em seguida, os alunos resolveram três itens elaborados com informações do texto sobre as pirâmide e auxiliados pela tabela de substituição egípcia. Ao ler o texto, mostrado na Figura 5.14, esperava-se que o aluno percebesse que como foram citados o nome de três faraós, Queóps, Quéfren e Miquerinos, e mencionado que cada pirâmide serve como tumba para cada um deles, o primeiro número a ser decifrado, que está sendo representado pelo símbolo , e se refere à quantidade de pirâmides, é o número três. Caso os alunos

Figura 5.13: Texto Complementar

Os números do texto acima foram substituídos por símbolos do sistema de numeração egípcia, usando-se um método antigo e mundialmente conhecido por criptografia, no qual cada letra ou número da palavra original é substituído por outra letra, número ou símbolo a partir de um critério preestabelecido. Nesse caso, usou-se uma tabela de substituição egípcia na qual a linha indicada pelo algarismo 0 representa a posição original de cada símbolo e cada uma das outras linhas representa uma posição alterada em relação a original. A chave 1 indica que pulou-se uma posição. A chave 2 designa que pulou-se duas posições e assim sucessivamente. Portanto, as possíveis chaves a serem utilizadas para codificar o texto acima variam de 1 a 6. Por exemplo, codificar o ano 2018, no sistema de numeração egípcia, usando a chave 2, é escrever 

Fonte: Próprio Autor (2018)

Figura 5.14: Item A - Atividade 1

No texto sobre as pirâmides, um dos números codificados pode ser facilmente desvendado a partir de informações contidas no próprio texto. Ele que o levará a descobrir qual foi a chave criptográfica usada para codificar todos os outros números. Diga que número é esse e qual foi a chave criptográfica usada para cifrar as informações do texto.

Se você já leu o texto, várias vezes, e não conseguiu descobrir peça uma dica ao seu professor, mas é só uma dica! Vamos lá, agora você consegue!

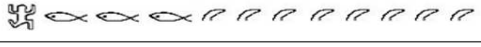
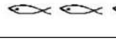
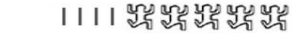
Fonte: Próprio Autor (2018)

tivessem dificuldade em perceber sozinhos essa informação, o professor poderia dizer ao aluno, como uma dica, que a quantidade de pirâmides é a quantidade de faraós.

Sabendo que a quantidade de pirâmides é 3 o aluno procura na tabela em qual linha o símbolo  , está representando a unidade. Assim ele decobre que a chave usada para codificar os números do texto é 4.

Figura 5.15: Item B - Atividade 1

b) Use a chave que você descobriu no item anterior para descobrir todos os números que estão codificados na mensagem. Complete a tabela colocando seus respectivos valores.

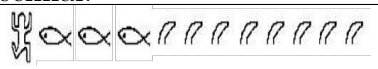
	
	
	
	
	
	

Fonte: Próprio Autor (2018)

Sabendo que a chave criptográfica é 4, o aluno buscava na linha indicada pelo

algarismo 4, da tabela de substituição egípcia, o valor correspondente a cada símbolo para essa chave. Como o pré-requisito para o desenvolvimento dessa atividade, o Sistema de Numeração Egípcio deve ser de conhecimento dos alunos, pois esse sistema é baseado no princípio aditivo do valor numérico, associado a cada símbolo. Contudo, essa informação foi repassada aos alunos na forma de lembrete. Sendo assim, no desenvolvimento do item B, mostrado na Figura 5.15 e Tabela 5.1, os alunos somaram os valores de cada símbolo e assim obtiveram um número que pertencente ao Sistema de Numeração Indo-Arábico.

Tabela 5.1: Substituição dos símbolos egípcios por números do sistema de numeração decimal.

	$100+10+10+10+1+1+1+1+1+1+1+1$	138

O item C, mostrado na Figura 5.16, último item da atividade, pedia que o aluno fizessem uso livre da tabela de substituição egípcia escolhendo uma chave de sua preferência e criptografando algumas informações pessoais.

Figura 5.16: Item C- Atividade 1

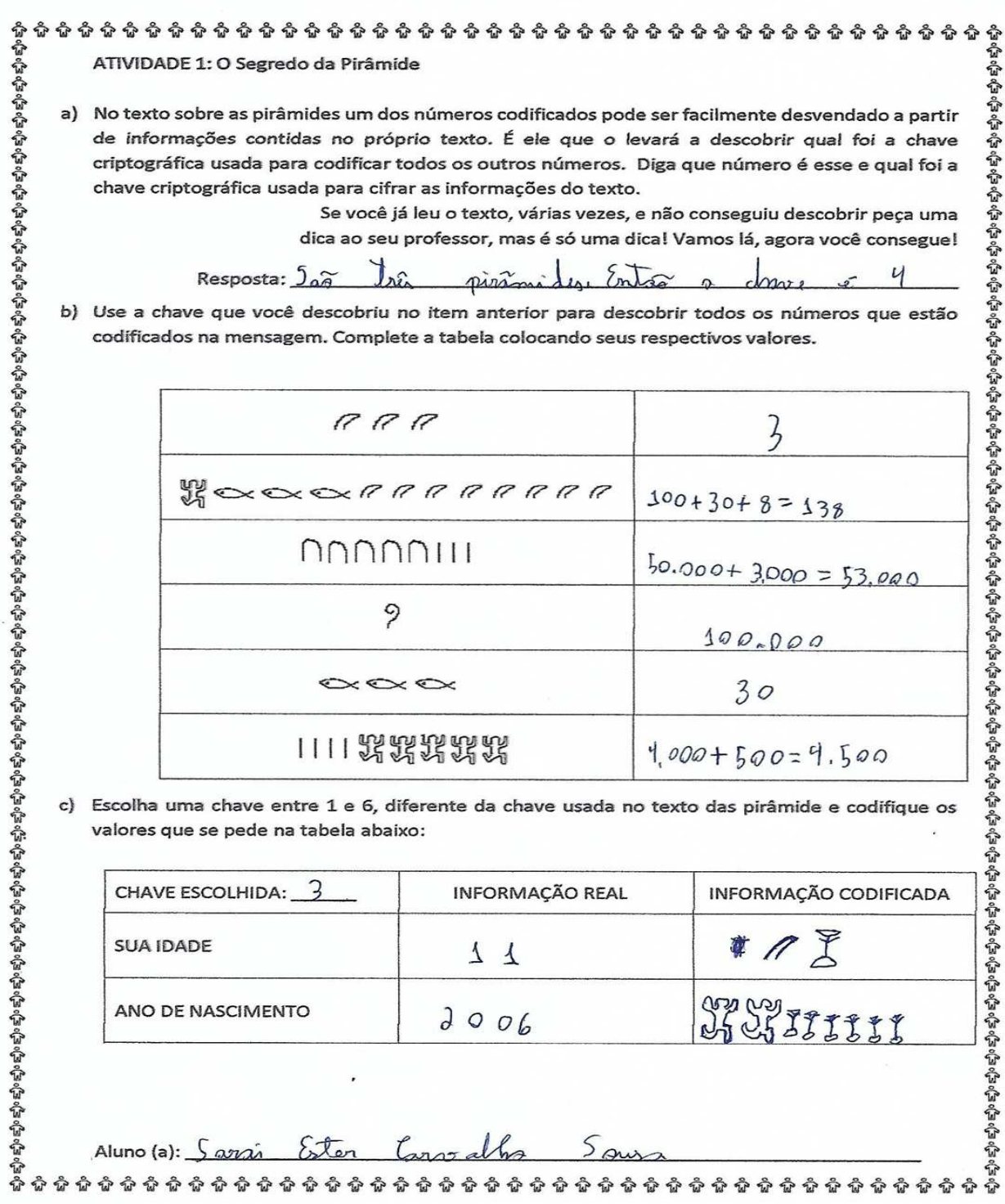
Escolha uma chave entre 1 e 6, diferente da chave usada no texto das pirâmide, e codifique os valores que se pede na tabela abaixo:

CHAVE ESCOLHIDA: _____	INFORMAÇÃO REAL	INFORMAÇÃO CODIFICADA
SUA IDADE		
ANO DE NASCIMENTO		

Fonte: Próprio Autor (2018)

A Figura 5.17 mostra a atividade, O Segredo da Pirâmide, desenvolvida por uma aluna do 6º ano, participante do projeto "Desvendando Segredos".

Figura 5.17: Atividade 1: O Segredo da Pirâmide.



ATIVIDADE 1: O Segredo da Pirâmide

a) No texto sobre as pirâmides um dos números codificados pode ser facilmente desvendado a partir de informações contidas no próprio texto. É ele que o levará a descobrir qual foi a chave criptográfica usada para codificar todos os outros números. Diga que número é esse e qual foi a chave criptográfica usada para cifrar as informações do texto.

Se você já leu o texto, várias vezes, e não conseguiu descobrir peça uma dica ao seu professor, mas é só uma dica! Vamos lá, agora você consegue!

Resposta: São três pirâmides. Então a chave é 4

b) Use a chave que você descobriu no item anterior para descobrir todos os números que estão codificados na mensagem. Complete a tabela colocando seus respectivos valores.

	3
	100+30+8=138
	50.000+3.000=53.000
	100.000
	30
	4.000+500=4.500

c) Escolha uma chave entre 1 e 6, diferente da chave usada no texto das pirâmide e codifique os valores que se pede na tabela abaixo:

CHAVE ESCOLHIDA: 3	INFORMAÇÃO REAL	INFORMAÇÃO CODIFICADA
SUA IDADE	11	
ANO DE NASCIMENTO	2006	

Aluno (a): Sarai Ester Carvalho Sousa

Fonte: Próprio Autor (2018)

5.2.2 Atividade 2: Quem quer ser o Imperador?

Nível: Ensino Fundamental

Conteúdo Matemático Relacionado: Conjuntos, Relações

Recurso: CD Criptográfico

Figura 5.18: CD Criptográfico

Fonte: Próprio Autor (2018)

O CD Criptográfico, mostrado na Figura 5.18, é um recurso adaptado do livro Aprendendo Criptologia de Forma Divertida, dos autores Bezerra, Malagutti e Rodrigues.

Esse recurso auxilia os alunos na cifragem e decifragem de mensagens usando a substituição monoalfabética a partir do código de César. De acordo com esse código, cada letra do alfabeto é substituída por outra que esteja a uma determinada posição depois dela. A quantidade de posições que se pula corresponde à chave criptográfica do código. Por exemplo, ao usar a chave 3, deve-se trocar cada letra do alfabeto pela que está a 3 posições depois dela. Dessa forma, o A será substituido pelo D, o B pelo E, o C pelo F e assim sucessivamente. Nesse processo, tem-se 25 possibilidades de chaves distintas e, quanto maior o valor da chave, mais lento e trabalhoso se torna esse método. Com o CD Criptográfico, a substituição é mais simples e ágil.

Para confeccionar o CD Criptográfico, utiliza-se um cd, novo ou usado, a capa do cd e dois círculos que contém as letras do alfabeto. Um círculo é fixo e colado na parte

externa da capa do cd. O outro círculo é móvel e colado no próprio cd, como mostra a Figura 5.19.

Figura 5.19: Composição do CD Criptográfico

Fonte: Próprio Autor (2018)

Se os dois círculos estiverem com as letras correspondentes alinhadas, A com A, B com B, ..., Z com Z, a chave cripográfica é zero e portanto não há substituição de letras, logo, não há cifragem ou decifragem de mensagem. Ao girar a parte interna do CD, uma posição, ou seja, A com B, B com C, C com D, como mostrado na Figura 5.20, a chave criptográfica é 1 e as letras da mensagem original, que correspondem às letras do círculo da capa do cd, deverão ser substituídas pelas letras que estão indicadas no círculo interno do cd, dando origem a uma nova palavra que estará criptografada.

Figura 5.20: CD Criptográfico na Chave 1

Fonte: Próprio Autor (2018)

Descrição da atividade: os alunos deverão ser divididos em duplas, no qual cada integrante da dupla receberá uma mensagem, entregue pelo professor, e que deverá ser de conhecimento exclusivo de quem a recebeu. Ou seja, um integrante da dupla não pode ter conhecimento da mensagem do outro.

Com o auxílio do CD criptográfico, e utilizando os princípios da cifra de César, cada aluno deverá criar sua chave criptográfica e, a partir dela, cifrar a mensagem recebida. Após a cifragem, os alunos passarão a mensagem para o outro colega da dupla, sem informar qual foi a chave que ele utilizou.

O aluno da dupla que conseguir identificar a chave criada pelo colega e decifrar a mensagem primeiro, será o Imperador.

Caso ainda tenha tempo, o professor poderá prosseguir com a atividade formando novas duplas com os alunos vencedores da primeira rodada e repetindo o processo, utilizando novas mensagens, até que sobre apenas uma dupla e se tenha um único Imperador na sala.

As Figuras 5.21, 5.22 e 5.23, mostram duas das atividades desenvolvidas, pelos alunos, durante o projeto "Desvendando Segredos".

Figura 5.21: Atividade "Quem quer ser o Imperador?" - Dupla 1

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

ATIVIDADE 1: Quem quer ser o Imperador?

Utilizando os princípios da Cifra de César, crie uma chave criptográfica e a partir dela cifre a frase abaixo:

"SER OU NÃO SER EIS A QUESTÃO!"

CHAVE: 20

MENSAGEM CIFRADA: MyL iO HUi MyL ycM U KOyMNUi

Aluno (a): Damaris Adrielly Cruz Costa

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

ATIVIDADE 2: Quem quer ser o Imperador?

Descubra qual foi a chave utilizada por seu colega para cifrar a frase e depois decifre a mensagem escrevendo a frase original.

