UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENSINO DE CIÊNCIAS EXATAS - PPGECE

VALDEMAR DANILO DE CARVALHO

UMA METODOLOGIA COM USO DE CRIPTOGRAFIA PARA ENSINO DE FUNÇÕES

SOROCABA
AGOSTO/2020

UNIVERSIDADE FEDERAL DE SÃO CARLOS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENSINO DE CIÊNCIAS EXATAS - PPGECE

VALDEMAR DANILO DE CARVALHO

UMA METODOLOGIA COM USO DE CRIPTOGRAFIA PARA ENSINO DE FUNÇÕES

Dissertação apresentada ao Programa de Pós-Graduação em Ensino de Ciências Exatas– PPGECE, do Centro de Ciências Exatas e Tecnologia da Universidade Federal de São Carlos, como exigência parcial para obtenção do título de Mestre em Ensino de Matemática.

Orientação: Prof.ª Dr.ª Sílvia Maria Simões de Carvalho

SOROCABA
AGOSTO/2020

Carvalho, Valdemar Danilo de

Uma metodologia com uso de criptografia para o ensino de funções / Valdemar Danilo de Carvalho -- 2020.
72f.

Dissertação (Mestrado) - Universidade Federal de São Carlos, campus Sorocaba, Sorocaba
Orientador (a): Prof.ª Dr.ª Sílvia Maria Simões de Carvalho
Banca Examinadora: Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar, orientadora), Prof. Dr. Mayk Vieira Coelho (UNIFAL), Prof. Dr. Antonio Noel Filho (IFSP).
Bibliografia

1. Ensino e Aprendizagem. 2. Funções. 3. Criptografia. I. Carvalho, Valdemar Danilo de. II. Título.

Ficha catalográfica desenvolvida pela Secretaria Geral de Informática (SIn)

DADOS FORNECIDOS PELO AUTOR

Bibliotecário responsável: Maria Aparecida de Lourdes Mariano - CRB/8 6979

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ensino de Ciências Exatas

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Valdemar Danilo de Carvalho, realizada em 28/08/2020.

Comissão Julgadora:

Profa. Dra. Silvia Maria Simões de Carvalho (UFSCar)

Prof. Dr. Mayk Vieira Coelho (UNIFAL)

Prof. Dr. Antonio Noel Filho (IFSP)

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.
O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Ensino de Ciências Exatas.

Dedico este trabalho a minha mãe, Vani, aos meus alunos e meus colegas de turma, que de alguma forma sempre me fizeram correr atrás dos meus sonhos e me incentivaram a continuar até o fim.A inesquecível turma de química 010ufscar Sorocaba que são uma família. Dedico também a Deus,pela graça da vida,perseverança e força para vencer mais essa etapa de minha formação.

AGRADECIMENTO

Agradeço a Deus pela oportunidade e força de percorrer mais essa etapa de minha formação.

A minha mãe que de alguma forma me motivava a me esforçar e não desistir nos momentos mais difíceis.

Aos meus colegas de turma que tornaram as sextas feiras mais prazerosas e produtivas.

Aos meus professores da Ufscar-sorocaba pela paciência, incentivo e conhecimentos passados.

A meus alunos que me incentivaram a continuar até o fim sem deixar meu animo esmorecer nos momentos mais difíceis dessa etapa.

Agradeço Danielle Gottardi, Carolina Golveia e Marcela Sette pelo apoio e incentivo.

A todos da escola estadual "E. E. Profª Maria Aparecida Rechineli Modanezi", pela abertura e disposição, em especial a minha amiga e professora Daniele Góes.

Agradeço principalmente à minha orientadora, professora Dra. Sílvia Maria Simões de Carvalho, pela abertura, confiança, paciência, ensinamentos e apoio durante esse processo. Muito obrigado por ter me aceito como seu orientando.

Faça o seu melhor, na condição que você tem, enquanto você não tem condições melhores para fazer melhor ainda!"

Mario Sérgio Cortella

RESUMO

Uma das maiores dificuldades enfrentadas pelos educadores no ensino de hoje é a falta de interesse por parte dos alunos em conteúdos programáticos da matemática, que muitas vezes é reduzida a um conjunto de técnicas, regras e algoritmos sem nenhuma aplicabilidade ou justificativa. O objetivo deste trabalho é investigar e analisar possíveis contribuições no ensino-aprendizagem de funções tendo como abordagem metodológica a resolução de problemas/investigação matemática utilizando um jogo de caça-tesouro relacionando a teoria das funções com a ideia de criptografia que está presente no cotidiano do aluno.

Palavras-chaves: Aprendizagem. Funções. Criptografia. Ensino.

ABSTRACT

One of the biggest difficulties faced by teachers, nowadays, is the lack of interest from students in math's programmatic contentes, wich, plenty of times, is reduced to a set of techniques, rules and algorithms without applicability or justification. This research's objective is to investigate and analyze some possible contributions to mathematical functions' teach-leraning using, as methodological approach, the resolution of math problems/ investigation utilizing a treasure hunt game, relating mathematical functions theory to the idea of cryptography, wich is part of the students' routine.

Keywords: Learning. Mathematical Functions. Cryptography. Teaching.

Lista de Ilustrações

Lista de Gráficos

Lista de Quadros

Lista de Tabelas

Sumário

1. Introdução

Na atualidade com a globalização e a disseminação da internet o mundo está ao alcance em um simples clique. Nos comunicamos com pessoas do outro lado do mundo com grande facilidade graças as inovações tecnológicas que tornaram nossa comunicação e interação muito mais ágeis.

Operações comerciais pela internet são cada vez mais comuns entre as pessoas. A criptografia, uma arte milenar que vem evoluindo desde antes de Cristo, é o que garante a segurança dos nossos dados nessas operações e interações. Durante o processo histórico de evolução da criptografia foram desenvolvidos vários métodos até se chegar ao método RSA mais utilizado atualmente pelo seu alto grau de segurança gerado pelas suas chaves.

Com a evolução tecnológica e os atrativos da internet os alunos estão cada vez mais desinteressados pelas aulas tradicionais. Isso exige do professor mais criatividade e dedicação na construção de suas aulas.

É preciso oferecer ao educando a oportunidade de um aprendizado com significado, e para isso é indicado nos documentos educacionais vigentes (SÃO PAULO, 2011) que se realize uma atividade prática ou uma contextualização do conteúdo teórico pretendido com o cotidiano do aluno, buscando mostrar a importância desse conhecimento através de sua aplicabilidade.

Entre os conteúdos matemáticos que são vistos pelos alunos do ensino médio um dos mais difíceis é o que aborda sobre funções. O processo ensino aprendizagem deste conteúdo é um desafio necessário e dever dos professores. Criar estratégias de ensino que consigam despertar o interesse e propiciar uma aprendizagem significativa com o desenvolvimento de habilidades cognitivas e socioemocionais é um desafio, uma necessidade e um dever do professor.

Pensando nisso foi criado e aplicado o Caça Tesouro mostrado no capitulo 9 deste trabalho, onde buscamos relacionar o conteúdo funções com a temática criptografia, visando estimular os alunos a participarem da atividade construindo um ambiente propicio para a assimilação do conteúdo proposto.

Assim, iremos testar e discutir a eficácia da atividade e da temática utilizada em relação ao interesse dos alunos e ao aprendizado dos conceitos teóricos pretendidos em comparação a aulas com giz e lousa.

O capítulo 2 apresenta alguns métodos de criptografia, sua importância histórica e a evolução dessa arte milenar. No capítulo 3 teremos algumas propriedades relacionadas aos números inteiros e as operações entre eles, abordam-se também os números primos e alguns métodos básicos de fatoração. As funções são o assunto do capítulo 4 que trás algumas características importantes destas, o ensino de funções nas escolas é apresentado segundo os documentos vigentes que regem a educação no país. No capítulo 5 temos um panorama da criptografia como tema de aula e seus benefícios. No capítulo 6 temos uma atividade prática que envolve brincadeira, criptografia, funções e aprendizado. Os resultados são apresentados e discutidos no capítulo7. O capítulo seguinte é a conclusão do trabalho desenvolvido.

2. Evolução da criptografia durante a história

A criptografia foi usada por diferentes civilizações, com o propósito de ocultar informações sigilosas durante muitas eras. Um dos registros mais antigos da utilização da criptografia foi há 2000 a.C., no Antigo Egito, onde eram usados hieróglifos no túmulo de membros da nobreza egípcia, aos quais a população não tinha conhecimento do seu significado.

O povo sempre teve interesse em codificar mensagens para ocultar seus conteúdos. Na antiguidade, usavam as cifras hebraicas que consistiam em inverter a ordem das letras do alfabeto e usar a nova posição para codificar as mensagens.

Por volta de 500 a.C., surge o Bastão de Licurgo, uma cifra de transposição que consiste em uma fita de couro ou papiro enrolado em um bastão cilíndrico, de modo que a fita fique lado a lado cobrindo todo bastão,depois de enrolado se escreve a mensagem no sentido do comprimento do bastão. Terminada a escrita, desenrolava-se a fita que era transportada como um cinto com a escrita voltada para dentro, o receptador para conseguir ler a mensagem tinha que enrolar essa fita novamente em um bastão de mesmo diâmetro, para que as letras se alinhassem corretamente. Esse método foi muito utilizado pelos espartanos entre governantes e generais de Esparta, era uma grande arma militar auxiliando os espartanos em suas enumeras batalhas.

Em meados de 200 a.C. surge o Código de Políbio (código de substituição) que consiste em substituir cada letra do alfabeto por uma combinação de duas letras, utilizando somente 5 letras do alfabeto. Substituindo as 5 letras do código pelos 5 primeiros algarismos, pode-se representar cada letra por um número de dois dígitos, assim as mensagens poderiam ser transmitidas a partir de tochas de fogo, usadas para sinalizar os números de dois dígitos um em cada mão, passando a mensagem letra a letra.

O código de César (substituição simples) surgiu entre 60 e 50 a.C., era o método utilizado pelo Imperador Julio César (100-44 a.C.) para mandar mensagens secretas a seus generais. Nesse método as letras eram substituídas pela letra que estava a três posições à direita formando um texto sem sentido. Esse código monoalfabético é simples, mas na época poucas pessoas sabiam ler e escrever, sendo assim, o código de César teve grande utilidade para o período [1].

No livro Kama-Sutra escrito na Índia no ano de 400, indica-se as mulheres que saibam algumas artes especiais, entre elas uma espécie de escrita secreta (tipo de criptografia) para que pudessem guardar seus segredos.

A Idade Média (476-1453) foi um tempo difícil para a criptografia, principalmente na primeira metade considerada a idade das trevas na Europa. O conhecimento cientifico foi desvalorizado, sendo uma época escura para a ciência, com falta de novas ideias. Nesses tempos de "escuridão" a criptografia era vista como arte das trevas, e seus praticantes eram perseguidos e condenados, isso provocou a perda de parte do conhecimento que existia sobre criptografia. Um dos poucos sinais de uso da criptografia nessa época era por parte dos monges, como brincadeiras para passar o tempo e se divertirem em seus grupos religiosos.

A Idade de Ouro da civilização Árabe se inicia no ano de 750 com grande desenvolvimento cientifico, elevando o nível do comércio e da indústria, com um gerenciamento eficaz graças a visão dos Califás Árabes de não investir em guerras desnecessárias, mas sim em conhecimentos, fazendo uso da criptografia para se comunicar e proteger suas descobertas [2].

Nessa época surge a criptoanálise, com o método da análise de frequências descrito por al-Kindi (801-873). Esse método consiste em verificar as letras que mais aparecem em textos da língua desejada, e comparar com as frequências dos símbolos do texto criptografado. Depois desse método, criadores e decifradores de códigos vem travando uma guerra incessante.

A Ordem dos Templários, nos anos de 1119 a 1311, utilizou da criptografia com a substituição simples por símbolos retirados da cruz das Oito Beatitudes (emblema da ordem), para trocar informações financeiras e comerciais sem serem descobertos, acumulando grandes riquezas [1].

Em meados do ano de 1300 com o surgimento dos primeiros indícios do Renascimento com novas ideias promovendo a evolução cientifica, artística, política e mudando a visão de mundo, surge o primeiro país a ter uma visão profissional e a considerar como questão de estado o emprego da criptografia, a Itália. Impulsionado pelas relações diplomáticas nesse importante momento histórico, observou-se um grande avanço na criptografia nesse país durante o século XV [2].

Nessa época Leon Battista Alberti, grande renascentista, em 1466 divulga sua nova criação na área da criptografia, a substituição polialfabética, que era realizada através de um disco de cifragem, onde se tinha dois círculos, um dentro do outro, com o maior sendo fixo e o menor móvel (girava). Os discos eram divididos em 24 pedaços iguais, tipo uma pizza, cada pedaço dos círculos continha uma letra do alfabeto, no disco maior as letras eram maiúsculas e em ordem alfabética, no menor (de dentro) eram letras minúsculas e aleatórias.

Para se cifrar uma mensagem, era só escolher uma letra padrão, para o alinhamento da primeira palavra, essa letra era girada no disco menor e encaixada com a letra da palavra desejada no disco maior, depois se olhava a letra desejada da palavra no disco menor, e se marca a letra do disco maior correspondente. O disco tem que ser realinhado para cada letra da palavra chave do texto, depois se repete o alinhamento dessas letras da palavra chave, até acabar o texto, por isso o nome polialfabético, para decifrar é preciso saber a letra chave e a palavra chave, além disso o emitente e o destinatário tem que possuir discos idênticos. Com o disco de Alberti se introduziu a mecanização do processo de cifragem.

Em 1563 surgiu uma nova cifra, a cifra de Della Porta, criada por Giovanni Battista Della Porta, que indicou uma nova estratégia para enganar a análise de frequência, utilizando palavras com erros ortográficos e sinônimos, seu método utilizava da substituição polialfabética com palavra-chave [1].

O império espanhol comandava grande parte do planeta no final do século XVI, o rei Felipe II travava muitas batalhas, e se comunicava com seus generais comandantes, através de uma cifra representada por 500 caracteres, mas essa cifra também foi quebrada pelo matemático Viéte.

No final do século XVI e inicio do século XVII, com o rei Luis XIV, a França assume papel de liderança na criptologia. Surge ai a grande cifra de Luis XIV, ou Grande Cifra de Rossignol, criada por Rossignol e Bonaventure, seu filho. Essa cifra era diferente de todas que já se tinham conhecimento, usava mais de 500 números que eram associados às sílabas francesas, cifra homófona [2].

Também no fim do século XVI, por volta de 1580, surge a cifra de Vigenére, substituição polialfabética com palavra-chave, criada por Blaise de Vigenére, aparentemente eficaz contra a análise de frequência, por causa de sua complexidade. A Europa há usou muito pouco nessa época, mas com a evolução da mecanização, a cifra de Vigenére foi amplamente usada em toda Europa, após 200 anos de sua criação.

