Universidade Federal do Vale do São Francisco

Mestrado Profissional em Matemática em Rede Nacional – Profmat

SUMAIA ALMEIDA RAMOS

O JOGO CAÇA AO TESOURO COMO RECURSO DIDÁTICO PARA O ENSINO DA ARITMÉTICA MODULAR

Juazeiro – BA

2017

SUMAIA ALMEIDA RAMOS

O JOGO CAÇA AO TESOURO COMO RECURSO DIDÁTICO PARA O ENSINO DA ARITMÉTICA MODULAR

Dissertação apresentada ao Programa de Pós-graduação em Matemática da Universidade Federal do Vale do São Francisco – UNIVASF, Campus Juazeiro-BA, como requisito para obtenção do título de Mestre em Matemática.

Orientador: Prof. Severino Cirino de Lima Neto

Juazeiro – BA

2017

	Ramos, Sumaia Almeida.
R175j	O jogo caça ao tesouro como recurso didático para o ensino da aritmética modular / Sumaia Almeida Ramos. – Juazeiro/BA, 2017.
	XI, 123 f. : il. ; 29 cm.
	Trabalho de Conclusão de Curso (Mestrado Profissional em Matemática em Rede Nacional-PROFMAT) - Universidade Federal do Vale do São Francisco, Campus Juazeiro-BA, 2017.
	Orientador (a): Prof. Dr Severino Cirino de Lima Neto.
	1. Aritmética Modular. 2. Matemática – Estudos e ensino. 3. Determinantes. I. Título. II. Lima Neto, Severino Cirino. III. Universidade Federal do Vale do São Francisco.
	CDD 513

Ficha catalográfica elaborada pelo Sistema Integrado de Biblioteca SIBI/UNIVASF
Bibliotecário: Renato Marques Alves

Universidade Federal do Vale do São Francisco
Mestrado Profissional em Matemática em Rede Nacional
PROFMAT/UNIVASF

O JOGO CAÇA AO TESOURO COMO RECURSO DIDÁTICO PARA O ENSINO DA ARITMÉTICA MODULAR

Por:

SUMAIA ALMEIDA RAMOS

Dissertação aprovada em 29 de setembro de 2017.

Prof. Dr. Severino Cirino de Lima Neto
Orientador - PROFMAT/UNIVASF

Prof. Dr. Alexandre Ramalho Silva
Examinador Interno - PROFMAT/UNIVASF

Prof. Dr. Orlando Stanley Juriaans
Examinador Externo – IME/USP

Juazeiro
2017

Dedico esta pesquisa a minha família, meus amigos e meus alunos.

AGRADECIMENTOS

Ao Prof. Dr. Severino Cirino de Lima Neto, pela confiança, por todos os ensinamentos, pela oportunidade de trabalhar ao seu lado e por ser um grande incentivador na superação dos meus limites.

O meu agradecimento mais profundo dedico a minha grande amiga, Ma. Diana de Souza Carvalho, quem sempre me incentivou, me fazendo acreditar que chegaria ao final desta difícil, porém gratificante etapa.

Aos meus pais Simone Almeida Ramos e Divanildo Soares Ramos, a quem eu devo a minha eterna gratidão, por me ensinar a ser a mulher que sou hoje.

À Justino Ermeson Lima Araújo, pelo apoio e dedicação em contribuir na criação do programa de criptografia e mais novo parceiro de pesquisa.

À Jackson dos Santos Silva, pela colaboração inestimável.

À toda equipe do NUPEMAT.

Aos meus colegas de sala Romênia e Edson Binga.

À minha irmã Sulaine Almeida Ramos e Suiani Almeida Ramos, pelo companheirismo.

À minha prima Patrícia Gonçalves, pela amizade, carinho e disponibilidade.

Agradeço a todos que de forma direta ou indireta contribuíram e torceram pelo sucesso deste trabalho.

“Graças ao seu gênio, os números deixaram de ser apenas coisas usadas meramente para contar e calcular e passaram a ser apreciados por suas próprias características.” (SINGH, p. 28, 2010)

RESUMO

Dados publicados pelo Inep e SAEPE revelam que estudantes dos anos finais do ensino fundamental apresentam um baixo rendimento na disciplina de exatas, sobretudo quando comparados aos dados dos anos iniciais desta etapa; as operações aritméticas, fundamentais ao ensino da matemática, figuram entre aos conteúdos que aumentam tais dificuldades. Nesta perspectiva, considerando que criptografia trabalha as habilidades contempladas nos Parâmetros Curriculares Nacionais para os Anos Finais da Educação Básica, essenciais à compreensão dos conceitos mais complexos da matemática, este trabalho teve como objetivo analisar a viabilidade do ensino de congruência modular e determinantes aplicadas à criptografia com uso de jogos. Para tanto, foi realizado estudos com estudantes dos anos finais do ensino fundamental, inseridos na rede pública do município de Petrolina/PE, usando-se o jogo “Caça ao Tesouro”, tendo com suporte em pergaminhos criptografados. Para validar esta proposta, foram aplicados questionários que permitiram inferir a viabilidade do uso do jogo como um recurso didático no desenvolvimento de habilidades desse público. Os conteúdos básicos de matemática podem ser ensinados por meio de recursos pedagógicos que reproduzam situações problemas do dia-a-dia, capazes de auxiliar na otimização da aprendizagem significativa, refletindo em um melhor desempenho nos resultados de provas internas e externas que avaliam a qualidade da educação.