MENSAGEM CIFRADA: MyL iO HUi MyL ycM U KOyMNUi

CHAVE: 20

MENSAGEM DECIFRADA: SER OU NÃO SER EiS A Questão

Atividade desenvolvida por:

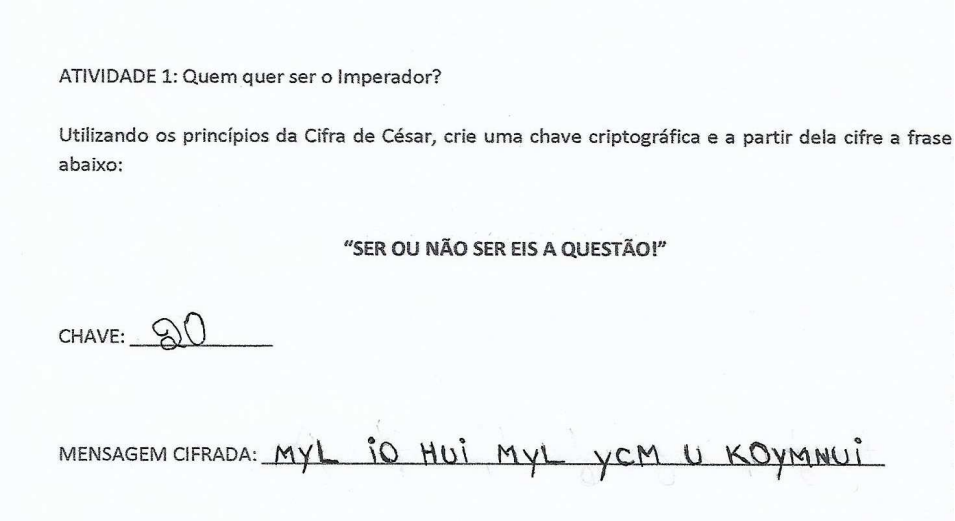
Aluno (a): Bruno Eduardo

A mensagem decifrada nesta atividade foi cifrada na atividade 1 por:

Aluno (a): Damaris Adrielly Cruz Costa

Fonte: Próprio Autor (2018)

Figura 5.22: Atividade 1 - Dupla 1



ATIVIDADE 1: Quem quer ser o Imperador?

Utilizando os princípios da Cifra de César, crie uma chave criptográfica e a partir dela cifre a frase abaixo:

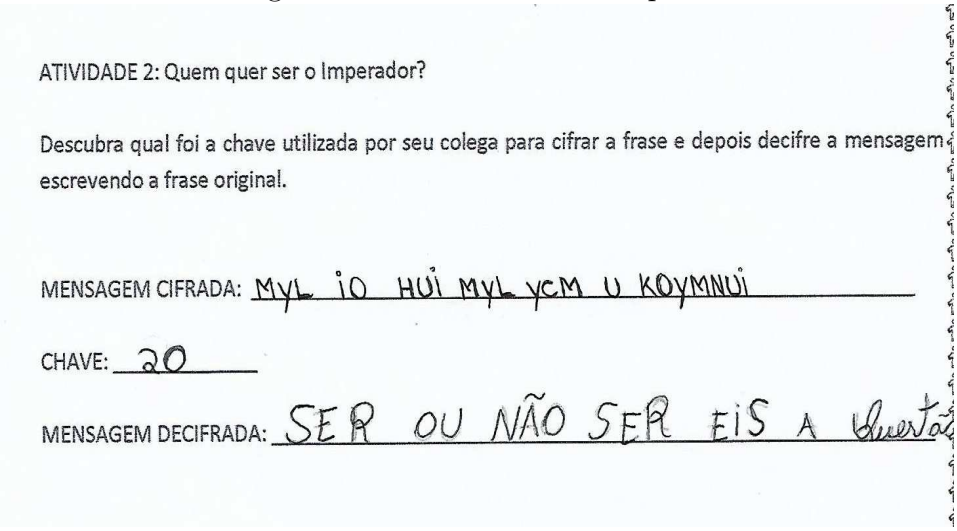
"SER OU NÃO SER EIS A QUESTÃO!"

CHAVE: 20

MENSAGEM CIFRADA: MyL iO HUi MyL ycM U KOyMNUi

Fonte: Próprio Autor (2018)

Figura 5.23: Atividade 2 - Dupla 1



ATIVIDADE 2: Quem quer ser o Imperador?

Descubra qual foi a chave utilizada por seu colega para cifrar a frase e depois decifre a mensagem escrevendo a frase original.

MENSAGEM CIFRADA: MyL iO HUi MyL ycM U KOyMNUi

CHAVE: 20

MENSAGEM DECIFRADA: SER OU NÃO SER EIS A Questão

Fonte: Próprio Autor (2018)

Resultados observados: a atividade foi muito bem recebida pelos estudantes que imediatamente formaram suas duplas e iniciaram os trabalhos. O silêncio que tomou a sala vez ou outra era quebrado por comentários do tipo: "Eu vou ser o Imperador!", "Ninguém vai me vencer, sou o mais rápido!"ou "Quer aprender a decifrar? Deixa que eu te ensino!". Daí surgiam muitos risos sendo, às vezes, necessária a intervenção da professora para a retomada do silêncio e o prosseguimento dos trabalhos, o que demonstrando o entusiasmo e o interesse gerado nos estudantes, durante a produção da atividade.

A maioria dos alunos demonstrou muita habilidade no manuseio do CD Criptográfico, conseguindo, rapidamente, cifrar a mensagem recebida. No entanto, alguns

alunos precisaram de auxílio para entender o seu funcionamento e concluir a atividade.

O aluno mais rápido cifrou a mensagem em, aproximadamente, 5 minutos, sendo o tempo médio para concluir a cifragem da mensagem de, aproximadamente, 10 minutos. Dessa média, foi excluída uma amostra, correspondente a uma aluna do 6º ano, que levou 40 minutos, aproximadamente, para concluir sua atividade. Ela ficou muito nervosa ao perceber que os colegas estavam terminando e ela estava tendo dificuldades, parando várias vezes o trabalho e retomando, apenas, quando era auxiliada e estimulada a concluir pela professora e pelos colegas.

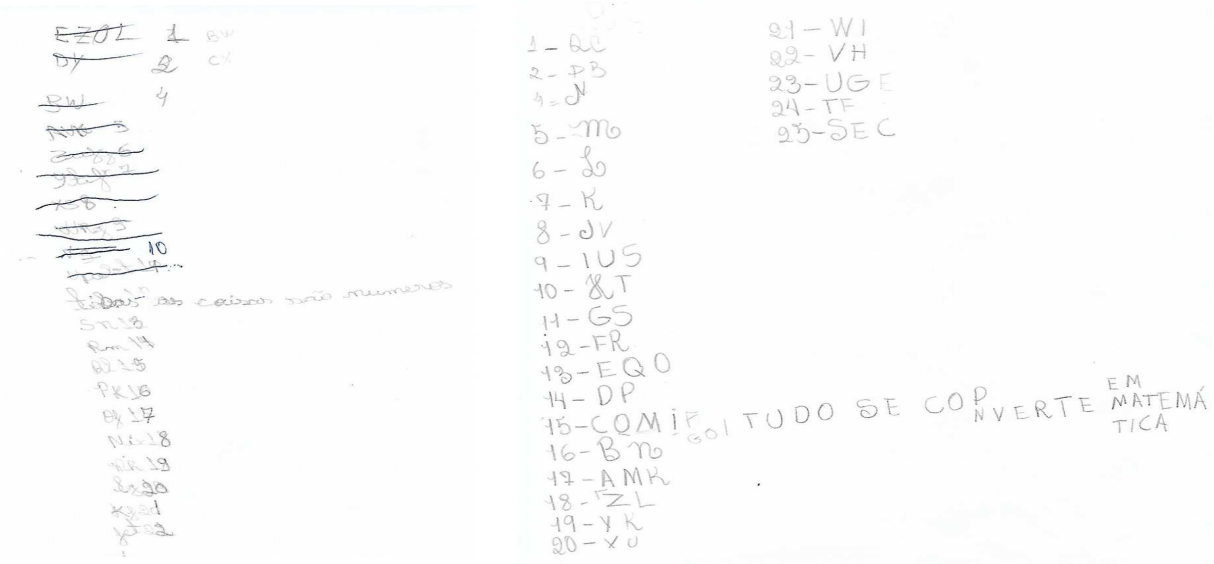
Ao concluir a primeira etapa dessa atividade, que era escolher uma chave criptográfica, a seu critério, e cifrar a mensagem recebida com a chave escolhida os alunos receberam uma outra folha de papel, que continha um espaço a ser preenchido pela sua mensagem codificada. Essa folha deveria ser ser entregue ao outro colega, a fim de que ele tentasse descobrir a chave usada e deifrasse a mensagem, lendo para seu colega a mensagem original.

Durante a segunda etapa da atividade, observou-se que a maior dificuldade enfrentada pelos alunos foi descobrir a chave escolhida pelo colega. A professora precisou intervir e explicar que o método para chegar à chave era o da tentativa e erro, também conhecido como **ataque por força bruta**. Sendo assim, eles deveriam tentar usar cada uma das possíveis chaves até que encontrassem uma tradução intelegível do texto cifrado para o texto original. Essa etapa poderia ser extremamente demorada, caso os alunos não percebessem, imediatamente, que uma determinada chave não era possível, decindindo então tentar outra chave. Porém, foi observado que os alunos criaram suas estratégias e à medida que percebiam que a palavra não fazia sentidio, descartavam aquela chave e tentavam uma outra, como mostrado na Figura 5.24.

Com isso, a segunda etapa da atividade foi a mais demorada, devido à quantidade de possibilidades para se descobrir a chave, levando, em média, 30 minuntos para que todos os alunos concluissem os trabalhos. O aluno mais rápido levou 18 minutos para encontrar a chave e decifrar a mensagem, recebendo assim o título de Imperador.

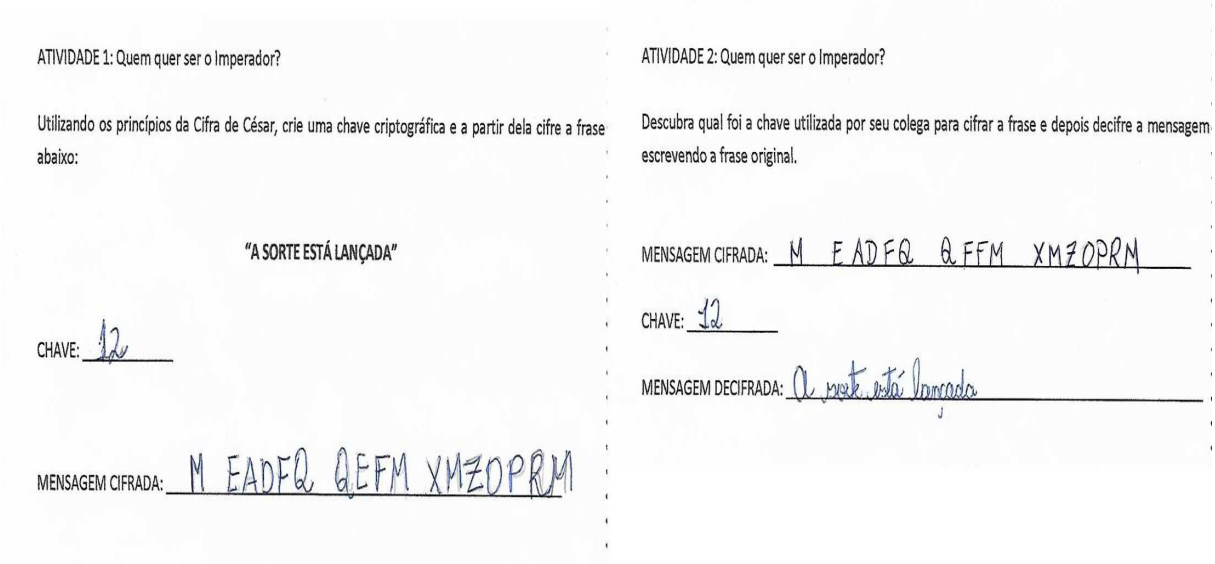
A dupla, da qual fazia parte a aluna do 6º ano que ficou nervosa, foi excluída do cálculo do tempo médio.

Figura 5.24: Rascunhos: Tentativa e Erro



Fonte: Próprio Autor (2018)

Figura 5.25: Atividade "Quem quer ser o Imperador?- Dupla 2



Fonte: Próprio Autor (2018)

5.2.3 Atividade 3: A chave é o mistério.

Nível: Ensino Fundamental

Conteúdos Matemáticos Relacionados: Conjuntos Numéricos/Expressões Numéricas

Recurso: Régua deslizante

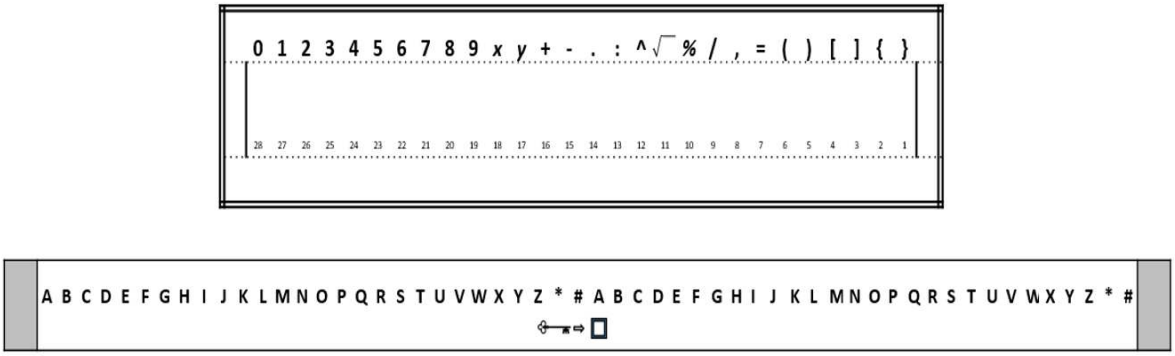
A régua deslizante é um recurso adaptado do livro Aprendendo Criptologia de Forma Divertida, dos autores Bezerra, Malagutti e Rodrigues.

Esse recurso auxilia os alunos na cifragem e decifragem de mensagens usando a substtuição monoalfabética. Contudo as informações a serem codificadas devem estar na forma de uma expressão matemática, que será transformada em uma sequência alfabética.

Na régua, cada letra do alfabeto está associada a um número ou a um símbolo matemático.Dessa forma, pode-se transformar expressões numéricas, expressões algébricas, polinômios ou equações em uma mensagem criptografada.

A régua é composta de uma parte fixa, que contém os símbolos matemáticos, e uma parte móvel, que contém as letras, como mostrado na Figura 5.26.