A “câmara negra” criada em Viena, em 1750, interceptava todas as correspondências que passavam pela cidade. As cartas eram abertas, copiadas e lacradas novamente para reenvio, como se nada tivesse acontecido. As cópias eram decifradas pelos criptoanalistas. Foi um esquema muito bem-sucedido, eficiente e organizado, prestando serviço as nações aliadas da Europa [2].

Thomas Jefferson em 1795, também contribuiu para a evolução da criptografia, inventando a Cifra de Roda, um mecanismo em forma de cilindro, que facilitava a aplicação da cifra de substituição polialfabética, possibilitando a utilização da cifra de Vigenére por toda a Europa [2].

Em 1844, Samuel Morse revolucionava o mundo da criptografia com a criação do Código Morse e a invenção do telégrafo, com isso a cifragem se tornou uma necessidade, pela facilidade de interceptação e falta de sigilo na troca dessas mensagens. Com a evolução do telégrafo, Marconi inicia o desenvolvimento de uma nova e poderosa ferramenta de comunicação, mais eficiente e sem fios, o rádio [2].

Após uns 300 anos de sua criação, a cifra de Vigenére, que era vista como inquebrável, é desvendada por Charles Babbage em 1854, um matemático e cientista Inglês, que criou grandes máquinas. A mais importante, foi a Maquina Analítica, que era capaz de resolver cálculos impressionantes, mas foi construída somente após a sua morte. Hoje é considerada o modelo mais primitivo do nosso computador.

A criptografia também participou da Primeira Guerra Mundial, com a utilização da cifra ADFGVX criada pelo exercito alemão, em 1918, com uma combinação de substituição e transposição. Depois de pouco mais de 2 meses, o código ADFGVX foi decifrado pelo tenente francês Painvin, com o código descoberto os franceses conseguem decifrar todas as mensagens interceptadas dos alemães, a mais importante revelou o local do ataque a Paris, eliminando o elemento surpresa e reforçando as defesas do local, forçando o exercito alemão a recuar.

Em 1920, os Estados Unidos entram no conflito graças à mensagem alemã, direcionada ao embaixador em Washington, interceptada pelos ingleses e decifrada pelos seus criptoanalistas em 1917 e ficou conhecido como o famoso telegrama Zimmermann.

Lester S. Hill em 1929, cria a cifra de Hill que faz uso da multiplicação de matrizes, sendo um sistema polialfabético de criptografia [1].

Na Segunda Guerra Mundial (1939 – 1945), ressurge uma maquina de cifras, chamada Enigma, criada em 1918 por Arthur Scherbius (alemão), para ser utilizada pelos comerciantes, depois de aperfeiçoada, foi utilizada pela Alemanha Nazista, como importante ferramenta na guerra [1].

Essa maquina usava uma chave simétrica e um método complexo de cifragem. Por segurança se trocava a chave a cada mensagem. Em contraposição, os britânicos criaram as maquinas de Alan Turing e a Colossus, usadas para quebrar os códigos da Enigma rapidamente, dando grande contribuição para a vitória dos aliados.

A criação e utilização do computador no século XX causou uma revolução no mundo da criptografia. Com a evolução das capacidades operacionais dos computadores, foram necessários novos algoritmos para cifrar as mensagens e garantir seu sigilo, um desses algoritmos recebeu o nome de Lúcifer [3].

Logo após algumas modificações, em 1976, o algoritmo Lúcifer ficou conhecido como a cifra de bloco DES (Data Encryption Standard). Foi publicada como padrão de cifragem dos Estados Unidos. Esse processo possuía 19 etapas, com milhões de operações só possíveis de serem realizadas em um computador.

A cifra RSA (iniciais dos criadores) foi criada em 1977, pelos pesquisadores Rivest, Shamir e Adleman, trazia a inovação de uma chave publica/privada. É um dos mais fortes algoritmos criptográficos que a humanidade já viu. Nesse algoritmo, que funciona através dos números primos e aritmética modular temos duas chaves interligadas matematicamente, sendo uma publica para cifragem, outra privada para decifragem, sendo essas chaves assimétricas (não inversa) diferente das chaves anteriores, que eram simétricas [2].

Somente em 1991, Phil Zimmermann liberou o PGP (Pretty Good Privacy), que veio a se tornar a criptografia ideal para uso da população [2].

Os Estados Unidos em 1999 tem seu código de encriptação (DES) quebrado em menos de 1 dia, assim o governo adota um novo código mais seguro e resistente, o Triple-DES [2].

Os estudos e avanços tecnológicos indicam a criação de um computador quântico, que usam fótons para transmitir um fluxo de bits, o que tornará as operações computacionais ainda mais rápidas, o que trará novos desafios para a criptografia.

3. Números inteiros e operações aritméticas

Os números surgiram da necessidade de representação durante a evolução do homem durante os tempos. No começo para contar seus rebanhos os homens das cavernas usavam a correspondência com objetos como pedras, ossos e até mesmo os dedos das mãos, mas esses métodos não garantiam a segurança dessa contagem, pois os objetos poderiam ser retirados e os dedos esquecidos [4].

Com o passar do tempo dessa necessidade surgiu o registro numérico escrito através de riscos ou desenhos nas paredes das cavernas, ossos ou pedras. Mas só por volta de 3500 a.C. que os antigos sumérios e egípcios começaram a usar números escritos com símbolos próprios e seguindo uma organização de escrita.

Foi no antigo Oriente Médio que se fixaram as primeiras civilizações antigas como a mesopotâmica e egípcia. Da interação desses povos surge o comercio onde o uso da contagem, dos números, ou seja, da Aritmética foi de extrema importância [4].

Com a utilização de métodos mais simples para realizar os cálculos do que os já existentes na época (por exemplo, os sistemas gregos e romanos) se obteve a criação dos algarismos indo-arábico, resultando em um avanço na popularização dos cálculos matemáticos.

As primeiras citações sobre os algarismos hindus encontram-se datada por volta de 662 d.C.. Destacou-se nesse sistema de numeração o uso de um símbolo para cada número de 0 a 9, um símbolo para o zero, a utilização de uma base decimal e o valor posicional dos números.

O poder do Clero da época era dominante. Eram eles que ensinavam cálculo quase que exclusivamente. Eles não queriam a popularização do cálculo, pois conhecimento é poder, assim criticaram o método árabe sugerindo que por ser fácil e engenhoso ele seria demoníaco. Logo as pessoas tiveram medo de usar esse método.

Uma parte da população mais especificamente os comerciantes foram aprendendo e se familiarizando com a numeração indo-arábico a utilizando como um código secreto, fazendo assim com que o povo usasse cada vez mais esse método e disseminando esse conhecimento.

Lutero defendendo os quatro evangelhos comerciais (adição, subtração, multiplicação e divisão) foi responsável pela popularização da Aritmética, invadindo assim a vida social da humanidade. Ele propagava que todos os meninos deveriam aprender a calcular.

O poder da igreja católica foi sobrepujado pela expansão do comércio europeu expandindo assim os métodos de cálculo. Os métodos evoluíram conforme as nossas necessidades. Hoje em dia a Aritmética é parte constituinte de nossa vida como cidadão de extrema importância em nosso cotidiano e está presente obrigatoriamente em todos os currículos de ensino do mundo [4].

3.1. Propriedades dos números inteiros $(\boldsymbol{Z})$

Denotamos o conjunto dos números inteiros como:

$$Z = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

onde tem-se definidas as operações de soma $(+)$ e a multiplicação $(\cdot)$, sendo que a soma de dois números inteiros sempre resulta em um número inteiro e o produto de dois números inteiros é sempre um outro número inteiro, essa é uma importante propriedade dos números inteiros:

Propriedade de Fechamento de Z:

$$\forall a, b \in Z \to (a + b) \in Z \;\text{ e }\; \forall a, b \in Z \to a \cdot b \in Z$$

3.2. Propriedades para soma dos números inteiros

I. Comutativa: $\forall a, b \in Z \to a + b = b + a$
II. Associativa: $\forall a, b, c \in Z \to a + (b + c) = (a + b) + c$
III. Elemento neutro: $\exists 0 \in Z / \forall a \in Z \to a + 0 = 0 + a = a$
IV. Elemento simétrico: $\forall a \in Z\ \exists (-a) \in Z / a + (-a) = 0$
V. Lei do cancelamento: $\forall a, b, c \in Z / a + c = b + c \leftrightarrow a = b$.

Para fins de exemplificação faremos apenas uma demonstração [5].

Demonstração propriedade (V):

(ida→) Por hipótese temos que $a = b$ *com* $\forall a, b \in Z$. *Seja* $\forall c \in Z$, *somando c em ambos os lados da igualdade temos:* $a + c = b + c$.

(volta←) Temos por hipótese que $a + c = b + c$, *aplicando o simétrico de c em ambos os lados da igualdade, com* $\forall a, b, c, (-c) \in Z$, *temos:* $a + c + (-c) = b + c + (-c)$, *sendo* $c + (-c) = 0$ *logo* $a = b$.

3.3. Propriedades para a multiplicação dos números inteiros

I. Comutativa: $\forall a, b \in Z \rightarrow a \cdot b = b \cdot a$
II. Associativa: $\forall a, b, c \in Z \rightarrow a \cdot (b \cdot c) = (a \cdot b) \cdot c$
III. Elemento neutro: $\exists 1 \in Z, \forall a \in Z \rightarrow a \cdot 1 = 1 \cdot a = a$
IV. Distributiva: $\forall a, b, c \in Z \rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$
V. Lei do cancelamento: $\forall a, b, c \in Z / a \cdot c = b \cdot c \rightarrow a = b$
VI. $\forall a \in Z \ temos \ que \ a \cdot 0 = 0$

Para fins de exemplificação faremos apenas uma demonstração [5].

Demonstração propriedade (VI):
Aplicando a propriedade do elemento simétrico temos:

$$a \cdot 0 = a \cdot \big(b + (-b)\big) \ com \ \forall a, b, (-b) \in Z$$

$$a \cdot 0 = a \cdot b + (-a \cdot b)$$

Como $a, b \in Z$ *então* $a \cdot b = c, com \ c \in Z,$ *assim temos que* $a \cdot 0 = c + (-c),$ *pela propriedade do elemento simétrico da soma temos que* $c + (-c) = 0,$ *logo* $a \cdot 0 = 0.$

3.4. Comparação entre números inteiros

A comparação vem de uma relação entre dois ou mais números através de uma análise entre estes, assim temos definidas na matemática algumas propriedades que nos auxiliam como:

- **Princípio da boa ordem:** para todo subconjunto $A \in Z$ formado por números inteiros e limitado inferiormente temos um elemento mínimo, ou seja:

$$\exists n_0 \in A / n_0 \leq n, \forall n \in A$$

- **Relação de ordem $(\boldsymbol{R})$:** Seja A um conjunto não nulo e $a, b, c \in A,$ para que R seja uma relação de ordem, as três propriedades devem ser válidas:

i. Reflexiva: $\forall a \in A / aRa$
ii. Antissimétrica: $\forall a, b \in A / aRb \ e \ bRa \rightarrow a = b$
iii. Transitiva: $\forall a, b, c \in A / aRb \ e \ bRc \rightarrow aRc$.

- **Tricotomia:** é a comparação entre dois números que possui três situações possíveis, sendo $a, b \in Z$ então:
  - ✓ $a = b \quad ou$
  - ✓ $a < b \rightarrow b - a \in N \quad ou$
  - ✓ $b < a \rightarrow a - b \in N.$

- **Transitividade:** $\forall a, b, c \in Z.\ Se\ a < b\ e\ b < c \rightarrow a < c$

Demonstração: Sabendo que $\begin{cases} a < b \text{ então } b - a \in N \\ b < c \text{ então } c - b \in N \end{cases}$

Pelo fechamento dos números naturais (a soma de dois números naturais sempre resulta em um número também natural) temos que $(b - a) + (c - b) \in N$, *assim aplicando o elemento simétrico da soma temos* $c - a \in N$, *logo* $a < c$.

Portanto $para\ \forall a, b, c \in Z$ *temos que se* $a < b$ *e* $b < c$, *logo* $a < c$.

- **Proposição 3.4.1:** $\forall a, b \in Z\ e\ c \in N, temos\ a < b \leftrightarrow a \cdot c < b \cdot c.$

Demonstração:(ida→) Por hipótese temos $\begin{cases} a < b \text{ então } b - a \in N \\ c \in N. \end{cases}$; *pelo fechamento do conjunto dos números naturais temos* $(b - a) \cdot c \in N$, *aplicando a propriedade da distributiva obtemos* $b \cdot c - a \cdot c \in N$, *logo* $a \cdot c < b \cdot c$.

(volta←) Temos por hipótese $a \cdot c < b \cdot c$, *pela tricotomia sabemos que somente um dos três casos pode acontecer:* $a = b$ *ou* $a < b$ *ou* $b < a$. *Testando os casos temos:*

Supondo $a = b$ *multiplicando ambos os lados da igualdade por c obtemos* $a \cdot c = b \cdot c$, *o que é falso pela hipótese.*

Supondo $b < a$ *multiplicando ambos os lados da desigualdade por c obtemos* $b \cdot c < a \cdot c$, *o que é falso conforme mostrado na primeira parte da demonstração (mostrado na parte da ida da demonstração).*

Logo pela tricotomia só podemos ter $a < b$.

Portanto para $\forall a, b \in Z\ e\ c \in N, temos\ a < b\ se\ somente\ se\ a \cdot c < b \cdot c.$

- **Proposição 3.4.2:** Entre os números 0 e 1 não existe nenhum número inteiro.
- **Proposição 3.4.3:** Entre dois números inteiros consecutivos, não existe outro número inteiro.

Demonstração: Vamos provar por absurdo. Supondo que $\exists m \in Z/n < m < n+1$, *com* $n \in Z$. *Tendo assim* $S = \{m \in Z/n < m < n+1\} \neq 0$. *Somando o simétrico de n em cada membro da desigualdade temos:* $n + (-n) < m + (-n) < n + 1 + (-n)$, *obtemos* $0 < k < 1$, *sendo* $k \in Z/\, k = m + (-n)$, *pela proposição II sabemos que não existe um número inteiro entre 0 e 1, assim temos que isso é um absurdo. Portanto,* $\nexists m \in Z/n < m < n+1$.

- **Desigualdade triangular:** $\forall a, b \in Z, |a+b| \leq |a| + |b|$

Demonstração: $|a+b|^2 = (a+b)^2 = a^2 + 2ab + b^2 \leq |a|^2 + 2|a| \cdot |b| + |b|^2 = (|a|+|b|)^2$, *assim temos* $|a+b|^2 \leq (|a|+|b|)^2$, *logo pela definição de módulo temos* $|a+b| \leq |a| + |b|$.