Palavras-chave: Criptografia. Aritmética Modular. Determinantes.

ABSTRACT

Data published by Inep and SAEPE show that students in the final years of elementary school have a low performance in the exact of discipline, especially when compared to the data of the initial years of this stage; The arithmetical operations, fundamental to the teaching of mathematics, are among the contents that increase such difficulties. In this perspective, considering that cryptography works the abilities contemplated in the National Curricular Parameters for the Final Years of Basic Education, essential to the comprehension of the more complex concepts of mathematics, this work had as objective to analyze the viability of the teaching of modular congruence and determinants applied to cryptography With use of games. For this, studies were carried out with students from the final years of elementary school, enrolled in the public network of the municipality of Petrolina / PE, using the game "Treasure Hunt", with support in encrypted scrolls. In order to validate this proposal, questionnaires were applied that allowed to infer the viability of the use of the game as a didactic resource in the development of abilities of this public. The basic contents of mathematics can be taught by means of pedagogical resources that reproduce situations of everyday problems, which can help in the optimization of meaningful learning, reflecting in a better performance in the results of internal and external tests that evaluate the quality of the education.

Key-words: Cryptography. Modular Arithmetic. Determinants.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

De acordo com as pesquisas realizadas pelo Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP) os índices de desenvolvimento educacional dos estudantes brasileiros apresenta dados sempre menores à medida que avança etapas na educação básica. Isso gera preocupações, uma vez que, os dados permitem inferir que os estudantes da educação infantil, apresentarão índice de desenvolvimento educacional menor, quando for ingressar no ensino fundamental.

Com isso discussões são geradas, afim de, diagnosticar e compreender os possíveis motivos dessa queda. A terceira versão da Base Nacional Comum Curricular (BNCC) julga essa queda como uma falha de conexão entre os currículos das etapas da educação básica, sendo este documento uma proposta curricular na qual, permite uma conversa entre as três etapas, educação infantil, ensino fundamental e ensino médio.

Com isso, diante dos diversos problemas da educação básica os estados brasileiros buscam formas de diagnosticar o rendimento escolar. A título de exemplo, o estado de Pernambuco criou o Sistema de Avaliação Educacional de Pernambuco (SAEPE), na qual por meio de avaliações anuais, descreve quais os descritores que seus estudantes já dominam e os que precisam melhorar por meio de atividades de intervenção.

Segundo SAEPE, mais de 50% dos estudantes de matemática dos anos finais do ensino fundamental, não possuem as habilidades esperadas pelo estado de Pernambuco na disciplina de matemática. È possível inferir, que este percentual possa está influenciado pela falta de comunicação entre os currículos da educação básica.

Porém, apenas isso não pode ser utilizado como justificativa para os baixos rendimentos em matemática. Existem outros fatores, como por exemplo, a abordagem em sala de aula e o contexto sócio cultural da escola e do aluno. Diante disso, pesquisas são realizadas, a fim de contribuir para inovação das práticas pedagógicas com o uso de recursos como jogos e tecnologia.

O uso de novos recursos no ensino da matemática aparece com a ideia de atrair a atenção do estudante para uma atividade prazerosa e divertida, provocando a

curiosidade pelo conhecimento. No entanto, esse tipo de atividade exige do professor uma maior atenção e tempo durante o planejamento.

Pensando nisso, essa pesquisa tem como objetivo principal analisar a viabilidade do uso do jogo Caça ao Tesouro como uma ferramenta de auxilio na socialização de conhecimentos aritméticos aplicados à criptografia.

A ideia é que durante a busca de um tesouro os estudantes possam aplicar e/ou revisar conceitos abordados durante a aula. Assim, o objetivo do jogo é encontrar o tesouro perdido, e para isso, deverão decifrar as mensagens secretas presentes em pergaminhos estrategicamente escondidos na escola, pelo professor.

Para auxiliar durante a atividade, foi criado um programa de criptografias primitivas. Por meio deste programa, os estudantes podem de forma rápida cifrar e decifrar os pergaminhos, contribuindo no controle do tempo da aula e do jogo, bem como ampliar as possibilidades de trabalhar com outros conteúdos da matemática.

