UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE LORENA

SÁVIA CRISTINA VIDAL

**Criptografia como ferramenta educacional no ensino da Análise
Combinatória**

Lorena
2019

SÁVIA CRISTINA VIDAL

Criptografia como ferramenta educacional no ensino da Análise Combinatória

Dissertação apresentada à Escola de Engenharia de Lorena da Universidade de São Paulo para obtenção do título de Mestre em Ciências do Programa de Mestrado Profissional em Projetos Educacionais de Ciências.

Orientador: Prof. Dr. Estaner Claro Romão

Versão Corrigida

Lorena
2019

AUTORIZO A REPRODUÇÃO E DIVULGAÇÃO TOTAL OU PARCIAL DESTE TRABALHO, POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE

Ficha catalográfica elaborada pelo Sistema Automatizado
da Escola de Engenharia de Lorena,
com os dados fornecidos pelo(a) autor(a)

Vidal, Sávila Cristina

Criptografia como ferramenta educacional no ensino da Análise Combinatória / Sávila Cristina Vidal; orientador Estaner Claro Romão - Versão corrigida. - Lorena, 2019.

120 p.

Dissertação (Mestrado em Ciências - Programa de Mestrado Profissional em Projetos Educacionais de Ciências) - Escola de Engenharia de Lorena da Universidade de São Paulo. 2019

1. Análise combinatória. 2. Criptografia. 3. Princípio Fundamental da Contagem. I. Título. II. Romão, Estaner Claro, orient.

Dedico esse trabalho primeiramente a Deus e aos meus alunos, ex-alunos e futuros alunos, sem eles não poderia exercer, com tanto carinho, a missão de ser professora.

AGRADECIMENTOS

Agradeço a Deus por ter me dado força para superar todas as dificuldades e conseguir concluir esse trabalho.

As minha irmãs, Tâmires Vidal e Maria Clara Vidal, por todo carinho e o apoio ao longo dessa jornada.

Ao meu noivo, Romy Antunes, por toda a paciência e compreensão ao longo dessa jornada, sem o seu apoio eu não teria chegado até aqui.

Aos meus amigos Taís Ribeiro e Júlio César Freitas, que acreditaram em mim e me deram forças todos os dias.

Aos meus companheiros de estudos Nadielle Monteiro, Neimar Juliano e Leonardo Melo Souza que fizeram parte dessa etapa da minha vida.

Ao meu orientador Professor Dr. Estaner Claro Romão e a professora Maria da Rosa de Capri, os quais me auxiliaram no desenvolvimento desse trabalho.

Agradeço também a instituição de ensino que abriu as portas para que eu aplicasse o projeto aqui apresentado e aos alunos participantes.

Esse trabalho é meu e de todos vocês que estiveram comigo nessa jornada!

“Se não houver frutos, valeu a beleza das flores; se não houver flores, valeu a sombra das folhas; se não houver folhas, valeu a intenção da semente.”

(Henfil)

RESUMO

Vidal, Sávia Cristina. **Criptografia como ferramenta educacional no ensino da Análise Combinatória**. 2019. 120 p. Dissertação (Mestrado em Ciências) – Escola de Engenharia de Lorena, Universidade de São Paulo, Lorena, 2019.

Este trabalho tem como objetivo verificar a viabilidade da aplicação de uma sequência didática para a Análise Combinatória com ênfase no Princípio Fundamental da Contagem utilizando a Criptografia como ferramenta educacional para o 2º ano do Ensino Médio. Para isso, foi aplicado um projeto, no segundo semestre de 2017, com duração de 26 horas-aula, em uma turma do 2º ano do Ensino Médio, de uma escola pública do interior de São Paulo. Essa proposta de ensino se apropriou da Engenharia Didática como metodologia de pesquisa qualitativa, a qual possibilitou o desenvolvimento de uma sequência didática. Essa por sua vez, foi dividida em cinco etapas, as quais abordaram as técnicas de contagem, sem o uso de fórmulas, por meio da criptografia dos números binários, o código de César e a criptografia presente no filme: O Código da Vinci. Esse estudo foi exposto na feira de ciências, realizada pela escola, pelos alunos participantes do projeto, a qual apresentou um ótimo desenvolvimento. A fim de analisar a evolução da aprendizagem dos alunos participantes foi aplicado um pré-teste e pós-teste, o qual apresentou uma evolução satisfatória, com um ganho educacional, considerado médio. Foi possível perceber também, durante a aplicação do projeto, o desenvolvimento das habilidades de: trabalho em equipe, autoconfiança, oratória, gestão do tempo e autonomia na busca do saber.

Palavras-chave: Análise Combinatória. Criptografia. Princípio Fundamental da Contagem.

ABSTRACT

Vidal, Sávia Cristina. **Cryptography as an educational tool in the teaching of Combinatorial Analysis**. 2019. 120 p. Dissertation (Master of science) – Escola de Engenharia de Lorena, Universidade de São Paulo, Lorena, 2019.

This work aims to verify the feasibility of applying a didactic sequence for Combinatorial Analysis with emphasis on the Fundamental Principle of Counting using cryptography as an educational tool for the 2nd year of High School. For this purpose, a project was applied in the second semester of 2017, during 26 class hours, in a 2nd years class of a public High School, in the São Paulo's country town. This teaching proposal appropriated a didactic engineering as a qualitative research methodology, which enabled a didactic sequence development. This in turn was divided into five stages, which addressed techniques of counting, without using formulas, using a binary numbers encryption, the Caesar's code and the encryption present in the film: The Da Vinci Code. This study was presented at the science fair, held by the school, the students participating in the project, which presented a great development. Aiming to analyze the learning evolution of participating students, a diagnostic evaluation and a final test were applied, which presented a satisfactory evolution, with an average educational gain. It was also possible realize, during the project's application, the development of the skills of: teamwork, self-confidence, oratory, time management and autonomy in the search for knowledge.

Keywords: Combinatorial Analysis. Encryption. Fundamental Principle of Counting.

SUMÁRIO

1 INTRODUÇÃO	17
1.1 Objetivos.....	20
1.2 Apresentação do Trabalho	20
2 ANÁLISE COMBINATÓRIA	22
2.1 Análise Combinatória: Um ramo da Matemática	22
2.2 Ensino e aprendizagem da Análise Combinatória	26
2.3 Análise de conteúdos didáticos	28
2.3.1 Análise dos livros didáticos	29
2.3.2 Análise de dissertações	37
3 CRIPTOGRAFIA	44
3.1 Conceitos básicos de Criptografia	44
3.2 Breve estudo histórico da criptografia	46
3.3 A Criptografia como ferramenta educacional da Matemática	52
4 METODOLOGIA	56
4.1 Metodologia de pesquisa	56
4.1.1 Engenharia Didática.....	56
4.2 Público-alvo.....	58
4.3 Instrumentos de coleta de dados	58
4.4 Atividades desenvolvidas em sala de aula	59
5 DESENVOLVIMENTO E ANÁLISE DOS RESULTADOS	69
5.1 Primeira fase: Análises Preliminares	69
5.1.1 Primeiro encontro.....	69
5.1.2 Segundo encontro.....	73
5.1.3 Resultado da primeira etapa: Análises preliminares	73
5.2 Segunda fase: concepção e análise a <i>priori</i>	78
5.3 Terceira fase: aplicação de uma Sequência Didática	79
5.3.1 Primeira etapa	79
5.3.1.1 Atividade 1	79
5.3.1.2 Atividade 2	81
5.3.2 Segunda etapa	83
5.3.3 Terceira etapa.....	85

5.3.4 Quarta etapa	87
5.3.5 Quinta etapa	92
5.3.6 Pós-teste e correção	94
5.4 Quarta fase: análise a <i>posteriori</i> e validação	98
6 CONCLUSÃO	103
REFERÊNCIAS.....	106
APÊNDICE (S)	112

1 INTRODUÇÃO

O PISA é um Programa Internacional de Avaliação de Alunos, desenvolvido pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE) que promove avaliações internacionais independentes em 70 países dos cinco continentes. Seu objetivo é verificar o nível de conhecimentos e de habilidades e competências associadas a disciplinas do currículo básico. Em relação à Matemática, a edição mais recente para avaliar os alunos nesta disciplina, 2015, trouxe como resultado a média significativamente inferior, de acordo com os dados colhidos pelo Instituto Nacional de Pesquisas Educacionais Anísio Teixeira - INEP. Em seu relatório, este órgão aponta que a pontuação média dos alunos foi de 377 pontos, enquanto a média mundial em Matemática foi de 490 pontos (BRASIL, 2016).

Além dos dados do PISA, temos o Saeb – Sistema de Avaliação da Educação Básica, o qual serve para medir a aprendizagem dos alunos do ensino básico do Brasil. Essa avaliação é aplicada a cada dois anos para os alunos do 5º e 9º ano do Ensino Fundamental e para o 3º ano do Ensino Médio. Este sistema visa analisar os resultados dos conteúdos de Português e Matemática por meio da Prova Brasil, aplicada em todas as escolas públicas. Os resultados de 2017 mostraram que dos 27 estados brasileiros, apenas 5 conseguiram obter ganho de aprendizagem em Matemática no ensino médio. O ganho de Aprendizagem é medido em relação aos resultados das avaliações anteriores, ou seja, se a média ultrapassar os anos anteriores, houve ganho de aprendizagem, caso contrário, não. Os dados de 2017 são comparados com os resultados de 2011, 2013 e 2015 (BRASIL, 2017).

Diante de resultados como esses, torna-se urgente encontrar meios de modificar tal cenário de ineficiência no ensino e no aprendizado em Matemática no Ensino Básico, especialmente para definir métodos diferenciados para que a aprendizagem dos conteúdos da disciplina envolva, de fato, as habilidades e competências necessárias para a formação de um

sujeito capaz de operar e de utilizar o conhecimento matemático nas mais diversas áreas de sua vida (GONÇALVES, 2014).

Dentre os conteúdos de Matemática definidos para o Ensino Médio nos Parâmetros Curriculares Nacionais (BRASIL, 2001) e no Currículo Oficial do Estado de São Paulo (SÃO PAULO, 2011), o de Análise Combinatória tem grande resistência quanto ao seu aprendizado em sala de aula. Diversos fatores levam a essa resistência e discutí-las contribui não apenas para o aprendizado da Análise Combinatória, mas também de outros ramos da Matemática amplamente aplicados em nosso cotidiano, conforme afirmam Roa e Navarro-Pelayo (2001, p. 1):

Os problemas combinatórios e as técnicas para sua resolução tiveram e têm profundas implicações no desenvolvimento de outras áreas da matemática como a probabilidade, a teoria dos números, a teoria dos autômatos e inteligência artificial, investigação operativa, geometria e topologia combinatórias.

Embora classifique a Análise Combinatória como um conteúdo que não oferece grandes dificuldades, Carvalho (2015) afirma que a Análise Combinatória é vista como uma matéria “complexa”, pois a resolução de situações-problema associados a este ramo da Matemática necessita de uma flexibilidade de raciocínio, visto que não há um algoritmo ou modelo pronto para ser seguido, em contrapartida há uma visão em senso comum sobre a disciplina: um conjunto de fórmulas a serem memorizadas e aplicadas em situações-problema parecidos.

Frente a essa problemática, essa pesquisa traz uma proposta para o ensino e a aprendizagem da Análise Combinatória, tema que se encaixa no eixo temático direcionado ao estudo dos números (São Paulo, 2011). Essa proposta se apropria da Criptografia como ferramenta educacional, ou seja, ela utiliza conceitos de Criptografia para introduzir o conceito de Análise Combinatória, a qual vai ser estudada como consequência, e não com o foco principal. Ou seja, a Criptografia, de imediato será o assunto principal e as técnicas de contagem serão aprendidas como meios para solucionar

questões referentes a essa temática, após a introdução desses conceitos, a aprendizagem se voltará ao estudo da Análise Combinatória.

A Criptografia é uma ciência que estuda métodos para esconder o conteúdo de uma mensagem. Essa temática pode proporcionar aos professores a criação de uma ponte entre os conteúdos vistos em sala de aula com sua aplicação no mundo real, pois a Criptografia é uma ciência repleta de Matemática. Singh (2003, p.13) discorre que

Já se falou que a Primeira Guerra Mundial foi a guerra dos químicos, devido ao emprego, pela primeira vez, do gás mostarda e do cloro, e que a segunda Guerra Mundial foi a guerra dos físicos devido a bomba atômica. De modo semelhante se fala que uma terceira Guerra Mundial seria a guerra dos matemáticos, pois os matemáticos terão o controle sobre a próxima grande arma de guerra, a informação. Os matemáticos têm sido responsáveis pelo desenvolvimento dos códigos usados atualmente para a proteção das informações militares. E não surpreende que os matemáticos também estejam na linha de frente da batalha para tentar decifrar esses códigos.

Jesus (2013) afirma que a Criptografia pode ser usada como ferramenta educacional em sala de aula para introduzir, reforçar, revisar e desenvolver conceitos matemáticos, além de possibilitar ao professor desenvolver atividades de codificação e decodificação. Cantoral *et al.* (2000) acrescenta que essa temática possibilita o desenvolvimento de atividades que estimulem o interesse, a vontade em aprender e a curiosidade dos alunos referentes aos conteúdos estudados.

Como apresentado, utilizar a ciência da Criptografia como ferramenta educacional no Ensino da Análise Combinatória no Ensino Médio emerge a possibilidade de ocorrer um aprendizado satisfatório, o qual poderá proporcionar o desenvolvimento de competências, como: Utilizar estratégias matemáticas para interpretar situações em diversos contextos, utilizar os conceitos matemáticos para analisar possíveis resultados e desenvolver o raciocínio matemático na resolução de problemas.

A fim de verificar essa proposta, desenvolvemos essa pesquisa com o uso da Engenharia Didática como metodologia de pesquisa qualitativa.

Artigue (1996) a descreve como um processo empírico que intenciona conceber, realizar, observar e analisar as situações didáticas. Nessa metodologia o professor, com base em estudos teóricos, propõe uma sequência de aulas, organizadas e adaptadas a certa população de estudantes, a fim de produzir um material didático, que seja eficiente no processo de ensino e aprendizagem.

Sendo assim, esse trabalho propõe uma sequência didática do conteúdo de Análise Combinatória com o uso da Criptografia como ferramenta educacional, que foi aplicada em uma turma do 2º ano do Ensino Médio, composta por 22 alunos de uma escola pública do interior do Estado de São Paulo.

1.1 Objetivos

Este trabalho tem como objetivo geral analisar a viabilidade de implementar uma sequência didática para o processo de ensino e de aprendizagem da Análise Combinatória utilizando a Criptografia como ferramenta educacional. Para isso, foram definidos os seguintes objetivos específicos: Estudar as estratégias utilizadas no processo de ensino e de aprendizagem da Análise Combinatória e criar e aplicar uma sequência didática relacionando Criptografia e Análise Combinatória baseada no Princípio Fundamental da Contagem (PFC).

1.2 Apresentação do Trabalho

Esse trabalho aborda o conceito de Análise Combinatória em uma perspectiva diferenciada, ou seja, utilizando a Criptografia como ferramenta educacional, a fim de obter um aprendizado satisfatório.

O Capítulo 2 apresenta um estudo sobre a teoria da Análise Combinatória, a importância desse ramo da Matemática e um breve estudo sobre o atual ensino e aprendizagem desse conteúdo.

O Capítulo 3 aborda o conceito de Criptografia, faz um breve estudo histórico e a sua relação com o ensino básico de Matemática.

O Capítulo 4 traz conceitos sobre a metodologia de pesquisa, detalhes sobre o público beneficiado pela aplicação do projeto, e expõe as etapas desenvolvidas na sequência didática utilizada.

O Capítulo 5 se refere ao desenvolvimento de cada etapa da engenharia didática analisando, de forma linear os seus respectivos resultados.

O último capítulo traz a conclusão, sendo ela, uma análise geral do trabalho aqui apresentado.

2 ANÁLISE COMBINATÓRIA

2.1 Análise Combinatória: Um ramo da Matemática

De acordo com os Parâmetros Curriculares Nacionais (BRASIL, 2001), o ensino da Análise Combinatória é recomendado a ser estudado no 2º ano do Ensino Médio. Nas escolas estaduais de São Paulo esse tema é abordado de acordo com o referido documento citado, sendo apresentado no 3º bimestre.

Pode-se apresentar a Análise Combinatória como um ramo da Matemática que estuda as quantidades possíveis de agrupamento de um conjunto finito de elementos, de acordo com a regra dada (SÃO PAULO, 2017). Na definição de Iezzi e Hazzan (1977, p. 1-E)

A Análise Combinatória visa desenvolver métodos que permitam contar o número de elementos de um conjunto, sendo estes elementos, agrupamentos formados sob certas condições.

Analisando isoladamente as definições aqui apresentadas para este tema, surge o questionamento: Por que destinar um ramo da Matemática para estudar no Ensino Médio a contar?

Pois bem, inicialmente, o estudo das técnicas de contagem, parece ser desnecessário, pois, contar não é um trabalho complexo, entretanto esta visão será válida apenas se o número de elementos a serem contados for pequeno, caso contrário, esse trabalho torna-se praticamente impossível sem o uso de técnicas matemáticas, devido à exaustão e a enorme probabilidade de cometer falhas imperceptíveis (IEZZI; HAZZAN, 1977). Sendo assim, torna-se necessário, destinar-se uma parte da Matemática ao estudo sobre os problemas de contagem, visto a quantidade de problemas, presentes no mundo atual, que envolve esse tema.

A seguir são expostas duas situações problemas, retiradas de Dante (2008), para exemplificar o que foi dito acima, ou seja, um exercício sobre Análise Combinatória em que o primeiro não necessita de técnicas matemáticas e outro, é fundamental.

Exemplo 1:

De quantas maneiras diferentes, pode-se vestir uma pessoa que tenha quatro camisas, sendo elas: rosa, vermelha, azul e verde e duas calças, sendo elas: preta e branca?

Resolução:

Combinando os elementos, um a um, chegamos à conclusão de que há oito possibilidades de combinações diferentes de vestuário.

Evidentemente, é perceptível que esse exercício é possível ser resolvido sem o uso de técnicas matemáticas, apenas combinando os elementos.

Entretanto com o uso das estratégias da Análise Combinatória, há um caminho mais curto, sendo ele a aplicação do Princípio Multiplicativo, ou também conhecido como Princípio Fundamental da Contagem, que diz:

Se um evento é composto por duas etapas sucessivas e independentes de tal maneira que o número de possibilidades na primeira etapa é **m** e para cada possibilidade da primeira etapa o número de possibilidades na segunda etapa é **n**, então o número total de possibilidades de o evento ocorrer é dado pelo produto **mn**". (DANTE, 2008, p. 284).

Para aplicar essa relação, vamos considerar o número de possibilidades da escolha da camisa como "m" e o número de possibilidades de escolha da calça como "n". Teremos então:

$$m = 4 \text{ e } n = 2 \quad \therefore \quad 4 \times 2 = 8 \text{ possibilidades}$$

Exemplo 2:

Em um sistema de emplacamentos de carros, no qual são utilizadas três letras e quatro algarismos, exceto placas que contenham a sequência 0000, quantos veículos podem ser emplacados?

Resolução:

Consideraremos **C** o conjunto de todas as possíveis placas de carros de acordo com o sistema apresentado no exemplo:

$$C = \{ \text{AAA 0001, AAB 0011, ABB 1111, ..., ZZZ 9999} \}$$

Nota-se que nesse exemplo, listar todas as combinações torna-se exaustivo e com grandes possibilidades de falhas, pois existem muitas combinações de placas de carros, sendo necessária a utilização de técnicas matemáticas para a resolução desse exemplo. Para isso, utiliza-se novamente o Princípio Multiplicativo. Aqui considera-se o número de possibilidades da escolha das letras como **m** e o número de possibilidades da escolha dos dígitos como **n**, e assim tem-se:

$$m = 26 \text{ e } n = 10$$

Placas de carros

Nesse exemplo é importante perceber a ordem pré-estabelecida no enunciado, que diz: exceto placas que contenham a sequência 0000. Para iniciar calcula-se a quantidade de todas as possíveis placas de carros que contenham 3 letras e 4 algarismos, inclusive as que possuem a sequência 0000:

$$26 \times 26 \times 26 \times 10 \times 10 \times 10 \times 10 = 175\,760\,000$$

Em continuidade, calcula-se todas as possíveis placas de carro que contenham 3 letras e 4 algarismos, sendo esses algarismos, somente os dígitos 0000, nesse caso, a etapa da escolha dos números n passa a ser 1, pois busca-se somente um único dígito, sendo ele o número 0. Dessa forma, tem-se:

$$m = 26 \text{ e } n = 1$$

$$26 \times 26 \times 26 \times 1 \times 1 \times 1 \times 1 = 17\,576$$

Como não estão sendo buscadas as placas com a sequência 0000, subtraí-se a quantidade de possibilidades de esse fato ocorrer com o total de placas possíveis:

$$175\,760\,000 - 17\,576 = 175\,742\,424$$

Resposta: Logo, tem-se que a quantidade de carros que podem ser emplacados de acordo com a regra pré-estabelecida é 175 742 424.