3.5. Divisibilidade

Na atualidade vários símbolos são utilizados para representar uma divisão. Graças a um livro de álgebra suíço do século XVII (Teutsche Algebra) escrito por Johann Rahn o símbolo $\div$ é usado para indicar uma divisão [6].

Os autores europeus da época não aderiram ao sinal, preferiram seguir a representação de Leibniz que em 1684 adotou o sinal de dois pontos (:) para indicar uma divisão [6].

A Mathematical Association of América em 1923 sugeriu uma nova e única representação. A representação fracional em vez das outras citadas, mas a sugestão não conseguiu eliminar da aritmética as outras duas representações que eram usadas e até hoje usamos essas três representações citadas para indicar uma divisão [6].

A divisibilidade é um conceito básico e muito importante. Para $\forall a, b \in Z,$ se a divide b, escrevemos $a \mid b$ isso significa que $\exists c \in Z/\, b = a \cdot c$, ou ainda que b é múltiplo de a. Para $a, b, c, d \in Z$ temos algumas propriedades:

I. $a \mid a$

II. $a \mid b \rightarrow a \cdot c \mid b \cdot c$

III. $1 \mid a$

IV. $a \mid 0$

V. $a \mid b$ e $b \mid a \rightarrow a = b$ com $a, b \in N$

VI. $a \mid b$ e $b \mid c \rightarrow a \mid c$

VII. $a \mid b$ e $c \mid d \rightarrow a \cdot c \mid b \cdot d$

Para fins de exemplificação faremos apenas algumas demonstrações [5].

Demonstração III: Sabendo que $1 \mid a$ *com* $a \in Z$, *temos pela definição de divisibilidade que* $\exists c \in Z /\ a = 1 \cdot c$. *Sabendo que 1 é o elemento neutro da multiplicação temos que* $a = c$, *assim* $a = 1 \cdot a$, *logo pelo elemento neutro da multiplicação temos* $a = a$. $\therefore 1 \mid a$.

Demonstração VI: Por hipótese temos que: $\begin{cases} a \mid b \rightarrow \exists f \in Z/b = f \cdot a \\ b \mid c \rightarrow \exists g \in Z/c = g \cdot b \end{cases}$ *e*

Logo substituindo $b = f \cdot a$ *em* $c = g \cdot b$, *obtemos* $c = g \cdot (f \cdot a)$, *pela propriedade da associativa da multiplicação temos* $c = a \cdot (f \cdot g)$, *como* $f, g \in Z$ *temos pelo fechamento dos números inteiros que* $f \cdot g = k$, *com* $k \in Z$ *então* $c = k \cdot a \therefore a \mid c$.

Demonstração VII: Por hipótese temos que: $\begin{cases} a \mid b \rightarrow \exists f \in Z/b = f \cdot a \\ c \mid d \rightarrow \exists g \in Z/d = g \cdot c \end{cases}$ *e*

Então temos $b \cdot d = (f \cdot a) \cdot (g \cdot c)$*pela associativa da multiplicação temos* $b \cdot d = (f \cdot g) \cdot (a \cdot c)$, *pelo fechamento dos números inteiros temos* $f \cdot g = k$, *com* $k \in Z$, *assim* $b \cdot d = k \cdot (a \cdot c)$, *logo* $b \cdot d$ *é múltiplo de* $a \cdot c$ *logo* $a \cdot c \mid b \cdot d$.

3.6. Números primos

Os números primos foram pensados pela primeira vez por Pitágoras, por volta de 530 a.C. e tinham o significado de primários [10]. Um número é chamado de primo quando possui somente dois divisores positivos: 1 e ele mesmo. Assim é dito que eles são indivisíveis e não podem ser escrito na forma de uma multiplicação usando dois números menores que ele mesmo [11].

Os números primos tem grande importância na matemática, pois a partir deles conseguimos escrever todos os outros números usando a multiplicação. Esses números formados pela multiplicação de números primos são os que chamamos de números compostos.

Mesmo com sua aparente simplicidade e seu caráter indispensável, os números primos vêm se mantendo como um dos objetos mais intrigante já estudado pelos matemáticos. Não é possível identificar quando surgirá o próximo número primo, eles não apresentam nenhuma regularidade se escritos em uma lista, não há um padrão observado.

3.6.1. Fatoração

Se um número não é primo então ele é composto, ou seja, pode ser escrito como produto de números primos. O processo utilizado para se determinar os fatores primos de um número composto é chamado de fatoração.

Existem inúmeros algoritmos de fatoração. A eficácia destes depende do tipo de fator que apresenta o número que se deseja fatorar. Se o número é grande fatorá-lo pode ser trabalhoso e demorado. Até hoje apesar dos avanços tecnológicos não se descobriu um algoritmo de fatoração que funcione adequadamente, ou seja, que um computador possa executar em um tempo razoável para qualquer número inteiro, não importe o tamanho.

È dessa dificuldade que se baseiam e se beneficiam os métodos de criptografia mais atuais, como a criptografia RSA [11].

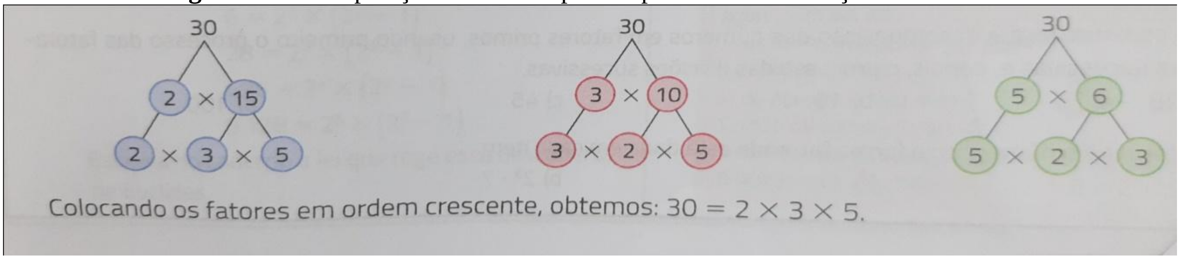
Neste momento vamos citar e dar uma breve descrição dos dois métodos de fatoração mais conhecidos e usados manualmente.

3.6.2. Algoritmo usual

Esse algoritmo se baseia em tentar intuitivamente dividir o número por cada um dos inteiros positivos menores que seu valor absoluto. Não demorou muito para se perceber que se o número N for composto do tipo $N = a \cdot b$ um dos fatores a ou b será necessariamente menor ou igual que $\sqrt{N}$.

Esse método é ensinado nas escolas de ensino básico para se decompor os números em fatores primos, através de divisões sucessivas.

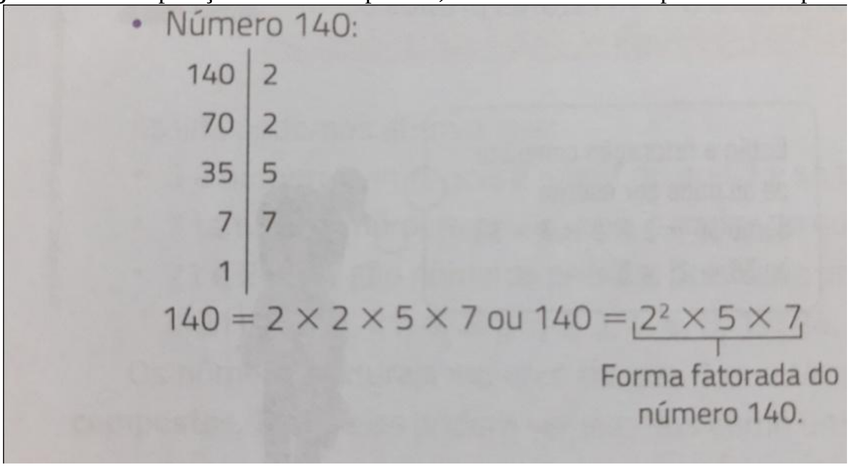
Figura 1: Decomposição em fatores primos por meio de fatorações sucessivas.



Fonte: Teláris matemática, 6º ano: ensino fundamental, anos finais, 2018; pg 113.

Na Figura 1 a decomposição em fatores primos é feita através de fatorações sucessivas por qualquer número natural até não se conseguir fatorar mais, determinando assim que os números presentes no fim do processo são os fatores primos do número inicial. Nesse processo existem vários caminhos como mostrado mas o resultado final é o mesmo para todos.

Figura 2: Decomposição em fatores primos, através de divisões por números primos



Fonte: Teláris matemática, 6º ano: ensino fundamental, anos finais, 2018; pg 114.

A Figura 2, mostra um exemplo de uma fatoração na vertical onde as divisões sucessivas só podem ser feitas por divisores primos até que o resultado seja 1. Esse resultado indica o fim da fatoração e a coluna da direita mostrará todos os fatores primos do número inicial. A ordem em que esses fatores aparecem durante o processo não importa, o importante é a quantidade de cada fator.

3.6.3. Fatoração de Fermat

Esse processo é muito eficaz caso o número *N* tenha um de seus fatores próximo de $\sqrt{N}$. O algoritmo criado por Fermat consiste em tentar encontrar números inteiro x e y, sendo que $N = x^2 - y^2$. Assim teremos:

$$N = x^2 - y^2 = (x + y) \cdot (x - y)$$

Substituindo *x* pelo menor valor inteiro k maior que $\sqrt{N}$, se encontrar uma solução para a igualdade $N = x^2 - y^2$ onde y seja um inteiro você terá encontrado dois fatores de *N*, já que $(x + y)$ e $(x - y)$ são fatores de *N*, caso *y* não seja inteiro repita o processo para $x = k + 1$ e assim por diante até $x = \frac{(N+1)}{2}$, caso não se encontre um *y* inteiro podemos concluir que *N* é um número primo [11].

No caso da criptografia de RSA não se deve escolher dois números primos pequenos e nem muito próximos para a chave, pois se não sua fatoração será viável. O ensino desse método possibilita o entendimento da dificuldade em se quebrar os códigos usados e revela a importância dos conhecimentos matemáticos para nossa segurança.

4. Funções

São instrumentos de representação de situações mundanas, que facilitam o estudo e previsão de situações futuras através da formalização de padrões matemáticos em forma de tabelas, gráficos, equações algébricas ou verbalmente.

Uma função representa a relação de dependência entre dois conjuntos, como por exemplo: para ir de São Paulo a Minas Gerais a uma velocidade A se gasta um tempo B, se for a uma velocidade C, com C > A, gastará um tempo D, com D < B, pois a proporcionalidade entre essas grandezas é inversa, ou seja, temos um conjunto independente (conjunto de entrada) e outro dependente (de saída) que é resultado da transformação realizada pela função a qual o conjunto de entrada foi submetido [7]. Logo podemos definir função como:

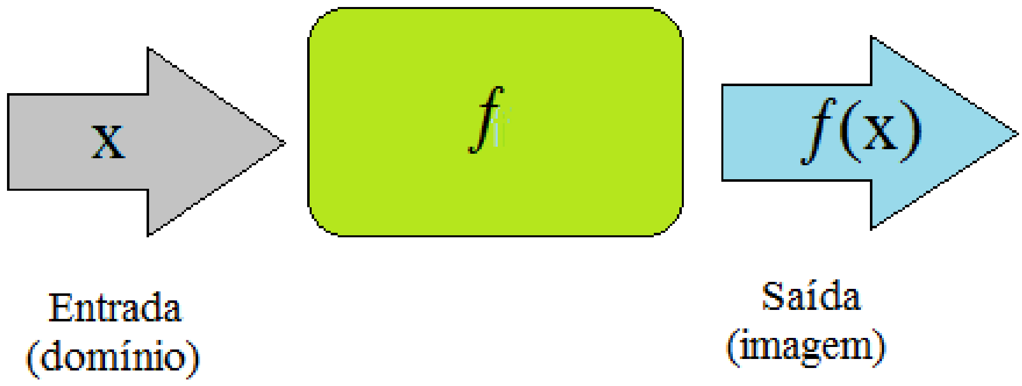
Definição 4.1: Uma função f: A→B, com A e B não vazios, é uma lei na qual cada elemento x pertencente ao conjunto A corresponde unicamente a um elemento y do conjunto B, sendo $f(x) = y$.

O conjunto de entrada A de todos os valores possíveis da função é chamado de **domínio** da função, e o conjunto B de saída ou reposta é chamado de **imagem** da função. O domínio e a imagem podem ser qualquer conjunto de elementos, mas usamos frequentemente para cálculos conjuntos de números reais, ligados ao sistema de coordenadas cartesianas [8].

O domínio de uma função pode ser real, ou seja, todos os números reais são possíveis de serem aplicados a equação da função em questão, ou predefinido em intervalos pelo contexto de aplicação. O domínio e a imagem das funções são intervalos ou combinações destes, que podem ser abertos, fechados ou semiabertos, podem ser finitos ou infinitos.

Uma função f pode ser vista como uma máquina, que transforma a matéria prima (conjunto de entrada: conjunto domínio), em um produto final (conjunto de saída: imagem), assim matematicamente temos: toda vez que inserimos um número cabível a função, ela nos fornece uma única resposta possível.

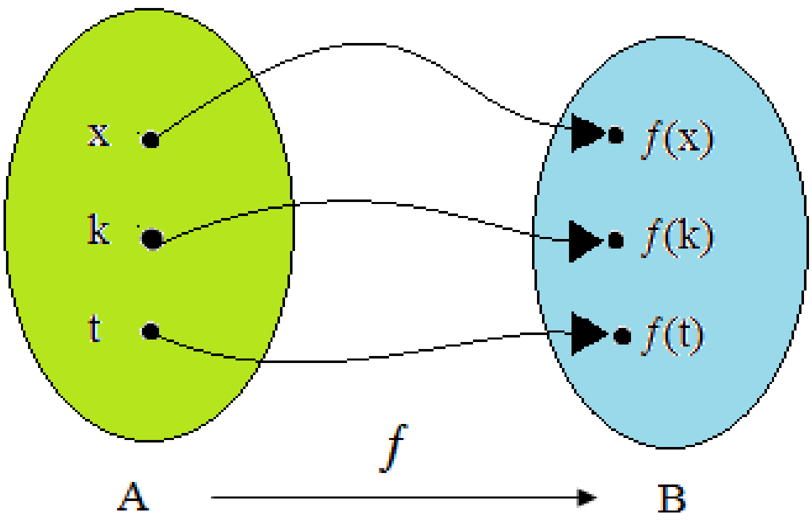
Figura 3: Diagrama que mostra a função como um tipo de máquina.



Fonte: Autor.