A proposta foi aplicada em minicurso na Universidade Federal do Vale do São Francisco (Univasf), para um público de 45 estudantes do 6º ao 9º ano das escolas públicas do município de Petrolina/PE. A fim de compreender a realidade desses estudantes, foi investigado cerca de 20 professores, que trabalham nas mesmas escolas que frequentava os estudantes do curso. O objetivo foi confrontar os dados coletados pelos estudantes e os dos docentes de forma a auxiliar na compreensão da realidade desses sujeitos.

Espera-se que esta proposta possa auxiliar os docentes no planejamento de novas propostas para o ensino da matemática em sala de aula, capaz de promover uma aprendizagem significativa. Preocupados com a melhor forma de apresentar à estrutura deste trabalho, atraindo à atenção dos professores a obra está dividida em cinco capítulos.

No primeiro capítulo foi realizada uma breve introdução da criptologia como ciência que estuda a criptografa, esteganografia e criptoanálise. O objetivo é apresentar por meio da história, os principais eventos históricos que culminou o avanço dessa ciência e a sua importância nos dias atuais.

O segundo capítulo é um referencial teórico com a abordagem da matemática presente nas criptografias abordadas na proposta do curso, facilitando a compreensão dos cálculos aplicados nas cifras presentes nos pergaminhos. Assim, a escrita neste capítulo foi pensada em facilitar o estudo do professor ou estudante de graduação, demonstrando e justificando o uso das operações.

Após este estudo, o terceiro capítulo apresenta toda a metodologia aplicada durante a pesquisa, justificando os processos utilizados durante a coleta, organização e apresentação dos dados coletados.

Os resultados da pesquisa são discutidos no quarto capítulo, que inicia com a discussão sobre o perfil dos estudantes e os seus desempenhos durante a abordagem dos conteúdos de aritmética, refletindo sobre os desafios encontrados durante a prática. Em seguida, apresenta as criptografias utilizadas durante o curso e o por fim, as regras do Jogo Caça ao Tesouro e os dados de sua aplicação.

O capítulo 5 compõe as considerações finais obtidas com a experiência vivida durante a pesquisa, refletindo sobre as discussões de teóricos e os dados coletados na prática.

Acredita-se que após a leitura deste trabalho, o professor se sentirá atraído em utilizar esta proposta em suas aulas de matemática. E como continuidade desta pesquisa, pretende-se produzir uma cartilha com orientações pedagógicas para o uso do Jogo Caça ao tesouro, com a capacidade de ser adaptado a outras disciplinas e o programa será adaptado para linguagem que permita ser utilizado em celulares e tablets.

CAPÍTULO 1
1 BREVE INTRODUÇÃO À CRIPTOLOGIA

O avanço das tecnologias digitais tornou possível a comunicação virtual nos dias atuais. Parte desta comunicação é realizada por redes sociais compostas por pessoas ou organizações conectadas com objetivos e valores comuns. Esses tipos de conversas possuem conteúdos que só podem ser visualizados por um grupo limitado de pessoas, exigindo o sigilo dos dados compartilhados durante a comunicação. Nesse contexto, a segurança dos dados é importante para que pessoas possam manter conversas em tempo e espaços diferentes de forma segura, tendo como suporte a Criptologia, que surgiu a partir da preocupação em proteger conteúdos.

Houve um tempo em que as técnicas de envio de mensagens secretas eram consideradas uma arte, entretanto com o desenvolvimento do conhecimento percebeu-se que os avanços de seus estudos poderiam levar a descobertas inusitadas e de grande importância para o meio cientifico. De acordo com Malagutti (2015), Cruz (2009) e Singh (2002), a criptologia é a ciência que estuda os métodos de enviar uma mensagem secreta, e pode ser dividida em três ramos: esteganografia, criptografia e criptoanálise, como organizado abaixo:

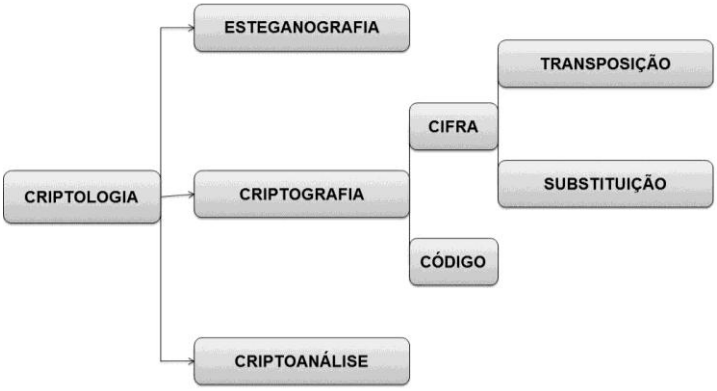


Figura 01: Ilustração das divisões da criptologia
Fonte: Adaptado de SINGH, 2002.