O segundo exemplo foi uma simples questão que necessitou da utilização das técnicas matemáticas para “contar”, porém existem muitos outros tipos de problemas que necessitam do conceito de combinatória. Morgado et al. (1991) afirma que Análise Combinatória, trata vários outros tipos de questões, e além de Combinações, Arranjos e Permutações possui outras técnicas, como: o Princípio da Inclusão e Exclusão, o Princípio das Gavetas de Dirichlet, as Funções Geradoras e a teoria de Ramsey.

2.2 Ensino e aprendizagem da Análise Combinatória

É comum ouvir dos alunos que a disciplina de Matemática é complicada, difícil e é uma matéria para poucos, o argumento mais usado é que a maioria dos conteúdos vistos nas escolas não são aplicáveis no dia-a-dia, fato que dificulta o entendimento, pois dessa forma, o aprendizado da Matemática não possui significado. Entretanto, a Análise Combinatória é um tema que desde a introdução até a conclusão de seu estudo, são abordadas situações presentes no cotidiano, como: as possíveis quantidades de combinações de roupas, as quantidades possíveis de placas de carros, números de telefone, possíveis combinações em jogos de azar, entre outros, e mesmo assim, esse assunto causa grandes dificuldades, tanto no seu ensino, quanto na sua aprendizagem. Perante a essa contradição, surge o questionamento: Por que a Análise Combinatória apresenta-se como um tema tão desafiador aos professores e alunos?

Para Morgado et al. (1991), um dos encantos da Análise Combinatória está nos problemas, que muitas vezes, pelo enunciado, aparentam ser de uma simples solução, entretanto é necessária uma alta dose de criatividade e certa engenhosidade para resolvê-los. Essa afirmação nos direciona a uma possível resposta para a pergunta anterior, a qual nos faz perceber que a dificuldade em Análise Combinatória pode estar ligada a maneira como a Matemática vem sendo ensinada, ou seja, de forma mecanizada.

Muitos estudantes possuem dificuldades em Matemática pela maneira que é ensinada, isto é, por meio de exemplos e algoritmos memorizados, e qualquer problema que fuja desses padrões se torna de solução impossível aos olhos dos estudantes (GONÇALVES, 2014). Sendo assim, quando os alunos deparam-se com exercícios de contagem, acabam encontrando dificuldade para desenvolver a engenhosidade e a criatividade citada por Morgado et al. (1991), pois essa competência é pouco desenvolvida nos alunos.

Normalmente, o que vemos em sala de aula, são padrões educacionais nos quais a teoria matemática é exposta de forma breve, seguida da resolução de problemas modelos, nos quais os estudantes os usarão como base para responder os próximos exercícios; fato que não favorece a inteligência lógico-matemática. Antunes (2012, p. 92) explica que:

A inteligência lógico-matemática está ligada à competência em compreender os elementos da linguagem algébrica e numérica, permitindo aos que a possuem em nível elevado ordenar símbolos numéricos e algébricos, assim como noções gerais sobre quantidades e reflexões que envolvem análises de espaço e tempo.

Mello (2017) acrescenta que o grande obstáculo na aprendizagem da Análise Combinatória está associado à forma como esse estudo é dirigido, ou seja, por livros didáticos que modelam as diferentes formas de contagem, por meio de seus rótulos, induzindo o discente a ideia de que todo o problema de Análise Combinatória se resume a tarefa de identificar qual o tipo de caso: Arranjo, Combinação ou Permutação, o problema se refere, para em seguida aplicar a fórmula correspondente. Hariki (1996, p. 29) afirma:

Problemas combinatórios são usualmente considerados difíceis pela maioria dos alunos e professores de matemática. Talvez a principal dificuldade seja a da conexão correta entre o problema dado e a teoria matemática correspondente. É difícil determinar se o problema combinatório dado é um problema de arranjo, de permutação ou de combinação, ou então se é suficiente usar diretamente o princípio multiplicativo.

Além disso, Mello (2017) acrescenta que as fórmulas apresentam um caminho mais curto e imediato, entretanto dificulta o senso crítico e criativo do estudante, prejudicando um raciocínio combinatório, pois aluno se condiciona a enxergar a Matemática como um conjunto de fórmulas, resumindo a apenas, saber aplicá-las. De acordo com os Parâmetros curriculares nacionais de Matemática (BRASIL, 1999, p. 54):

A Contagem, ao mesmo tempo que possibilita uma abordagem mais completa da probabilidade por si só, permite também o desenvolvimento de uma nova forma de pensar em Matemática denominada raciocínio combinatório. Ou seja, decidir sobre a forma mais adequada de organizar números ou informações para poder contar os casos possíveis não deve ser aprendido como uma lista de fórmulas, mas como um processo que exige a construção de um modelo simplificado e explicativo da situação.

Abordar o conteúdo com foco no Princípio Multiplicativo não exclui a apresentação e até mesmo o uso das fórmulas utilizadas em contagem, mas proporciona ao aluno a percepção de padrões nas resoluções dos exercícios, ou seja, a dedução das fórmulas, compreendendo assim, que essas são ferramentas que o auxiliarão caso necessário, além da liberdade que o estudante terá para decidir qual método irá utilizar - fórmulas ou Princípio Multiplicativo.

Em uma pesquisa online, realizada por Gonçalves (2014) intitulada “Aprendendo Análise Combinatória”, aplicada a alunos do terceiro ano do Ensino Médio e recém-formados, revela que 63%, dos participantes aprenderam Análise Combinatória por meio da aplicação de fórmulas e 37%, pelo Princípio Multiplicativo e Aditivo. A maioria dos entrevistados acrescentaram comentários sobre a preferência pelo Princípio Multiplicativo, justificando como menos confuso e livre de uma “decoreba”.

2.3 Análise de conteúdos didáticos

Apresenta-se aqui, uma breve análise dos livros didáticos e dissertações desenvolvidas sobre a Análise Combinatória, sem a intenção

de julgá-las, mas sim, proporcionar uma visão sobre como esse tema vem sendo abordado no ensino básico.

2.3.1 Análise dos livros didáticos

Foram selecionados três livros, do segundo ano do Ensino Médio, para análise, sendo eles:

(i) Matemática - Ciência e Aplicações. Escrito por Gelson Iezzi, Osvaldo Dolce, David Degenszajn, Roberto Périco e Nilze de Almeida. Editora Saraiva, 9ª edição, 2016.

(ii) Matemática Paiva. Escrito por Manoel Paiva. Editora Moderna, 3ª edição, 2015.

(iii) Conexões com a Matemática. Obra coletiva concebida, desenvolvida e produzida pela editora Moderna, 3ª edição, 2016.

A escolha por essas três obras se deu por serem os livros utilizados na escola onde se realizou a pesquisa prática aqui apresentada, sendo eles, obras indicadas pelo PNLD (Programa Nacional do Livro Didático).

O livro *Matemática – ciência e aplicações* - aborda a Análise Combinatória no seu décimo capítulo, no qual é subdividido nos seguintes tópicos:

- Princípio fundamental da contagem;
- Fatorial de um número;
- Agrupamento simples;
- Permutações;
- Arranjos;
- Combinações;
- Permutação com elementos repetidos;
- 1º caso: Apenas um elemento se repete;
- 2º caso: Dois elementos diferentes se repetem;
- Caso geral.

Ao introduzir o Princípio Fundamental da Contagem o livro apresenta quatro problemas de contagem, sem a resolução, com a finalidade de mostrar quais os tipos de problemas a Análise Combinatória procura estudar. Em seguida são apresentadas mais quatro situações problemas,

distintas das anteriores, porém resolvidas pelo diagrama de árvore, ou seja, são listadas detalhadamente todas as possíveis respostas para o problema proposto, seguido da definição formal do Princípio Fundamental da Contagem. Após a definição, são apresentados três exemplos resolvidos pela estratégia matemática do PFC e para finalizar esse tópico são propostos vinte e sete exercícios.

O Fatorial de um número é definido de maneira direta, faz-se uma breve explicação sobre a utilização da multiplicação de números naturais e consecutivos no PFC, seguido da definição de Fatorial, para esclarecer seu cálculo, são expostos seis exemplos do cálculo de números pequenos. Os autores apresentam, por meio de um exemplo, uma simplificação de expressões envolvendo Fatorial de um número e outro sobre equações, utilizando também esse conceito. Para finalizar, são propostos sete exercícios.

O tópico que aborda os agrupamentos simples: Permutação, Arranjo e Combinação seguem os mesmos padrões. Inicialmente é apresentado um problema contextualizado, com nível médio de dificuldade; a resolução é feita de duas maneiras: listando todas as possibilidades e pelo PFC. A partir da resolução, os autores definem qual o tipo de agrupamento está envolvido naquela situação problema, e a fórmula a ser utilizada para tal agrupamento. Os três tipos de agrupamentos apresentam exercícios resolvidos seguidos de exercícios de fixação, com uma média de doze exercícios por tipo de agrupamento.

O último tópico do capítulo de Análise Combinatória, sobre permutações com elementos repetidos, se apresenta de forma breve, apresentando um exemplo do 1º caso (apenas um elemento se repete) e um exemplo do 2º caso (dois elementos diferentes se repetem). A resolução desses exemplos utiliza as fórmulas já apresentadas como ferramentas para chegar a uma nova fórmula para a Permutação com repetição, o qual o livro denominou como *caso geral*. Em seguida é apresentado um exemplo com a resolução e sete exercícios são propostos. Para finalizar o capítulo os autores convidam os estudantes a um desafio sobre Análise Combinatória.

No livro *Matemática Paiva* a Análise Combinatória é dividida em dois capítulos, sendo eles:

- Capítulo 6: Os princípios da Análise Combinatória. O qual aborda o conceito de Análise Combinatória; O PFC; O princípio aditivo da contagem e fatorial.
- Capítulo 7: Agrupamentos e métodos de contagem. Aborda as classificações dos agrupamentos; Arranjos; Permutações; Combinação simples.

Para introduzir o conceito de Análise Combinatória, o autor utiliza, no início do capítulo um jogo visualmente chamativo (Figura 1) e levanta uma questão importante, sobre a segurança das senhas utilizadas na internet, a qual ele nomeou como: “As piores senhas do mundo”.

Figura 1: Capítulo 6 do livro Matemática Paiva.

Fonte: Paiva (2015).

Pode-se considerar uma questão relevante para introduzir a Análise Combinatória, pois, segurança de dados e privacidade é um assunto de interesse coletivo.

Ao iniciar o capítulo o livro traz quatro problemas de contagem, com o objetivo de mostrar aos estudantes a necessidade de se estudar Análise Combinatória. Em seguida são expostas duas questões de combinatória, que são resolvidas de duas maneiras: listando todas as possibilidades e utilizando o Princípio Multiplicativo, a partir dessas resoluções define-se o PFC. Segue-se com exemplos resolvidos e exercícios propostos.

Após a resolução dos exercícios são propostas duas atividades pertencentes as seções: (i) Criando problemas e (ii) Conectado.

A seção *criando problemas* tem o objetivo de incentivar a elaboração de problemas, sendo assim, nesse contexto os estudantes são desafiados a criarem e resolverem uma situação problema de Análise Combinatória, baseada nos exercícios resolvidos anteriormente, que envolvam situações do cotidiano.

Após essa atividade, chega-se a seção *conectado*, que utiliza a internet para complementar o estudo, sendo assim os alunos são estimulados a pesquisar sobre a resolução dos exercícios sobre o PFC por meio do diagrama de árvores, registrando a teoria e exemplos.

Para introduzir o princípio aditivo da contagem, o autor apresenta a resolução de uma situação problema, e a partir disso, define-se o conteúdo em questão. Segue-se com exercícios resolvidos, para que o estudante consiga compreender melhor a teoria exposta e em seguida, ter a capacidade de resolver outros problemas, que são apresentados na obra. Para finalizar esse tópico, é proposto, na seção *criando problemas*, que os estudantes elaborem e resolvam um problema sobre o princípio aditivo da contagem que esteja relacionado com uma situação do dia a dia.

O tema Fatorial foi explicado de maneira breve e sucinta, mostrando-lhes que o fatorial serve para simplificar as operações de Análise Combinatória. Para que haja uma melhor compreensão da teoria, é exposta a resolução de quatro exercícios. Em seguida define-se a propriedade

fundamental dos fatoriais, posteriormente, apresenta-se exercícios resolvidos e exercícios propostos.

Em continuidade nos deparamos com a seção *MENTES BRILHANTES*, que são “apresentados feitos de pessoas que revolucionaram a Matemática ou a Ciência em sua época” (PAIVA, p. 3, 2015). Nesta ordem, é apresentado “O problema básico da telefonia” que aborda o feito do Matemático Erlang, o qual conseguiu estimar a probabilidade de ligações que não se completariam pelo congestionamento da central telefônica de Copenhague.

O capítulo segue-se com exercícios complementares, para aprofundar o conceito estudado, além de propor questões importantes, que servem como exercícios de revisão, são denominados como *pré-requisitos* para o capítulo 7.

Para finalizar o capítulo 6, é sugerido completar a seção *Trabalhando em equipe*, que propõe o desenvolvimento de uma habilidade importantíssima no mundo atual, sendo ela, o saber trabalhar em equipe. Essa seção é dividida em duas partes: *ANÁLISE DA RESOLUÇÃO*, que mostra os erros mais comuns nas resoluções dos problemas sobre o conteúdo abordado e *MATEMÁTICA SEM FRONTEIRAS*, que traz textos sobre a aplicação da matemática no cotidiano.

Nessa seção, inicialmente é proposto às equipes formadas a identificação do erro de uma questão exposta no livro. Seguido de uma atividade que envolve a aplicação da Análise Combinatória na biologia, mais especificadamente no DNA, além de propor aos alunos um trabalho sobre a *cibercultura*, que tem como objetivo buscar técnicas criptográficas e formas de elaboração e memorização de senhas.

O capítulo 7, que aborda os agrupamentos e métodos de contagem tem início com uma breve explicação sobre a classificação dos agrupamentos, mostrando a diferença entre Arranjos e Combinações, enfatizando com exemplos que nas Combinações a ordem dos elementos não é considerada. É proposto um exercício com seis alternativas, nas quais

os estudantes necessitam apenas identificar o tipo de agrupamento: Arranjo ou Combinação.

Na definição de Arranjo, o autor utiliza uma linguagem mais elaborada, ou seja, termos técnicos da área da matemática, novamente ele utiliza um exemplo, no qual o resolve listando todas as possibilidades, para então chegar à fórmula desse conceito. Posteriormente são apresentados quatro exercícios resolvidos seguidos de sete exercícios propostos. Na seção *CRIANDO PROBLEMAS* os estudantes são desafiados a elaborar e resolver um exercício baseado nos resolvidos anteriormente, lembrando-os que os exercícios precisam ser contextualizados. Segue-se com a seção *MENTES BRILHANTES*, trazendo uma curiosidade do Cubo Mágico.

Para definir os conceitos de Permutação Simples e Permutação com Repetição são utilizados os conhecimentos prévios até se chegar às fórmulas desejadas, seguidas de exercícios resolvidos e exercícios propostos. O tópico sobre a Permutação Simples apresenta o desafio da seção *CRIANDO PROBLEMAS* e desafia os estudantes, por meio da seção *CONECTADO* a pesquisarem e registrarem o que é Permutação Circular.

Ao abordar a Combinação Simples o autor traz uma situação problema e a resolve listando todas as possibilidades, enfatizando que nesse tipo de a ordem dos elementos não altera a combinação. Em seguida a define formalmente e utiliza de exemplos resolvidos para se chegar à fórmula desejada, para um melhor entendimento é apresentado exercícios resolvidos. Segue-se com um breve texto que expõe alguns critérios que ajudam a diferenciar Arranjos e Combinações. Para fixar o conteúdo são propostos dez exercícios. A seção *CRIANDO PROBLEMAS* propõe a elaboração e resolução de um exercício contextualizado sobre Combinação Simples.

O capítulo tem continuidade com exercícios complementares e exercícios de revisão, que são denominados *PRÉ-REQUISITOS PARA O CAPÍTULO 8*. Para finalizar o estudo da Análise Combinatória a seção

trabalhando em equipe propõe a análise de erro em uma questão apresentada no livro seguida de uma atividade sobre criptografia, oferecendo um breve texto sobre a história da criptografia, com ênfase na cifra de César e a criptografia presente no século XXI, como a marca d'água nas cédulas de dinheiro, sendo essa, um ramo da criptologia, chamada de esteganografia; que estuda métodos para ocultar a existência de uma mensagem.

Após a leitura do texto, o autor propõe duas atividades, uma para decodificar uma mensagem, utilizando os conceitos da cifra de César e a outra sobre os números binários.

O livro *Conexões com a Matemática* aborda a Análise Combinatória em seu décimo capítulo, subdividido em:

- Contagem;
- Fatorial de um número natural;
- Permutações;
- Arranjo simples;
- Combinações simples.

A abertura do décimo capítulo apresenta um infográfico intitulado “Está na hora de alterar suas senhas?” e explica os objetivos do estudo da Análise Combinatória. Ao iniciar o estudo da Contagem, o autor retoma as informações do infográfico e discute sobre os dados indicados, levando os estudantes a pensarem nas possibilidades de se criar senhas seguras. Além disso, o livro traz outros três exemplos sobre contagem, em contextos diferentes, que são resolvidos por meio do diagrama de árvore. O Princípio Multiplicativo é apresentado de forma clara e objetiva, definindo-o sem mais delongas. Para a compreensão desse conceito são expostos cinco exercícios resolvidos, e para fixação do conteúdo são propostos quinze exercícios.

O tema fatorial de um número natural é definido com uma linguagem matemática, em sua maioria, composta por uma linguagem simbólica, seguida de exemplos, exercícios resolvidos e exercícios proposto.

A Permutação Simples, Permutação com Repetição, Arranjo Simples e Combinação, são apresentadas seguindo o mesmo padrão, ou seja, a obra parte de um problema inicial, apresenta a resolução por meio do Princípio Multiplicativo e encaminha o estudante para a definição formal de cada tipo de agrupamento apresentando-lhes a fórmula correspondente. Ao abordar o tópico da Combinação, o livro enfatiza a diferença entre os outros agrupamentos, destacando que nesse conteúdo a ordem dos elementos não irá alterar o resultado. Seguem-se de exercícios resolvidos e exercícios propostos.

Após o estudo dos tópicos apresentados o livro propõe uma lista de vinte e cinco exercícios, divididos em exercícios de aplicação, de aprofundamento e desafios. Posteriormente, há uma lista de oito exercícios baseados nos principais conceitos a serem aprendidos, esses exercícios são propostos aos estudantes para que eles possam fazer uma autoavaliação de sua aprendizagem, para isso, após a resolução desses exercícios, os estudantes preenchem uma tabela, a qual irá orientá-los a retomar os conceitos não fixados, se for o caso.

Para finalizar o estudo da Análise Combinatória, o livro propõe uma atividade intitulada: Pesquisa e ação, objetivando desenvolver atividades práticas e em grupos, envolvendo uma pesquisa e a elaboração de um produto final. Para a Análise Combinatória o trabalho proposto é sobre Quick Response - QR Code, no qual os estudantes terão de estudar as origens do QR Code, seu funcionamento e suas aplicações, para em seguida criar seus próprios Códigos e decodificarem os códigos criados pelos colegas.

Com a análise desses três livros, pode-se ver que, em alguns casos, o estudo da Análise Combinatória apresenta um padrão, sendo ele: definição, exemplos e exercícios de fixação. Entretanto percebe-se a preocupação em apresentar atividades diferenciadas, como trabalhos em grupo, criação de problemas e a busca por aplicações reais do conteúdo em questão, a fim de desenvolver as habilidades e competências necessárias para o século XXI.

2.3.2 Análise de dissertações

Aqui, inicia-se a análise de algumas dissertações, que segundo Fusel (2013) ainda existem poucos estudos sobre o processo de ensino de aprendizagem da Análise Combinatória. De acordo com o documento do PROFMAT (SOCIEDADE BRASILEIRA DE MATEMÁTICA, 2017) apenas 2,7% do total de dissertações se preocuparam em estudar o ensino e a aprendizagem da Análise Combinatória.