Figura 5.26: Régua deslizante



Fonte: Próprio Autor (2018)

Na parte móvel, logo abaixo da segunda letra A da régua, encontra-se um espaço vazado no qual será visualizada a chave criptográfica, que corresponde a um número variando de 1 a 28, e que será utilizada na cifragem ou decifragem da mensagem. Assim, ao ser determinada a chave criptográfica o aluno deverá deslizar a parte móvel sobre a parte fixa da régua até que a chave escolhida aprareça no local indicado pelo desenho da chave. Dessa forma, o aluno poderá iniciar o processo de criptografia.

Dois dos símbolos contidos na parte fixa da régua devem previamente ser explicados aos alunos antes do início das atividade. O primeiro é o acento circunflexo ($\wedge$), que nesse caso, representa uma potência. Logo, se esse símbolo aparecer antes de um número qualquer, indicará que o aluno tem que resolver um potência com aquele expoente. O outro símbolo é a barra inclinada ($/$) que corresponde a barra de fração. Na parte móvel, foram acrescentados dois símbolos, o asterísco ($*$) e o jogo da velha ($\#$), para que assim pudesse coincidir a quantidade de símbolos na parte fixa com a quantidade de símbolos na parte móvel.

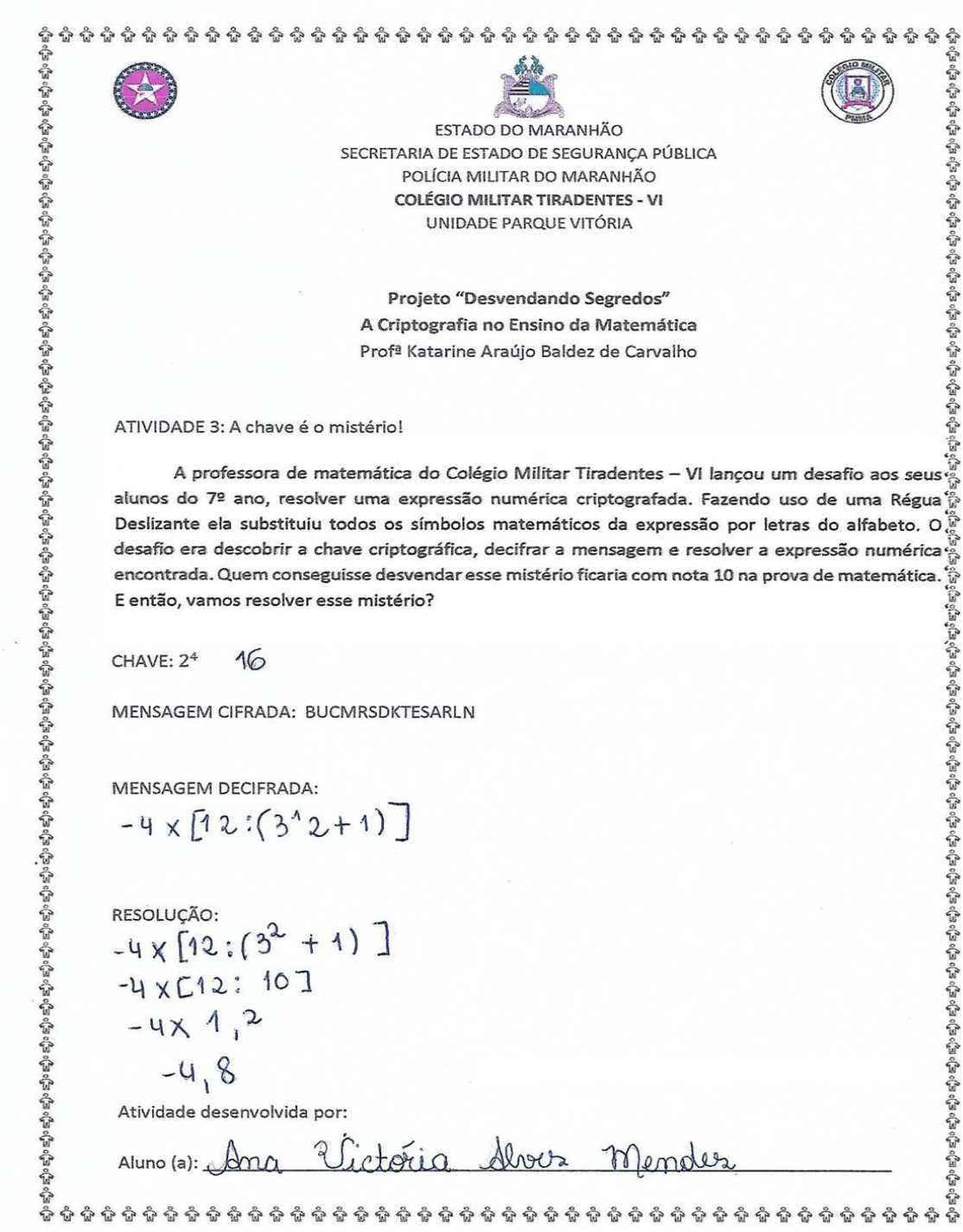
Descrição da atividade: cada aluno terá em seu poder uma régua numérica deslizante. O professor entregará aos alunos uma expressão matemática cifrada e uma chave que também estará cifrada. A chave consiste em uma operação fundamental simples que não contenha mais de uma operação e que resulte em um número natural entre 1 e 28.

O primeiro desafio dos alunos será desvendar a chave criptográfica. Depois, de posse da chave, decifrar a mensagem ou a expressão matemática e resolvê-la. A Figura 5.27, mostra uma das atividades desenvolvidas pelos alunos, durante o projeto "Desvendando Segredos".

Resultados observados: como primeira etapa da atividade, os alunos deveríam encontrar a chave criptográfica, que nessa atividade foi representada por uma potência simples. Todos os alunos conseguiram resolver com muita facilidade essa etapa. De posse da chave, e fazendo uso da régua deslizante, os alunos começaram a decifrar a mensagem. Esse processo foi estável e todos os alunos conseguiram encontrar a expressão numérica procurada.

A maior dificuldade enfrentada, por um pequeno número de alunos, ocorreu durante a solução da expressão matemática. Alguns demonstraram dúvidas nas operações e apenas um aluno precisou de um auxílio mais contundente da professora para que conseguisse resolver a atividade.

Figura 5.27: Atividade 3- A chave é o mistério



ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

ATIVIDADE 3: A chave é o mistério!

A professora de matemática do Colégio Militar Tiradentes – VI lançou um desafio aos seus alunos do 7º ano, resolver uma expressão numérica criptografada. Fazendo uso de uma Régua Deslizante ela substituiu todos os símbolos matemáticos da expressão por letras do alfabeto. O desafio era descobrir a chave criptográfica, decifrar a mensagem e resolver a expressão numérica encontrada. Quem conseguisse desvendar esse mistério ficaria com nota 10 na prova de matemática. E então, vamos resolver esse mistério?

CHAVE: 2^4 16

MENSAGEM CIFRADA: BUCMRSDKTESARLN

MENSAGEM DECIFRADA:

$-4 \times [12 : (3^2 + 1)]$

RESOLUÇÃO:

$-4 \times [12 : (3^2 + 1)]$
$-4 \times [12 : 10]$
$-4 \times 1,2$
$-4,8$

Atividade desenvolvida por:

Aluno (a): Ana Victória Alves Mendes

Fonte: Próprio Autor (2018)

5.2.4 Atividade 4: Questão da OBMEP 2007.

Nível: Ensino Fundamental

Conteúdos Matemáticos Relacionados: Conjuntos/Relações/Função

Recurso: Disco Giratório

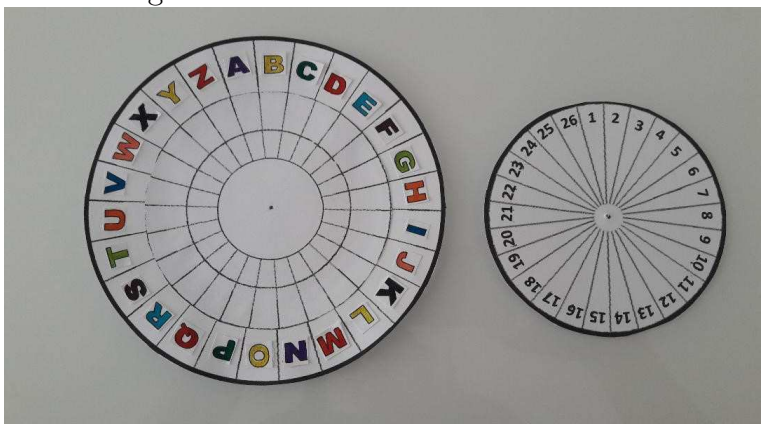
Figura 5.28: Disco Giratório

Fonte: Próprio Autor (2018)

O Disco Giratório, mostrado na Figura 5.28, é um recurso que auxilia os alunos na cifragem e decifragem de mensagens usando a substtuição monoalfabética e usando como princípio de funcionamento o código de César. O disco é composto por uma sobreposição de dois círculos de diâmetros diferentes.

O círculo maior contém as 26 letras do alfabeto, localizadas próximo a sua borda, e que correspondem às letras da mensagem que será criptografada. No círculo menor, estão distribuídos 26 números, variando de 1 a 26, que são usados como substitutos das letras na mensagem cifrada, como mostrado na Figura 5.29.

Figura 5.29: Partes do Disco Giratório



Fonte: Próprio Autor (2018)

No Disco Giratório, cada uma das 26 letras do alfabeto é associada à um número, que varia de 1 a 26. A chave criptográfica é o número que está associado à letra A. Ao posicionar o disco menor na chave 1, a correspondência letra e número é a mostrada na Tabela 5.2.

Tabela 5.2: Correspondência letra e número - Atividade 4

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

Portanto, à medida que se altera a chave criptográfica, utilizada para cifrar ou decifrara uma mensagem, a associção letra e número sofrerá uma nova ordenação. De modo que, se a chave usada é 3, a letra A será substituída pelo número 3, a letra B pelo número 4, a letra C pelo número 5, e assim, sucessivamente, como mostra a Figura 5.30.

Figura 5.30: Disco Giratório na chave 3

Fonte: Próprio Autor (2018)

Descrição da atividade:

essa atividade refere-se a uma questão que foi aplicada na segunda etapa da Olimpíada Brasileira de Matemática das Escolas Públicas - OBMEP, no ano de 2007, e que foi incluída nesse trabalho com o objetivo de avaliar o desempenho dos alunos participantes da pesquisa em duas situações distintas.

A primeira foi uma simulação da participação de um grupo de 10 alunos, cinco alunos do 8º ano e cinco alunos do 9º ano, na segunda etapa da OBMEP. Nesse etapa, os alunos tiveram que desenvolver a questão sem o auxílio de nehum tipo de recurso. Ao mesmo tempo, um outro grupo de 10 alunos, cinco alunos do 8º ano e cinco alunos do

9º ano, desenvolveram a mesma questão, porém esse grupo fez uso do Disco Giratório. O dico foi empregado na questão aplicada pela OBMEP apenas como ilustração, como mostra a Figura 5.31.

As informações dos dois grupos foram anotadas para que fosse feita a análise dos resultados posteriormente, buscando-se verificar se uso do recurso contribuiu ou não para um melhor desempenho desses alunos.

MODELO QUESTÃO OBMEP - 2007

Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda a letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado, a chave é 5 e a palavra *PAI* é codificada 20-5-13.

(a) Usando a chave indicada na figura, descubra qual a palavra foi codificada como 23-25-7-25-22-13.

(b) Codifique OBMEP usando a chave 20.

(c) Chicó codificou uma paravra de 4 letras com a chave 20, mas esqueceu-se de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

(d) Em uma outra chave, a soma dos números que representam as letras A, B, e C é 52. Qual é essa chave?

Figura 5.31: Ilustração do Disco Giratório usado na OBMEP - 2007

Fonte: (OBMEP - 2007)

Resultados observados: a realização dessa atividade tinha como principal objetivo avaliar se o uso do recurso tem infuência ou não em um melhor desempenho dos alunos no desenvolvimento da atividade. Alguns quesitos importantes, observados durante e depois da realização da tarefa, foram listados abaixo:

1. O grupo que fez a atividade sem o uso do recurso aparentava estar tenso e preocupado comparado com o grupo que usou o recurso, que parecia bem mais tranquilo.

2. 60% dos alunos, do grupo que fez a atividade sem o recurso, deixou de responder pelo menos uma das quatro questões da atividade. Por outro lado, do grupo que usou o recurso, apenas 20% deixou alguma das questões em branco.

3. Do grupo que não usou o recurso na atividade, o aluno mais rápido terminou a tarefa com um tempo de 17 minutos e 32 segundos. Por sua vez, o aluno mais rápido do grupo, que usou o recurso, terminou a atividade com 8 minutos e 03 segundos.

Os dados relativos ao desempenho de cada grupo em relação aos quatro itens da atividade estão dispostos na Tabela 5.3.