Dentro dos ramos da Criptologia, a esteganografia se caracteriza pelo ato de esconder uma mensagem sem, contudo, modificar o conteúdo (CRUZ, 2009; SINGH, 2002). Os primeiros registros de uso dessa técnica datam do século V a. C., usada por Heródoto, nos quais relatam a tentativa fracassada dos persas em conquistar a Grécia. Neste relato, a mensagem secreta foi enviada escrita em um

par dobrável de placas de madeira, que em seguida, eram cobertas com cera. Para ler a mensagem bastava raspar a cera da placa (CRUZ, 2009).

O uso da esteganografia é descrito por alguns autores, em situações diversas, como a utilização do leite da planta como tinta invisível, em que a mensagem ficava aparente quando esse papel era exposto ao sol. O relato do cientista italiano Giovanni Porta no século XVI na qual, descreve como esconder uma mensagem dentro de um ovo cozido. E a prática dos chineses, em raspar a cabeça do mensageiro para escrever a mensagem, que era enviada após o crescimento dos pelos. O receptor visualizava a mensagem raspando a cabeça do mensageiro (SINGH, 2002).

Observe que a prática dos Chineses exige um grande tempo para envio da mensagem, o que não é interessante quando se tem urgência que chegue ao destinatário.

Nos dias atuais a esteganografia é perceptível em situações como o método utilizado para transportar drogas ilícitas, onde algumas pessoas transportam dentro do estomago ou outras partes do corpo tentando despistar as fiscalizações (CRUZ, 2009).

A figura 2 apresenta outro exemplo de esteganografia nos dias atuais. Esta se faz presente nas cédulas da moeda brasileira. O tipo de esteganografia presente são as de micropontos, onde a mensagem é reduzida a pontos bem pequenos sendo possível sua visualização por meio de lupas, além disso, usa-se também a marca-d'água que pode ser visualizada quando exposta a um foco de luz.

Figura 02: Exemplo de esteganografia nas cédulas de cem reais.
Fonte: Site do Banco Central[1]

Provos e Honeyman (2003) explicam como realizar esteganografia com a manipulação de *pixels* das imagens, sem alterar o conteúdo, isto é, apenas esconder informações. Este método se baseia em trocar

pixel menos significantes pela informação que se deseja transmitir. A eficiência é descrita pela capacidade de inserir informações sem tantas alterações nas imagens.

No entanto, esta esteganografia moderna utiliza de uma teoria semelhante à criptografia. A mensagem é descoberta caso tenha a imagem original e a imagem modificada, assim comparando consegue identificar as diferenças, ou seja, o segredo escondido na imagem modificada, neste caso o seguro é manter a imagem original em segredo, pois ela será a chave para esta esteganografia. Para quem deseja se aprofundar no assunto consulte a obra de Provos e Honeyman (2003).

1.1 CRIPTOGRAFIA

Segundo Singh (2002) a evolução da criptografia ocorreu paralela a esteganografia, por considerarem que não era mais seguro apenas esconder a mensagem, já que escondida, quem interceptasse não enfrentaria dificuldades em ler, em contrapartida, a mensagem criptografada se torna um obstáculo para pessoas não autorizadas a ler o conteúdo.

A palavra criptografia é derivada das palavras gregas *kriptos* (secreto) e *grafo* (escrita). Este ramo da criptologia é responsável por estudar os métodos de codificar (substituir palavras por outras) e cifrar (alterar as letras e/ou sua posição) mensagens secretas (FALEIRO, 2011).

Observe que a criptografia pode ser realizada em códigos ou em cifras, ao cifrar o método pode ser classificado em cifra por transposição ou cifra por substituição. A cifra por transposição não altera a identidade das letras da mensagem original, apenas muda suas posições, seguindo um rigor matemático, diz-se que as letras são permutadas.

Desta forma, uma mensagem que contém 20 letras pode gerar $20!$ cifras diferentes, algo passando das casas dos bilhões. No entanto, quando se faz esta contagem está incluindo todos os métodos possíveis de permutar, ou seja, de criptografar.

Por exemplo, seja a mensagem original *CORRA PARA O NORTE*, existem $15!$ formas de permutar as letras, ou seja, $15!$ métodos distintos de cifrar, caso deseje, cifrar com o método de escrever as letras da palavra da direita para a esquerda, obtém-se, *ETORN O ARAP ARROC*, neste caso, esta cifra é apenas uma das $15!$ cifras possíveis e com método específico para cifrar.