Das dissertações publicadas pelo Mestrado Profissional em Matemática em Rede Nacional - PROFMAT foram escolhidas três para a análise aqui apresentadas, sendo elas:

- (i) Uma abordagem alternativa para o ensino de Análise Combinatória no Ensino Médio: a utilização do Princípio Multiplicativo e da resolução de problemas como ferramenta didático-pedagógica. Escrito por Rafaela Ramos Soares Gonçalves, que desenvolveu sua pesquisa no Instituto Nacional de Matemática Pura e Aplicada – IMPA. Publicada em 2014.
- (ii) Análise Combinatória: Uma abordagem diferenciada sem a utilização de fórmulas. Escrito por Thiago Miguel Roda, o qual desenvolveu sua pesquisa na Universidade Federal de São Carlos. Publicada em 2018.
- (iii) Utilizando o material concreto para o ensino de Análise Combinatória. Escrito por Diego Suzano Ferreira Jacinto, o qual desenvolveu sua pesquisa no Instituto de Ciências Exatas do Rio de Janeiro. Publicado em 2015.

A escolha pelas dissertações (i) e (ii) se deu pelo motivo de ir ao encontro a um dos objetivos específicos dessa dissertação, sendo ele, o ensino da Análise Combinatória com ênfase no PFC. A dissertação (iii) foi

selecionada, pois apresenta uma estratégia diferenciada para o ensino e a aprendizagem da Análise Combinatória.

A dissertação de Gonçalves (2014) teve como objetivo estudar os métodos de ensino da Análise Combinatória e propor uma metodologia de ensino baseada no Princípio Fundamental da Contagem.

Para o desenvolvimento do trabalho, foi utilizada a engenharia didática como metodologia de pesquisa. Sua aplicação ocorreu em uma escola de uma cidade do interior do estado do Rio de Janeiro, da rede privada, em quatro turmas do Ensino Médio, totalizando 87 alunos. A professora pesquisadora era a professora titular de Matemática das turmas, a qual afirma ter sido motivada a pesquisar o ensino e a aprendizagem da Análise Combinatória, por perceber a dificuldade encontrada pelos alunos e pelos professores no processo de ensino e de aprendizagem do conteúdo em questão. Das quatro turmas que ela lecionava duas ela utilizou a metodologia de resolução de problemas baseado no Princípio Fundamental da Contagem e nas outras duas, utilizou o método tradicional, ou seja, teoria, fórmula e aplicação. No início da experimentação, fase assim denominada a prática em sala de aula, pela engenharia didática, foi aplicado uma avaliação diagnóstica, que foi resolvida pelos alunos em grupos de até cinco participantes.

A professora-pesquisadora afirma ter sido necessária uma intervenção na resolução dessa avaliação, pois os alunos estavam confusos e inseguros. Por meio dessa atividade foi perceptível que os alunos já tinham uma noção de Análise Combinatória, porém a maioria dos alunos resolveram as questões listando todas as possibilidades, porém surgiu o questionamento sobre quando se depararem com uma situação problema no qual apareça muitas possibilidades, pois, listá-las não seria conveniente. Frente a esses conteúdos, foi apresentada a necessidade de destinar uma área da matemática a contagem.

Ao desenvolver a Análise Combinatória pelo método fórmula-aplicação, as dúvidas mais frequentes eram sobre o tipo de agrupamento que cada problema pertencia. Nas turmas que, a Análise Combinatória foi

trabalhada pelo PFC, foi notório a confiança na resolução dos problemas propostos. Entretanto, os sub-tópicos dessa área da Matemática (Arranjo, Permutação e Combinação) foram apresentados aos alunos para que eles pudessem, ao menos, saber que existem outros modos de resolver os exercícios de contagem.

Na avaliação final, percebeu-se um desempenho satisfatório, tanto das turmas favorecidas da metodologia baseada na resolução de problemas pelo PFC, como as turmas que estudaram por meio de fórmula-aplicação. Porém, no ano seguinte, a professora-pesquisadora, ao revisar o conceito de Análise Combinatória, decidiu utilizar à mesma metodologia nas quatro turmas, ou seja, com ênfase no PFC. Ao realizar, uma avaliação da revisão, percebeu que todos os alunos utilizaram o PFC, até mesmo, aqueles, que no ano anterior, aprenderam o conteúdo com ênfase na aplicação de fórmulas. Em uma conversa informal da professora-pesquisadora com os alunos, foi colhida a informação de que os alunos se sentem mais confortáveis ao solucionarem os exercícios pelo PFC, pois não necessitam descobrir que tipo de agrupamento o problema pertence.

Ao finalizar esse estudo, a professora-pesquisadora concluiu que ao trabalhar a Análise Combinatória por meio do PFC, este proporcionou ao aluno o desenvolvimento de um raciocínio combinatório, ajuda-o a desenvolver a competência de resolução de problemas, nessa e em outras áreas do conhecimento humano, além de possibilitar uma maior segurança ao resolver os exercícios, pois não se limitam a descobrir qual o tipo de agrupamento e a fórmula a ser utilizada.

A dissertação de Roda (2018) teve como motivação as experiências pessoais do próprio pesquisador, o qual por muito tempo como professor do ensino básico percebeu a dificuldade encontrada por professores e alunos no ensino e na aprendizagem da Análise Combinatória.

Em sua pesquisa, ele afirma que o estudo da Análise Combinatória, em muitos casos, se limita a apresentar brevemente um problema modelo, seguido da aplicação de fórmulas, tornando assim, um aprendizado mecanizado; método que pouco favorece a competência de resolver

problemas. Dessa forma, o objetivo dessa dissertação é abordar a Análise Combinatória sem o uso de fórmulas, utilizando apenas o PFC como estratégia na resolução de situações problemas.

A metodologia adotada é a resolução de problemas, a aplicação ocorreu em uma escola estadual do interior de São Paulo, em uma classe do 2º ano do Ensino Médio, composta por 25 alunos, sendo que a aplicação do projeto teve duração de 15 horas-aula. Para dar início, o professor propôs um exercício a ser entregue, a maioria dos alunos o resolveram listando todas as possibilidades, porém teve resoluções utilizando o PFC. Para definir tal estratégia, o professor, que é também o pesquisador, propôs um novo exercício, o qual foram discutidos e resolvidos pelas duas maneiras, pelo PFC e listando todas as suas possibilidades. A partir de então os conceitos de Permutação, Arranjo e Combinação foram trabalhados pela estratégia ensinada, todas a partir de situações problemas que o professor-pesquisador propunha aos alunos. Para finalizar, foi aplicada uma avaliação, a qual os alunos apresentaram um bom desempenho.

O autor afirma que com a aplicação desse projeto foi possível perceber uma grande interação dos alunos e um aprendizado satisfatório, entretanto afirma que se tivesse mais tempo disponível, o assunto poderia ser aprofundado.

Por fim, a dissertação de Jacinto (2015) não difere das dissertações aqui mencionadas sobre sua motivação, sendo ela, a dificuldade encontrada por professores e alunos quando se aborda o conteúdo de Análise Combinatória, porém o autor acrescenta que faltam trabalhos relevantes desenvolvidos nesse ramo da Matemática por isso, torna-se necessário a busca por novas pesquisas, outro elemento que foi considerado motivador.

Essa dissertação se fundamentou na teoria construtivista tendo como objetivo geral propor e avaliar uma maneira alternativa para o ensino e aprendizagem da Análise Combinatória. Foi desenvolvido em uma cidade do Estado do Rio Janeiro, em três turmas do Ensino Médio, 1º, 2º e 3º ano, nesse caso, o pesquisador não era o professor titular das turmas.

O uso dos materiais concretos foi utilizado somente no 1º ano do Ensino Médio (EM), já nas outras duas turmas foi utilizado a metodologia tradicional, a fim de comparar os resultados obtidos. Vale ressaltar que a utilização dos materiais concretos foram usados para introduzir novos conceitos; os exercícios de fixação foram os mesmos para as três turmas.

Ao dar início ao estudo da Análise Combinatória o pesquisador dividiu a classe beneficiada da aplicação do projeto em grupos e entregou-lhes a atividade 1, composta pela problemática de combinação de roupas, e para resolvê-la era necessário listar todas as possibilidades em forma de pintura, como mostra a Figura 2.

Figura 2: Atividade 1.

1) Um jovem possui 5 camisas e 3 bermudas de cores diferentes

- Cores de camisas – amarela, verde, vermelha, branca, azul claro;
- Cores de bermudas – preta, azul, vermelha.

Pinte as figuras fazendo todas as combinações possíveis

Atividade 1- colorir bermudas e blusas

Total de possibilidades	
bermuda preta:	_____
bermuda azul:	_____
bermuda vermelha:	_____
Total:	_____

Dica: escolha uma cor de bermuda e combine com todas as camisas, após troque a cor da bermuda e faça o mesmo processo.

- Qual o número total de vestimentas que encontrou? Você(s) acha(m) que existem mais possíveis?
- Qual o total de possibilidades se contar somente as bermudas preta e azul?
- Seria capaz de responder qual o total de vestimentas, se fossem 5 bermudas e 8 camisetas?

Fonte: Jacinto (2015).

Após a realização dessa atividade fez-se um debate sobre as formas de resolução seguido da definição do PFC e resolveram mais dois exercícios em folhas separadas, seguindo esse modelo apresentado. Um era para pintar uma bandeira retangular dividida horizontalmente em três partes, com três cores diferentes, sendo que duas faixas consecutivas não poderiam ser pintadas da mesma cor; a outra atividade era sobre formas diferentes de se montar um pedido com três opções de comidas diferentes tendo a disposição nove tipos de comidas. Após essas atividades foram resolvidos outros exercícios, no caderno, para fixação.

Para introduzir o conceito de Permutação, foi entregue aos alunos uma folha com uma situação problema sobre o posicionamento de quatro pessoas em quatro cadeiras, os personagens envolvidos foram representados concretamente em EVA, para que consigam visualizar melhor o que está sendo pedido e para que facilite a manipulação dos objetos.

Ao fim dessa atividade foi definido o conceito de Permutação. A seguir os alunos foram desafiados a montar anagramas com as letras da palavra MAIS, a qual foi entregue concretamente em EVA, para que pudessem manipulá-las. O mesmo foi feito com a palavra CASA, para que percebessem a diferença quando há repetição de letras. Apresentou-se assim aos alunos o conceito de Permutação com Repetição.

Ao trabalhar Arranjo e Combinação, foi entregue aos alunos duas folhas com exercícios, nos quais era pedido para que os alunos listassem todas as possibilidades. Um exercício era sobre a formação de duplas de um dado conjunto e no outro era para listarem as possibilidades de se obter dois vencedores de um conjunto finito de uma dada competição, sendo que um ocuparia o primeiro lugar e o outro o segundo lugar. Após a resolução desses exercícios foi explicado sobre a interferência na ordem das possíveis respostas para as questões apresentadas, para que o aluno compreendesse a diferença entre os tipos de agrupamento, com ênfase naqueles em que a ordem importa e aqueles em que a ordem não importa.

Apesar do autor não ter mencionado o uso efetivo de softwares na aplicação do seu projeto, ele menciona o **COMBS** e o **COMBINA**, como

ferramentas a serem utilizadas no processo de ensino e de aprendizagem da Análise Combinatória, pois esses programas são capazes de mostrar a quantidade de possibilidades de um problema dado e ainda listá-las.

Para avaliar o resultado do projeto, foram propostas as três turmas participantes, um mesmo teste, para análise de comparação, composto por nove questões, que foram retiradas de vestibulares e livros didáticos.

A média obtida pelo 1º ano, turma que se beneficiou das atividades aqui apresentadas, foi de 76,7; já as turmas do 2º e 3º ano, que foi trabalho a Análise Combinatória de forma tradicional, teve uma média de 51,9.

O autor conclui que percebeu de forma significativa a capacidade de abstração que os alunos do 1º ano desenvolveram nesse conteúdo em relação ao 2º e 3º ano, além de mostrarem-se mais motivados e abertos a novos aprendizados.

A partir da análise das dissertações aqui apresentadas, pode-se perceber a preocupação dos pesquisadores em encontrar maneiras alternativas para se ensinar e aprender Análise Combinatória, pois esse conteúdo vem indicando há muito tempo um baixo rendimento. Apesar de ainda não se ter muitos estudos voltados para esse conteúdo faz-se cada vez mais necessário buscar modos alternativos para solucionar o déficit de aprendizagem do conteúdo em questão.

3 CRIPTOGRAFIA

Ao longo do desenvolvimento humano, sempre houve a preocupação em enviar mensagens secretas, em que somente o destinatário as entendesse. Zochio (2016) afirma que a criptografia surgiu para fins militares, a necessidade de zelar pela segurança da informação, pelas estratégias de guerras das forças inimigas, desde os primórdios, deu início e o aprimoramento as técnicas de criptografar mensagens. Hoje, essa arte se tornou um ramo da ciência, conhecida como Criptologia. Com o passar do tempo, com o avanço das tecnologias digitais, estamos cada vez mais dependentes dessa ciência, a exigência pela segurança de dados está proporcionando aos estudiosos uma corrida armamentista intelectual. Ou seja, a luta pela segurança de dados, pelas maneiras mais elaboradas de se criptografar uma mensagem anda lado a lado com a criptoanálise, área da criptologia que se dedica a estudar métodos para decifrar uma mensagem.

3.1 Conceitos básicos de Criptografia

Criptografia é uma palavra de origem grega, vinda da união da *Kryptós*, que significa escondido, com grafia, vinda de *graphé*, que significa escrita, ou seja, pode-se interpretá-la como uma escrita oculta, escrita secreta. Coutinho (2015), afirma que a criptografia estuda métodos para codificar uma mensagem de modo que só o seu destinatário consiga compreendê-la.

Apesar de muitas pessoas associarem a criptografia a mapas do tesouro, filmes de agentes secretos, isso não é sua aplicação primordial. Essa Ciência é muito importante no sigilo de bancos de dados, em investigações governamentais, dados hospitalares, informação de crédito pessoal, comandos militares, comércio eletrônico, entre outros (BEZERRA; MALAGUTTI; RODRIGUES, 2010).

Por muito tempo, a criptografia foi considerada uma arte. Entretanto, devido a sua importância ao longo do desenvolvimento humano, passou a

ser considerada um ramo da ciência da Criptologia, a qual se originou da união dos estudos baseados em maneiras, cada vez mais complexas, de codificar uma mensagem e em contrapartida, maneiras de decodificá-las.

A Criptologia é definida como a ciência que estuda os meios de ocultação e quebra de informações criptografadas, a qual se divide em três ramos: a esteganografia, criptografia e a criptoanálise (BEZERRA; MALAGUTTI; RODRIGUES, 2010).

A esteganografia tem por finalidade esconder a existência de uma mensagem; o que difere do ramo da criptografia, que tem o objetivo de tornar uma mensagem incompreensível a qualquer outra pessoa, a não ser o destinatário. Há muito tempo o homem já utilizava técnicas da esteganografia para enviar recados, Singh (2003) relata que no período de conflitos entre a Grécia e a Pérsia, os informantes escreviam mensagens no couro cabeludo dos mensageiros, e somente após o crescimento do cabelo eles iam ao encontro do seu destinatário, e para transmitir a mensagem, raspavam a cabeça para que então, a mensagem pudesse ser lida. Dessa forma, o mensageiro não era incomodado, pois aparentemente não levava nenhuma informação relevante.

Um exemplo atual da aplicação da esteganografia é a marca d'água presente nas cédulas de dinheiro, que são utilizadas para ajudar a verificar se a cédula é falsificada. Atualmente a esteganografia é muito usada na luta contra a pirataria e o terrorismo (BEZERRA; MALAGUTTI; RODRIGUES, 2010).

Já a criptoanálise estuda as maneiras de decodificar as mensagens, ou seja, de quebrar um código sem saber, inicialmente, a sua chave. Um detalhe importante a ser tratado é a diferença entre a quebra de um código e a decifração de uma mensagem; quebrar um código significa descobrir a chave e então tornar legível uma mensagem; decifrar significa transformar uma mensagem compreensível quando se conhece a chave.

3.2 Breve estudo histórico da criptografia

Segundo Almeida (2012) a ocultação de mensagens já era usada desde o Egito antigo, por volta de 1900 a. C. pelos escribas dos faraós, que acrescentavam ou substituíam palavras nos documentos valiosos, por alguns símbolos diferentes, a fim de evitar que possíveis ladrões compreendessem a informação ali contida.

Antigamente, as principais aplicações da criptografia se voltavam para o militarismo, tendo como objetivo, a compreensão de suas mensagens somente pelas forças aliadas. Um dos primeiros sistemas criptográficos, que há registros, usados para fins militares, é o bastão de Licurgo, ou também conhecido como cítala (Figura 3) que foi utilizado por soldados espartanos. Essa técnica consistia basicamente em enrolar uma tira de couro de forma espiral em um bastão, com uma largura pré-determinada e a escrita da mensagem era feita de forma longitudinal. Após o registro da informação, a tira era desenrolada e enviada como se fosse um cinto por um mensageiro, o receptor necessitava apenas de um bastão de mesma largura, para poder enrolar novamente a tira e compreender a mensagem; nesse caso se o bastão não fosse da mesma largura, provavelmente a informação não seria decifrada. Pode-se considerar que esse tipo de criptografia possui como algoritmo o enrolar da tira e como chave, a largura do bastão.

Figura 3: Bastão de Licurgo ou Cítala.

Fonte: Singh (2003).

Outro sistema muito conhecido e muito utilizado foi a criptografia desenvolvida pelo General Júlio César do Império Romano, que desenvolveu uma cifra de substituição monoalfabética para codificar informações governamentais. De acordo com Malagutti (2015) essa cifra consiste em substituir cada letra do alfabeto pela terceira letra que a segue. Isto é, para cifrar um texto, César trocava a letra A pela letra D, a letra B por E, C por F e assim por diante. Vejamos a seguir a correspondência que César utilizava para cifrar suas mensagens (Tabela 1).

Tabela 1: Método de substituição usado por Júlio César.

Alfabeto Normal	A	B	C	D	E	F	G	...	T	U	V	W	X	Y	Z
Alfabeto Cifrado	D	E	F	G	H	I	J	...	W	X	Y	Z	A	B	C

Fonte: Adaptado de Singh (2003).

Nesse sistema de cifragem a mensagem “Criptografia de Júlio César” fica codificada como: fulswrjudild gh mxolr fhvdu. Sendo assim, podemos dizer que a chave dessa técnica é TRÊS, pois cada letra do alfabeto é substituída pela terceira que a segue.

Sing (2003) relata que no século IX, Al-kindí, conhecido como “o filósofo dos árabes” começou a estudar a frequências das letras a fim de quebrar os códigos das mensagens cifradas. Esse procedimento consistia em analisar quais letras eram mais frequentes no idioma em questão, e em seguida, analisar a mensagem cifrada, e fazer uma correspondência entre as letras e os símbolos mais frequentes. Dessa forma, a cifra de César ficou vulnerável, pois, facilmente os criptoanalistas conseguiriam quebrá-la, forçando os criptógrafos a encontrarem novos métodos de cifragem.

Além disso, Sing (2003) afirma que a solução encontrada no século XVI, foi a criação de uma cifra polialfabética, a qual foi encontrada pelo Frances Blaise de Vigenère, que ficou conhecida como Cifra de Vigenère.

Essa técnica utiliza 26 alfabetos cifrados (Tabela 2) que servem para criptografar uma mensagem.

Tabela 2: Quadro de Vigenère.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fonte: Adaptado de Singh (2003).

Para codificar mensagens usando essa técnica, o remetente da informação pode, por exemplo, codificar a primeira letra de acordo com a

linha 7, a segunda de acordo com a linha 2 e a terceira de acordo com a linha 25, e assim sucessivamente.

Para decifrar a mensagem, o destinatário necessita ter o conhecimento de qual alfabeto foi usada para cada letra, essa informação está contida em uma palavra-chave. “Por exemplo, a frase “eu amo estudar”, pode ser codificada como “io egs ywnyxel”, tendo como palavra-chave: EU, como essa palavra tem duas letras, então a mensagem foi cifrada usando 2 alfabetos de Vigenère. Ou seja, a primeira letra foi cifrada de acordo com o alfabeto que tem início em E, a segunda com o alfabeto que tem início em U, a terceira com o alfabeto que tem início em E e assim em diante.

Essa cifra foi considerada como a “cifra indecifrável” por quase dois séculos, pois ela é que resiste a análise de frequência e possui muitas possibilidades para chaves diferentes. Entretanto, por volta de 1850, o matemático inglês Charles Babbage conseguiu quebrá-la por meio de um estudo que tabelava o padrão que a palavra-chave formava ao ser aplicada ao longo do texto.