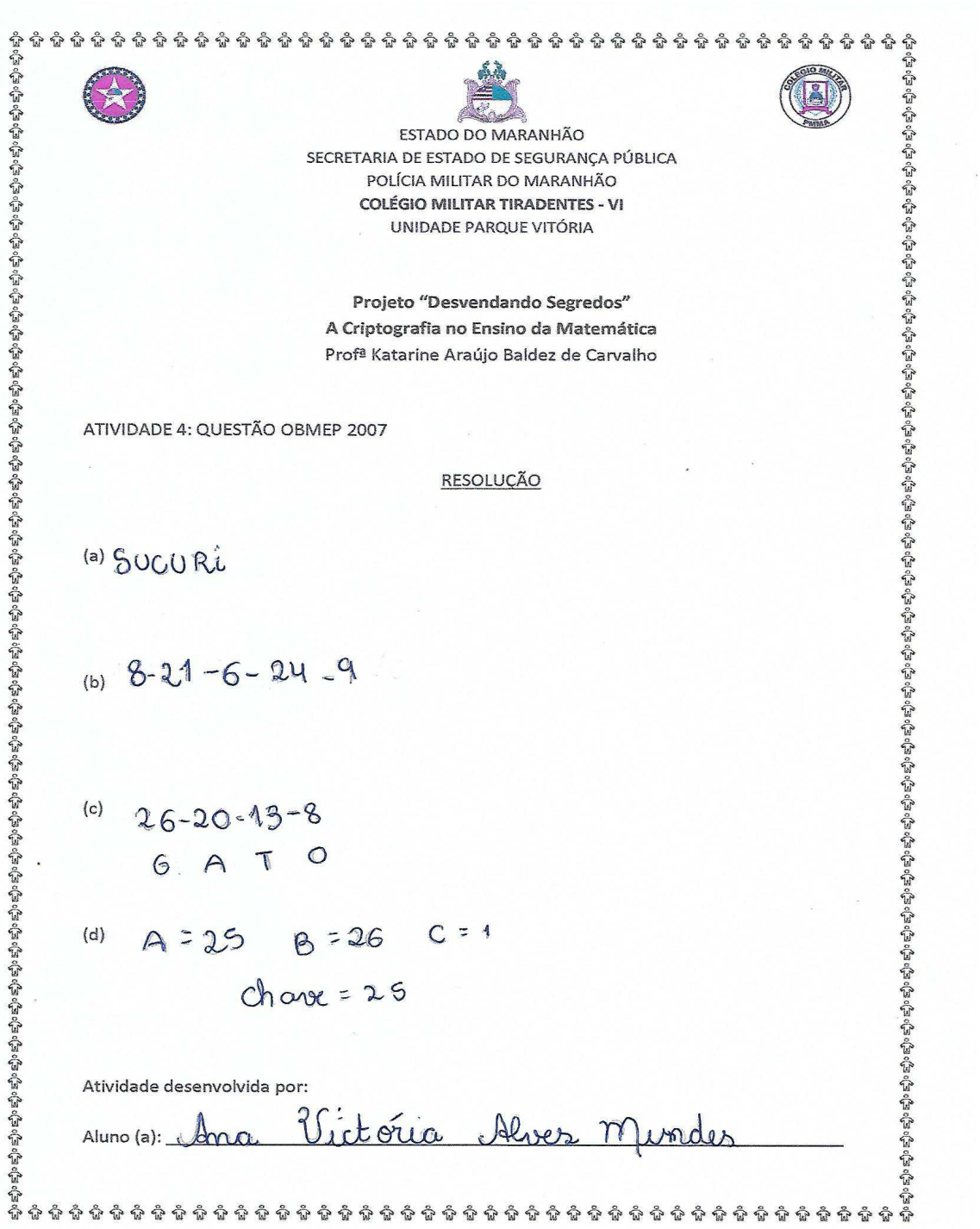
Tabela 5.3: Desempenho dos grupos por item da atividade 4.

	Grupo sem recurso		Grupo com recurso	
	% Acertos	% Erros	% Acertos	% Erros
Item A	100	0	100	0
Item B	70	30	100	0
Item C	70	30	100	0
Item D	40	60	80	20

De acordo com os dados obtidos, conclui-se que o uso do recurso na realização dessa atividade apontou resultado satisfatório em relação ao desempenho dos alunos, comparado ao grupo que não fez uso do recurso.

Em questionamentos feitos aos alunos do grupo que não fez uso de recurso, constatou-se que a principal causa de alguns alunos não terem conseguido resolver todos os itens da atividade foi a dificuldade em entender o funcionamento do disco somente através da ilustração. Assim, mesmo tendo sido informado no enunciado da questão, alguns alunos não conseguiram perceber que a chave criptográfica correspondia ao valor numérico que estava associado à letra A. De modo que, sem esse entendimento, esses alunos não resolveram os itens b, c e d da atividade. A Figura 5.32, mostra uma das atividades desenvolvidas por uma aluna do 8º ano que fez uso do Disco Giratório.

Figura 5.32: Atividade 4 - Desenvolvida por uma aluna do 8º ano com uso do recurso.



ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

ATIVIDADE 4: QUESTÃO OBMEP 2007

RESOLUÇÃO

(a) SUCURI

(b) 8-21-6-24-9

(c) 26-20-13-8
G A T O

(d) A = 25 B = 26 C = 1
Chave = 25

Atividade desenvolvida por:

Aluno (a): Ana Victória Alves Mendes

Fonte: Próprio Autor (2018)

5.2.5 Atividade 5: Minha função é descobrir!

Nível: Ensino Médio

Conteúdo Matemático Relacionado: Funções

Desenvolvimento da atividade

A atividade proposta foi desenvolvida por alunos do 9º ano, que ainda não haviam estudado o conteúdo de Função, em virtude do projeto ter sido desenvolvido no início do ano letivo. Portanto, foi necessário, primeiramente, trabalhar este conteúdo com os alunos participantes do projeto, antes da realização da atividade.

Por se tratar de um conteúdo recém estudado e no intuito de consolidar o seu aprendizado, sem dificultar o entendimento do mesmo, optou-se pelo desenvolvimento da atividade com os estudantes sem o uso de congruência.

No entanto, são apresentadas duas opções para essa atividade, com suas respectivas soluções. A primeira opção, sem o uso de congruência, como foi adotada durante o projeto. A segunda opção, fazendo uso de congruência, como sugestão para uma aplicação aos alunos do ensino médio.

Primeira opção - sem uso de congruência:

Descrição da atividade

Arthur desejava enviar uma mensagem para seu amigo Felipe, durante a aula de matemática. Desejando transmitir a mensagem sem que seus colegas de sala tivessem conhecimento do seu conteúdo, Arthur resolveu codificá-la usando uma técnica de criptografia que ele e Felipe conheciam.

Para cifrar (codificar) a mensagem, Arthur usou a função$f(x) = -2x + 13$ que o seu professor havia colocado no quadro e montou a tabela de substituição abaixo, que associa cada letra do alfabeto a um valor numérico de 0 a 25. Para representar o espaço entre as palavras, ele usou o símbolo $\sqcup$ e o associou ao número 26.

Dessa forma, Artur substituiu, na função, o valor de cada letra da mensagem e o resultado obtido era usado para trocar a letra anterior por uma nova letra que corresponderia ao valor encontrado. Responda o que se pede:

(a) A mensagem que Arthur desejava enviar para Felipe era: **"Amanhã não virei para a escola"**. Usando a função $f(x) = -2x + 13$, cifre a mensagem de Arthur. (Para separar um número do outro, na mensagem cifrada, use ponto e vírgula.)

Tabela 5.4: Correspondência letra e número - Atividade 5

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

(b) Determine a função inversa da função $f(x) = -2x + 13$.

(c) Utilizando a função inversa, encontrada no item b, decifre a mensagem abaixo, que foi cifrada por Felipe e enviada para Arthur como resposta ao item a.

Tabela 5.5: Mensagem cifrada

-25	-27	7	-15	-39	11	5	-11	-39	13	-29	-3	-23	13	-21
5	-3	-39	-15	-39	-17	-21	-15	3	5	-23	-23	-15	-21	

Solução:

Item (a): Inicialmente, o aluno verifica na Tabela 5.4 qual é o valor que cada letra da mensagem está associada, observando que, para os espaços entre as palavras, é usado o símbolo ⊔.

Posteriormente, cada um desses valores é substituído na função $f(x) = -2x+13$, a fim de se obter um número, ou seja, a imagem da função. A imagem da função corresponde ao código para aquela letra na mensagem cifrada, como mostrado na Tabela 5.6. Ao final da substituição de todos os valores, tem-se a mensagem cifrada, mostrada na Tabela 5.7.

Tabela 5.6: Codificação da mensagem **AMANHÃ NÃO VIREI PARA A ESCOLA.**

Letra	Sequência Numérica (x)	Cálculo da imagem da função $f(x) = -2x + 13$
A	0	$f(0) = 13$
M	12	$f(12) = -11$
N	13	$f(13) = -13$
H	7	$f(7) = -1$
O	14	$f(14) = -15$
V	21	$f(21) = -29$
I	8	$f(8) = -3$
R	17	$f(17) = -21$
E	4	$f(4) = 5$
P	15	$f(15) = -17$
S	18	$f(18) = -23$
C	2	$f(2) = 9$
L	11	$f(11) = -9$
⊔	26	$f(26) = -39$

Tabela 5.7: Correspondência mensagem original e mensagem cifrada.

Mensagem original	A	M	A	N	H	Ã	⊔	N	Ã	O	⊔	V	I	R	E
Mensagem cifrada	13	−11	13	−13	−1	13	−39	−13	13	−15	−39	−29	−3	−21	5

Mensagem original	I	⊔	P	A	R	A	⊔	A	⊔	E	S	C	O	L	A
Mensagem cifrada	−3	−39	−17	13	−21	13	−39	13	−39	5	−23	9	−15	−9	13

Item (b): Nesse item o aluno deve usar os seus conhecimentos matemáticos para encontrar a função inversa da função $f(x) = -2x + 13$. Essa informação será necessária para dar continuidade ao desenvolvimento da questão, pois é a função inversa que é usada para decifrar a mensagem. Assim como solução tem-se:

$$f(x) = -2x + 13 \Leftrightarrow y = -2x + 13 \Rightarrow$$

$$\Rightarrow x = -2y + 13 \Rightarrow$$

$$\Rightarrow 2y = -x + 13 \Rightarrow$$

$$\Rightarrow y = \frac{-x + 13}{2} \Rightarrow$$

$$\Rightarrow f^{-1} = \frac{-x + 13}{2}.$$

Logo, a função inversa da função $f(x) = -2x + 13$ é a função $f^{-1} = \dfrac{-x + 13}{2}$.

Item (c): Usando a função $f^{-1} = \dfrac{-x + 13}{2}$, encontrada no item b, o aluno substitui cada um dos os valores de x, descritos na Tabela 5.5, para encontrar o seu correspondente f^{-1}, como mostratado na Tabela 5.2.5.

Posteriormente, verifica-se na Tabela 5.4, qual letra está associada àquele valor encontrado.

Ao final da substituição de cada um dos valores da mensagem cifrada, tem-se a mensagem decifrada, como mostra a Tabela 5.2.5.

As Figuras 5.33, 5.34 e 5.35 mostram o desenvolvimento dessa atividade, realizada por um aluno do 9º ano.

Tabela 5.8: Decifrando a mensagem

Valor Numérico (x)	Cálculo da imagem da função $f^{-1}(x)$	Letra correspondente
-25	$f^{-1}(-25) = 199$	T
-27	$f^{-1}(-27) = 20$	U
7	$f^{-1}(7) = 3$	D
-15	$f^{-1}(-15) = 14$	O
-39	$f^{-1}(-39) = 26$	$\sqcup$
11	$f^{-1}(11) = 1$	B
5	$f^{-1}(5) = 4$	E
-11	$f^{-1}(-11) = 12$	M
13	$f^{-1}(13) = 0$	A
-29	$f^{-1}(-29) = 21$	V
-3	$f^{-1}(-3) = 8$	I
-23	$f^{-1}(-23) = 18$	S
-21	$f^{-1}(-21) = 17$	R
-17	$f^{-1}(-17) = 15$	P
3	$f^{-1}(3) = 5$	F

Tabela 5.9: Correspondência entre mensagem cifrada e mensagem decifrada

Mensagem cifrada	-25	-27	7	-15	-39	11	5	-11	-39	13	-29	-3	-23	13	-21
Mensagem decifrada	T	U	D	O	$\sqcup$	B	E	M	$\sqcup$	A	V	I	S	A	R

Mensagem cifrada	5	-3	-39	-15	-39	-17	-21	-15	3	5	-23	-23	-15	-21
Mensagem decifrada	E	I	$\sqcup$	O	$\sqcup$	P	R	O	F	E	S	S	O	R

Segunda opção - com uso de congruência:

Descrição da atividade

Arthur desejava enviar uma mensagem para seu amigo Felipe, durante a aula de matemática. Desejando transmitir a mensagem sem que seus colegas de sala tivessem conhecimento do seu conteúdo, Arthur resolveu codificá-la usando uma técnica de criptografia que ele e Felipe conheciam.

Para cifrar (codificar) a mensagem, Arthur usou a função$f(x) = -2x + 13$ que o seu professor havia colocado no quadro e montou a tabela de substituição abaixo, que associa cada letra do alfabeto a um valor numérico de 0 a 25. Para representar o espaço entre as palavras, ele usou o símbolo $\sqcup$ e o associou ao número 26.

Dessa forma, Artur substituiu, na função, o valor de cada letra da mensagem e o resultado obtido era usado para trocar a letra anterior por uma nova letra que corresponderia ao valor encontrado. Responda o que se pede:

(a) A mensagem que Arthur desejava enviar para Felipe era: **"Amanhã não virei para a escola"**. Usando a função $f(x) = -2x + 13$, cifre a mensagem de Arthur.

Tabela 5.10: Correspondência letra e número - Atividade 5

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

(Para separar um número do outro, na mensagem cifrada, use ponto e vírgula.)

(b) Determine a função inversa da função $f(x) = -2x + 13$.

(c) Utilizando a função inversa, encontrada no item b, decifre a mensagem abaixo, que foi cifrada por Felipe e enviada para Arthur como resposta ao item a.

CAHMPLFQPNZYENGFYPMPKGMDFEEMG

Solução:

Item (a): Primeiramente, verifica-se na Tabela 5.10, a que valor cada letra da mensagem original está associada, observando-se que, para os espaços entre as palavras é usado o símbolo ⊔. Posteriormente, cada um desses valores é substituído na função $f(x) = -2x+13$, a fim de se obter a sua imagem. Aos resultados encontrados, usa-se a congruência módulo 27 e associa-se cada valor a uma letra de acordo com Tabela 5.10, obtendo-se, ao final de todas as substituições, a mensagem cifrada. O processo descrito é mostrado na Tabela 5.11.