No entanto, na criptografia este método não ocorre de modo aleatório, seus critérios são pré-estabelecidos, com o cuidado para que seja a mais segura possível. Além disso, a retirada dos acentos ortográficos é uma estratégia para tornar a mensagem mais secreta e não deixar pistas para que descubra a chave utilizada.

Na cifra de substituição a identidade das letras é alterada, visto que, as letras da mensagem original são substituídas por outras pertencentes ao alfabeto cifrado. O alfabeto cifrado é obtido por meio do deslocamento das letras do alfabeto original, esse deslocamento é definido de acordo com a chave utilizada para cifrar. Existem cifras que utilizam um alfabeto cifrado, sendo chamadas de monoalfabéticas e quando utilizam mais de um alfabeto cifrado, são chamadas de polialfabéticas (FALEIRO, 2011).

Uma das cifras monoalfabeticas mais antiga é a Cifra de Júlio César, que se caracteriza por seu alfabeto cifrado ser formado pelo deslocamento do alfabeto original em três casas (tabela 1). Esta cifra recebe este nome justamente por ter sido o Imperador Júlio César quem a utilizou durante suas batalhas (FALEIRO, 2011).

Tabela 1: Correspondência de letras entre o alfabeto original e o alfabeto cifrado

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
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

Fonte: Próprio autor

A cifra consistiu em substituir cada letra da mensagem original pela letra do alfabeto cifrado em correspondência com o alfabeto original (tabela 1). Por exemplo, ao utilizar a cifra de César para cifrar o velho ditado chinês “*QUANDO VOCÊ VIR UM HOMEM COM FOME, NÃO LHE DÊ UM PEIXE...ENSINE O A PESCAR!”***.**

A letra Q deverá ser substituída pela letra T e a letra U pela letra X, seguindo esta estratégia a cifra obtida será: *TXDQGR YRFH YLU XP KRPHP FRP IRPH, QDR OKH GH XP SHLAH HQVLQH R D SHVFDU.*

Para decifrar, basta criptografar a mensagem cifrada substituindo as letras da mensagem pelas letras do alfabeto original em correspondência com o alfabeto cifrado, ou seja, realizar o processo inverso. Logo, a letra T deverá ser substituída pela letra Q e a letra X pela letra U, e assim sucessivamente.

Neste caso, o algoritmo de Júlio César expressa-se em substituir uma letra por outra, mas para isso depende de uma chave, na qual será responsável por informar quantas casas o alfabeto foi transladado, por exemplo, a utilizada por Júlio César é a chave três, uma vez que, o alfabeto transladou três casas.

Segundo Singh (2002) em 1883 o linguista holandês Auguste Kerckhoff von Nieuwenhof, em seu livro *La Cryptographie Militaire* publicou um princípio que recebe o seu nome “Princípio de *Kerckhoff*”, na qual a segurança não está em manter o método de criptografar em segredo, mas manter a chave em segredo. No entanto, além de manter a chave em segredo um sistema é considerado seguro, se houver uma grande quantidade de chaves.

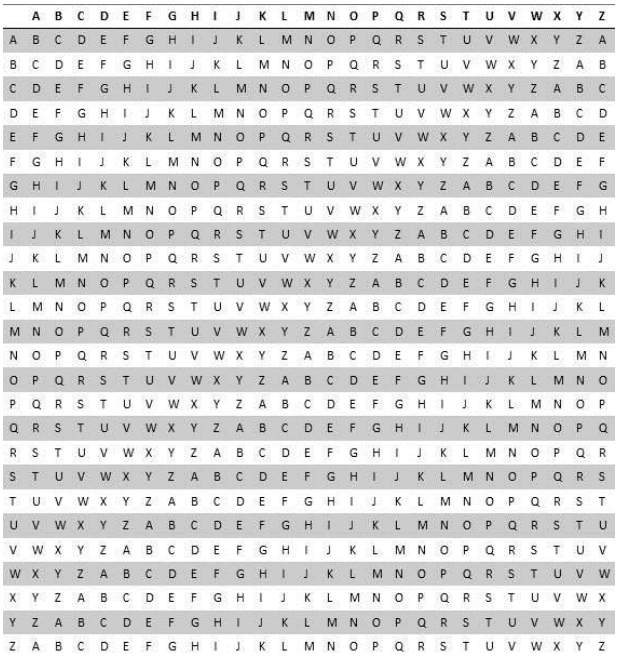
Isso justifica o fato da criptografia de César ser considera frágil, pois só existem 25 chaves possíveis. Neste caso alguém pode interceptar a mensagem e perceber que o método utilizado foi por substituição. Está pessoa não possui a chave, isto é, não sabe qual o alfabeto cifrado foi utilizado. No entanto, devido à fraqueza do método bastam testar as 25 chaves possíveis, até decifrar o conteúdo.