Outra forma de representar uma função é como um diagrama de flechas como mostrado na Figura 4, onde cada flecha conecta um elemento do conjunto A (domínio) a um único elemento do conjunto B (imagem).

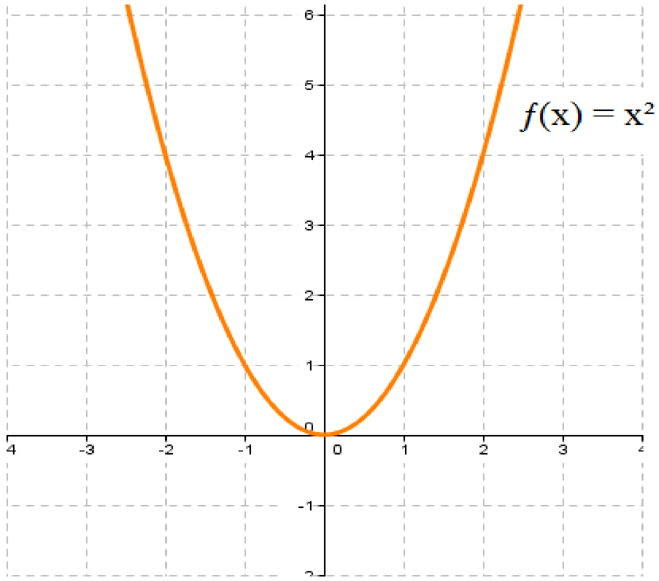
Figura 4: Diagrama de flechas.



Fonte: Autor.

A estratégia mais usada é a construção do gráfico da função. Tendo A como conjunto domínio da função f, teremos então seu gráfico formado pelo conjunto de pares ordenados $\{(x, f(x)) \mid x \in A\}$.Veja o exemplo na Figura 5:

Figura 5: Gráfico da função $f(x) = x^2$



Fonte: Autor.

Veja na Tabela 1, exemplos de domínio e imagem de algumas funções simples, sendo o domínio os valores de x para os quais a função apresente solução.

Tabela 1: Exemplos de funções e seus respectivos conjuntos domínio e imagem.

Função	Domínio (x)	Imagem (y)
y = x	(-10, ∞)	(-10, ∞)
y = x²	(-5, ∞)	[0,∞)
y = 1/x	(-∞, 0) ∪ (0, ∞)	(-∞, 0) ∪ (0, ∞)
y = √x	[0, 100)	[0, 10)

Fonte: Autor.

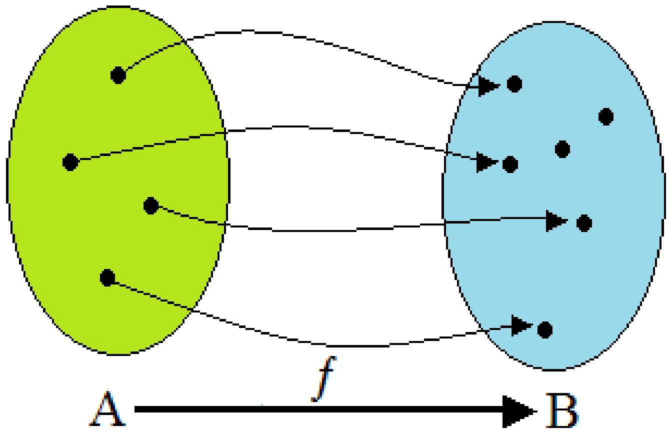
4.1. Função injetora

Uma função f: A→B é injetora ou injetiva quando os valores de entrada de A apresentam valores diferentes de saída em B para todos os elementos, mas pode sobrar elemento no conjunto B, ou seja, não há elemento em B que seja imagem de mais de um elemento do domínio A [9]. Assim temos:

$$x_1 \neq x_2 \; em \; A \rightarrow f(x_1) \neq f(x_2) \; em \; B$$

Na Figura 6 temos um exemplo de função injetora com todos os elementos do conjunto A com um único correspondente no conjunto B.

Figura 6: Exemplo de uma função injetora na forma de um diagrama de flechas.



Fonte: Autor.

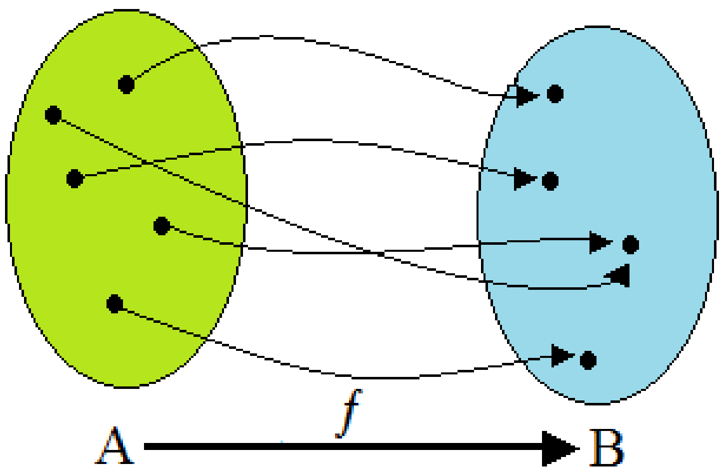
4.2. Função sobrejetora

Uma função f: A→B é sobrejetora ou sobrejetiva quando todos os elementos do conjunto de saída B são correspondentes de algum elemento do conjunto de entrada A, ou seja, todo elemento de B é imagem de pelo menos um elemento do conjunto domínio A [9]. Assim tem-se:

$$Im(f) = B$$

Na Figura 7 é apresentado um exemplo de função sobrejetora onde todos os elementos do conjunto B são correspondentes de pelo menos um elemento do conjunto A.

Figura 7: Exemplo de uma função sobrejetora na forma de um diagrama de flechas.



Fonte: Autor.

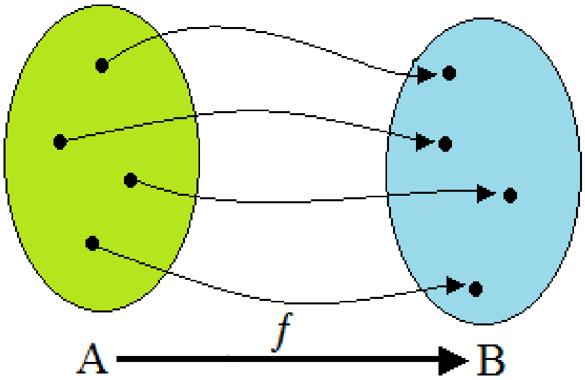
4.3. Função bijetora

Uma função f: A→B é bijetora ou bijetiva quando não há elemento em B que seja imagem de mais de um elemento de A ao mesmo tempo em que todo elemento de B é imagem de pelo menos um elemento do conjunto A, ou seja, se essa função for injetora e sobrejetora simultaneamente [9]. Assim tem-se:

$$x_1 \neq x_2 \; em \; A \rightarrow f(x_1) \neq f(x_2) \; em \; B \;\; \mathbf{e} \;\; Im(f) = B$$

Na Figura 8 é mostrado um exemplo de função bijetora onde todos os elementos do conjunto A tem um único correspondente em B e ao mesmo tempo todos os elementos de B tem um único correspondente em A.

Figura 8: Exemplo de uma função bijetora na forma de um diagrama de flechas.



Fonte: Autor.

4.4. Funções inversas (f^{-1})

Uma função f transforma o domínio x em sua imagem y, assim temos que sua função inversa faz o caminho contrario. Quando aplicamos f^{-1} em y obtemos x como resposta, logo temos que os conjuntos domínio e imagem são invertidos.

Não é toda função que possui inversa para isso ela precisa ser injetora no domínio pretendido, ou seja, se dois valores de entrada são diferentes seus valores de saída devem ser diferentes.

Definição 4.4.1.: Suponha que f é uma função injetora em um domínio D com imagem R. A função inversa f^{-1} é definida por $\boldsymbol{f^{-1}(b) = a}$ se $\boldsymbol{f(a) = b}$. O domínio de f^{-1} é R, e a imagem de f^{-1} é D [7].

4.5. O ensino de funções segundo os documentos vigentes

Em uma sociedade em constante crescimento e evolução, o conhecimento é uma característica imprescindível para os cidadãos do século XXI, já que ele é ferramenta para trabalhar, conviver, exercer a cidadania e para cuidar do ambiente em que se vive. Com o uso intensivo do conhecimento, a qualidade da educação passa a ser um diferencial nessa sociedade, as competências e habilidades desenvolvidas na vida escolar serão decisivas na participação do indivíduo em sua sociedade, como um cidadão crítico e capaz [13].

O ensino médio é a parte final da educação básica onde a matemática deve ser compreendida como parte do conhecimento humano essencial para a formação de todos. Contribuindo para a construção de uma visão de mundo, para ler e interpretar a realidade e desenvolvendo capacidades que serão exigidas deles ao longo da vida social e profissional [12].

De forma contextualizada o ensino da matemática integra e relaciona a outros conhecimentos, desenvolve no aluno competências e habilidades essencialmente formadoras. À medida que instrumentalizam e estruturam o pensamento do estudante o capacitando a interpretar e compreender situações, a se apropriar de linguagens especificas, argumentar, analisar e avaliar, tirando suas próprias conclusões e tomando suas próprias decisões.

O aprimoramento das capacidades de agir, pensar e atuar em sociedade, é um processo de aprimoramento pessoal do indivíduo e depende do desenvolvimento de suas competências e habilidades, assim como atribuir significados e ser percebido, se inserindo no mundo, construindo uma identidade, com autonomia e liberdade. Isso está previsto no currículo do Estado de São Paulo.

O trabalho em grupo é uma estratégia importante para desenvolver as competências. Um aspecto que deve ser valorizado é a importância da comunicação na matemática. A comunicação oral é muito bem desenvolvida em trabalhos em grupo. Nessas ocasiões os alunos aprendem uns com os outros e organizam seus conhecimentos para se fazerem entender perante aos outros, usando a linguagem que esta sendo aprendida e relacionando a outras já adquiridas.

Um dos maiores problemas nesse processo de ensino aprendizagem segundo Neri 2013, é o desinteresse por parte dos alunos durante as aulas, sem o interesse fica difícil desenvolver as competências e habilidades necessárias [14]. O aluno não saber um conteúdo não é o problema, pois é só alguém ensinar. Mas o verdadeiro problema é o aluno não querer aprender. É preciso que o professor estimule o interesse do aluno os motivando a aprender.

Uma das competências essenciais em todas as áreas é a de comunicar, expressar, representar, argumentar, ou seja, as várias formas de linguagens, inclusive as de leitura e escrita. A costumeira abordagem enciclopédica acaba restringindo o aluno, a mero observador passivo. Para se evitar que isso aconteça se deve garantir no processo de ensino aprendizagem algumas interações como [13]:

1- Atividades onde os alunos participem e cooperem entre si e tenham que tomar uma posição em relação ao assunto;

2- Temáticas que relacionem a vivência do aluno com o contexto escolar, antes de sair do seu universo vivencial;

3- Observações que necessitem e desenvolvam a percepção de mundo do individuo e gerem participação e registros relevantes feitas pelos alunos.

Não existe tempo de aula ideal para cada tema proposto. Essa noção de tempo ideal é muito relativa e depende do desenvolvimento de cada turma, da escola e do professor. É sempre possível ensinar significativamente determinado assunto. Cabe ao professor adequar o grau de aprofundamento de acordo com as condições e necessidades do seu publico alvo.

A lei prevê que a relação entre a teoria e a prática aconteça em todas as disciplinas do currículo. Isso é de estrema importância já que uma das causas dos problemas de qualidade de ensino ocorre por causa da dificuldade em relacionar a teoria com a prática, tornando o conhecimento verbalista e abstrato.

Não é só em experimentos de laboratório ou construção de objetos que a relação teoria e prática se faz presente. Ao se compreender como a teoria se aplica em contextos reais ou simulados a relação também se estabelece.

A caracterização dos conteúdos disciplinares como ferramenta para a construção cognitiva do indivíduo traz a necessidade de sua contextualização, uma vez que a falta de relação da teoria com a realidade concreta torna mais difícil a compreensão dos fins a que se destina [13].

É de extrema importância que haja um equilíbrio entre a valorização da cotextualização e o desenvolvimento da capacidade de abstrair o contexto já que ambas são de grande importância para o desenvolvimento. Sem essa capacidade de abstração estaríamos condenados a apenas reproduzir os conhecimentos já existentes, sem novas descobertas.

Tem-se no currículo competências a serem desenvolvidas pelos alunos ao longo do ensino básico. Elas formam três eixos norteadores da ação educacional, que são eles:

- Expressão/compreensão: a capacidade de expressão do eu utilizando múltiplas linguagens e a compreensão do outro como seu complementar. Isso inclui a leitura de textos, tabelas, gráficos e até a compreensão de fenômenos históricos, sociais, econômicos, naturais etc;
- Argumentação/decisão: a capacidade de argumentar, analisar e de relacionar as informações com as relações possíveis, possibilitando a comunicação e a ação comum. Visando nesse processo a tomada de decisão, a proposição e realização de ações efetivas;
- Contextualização/abstração: relação teoria e prática, a capacidade de contextualização dos conteúdos estudados com a realidade, principalmente com o mundo de trabalho. A capacidade de abstração, usar a imaginação e considerar novas perspectivas com potencialidades permite a evolução do conhecimento e a descoberta do que ainda não existe.

Na matemática o conceito de funções é visto como um dos mais importantes já que seus aspectos mais básicos estão presentes nas partes mais simples até as mais complexas dessa ciência.

O estudo de funções é muito mais que fórmulas e incógnitas, ele permite ao estudante se apropriar da linguagem algébrica como sendo a linguagem das ciências. Sendo necessária e imprescindível para expressar relações entre grandezas e representar situações problemas. Construindo modelos descritivos de fenômenos, permitindo diversas conexões na própria matemática e também fora dela.

Logo o foco do estudo de diferentes funções deve estar no conceito de função e em suas propriedades referentes as operações, na leitura e interpretação de seus gráficos e na aplicação dessas funções principalmente no cotidiano do aluno.

O ensino de função pode ser iniciado diretamente pelo seu conceito, descrevendo a dependência entre duas grandezas, partindo de situações contextualizadas descritas algébrica e graficamente. Construindo um saber mais consistente por parte do aluno.

Todo o peso da linguagem excessivamente formal que envolve as funções deve ser minimizado pelo professor. Assim como os estudos sobre funções injetora, sobrejetora, compostas e modulares que devem ser ensinadas, mas sem muita ênfase já que o foco deve estar no conceito de funções, na interpretação destas e suas respectivas aplicações [12].