Tabela 5.11: Codificação da mensagem **AMANHÃ NÃO VIREI PARA A ESCOLA.**

Letra	Sequência Numérica (x)	Cálculo $f(x) = -2x + 13$	Letra correspondente
A	0	$f(0) = 13 \equiv 13\ (mod 27)$	N
M	12	$f(12) = -11 \equiv 16\ (mod 27)$	Q
N	13	$f(13) = -13 \equiv 14\ (mod 27)$	O
H	7	$f(7) = -1 \equiv 26\ (mod 27)$	⊔
O	14	$f(14) = -15 \equiv 12\ (mod 27)$	M
V	21	$f(21) = -29 \equiv 25\ (mod 27)$	Z
I	8	$f(8) = -3 \equiv 24\ (mod 27)$	Y
R	17	$f(17) = -21 \equiv 6\ (mod 27)$	G
E	4	$f(4) = 5 \equiv 5\ (mod 27)$	F
P	15	$f(15) = -17 \equiv 10\ (mod 27)$	K
S	18	$f(18) = -23 \equiv 4\ (mod 27)$	E
C	2	$f(2) = 9 \equiv 16\ (mod 27)$	Q
L	11	$f(11) = -9 \equiv 18\ (mod 27)$	S
⊔	26	$f(26) = -39 \equiv 15\ (mod 27)$	P

Logo, a mensagem cifrada é NQNO⊔NPONMPZYGFYPKNGPFEJMSN.

Item (b) Determinação da função inversa

$$f(x) = -2x + 13 \Rightarrow f(x) = 25x + 13,\ pois\ -2 \equiv 25\ mod\ 27.$$

Portanto,

$$f^{-1}(x) = 13x - 13 \cdot 13,\ pois\ 25 \cdot 13 = 325 \equiv 1\ mod\ 27$$

$$f^{-1}(x) = 13x - 7,\ pois\ -13 \cdot 13 = -169 \equiv -7\ mod\ 27$$

$$f^{-1}(x) = 13x + 20,\ pois\ -7 \equiv 20\ mod\ 27$$

Assim, $f(x) = -2x + 13 \Rightarrow f^{-1}(x) = 13x + 20$.

Item (c) Primeiramente, associa-se cada letra da mensagem cifrada a um número de acordo com a Tabela 5.10.

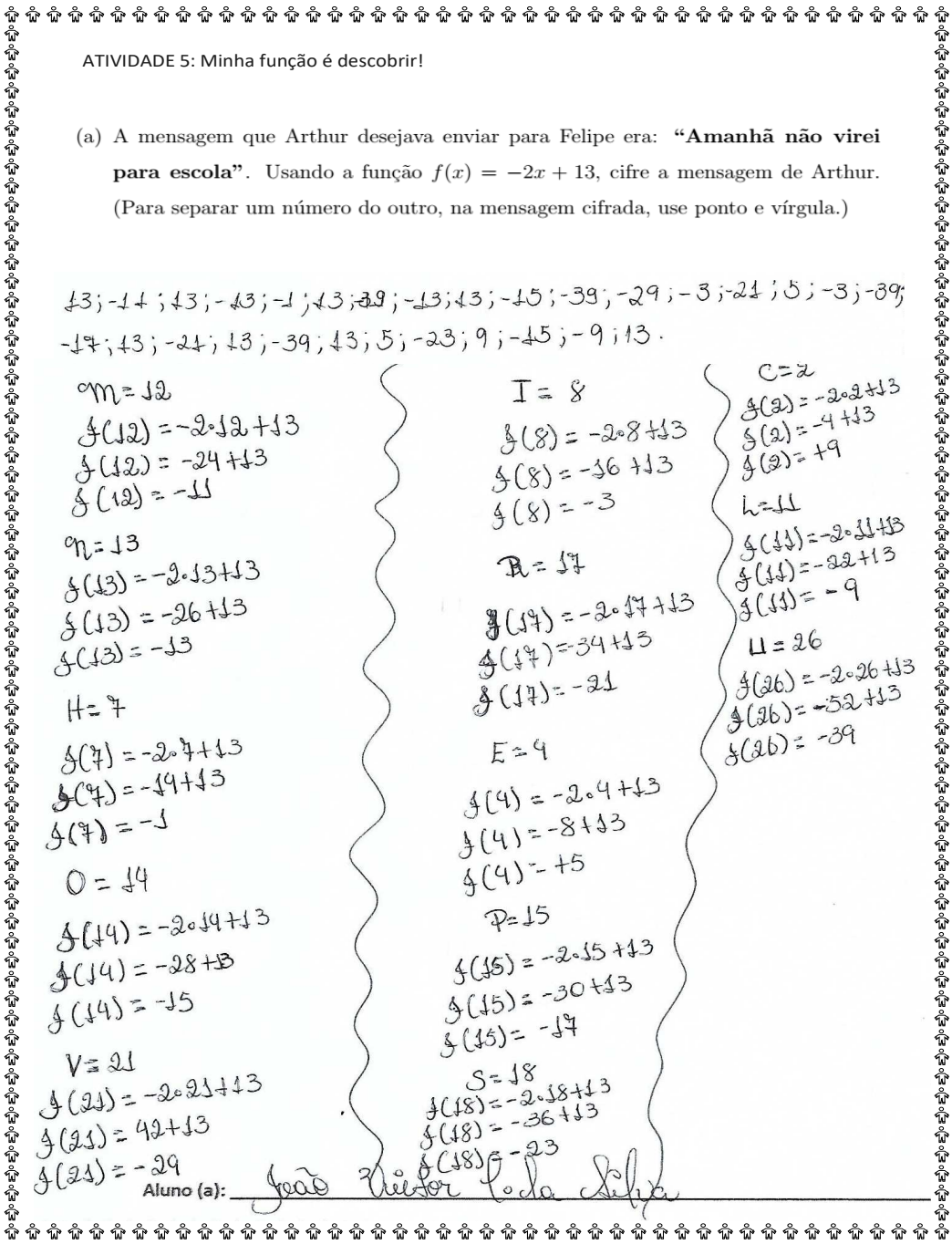
Posteriormente, usando a função $f^{-1}(x) = 13x + 20$, encontrada no item b, deve-se substituir em x, cada um desses valores, para encontrar o seu correspondente $f^{-1}(x)$. Em seguida, faz-se a congruência módulo 27 para cada um dos $f^{-1}(x)$ encontados, como mostra a Tabela 5.12.

Finalmente, verifica-se na Tabela 5.10, qual letra está associada ao valor encontrado e assim, ao final da substituição de cada valor por sua respectiva letra, tem-se a mensagem decifrada: "TUDO BEM, AVISAREI O PROFESSOR".

Tabela 5.12: Decifrando a mensagem

Letra cifrada	Sequência Numérica (x)	Cálculo da imagem da função $f^{-1}(x)$	Letra correspondente
C	2	$f^{-1}(2) = 46 \equiv 19$ mod27	T
A	0	$f^{-1}(0) = 20 \equiv 20$ mod27	U
H	7	$f^{-1}(7) = 111 \equiv 3$ mod27	D
M	12	$f^{-1}(12) = 176 \equiv 14$ mod27	O
P	15	$f^{-1}(15) = 215 \equiv 26$ mod27	⊔
L	11	$f^{-1}(11) = 163 \equiv 1$ mod27	B
F	5	$f^{-1}(5) = 85 \equiv 4$ mod27	E
Q	16	$f^{-1}(16) = 228 \equiv 12$ mod27	M
N	13	$f^{-1}(13) = 189 \equiv 0$ mod27	A
Z	25	$f^{-1}(25) = 345 \equiv 21$ mod27	V
Y	24	$f^{-1}(24) = 332 \equiv 8$ mod27	I
E	4	$f^{-1}(4) = 72 \equiv 18$ mod27	S
G	6	$f^{-1}(6) = 98 \equiv 17$ mod27	R
K	10	$f^{-1}(10) = 150 \equiv 15$ mod27	P
D	3	$f^{-1}(3) = 59 \equiv 5$ mod27	F

Figura 5.33: Atividade 5 - Item A



ATIVIDADE 5: Minha função é descobrir!

(a) A mensagem que Arthur desejava enviar para Felipe era: **"Amanhã não virei para escola"**. Usando a função $f(x) = -2x + 13$, cifre a mensagem de Arthur. (Para separar um número do outro, na mensagem cifrada, use ponto e vírgula.)

13; -11; 13; -13; -1; 13; 29; -13; 13; -15; -39; -29; -3; -21; 5; -3; -39; -17; 13; -21; 13; -39; 13; 5; -23; 9; -15; -9; 13.

m = 12
f(12) = -2·12 + 13
f(12) = -24 + 13
f(12) = -11

n = 13
f(13) = -2·13 + 13
f(13) = -26 + 13
f(13) = -13

H = 7
f(7) = -2·7 + 13
f(7) = -14 + 13
f(7) = -1

O = 14
f(14) = -2·14 + 13
f(14) = -28 + 13
f(14) = -15

V = 21
f(21) = -2·21 + 13
f(21) = 42 + 13
f(21) = -29

I = 8
f(8) = -2·8 + 13
f(8) = -16 + 13
f(8) = -3

R = 17
f(17) = -2·17 + 13
f(17) = -34 + 13
f(17) = -21

E = 4
f(4) = -2·4 + 13
f(4) = -8 + 13
f(4) = +5

P = 15
f(15) = -2·15 + 13
f(15) = -30 + 13
f(15) = -17

S = 18
f(18) = -2·18 + 13
f(18) = -36 + 13
f(18) = -23

C = 2
f(2) = -2·2 + 13
f(2) = -4 + 13
f(2) = +9

L = 11
f(11) = -2·11 + 13
f(11) = -22 + 13
f(11) = -9

U = 26
f(26) = -2·26 + 13
f(26) = -52 + 13
f(26) = -39

Aluno (a): João Victor Costa Silva

Figura 5.34: Atividade 5 - Item B

ATIVIDADE 5: Minha função é descobrir!

(b) Determine a função inversa da função $f(x) = -2x + 13$.

$f(x) = -2x + 13$

$y = -2x + 13$

$x = -2y + 13$

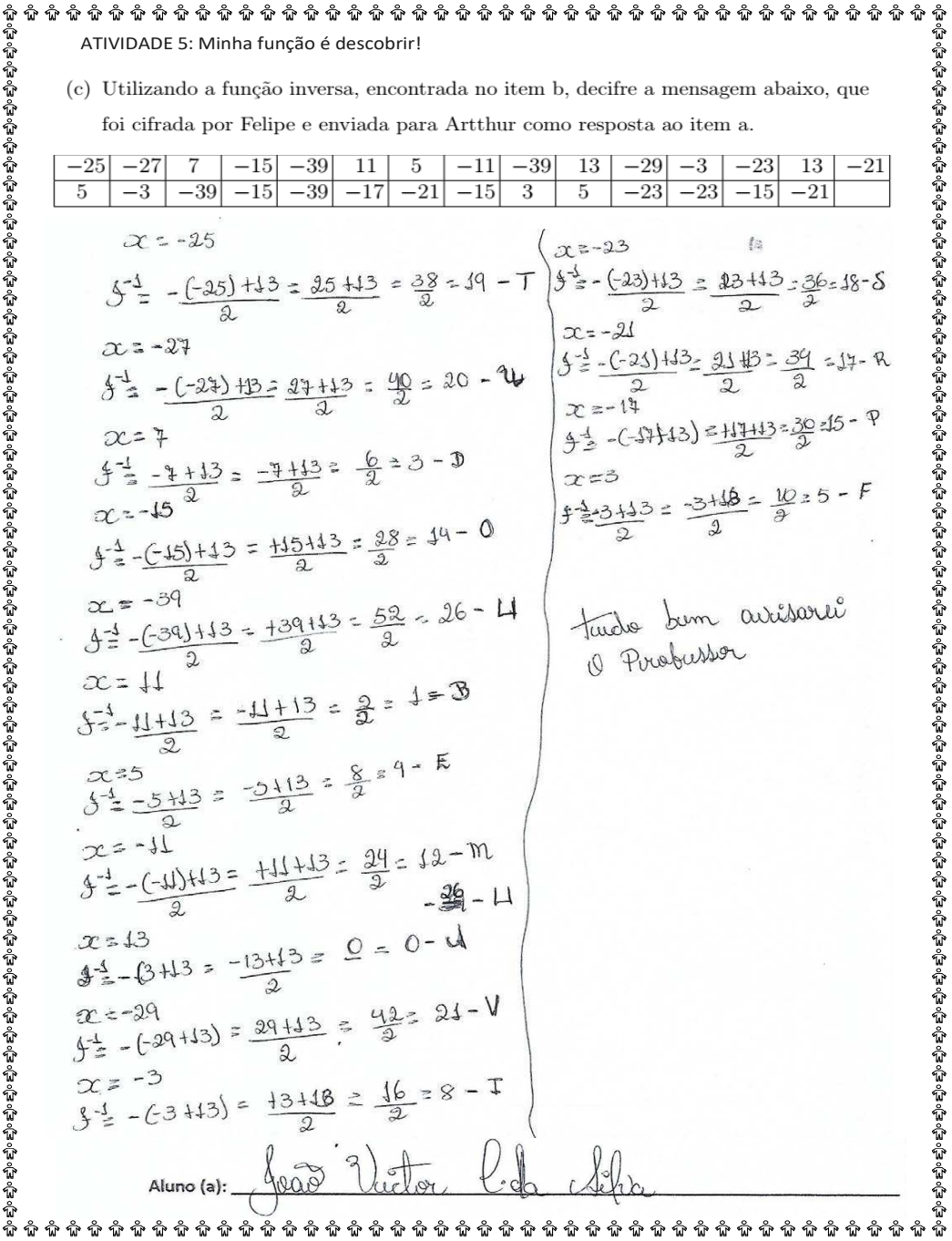
$2y = -x + 13$

$y = \frac{-x+13}{2}$

$f^{-1} = \frac{-x+13}{2}$

Aluno (a): Wanderson Sabato de Sousa.

Figura 5.35: Atividade 5 - Item C



ATIVIDADE 5: Minha função é descobrir!

(c) Utilizando a função inversa, encontrada no item b, decifre a mensagem abaixo, que foi cifrada por Felipe e enviada para Artthur como resposta ao item a.