Uma notória aplicação da criptografia em conflitos militares foi na segunda guerra mundial, com o desenvolvimento da máquina alemã, chamada Enigma, criada em 1918 por Arthur Scherbius. Em 1928 o exército alemão aprimorou essa máquina, elaborando uma versão própria, que ficou conhecida como a *Enigma G* (Figura 4). Essa poderosa máquina funcionava da seguinte forma:

Uma letra do texto é pressionada no teclado, uma corrente elétrica passa pelos diversos componentes de cifragem da máquina, acendendo uma luz no “painel de lâmpadas”, a letra acendida é a codificação da letra digitada. E cada vez que uma letra é pressionada, as peças móveis da máquina mudam de posição e, se numa próxima vez que a mesma letra for teclada, provavelmente será cifrada como algo diferente. (BEZERRA; MALAGUTTI; RODRIGUES, 2010, p. 76).

Visto que as configurações se alteravam, o método de análise de frequência de letras, não era viável. Para decifrar uma mensagem

codificada pela máquina enigma, era necessário possuir outra máquina, e então digitar a mensagem codificada, e se as duas estivessem configuradas da mesma forma, a mensagem original era obtida pelas letras que apareciam no painel de lâmpadas.

Figura 4: Máquina Enigma.

Fonte: Bezerra; Malugutti; Rodrigues (2010).

Apesar dos alemães considerarem que era impossível as forças inimigas quebrarem o código da máquina Enigma, o matemático inglês Allan Turing e sua equipe, composta por Conel Hugh, O'Donel Alexander, Marian Rejewski, Jerzy Różycki e Henryk Zygalski, conseguiram decifrá-la. Para tal feito, construíram o primeiro computador operacional, que pertenceu ao serviço de inteligência britânico, o qual foi nomeado por *Colossus* (Figura 5).

Figura 5: Colossus.

Fonte: Singh (2003).

Os tipos de criptografia citados até o presente momento são exemplos de criptografias de chave simétricas, ou seja, o mesmo método utilizado para cifrar é também usado para decifrar. Com o desenvolvimento das tecnologias e o aprimoramento estudantil dos criptoanalistas, esse tipo de criptografia se torna vulnerável. Surge então, na década de 70 a criptografia assimétrica, também conhecida como criptografia de chave pública. A criptografia assimétrica faz uso de duas chaves, uma para cifrar e outra para decifrar, nesse sistema as duas chaves são relacionadas matematicamente.

A criptografia de chave pública mais conhecida e uma das mais utilizadas é o sistema RSA, criado em 1977 por Rivest, Shamir e Adleman. Coutinho (2015) explica que o primeiro passo para implementar esse sistema é escolher dois números primos muito grandes p e q , com no mínimo 100 algarismos cada; em seguida calcula-se o produto $p \times q = n$. Para codificar a mensagem usa-se o número n e para decodificá-la usa-se p e q ; nesse método o número n pode se tornar público, mas p e q necessita ser mantido em sigilo.

Aparentemente, quebrar esse código é simples, basta fatorar n , que encontramos os fatores primos p e q , porém, o número n será composto no mínimo de 200 algarismos, e para fatorá-lo, talvez seja necessário zilhões de anos, mesmo usando os computadores mais potentes existentes atualmente.

A sociedade do século XXI é totalmente dependente da criptografia, Carvalho (2016) afirma que não é exagero dizer que as nossas vidas dependem dessa ciência, pois nossas informações estão espalhadas nos diversos bancos de dados, seja a internet, instituições governamentais ou privadas.

3.3 A Criptografia como ferramenta educacional da Matemática

O processo de ensino e de aprendizagem da Matemática vem se tornando cada vez mais um objeto de estudo dos pesquisadores, sempre com a preocupação em melhorá-lo. Infelizmente a Matemática ainda é vista como uma disciplina para poucos, composta por técnicas complexas e sem aplicabilidade no cotidiano; esse fato faz com que muitos estudantes não encontrem um significado para o aprendizado da Matemática, desmotivando-os cada vez mais.

Perante essa dificuldade, apresenta-se aqui a proposta de incluir no processo de ensino e de aprendizagem da Matemática o tema “Criptografia” para a sala de aula, com o intuito de despertar nos estudantes o interesse, a curiosidade e motivação para adquirir conhecimentos matemáticos. A escolha por esse tema é devido a sua aplicabilidade no dia-a-dia e a curiosidade que desperta, por se tratar de um assunto “misterioso”.

A ciência da Criptografia está repleta de conteúdos matemáticos, podemos afirmar, que essa ciência caminha lado a lado da Matemática, a qual utiliza de forma direta seus princípios na segurança de dados. Sendo assim, utilizá-la em sala de aula, tem grandes chances de proporcionar uma melhora no ensino e no aprendizado de Matemática.

Esse tema nos permite trabalhar no ensino básico conceitos de Funções, Matrizes, Análise Combinatória, Números Binários, sequências, módulo de um número, números primos, critérios de divisibilidade, potenciação, além de conteúdos do ensino superior. Jesus (2013) afirma que a Criptografia, pode servir para introduzir, revisar, reforçar e até mesmo, aprofundar conteúdos matemáticos.

Na visão de Groenwald e Franke (2008) a criptografia permite aos professores de Matemática criar uma ponte entre os conteúdos vistos em sala de aula, com situações cotidianas, ajudando-lhes a desenvolver a competência da resolução de problemas.

Como viu-se no capítulo anterior, alguns livros didáticos já trazem essa temática para a sala de aula. Os livros analisados nesse trabalho “Matemática Paiva” e “Conexões com a Matemática” utilizaram atividades de criptografia no final do capítulo de Análise Combinatória, trazendo propostas de atividades diferenciadas, a fim de fixar o conteúdo.

Além dos livros didáticos, é possível encontrar materiais para ensino básico que abordam a criptografia como ferramenta educacional no site da Olimpíada Brasileira de Matemática (OBEMP). Os alunos premiados nessa competição participam de um Programa de Iniciação Científica Jr. (PIC), que tem como finalidade despertar o interesse em pesquisas matemáticas. O material utilizado nesse programa está disponível no site: <http://www.obmep.org.br/apostilas.htm>. Entre as apostilas disponibilizadas, duas delas, são sobre Criptografia.

A primeira é intitulada “Criptografia” escrita por Severino Coutinho, que tem como foco a criptografia RSA. Ela composta por teoria e exercícios, abordando os seguintes tópicos:

- Números inteiros;
- Aritmética Modular;
- Inversos Modulares;
- Algoritmo Chinês do Resto;
- Potências;
- Criptografia RSA;
- Encontrando Primos.

O outro Material é uma apostila denominada: “Atividades de contagem a partir da Criptografia”, escrita por Pedro Luiz Malagutti. Esse trabalho tem início com o estudo do PFC e permutações, trazendo atividades baseadas na cifra de Júlio César, e proporciona aos estudantes a construção de aparatos que o ajudarão na codificação e decodificação de mensagens, utilizando essa cifra. Esta apostila também apresenta os métodos utilizados na antiguidade para decifrar a cifra de César, sendo ela, a frequência das letras do idioma em questão, posteriormente, é proposto aos alunos atividades de contagem que envolvem em seu enunciado conhecimentos sobre essa cifra.

Para desenvolver atividades sobre Combinação, a apostila trabalha com a escrita Braile e o código binário, esse material, traz também alguns pequenos textos sobre alguns matemáticos que foram relevantes no desenvolvimento da Matemática e que de certa forma, estavam ligados ao estudo da Criptografia.

Além dessas apostilas, encontramos também um material que traz teoria e atividades voltadas ao ensino básico, intitulado: “Aprendendo Criptologia de forma divertida” escrito por Débora de Jesus Bezerra, Pedro Luiz Malagutti e Vânia Cristina da Silva Rodrigues. Esse trabalho tem início com uma breve introdução histórica e apresenta as vertentes da criptologia, sendo ela: a Criptografia, a Esteganografia e a Criptoanálise. Em seguida traz considerações sobre o código de barras, a identidade de um livro – ISBN (International Standard Book Number), mostra como é feito o CPF (Cadastro de Pessoas Físicas), aborda os métodos de ciframento por substituição e transposição, classifica a criptografia quanto as suas chaves: simétricas e assimétricas. O código Morse, a máquina Enigma, a máquina de Lorenz são tipos de criptografias que também são citados nesse trabalho, além da criptografia RSA e a escrita Braile, o código de César, a escrita binária e a criptografia presente no DNA.

Esse trabalho traz grandes contribuições para o ensino básico, pois podem ser realizadas muitas atividades de Matemática utilizando esse material de apoio, como a ligação da Matemática com a Biologia e até

mesmo no Ensino Fundamental I, utilizando o tema do cálculo do CPF, pois necessita apenas de conhecimentos sobre adição e multiplicação.

Esses dois últimos materiais citados foram de grande importância no desenvolvimento dessa dissertação.

Apesar de ter sido encontrado a apostila de “Atividades de Contagem a partir da criptografia” e abordagens sobre isso nos livros didáticos, não encontramos nenhuma dissertação e/ou tese que estudasse a criptografia como ferramenta no ensino da Análise Combinatória. Além de que, essa dissertação se diferencia dos materiais aqui apresentados, pelo modo como utilizou a Criptografia, ou seja, inicialmente ela foi o objetivo principal de estudo, sendo que a Análise Combinatória foi estudada de forma implícita, sendo utilizada para resolver atividades referentes a Criptografia e assim, o aluno foi adquirindo conhecimento sobre as técnicas de contagem por consequência, para então, poder estudar propriamente a Análise Combinatória.

4 METODOLOGIA

A metodologia apresenta um caminho para se alcançar um determinado objetivo, assim a função da metodologia é mostrar como trilhar nos ‘caminhos das pedras’ para a investigação de uma prática de sala de aula, com a pretensão de ajudar o pesquisador/professor a ter uma visão diferente do que está acostumado, despertando um olhar organizador, dedutivo, curioso, indagador e criativo (POMMER, 2013).

4.1 Metodologia de pesquisa

Dentre as metodologias de pesquisas voltadas para a Educação Matemática, encontrou-se a Engenharia Didática, a qual pode ser utilizada de duas formas: (I) para a produção de materiais para o ensino ou (II) uma metodologia de pesquisa qualitativa (ARTIGUE, 1996). Nesse trabalho será abordado de forma a unir as duas opções, a qual serviu como metodologia de pesquisa.

4.1.1 Engenharia Didática

A Engenharia Didática surgiu na França, no final da década de 1960, o nome Engenharia foi dado, pois essa metodologia funciona de modo semelhante ao:

“[...] ofício do engenheiro que, para realizar um projeto preciso, se apoia sobre conhecimentos científicos de seu domínio, aceita submeter-se a um controle de tipo científico, mas, ao mesmo tempo, se vê obrigado a trabalhar sobre objetos bem mais complexos que os objetos depurados na ciência e, portanto, a enfrentar [...] problemas que a ciência não quer ou não pode levar em conta” (ARTIGUE, 1996, p. 193).

De acordo com Pais (2005) a Engenharia Didática é composta por quatro fases, sendo elas: (I) análises preliminares; (II) concepção e análise *a priori*; (III) aplicação de uma sequência didática e (IV) análise *a posteriori* e validação. Vale ressaltar que as quatro fases da Engenharia Didática não têm a necessidade de ocorrer linearmente, pois essa metodologia necessita, em alguns momentos, da articulação, da antecipação e até mesmo da superposição dos elementos de cada fase (POMMER, 2013).

Na primeira fase, das análises preliminares, ocorre a identificação do problema de pesquisa, que pode se dar, inicialmente, pela observação ou até mesmo pela aplicação de atividades diagnósticas. Além disso, é feito um levantamento teórico das dificuldades que os alunos, em geral, apresentam e dos estudos que foram e vem sendo feitos sobre o tema em questão. Machado (2002) afirma que nessa fase são feitas ponderações sobre o quadro teórico didático mais geral, mas também, aborda questões sobre os conhecimentos específicos do tema da pesquisa.

Na segunda etapa, da concepção e análise *a priori*, faz-se uma sondagem sobre as possíveis soluções para o problema encontrado e as possibilidades de melhora no processo de ensino e de aprendizagem do tema em questão, elaborando uma sequência didática. Berenguer (2010) afirma que nessa fase, o pesquisador tem como tarefa descrever as características da situação didática, verificar as possibilidades de ações dos estudantes e analisar qual seria o comportamento dos alunos perante a situação aplicada.

A terceira fase é responsável pela experimentação, é o momento em que o professor-pesquisador aplica a sequência didática, em um público pré-determinado, e registra as informações obtidas durante o decorrer das aulas. Pannuti (2004) descreve a sequência didática como uma modalidade organizada baseada em uma série de ações sequenciadas, planejadas e orientadas com a finalidade de promover uma aprendizagem específica e definida do tema em questão.

Almouloud e Silva (2012) definem a quarta fase, da análise *a posteriori* e validação, como um conjunto de dados coletados durante a aplicação, a

fim de validá-los. Nessa etapa é a qual ocorre a comparação das hipóteses levantadas na análise *a priori*, com os resultados obtidos na experimentação.

Os dados coletados devem ser previamente estipulados pelo pesquisador, o qual pode ser por meio de relatórios, entrevistas, avaliações escritas e até mesmo pela observação durante a aplicação da sequência didática. Sendo assim, torna-se possível analisar se existe e quais são as contribuições do trabalho elaborado, para a solução do problema de pesquisa. (ALMOULOU; SILVA, 2012).

A Engenharia Didática, como metodologia para área educacional, possibilita a união entre teoria e prática, levando o professor a refletir sobre suas práticas em sala de aula. Sendo assim, Pommer (2013) afirma que conhecendo os fundamentos que regem as quatro etapas dessa metodologia, o professor obtém um domínio da formulação das situações de aprendizagem, o que aprimora a relação dos estudantes com o conhecimento.

4.2 Público-alvo

A aplicação desse projeto foi realizada em uma escola pública da rede estadual do estado de São Paulo, em uma turma do 2º ano do Ensino Médio, composta por 22 alunos, os quais são nomeados por: aluno 1, aluno 2, aluno 3, ..., aluno 22, a fim de preservar a identidade dos estudantes. A aplicação do projeto teve a duração de 26 horas-aula, que aconteceram entre os meses de setembro a novembro de 2017, na grade horária curricular de Matemática. Vale ressaltar que a professora-pesquisadora não era a professora titular da turma participante do projeto, entretanto, o professor titular participou de todos os encontros.

4.3 Instrumentos de coleta de dados

Para a coleta de dados, foi aplicado um pré-teste (Apêndice A) no primeiro dia do encontro da professora-pesquisadora com a turma, tendo a

finalidade de verificar o nível de conhecimento dos estudantes em relação às técnicas de contagem da Análise Combinatória, e na penúltima aula, após a realização de todas as atividades propostas, foi aplicado um pós-teste (Apêndice B), a fim de verificar se os alunos conseguiram adquirir um conhecimento superior ao que tinham no início do projeto. As duas avaliações cobraram o mesmo conteúdo, da mesma forma, alguns exercícios com enunciados diferentes e outras questões idênticas.

A professora-pesquisadora, junto ao professor titular de Matemática e a equipe pedagógica da escola, definiram que todas as atividades realizadas durante a aplicação do projeto seriam atribuídas uma nota, a qual iria contabilizar na disciplina de Matemática. Sendo essa nota, a média entre as atividades apresentadas a seguir na Tabela 3.

Tabela 3: Atividades referentes à atribuição de notas na disciplina de Matemática.

Atividade		Peso Máximo	
Trabalhos realizados	Pesquisa sobre a Matemática dos Cartões Mágicos	2,5	10
	Trabalho relacionado ao filme: "O código da Vinci"	2,5	
	Lista de exercícios	5	
Feira de Ciências		10	
Pós-teste		10	

Fonte: Próprio autor.

Essas atividades também serviram para a coleta de dados, além da observação direta do comportamento e da fala dos alunos, feitas pelo professor/pesquisador e o professor titular.

4.4 Atividades desenvolvidas em sala de aula

As atividades desenvolvidas na sequência didática foram divididas em 6 etapas, sendo elas:

Atividade 1: Criptografia dos cartões mágicos

Objetivo: Despertar a curiosidade dos alunos em relação à “matemática” utilizada nos cartões mágicos, para que assim, o tema criptografia seja introduzido.

Materiais: Data show, computador, lousa e giz.

Tempo de aplicação: 2 horas-aula.

Desenvolvimento: Na primeira aula, foi apresentado aos alunos, por meio de um data show, os cartões mágicos (Figura 6), e em seguida a professora pediu para que três alunos se voluntariassem para participar da mágica, para que a brincadeira fosse feita três vezes. A função dada ao aluno voluntário, foi que ele escolhesse um número entre 1 e 63 e revelasse esse número somente para os colegas da sala de aula, a professora não teve acesso ao número escolhido. Após todos os colegas terem conhecimento sobre o número “secreto”, a professora aplicou a mágica e o adivinhou. Para isso, os alunos responderam o seguinte questionamento feito pela professora: “O número escolhido tem na primeira tabela?” os estudantes respondiam apenas, sim ou não, essa pergunta foi feita para todas as seis tabelas. Assim que a professora teve acesso a todas as tabelas que o número pertencia, ela o “descobriu”.

Após a brincadeira, foi proposto aos alunos que encontrassem a matemática desses cartões; essa proposta foi passada como um dever de casa, o qual compunha uma parte da nota dada aos “trabalhos realizados”.

Na segunda aula os alunos apresentaram o resultado da pesquisa proposta e compartilharam a matemática dos cartões mágicos. A professora-pesquisadora, além de auxiliá-los no entendimento do truque utilizado, fez uma roda de conversa sobre o conceito de criptografia, citando tópicos da sua história, além de enfatizar a importância dos números binários para o desenvolvimento das tecnologias.

Figura 6: Cartões Mágicos.

1	3	5	7	9	11	13	15	8	9	10	11	12	13	14	15
17	19	21	23	25	27	29	31	24	25	26	27	28	29	30	31
33	35	37	39	41	43	45	47	40	41	42	43	44	45	46	47
49	51	53	55	57	59	61	63	56	57	58	59	60	61	62	63

2	3	6	7	10	11	14	15	16	17	18	19	20	21	22	23
18	19	22	23	26	27	30	31	24	25	26	27	28	29	30	31
34	35	38	39	42	43	46	47	48	49	50	51	52	53	54	55
50	51	54	55	58	59	62	63	56	57	58	59	60	61	62	63

4	5	6	7	12	13	14	15	32	33	34	35	36	37	38	39
20	21	22	23	28	29	30	31	40	41	42	43	44	45	46	47
36	37	38	39	44	45	46	47	48	49	50	51	52	53	54	55
52	53	54	55	60	61	62	63	56	57	58	59	60	61	62	63

Fonte: Chá Mate (2017).

Resultados esperados: Espera-se que o estudante descubra que o truque dos cartões mágicos está na codificação e decodificação dos números indo arábico em números binários, despertando assim a curiosidade pelo tema: criptografia. Isto é, esperamos que o aluno perceba que, ao escolher o número 23, por exemplo, para adivinhá-lo basta somar os números 1 com 2, 4 e 16, pois o número 23 pertence as tabelas que começam com esses algarismos e essa soma resulta em 23.

Ou seja, a chave dessa criptografia é somar os primeiros números no qual o número escolhido pertence. Vale ressaltar que todos os primeiros números dos cartões mágicos são potências de base dois, logo se percebe que os cartões são baseados no sistema binário.

Voltando ao exemplo do número 23, tem-se que ele escrito na forma binário corresponde a 10111, sendo assim, temos a seguinte correspondência, apresentada na Tabela 4.

Tabela 4: Codificação e decodificação do número indo arábico em número binário.

Número Binário (codificado)	1	0	1	1	1	Número indo arábico
Valor dos números de acordo com a sua posição	2^4	2^3	2^2	2^1	2^0	23
Decodificação	16 +	0 +	4 +	2 +	1 =	

Fonte: Próprio autor.

É importante salientar que quando é dito que um número não está na tabela, é porque na escrita binária essa posição corresponde ao dígito zero.

Observação: Caso os alunos não tenham o conhecimento de números binários, será necessário trabalhar, de modo breve, esse conteúdo. Caso os alunos já tenham estudado é importante revê-lo.

Atividade 2: Crifra de César

Objetivo: Conhecer a cifra de César e aplicá-la na codificação e decodificação de palavras.

Materiais: Lousa, giz e apagador.

Tempo de aplicação: 2 horas-aula.