Normalmente as situações problemas são deixadas para o final do processo ensino aprendizagem. No entanto problemas de aplicação devem ser usados como contexto para a construção de conceitos, possibilitando uma aprendizagem mais significativa ao aluno. Usando exemplos e situações do cotidiano, formas gráficas de outras áreas usadas para demonstrar a relação entre grandezas que estão disponíveis em vários meios de comunicação, explorando esse amplo campo de situações envolvendo funções é possível estruturar de melhor forma o ensino.

No estudo especifico de alguns tipos de função não pode deixar de mostrar além das particularidades as generalidades entre os casos. Mostrando que estes permitem uma visão mais critica e analítica sobre as situações descritas.

Nos Quadro 1, Quadro 2 e Quadro 3 são apresentados os conteúdos e habilidades relacionados a funções exceto as funções trigonométricas, a serem desenvolvidos nas séries em questão segundo o currículo paulista.

Quadro 1: Conteúdos e habilidades de matemática nos 1º e 2º bimestres da 1ª série do Ensino Médio.

1ª série do Ensino Médio		
	Conteúdos	**Habilidades**
1º Bimestre	**Números** Números e sequências • Conjuntos numéricos • Regularidades numéricas: sequências • Progressões aritméticas e progressões geométricas	• Saber reconhecer padrões e regularidades em sequências numéricas ou de imagens, expressando-as matematicamente, quando possível • Conhecer as características principais das progressões aritméticas – expressão do termo geral, soma dos n primeiros termos, entre outras –, sabendo aplicá-las em diferentes contextos • Conhecer as características principais das progressões geométricas – expressão do termo geral, soma dos n primeiros termos, entre outras –, sabendo aplicá-las em diferentes contextos • Compreender o significado da soma dos termos de uma PG infinita (razão de valor absoluto menor do que 1) e saber calcular tal soma em alguns contextos, físicos ou geométricos
2º Bimestre	**Relações** Funções • Relação entre duas grandezas • Proporcionalidades: direta, inversa, direta com o quadrado • Função de 1º grau • Função de 2º grau	• Saber reconhecer relações de proporcionalidade direta, inversa, direta com o quadrado, entre outras, representando-as por meio de funções • Compreender a construção do gráfico de funções de 1º grau, sabendo caracterizar o crescimento, o decrescimento e a taxa de variação • Compreender a construção do gráfico de funções de 2º grau como expressões de proporcionalidade entre uma grandeza e o quadrado de outra, sabendo caracterizar os intervalos de crescimento e decrescimento, os sinais da função e os valores extremos (pontos de máximo ou de mínimo) • Saber utilizar em diferentes contextos as funções de 1º e de 2º graus, explorando especialmente problemas de máximos e mínimos

Fonte: Currículo do Estado de São Paulo: Matemática e suas tecnologias / Secretaria da Educação; p.65.

Quadro 2: Conteúdos e habilidades de matemática nos 3º e 4º bimestres da 1ª série do Ensino Médio.

1ª série do Ensino Médio		
	Conteúdos	**Habilidades**
3º Bimestre	**Relações** Funções exponencial e logarítmica • Crescimento exponencial • Função exponencial: equações e inequações • Logaritmos: definição e propriedades • Função logarítmica: equações e inequações	• Conhecer a função exponencial e suas propriedades relativas ao crescimento ou decrescimento • Compreender o significado dos logaritmos como expoentes convenientes para a representação de números muito grandes ou muito pequenos, em diferentes contextos • Conhecer as principais propriedades dos logaritmos, bem como a representação da função logarítmica, como inversa da função exponencial • Saber resolver equações e inequações simples, usando propriedades de potências e logaritmos
4º Bimestre	**Geometria/Relações** Geometria-Trigonometria • Razões trigonométricas nos triângulos retângulos • Polígonos regulares: inscrição, circunscrição e pavimentação de superfícies • Resolução de triângulos não retângulos: Lei dos Senos e Lei dos Cossenos	• Saber usar de modo sistemático relações métricas fundamentais entre os elementos de triângulos retângulos, em diferentes contextos • Conhecer algumas relações métricas fundamentais em triângulos não retângulos, especialmente a Lei dos Senos e a Lei dos Cossenos • Saber construir polígonos regulares e reconhecer suas propriedades fundamentais • Saber aplicar as propriedades dos polígonos regulares no problema da pavimentação de superfícies • Saber inscrever e circunscrever polígonos regulares em circunferências dadas

Fonte: Currículo do Estado de São Paulo: Matemática e suas tecnologias / Secretaria da Educação. P.66

Quadro 3: Conteúdos e habilidades de matemática nos 3º e 4º bimestre da 3ª série do Ensino Médio.

3ª série do Ensino Médio		
	Conteúdos	**Habilidades**
3º Bimestre	**Relações** Estudo das funções • Qualidades das funções • Gráficos: funções trigonométricas, exponencial, logarítmica e polinomiais • Gráficos: análise de sinal, crescimento e taxa de variação • Composição: translações e reflexões • Inversão	• Saber usar de modo sistemático as funções para caracterizar relações de interdependência, reconhecendo as funções de 1º e de 2º graus, seno, cosseno, tangente, exponencial e logarítmica, com suas propriedades características • Saber construir gráficos de funções por meio de transformações em funções mais simples (translações horizontais, verticais, simetrias, inversões) • Compreender o significado da taxa de variação unitária (variação de f(x) por unidade a mais de x), utilizando-a para caracterizar o crescimento, o decrescimento e a concavidade de gráficos • Conhecer o significado, em diferentes contextos, do crescimento e do decrescimento exponencial, incluindo-se os que se expressam por meio de funções de base e
4º Bimestre	**Números/Relações** Estatística • Gráficos estatísticos: cálculo e interpretação de índices estatísticos • Medidas de tendência central: média, mediana e moda • Medidas de dispersão: desvio médio e desvio padrão • Elementos de amostragem	• Saber construir e interpretar tabelas e gráficos de frequências a partir de dados obtidos em pesquisas por amostras estatísticas • Saber calcular e interpretar medidas de tendência central de uma distribuição de dados: média, mediana e moda • Saber calcular e interpretar medidas de dispersão de uma distribuição de dados: desvio padrão • Saber analisar e interpretar índices estatísticos de diferentes tipos • Reconhecer as características de conjuntos de dados distribuídos normalmente; utilizar a curva normal em estimativas pontuais e intervalares

Fonte: Currículo do Estado de São Paulo: Matemática e suas tecnologias / Secretaria da Educação. p.70.

5. A criptografia como tema de aula

O professor deve ser um agente motivador no processo ensino-aprendizagem instigando a busca de novos conhecimentos pelo educando, tornando suas aulas um local de prazer e descobertas fazendo com que os estudantes sintam-se motivados.

Quando o professor oferece o ensino da matemática de forma dinâmica, atrativa e crítica ele estimula no educando o desenvolvimento do pensamento critico, a confiança de seu potencial mental e o raciocínio lógico, senso de investigação e criação, além do habito de empregar suas competências com autonomia.

Nunca deve-se esquecer de que quando é permitido ao aluno fazer relações, experiências e ter contato com o material concreto isso aumenta suas chances de aprender.

Pensando nisso, a escolha de temas deve ser bem elaborada e planejada visando estimular, permitir e dar condições para que o educando se aprofunde e exercite os conteúdos já trabalhados em séries anteriores, tenham autonomia na resolução das atividades e trabalhem em equipe, aprimorando sua formação acadêmica e social.

Um assunto importante e que atrai olhares no nosso contexto atual é a criptografia. Esse tema vem sendo cada vez mais utilizado em sala de aula, pois acredita-se que sua utilização desperta um algo a mais no educando, motivando-os a aprender os conteúdos matemáticos pretendidos e ajudando o professor a driblar as dificuldades encontradas ao tentar estimular seus alunos.

O tema criptografia acaba despertando a curiosidade e levando a um processo que possibilita ao educando a construção de novos conhecimentos. Logo, esse tema pode ser utilizado como motivador eficiente de atividades didáticas que conseguem revisar, exercitar, fixar e aprofundar os conteúdos matemáticos designados para o ano/série [15].

Para se aplicar atividades que envolvam a criptografia em sala de aula é preciso seguir uma ordem de fatos para que os alunos não se percam do seu principal objetivo, por exemplo, o professor pode iniciar com uma aula expositiva sobre o tema criptografia, mostrando a evolução durante a história da humanidade e seu importante papel na sociedade até os dias de hoje, procurado relacionar o tema com o cotidiano do aluno com aplicações nos dias atuais.

Então, é interessante a realização de uma atividade prática em sala de aula para que o aluno compreenda todo o processo e possibilite o entendimento da atividade a ser realizada e sua relação com o cotidiano, buscando assim uma aprendizagem significativa.

5.1. A criptografia presente no cotidiano

Com os avanços tecnológicos do século XXI o acesso a tecnologia se tronou mais viável a todas as classes sociais. Hoje em dia a maior parte da população utiliza de alguma maneira recursos de comunicação e transações eletrônicas pela internet ou outros. Mas o que garante a segurança dessas interações digitais? É a criptografia.

São as operações, funções, combinações e muitas outras ferramentas matemáticas utilizadas para que a cada mensagem trocada seja gerada uma nova chave de criptografia.

Um aplicativo de troca de mensagens muito usado nos dias de hoje é o WhatsApp, onde as mensagem são criptografadas com um cadeado único onde somente você e o destinatário possuem a chave secreta para abrir e ler a mensagem. Isso ocorre para cada mensagem enviada com uma chave e um cadeado diferente automaticamente.

No sistema de chaves assimétricas se tem a maior segurança criptográfica, onde a chave é protegida por uma outra chave de segurança. Muitas entidades utilizam esse sistema como uma ferramenta para proteção de suas informações e de seus clientes [16].

Quase ninguém pensa na verdadeira função do aparelho que exibe uma sequência numérica e a cada espaço de tempo muda essa sequência de forma constante. Em meados de 2015 os bancos financeiros forneciam a cada cliente um aparelho deste como uma segurança a mais nas transações bancarias, agora é o próprio APP que fornec.

As senhas para sistemas eletrônicos em geral são um bom exemplo de chave de criptografia, como as senhas das contas bancarias por exemplo. A senha ativa o sistema de decodificação sempre que o usuário requeira uma informação.

O mais conhecido e utilizado método de criptografia nos dias atuais é o RSA. Muito utilizado em transações comerciais. É o primeiro algoritmo de chave publica completo, um algoritmo que funciona para criptografia e assinaturas digitais.

Esse algoritmo é fácil de entender. Funciona com base de que é muito difícil fatorar um número que seja o produto de dois números primos com muitos dígitos.

Nesse método se tem uma chave pública, que pode ou não ser do conhecimento de todos, formada pelo produto entre dois números primos grandes que são usados para criptografar a mensagem e uma chave secreta formada por outros números que possibilitam o portador a descriptografar a mensagem. Assim se outra pessoa sem a chave secreta quiser quebrar a criptografia, está terá que fatorar os números enormes para descobrir os números primos envolvidos no processo [16].

Até o momento não existem algoritmos rápidos e eficientes de fatoração para números suficientemente grandes. Quanto maior forem os números primos utilizados, maior será a segurança de sigilo do código RSA. Os números primos servem como base de vários algarismo de segurança.

Sabendo disso podemos entender a importância e a relevância dos números primos para segurança de nossas informações. Pesquisadores investem tempo e dinheiro para descobrir novos números primos cada vez maiores. O ultimo número primo descoberto atualmente tem mais de 22 milhões de dígitos. Essas descobertas de novos números primos cada vez maiores garantem a segurança dos códigos, até que no futuro se consiga criar um algoritmo rápido e eficiente para se fatorar grandes números.

5.2. Os jogos como estratégia de ensino

Os educadores encontram um grande desafio, tornar a matemática atrativa e relevante para os educandos, integrado no mundo de hoje.

A utilização de jogos em sala de aula representa uma atividade lúdica, que mexe com o desejo e o interesse do jogador pela própria ação, que envolve a competição e o desafio que o motiva a conhecer suas possibilidades e limites.

O jogo é uma forma de valorizar o conhecimento prévio do aluno, já que este vai adquirindo autoconfiança, incentivado a questionar e corrigir suas ações, analisar e comparar diferentes pontos de vista, organizar e cuidar dos materiais utilizados. Deste modo a matemática passa de inatingível á acessível, tendo a participação do sujeito na construção do seu próprio saber [17].

O professor precisa de um planejamento organizado e de um jogo que incite o aluno a procurar o resultado, ele precisa ser interessante e desafiador. O jogo deve ser pensado e construído de forma a atingir um objetivo e um conteúdo proposto de forma a possibilitar a consolidação de conhecimentos prévios e propiciando a aquisição de novos saberes.

A possibilidade de criar regras e tomar decisões juntos em um jogo fazem com que o estudante deixe de ser um mero observador passivo e passe a ser um membro ativo no processo de aprendizagem.

Normalmente em sala de aula temos livros, cadernos e lápis, mas um bom jogo encanta, traz fluidez, barulho, alegria e certa vida ao ambiente.

Quando bem planejados e aplicados os jogos possibilitam a construção do conhecimento matemático de forma prazerosa, envolvente e significativa. Essa estratégia, se bem elaborada de acordo com as necessidades de cada turma, desenvolve o interesse e estimula a participação dos estudantes, propiciando uma aprendizagem com significado [17].

6. Aplicação de criptografia no ensino médio

No ensino médio um dos conteúdos matemáticos que mais assusta os estudantes são as funções. Esse terror é causado em grande parte pela má compreensão dentro da sala de aula.

As funções permeiam o nosso cotidiano. Já que vivemos em uma sociedade organizada e em constante mudança, onde o fluxo de informações aumenta em proporção geométrica tornando seu estudo indispensável. Compreender de forma construtiva as definições gerais e específicas das funções através de aplicações conduz o estudante a ver o mundo a sua volta de forma diferenciada e mais clara diante dos saberes matemáticos [16].

Segundo MENEZES e CARVALHO (2010), o aprendizado só é possível quando se relaciona a realidade e as expectativas dos nossos alunos usufruindo dos diferentes recursos para nos auxiliar no processo de ensino aprendizagem da matemática.

Diante destes desafios encontrados em salas de aula todos os dias desenvolveu-se uma atividade prática, o caça tesouro, com o intuito de verificar se a criptografia desperta o interesse dos alunos, e estimula estes no processo de ensino melhorando a aprendizagem em funções, comparado aos métodos tradicionais já utilizados nestes em séries anteriores.

6.1. Descrição da unidade escolar

A unidade escolar em questão E.E. Profª. Maria Aparecida Rechineli Modanezi, que se localiza na periferia da cidade na Rua Pedro Heleodoro Pinto – Bairro: Santa Cecilia, Nº: 524, na cidade de Pilar do Sul-SP, atende ao ensino fundamental 2 e ao ensino médio, funciona nos dois períodos (manhã e tarde), sendo na parte da manhã nove salas de aulas, sendo sete salas do ensino médio e duas salas do ensino fundamental 2, no período da tarde funcionam nove salas do ensino fundamental 2. A atividade foi realizada em uma sala do 3º ano do ensino médio composta por 23 alunos.