Este fato caracteriza o papel da criptoanálise que é a responsável por estudar os métodos de quebrar códigos, ou seja, descobrir qual a chave utilizada para cifrar determinada mensagem.

De acordo com Danziger e Henriques (2012) os cifradores são vulneráveis pelo menos a um tipo de ataque. Quando se tenta todas as chaves possíveis é chamado de ataque ao algoritmo por exaustão (força bruta), no entanto nem sempre é possível quando existe uma quantidade muito grande de chaves, o que poderia levar anos para testar todas.

Uma forma muito utilizada para quebrar os códigos de cifras monoalfabéticas era a análise de frequência com que as letras surgiam no texto. Para isso, os criptoanalistas baseavam-se nas frequências de ocorrência das letras em determinada língua. Neste caso, faz uma comparação da ocorrência de letras no texto cifrado, com o gráfico de frequência de ocorrência das letras nos textos originais (FALEIRO, 2011; SINGH, 2010).

Devido à fraqueza das cifras monoalfabéticas, buscou se por cifras mais seguras, com isso ainda no século XVI o criptografo francês Blaise de Vigenère divulgou um método polialfabético de criptografar. O seu método baseava se em aplicar a cifra de César em cada letra de acordo com a chave (FALEIRO, 2011; SINGH, 2002; CRUZ, 2009). Normalmente a chave era uma palavra, por exemplo, *NUPEMAT* e utilizava-se a tabela da figura 03. Note que, cada linha é uma Cifra de César, por exemplo, a linha quatro é a Cifra de César de chave três.



	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Figura 03: Exemplo do quadro utilizado na cifra de Vigenère
Fonte: Próprio Autor

Observe como cifrar a frase *“O ATAQUE SERÁ NA NOITE DE AMANHÃ*”. Escreve-se sobre a mensagem original, a palavra que representa a chave, até cobrir todas as letras, repetindo a palavra o quanto for necessário (tabela 2).

Tabela 2: primeiro passo para cifrar a mensagem

CHAVE	**N**	**U**	**P**	**E**	**M**	**A**	**T**	**N**	**U**	**P**	**E**	**M**	**A**	**...**
MENSAGEM ORIGINAL	O	A	T	A	Q	U	E	S	E	R	A	N	A	...

Fonte: Próprio autor

Agora, basta acompanhar a figura 03, onde cada letra da cifra é obtida pela interseção da linha iniciada pela letra da palavra chave com a coluna iniciada pela letra do texto. Neste caso, a primeira letra da mensagem cifrada será a interseção entre a linha que inicia pela letra O e a coluna que inicia pela letra N. A segunda letra será a interseção da linha que começa pela letra A com a coluna que começa com a letra U. A terceira letra será a interseção da linha que começa pela letra T com a coluna que começa com a letra P.

Ao repetir este processo até a ultima letra da mensagem, obtendo a cifra *CVJFDVYGZHFABHCEJJQFUAVDUB.* Note que neste método a letra A foi cifrada pelas letras V, F, B e U, enquanto que a letra E foi cifrada pelas letras Y, Z, J e F, isso faz com que a cifra de Vigenère se torne mais segura.

Além disso, seguindo o princípio de Kerckhoff, a cifra de Veginère pode ser considerada segura pela sua quantidade de chaves, uma vez que, a quantidade de chaves de quatro caracteres é 26^4 chaves, o equivalente a 456 976 chaves

possíveis. Para o caso de uma chave de *n* caracteres seriam 26^n chaves possíveis. O que exige anos para tentar descobrir a chave por força bruta.

Desta forma, durante três séculos a cifra de Vigenère foi considerada inquebrável, sendo no século XIX quebrada pelo criptoanalista britânico Charles Babbage. Neste mesmo século já era registrado o uso do telegrafo elétrico e do código *Morse*, onde a prática da criptografia não era apenas em papel, e o tempo de envio era menor (SINGH, 2002).

De acordo com Strathern (2000) em 1823 Babbage começa a trabalhar em uma máquina de calcular concluindo sua invenção sete anos depois. Este é um fato marcante no percurso do avanço dos conhecimentos que ajudaram Alan Turing a começar a questionar a possibilidade da criação de uma máquina inteligente. Seguindo esta linha, em 1854 Boole publica um artigo sobre lógica binária, para então em 1937 Alan Turing publicar o artigo *On computable numbers* com argumentos que dão origem a um computador futuro.

Por conseguinte, na Segunda Guerra Mundial a criptografia foi marcada pelo uso de máquinas eletromecânicas para criptografar mensagens. Como a Máquina Enigma criada pelo alemão Arthur Schebius, utilizada pela Alemanha durante vários anos. A Enigma era considerada muito segura, de tal forma, que durante treze anos os criptoanalistas a consideraram indecifrável, até que o matemático Alan Turing e sua equipe consegue quebrar o código desta máquina (SINGH, 2002; ELLIS, 2005).