Desenvolvimento: Para o desenvolvimento dessa atividade, os alunos foram agrupados em times compostos por no máximo quatro alunos. A professora-pesquisadora entregou para cada grupo uma folha com as seguintes palavras codificadas:

1º) R F Y J R F Y N H F

2º) G V M T X S K V E J M E

Assim que todos os grupos receberam a folha, foi explicado que essas palavras estavam cifradas e os desafiou a decifrá-las e encontrar a sua chave, os alunos puderam recorrer a pesquisas por meio do celular,

acessando a internet. Nesse momento a professora-pesquisadora assumiu papel de mediadora, auxiliando e orientando os grupos, quando necessário. Após a decodificação a professora-pesquisadora entregou uma nova folha a cada time, contendo o molde da régua de criptografar (Anexo A), para que os alunos a utilizassem para codificar uma nova palavra, com uma chave diferente, e desafiar um outro grupo a decodificá-la e encontrar a chave utilizada. No final da aula, fez-se uma breve roda de conversa sobre a história da criptografia de Júlio César.

Resultados esperados: Espera-se que os alunos consigam encontrar a chave de codificação e decifrem as duas palavras, que no caso, são: (1º) Matemática, (2º) Criptografia, por meio do método de frequência das letras, e também que sejam capazes de codificar uma palavra usando uma chave diferente.

Atividade 3: Atividades de contagem a partir dos cartões mágicos e a cifra de César

Objetivo: Ensinar técnicas de contagem, utilizando inicialmente exercícios sobre os cartões mágicos e a cifra de César, abordando os conteúdos de: fatorial, Permutação Simples e Arranjo Simples, sem o uso de fórmulas, utilizando somente o Princípio Multiplicativo.

Materiais: Lousa, giz e apagador;

Tempo de aplicação: 3 horas-aula

Desenvolvimento: As duas primeiras aulas foram conduzidas a partir dos seguintes exemplos:

- a) Quantos números binários podemos formar utilizando 4 bits (quatro dígitos)?
- b) Pela criptografia de Júlio César, quantos são as possíveis chaves para essa codificação?

- c) Se ao aplicarmos a técnica de substituição para criptografar mensagens, utilizando as 26 letras do alfabeto, sem uma ordem pré-determinada, quantos modos diferentes de criptografar podemos ter?

A professora resolveu os exercícios concomitantemente aos alunos, partindo do conhecimento prévio que eles possuíam sobre contagem, para que eles pudessem perceber o raciocínio envolvido em cada resolução. Em seguida ela propôs as seguintes perguntas, na qual os alunos tiveram um tempo para tentar resolvê-las individualmente:

- 1) Quantas maneiras distintas uma pessoa que tem 5 blusas, 3 calças e 2 sapatos pode se vestir?
- 2) Quantos anagramas, com ou sem sentido, podemos formar com a palavra AMOR?
- 3) Quantas palavras de três letras (com ou sem sentido) podemos escrever utilizando as letras: A, B, C, D, E, F, G, H, I e J?

Para finalizar, a professora-pesquisadora corrigiu os exercícios na lousa. Na aula seguinte os alunos foram divididos em grupos para resolver as seguintes questões:

- 1) Digamos que no planeta Tico o alfabeto seja formado por 45 letras. Quantas maneiras diferentes teremos para criptografar as mensagens? Sendo que a técnica utilizada seja a de substituição, sem uma ordem pré-determinada.
- 2) Quantos números de quatro algarismos distintos podemos formar utilizando os dígitos 0, 1, 2, 3, 4, 5 e 6?
- 3) Quantos números binários de 5 bits podemos formar, sendo que o 3º algarismo (contando a posição da esquerda para a direita) seja ocupado pelo bit 1?

Nessa aula a professora pesquisadora e o professor titular assumiram papéis de mediadores, apenas direcionando os alunos na resolução dos exercícios, quando necessário. Para finalizar, foi feita a correção dos exercícios na lousa.

Resultados esperados: Espera-se que os alunos compreendam o Princípio Multiplicativo como uma técnica de contagem, e consigam aplicá-lo em situações diversas, além de aprender a calcular o fatorial de um número.

Atividade 4: Criptografia presente no filme: O código da Vinci

Objetivo: Desenvolver o conceito de Permutação com Repetição, Arranjo com Repetição e Combinação Simples, sem o uso de fórmulas, apenas pelo Princípio Multiplicativo e Aditivo, baseado nos códigos apresentados no filme.

Materiais: Lousa, giz, apagador, data show, computador e caixa de som.

Tempo de aplicação: 5 horas-aula

Desenvolvimento: Inicialmente, foi passado para os alunos o filme: O Código da Vinci, o qual necessitou de 3 horas-aula. Os alunos tiveram como dever de casa, entregar, via e-mail ou Facebook para a professora-pesquisadora um documento digitalizado, contendo: o resumo do filme, a Matemática do Código da Vinci e a opinião pessoal de cada estudante; essa atividade compunha uma parte da nota dada aos “trabalhos realizados”.

Nas próximas duas aulas a professora-pesquisadora entregou aos alunos uma folha (Apêndice C) com os códigos apresentados no filme, para que, a partir deles, fosse introduzido o conceito de Permutação com Repetição, Arranjo com Repetição e Combinação Simples, sem serem rotulados, ou seja, desenvolvidos por meio do Princípio Multiplicativo e Aditivo.

Resultados esperados: Espera-se que os alunos apliquem o Princípio Multiplicativo e o Aditivo na resolução dos exercícios que foram baseados nos códigos apresentados no filme, que envolvem conceitos de Permutação com Repetição, Arranjo com Repetição e Combinação Simples, sem o uso de fórmulas. É essencial que o aluno perceba a diferença que existe no modo de resolver os exercícios em que a ordem dos elementos formará

grupos distintos e exercícios em que a ordem dos elementos são indiferentes, pois formam o mesmo grupo.

Atividade 5: Apresentação das fórmulas de Contagem

Objetivo: Mostrar aos alunos a existência das fórmulas de contagem e ensiná-los e aplicá-las;

Materiais: Lousa, giz e apagador.

Tempo de aplicação: 4 horas-aula;

Desenvolvimento: Nas duas primeiras aulas a professora-pesquisadora retomou alguns exercícios já resolvidos anteriormente e acrescentou alguns exercícios diferentes, classificando cada um de acordo com seu tipo, ou seja, se o exercício se tratava de Permutação Simples ou com Repetição, se era Arranjo Simples ou com Repetição ou Combinação.

Em seguida definiu cada tópico e apresentou suas fórmulas, após a explicação os alunos foram desafiados a resolver 8 exercícios, todos com duas formas de resolução: com e sem o uso de fórmula. Todos os exercícios foram corrigidos na lousa, e logo após a correção foi entregue para os estudantes uma folha com cinco questões (Apêndice D) para serem entregues na próxima aula; os alunos tiveram a liberdade para resolvê-los com ou sem o uso de fórmulas.

Esses exercícios foram os que compuseram a Avaliação de Aprendizagem em Processo, o qual os alunos já haviam realizado no ano letivo de 2017. A resolução desses exercícios foi parte da nota destinada a “trabalhos realizados”.

Nas outras duas aulas, foi realizada a correção na lousa dos exercícios propostos, todos, com e sem o uso de fórmulas.

Resultados esperados: Espera-se nessa atividade que os alunos percebam como a Análise Combinatória é dividida e que compreendam suas fórmulas, e a encarem como uma ferramenta auxiliar, destinada a facilitar os cálculos. Porém é necessário que percebam que a maioria dos exercícios de

contagem podem ser resolvidos pelo Princípio Multiplicativo e Aditivo, tendo então a sua disposição dois métodos de resolução de problemas: Com o uso de fórmulas e sem o uso de fórmulas.

Atividade 6: Feira de Ciências

Objetivo: Colocar em prática a teoria estudada, aprimorar a comunicação oral, compartilhar o conhecimento adquirido e incentivá-los na busca de conhecimentos científicos.

Tempo de aplicação: 4 horas-aula.

Desenvolvimento: Na primeira aula foi explicado aos alunos o objetivo da feira de ciências. Em seguida os alunos foram divididos em 5 grupos e a professora-pesquisadora propôs a tarefa de cada time, sendo eles: (i) Apresentação da feira, conceito de Criptografia e a aplicação da Matemática nessa ciência, (ii) Os cartões Mágicos e a matemática presente, (iii) Os códigos presentes no filme: O Código da Vinci, com ênfase nos anagramas, (iv) Criptex e suas possíveis senhas e (v) A cifra de César.

Na segunda aula, foi passado para os estudantes um vídeo intitulado “Dicas poderosas para se dar bem ao falar em público”, disponível em: https://www.youtube.com/watch?v=Brm_rfIXN10, seguido de algumas dicas da professora-pesquisadora e do professor titular. Nessa mesma aula houve um ensaio das apresentações. Nas duas próximas aulas, ocorreu de fato a feira de ciências, que contou com a presença dos membros da direção e da coordenação da escola e a presença de um professor da Universidade de São Paulo - USP. Essa feira de ciências compôs uma nota, valendo de 0 a 10.

Resultados esperados: Espera-se que os alunos percebam a aplicação do conteúdo estudado, despertando um interesse pela comunidade científica, além de aprimorar a comunicação oral e o interesse em compartilhar o conhecimento adquirido.

No próximo capítulo será explicado com mais detalhes como ocorreu à aplicação e o desenvolvimento de cada atividade.

5 DESENVOLVIMENTO E ANÁLISE DOS RESULTADOS

Nesse capítulo será descrito as atividades realizadas durante a aplicação do projeto de acordo com os passos da Engenharia Didática. São apresentados os dados obtidos, além da discussão e análise dos resultados de cada fase.

5.1 Primeira fase: Análises Preliminares

Na primeira fase são analisadas as concepções dos alunos, o ensino atual e seus efeitos, e o estudo sobre o sistema educativo no qual se insere o projeto (ARTIGUE, 1988).

Dessa forma, nas análises preliminares foi feito um estudo teórico sobre o ensino e a aprendizagem da Análise Combinatória e sobre a utilização da criptografia como ferramenta educacional no ensino da Matemática. Em relação à pesquisa aplicada em sala de aula, para verificar o nível de conhecimento dos alunos sobre as técnicas de contagem da Análise Combinatória, foi proposto um pré-teste, que foi realizada em sala de aula.

5.1.1 Primeiro encontro

O primeiro encontro se deu em um período de duas horas-aula, iniciando com a apresentação da professora-pesquisadora para a turma, a qual explicou que desenvolveriam um trabalho, que faz parte de uma pesquisa de mestrado, e que tem como objetivo verificar a viabilidade da implementação de uma sequência didática para a Análise Combinatória utilizando a Criptografia como ferramenta educacional. Acrescentou que, por se tratar de uma pesquisa, era necessário obter dados, a fim de verificar se o método que estava sendo desenvolvido seria viável.

A professora-pesquisadora enfatizou que a maioria das atividades desenvolvidas no projeto iriam contabilizar notas na disciplina de

Matemática, como ficou combinado com o professor titular e a coordenação da escola, sendo essa nota a média de três notas, sendo a primeira destinada a “trabalhos realizados”, que foi composto por 3 trabalhos, a segunda, sobre Feira de Ciências e a terceira do pós-teste.

Após a apresentação do projeto para os alunos participantes a professora propôs um pré-teste, composto pelas seguintes questões:

- 1) Na Matemática, muitas vezes aparece o ponto de exclamação, porém com um significado diferente da gramática, como por exemplo: 5! Qual o significado desse ponto na área de exatas?

Objetivo: Verificar se os alunos possuem o conhecimento sobre *fatorial*, e em caso positivo, se sabem explicá-lo.

- 2) De quantas maneiras diferentes se pode vestir uma pessoa que tenha 5 camisas e 3 calças?

Objetivo: Verificar como os alunos reagem sobre um problema de contagem que possui uma pequena quantidade de possibilidades, e analisar o modo de resolução, ou seja, se possuem um conhecimento prévio sobre o Princípio Multiplicativo ou se listam todas as possibilidades para se chegar a resposta final.

- 3) Quantos números de três algarismos podemos escrever com os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9?

Objetivo: Analisar o modo de resolução dos exercícios de contagem que possui uma grande quantidade de possibilidades.

- 4) Quantos números de três algarismos podemos escrever com os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9?

Objetivo: Averiguar se os alunos conseguem distinguir a diferença desse exercício para o anterior, ou seja, se irão perceber o que o dígito zero não poderá ocupar a ordem da centena simples.

- 5) Quantos números de três algarismos DIFERENTES podemos escrever usando os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9.

Objetivo: Examinar se os estudantes conseguem diferenciar o enunciado desse exercício com o exercício três e em caso positivo, se conseguem aplicar alguma técnica de contagem que os ajudem na resolução.

- 6) Anagrama é um substantivo que significa uma palavra ou frase que é construída por meio da alteração das letras de uma outra palavra ou frase, por exemplo: Com as letras da palavra AMOR podemos escrever a palavra ROMA.

Com base na informação acima, quantos anagramas (com ou sem sentido) conseguimos formar com as letras das palavras:

- a) Porta
- b) Matemática

Objetivo: Verificar se os alunos, que não conhecem o significado da palavra anagrama, conseguem compreender pelo exemplo dado no enunciado e analisar o modo de resolução dos estudantes.

- 7) A escrita Braille para cegos é um sistema de símbolos no qual cada caractere é um conjunto de 6 pontos dispostos em forma retangular, dos quais pelo menos um se destaca em relação aos demais.

Por exemplo, a letra A é representada por:

O número total de caracteres que podem ser representados no sistema Braille é?

Objetivo: Verificar se o aluno possui algum conhecimento prévio sobre a escrita Braille, pois é um tipo de criptografia e como os alunos reagem perante a situações problemas que envolvem conhecimentos contextualizados.

- 8) De quantas maneiras diferentes um técnico pode escalar seu time de basquete tendo a sua disposição 12 atletas que jogam em qualquer posição?

Objetivo: Verificar se o aluno consegue distinguir a diferença desse exercício com os demais, ou seja, se ele consegue perceber que a ordem dos elementos não formará conjuntos diferentes.

- 9) (OBMEP 2007) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda a letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

- Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.
- Codifique *OBMEP* usando a chave 20.
- Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.
- Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave?

Objetivo: Introduzir o conceito de criptografia e verificar a interpretação do exercício.

No momento da aplicação do pré-teste houve grande rejeição dos alunos, pois alegaram que não haviam estudado, pois não sabiam que participariam de uma avaliação, e que não tinham conhecimento profundo sobre o assunto, mas quando a professora-pesquisadora explicou o objetivo do teste, que foi de verificar o conhecimento prévio dos alunos, e falou que não iria atribuir nota por essa atividade, os estudantes se acalmaram e deram início a resolução.

5.1.2 Segundo encontro

O segundo encontro da professora-pesquisadora com os alunos teve a duração de uma hora-aula, a qual foi destinada a discussão dos exercícios propostos no pós-teste.

5.1. 3 Resultado da primeira etapa: Análises preliminares

Em relação ao estudo teórico, foi possível perceber que ainda há poucas pesquisas voltadas para esse ramo da Matemática, apesar de ser uma área que apresenta grandes dificuldades, tanto em seu ensino, quanto em sua aprendizagem. Percebe-se que a maioria das pesquisas voltadas para a Análise Combinatória, concentra-se em propor metodologias de ensino baseadas na resolução de problemas e sem o uso excessivo de fórmulas. Em relação à criptografia, foi possível perceber que essa pode ser uma grande aliada ao ensino e aprendizagem da Matemática.

Já pelos resultados do pré-teste, foi possível perceber que os alunos possuíam um conhecimento raso sobre as técnicas de contagem.

Na primeira questão não houve nenhum acerto, entretanto dois alunos afirmaram que $5!$ representa um número primo. Esses estudantes afirmaram já ter visto esse símbolo em Matemática, mas não lembravam exatamente do que se tratava, e associaram a número primo, porque o 5 é número primo, sendo a única associação lógica que conseguiram pensar. Com essa questão pode-se perceber que os alunos não tinham nenhum conhecimento sobre como calcular o fatorial de um número.

Na segunda questão houve um total de 16 acertos, sendo que 10 foram resolvidos pelo diagrama de árvore e 6 pelo Princípio Multiplicativo. Os alunos que acertaram essa questão, afirmaram que essa operação, de verificar as possibilidades de combinação de roupas, faz parte do dia-a-dia, por isso, conseguiram resolvê-la. Os que erraram, justificaram que ao ler a questão, não entenderam na prática, o que exatamente acontecia, sendo assim, não sabiam nem como começar a resolvê-la.

Já na terceira, quarta e quinta questões não houve nenhum acerto, porém três alunos tentaram resolvê-las pelo Princípio Multiplicativo, mas os três aplicaram erroneamente, e da mesma forma, conforme mostra a Figura 6, sendo essa resolução, feita pelo aluno 14. Dois alunos tentaram resolvê-las listando todas as possibilidades, mas não conseguiram chegar à resposta correta.

Figura 6: Resolução do aluno 14.

3) Quantos números de três algarismos podemos escrever com os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9? *27 números*
$$\begin{array}{r} 9 \times \\ 3 \times \\ \hline 27 \end{array}$$

4) Quantos números de três algarismos podemos escrever com os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9? *30 números*
$$\begin{array}{r} 10 \times \\ 3 \times \\ \hline 30 \end{array}$$

5) Quantos números DIFERENTES podemos escrever usando os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9. *de 3 algarismos*
$$\begin{array}{r} 10 \times \\ 3 \times \\ \hline 30 \end{array}$$
 30?

Fonte: Próprio autor.

Os estudantes que tentaram resolvê-la pelo Princípio Multiplicativo, falaram que tentaram seguir o mesmo raciocínio da questão anterior, ou seja, se o número era composto por três algarismos e havia nove números a sua disposição, bastava multiplicar nove por três. Esses alunos não consideraram que para cada algarismo havia uma quantidade de possibilidades, como por exemplo, na questão 3, teriam de pensar que para o algarismo das unidades haviam 9 possibilidades, para o algarismo das dezenas, haviam 9 possibilidades e para o algarismo das centenas, haviam novamente 9 possibilidades, ficando com $9 \times 9 \times 9 = 729$ possibilidades.

Já os estudantes que tentaram listar todas as possibilidades, disseram que não enxergava outro meio para encontrar a resposta, afirmação na qual a maioria dos estudantes se apoiaram, entretanto afirmaram ter preguiça de tentar listá-los, pois parecia ter muitas possibilidades, e como o teste aplicado não iria contabilizar nota, o esforço seria em vão.

Muitos alunos afirmaram que não conseguiram perceber a diferença entre a questão 3, 4 e 5, pois os enunciados eram muito parecidos e não conseguiram distinguir na prática o que mudaria de uma questão para a outra.

Na questão 6, o assunto pedido se referia a quantidade de anagramas possíveis de realizar com as palavras: PORTA e MATEMÁTICA. A maioria dos alunos não tinham conhecimento sobre o que é um anagrama, então, fez-se necessário, uma breve explicação sobre isso, mesmo sendo explicado no enunciado da questão. Porém, nenhum aluno conseguiu chegar à resposta correta, apresentando apenas palavras que faziam sentido no vocabulário deles, como: ORTA, TEMÁTICA, MATE e AMA, resposta na qual mostrou que mesmo com a explicação não compreenderam o que de fato é um anagrama.

Na questão 7 nenhum aluno chegou a resposta correta. Os que tentaram resolver, afirmaram ter 6 possibilidades, justificando que para formar um caractere em Braille temos 6 pontos disponíveis, informação disposta no enunciado. Os alunos não levaram em consideração que, para cada um, desses seis pontos disponíveis para formar um caractere, haviam duas possibilidades, ou o ponto se destacava ou não, sendo assim, haviam 2^6 possibilidades de caracteres que podem ser representadas na escrita Braille. Muitos afirmaram, nunca terem visto um material que representassem a escrita Braille, logo não conseguiram visualizar o que o exercício realmente estava pedindo.

Na oitava questão, não houve nenhum acerto e nem uma tentativa de resolução. Os estudantes afirmaram que não sabiam quantos jogadores de basquete vão a quadra, porém no momento da realização do pré-teste, nenhum aluno levantou essa dúvida a professora-pesquisadora e ao professor titular.

Na alternativa *a* da questão 9, 14 alunos responderam corretamente, o restante justificou não ter entendido o enunciado. Na alternativa *b*, 8 alunos a codificaram usando a chave 5; eles afirmaram não ter entendido como funciona a chave de codificação, então seguiram o desenho disposto

no enunciado; apenas o aluno 12 chegou na resposta correta, conforme mostra a Figura 7. Na alternativa *c* apenas três alunos tentaram resolvê-la, dois erraram e novamente o aluno 12 conseguiu chegar à resposta correta. Os alunos que erraram a questão *b* confundiram novamente a chave 20 com a chave 5, cometendo o mesmo erro, como pode ser exemplificado pela resolução do aluno 1 (Figura 8). Não houve nenhuma tentativa de resolução da alternativa *d*, os alunos falaram que não entenderam o enunciado.