Essa unidade escolar funciona em um prédio de dois andares, tem em seu espaço físico uma biblioteca, cozinha, secretaria, diretoria, sala dos professores, uma sala de aula, um pequeno palco, banheiro feminino e masculino, uma pequena cantina e pátio no andar térreo, no andar superior possui oito salas de aula, a sala da coordenação, e a sala do acessa escola com dez computadores, ao lado do prédio de aulas possui-se uma quadra de esportes coberta.

Na equipe de gestão escolar possui uma diretora e uma vice-diretora, possui alem destas um colaborador, que é responsável pelo programa da escola da família que funciona nesta unidade escolar nos finais de semana, possui também um coordenador pedagógico, sendo um responsável pelo E.M e ensino fundamental. Esta unidade escolar ainda conta com 3 funcionários na secretaria, 3 cozinheiras, 3 agentes de organização (inspetores), além dos 25 professores, sendo destes 11 efetivos na unidade escolar.

A unidade em questão possui cerca de 500 alunos, distribuídos nos dois turnos desta maneira: no período da manhã 230 alunos, à tarde 270 alunos.

6.2. Metodologia do Caça Tesouro

Parte 1 (1h e 30min)

Iniciou-se a atividade com uma introdução histórica, com a evolução e contribuição da criptografia para a humanidade, feita em slides com imagens e frases para chamar a atenção com simulação dos métodos de criptografia. Depois dessa parte histórica realizou-se uma atividade introdutória, onde os alunos foram separados em grupos de 4 a 5 pessoas e decodificaram uma mesma mensagem criptografada com o auxilio do professor. A atividade desenvolvida é apresentada a seguir:

Chave utilizada para codificação: $y = x^2 + 4$, essa chave foi fornecida a cada grupo, juntamente com a mensagem codificada. Foi lembrado aos alunos que os números encontrados representam as letras do alfabeto conforme sua posição.

Mensagem codificada: 5 – 173,5,404,29,173,5,404,85,13,5 – 29 – 229 – 5,148,40,5,8,29,404,229 – 13,229,173 – 229 – 293,445,5,148 – 20,29,445,365 – 29,365,13,328,29,488,29,445 – 229 – 445,200,85,488,29,328,365,229.

Resposta: A matemática é o alfabeto com o qual DEUS escreveu o universo. (Pitágoras) Disponível em << https://mensagens.culturamix.com/frases/frases-interessantes-sobre-a-matematica >> acesso em 23/10/2019.

Na Tabela 2 é apresentado o código utilizado para essa chave de codificação. Observe a letra e sua posição no alfabeto e seu respectivo código transformado pela chave $y = x^2 + 4$.

Tabela 2: Códigos para a chave $y = x^2 + 4$.

LETRAS	POSIÇÃO	CODIFICADO

	NO ALFABETO	
A	1	5
B	2	8
C	3	13
D	4	20
E	5	29
F	6	40
G	7	53
H	8	68
I	9	85
J	10	104
K	11	125
L	12	148
M	13	173
N	14	200
O	15	229
P	16	260
Q	17	293
R	18	328
S	19	365
T	20	404
U	21	445
V	22	488
X	23	533
W	24	580
Y	25	629
Z	26	680

Fonte: Autor.

Após a decodificação da mensagem pelos grupos foi realizado um questionário, com o intuito de gerar algumas reflexões e guiar os alunos no propósito da atividade, que é o estudo de funções. Esse questionário foi desenvolvido em forma de conversa com toda a sala. Discutindo os pontos mais importantes e as características mais relevantes da função em questão. Nessa discussão o objetivo foi instigar o aluno a dar sua opinião e construir o conceito teórico, valorizando o conhecimento prévio destes.

Questionário pós-atividade para discussão e estudo:

a) Qual a chave de decodificação da mensagem?
b) Construa com o auxilio de um aplicativo (geogebra) o gráfico das funções de codificação e decodificação da mensagem.
c) Podemos usar qualquer número real nessa chave de codificação?
d) Porque temos na mensagem codificada somente números maiores que 4?
e) Compare o conjunto domínio e imagem das duas funções.

Parte 2: O caça tesouro (1h e 40min)

Realizou-se um caça tesouro, onde as dicas estavam escondidas nas repartições da escola. Os alunos da sala foram separados em grupos (de 4 a 5 pessoas), cada um com uma cor, tiveram que decodificar as mensagens codificadas com as dicas em cada envelope de cores correspondentes a do seu grupo, com ordens diferentes para cada grupo, todos passando pelos mesmos locais com as mesmas dicas e chaves, mas em ordens diferentes para evitar a copia entre os grupos. Utilizando funções variadas como chaves e com suas respectivas inversas para decodificarem as pistas.

A chegada foi no mesmo local para todos, nesse local havia um saco com algumas guloseimas, um saco para cada grupo para que todos fossem premiados pelo esforço e se sentissem motivados a ir até o final.

Antes do início do caça tesouro foram dadas algumas instruções: Vocês vão iniciar uma caça ao tesouro pela escola, para conseguir alcançar seu objetivo trabalhe em grupo e seja rápido ou alguém pode pegar seu tesouro. Siga as pistas, vocês terão que decodificá-las, para isso utilize o alfabeto com a posição das letras como suas numerações correspondentes, exemplo: A = 1, pois ocupa a primeira posição. Escreva a mensagem descriptografada em cada envelope correspondente e entregue todos ao final para retirar seu tesouro. Use seus conhecimentos e construa seu caminho, boa sorte.

O envelope 1 foi distribuído na sala, ele determinou a sequência que cada grupo seguiu já que os caminhos foram diferentes, mas passaram pelos mesmos pontos.

Os outros envelopes foram distribuídos pela escola previamente conforme a organização apresentada na Tabela 3. Nela estão as cores e os números de cada envelope que estavam em cada sala. Essa logística é importante para que todos os grupos passem pelos mesmos lugares em ordens diferentes e consigam chegar ao lugar do tesouro.

Tabela 3: Distribuição dos envelopes.

Cor / Localização	Amarelo	Verde	Vermelho	Azul	Laranja
Início	1	1	1	1	1
Sala 1	3	2	4	5	2
Biblioteca	5	4	2	4	5
Secretaria	2	3	3	3	4
Sala de computação	4	5	5	2	3
Chegada	Diretoria				

Fonte : Autor.

Os envelopes foram colocados em cada sala conforme mostram a Figura 9 e Figura 10.

Figura 9: Envelopes na sala de computação.

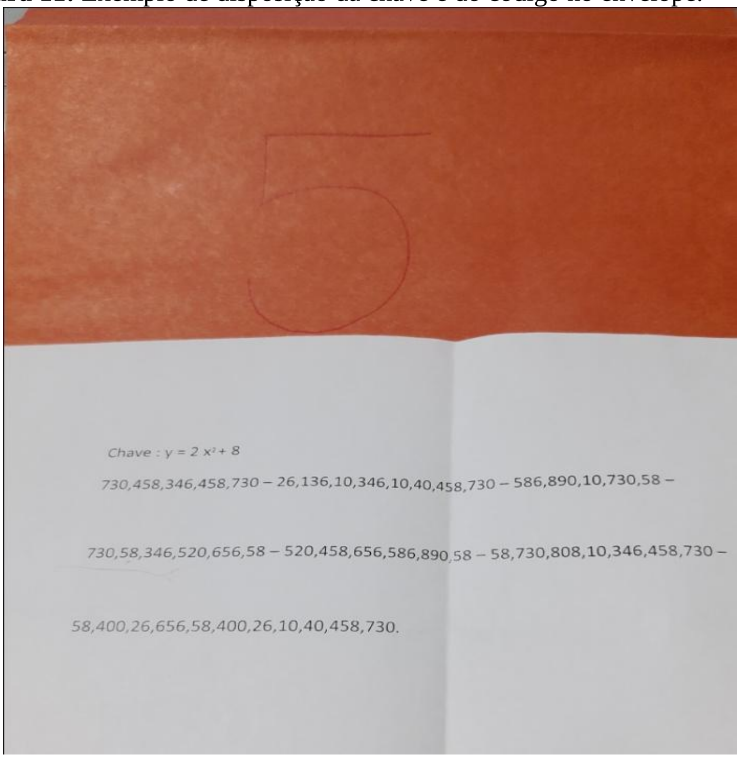
Fonte: Autor.

Figura 10: Envelopes na Sala 1.

Fonte: **Autor**

Em cada envelope foi colocada a chave de codificação e a mensagem codificada (código) correspondente conforme distribuição apresentada na Tabela 3, assim como mostra a Figura 11.

Figura 11: Exemplo de disposição da chave e do código no envelope.



Fonte: Autor.

A seguir são apresentadas as sequências das pistas utilizadas nos envelopes, separadas por cor para cada grupo.

Grupo verde

1- A sala onde iniciamos nossa caminhada juntos.(sala 1)

Chave: $y = 10^X$

10^1 – $10^{19},10^1,10^{12},10^1$ – $10^{15},10^{14},10^4,10^5$ – $10^9,10^{14},10^9,10^3,10^9,10^1,10^{13},10^{15},10^{19}$ – $10^{14},10^{15},10^{19},10^{19},10^1$ – $10^3,10^1,10^{13},10^9,10^{14},10^8,10^1,10^4,10^1$ – $10^{10},10^{21},10^{14},10^{20},10^{15},10^{19}$.

Tabela 4: Código para a chave $y = 10^X$.

LETRAS	POSIÇÃO NO ALFABETO	CODIFICADO
A	1	10^1
B	2	10^2
C	3	10^3
D	4	10^4
E	5	10^5
F	6	10^6
G	7	10^7
H	8	10^8
I	9	10^9
J	10	10^{10}
K	11	10^{11}
L	12	10^{12}
M	13	10^{13}
N	14	10^{14}
O	15	10^{15}
P	16	10^{16}
Q	17	10^{17}
R	18	10^{18}
S	19	10^{19}
T	20	10^{20}
U	21	10^{21}
V	22	10^{22}
X	23	10^{23}

W	24	10^{24}
Y	25	10^{25}
Z	26	10^{26}

Fonte: Autor.

2- Funciona a parte administrativa da escola, e você retira e entrega documentos no balcão. (secretaria)

Chave: $y = 2x + 3$

15,45,31,9,21,33,31,5 – 5 – 35,5,39,43,13 – 5,11,29,21,31,21,41,43,39,5,43,21,47,33 – 11,5 – 13,41,9,33,27,5 – 13 – 47,33,9,13 – 39,13,43,21,39,5 – 13 – 13,31,43,39,13,17,5 – 11,33,9,45,29,13,31,43,33,41 – 31,33 – 7,5,27,9,5,33.

Tabela 5: Códigos para chave y = 2x + 3.

LETRAS	POSIÇÃO NO ALFABETO	CODIFICADO
A	1	5
B	2	7
C	3	9
D	4	11
E	5	13
F	6	15
G	7	17
H	8	19
I	9	21
J	10	23
K	11	25
L	12	27
M	13	29
N	14	31
O	15	33
P	16	35
Q	17	37
R	18	39

S	19	41
T	20	43
U	21	45
V	22	47
X	23	49
W	24	51
Y	25	53
Z	26	55

Fonte: Autor.

3- Onde se pode viajar com sua imaginação sem sair do lugar. (biblioteca)

Chave: $y = 2^X$

32768,16384,16,32 – 524288,32 – 65536,32768,16,32 – 4194304,512,2,1024,2,262144 – 8,32768,8192 – 524288,2097152,2 – 512,8192,2,128,512,16384,2,8,2,32768 – 524288,32,8192 – 524288,2,512,262144 – 16,32768 – 4096,2097152,128,2,262144.

Tabela 6: Códigos para a chave $y = 2^X$.

LETRAS	POSIÇÃO NO ALFABETO	CODIFICADO
A	1	2
B	2	4
C	3	8
D	4	16
E	5	32
F	6	64
G	7	128
H	8	256
I	9	512
J	10	1024
K	11	2048
L	12	4096
M	13	8192
N	14	16384

O	15	32768
P	16	65536
Q	17	131072
R	18	262144
S	19	524288
T	20	1048576
U	21	2097152
V	22	4194304
X	23	8388608
W	24	16777216
Y	25	33554432
Z	26	67108864

Fonte: Autor.

4- Estou entre a cinco e a oito, quase sempre trancada. (sala de computação)

Chave: $y = x^3 - 2$

123,6857,7998,3373,9259 – 123,2742,7998,5830,123 – (-1) – 25,727,2742,25,3373 – 123 – (-1) – 3373,727,7998,3373 – 4911,9259,(-1),6857,123 – 6857,123,2195,4094,5830,123 – 7998,5830,(-1),2742,25,(-1),62,(-1).

Tabela 7: Códigos para a chave $y = x^3 – 2$.

LETRAS	POSIÇÃO NO ALFABETO	CODIFICADO
A	1	-1
B	2	6
C	3	25
D	4	62
E	5	123
F	6	214
G	7	341
H	8	510
I	9	727
J	10	998

K	11	1329
L	12	1726
M	13	2195
N	14	2742
O	15	3373
P	16	4094
Q	17	4911
R	18	5830
S	19	6857
T	20	7998
U	21	9259
V	22	10646
X	23	12165
W	24	13822
Y	25	15623
Z	26	17574

Fonte: Autor.

5- Somos chamados, quase sempre porque estamos encrencados. (diretoria)

Chave : $y = 2x^2 + 8$

730,458,346,458,730 – 26,136,10,346,10,40,458,730 – 586,890,10,730,58 – 730,58,346,520,656,58 – 520,458,656,586,890,58 – 58,730,808,10,346,458,730 – 58,400,26,656,58,400,26,10,40,458,730.

Tabela 8: Códigos para a chave $y = 2x^2 + 8$.

LETRAS	POSIÇÃO NO ALFABETO	CODIFICADO
A	1	10
B	2	16
C	3	26
D	4	40
E	5	58
F	6	80

G	7	106
H	8	136
I	9	170
J	10	208
K	11	250
L	12	296
M	13	346
N	14	400
O	15	458
P	16	520
Q	17	586
R	18	656
S	19	730
T	20	808
U	21	890
V	22	976
X	23	1066
W	24	1160
Y	25	1258
Z	26	1360

Fonte: Autor.