Ellis (2005), Strathern (2000) e Singh (2010) descreve que foi em 1938 que a história do computador começa no Bletchey Park, quando um jovem engenheiro polonês Robert Lewinski afirmou para a embaixada britânica ter trabalhado em uma fábrica na Alemanha onde estava sendo construídas máquinas de criptografar, imediatamente o levaram para Paris onde supervisionou a construção de uma máquina de nome Enigma.

O sistema da Enigma era composto por duas máquinas, a emissora e a receptora. Na máquina emissora fixava se uma chave e a mensagem original era inserida por meio da datilografia, que em seguida era embaralhada pelo movimento dos rotores, até imprimir a cifra. A máquina receptora ficava configurada com a mesma chave, ao inserir a cifra a máquina embaralhava a mensagem, imprimindo a mensagem decifrada. O que a tonava tão segura, era a sua possibilidade de chaves superior a casa dos bilhões e a chave era trocada a cada três horas Strathern (2000).

Ellis (2005) e Strathern (2000) descreve que 1939 o governo britânico tinha como base secreta instalada no *Bletchley Park* , na qual o matemático Alan Turing fazia parte. Alan Turing defendia que única forma de quebrar a Enigma era criando uma máquina capaz de pensar mais rápido que o homem, uma vez que, a segurança do Enigma baseava-se nas escolhas de chaves diferentes a cada dia.

O ataque por exaustão seria falho, uma vez que era impossível testar todas as chaves até o fim do dia, já que a cada três horas as chaves eram modificadas. Este era o momento de colocar em prática a máquina descrita teoricamente por Turing no seu artigo *On computable numbers,* e assim ele fez ao construir a Colossos.

A máquina colossos era utilizada para descobrir a chave da mensagem interceptada, o que foi realizado com sucesso. Este foi uma dos fatos mais marcantes para a tecnologia na segunda guerra mundial, onde Alan Turing quebra o código de uma das máquinas mais seguras da época, mudando completamente o percurso da guerra, favorecendo que os Britânicos conhecessem os planos alemães. Colossos é um embrião do que atualmente conhecemos como computador e a partir daí, começa uma nova era para a criptografia, chamada criptografia computacional (SINGH, 2002).

Após a segunda guerra mundial, as pesquisas em busca da criação de uma máquina inteligente não cessaram, e os avanços foram mais significativos, construindo máquinas de alta tecnologia. Singh (SINGH, 2002) deixa bem claro, que as informações descritas em sua obra, foram mantidas em sigilo por um bom tempo. Desta forma, com a afirmação do autor permite inferir que atualmente o avanço da tecnologia, pode ser superior ao que a sociedade conhece.

A atual criptografia é muito avançada para ser praticada com lápis e papel, além disso, por ser responsável pelo avanço tecnológico, faz com que a briga entre criptógrafos e criptoanalistas tenha como cenário o mundo virtual. Um exemplo é a criptografia de chave pública, muito comum nas comunicações eletrônicas como o uso de cartões de crédito. Este método possui duas chaves, uma pública e outra privada, por este motivo é denominado criptografia de chaves assimétricas, os casos anteriores são criptografias de chaves simétricas por possuírem apenas uma chave.

Um sistema criptográfico com esta característica é o RSA, criado em 1978 por Ronald L. Revest, Adi Shamir e Leonard M. Adelman, na qual possui duas chaves uma pública e outra privada. E sua segurança estar no fato da escolha da chave ser

um produto entre números primos com uma grande quantidade de algarismos o que torna impossível a sua fatoração, pois nos dias atuais ainda não se tem tecnologia para tal fim. Com isso, muitos matemáticos direcionam suas pesquisas para a decomposição de primos muito grandes, afim de, obter um método de quebrar os códigos da criptografia RSA (SINGH, 2002).

Desta forma, a matemática na atual sociedade tecnológica exerce funções muito mais importantes do que apenas efetuar operações. Por este motivo, exige que os órgãos responsáveis pela educação no Brasil, realizem discussões com o objetivo de propor uma educação capaz de atender as necessidades desta nova era. Assim como a criptologia, outras ciências acompanham seu desenvolvimento marcado pelo avanço da matemática. Então, por que não levar isso para a sala de aula?

Contextualização, interdisciplinar, transdisciplinar, são palavras comuns nas novas discussões, com isso exige novas propostas de ensino que leve para a sala de aula, a oportunidade do aluno de organizar o conhecimento, estruturar dados e informações, tomar decisões, ou seja, desenvolver o seu pensamento critico. A informação no mundo da internet é de fácil acesso para qualquer estudante, o que ele precisa é de orientações para que possa dessas informações adquirir conhecimento.