Figura 7: Resolução do exercício feito pelo aluno 12.

9) (OBMEP 2007) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda a letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

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

(b) Codifique *OBMEP* usando a chave 20. 8-21-6-24-3 ✓

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou. *GATO* 26-20-13-8 ✓

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

Fonte: Próprio autor.

Figura 8: Resolução do exercício feito pelo aluno 1.

9) (OBMEP 2007) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda a letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

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

(b) Codifique *OBMEP* usando a chave 20. *19-6-17-9-20* ✗

(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou. *26-20-13-8 (VPID)* ✓

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

Fonte: Próprio autor.

A partir dessa avaliação pode-se perceber que os alunos ainda não haviam tido contato, de fato, com o estudo da Análise Combinatória, apresentando uma média de acertos de 10% do total da prova.

Vale ressaltar, que essa turma sofreu com a troca de professor, pois o professor que iniciou o ano letivo com eles teve que abandonar as aulas, e houve um tempo de dois meses para que essas aulas fossem atribuídas e, de acordo com os alunos, nesse período, alguns professores eventuais trabalharam exercícios parecidos com os que encontraram no pré-teste, entretanto, o assunto foi abordado superficialmente, pois nem sempre o eventual era o mesmo, e geralmente desenvolviam atividades com

conteúdos aleatórios. Fato que justifica o pouco conhecimento sobre o assunto abordado.

5.2 Segunda fase: concepção e análise *a priori*

A segunda fase de acordo com Bitencourt (2017) fundamenta-se no levantamento das hipóteses e no planejamento da sequência didática, ou seja, nessa fase a pesquisa é focada no aluno.

Sendo assim, na fase de concepção e análise *a priori* elaborou-se a Sequência Didática, apresentada na Tabela 5.

Tabela 5: Sequência Didática.

Etapas	Atividades desenvolvidas	Tempo Hora- aula
1ª Introdução à Criptografia	Atividades 1 e 2	4
2ª Introdução a Técnicas de Contagem	Atividade 3	3
3ª Desenvolvimento de técnicas de contagem a partir do filme: O Código da Vinci	Atividade 4	5
4ª Feira de Ciências	Atividade 5	4
5ª Uso das fórmulas de contagem	Atividade 6	4

Fonte: Próprio autor.

A partir dessa Sequência Didática, acredita-se que é possível obter um bom aprendizado das técnicas de contagem da Análise Combinatória, pois aliando o conteúdo matemático a criptografia, tem-se a chance de despertar a curiosidade dos estudantes, fazendo com que o aprendizado ocorra por consequência. Ou seja, de imediato o aluno não estará preso a decorar uma fórmula para aplicá-la na resolução de um problema matemático, mas estará descobrindo técnicas de contagem a partir do conhecimento de uma nova ciência; técnicas nas quais, em seguida, aplicará em outros contextos matemáticos.

Além disso, essa maneira de ensinar possibilita o desenvolvimento e aprimoramento de habilidades como: o trabalho em equipes e a divisão de tarefas, liderança, organização, domínio do tempo e a autonomia no processo de aquisição de conhecimento.

5.3 Terceira fase: aplicação de uma Sequência Didática

Nessa etapa, foi aplicado a Sequência Didática e o pós-teste, seguido de sua correção. Para isso, foram necessárias vinte e seis horas-aula, sendo três destinadas a apresentação do projeto e aplicação do pré-teste; vinte horas-aula para a aplicação da sequência didática e três para aplicação do pós-teste e sua correção. A Sequência Didática foi dividida em cinco etapas, e teve início no terceiro encontro.

5.3.1 Primeira etapa

Na primeira etapa realizou-se o desenvolvimento das atividades 1 e 2, que foram desenvolvidas em 4 aulas, sendo 2 para cada atividade.

5.3.1.1 Atividade 1

No início dessa atividade a professora-pesquisadora mostrou aos alunos os cartões mágicos, por meio de um data show e aplicou a mágica. A princípio a professora pediu para que três alunos se voluntariassem para participar da brincadeira, entretanto, após a participação desses três, a maioria dos alunos quiseram participar. Os estudantes ficaram maravilhados com a “mágica” e queriam que o truque fosse revelado, a professora-pesquisadora deu um tempo para os estudantes tentarem descobrir o truque utilizado, mas nenhum aluno conseguiu descobri-lo, apesar de terem tentado muito, alguns alunos afirmaram que era “pegadinha” e outros tentaram achar padrões numéricos na tabela. O aluno 8, afirmou ter descoberto o truque e quis aplicar com a professora-pesquisadora, no entanto, a tentativa falhou,

vale ressaltar que esse aluno, de acordo com o professor titular, raramente participa das aulas.

Em seguida, foi proposto aos alunos uma pesquisa, que fez parte da nota destinada a “trabalhos realizados”, para ser entregue na próxima aula, a qual seria composta pela explicação matemática do truque presente nos cartões mágicos.

Quando terminou a aula, o aluno 8 fez o seguinte comentário com a professora: “É dona, sacanagem isso aí, vacilona a senhora hem, deixa a gente curioso e vai embora”. Com essa fala, foi possível perceber que a atividade realizada, realmente despertou interesse nesse aluno e que ela não foi vista como algo “chato”, mas sim descontraído e interessante. Após esse comentário a professora estimulou esse aluno e toda a turma a realizar a pesquisa, para então descobrir a mágica.

Na aula seguinte, apenas nove alunos apresentaram a pesquisa realizada, incluindo o aluno 8, o professor titular se surpreendeu com esse fato, pois como dito anteriormente, ele não era participativo nas aulas e consequentemente, quase não realiza as tarefas propostas na escola.

Os estudantes, que pesquisaram, afirmaram não ter entendido a matemática envolvida nos cartões mágicos, mas descobriram que para encontrar o número “secreto” basta somar os primeiros números da tabela. Alguns estudantes que fizeram a pesquisa imprimiram o cartão e aplicaram a mágica com o restante da sala, explicando a forma que encontram o resultado desejado, nesse momento, a professora-pesquisadora não interferiu, proporcionando um tempo da aula para essa troca de conhecimentos.

Em seguida, a professora-pesquisadora explicou o truque utilizado, ou seja, como é codificado e decodificado os números da tabela para que a mágica possa acontecer. Porém, nesse momento houve um empecilho, pois a maioria dos estudantes não tinham conhecimento sobre números binários, então fez-se necessário uma breve explicação, para poder explicar os cartões mágicos. Em seguida foi realizada uma roda de conversa sobre o tema: Criptografia; citando a sua importância nas guerras, na tecnologia e na

segurança pessoal. Muitos alunos associaram esse tema a códigos que eles usam para comunicar entre si, citaram alguns filmes em que a criptografia é utilizada, e comentaram sobre a mensagem que aparecia no WhatsApp, que se referia a uma criptografia de ponta-a-ponta. Os estudantes demonstraram ter interesse e curiosidade sobre o tema.

Aplicar a atividade dos cartões mágicos no início da aplicação do projeto foi uma excelente escolha, pois possibilitou despertar nos alunos uma enorme curiosidade sobre o truque utilizado e a introduzir o tema de criptografia utilizando esse conceito, o qual os alunos demonstraram grande interesse. O aluno 10 fez o seguinte comentário, perante os colegas de classe, no final da aula: “Nossa dona, eu não gosto de Matemática, mas ela é muito louca, tem cada coisa da hora”. Fala que a maioria dos alunos concordaram.

5.3.1.2 Atividade 2

Para iniciar, os alunos foram agrupados em times, de no máximo 4 alunos, o qual eles mesmo formaram. Logo depois, receberam uma folha com duas palavras codificadas e foram desafiados a decodificá-las. A professora explicou somente o que era para ser feito, mas não deu nenhuma dica sobre como decifrar as palavras, entretanto autorizou o acesso à internet via celular, somente para quem tivesse acesso imediato. Apenas dois alunos, participantes do mesmo grupo, consultaram a internet; esse grupo foi o primeiro a decifrar a mensagem. Entretanto, logo que conseguiram decodificar as palavras, falaram em voz alta o seu significado, fato que desestimulou os outros grupos a continuarem tentando. Mas após falarem a resposta correta, todos os integrantes desse grupo foram auxiliar e mostrar aos demais como conseguiram chegar à resposta.

Ao explicar para a professora, como chegaram à resposta correta, afirmaram que começaram pela primeira palavra, pois aparentemente estava mais fácil de descobrir, sendo que a letra F se repetia 3 vezes, logo, associaram o F ao A, e pensaram nessa palavra como uma brincadeira da

força, no qual, fizeram o seguinte esquema: _ A _ _ _ A _ _ _ A e dessa forma, foram tentando várias palavras que se encaixava nesse esquema, quando encontraram a palavra MATEMÁTICA, não tiveram dúvidas que era a palavra certa, pois está relacionada a área de ensino da professora-pesquisadora; usando o mesmo raciocínio, ficou mais fácil descobrir a segunda palavra, que provavelmente também estaria relacionada a área de ensino, então, chegaram rapidamente a conclusão de que a segunda palavra era CRIPTOGRAFIA.

Esse raciocínio foi excelente, pois mesmo sem perceber, os alunos utilizaram o conceito de frequência das letras para começar a resolução.

Após essa atividade foi entregue a cada grupo um molde com a régua de criptografar, a professora fez uma breve explicação sobre a criptografia de César e explicou como que a régua de criptografar iria os ajudar a codificar e decodificar uma mensagem por meio dessa cifra. Nesse momento foi introduzido o conceito de chave de codificação e sobre o método de frequência de letras utilizado para quebrar cifras de substituição. Nesse momento, os alunos lembraram-se da questão 9 do pré-teste, que abordava esse tipo de conceito, e alguns perceberam seu erro.

Após a explicação, foi proposta a turma a codificar uma palavra e desafiar outro grupo a decodificá-la e encontrar sua chave. Nessa atividade a professora-pesquisadora assumiu papel de mediadora, mas quase todos os grupos necessitaram de um apoio. Os estudantes procuraram codificar palavras que não tinham letras repetidas. Apenas um grupo conseguiu decodificar a palavra proposta pelos colegas. Nessa parte da atividade, houve muitas dúvidas, fato que levou a professora-pesquisadora interromper a atividade para poder explicar novamente, por meio de exemplos, a técnica de frequência de letras para quebrar um código, e a manipulação da régua de criptografar.

No final da aula, teve uma roda de conversa sobre a criptografia de Júlio César e sobre a opinião dos alunos sobre essa técnica. Muitos alunos acharam confuso, mas afirmaram que depois que a professora-pesquisadora exemplificou ficou mais fácil de entender. Alguns alunos comentaram que

essa técnica iria auxiliá-los na hora das provas, pois poderiam “colar” sem serem descobertos.

5.3.2 Segunda etapa

Na segunda etapa foi aplicado a atividade 3, a qual foi desenvolvida em três aulas, distribuídas em 2 dias.

Nas duas primeiras aulas, foi introduzido as técnicas de contagem a partir de exemplos e exercícios sobre números binários e a cifra de César. Em uma primeira explicação, com a apresentação dos três questionamentos, foi possível perceber que a maioria dos alunos acreditavam que, para resolver problemas de contagem era necessário listar todas as possibilidades, mas não levaram em consideração que esse método é viável somente se o número a ser contado for pequeno.

A fim de estimular o raciocínio dos alunos, a professora utilizou exemplos como: Quantas placas de carros, que possuem 3 letras e 4 números podemos formar? Para que, dessa forma, os alunos percebessem que listar todas as possibilidades, em exercícios que o número de elementos a ser contado é muito grande, não é viável, pois se torna exaustivo e com grandes chances de erros. Dessa forma, introduziu o Princípio Multiplicativo, mostrando seu objetivo e sua aplicação nos exemplos dados.

Em seguida a professora propôs três exercícios para que os alunos tentassem resolvê-los individualmente. Os alunos mostraram bastante dificuldade em solucionar as questões por meio do Princípio Multiplicativo, a técnica da listagem das possibilidades foi muito utilizada. A correção foi feita na lousa, seguida de uma explicação detalhada de cada exercício, por meio do Princípio Multiplicativo.

Nesse momento foi possível perceber que os alunos tiveram muita dificuldade em aplicar a técnica ensinada, porque eles focavam em quais eram as possibilidades e não quantas eram as possibilidades, fato que foi esclarecido durante a resolução feita pela professora. Um comentário no qual chamou a atenção foi do aluno 7, que disse: “Dona, se eu não colocar

todas as possibilidades, como eu vou ter certeza que essas quantidades são verdadeiras?”, as quantidades a qual ele se referia, foi sobre o resultado obtido por meio do Princípio Multiplicativo.

Então a professora explicou que existe uma área da Matemática, chamada Análise Combinatória, que tem por objetivo desenvolver ferramentas para facilitar a contagem, e como no início da aula, a professora havia resolvido dois exemplos extras por meio do diagrama de árvore e pelo Princípio Multiplicativo, ela os retomou e enfatizou que pelos dois modos, obteve o mesmo resultado, e nesse momento, aproveitou para falar sobre o desenvolvimento da Matemática, alguns matemáticos, sobre provas e demonstrações, e sobre a evolução histórica dessa ciência.

Na aula seguinte, a sala foi agrupada em times, formados pelos próprios alunos e foram desafiados a resolver três exercícios. A professora-pesquisadora e o professor titular auxiliaram os grupos, os quais apresentaram pequenas dúvidas nos exercícios 1 e 2, e grande dificuldade no exercício 3, sendo necessário uma explicação mais detalhada sobre o mesmo.

Após os alunos terem tentado resolver as questões, a professora-pesquisadora fez a correção na lousa e foi surpreendida com o seguinte comentário do aluno 17, o qual se destaca por possuir boas notas “Professora, eu troquei letras, fiz mágica e agora só estou fazendo continha de multiplicação, e isso eu já sei, o que de novo eu estou aprendendo?” antes da professora-pesquisadora responder, o aluno 19 respondeu “nossa pobre é pobre e sempre vai ser pobre, você não viu a dona explicar a outra aula que isso faz parte de negócio da Matemática, e agora se você pegar a prova que ela deu no começo, você vai saber resolver um monte e na nossa prova do governo caiu um monte de questão dessa”, nesse momento a professora fez uma intervenção, e conversou com o aluno 19, o qual afirmou que estava acostumado com fórmulas e aplicações de fórmulas, por isso demonstrou esse estranhamento na forma de ensinar e de aprender.

A professora-pesquisadora novamente explicou sobre o conceito de Análise Combinatória e acrescentou que futuramente, as fórmulas presentes

nesse conteúdo seriam apresentadas, entretanto, o objetivo naquele momento era desenvolver o raciocínio combinatório, sem o uso das fórmulas, para que eles desenvolvessem a competência de resoluções de problemas.

Essa etapa foi de fundamental importância para introduzir o conceito do Princípio Multiplicativo. A maioria dos alunos participaram da aula e conseguiram absorver o conteúdo trabalhado, nessa etapa os alunos conseguiram entender de fato o que é um anagrama, tiveram conceitos iniciais sobre a definição de fatorial, que, de imediato gostaram, por ser uma forma de representar o resultado sem a necessidade de efetuar muitas operações, e mesmo sem rotular, resolveram exercícios sobre Arranjo Simples, por meio do Princípio Multiplicativo.

Vale ressaltar, que o aluno 8, teve uma participação significativa, o qual, geralmente, não acontecia nas outras aulas; outra surpresa foi o aluno 7, que tinha um comportamento extremamente ativo, fato que dificultava a concentração nas explicações e na resolução individual das atividades propostas, entretanto, na atividade em grupo, ele mostrou ter compreendido o assunto, fato que o levou a explicar o conteúdo para os integrantes do seu time, o qual era composto por alunos com desempenho satisfatório na disciplina de Matemática.

5.3.3 Terceira etapa

Nessa etapa foi desenvolvida a atividade 4, em um período de 5 horas-aula, sendo guiada pelo filme: O Código da Vinci. Para que o filme não fosse interrompido, foram necessárias 3 horas-aula seguidas, sendo assim, a professora de português contribuiu com uma aula, e as outras duas pertenciam à grade horária de Matemática.

No decorrer da obra muitos alunos se dispersaram, posteriormente se justificando dizendo que o filme foi muito longo e de difícil compreensão.

Nessa etapa, a professora propôs aos alunos uma atividade, que era parte da nota destinada a “trabalhos realizados” na qual era para ser

entregue digitalizado, via e-mail ou facebook com o resumo do filme, a matemática presente e a opinião pessoal. Somente oito alunos apresentaram a atividade feita; desses oito, cinco alunos copiaram o resumo da internet. Sobre a Matemática do filme, todos os que fizeram, citaram os anagramas e a sequência de Fibonacci. Em relação à opinião pessoal, seis alunos demonstraram ter gostado; um fato marcante, foi a opinião do aluno 6, o qual demonstrou ter um conhecimento histórico sobre os fatos apresentados no filme, pois contextualizou a ficção do filme com a realidade. Ainda em relação à opinião pessoal dos estudantes, os alunos 12 e 17 afirmaram não ter gostado do filme, frisando que é desnecessário envolver religião para abordar conceitos matemáticos.

No próximo encontro, composto por duas aulas seguidas, fez-se uma roda de conversa sobre o filme, enfatizando que a obra abordava uma ficção e o intuito educativo foi que os alunos percebessem que o filme é guiado por códigos, os quais são envolvidos pela ciência da Matemática, a qual iríamos estudar, além de enfatizar, que religião, muitas vezes será abordado na escola, principalmente nos conteúdos de história, fato que não precisa interferir na religiosidade de cada um.

Em seguida foi entregue uma folha com cinco exercícios, envolvendo um estudo matemático de alguns códigos apresentados no filme, sendo eles:

- 1) Quantos possíveis anagramas existiam na frase cifrada do primeiro código? (Sem levar em consideração os espaços entre as palavras)
- 2) Quantos anagramas existiam na frase cifrada do segundo código? (Sem levar em consideração os espaços entre as palavras)
- 3) Quantas possíveis senhas Sophie Neveu e Robert Langdon tinham para descobrir a senha correta do banco em que estava o Criptex? (Utilizando os números deixados por Jacques Saunière)
- 4) Quantas possibilidades existiam para a senha do Criptex? Sendo que ele era formado por 5 anéis, e cada um era composto pelas 26 letras do alfabeto.

- 5) Quantas comissões de três integrantes podem ser formadas, tendo a disposição Robert Langdon, Jacques Saunière, Sophie Neveu, Silas, Fache e o Bispo Manuel, para compor o priorado de Sião?

No primeiro e segundo exercícios os alunos aplicaram o Princípio Fundamental da Contagem sem levar em consideração os elementos repetidos, sendo assim, foi necessária uma explicação mais detalhada. O terceiro e o quarto exercícios não apresentaram muitas dificuldades, já no quinto exercício, foi fundamental a exemplificação de outras situações, para que o aluno percebesse a diferença entre um exercício que, a ordem dos elementos agrupados altera o resultado, e os que a ordem não altera, pois se tratava de um problema de Combinação.

Nessa etapa, foi possível perceber que os alunos já haviam absorvido o básico do conteúdo ensinado, porém o conteúdo de Combinação precisava ser abordado com mais frequência, para que os alunos compreendessem de fato a diferença entre as diversas situações problemas.

5.3.4 Quarta etapa

Nessa etapa foi desenvolvida a atividade 5, a qual ocorreu a feira de Ciências, que teve a duração de 4 horas-aula. É importante ressaltar que a Feira de Ciências, foi uma atividade realizada pela escola, no qual cada professor, voluntariamente se encarregava de organizar a apresentação de uma turma, entretanto, nenhum professor se disponibilizou a se responsabilizar pelo 2º ano.

Perante a essa situação, a professora-pesquisadora entrou em contato com a direção e combinaram que, a apresentação do segundo ano seria baseada no projeto que estava sendo aplicado, no entanto, não seria possível apresentar no mesmo dia que os demais, o qual foi em um sábado letivo, pois o projeto ainda estava no início. Dessa forma adiaram em um mês a apresentação do segundo ano, o qual ocorreu em um dia letivo no período da aula de Matemática.

Para a realização da Feira de Ciências, foram destinadas duas aulas para a preparação e duas para a apresentação.

Inicialmente a turma foi dividida em cinco grupos, formada pelos próprios alunos, cada um, com uma tarefa diferente, conforme pode-se ver na Tabela 6.

Tabela 6: Tarefa de cada grupo.