−25	−27	7	−15	−39	11	5	−11	−39	13	−29	−3	−23	13	−21
5	−3	−39	−15	−39	−17	−21	−15	3	5	−23	−23	−15	−21	

$x = -25$

$f^{-1} = \frac{-(-25)+13}{2} = \frac{25+13}{2} = \frac{38}{2} = 19 - T$

$x = -27$

$f^{-1} = \frac{-(-27)+13}{2} = \frac{27+13}{2} = \frac{40}{2} = 20 - U$

$x = 7$

$f^{-1} = \frac{-7+13}{2} = \frac{-7+13}{2} = \frac{6}{2} = 3 - D$

$x = -15$

$f^{-1} = \frac{-(-15)+13}{2} = \frac{15+13}{2} = \frac{28}{2} = 14 - O$

$x = -39$

$f^{-1} = \frac{-(-39)+13}{2} = \frac{+39+13}{2} = \frac{52}{2} = 26 - L$

$x = 11$

$f^{-1} = \frac{-11+13}{2} = \frac{-11+13}{2} = \frac{2}{2} = 1 = B$

$x = 5$

$f^{-1} = \frac{-5+13}{2} = \frac{-5+13}{2} = \frac{8}{2} = 4 - E$

$x = -11$

$f^{-1} = \frac{-(-11)+13}{2} = \frac{+11+13}{2} = \frac{24}{2} = 12 - M$

$-\frac{26}{2} - L$

$x = 13$

$f^{-1} = -(3+13 = \frac{-13+13}{2} = \frac{0}{} = 0 - A$

$x = -29$

$f^{-1} = -(-29+13) = \frac{29+13}{2} = \frac{42}{2} = 21 - V$

$x = -3$

$f^{-1} = -(-3+13) = \frac{+3+18}{2} = \frac{16}{2} = 8 - I$

$x = -23$

$f^{-1} = -\frac{(-23)+13}{2} = \frac{23+13}{2} = \frac{36}{2} = 18 - S$

$x = -21$

$f^{-1} = \frac{-(-21)+13}{2} = \frac{21+13}{2} = \frac{34}{2} = 17 - R$

$x = -17$

$f^{-1} = -(-17+13) = \frac{+17+13}{2} = \frac{30}{2} = 15 - P$

$x = 3$

$f^{-1} = \frac{-3+13}{2} = \frac{-3+18}{2} = \frac{10}{2} = 5 - F$

Tudo bem avisarei
O Professor

Aluno (a): João Victor Leite Silva

5.3 Análise do Questionário 2

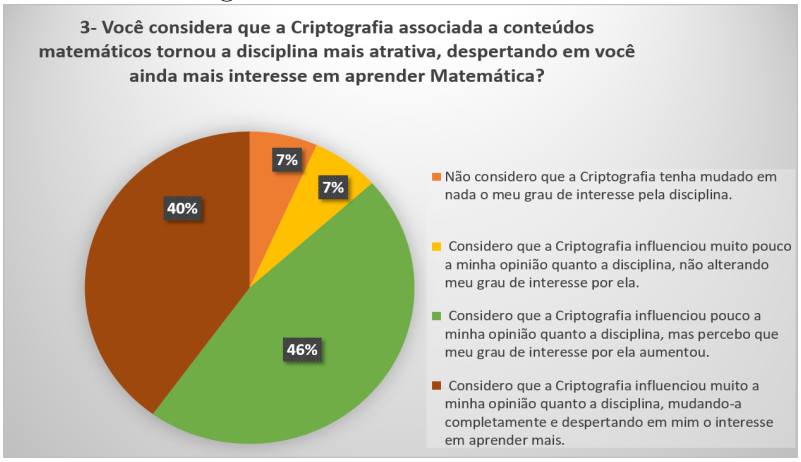
A aplicação do questionário 2, executada após a realização da última atividade do projeto, avaliou a metodologia adotado na execução das atividades propostas e se o uso da criptografia, associada a conteúdos, matemáticos, despertou nos estudantes um desejo maoir em aprofundar seus estudos na disciplina.

O primeiro item avaliou se o uso dos recursos na resolução das questões de matemática, como a Régua Deslizante, o CD Criptográfico e o Disco Giratório, tornaram as atividades mais interessantes e significativas. Nesse item, 100% dos alunos responderam sim a essa pergunta, comprovando que o uso dos recursos despertou o interesse e deu sentindo aos conteúdos trabalhados.

A análise do item 2 mostrou que 100% dos alunos gostaram de aprender criptografia, demonstrando que a escolha do tema da pesquisa atraiu a atenção dos estudantes.

O grafico que apresenta os resultados da análise do item 3, mostrado na Figura 5.36, revelou que 40% dos alunos disseram que a criptografia influenciou sua opinião quanto à matemática, mas que seu grau de interesse pela disciplina aumentou pouco. Enquanto 46% dos alunos entrevistados disseram que a criptografia influenciou sua opinião quanto a Matemática mudando completamente o seu grau de interesse pela disciplina e, ainda, despertou interesse em aprender mais a disciplina.

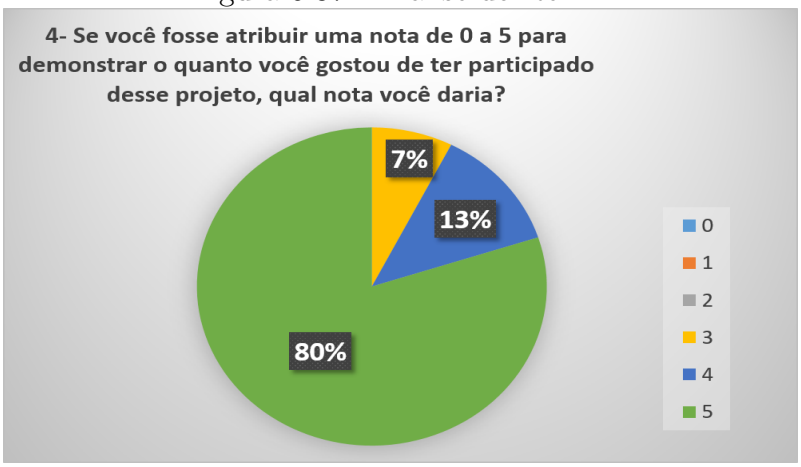
Figura 5.36: Análise do Item 3



Fonte: Dados obtidos na análise do Questionário 2

Com a análise do item 4, mostrada na Figura 5.37, constatou-se que 80% dos alunos entrevistados atribuíram nota máxima, quer dizer, nota 5, demonstrando que gostaram muito de participar do projeto. Não foram registrdas notas 0, 1 e 2 para esse item.

Figura 5.37: Análise do Item 4



Fonte: Dados obtidos na análise do Questionário 2

O último item do questionário pediu aos estudantes que descrevessem qual foi a importância de eles terem participado desse projeto e suas considerações positivas ou negativas sobre ele. Algumas respostas, apresentadas pelos estudantes, foram transcritas e listadas a seguir.

> "Foi muito bom, pois aprendi o que é matemática de verdade. Não é apenas contas e problemas. Também existe a diversão."(Estudante 1)
>
> "Amei! Gostei muito do projeto de criptografia no ensino da matemática. Antes, eu já me interessava. Agora, com esse trabalho, eu me interessei muito mais. Agora gosto muito mais da matéria de matemática."(Estudante 2)
>
> "A importância dessa atividade foi para nos aprimorar na matemática. Para eu ficar mais experiente na matéria. A criptografia eu não conhecia, mas agora que eu aprendi é muito bom, para quem quer sua privacidade."(Estudante 3)
>
> "Eu gostei muito de aprender. Eu não sabia sobre criptografia, mas agora eu sei. Gostei do projeto. Não sou muito bom em matemática, mas gostei bastante do que aprendi sobre criptografia. "(Estudante 4)
>
> "Foi muito importante, pois aprendi muitas coisas e tive a chance de aprender coisas que muitas pessoas não sabem. Foi um projeto muito legal, educativo, participativo e tudo muito bom."(Estudante 5)

6 CONSIDERAÇÕES FINAIS

Este trabalho apresentou uma proposta de abordagem da criptografia ao ensino da Matemática, associando cifras criptográficas a conteúdos matemáticos trabalhados no ensino fundamental e médio, por meio de atividades práticas, fazendo-se uso de recursos desenvolvidos para tornar as atividades lúdicas e dinâmicas.

A temática do trabalho foi escolhida em virtude da necessidade de tornar o conhecimento matemático mais compreensível e concreto. O questionamento motivador foi de que maneira os professores de matemática podem melhorar a sua prática de modo a desenvolver nos estudantes o interesse pela disciplina e o desejo de buscar novos conhecimentos, aprofundando aqueles que já lhes foram apresentados e lhes dando autonomia de investigar outros.

A principal hipótese apontava para que o uso de temas instigantes e motivadores, como a criptografia, aliados a atividades lúdicas desenvolvidas com o uso de materias concretos, são, de fato, aliados nesse processo de ensino-aprendizagem, pois tornam os conteúdos matemáticos mais atrativos, despertando no aluno a curiosidade e o prazer em aprender.

Nas aplicações, foram utilizadas cifras criptográficas associadas a conteúdos matemáticos, que exploraram o raciocínio lógico do aluno, abordando conceitos que abrangem conjuntos, relações, funções, teoria dos números e aritmética modular.

Por meio da realização do projeto "Desvendando Segredos", no qual aplicou-se atividades práticas, foi possível avaliar a eficácia da utilização da criptografia como instrumento motivador e facilitador no processo de ensino-aprendizagem da matemática, pois despertou o interesse e a curiosidade dos alunos que participaram do projeto.

Os objetivos propostos foram alcançados, uma vez que constatou-se que a utilização da criptografia, no ensino da matemática, serviu como intrumento de motivação, despertando o interesse em aprender ainda mais a disciplina e aguçando a cuiosidade dos alunos, que se mostraram dispostos a aprofundar e a aprender novos conteúdos, aumentando dessa forma o seu conhecimento.

A ideia de usar atividades práticas, associando a criptografia a conteúdos matemáticos, vir a modificar a maneira como os alunos veem e compreendem os conteúdos trabalhados foi confirrmada, já que, para todos os alunos participantes, a utilização dos recursos foi considerada eficaz e motivadora, conforme a análise da proposta feita no

Capítulo 5.

No que se refere a aplicação de atividades nas quais os alunos desenvolvem os materiais concretos que serão utilizados na realização dessas ou de outras atividades, é importante salientar que as aulas precisam ser ministradas de forma planejada, que estejam contempladas no seu plano de curso, com a finalidade de não comprometer o cronograma de atividades preestabelecido, bem como, deve-se ter objetivos claros e regras bem definidas.

Permitindo assim, conciliar as aulas tradicionais com as aulas práticas, servindo como uma alternativa para melhorar a prática docente e contrbuindo de forma significativa com a aprendizagem do aluno.

A inclusão de aulas práticas na rotina da sala de aula deve ser empregada pelos professores, a fim de aguçar a curiosidade e a criatividade do aluno, e de dar-lhes a possibilidade de interagir com materiais concretos, permitindo que o aluno atue de forma ativa na construção do seu próprio conhecimento.

Este trabalho é importante, pois fornece ao professor uma alternativa para motivar e despertar no aluno o desejo em aprender matemática, e servindo de estímulo para que ele possa buscar novos conhecimentos. Ao mesmo tempo, o projeto leva o professor a rever suas metodologias, proporcionando aulas mais atrativas e dinâmicas aos seus alunos. [**?**]

REFERÊNCIAS

ALMEIDA, Fernando M. M. B. **Sistemas de Numeração Precursores do Sistema Indo-Árabe**. Agosto de 2007. Faculdade de Ciências da Universidade do Porto, Departamento de Matemática Pura. Dissertação de Mestrado.

ANDRADE, A. S. **Números, Relações e Criptografia.** UFPB - Paraíba, 1997.

BEZERRA, D. J.; MALAGUTTI, P. L.; RODRIGUES, V. C. S. **Aprendendo Criptologia de Forma Divertida.** UFPB – Paraíba. Agosto, 2017. Disponível em: <https://docgo.net/aprendendo-criptologia-de-forma-divertida>. Acessado em: 06 de outubro 2017.

BEZERRA, Leonardo. **Origem do sistema de numeração decimal, egípcio e romano.** Abril, 2016. Blogspot Cursinho Exato. Disponível em: <http://cursinhoexato.blogspot.com/2016/04/origem-do-sistema-de-numeracao-decimal.html>. Acessado em: 24 de abril 2018.

CARDOSO, Ana Luiza. **Descrição de um sistema criptográfico de chave pública**. São Luís. 2011.

COUTINHO, S.C. **Criptografia.** 1ª ed. Rio de Janeiro: IMPA, 2016.

DANTAS, Andréa de Araújo. **A Criptografia no ensino Fundamental e Médio.** Caicó, 2016.

FILHO, João Coelho. **Introdução à Teoria dos Números: Algoritmo da Divisão, Números Primos e Aritmética Modular.** Notas de Aula. São Luís, 2012.

GALVÃO, M. E. E. L. **As origens da Matemática – dos processos de contagem aos sistemas de numeração.** IME- USP- São Paulo. 2º Semestre, 2014.

INSTITUTO SUPERIOR DE CIÊNCIAS APLICADAS - ISCA FACULDADES. **O que é Criptografia?** Curso Comunicação Social - Jornalismo 2016. (11m 24s). Disponível em <https://www.youtube.com/watch?v=ytzS3P_KIMg>. Acesso: 12 jan. 2018.

JANSEN, Jean Mendes. **Criptografia: Uma abordagem para o Ensino Médio.** Dissertação de Mestrado. 2016.

MACHADO, N. J. Simon Singh: **O livro dos Códigos.** São Paulo, 2012. Artigo apresentado no Seminário de Ensino de Matemática (SEMA-FEUSP). Disponível em: <http://www.nilsonjosemachado.net/sema20120427.pdf>. Acessado em: 05 de novembro 2017.

MEDEIROS, Fábio. **Criptografia: Bastão de Licurgo (scytale) em Python.** Maio, 2013. Siriarah. Disponível em: <http://https://siriarah.wordpress.com/2013/05/13/criptografia-bastao-de-licurgo-scytale-em-python/>. Acessado em: 10 novembro de 2017.

MIRANDA, Danielle. **Sistema de Numeração Babilônico**. Mundo Educação. Disponível em: <https://mundoeducacao.bol.uol.com.br/matematica/sistema-numeracao-babilo htm>. Acessado em: 18 de fevereiro 2018.

MOL, Rogério S.. **Introdução à História da Matemática**. Belo Horizonte, 2013. Universidade Federal de Minas Gerais - CAED-UFMG. Mundo Educação. Disponível em: <http://www.mat.ufmg.br/ead/acervo/livros/introducao_a_historia_da_matematica.pdf>. Acessado em: 09 de novembro 2017.