Os outros envelopes tinham as mesmas chaves e mensagens criptografadas, conforme a distribuição abaixo:

Grupo amarelo

1- Funciona a parte administrativa da escola, e você retira e entrega documentos no balcão. (secretaria)
2- A sala onde iniciamos nossa caminhada juntos. (sala 1)
3- Estou entre a cinco e a oito, quase sempre trancada. (sala de computação)
4- Onde se pode viajar com sua imaginação sem sair do lugar. (biblioteca)
5- Somos chamados, quase sempre porque estamos encrencados. (diretoria)

Grupo vermelho

1- Onde se pode viajar com sua imaginação sem sair do lugar. (biblioteca)

2- Funciona a parte administrativa da escola, e você retira e entrega documentos no balcão. (secretaria)

3- A sala onde iniciamos nossa caminhada juntos. (sala 1)

4- Estou entre a cinco e a oito, quase sempre trancada. (sala de computação)

5- Somos chamados, quase sempre porque estamos encrencados. (diretoria)

Grupo azul

1- Estou entre a cinco e a oito, quase sempre trancada. (sala de computação)

2- Funciona a parte administrativa da escola, e você retira e entrega documentos no balcão. (secretaria)

3- Onde se pode viajar com sua imaginação sem sair do lugar. (biblioteca)

4-A sala onde iniciamos nossa caminhada juntos. (sala 1)

5- Somos chamados, quase sempre porque estamos encrencados. (diretoria)

Grupo laranja

1- A sala onde iniciamos nossa caminhada juntos. (sala 1)

2- Estou entre a cinco e a oito, quase sempre trancada. (sala de computação)

3- Funciona a parte administrativa da escola, e você retira e entrega documentos no balcão. (secretaria)

4- Onde se pode viajar com sua imaginação sem sair do lugar. (biblioteca)

5- Somos chamados, quase sempre porque estamos encrencados. (diretoria)

Na secretaria os envelopes estavam guardados com a agente de organização que entregava os envelopes conforme solicitado. No ponto final (diretoria) a vice-diretora ficou na sala e escondeu os tesouros um a um, assim os grupos tiveram que procurar na diretoria.

Lembrando que as pistas foram feitas para essa turma, em outras turmas as pistas devem ser reformuladas de modo apropriado no contexto desses alunos.

Parte 3 (45 minutos)

Na aula após a realização do caça tesouro, foram exploradas as funções utilizadas como chaves na decodificação das pistas, com o auxilio de um aplicativo de celular (geogebra) solicitei aos alunos que construíssem os gráficos e discutimos em conjunto com a sala suas principais características. Explanamos o domínio e imagem e a relação entre esses conjuntos nas funções e suas inversas.

Após essa discussão os alunos responderam ao questionário para diagnosticar o resultado da atividade na aprendizagem e no interesse dos alunos.

Questionário aplicado aos alunos para avaliarem a atividade.

a) A atividade proposta despertou o interesse em participar, estimulando seu aprendizado? ( )sim ( )não

Por quê?

b) A atividade ajudou a compreender e relacionar os conceitos de função e função inversa? ( ) sim ( ) não

c) Com essa sequencia você conseguiu relembrar os conceitos de função aprendidos em séries anteriores? ( ) sim ( ) não

d) Você acha que essa atividade facilitou sua aprendizagem dos conceitos de funções em relação às aulas mais tradicionais de lousa e giz, com resolução de exercícios teóricos? (   ) sim ( ) não
   Por quê?

7. Resultados e Discussões

A atividade aplicada em uma sala do terceiro ano do ensino médio com 23 alunos, no decorrer do terceiro bimestre do ano letivo (agosto e setembro) em concordância com o conteúdo previsto no currículo paulista vigente no momento.

Já na aplicação da parte 1 com o breve resumo de algumas cifras mais importantes durante a história, os alunos se demonstraram interessados no assunto criptografia. Chegaram a relacionar algumas das cifras mostradas com jogos eletrônicos que eles já tinham jogado na internet.

A curiosidade em descobrir o que estava escrito na mensagem motivou os alunos a se esforçarem para decodificar. Diferente dos exercícios simples de resolução de funções, nesta atividade os alunos tinham um propósito mais claro, descobrir o conteúdo do texto. É esse propósito que os motivou no processo a realizarem os cálculos necessários.

Figura 12: Alunos decodificando a mensagem teste.

Fonte: Autor.

Durante o questionário os alunos se mostraram mais interessados, com mais observações e comentários pertinentes do que em aulas tradicionais (expositivas). A motivação destes durante a atividade facilitou a construção dos conceitos teóricos após a realização.

Para a aplicação do caça tesouro primeiro os alunos foram separados em 5 grupos de 4 a 5 pessoas conforme mostra a Figura 13. Optei pela melhor forma de agrupar meus alunos para alcançar o objetivo da aprendizagem proposta, escolhendo como capitães os melhores alunos da sala e eles foram escolhendo seus times, integrante por integrante seguindo uma ordem de sorteio, assim os grupos tinham afinidade para discutir estratégias e seus integrantes tinham diferentes níveis de aprendizagem possibilitando que ajudassem um ao outro. Essa separação foi escolhida, pois a sala em questão tem uma relação de amizade muito homogênea, e já estão acostumados a este tipo de agrupamento nas atividades.

Figura 13: Agrupamento dos alunos.

Fonte: Autor.

Para acelerar e ajudar no processo de cálculo disponibilizei para cada grupo uma calculadora convencional, já que tínhamos números considerados altos para os alunos o que poderia atrasar a realização da tarefa e estourar o tempo da aula prevista.

Os alunos se mostraram muito animados antes, durante e depois da atividade, também observei a atenção de alunos que em aulas mais tradicionais de giz e lousa não demonstram o mínimo interesse, mas que estavam empenhados em realizar os cálculos.

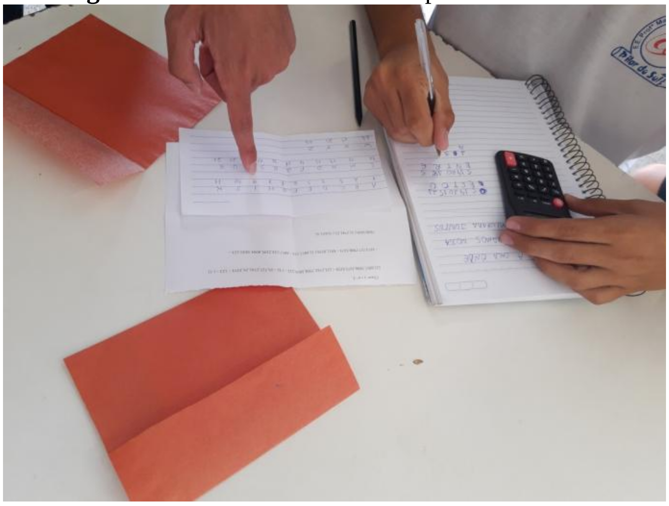
Eles se organizaram e dividiram tarefas dentro dos grupos, construíram tabelas para organizar e facilitar a decodificação como mostrado na Figura 14.

Figura 14: Organização dos alunos na decodificação.

Fonte: Autor.

Alguns alunos acharam que as calculadoras iriam facilitar e muito a decodificação, mas durante o processo perceberam que a calculadora só auxiliava nos cálculos básicos e que os processos que eram mais difíceis precisavam do raciocínio do grupo.

Figura 15: Usando a calculadora para decodificar.



Fonte: Autor.

A interação dos componentes em cada grupo auxiliou os alunos com mais dificuldade no processo de aprendizagem. Para poder ajudar seu grupo eles precisavam saber como resolver os cálculos e quanto mais gente ajudando mais rápido conseguiam decifrar as pistas. Assim os dois lados do processo tinham um interesse em comum, motivando-os a se ajudarem e superando suas dificuldades individuais e em grupo como mostra a Figura 16.

Figura 16: Interação entre os membros do grupo durante o processo.

Fonte: Autor.

No final todos os grupos conseguiram chegar ao tesouro que estava localizado na diretoria. Cada grupo ao seu tempo, cada um de uma vez. Eu observei a chegada na diretoria.

A vice-diretora escondeu os tesouros um de cada vez em lugares diferentes da sala. Quando os alunos chegaram tiveram receio de entrar, por ser a diretoria e pela presença da vice-diretora. Chegaram, olharam e como não viram nada, alguns grupos saíram e conferiram a pista novamente, depois voltaram e perguntaram para ela se era ali mesmo que estava escondido, e começavam a procurar bem cautelosos. Quando encontravam, agradeciam e saiam para dividir as guloseimas com uma expressão de realização e satisfação estampadas no rosto.

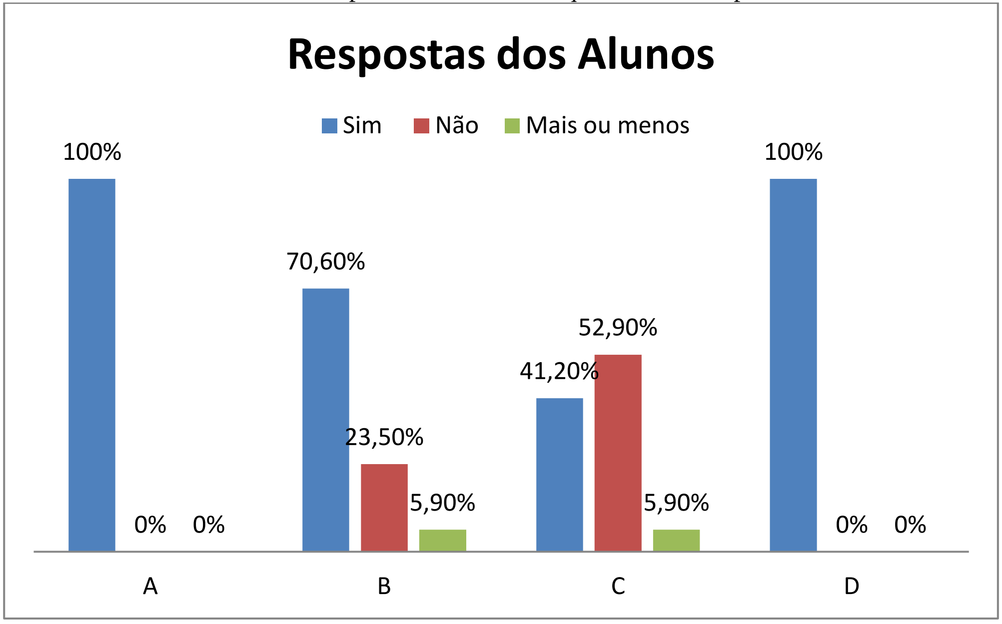
Figura 17: Tesouro encontrado pelos alunos.

Fonte: Autor.

Na parte 3 durante a discussão e estudo das funções utilizadas como chaves pode-se notar que os alunos estavam interessados e relacionaram as características dos gráficos com as propriedades das funções com mais facilidade e entusiasmo na discussão, se sentiram mais pertencentes ao processo de construção e não meros ouvintes.

O Gráfico 1 mostra a resposta dos alunos ao questionário aplicado pós a atividade do caça tesouro.

Gráfico 1: Resposta dos alunos ao questionário da parte 3.



Fonte: Autor.

Observando o Gráfico 1 podemos notar que a atividade proposta despertou o interesse dos alunos, estimulando-os no processo de ensino aprendizagem.

No Quadro 4 são apresentadas algumas respostas dadas pelos alunos no item “a” do questionário (A atividade proposta despertou o interesse em participar, estimulando seu aprendizado? Por quê?).

Quadro 4: Algumas respostas dos alunos ao item “a” do questionário aplicado.

Aluno	Respostas (Porquês)
A	Porque é uma atividade que sai da rotina e mostra o trabalho entre amigos.
B	Porque tinha prêmio KKK, e fez com que a gente se divertisse.
C	Porque é uma coisa diferente, você estava na matéria mais mesmo assim ajudou a sair da rotina.
D	Porque foi uma atividade muito dinâmica e atrativa, além de despertar o interesse de competição, o que estimulou ainda mais, colocou em prática nossos conhecimentos.

E	Porque foi uma atividade diferente do nosso dia a dia escolar.
F	Porque sai da rotina e da menos preguiça.
G	Pois foi um método diferente e divertido de realizar os exercícios.
H	Por ser algo diferente das aulas convencionais, o que chama mais atenção.
I	Pois foi uma atividade que necessitava de todos para ajudar pois cada um tinha seu papel no grupo.
J	Porque você fica curioso em saber o que esta escrito, e também é uma novidade.

Fonte: Autor.

Conforme mostra o Gráfico 1, 100% dos alunos acharam que a atividade despertou o interesse em participar, estimulando seu aprendizado. No Quadro 4 os alunos explicam porque eles tiveram essa opinião. Eles acharam a atividade diferente e divertida, tirando-os da rotina do cotidiano da sala de aula em que estavam acostumados. Um ponto importante apontado por eles foi a interação entre os membros do grupo.

A curiosidade dos alunos em saber quais eram as pistas e quais eram os doces também ajudou a despertar o interesse em participar da atividade, segundo os relatos dos alunos.

No Quadro 5 são apresentadas algumas respostas dadas pelos alunos no item “d” do questionário (Você acha que essa atividade facilitou sua aprendizagem dos conceitos de funções em relação às aulas mais tradicionais de lousa e giz, com resolução de exercícios teóricos?Por quê?).

Quadro 5: Algumas respostas dos alunos ao item “d” do questionário aplicado.

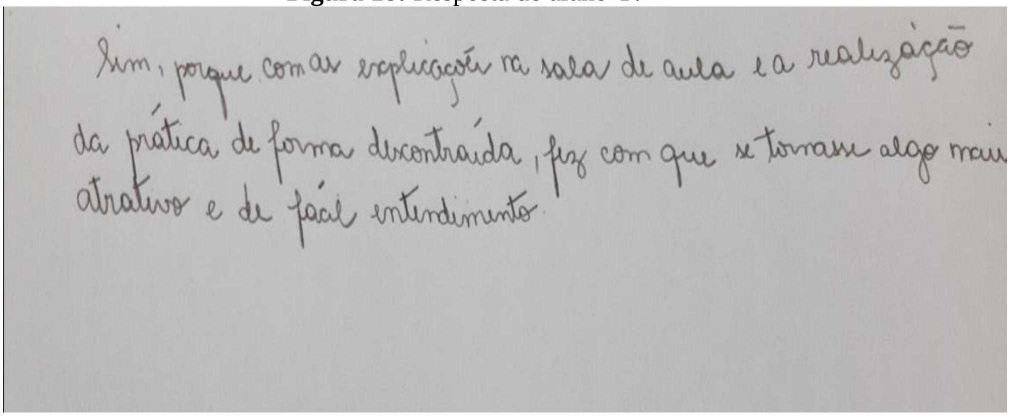
Aluno	Respostas (Porquês)
A	Porque é uma forma diferente e menos enjoativa e cansativa.
B	Porque eu tive vontade de fazer.
C	Porque no mesmo tempo que você está aprendendo, também está se divertindo.
D	Pois ao sair do ritmo de ficar só sentado e copiando, tudo fica melhor.
E	Porque ali você sente vontade de fazer para continuar a brincadeira.
F	Porque houve uma interação maior entre os colegas e por ser dinâmica estimulou muito.
G	Porque é mais interessante ao aluno.
H	Pois por conta do incentivo, o esforço e o interesse é maior.
I	Pois foi algo que estimulou a mente e exigiu participação de todos.
J	Porque você fica mais empenhado e tem a ajuda do grupo para resolver as funções.