Grupo	Tarefa
Grupo 1	Apresentação da feira, conceito de Criptografia e a aplicação da Matemática nessa ciência
Grupo 2	Os cartões Mágicos e a matemática presente
Grupo 3	Os códigos presentes no filme: O Código da Vinci, com ênfase nos anagramas
Grupo 4	Criptex e suas possíveis senhas
Grupo 5	A cifra de César

Fonte: Próprio autor.

Após a tarefa dada, foi criado um grupo no WhatsApp, com a participação da professora-pesquisadora e os alunos, a fim de que a professora-pesquisadora pudesse auxiliar, mesmo fora do horário de aula, os preparativos para a feira.

Em um dia anterior a apresentação da Feira de Ciências, foi reproduzido um vídeo com dicas para uma boa apresentação, intitulado: “Dicas poderosas para se dar bem ao falar em público”, além de que houve um ensaio da apresentação final, na qual os grupos 2, 4 e 5 apresentaram a professora-pesquisadora os aparatos que construíram para utilizar no dia da apresentação. O grupo 2 construiu um aparato para explicar a matemática dos cartões mágicos (Figura 9); o grupo 4 construiu um equipamento que

simulava o criptéx (Figura 10); e o grupo 5 construiu duas régulas de criptografar (Figura 11).

Figura 9: Aparato construído pelo grupo 2.

6 ^{to} tab	5 ^{to} tab	4 ^{to} tab	3 ^{to} tab	2 ^{to} tab	1 ^o tab	Regras
32	16	8	4	2	1	Regras tabelas usadas
2^5	2^4	2^3	2^2	2^1	2^0	Regras em potências de base 2
1	1	1	1	1	1	Nº codificado escrito em forma binária
32	16	8	4	2	1	Nº decodificado forma decimal

1 3 5 7 9 11 13 15	2 4 6 8 10 12 14 16	3 5 7 9 11 13 15 17
17 19 21 23 25 27 29 31	18 20 22 24 26 28 30 32	20 22 24 26 28 30 32 34
33 35 37 39 41 43 45 47	34 36 38 40 42 44 46 48	36 38 40 42 44 46 48 50
49 51 53 55 57 59 61 63	50 52 54 56 58 60 62 64	52 54 56 58 60 62 64 66
8 10 12 14 16 18 20 22	16 18 20 22 24 26 28 30	24 26 28 30 32 34 36 38
24 26 28 30 32 34 36 38	24 26 28 30 32 34 36 38	26 28 30 32 34 36 38 40
40 42 44 46 48 50 52 54	48 50 52 54 56 58 60 62	40 42 44 46 48 50 52 54
56 58 60 62 64 66 68 70	56 58 60 62 64 66 68 70	58 60 62 64 66 68 70 72

Fonte: Próprio autor.

Figura 10: Aparato construído pelo grupo 4.

Fonte: Próprio autor

Figura 11: Aparato construído pelo grupo 5.

Fonte: Próprio autor.

A apresentação final contou com a presença de um professor da USP, do vice-diretor, da coordenadora, do professor titular e dos professores e alunos do Ensino Médio, da escola de aplicação do projeto.

Essa atividade teve um peso de 0 a 10, sendo que foi avaliada pela professora-pesquisadora, pelo professor titular e o professor da USP, os quais preencheram uma ficha para cada grupo, contendo os seguintes quesitos.

- Postura no momento da apresentação;
- Clareza na explicação do conteúdo;
- Domínio do assunto abordado;
- Qualidade dos acessórios utilizados.

Cada quesito tinha um valor mínimo de 0 e máximo de 2,5.

Essa etapa foi extremamente importante no desenvolvimento do projeto, pois nesse momento, os alunos já não estavam com a mesma empolgação que no início. Apenas dois alunos não participaram dessa atividade, um porque não estava presente no dia e outro porque não se identificava com a professora-pesquisadora.

Um dia antes da apresentação os alunos combinaram entre si, e além dos objetos necessários para a apresentação, levaram aperitivos para fazer um café da manhã, e toalhas de mesa para enfeitar a sala. No dia da apresentação, quando a professora-pesquisadora chegou à escola, os alunos já haviam preparado a sala de aula, já estavam com os objetos dispostos e haviam ensaiado novamente, fato que surpreendeu.

As apresentações foram surpreendentes, o grupo 1, que foi composto por alunos com comportamentos retraídos, mostrou uma grande desenvoltura, mostraram ter pesquisado a fundo o tema e apresentaram com muita clareza e confiança. Os grupos 2 e 3 apresentaram de forma brilhante. O grupo 4, era formado por alunos que apresentaram baixo índice de presença e pouca participação nas aulas, entretanto, a apresentação foi excelente; esse grupo, além de apresentar a cifra de César propuseram aos participantes um desafio, e quem resolvesse era premiado com guloseimas (Figura 12).

Figura 12: Aplicação da atividade proposta pelo grupo 5.

Fonte: Próprio autor

No final da apresentação, o professor da USP e os participantes da coordenação da escola elogiaram e incentivaram os alunos a participarem da vida acadêmica e a dar continuidade na busca pelo conhecimento.

A realização dessa feira motivou novamente os alunos a darem continuidade no projeto.

5.3.5 Quinta etapa

De acordo com a didática da Matemática, é papel do professor propor aos alunos situações de aprendizagem contextualizadas, no qual os alunos possam dar sentido no conhecimento e ajudá-los no sentido inverso, ou seja, descontextualizando os conhecimentos, de modo análogo aos matemáticos, que conduzem as produções dos fatos universais e reutilizáveis em outras situações e contextos (POMMER, 2013).

Nesse sentido, essa etapa, que se apropria da atividade 6, teve como objetivo mostrar as fórmulas de contagem e aplicação de técnicas matemáticas em contextos diferentes. Para seu desenvolvimento, foi necessária a utilização de 4 horas-aula, divididas em dois encontros.

No primeiro encontro, a professora utilizou os exercícios já realizados em sala de aula, para que, a partir deles, pudessem apresentar as fórmulas, como por exemplo, na apresentação de Arranjo com Repetição, a professora retomou e escreveu na lousa o seguinte exercício:

- Quantas possibilidades existiam para a senha do Criptéx? Sendo que ele era formado por 5 anéis, e cada um era composto pelas 26 letras do alfabeto.

A professora o resolveu novamente com a turma, utilizando o Princípio Multiplicativo, conforme a seguir.

Resolução:

Se temos 5 anéis e cada um possui 26 possibilidades, tem-se que as possibilidades são dadas pela operação:

$$26 \times 26 \times 26 \times 26 \times 26 = 26^5$$

Em seguida, a professora-pesquisadora definiu esse exercício como: ARRANJO COM REPETIÇÃO e aplicou a seguinte fórmula:

$$A_{n,p} = n^p \quad (1)$$

Sendo n o número de elementos do conjunto e p a quantidade de elementos por agrupamento.

$$A_{26,5} = 26^5$$

Após definir o exercício como sendo um problema de Arranjo com Repetição e resolvê-lo utilizando a fórmula, a professora explicou o conceito de Arranjo Simples, o definiu e aplicou outros exercícios sobre o mesmo. Esse processo se repetiu com os conceitos de: Permutação Simples, Permutação com Repetição, Arranjo sem Repetição e Combinação Simples. No final da aula, foi entregue aos alunos uma folha, contendo cinco situações problemas de Análise Combinatória; exercícios que foram retirados da Avaliação de Aprendizagem em Processo de 2017, aplicada na turma do segundo ano, antes do início do projeto, a qual apresentaram baixo desempenho, segundo o professor titular.

No segundo encontro, ocorreu a correção dos exercícios, o qual fez parte da nota destinada a “trabalhos realizados”. Essa foi a primeira atividade que grande parte dos alunos tentaram resolver, dos 22 alunos, 18 apresentaram tentativas de resolução, as quais nenhuma utilizou as fórmulas. Entretanto, a maioria encontrou muita dificuldade nesses exercícios, afirmando serem muito complexos, mesmo após a explicação de cada um, pela professora-pesquisadora.

Nessa etapa, foi possível perceber que a apresentação das fórmulas gerou um sentimento de medo nos alunos. No momento em que as fórmulas foram apresentadas e aplicadas, muitos alunos afirmaram que a professora-pesquisadora estava confundindo a cabeça deles, que esse assunto era muito difícil, que eles tiveram a sensação de que não aprenderam nada e

muitos chegaram a dizer que odeia a Matemática por isso, ou seja, de imediato parece ser fácil, mas depois complica.

Na resolução dos exercícios em sala de aula, a maior dificuldade enfrentada foi em descobrir qual fórmula usar, mesmo com o auxílio da professora-pesquisadora e do professor titular. O aluno 17, que havia questionado a professora-pesquisadora sobre o método de ensino, a agradeceu por ensinar pelo método de “multiplicação”, pois eram muitas fórmulas e confusas entre si para poder aplicá-las. O aluno 8 interrompeu a professora, no momento em que apresentava as aulas, e disse: “aqui ó dona, eu só faço continha de vezes e chego na mesma resposta que a senhora, pra que usar esses bagulhos aí? eu não vou nem prestar atenção, porque vai confundir a minha mente”. A professora-pesquisadora explicou a ele e a turma que não era necessário decorar as fórmulas, mas a estava apresentando, pois é um segundo método de resolução, e pode ser que algum aluno se identificasse com essa ferramenta, e por isso não poderia deixar de apresentá-las e explicar sobre cada tópico separadamente.

5.3.6 Pós-teste e correção

O pós-teste foi aplicado em um período de 2 horas-aulas, o conteúdo exigido era o mesmo do conteúdo do pré-teste, com pequenas alterações, a fim de avaliar se os alunos conseguiram absorver o conteúdo de Análise Combinatória e se houve avanços em relação a primeira prova.

O objetivo dessa avaliação era de verificar se os alunos conseguiriam aplicar os conteúdos estudados em sala de aula em uma avaliação individual, da forma que se identificassem, ou seja, por meio de fórmulas ou pelo PFC ou pelo diagrama de árvore. E a questão sobre criptografia tinha como objetivo verificar se eles compreenderam essa técnica. Cada questão teve valor de 1 ponto.

As maiores dificuldades, encontradas pelos alunos, isto é, as questões que apresentaram o maior índice de erro, foram a primeira e décima questões.

Na primeira questão, a maioria dos estudantes conseguiram calcular o valor pedido, entretanto se confundiram na hora de explicar o conceito de fatorial. Vejamos na Tabela 7, algumas respostas.

Tabela 7: respostas da primeira questão.

Aluno	Resposta
Aluno 2	Esse ponto na área de exatas se chama fatorial, fatorar é multiplicar o mesmo número várias vezes, ou números diferentes em ordem decrescente.
Aluno 9	O significado desse ponto é que ele é fatorial. Recebe o nome de seis fatorial, seu valor é de: 6.5.4.3.2.1
Aluno 15	Recebe o nome de "fatorial". Significa que por trás tem uma sequência de números decrescente. Exemplo $6! = 6.5.4.3.2.1 = 720$

Fonte: Próprio autor.

Nessa questão, foi possível perceber a dificuldade que os alunos possuem em explicar os conhecimentos matemáticos.

As questões 2, 4, 5, 6, 7, 8 e 9 não apresentaram grandes dificuldades, entretanto, por elas, foi possível perceber que os alunos tinham dificuldades em resolver operações de multiplicação, dos 20 alunos que participaram do pós-teste, 14 cometeram erros na operação de multiplicação, como pode-se ver na Figura 13. Entretanto, por elas foi notório que os alunos conseguiram absorver o PFC e aplicá-los a situações problemas, como pode-se observar na Tabela 8.

Figura 13: Resolução com erros na operação de multiplicação.

Fonte: Próprio autor.

Tabela 8: Exemplos de resoluções corretas na avaliação final.

Questão	Resolução correta
2
4
5	<p>5) Anagrama é um substantivo que significa uma palavra ou frase que é construída por meio da alteração das letras de uma outra palavra ou frase, por exemplo: Com as letras da palavra AMOR podemos escrever a palavra ROMA.</p> <p>Com base na informação acima, quantos anagramas (com ou sem sentido) conseguimos formar com as letras das palavras:</p> <p>a) Escola $6!$</p> <p>b) Paralelepípedo $\frac{4!}{2!2!2!}$</p> <p>c) Bola, em que as letras O e L apareçam juntas e nessa ordem (OL) $4!$</p> <p>Handwritten calculations for permutations are shown for each option, with the final answer '4!' circled.</p>
6
7
8	<p>(a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13. SUCURI</p> <p>(b) Codifique OBMEP usando a chave 20. 8-21-6-24-9</p> <p>(c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou. 26-20-13-8 GATO</p> <p>(d) Em uma outra chave, a soma dos números que representam as letras A, B e C é 52. Qual é essa chave? (chave 25) A=25 B=26 C=1 = 52</p>
9

Fonte: Próprio autor.

No dia da correção do pós-teste os alunos justificaram que, nem ao menos tentaram, pois a questão parecia ser muito difícil, e muitos acrescentaram que já haviam garantido um “cinco” na prova, então já era o suficiente.

5.4 Quarta fase: análise *a posteriori* e validação

Na quarta fase ocorre a análise dos dados obtidos durante a aplicação do projeto, para que, as hipóteses levantadas nas análises *a priori* possam ser validadas.

Para isso, a professora-pesquisadora, no final do desenvolvimento da sequência didática, aplicou um pós-teste, para comparar a quantidade de acertos com o pré-teste, e medir o tamanho do ganho educacional de acordo com o fator $\langle g \rangle$ de Gery (1972).

O fator $\langle g \rangle$ Gery (1972) é calculado da seguinte maneira:

$$\langle g \rangle = \frac{\bar{n}_2 - \bar{n}_1}{\bar{n}_m - \bar{n}_1} \quad (2)$$

Sendo:

$\bar{n}_1$: Média de acertos do pré-teste;

$\bar{n}_2$: Média de acertos do pós-teste;

$\bar{n}_m$: Nota máxima que o aluno pode alcançar.

Os valores obtidos são classificados de acordo com a Tabela 9.

Tabela 9: Classificação dos valores do tamanho do ganho educacional pelo fator G de Gery.

Classificação	Valores
Ganho baixo	$0,00 < g < 0,30$
Ganho médio	$0,30 < g < 0,70$
Ganho alto	$g > 0,70$

Fonte: Gery (1972).

Analisando-se os resultados dos estudantes que participaram das duas provas, ou seja, 20 alunos dos 22 participantes, temos que a média do pré-teste foi de 1,2, com desvio-padrão de 0,6; enquanto a média do pós-teste foi de 6,2 com desvio-padrão de 1,3. Conforme pode-se observar pelo Gráfico 1.

Gráfico 1: Média e desvio-padrão da turma participante do projeto.

Fonte: Próprio autor.

Calculando o tamanho do ganho educacional $\langle g \rangle$ de toda a turma, obteve-se um valor de aproximadamente 0,57, o qual é considerado um ganho médio.

Entretanto, apenas 15 alunos obtiveram, no mínimo, 75% de presença nas aulas destinadas à aplicação do projeto, salientando que, esses 15 estudantes participaram das duas avaliações.

Comparando a média obtida no pré-teste com a média do pós-teste, dos 15 alunos que tiveram maior participação na aplicação do projeto, percebe-se uma evolução de 6,1 pontos, e um desvio-padrão de 0,7 no pré-teste e 1,1 no pós-teste; o qual se pode ver no Gráfico 2.

Gráfico 2: Média dos alunos frequentes no pré-teste e pós-teste.

Fonte: Próprio autor.

Calculando-se o tamanho do efeito do ganho educacional $\langle g \rangle$ desses 15 alunos, obteve-se um valor de aproximadamente 0,69, o que é considerado também, um ganho médio, quase um ganho alto.

Apesar do nome, ganho médio, indicar uma evolução mediana, foi considerado, na dissertação aqui presente, uma grande evolução, pois enxerga-se o processo de ensino e de aprendizagem como algo contínuo e que necessita de muito empenho e muita dedicação por um longo período de tempo para se chegar a obter uma evolução considerada alta. Sendo assim, no período que nos foi dado, ou seja, 26 horas aulas, se obter um ganho educacional médio é muito satisfatório.

Em relação ao desenvolvimento individual dos alunos, chamamos a atenção para as notas obtidas pelos alunos 6 e 8.

O aluno 6, teve um avanço considerado satisfatório, pois sua média em Matemática do primeiro e do segundo bimestre de 2017 foi de 2,5 já a nota alcançada no pós-teste foi de 4,8, o que consideramos um grande avanço, e como esse aluno realizou todas as atividades propostas, sua média final no projeto, foi de 7,3.

O aluno 8 que afirmava não gostar de Matemática e possuir um comportamento extremamente ativo, atingiu uma nota de 4,28 no pós-teste, o qual evoluiu, se comparado com as notas atingidas nos outros conteúdos de Matemática, que tem média de 2,23. Esse estudante alcançou uma média final, nesse projeto, de 7.

Dos 22 alunos participantes, apenas 2 alunos obtiveram média no projeto inferior a 5, como podemos ver no Gráfico 3.

Gráfico 3: Média dos estudantes no projeto.

Fonte: Próprio autor.

Os alunos que não atingiram uma média superior a 5 foram os alunos 4 e 22. O aluno 4 se recusou a participar da Feira de Ciências, pois afirmou não ter conhecimento do ocorrido, sendo assim, ele obteve zero nessa atividade, fato que diminui sua média, porém, sua nota no pós-teste foi de 8,25. Já o aluno 22, além de não participar da Feira de Ciências, por motivo de ausência, obteve uma nota de 2,23 no pós-teste, sendo assim, não atingiu uma média considerada razoável.

De acordo com esses resultados, ou seja, com a evolução vista na primeira e na última avaliação e com um ganho educacional considerado médio, percebemos que, com essa turma, foi possível ensinar técnicas de contagem utilizando a criptografia como ferramenta educacional. Além de

que, os tópicos da Análise Combinatória foram abordados baseados no Princípio Multiplicativo e Aditivo, mostrando-se eficiente, mesmo sabendo que os alunos foram conduzidos, desde o início do projeto a utilizar o Princípio Multiplicativo. Não condeno aqui o método fórmula-aplicação, mas priorizo o uso do raciocínio combinatório pelo PFC, o qual possibilita um maior desenvolvimento da competência de resolução de problemas.

O desenvolvimento desse projeto possibilitou aos alunos desenvolverem o exercício de trabalhar em grupo, aumentou a autoconfiança e a auto-estima, aprimorou a habilidade de falar em público, a terem uma melhor gestão do tempo e a autonomia na busca do saber.

No último encontro, alguns estudantes vieram até a professora-pesquisadora, pedindo referências de sites e videoaulas sobre Criptografia, pois acharam o tema interessante e afirmaram dar continuidade nesse estudo.

O aluno 12, a convite da professora-pesquisadora, fez uma apresentação voluntária da “Matemática dos cartões mágicos” em uma escola particular do interior de São Paulo, e pela desenvoltura e segurança que apresentou, foi presenteada pela diretora, com uma bolsa integral para cursar o terceiro ano do Ensino Médio.

O professor titular ficou surpreso com a participação de alguns alunos na sala de aula, e principalmente com a desenvoltura dos estudantes na Feira de Ciências. Ele afirmou ter gostado do método utilizado e ressaltou que, após a aplicação do projeto, os alunos salientaram que gostaram da metodologia utilizada, pois a aprendizagem não foi maçante como seguir uma apostila ou um livro didático, além de que não tinham a obrigação de decorar as fórmulas somente para aplicá-las na prova.

6 CONCLUSÃO

Como viu-se, por meio de pesquisas, o processo de ensino e de aprendizagem da Matemática enfrenta grandes desafios e buscar alternativas para solucioná-los torna-se cada mais necessário.

A área da Matemática destinada à contagem, a Análise Combinatória, apresenta uma resistência negativa tanto no ensino quanto na aprendizagem no ciclo básico.

Tem-se que uma das possíveis causas para a dificuldade no aprendizado desse conteúdo é o confronto que ocorre entre o método que a Matemática é ensinada no ensino básico e a forma como os problemas de contagem não se encaixam nesse padrão. Ou seja, o ensino da Matemática, em sua maioria, ocorre de forma mecanizada, no qual é exposto a teoria, seguido de exemplos, os quais os alunos utilizam a resolução como modelo para a aplicação nos próximos exercícios. Entretanto, quando se deparam com as situações problemas que envolvem conceitos de contagem, fica mais difícil seguir um padrão, pois os exercícios dessa área necessitam de uma flexibilidade de pensamento e de um bom raciocínio; competência que é pouca desenvolvida na disciplina de Matemática, devido a forma como vem sendo ensinada.