OLIVEIRA, D.; KRIPKA, R. M. L. **O uso da criptografia no ensino da matemática.** Recife. 2011. Acessado em: 10 de setembro de 2017. Disponível em: <www.lematec.net.br/CDS/XIIICIAEM/artigos/1817.pdf>.

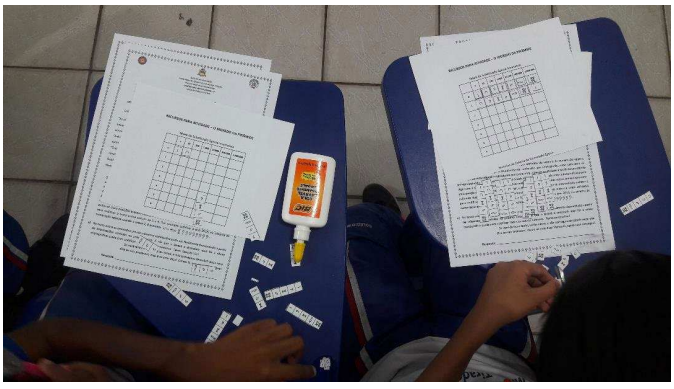
SCHLITTLER, Patricia Andréia. Blogger: **A história dos números.** Disponível em: <http://historiadosnumeros.blogspot.com/2008_08_01_archive.html> Acessado em: 05 de outubro de 2018.

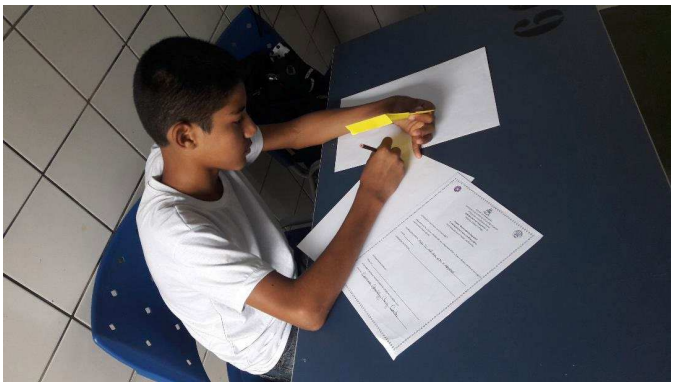
SINGH, Simon. **O livro dos códigos.** Tradução de Jorge Calife. 6ª ed. Rio de Janeiro: Record, 2007.

SOUZA, Maycon Pereira. **A Cifra de Hill**. Instituto Federal de Goiás - Campus Uruaçu. Disponível em <cts.luziania.ifg.edu.br/index.php/CTS1/article/download/100/pdf_30> Acessado em: 19 de setembro de 2018.

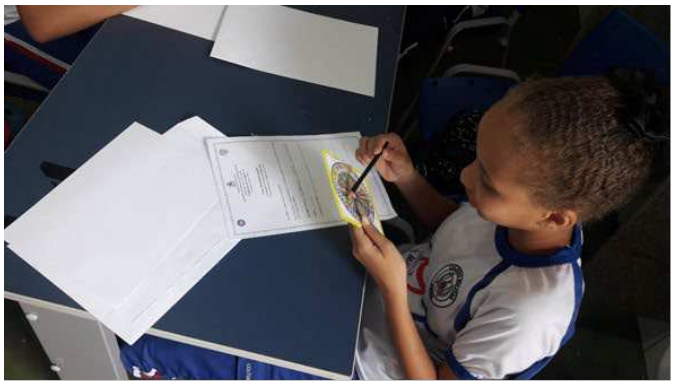
Apêndices

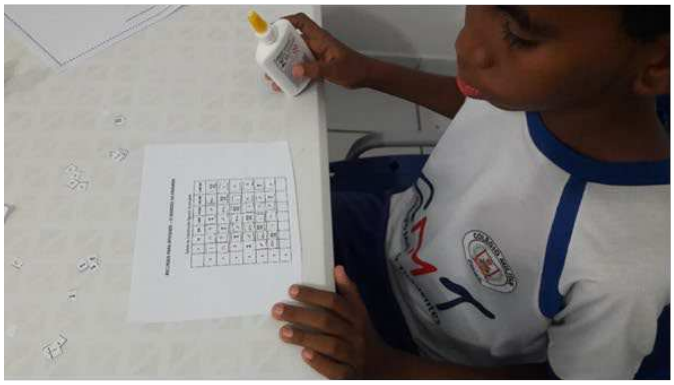
Apêndice A - Registro Fotográfico do Projeto Desvendando Segredos

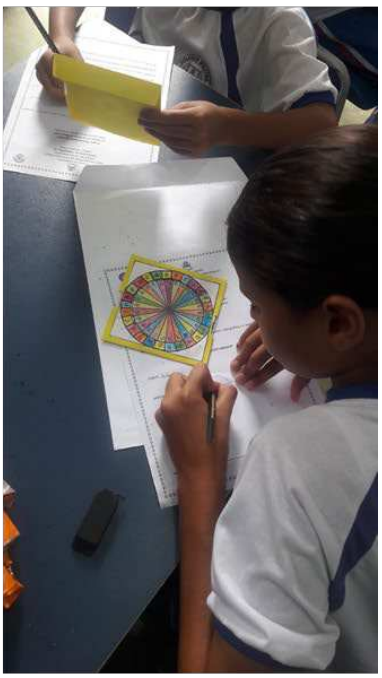




Apêndice B - Registro Fotográfico do Projeto Desvendando Segredos







Anexos

Anexo A - Solicitação de Autorização

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

SOLICITAÇÃO DE AUTORIZAÇÃO PARA PARTICIPAÇÃO EM PESQUISA

Senhores pais ou responsáveis pelo aluno(a):

_____

Venho solicitar a autorização da participação do seu(sua) filho(a), aluno do ___ Ano do Colégio Militar Tiradentes VI, Unidade Parque Vitória, para participar da pesquisa que estou realizando para minha dissertação do Mestrado Profissional em Matemática – PROFMAT, realizado pela Universidade Estadual do Maranhão – UEMA.

A pesquisa acontecerá no turno **matutino**, através da realização de uma semana de aulas e atividades práticas, tendo início no dia ____ e término no dia ____, no horário das 08:00 às 09:30, na área interna da escola.

Informo que o nome do(a) aluno(a) não será mencionado na pesquisa, mas peço que autorize a publicação das fotografias ilustrativas que serão necessárias, sem que se identifique diretamente o(a) aluno(a).

Aguardo sua compreensão e autorização.
Atenciosamente,
Profª Katarine Araújo Baldez de Carvalho
Contato (98) xxxxx-xxxx

São José de Ribamar, ___/___/___.

( ) Autorizo ( ) Não Autorizo

_____
Assinatura do pai ou responsável

Anexo B - Questionário 1

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

QUESTIONÁRIO - 1

1- Qual é o seu grau de interesse pela Matemática?

( ) MUITO PEQUENO ( ) PEQUENO ( ) MÉDIO ( ) GRANDE ( ) MUITO GRANDE

2- Qual dos itens abaixo você considera ter tido maior influência no grau de interesse que você tem hoje pela Matemática?

a) Não ter uma rotina de estudo diário.
b) Não ter o acompanhamento da família nos estudos.
c) Os professores de matemática não demonstram motivação ao ensinar.
d) Falta de relação entre a Matemática ensinada na escola e o cotidiano.
e) A forma como o professor de matemática ensina e avalia.
f) A falta de motivação própria em aprender.

3- Qual a avaliação que você faz das aulas de Matemática que você tem na sua escola?

a) São aulas monótonas e cansativas, que não chamam a atenção do aluno.
b) São aulas sem muito atrativo, mas que prendem a atenção pelo desempenho do professor, que consegue interagir com os alunos.
c) São aulas dinâmicas e produtivas, que prendem a atenção do aluno, levando-o a uma aprendizagem significativa.

4- O seu professor de Matemática costuma realizar atividades práticas e/ou lúdicas em sala de aula?

( ) NUNCA ( ) À VEZES ( ) SEMPRE

5- O que mais chamou sua atenção e que você considera ter sido fundamental na sua decisão de se inscrever para participar desse projeto?

a) A possibilidade de ficar fora de casa no contra turno.
b) Tive interesse apenas por que meus colegas se inscreveram.
c) Aprender algo novo e que possa aumentar seus conhecimentos.
d) O tema do projeto foi o que mais chamou minha atenção.
e) Outro motivo. _____

Anexo C - Questionário 2

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

QUESTIONÁRIO – 2

1- Você considera que trabalhar as questões de matemática com recursos como a Régua Numérica Criptográfica, CD Criptográfico e o Disco Giratório tornaram as atividades mais interessantes e significativas?

( ) SIM ( ) NÃO

2- Você gostou de aprender Criptografia?

( ) SIM ( ) NÃO

3- Você considera que a Criptografia associada a conteúdos matemáticos tornou a disciplina mais atrativa, despertando em você ainda mais interesse em aprender Matemática?

a) Não considero que a Criptografia tenha mudado em nada o meu grau de interesse pela disciplina.
b) Considero que a Criptografia influenciou pouco a minha opinião quanto a disciplina, não alterando meu grau de interesse por ela.
c) Considero que a Criptografia influenciou a minha opinião quanto a disciplina, aumentando um pouco meu grau de interesse por ela.
d) Considero que a Criptografia influenciou a minha opinião quanto a disciplina, mudando-a completamente e despertando em mim o interesse em aprender mais.

4- Se você fosse atribuir uma nota de 0 a 5 para demonstrar o quanto você gostou de ter participado desse projeto, qual nota você daria?

NOTA: _____

5- Descreva qual foi a importância, pra você, em ter participado desse projeto e suas considerações positivas ou negativas sobre ele.

_____
_____
_____
_____
_____

Anexo D - Avaliação Diagnóstica 6º ANO

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"

A Criptografia no Ensino da Matemática

Profª Katarine Araújo Baldez de Carvalho

AVALIAÇÃO DIAGNÓSTICA – 6º ANO

1- Uma biblioteca recebeu uma doação de 4 caixas com 1.000 livros didáticos, 6 caixas com 100 livros de literatura, 8 caixas com 10 livros infantis e 5 livros avulsos. Quantos livros essa biblioteca recebeu ao todo?

a) 4.685 livros
b) 4.658 livros
c) 5.684 livros
d) 5.846 livros

2- Uma menina completou um quebra-cabeça de 2.530 peças. Esse número é composto de:

a) 2 unidades de milhar, 5 dezenas e 6 unidades.
b) 2 unidades de milhar, 5 centenas e 3 dezenas.
c) 2 unidades de milhar, 53 centenas e 3 unidades.
d) 2 unidades de milhar, 53 centenas e 0 unidades.

3- Quais são os três próximos números da sequência?

1, 1, 2, 3, 5, 8, ...

a) 10, 12, 14
b) 13, 15, 17
c) 13, 21, 34
d) 21, 25, 32

4- A tabela abaixo mostra a população das 5 capitais mais populosas, de acordo com uma pesquisa realizada pelo IBGE, no ano de 2009.

CAPITAIS MAIS POPULOSAS DO BRASIL

Capitais	População
São Paulo - SAO	11.037.593
Rio de Janeiro - RIO	6.186.710
Salvador - SAL	2.998.056
Brasília - BSB	2.606.885
Fortaleza - FOR	2.505.552

Fonte: IBGE/2009

Substituindo as siglas das capitais pelas respectivas populações, o valor da expressão é?

SAO - RIO – SAL + FOR

a) 754.058
b) 2.986.723
c) 4.358.379
d) 4.459.385

5- Qual dos números a seguir tem o 3 como divisor?

a) 8
b) 10
c) 21
d) 35

6- Ao longo de toda sua vida como estudante a Matemática esteve presente em todos os anos que você estudou. Marque a alternativa que represente, de forma sincera, como você avalia a sua relação com esta disciplina.

a) Não gosto, não estudo e não tenho interesse em estudar Matemática.
b) Não gosto, não estudo, mas gostaria de aprender Matemática.
c) Não gosto, mas estudo porque sei que é importante aprender Matemática.
d) Gosto, estudo e sei que é importante estudar Matemática.

Anexo E - Avaliação Diagnóstica 7º/8º ANO

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

AVALIAÇÃO DIAGNÓSTICA – 7º/8º ANO

1- (OBMEP) Um time ganha 3 pontos por vitória, 1 ponto por empate e nenhum ponto em caso de derrota. Até hoje cada time já disputou 20 jogos. Se um desses times venceu 8 jogos e perdeu outros 8 jogos, quantos pontos ele tem até agora?
   a) 23
   b) 25
   c) 26
   d) 27
   e) 28

2- (SARESP) Eu tenho 1 320 figurinhas. Meu primo tem metade do que eu tenho. Minha irmã tem o triplo das figurinhas de meu primo. Quantas figurinhas minha irmã tem?
   a) 1 900
   b) 1 930
   c) 1940
   d) 1 980

3- O cubo de 4 é:
   a) 16
   b) 8
   c) 12
   d) 64

4- Quais são os três próximos números da sequência?

1, 1, 2, 3, 5, 8, ...

   a) 10, 12, 14
   b) 13, 15, 17
   c) 13, 21, 34
   d) 21, 25, 32

5- A tabela abaixo mostra a população das 5 capitais mais populosas, de acordo com uma pesquisa realizada pelo IBGE, no ano de 2009.

CAPITAIS MAIS POPULOSAS DO BRASIL

Capitais	População
São Paulo - SAO	11.037.593
Rio de Janeiro - RIO	6.186.710
Salvador - SAL	2.998.056
Brasília - BSB	2.606.885
Fortaleza - FOR	2.505.552

Fonte: IBGE/2009

Substituindo as siglas das capitais pelas respectivas populações, o valor da expressão é?

SAO - RIO – SAL + FOR

   a) 754.058
   b) 2.986.723
   c) 4.358.379
   d) 4.459.385

6- Ao longo de toda sua vida como estudante a Matemática esteve presente em todos os anos que você estudou. Marque a alternativa que represente, de forma sincera, como você avalia a sua relação com esta disciplina.
   a) Não gosto, não estudo e não tenho interesse em estudar Matemática.
   b) Não gosto, não estudo, mas gostaria de aprender Matemática.
   c) Não gosto, mas estudo porque sei que é importante aprender Matemática.
   d) Gosto, estudo e sei que é importante estudar Matemática.