Fonte: Autor.

Conforme mostra o Gráfico 1, 100% dos alunos acharam que a atividade facilitou a aprendizagem. Ao analisarmos as repostas no Quadro 5 verificamos que os alunos apresentaram essa maior facilidade por causa do interesse e da vontade deles mesmos em realisar o que foi proposto.

Na Figura 18 e na Figura 19 são mostradas outras respostas dos alunos em perguntas do questionário. Nestas respostas notamos a importância de despertar o interesse do aluno para as atividades a serem realisadas. É esse interesse que possibilita e facilita o aprendizado por parte do aluno. Notamos ainda que os alunos tem consciência de que o aprendizado deles depende de seu interesse nas atividades propostas.

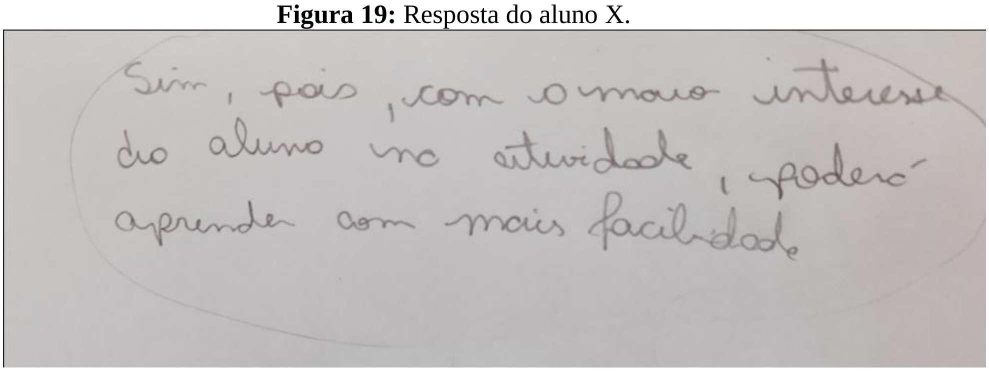
Figura 18: Resposta do aluno Y.



Sim, porque com as explicações na sala de aula e a realização da prática de forma descontraída, fez com que se tornasse algo mais atrativo e de fácil entendimento.

Fonte: Autor.

Figura 19: Resposta do aluno X.

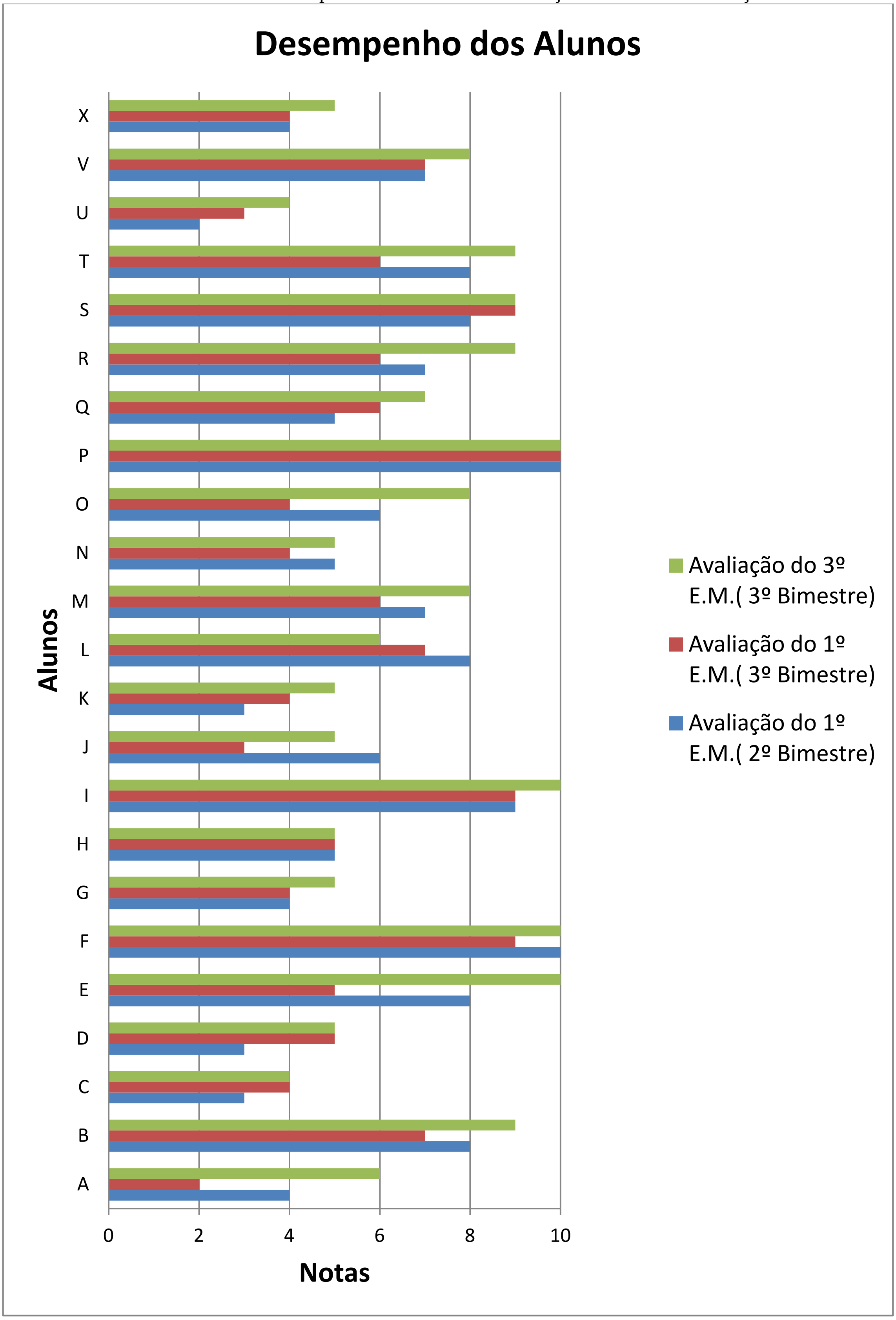


Sim, pois, com o maior interesse do aluno na atividade, poderá aprender com mais facilidade

Fonte: Autor.

O Gráfico 2 mostram o desempenho dos alunos submetidos a atividade proposta em avaliações referentes ao conteúdo funções, anteriores e posteriores a realização do caça tesouro.

Gráfico 2: Desempenho dos alunos nas avaliações escritas sobre funções.



Fonte: Autor.

Observando o Gráfico 2 podemos notar que os alunos apresentaram uma melhora considerável nos resultados das avaliações escritas às quais foram submetidos. Em sua maioria os alunos aumentaram suas notas nas avaliações de mesmo conteúdo programático depois da aplicação do caça tesouro em relação às avaliações anteriores.

Somente 8,7% dos alunos apresentaram uma queda de rendimento em nota nas avaliações escritas analisadas. Os outros 91,3% dos alunos apresentaram melhora ou mantiveram seu rendimento. O número de alunos com notas inferiores a 5 considerados reprovados pelo sistema do Estado de São Paulo caiu.

Alguns alunos disseram não ter conseguido relembrar os conceitos relacionados a funções no item B e C do questionário, apresentando justificativas como:

- Não tem como relembrar o que eu nem aprendi;
- Eu não sabia funções, pois não prestava atenção;
- Mais ou menos, pois eu tenho dificuldade nessa matéria;
- Não, pois só fiz os cálculos que me pediram no grupo;
- Não, pois eu estava apenas apoiando o grupo, então não me esforcei muito.

Isso nos mostra que as respostas negativas não foram referente a atividade em si, mas em relação a situações anteriores ou características pessoais..

Portanto a atividade proposta desempenhou com êxito o seu papel no processo de ensino aprendizagem. Despertou o interesse e mostrou indícios de que melhorou o desempenho dos alunos em questão.

Conclusão

Nesse trabalho apresentamos e testamos uma atividade didática para o ensino de funções tendo como tema de abordagem a criptografia. Verificamos que a atividade proposta atingiu seu objetivo de despertar e estimular o interesse dos alunos melhorando assim seu desempenho na atividade escrita.

A analise dos resultados nos mostra um indício de aumento significativo no desempenho dos alunos na atividade escrita após a aplicação do caça tesouro.

Além disso, o caça tesouro realizado promoveu a interação e a organização entre os alunos, desenvolvendo habilidades socioemocionais previstas nos documentos oficiais e essenciais para um cidadão.

O caça tesouro aplicado se mostrou eficaz na árdua tarefa diária do professor de despertar o interesse dos alunos e chamar sua atenção, além de estimular os estudantes a se esforçarem durante o processo de ensino aprendizagem.

Assim o caça tesouro com a temática criptografia, une duas coisas que devem ser asseguradas aos alunos durante as aulas: atividade prática e contextualização com o cotidiano do aluno, se mostrando eficaz na construção do conhecimento significativo e de um cidadão pleno.

Com base no que foi apresentado notamos a importância do professor desenvolver atividades práticas com seus alunos como jogos e brincadeiras bem planejadas e estruturadas em prol de um objetivo pré-determinado.

Quando estimulados com atividades atrativas e diferenciadas os alunos se atraem e alcançam um aprendizado mais significativo. Cabe ao professor favorecer esse ambiente diferenciado usando sua criatividade.

Um problema que foi notado foi a questão de tempo para o professor elaborar esse tipo de atividade diferenciada para cada turma em que leciona. Não é fácil pesquisar, adequar e elaborar novas atividades para suas turmas isso demanda tempo, coisa que na maioria das vezes os professores por excesso de trabalho não tem.

A falta de colaboração da equipe escolar também pode ser um problema, pois os alunos se deslocaram pelo ambiente escolar em diferentes momentos e lugares. Mas quando bem planejada a atividade, orientada a turma e a equipe escolar a atividade tem tudo para alcançar seu objetivo, como aconteceu neste caso.

Sempre encontramos dificuldades em nosso percurso, mas temos que enfrentá-las da melhor maneira possível. O professor não pode ter medo, ele deve tentar maneiras novas de conduzir os alunos a construir conhecimentos, buscando sempre despertar o interesse e tornar o aprendizado atrativo ao educando.

Apesar das dificuldades encontradas notamos nessa atividade a importância e a necessidade de novas estratégias de ensino, mais criativas e divertidas que despertem o interesse do aluno e o desenvolva como ser pensante.

Com certeza valeu a pena no final da atividade quando notei a melhora dos alunos em geral e a satisfação deles em terem participado ativamente. A alegria e a satisfação dos alunos se tornou a minha e todo tempo gasto para preparar essa atividade foi compensado pelo aprendizado alcançado e pelos sorrisos produzidos.

Referências

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

[2]. COSTA, Celso, e FIGUEIREDO, Luiz Manoel. Introdução à Criptografia. Volume 1. Fundação CECIERJ, consórcio CEDERJ. Rio de Janeiro: UFF / CEP – EB, 2010.

[3]. OLIVEIRA LOPES, Gabriela Lucheze de, e SILVEIRA LOPES, Jaques. Criptografia: a evolução histórica e seu potencial como ferramenta no ensino de teoria dos números nos cursos de licenciatura em matemática. Universidade Federal do Rio Grande do Norte. V Conedu- congresso nacional de educação.

[4]. LORENSATTI, Edi Jussara Candido; Aritmética: um pouco de história; UCS; IX ANPED SUL, Seminário de pesquisa em educação da região Sul, 2012.

[5]. LOPES,Maria Aparecida; Introdução a Teoria dos Números e dos Números Primos; Universidade Estadual da Paraíba, Centro de Ciências Humanas e Exatas, 2011.

[6]. BERLINGHOFF, William P. e GOUVÊA, Fernando Q.; A matemática através dos tempos: um guia fácil e pratico para professores e entusiastas; 2ª edição; São Paulo; editora Edgard Blucher Ltda, 2010.

[7]. THOMAS, George B., WEIR, Maurice D., HASS, Joel. Cálculo, Volume 1, 12ª edição, São Paulo, Pearson Education do Brasil,2012.

[8]. STEWART, James. Cálculo, Volume 1, 5ª edição, São Paulo, Cengage Learning, 2009.

[9]. DANTE, Luiz Roberto. Matemática: contexto e aplicações, Volume 1, 2ª edição, São Paulo, Ática, 2013.

[10]. DANTE, Luiz Roberto. Teláris matemática, 6º ano: ensino fundamental, anos finais. 3ª edição, São Paulo, 2018.

[11]. OKUMURA, Mirella Kiyo. Números primos e criptografia RSA. Dissertação de mestrado, Universidade de São Paulo, São Carlos, 2014.

[12]. BRASIL,Parâmetro Curricular Nacional do Ensino Médio <<http://portal.mec.gov.br/seb/arquivos/pdf/CienciasNatureza.pdf >> acesso em 25/01/2020.

[13]. SÃO PAULO, (Estado) Secretaria da Educação. Currículo do Estado de São Paulo: Matemática e suas tecnologias / Secretaria da Educação; coordenação geral, Maria

Inês Fini; coordenação de área, Nilson José Machado. – 1. ed. atual. – São Paulo : SE, 2011.

[14]. NERI, M. Motivos da evasão escolar. [S.l.], 2013. Disponível: <http://www.institutounibanco.org.br/wp-content/uploads/2013/07/motivos_da_evasao_escolar.pdf> Acesso: 28/02/2020.

[15]. OLIVEIRA JUNIOR, Gilmar Rezende de. Algumas aplicações da criptogrfia no ensino fundamental. Universidade Federal do Tocantins, Dissertação (Mestrado Profissional), Palmas- TO, 2015.

[16]. DANTAS, Andréa de Araujo. A Criptografia no Ensino Fundamental e Médio. Monografia (especialização), Universidade Federal do Rio Grande do Norte, Caicó - RN, 2016.

[17]. MACHINSKI, Alessandra e TROBIA, José. Utilizando jogos como estratégia para o ensino e aprendizagem da matemática. Cadernos PDE, secretaria de educação do Paraná, Volume 1, Paraná, 2016.

[18]. MENEZES, Luiza de Abreu. CARVALHO, Marcos Pavani. Criptografia na sala de aula, X Encontro Nacional de Educação Matemática, Salvador, 2010.