Apesar do método: Teoria-Exemplos-Exercícios ainda ser o mais utilizado em sala de aula, percebe-se que alguns livros didáticos já se preocupam em desenvolver habilidades e competências nos alunos, trazendo para a sala de aula temáticas diferenciadas e aplicáveis no dia-a-dia.

Um segundo ponto a ser abordado sobre a dificuldade apresentada nessa área é a confusão que se faz ao tentar descobrir a que tipo de agrupamento o problema pertence, para então, aplicar a fórmula correta.

Não critica-se aqui o método: Teoria-Exemplos-Exercícios e nem o uso de fórmulas no ensino da Análise Combinatória, mas propõe-se uma atividade diferenciada capaz de desenvolver habilidades e competências nos alunos, as quais esses outros métodos não muito contribuem.

A proposta desse trabalho para o ensino para a Análise Combinatória enfatiza o uso do PFC e utiliza a Criptografia como ferramenta educacional. A escolha pela Criptografia se deu ao fato de ser um tema atrativo, presente no dia-a-dia e repleto de Matemática.

Durante a aplicação do projeto, percebe-se que o processo de ensino e de aprendizagem desse conteúdo, da maneira citada acima, apresenta-se como uma maneira alternativa e atrativa aos alunos, e que, se trabalhada de forma coerente, as chances de trazerem bons resultados, são grandes.

A turma beneficiada pela aplicação da proposta aqui presente, apontou resultados satisfatórios. Inicialmente a temática da Criptografia chamou a atenção dos alunos e despertou a curiosidade dos mesmos. A Análise Combinatória aprendida como consequência, ou seja, inicialmente, foram usadas técnicas de contagem para resolver situações que envolviam conteúdos de criptografia, fez com que os alunos adquirissem conhecimentos sobre o PFC sem perceber diretamente que estavam aprendendo um novo conteúdo.

Dessa forma, quando foram propostos novos exercícios, fora do contexto de Criptografia, foi mais fácil trabalhar, pois os alunos já tinham apreendido, mesmo sem perceber, técnicas de contagem. De imediato, os alunos estranharam um novo tópico de Matemática, sem o uso e aplicação frequente de fórmulas, mas ao apresentar as fórmulas aos estudantes, muitos disseram preferir o método do PFC.

Como viu-se nos resultados apresentados no capítulo anterior, obteve-se um ganho educacional médio, o que foi considerado satisfatório.

Sendo assim, verifica-se que é possível implementar uma sequência didática para a Análise Combinatória utilizando o conceito de Criptografia com ênfase no PFC e obterem resultados satisfatórios, claro que adaptado a realidade escolar trabalhada.

Com base na realidade escolar da turma beneficiada da aplicação do projeto, percebeu-se que com esse método de ensino tem-se a possibilidade de desenvolver ou até mesmo aprimorar a competência de resolução de problemas, trabalhar as habilidades de gestão do tempo, autonomia na

busca pelo conhecimento, aprimorar o trabalho em equipe e a habilidade de falar em público, além de estimular a curiosidade em relação a aplicabilidade da Matemática no mundo real e a discussão de tópicos da história da humanidade.

Salientamos, que mesmo com todas as dificuldades impostas pelo sistema educacional, torna-se essencial desenvolver atividades diferenciadas, pelo menos, nos assuntos que causam mais dificuldades, pois dessa maneira, possibilitamos aos alunos o despertar pelo interesse e o gosto pela Matemática.

REFERÊNCIAS

ALMEIDA, P. J. **Criptografia e Segurança**. Departamento de Matemática; Universidade de Aveiro, 2012.

ALMOULOU, S. A.; SILVA, M. J. F. **Engenharia Didática: Evolução e Diversidade**. *Revista Revemat*, Florianópolis, v. 7, n. 2. 2012. Disponível em: <http://dx.doi.org/10.5007/1981-1322.2012v7n2p22> Acesso em: 15 ago. 2017.

ANTUNES, C. **Inteligências Múltiplas e seus Jogos**: introdução, 3. ed. Rio de Janeiro: Vozes, 2012. V.1.

ARTIGUE, M. Ingénierie Didactique. *Recherches en Didactique des Mathématiques*. Grenoble: La Pensée Sauvage, 1988. V. 9.3, p. 281- 308.

ARTIGUE, M. Engenharia Didática. In: BRUN, J. **Didática das Matemáticas**. Tradução de: Maria José Figueiredo. Lisboa: Instituto Piaget, 1996. Cap. 4. p. 193-217.

BERENGUER, M. I. S. **A Aplicação da Engenharia Didática no Ensino das Ciências Exatas**. 2010. 36 f. Monografia (Especialização) – Instituto a Vez do Mestre, Universidade Candido Mendes, Rio de Janeiro, 2010.

BEZERRA, D. de J; MALUGUTI, P. L; RODRIGUES, V. C. S. **Aprendendo Criptologia de forma divertida**. Paraíba, 2010. Disponível em: http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf Acesso em: 18 de mar. de 2017.

BRASIL. Ministério da Educação. Secretaria de Educação Média e Tecnológica. **Parâmetros Curriculares Nacionais: Ensino Médio**: Ciências da Natureza, Matemática e suas Tecnologias. Brasília: MEC, 2001.

_____. Análises e reflexões sobre o desempenho dos estudantes brasileiros/OCDE - **Organização para a Cooperação e Desenvolvimento Econômico**. São Paulo: Fundação Santillana, 2016. Disponível em http://download.inep.gov.br/acoes_internacionais/pisa/resultados/2015/pisa2015_completo_final_baixa.pdf Acesso em: 20 set. 2017.

_____. Ministério da Educação. Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira – INEP. **Resultados SAEB 2017**. Disponível em <https://medium.com/@inep/resultados-do-saeb-2017-f471ec72168d> Acesso em: 12 dez. 2018.

_____. Ministério da Educação e do Desporto. Secretaria do Ensino Fundamental. **Parâmetros Curriculares Nacionais: Matemática**. Brasília, 1999.

BITENCOURT, R. R. R. **Aplicações do conceito de proporcionalidade a partir da Engenharia Didática**. 2017. 76f. Dissertação (Mestrado profissional em Rede Nacional) – Universidade Federal do Amapá – UNIFAP, Macapá, 2017.

CANTORAL, R. et al. **Desarrollo del pensamiento matemático**. México, Trillas: ITESM, Universidade Virtua, 2000.

CARVALHO, L. R. **O uso de elementos da criptografia como estímulo matemático na sala de aula**. 2016. 78f. Dissertação (Mestrado profissional em Rede Nacional) – Universidade Estadual Paulista “Júlio de Mesquita Filho”, Rio Claro.

CARVALHO, P. C. P. **Métodos e contagem e probabilidade**. 11. ed. Rio de Janeiro: IMPA, 2015

CHÁ MATE. **O segredo das cartelas mágicas**. Disponível em: <http://chamate.blogspot.com.br/2010/09/o-segredo-das-cartelas-magicas.html> Acesso em: 20 fev 2017.

COUTINHO, S. C. **Criptografia**. 11. ed. Rio de Janeiro. IMPA, 2015

DANTE, L. R. **Matemática**, 1. ed. São Paulo: Editora Ática, 2008.

FUSEL, A. T. **O Ensino e a Aprendizagem da Análise Combinatória dentro do contexto de telefonia**. 2013. 135 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de São Carlos. São Carlos, 2013.

GERY, F. W. Does mathematics matter? In: WELCH, A. (ed.). **Research papers in economic education**. New York: Joint Council on Economic Education, 1972. p. 142-157.

GONÇALVES, R. R. S. **Uma abordagem alternativa para o ensino de Análise Combinatória no ensino médio**. 2014. 111f. Dissertação (Mestrado Profissional em Matemática) - Instituto Nacional de Matemática Pura e Aplicada Impa. Rio de Janeiro, 2014.

GROENWALD, C. L. O.; FRANKE, R. F. **Currículo de Matemática e o tema Criptografia no Ensino Médio**. Educação Matemática em Revista, Rio Grande do Sul, p. 51-57, 2008.

HARIKI, S. **Conectar problemas: uma nova estratégia de resolução de problemas combinatórios**. Revista Educação e Matemática, n. 37, 1996.

IEZZI, G.; HAZZAN, S. Fundamentos da Matemática Elementar 05: Combinatória e probabilidade. 3. ed. São Paulo Atual: Editora Ltda., 1977.

JACINTO, D. S. F. **Utilizando o material concreto para o ensino de Análise Combinatória**. 2015. 78 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituto de Ciências Exatas. Rio de Janeiro, 2015.

JESUS, A. L. N. **Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. 2013. 82f. Dissertação (Mestrado profissional em Matemática em Rede Nacional) – Universidade Federal do Vale do São Francisco, Juazeiro, 2013.

MACHADO, S. D. A. **Engenharia Didática**. In: MACHADO, S. D. A. (org.). **Educação Matemática: Uma introdução**. 2. ed. São Paulo: Educ., 2002. p. 197-208.

MALAGUTTI, P. L. **Atividades de Contagem a partir da Criptografia**. 1. ed. Rio de Janeiro: IMPA, 2015.

MELLO; H. P. D. M. **Desmistificando o ensino da Análise Combinatória**. 2017. 64f. Dissertação (Mestrado profissional em Matemática) – Instituto Nacional de Matemática Pura e Aplicada IMPA. Rio de Janeiro, 2017.

MORGADO, A.C.O. et al. **Análise Combinatória e Probabilidade**. 9. ed. Rio de Janeiro: Graftex, 1991.

PAIVA. M. **Matemática Paiva**. 3. ed. São Paulo: Editora Moderna, 2015.

PAIS, L. C. **Didática da Matemática** – Uma análise da influência francesa. 2.ed. Belo Horizonte: Autêntica, 2005.

PANNUTI, M.R.V. **Caminhos da prática pedagógica**. TVE Brasil. Rio de Janeiro, p. 01- 05, jun. 2004.

PASJO, K. **Chá de mate** (Matemática). Disponível em <http://cha-mate.blogspot.com.br/2010/09/o-segredo-das-cartelas-magicas.html> Acesso em: 22 dez. 2017

POMMER, W.M. **A Engenharia Didática em sala de aula**: Elementos básicos e uma ilustração envolvendo as Equações Diofantinas Lineares. São Paulo, 2013. Disponível em: <http://stoa.usp.br/wmpommer/files/3915/20692/Livro+Eng%C2%AA+Did%C3%A1tica+2013.pdf> Acesso em: 10 ago. 2017.

RODA, T. M. **Análise Combinatória: Uma abordagem diferenciada sem a utilização de fórmulas**. 2018. 65f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) – Universidade Federal de São Carlos. São Carlos, 2018.

ROA, R.; NAVARRO-PELAYO, V. **Razonamiento Combinatorio e Implicaciones para la Enseñanza de la Probabilidad**. In. Jornadas Europeas de Estadística, Ilhas Baleares, 2001.

SÃO PAULO. Secretaria da Educação (Estado). **Currículo do Estado de São Paulo: Matemática e suas tecnologias**. 1. ed. atual. São Paulo, 2011. Disponível em: <http://www.educacao.sp.gov.br/a2sitebox/arquivos/documentos/238.pdf> Acesso em: 21 ago. 2017.

_____. Governo do Estado de São Paulo. Secretária da Educação. **Caderno do Professor de Matemática**. Ensino Médio 2º Série, Volume 2. Nova Edição 2014 -2017. São Paulo, 2017. Disponível em: <https://cadernodoaluno.pro/respostas/2o-ano-ensino-medio/apostila-de-matematica-volume-2-2o-ano/> Acesso em: 02 jan. 2019.

SINGH, S. **O Livro dos Códigos**: A Ciências do Sigilo - do Antigo Egito à Criptografia Quântica. Rio de Janeiro: Record, 2003.

SOCIEDADE BRASILEIRA DE MATEMÁTICA. PROFMAT: Uma reflexão e alguns resultados. **Relatório**. Rio de Janeiro, 2017. Relatório digital.

Disponível em: http://www.profmat-sbm.org.br/wp-content/uploads/sites/23/2017/06/PROFMAT_relatorio_DIGITAL.pdf Acesso em: 15 ago. 2018.

ZOCHIO. M. F. **Introdução à Criptografia**. 1. ed. São Paulo: Novatec Editora Ltda, 2016.

ANEXO A

Figura A1: Régua de Criptografar

Fonte: Bezerra; Malagutti; Rodrigues (2010)

APÊNDICE (S)

APÊNDICE A

Pré-teste

Mestranda: Sávia Cristina Vidal

Orientador: Professor Dr. Estaner Claro Romão

Data: ____/____/____

Responda as seguintes questões e entregue a folha com os cálculos.
Desde já, agradeço sua colaboração.

- 1) Na Matemática, muitas vezes aparece o ponto de exclamação, porém com um significado diferente da gramática, como por exemplo: 5!
Qual o significado desse ponto na área de exatas?
- 2) De quantas maneiras diferentes se pode vestir uma pessoa que tenha 5 camisas e 3 calças?
- 3) Quantos números de três algarismos podemos escrever com os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9?
- 4) Quantos números de três algarismos podemos escrever com os algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9?
- 5) Quantos números de três algarismos DIFERENTES podemos escrever usando os algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9.
- 6) Anagrama é um substantivo que significa uma palavra ou frase que é construída por meio da alteração das letras de uma outra palavra ou frase, por exemplo: Com as letras da palavra AMOR podemos escrever a palavra ROMA.
Com base na informação acima, quantos anagramas (com ou sem sentido) conseguimos formar com as letras das palavras:
 - c) Porta
 - d) Matemática
- 7) (ENEM 2005) A escrita Braille para cegos é um sistema de símbolos no qual cada caractere é um conjunto de 6 pontos dispostos em forma retangular, dos quais pelo menos um se destaca em relação aos demais.

Por exemplo, a letra A é representada por:

O número total de caracteres que podem ser representados no sistema Braille é?

- 8) De quantas maneiras diferentes um técnico pode escalar seu time de basquete tendo a sua disposição 12 atletas que jogam em qualquer posição?
- 9) (OBMEP 2007) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda a letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

- (e) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.
- (f) Codifique *OBMEP* usando a chave 20.
- (g) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando

os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.

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

APÊNDICE B

Pós-teste

Mestranda: Sávia Cristina Vidal

Orientador: Professor Dr. Estaner Claro Romão

Nome: _____

Data: ____/____/____

Responda as seguintes questões e entregue a folha com os cálculos.
Desde já, agradeço sua colaboração.

- 1) Na Matemática, muitas vezes aparece o ponto de exclamação, porém com um significado diferente da gramática, como por exemplo: 6!
Qual o significado desse ponto na área de exatas? Qual nome que ele recebe? E qual o seu valor?
- 2) Quantos números pares de três algarismos podemos escrever com os dígitos 1, 2, 3, 4, 5, 6, 7, 8 e 9?
- 3) Quantos números de três algarismos **DISTINTOS** podemos escrever com os dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9?
- 4) Em uma corrida com 10 atletas competindo, pergunta-se: de quantos modos distintos podem ser conquistadas as medalhas de Ouro, Prata e Bronze?
- 5) Anagrama é um substantivo que significa uma palavra ou frase que é construída por meio da alteração das letras de uma outra palavra ou frase, por exemplo: Com as letras da palavra AMOR podemos escrever a palavra ROMA.
Com base na informação acima, quantos anagramas (com ou sem sentido) conseguimos formar com as letras das palavras:
 - a) Escola
 - b) Paralelepípedo
 - c) Bolsa, em que as letras O e L apareçam juntas e nessa ordem (OL)
- 6) Quantos números binários de 7 bits podemos escrever?

- 7) Quantas comissões de 3 integrantes podemos formar com 30 alunos de uma mesma classe?
- 8) (OBMEP 2007) Um antigo método para codificar palavras consiste em escolher um número de 1 a 26, chamado *chave* do código, e girar o disco interno do aparelho ilustrado na figura até que essa chave corresponda à letra A. Depois disso, as letras da palavra são substituídas pelos números correspondentes, separados por tracinhos. Por exemplo, na figura ao lado a chave é 5 e a palavra *PAI* é codificada como 20-5-13.

- a) Usando a chave indicada na figura, descubra qual palavra foi codificada como 23-25-7-25-22-13.
- b) Codifique *OBMEP* usando a chave 20.
- c) Chicó codificou uma palavra de 4 letras com a chave 20, mas esqueceu de colocar os tracinhos e escreveu 2620138. Ajude o Chicó colocando os tracinhos que ele esqueceu e depois escreva a palavra que ele codificou.
- d) Em uma outra chave, a soma dos números que representam as letras *A*, *B* e *C* é 52. Qual é essa chave?
- 9) No filme o “Código da Vinci” quantas eram as possibilidades de Robert Langdon descobrir o código do criptex? Sendo que esse objeto era formado por 5 anéis, nos quais cada um possui as 26 letras do alfabeto
- 10) Usando as quatro letras A, F, I, M podemos formar anagramas com quatro letras. Se esses anagramas são colocados em ordem alfabética, qual posição o anagrama M I A F

APÊNDICE C

Folha de exercícios referente ao filme “O Código da Vinci”

Códigos do filme: O Código da Vinci

Primeiro Código

Sequência de Fibonacci, com os 8 primeiros números, porém não estavam em ordem.

Frase codificada: Ó demônio draconiano, oh santa falsa.

Frase decodificada: Leonardo da Vinci, a Mona Lisa.

Esse código levou Sophie Neveu e Robert Langdon para o segundo código.

Segundo Código

Frase codificada: Tão sombria a traição dos homens.

Frase decodificada: Madona nas Pedras, da Vinci.

Esse código fez com que Sophie Neveu e Robert Langdon encontrassem a chave – flor de Liz.

Terceiro Código

Senha do banco – utilizaram a sequência de Fibonacci, que foi deixada no local do crime de Jacques Saunière, porém em

ordem, dessa forma tiveram acesso ao Criptex.

Quarto Código

Mensagem deixada na caixa do Criptex: Em Londres um cavaleiro que o Papa enterrou. O fruto de sua obra a ira santa causou. Busca o orbe da sua tumba ausente. De rósea pele e semeado ventre.

Esse enigma foi interpretado por Robert Langdon levando a descobrir a senha do Criptex e a localização do Santo Graal

Exercícios

- 1) Quantos possíveis anagramas existiam na frase cifrada do primeiro código? (sem levar em consideração os espaços entre as palavras)
- 2) Quantos anagramas existiam na frase cifrada do segundo código? (sem levar em consideração os espaços entre as palavras)
- 3) Quantas possíveis senhas Sophie Neveu e Robert Langdon tinham para descobrir a senha correta do banco em que estava o Criptex? Utilizando

os números deixados por Jacques Saunière

- 4) Quantas possibilidades existiam para a senha do Criptéx? Sendo que ele era formado por 5 anéis, e cada um era composto pelas 26 letras do alfabeto.

- 5) Quantas comissões de três integrantes podem ser formadas, tendo a disposição Robert Langdon, Jacques Saunière, Sophie Neveu, Silas, Fache e o Bispo Manuel, para compor o priorado de Sião?

APÊNDICE D

Folha de exercícios da 5ª ETAPA

Dever de casa

Obs: Todos os exercícios foram retirados da Avaliação de Aprendizagem em Processo (2017)

- 1) Em uma escola, 30 estudantes que participaram das Olimpíadas de Matemática foram premiados com medalhas ou menção honrosa conforme a tabela.

Premiação	Quantidade
Medalhas	9
Menção honrosa	21
Total	30

O diretor resolveu premia-los com uma viagem cultural. Para isso sorteará quatro estudantes, dois estudantes com medalhas e dois com menção honrosa.

As maneiras diferentes, em casa premiação, que os estudantes podem ser sorteados são?

- 2) Gabriel tem em seu guarda roupa dois tipos de calça: lisa e estampada; dois tipos de camisa: manga comprida e de manga curta; e dois pares de sapato: um marrom e um preto. Ao escolher uma calça, uma blusa e um par de sapatos, Gabriel pode fazer quantas combinações?
- 3) De quantas maneiras distintas podemos colorir a bandeira abaixo com as cores AZUL, BRANCA e VERMELHA, de modo que todas as cores apareçam com mesma área e cada retângulo menor seja pintado com uma mesma cor? Considere que os 9 retângulos menores são todos iguais.

- 4) Em uma pizzaria, o cliente pode pedir uma pizza básica com duas coberturas: queijo ou tomate. Pode ainda compor a sua pizza com os seguintes recheios: azeitonas, presunto, cogumelos e salame. Um cliente quer pedir uma pizza com dois recheios diferentes. Quantas combinações, o cliente poderá fazer?
- 5) Usando as cinco letras A, M, O, S e U, podemos formar anagramas com cinco letras.
Se esses anagramas são colocados em ordem alfabética, qual posição o anagrama USAMO ocupará?