Anexo F - Avaliação Diagnóstica 9º ANO

ESTADO DO MARANHÃO
SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA
POLÍCIA MILITAR DO MARANHÃO
COLÉGIO MILITAR TIRADENTES - VI
UNIDADE PARQUE VITÓRIA

Projeto "Desvendando Segredos"
A Criptografia no Ensino da Matemática
Profª Katarine Araújo Baldez de Carvalho

AVALIAÇÃO DIAGNÓSTICA – 9º ANO

1- (OBMEP) Um time ganha 3 pontos por vitória, 1 ponto por empate e nenhum ponto em caso de derrota. Até hoje cada time já disputou 20 jogos. Se um desses times venceu 8 jogos e perdeu outros 8 jogos, quantos pontos ele tem até agora?
   a) 23
   b) 25
   c) 26
   d) 27
   e) 28

2- Dada a equação $2x - 16 = 2 - x$, o valor de x é:
   a) 6
   b) 7
   c) 8
   d) 9

3- A forma fatorada do número 2 700 é:
   a) $2 . 3^2 . 5^2$
   b) $2^2 . 3^2 . 5^2$
   c) $2^2 . 3^3 . 5^2$
   d) $2^2 . 3^3 . 5$

4- Quais são os três próximos números da sequência?

1, 1, 2, 3, 5, 8, ...

   a) 10, 12, 14
   b) 13, 15, 17
   c) 13, 21, 34
   d) 21, 25, 32

5- A tabela abaixo mostra a população das 5 capitais mais populosas, de acordo com uma pesquisa realizada pelo IBGE, no ano de 2009.

CAPITAIS MAIS POPULOSAS DO BRASIL

Capitais	População
São Paulo - SAO	11.037.593
Rio de Janeiro - RIO	6.186.710
Salvador - SAL	2.998.056
Brasília - BSB	2.606.885
Fortaleza - FOR	2.505.552

Fonte: IBGE/2009

Substituindo as siglas das capitais pelas respectivas populações, o valor da expressão é?

SAO - RIO – SAL + FOR

   a) 754.058
   b) 2.986.723
   c) 4.358.379
   d) 4.459.385

6- Ao longo de toda sua vida como estudante a Matemática esteve presente em todos os anos que você estudou. Marque a alternativa que represente, de forma sincera, como você avalia a sua relação com esta disciplina.
   a) Não gosto, não estudo e não tenho interesse em estudar Matemática.
   b) Não gosto, não estudo, mas gostaria de aprender Matemática.
   c) Não gosto, mas estudo porque sei que é importante aprender Matemática.
   d) Gosto, estudo e sei que é importante estudar Matemática.

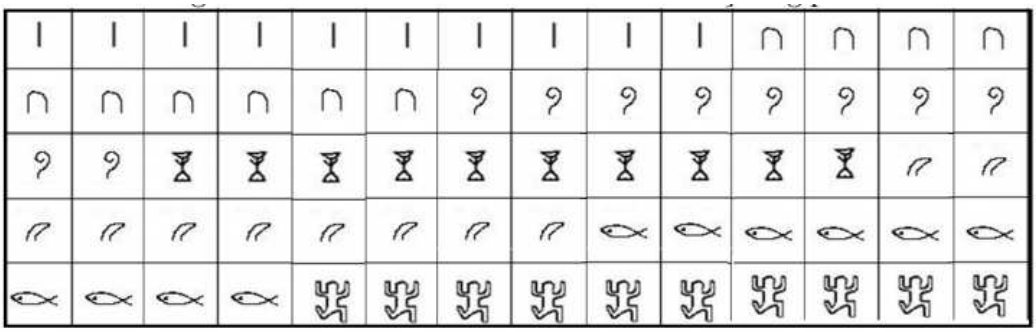
Anexo G - Tabela e Símbolos de Substituição Egípcio

RECURSOS PARA ATIVIDADE – O SEGREDO DA PIRÂMIDE

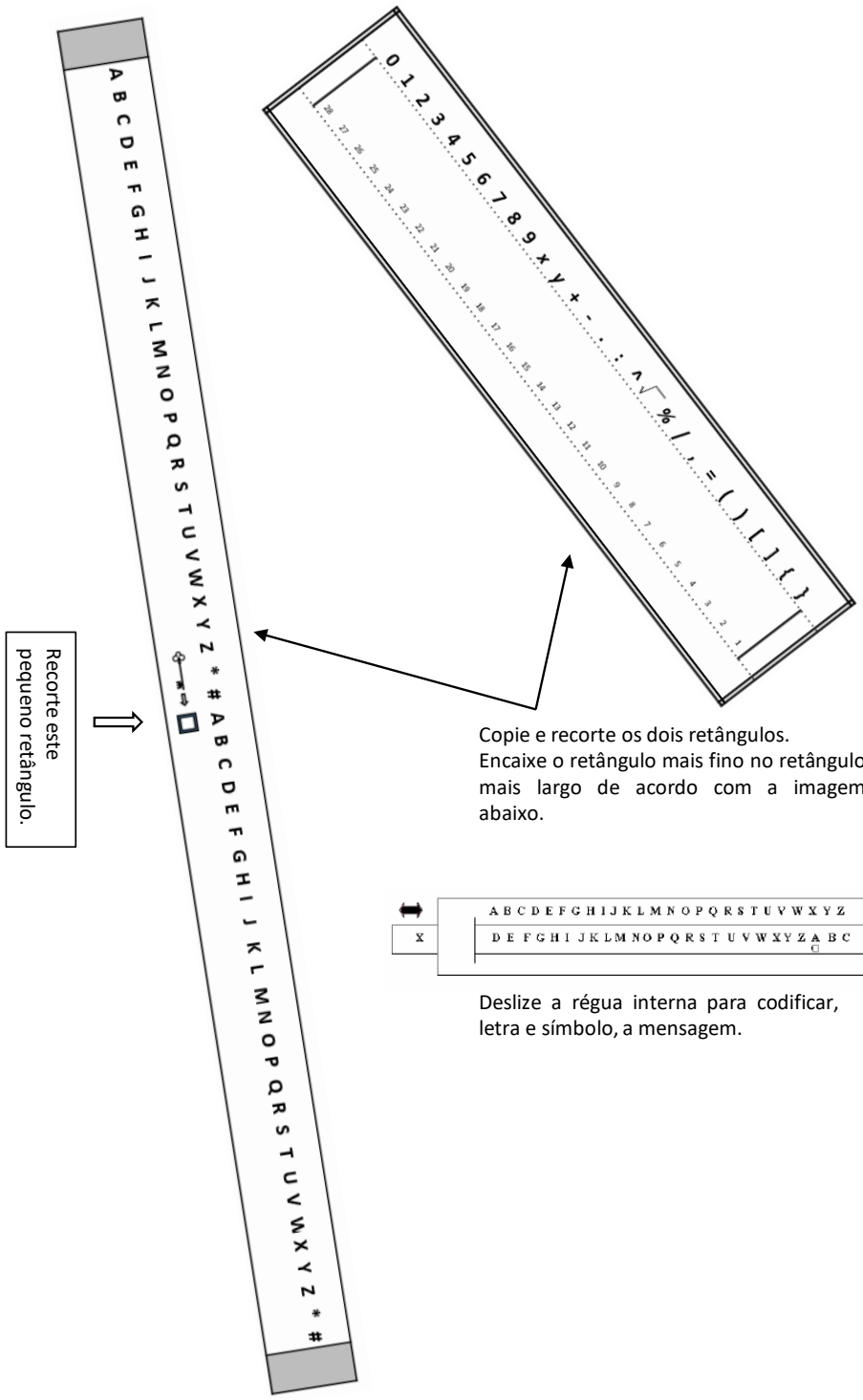
Tabela de Substituição Egípcia Incompleta

	1	10	100	1.000	10.000	100.000	1.000.000
0							
1							
2							
3							
4							
5							
6							

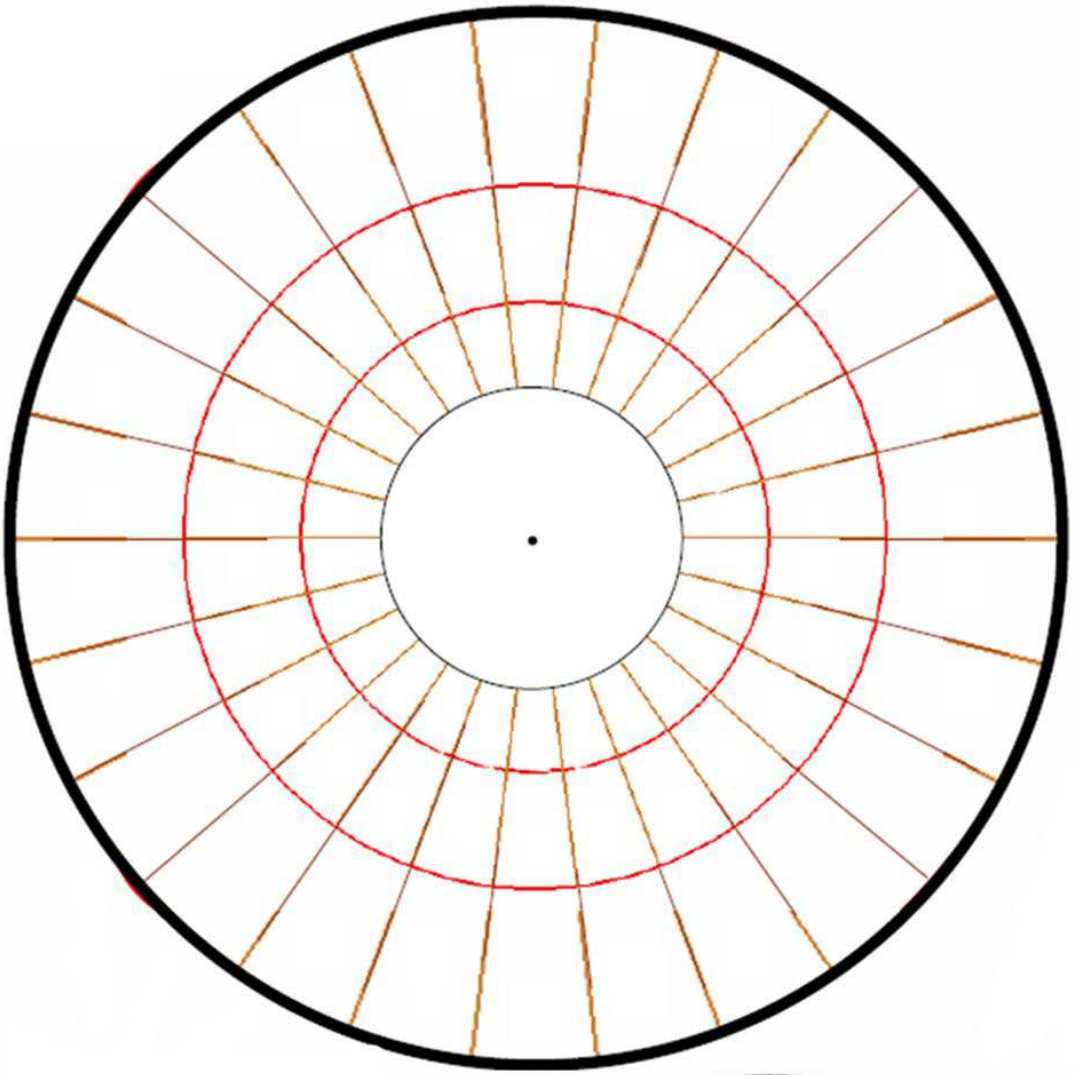
Símbolos do Sistema de Numeração Egípcio

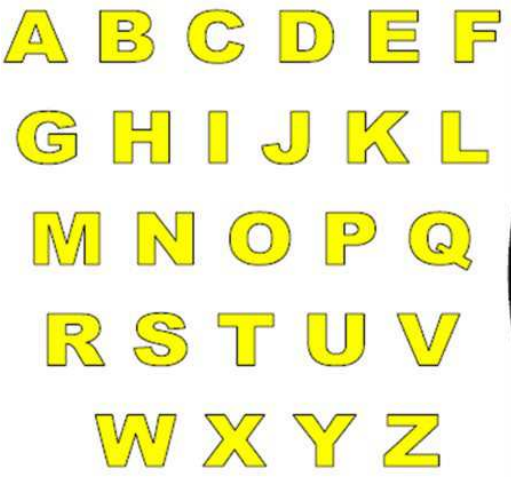


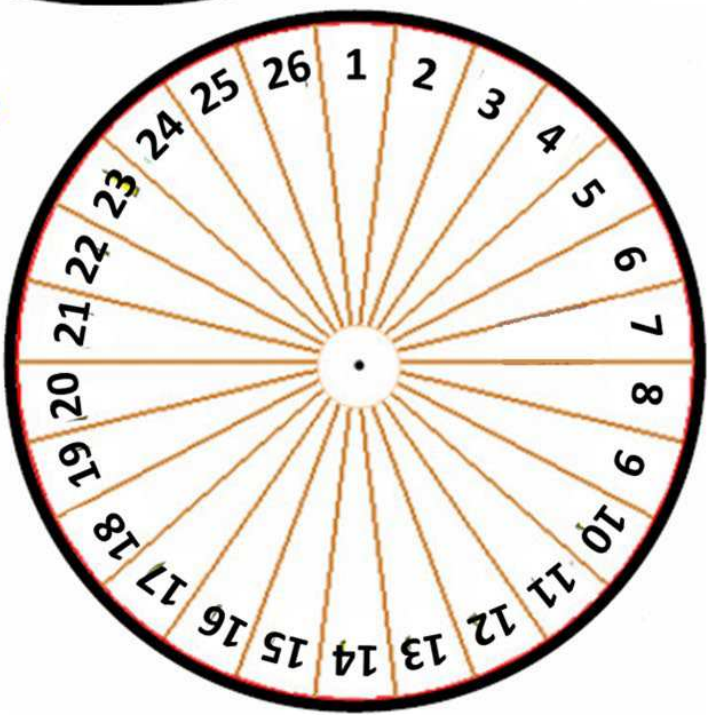
Anexo H - Régua Deslizante



Anexo I - Disco Giratório







Anexo J - CD Criptográfico