O capítulo a seguir, apresenta uma breve análise da matemática presente em algumas técnicas de criptografia, tais conteúdos estão presentes nos currículos da educação básica, o que permite analisar a possibilidade do ensino/aprendizagem desses conceitos aplicados à criptografia, como uma proposta significativa.

CAPÍTULO 2.

2. FUNDAMENTAÇÃO TEÓRICA

A matemática produzida na Babilônia e Egito não apresenta um rigor matemático na forma de apresentar este conhecimento. Toda matemática produzida era registrada em papiros como meras receitas, no entanto, a matemática produzida por estes povos foi de grande importância para esta ciência. De acordo com, Eves (2004) e Roque (2012) o escriba egípcio Ahmes, registrou no Papiro de Rhind[1], mais de 80 problemas de matemática.

Para uma noção desses problemas, a seguir tem-se um dos métodos de divisão que segundo Eves (2004) é encontrado no papiro de Rhind. Trata-se de uma divisão entre dois números naturais, de modo geral, pode ser interpretada como a seguir.

Sejam $a,b \in \mathbb{N}$, dividir *a* por *b* é encontrar $q,r \in \mathbb{N}$, tal que o algoritmo pode ser aplicado dobrando os valores de *b* até encontrar um valor maior ou igual a *a* (Veja a tabela a seguir).

Tabela 2. Ilustração das somas das parcelas: um processo generalizado. Processo realizado pelos egípcios.

Parcelas (*P*)	**Soma das Parcelas (S_P)**
1	*B*
2	*2b*
4	*4b*
8	*8b*
...	...
2^n	*$2^n b$*

Fonte: Próprio autor.

O algoritmo deve parar quando $2^i b \geq a, \mathrm{i} = 0,1,2,3...,\mathrm{n}$, isto é, $S_P \geq a,\ p = 1,2,4,8,...,2^n$. Em seguida, define-se as combinações de S_p, para o qual, o somatório seja igual a *a,* ou seja, $a = S_1 + S_2 + S_4 + \cdots + S_P$, tal que, $\sum_{i=0}^{n} S_{p=2^i} \leq a$. O

quociente (q) será a soma de *P*, que compõe os índices das parcelas combinadas no somatório e o resto (r) será definido de acordo com os dois casos a seguir.

i. $\sum_{i=0}^{n} S_{p=2^i} = a \Leftrightarrow r = 0.$

ii. $\sum_{i=0}^{n} S_{p=2^i} < a \Leftrightarrow r = a - \sum_{i=0}^{n} S_{p=2^i}.$

Por exemplo, seja o dividendo igual a 243 e o divisor igual a três, para encontrar o quociente e o resto, basta dobrar os valores do divisor sem exceder o dividendo.

Tabela 4. Aplicação do processo da tabela 2, na divisão de 243 por 3.

Parcelas (*P*)	**Soma das Parcelas (S_P)**
***1**	***3***
2	*6*
4	*12*
8	*24*
***16**	**48**
32	*96*
***64**	***192***

Fonte: Próprio autor.

Ora, como

243 = 192 +51
= 192 + 48 + 3

Observe que as parcelas de 243 correspondem aos números com os asteriscos na tabela 4, logo o quociente é 64+16+1 = 81 e o resto é 0.

Veja que neste processo, não exigia tanto conhecimento da tabuada de multiplicar, bastava conhecer o processo de adição. Dobrando se os valores era uma forma de contar quantas parcelas de 3 são necessárias para chegar em 243. No caso 64 parcelas de 3 possuem como soma 192, por este motivo colocar-se o (*) em mais parcelas, até a tingir 243. No entanto, após escolher 81 parcelas a soma é 243, e resto 0, que não permite combinar mais parcelas, visto que, ultrapassa o valor desejado. Portanto, o quociente é 81 e o resto é 0.

Por um bom tempo, a teoria dos números se manteve estagnada, que em decorrência da curiosidade de alguns matemáticos, essa área torna a avançar. Entre eles estão o matemático e físico Suíço Leonard Paul Euler[4] que demonstrou que os números primos podem ser escritos na forma $4n+1$ e $4n-1$ e o matemático francês Pierre de Fermat[5] que baseado nas obras de Diofanto conheceu os ternos pitagóricos e desafiou os matemáticos a demonstrarem que equações do tipo $a^n + b^n = c^n, \forall n > 2$, não possuem soluções inteiras (EVES, 2004; SINGH, 2010).

A base de todo esse conhecimento da teoria dos números è a operação de divisão conhecida como Euclidiana, que recebe este nome devido a Euclides[11] ter usado na demonstração para encontrar o Máximo Divisor Comum (mdc), no seu livro "Os elementos", o livros-texto mais conhecido no mundo, composta por uma matemática organizada, com postulados e axiomas, seguidos de teoremas demonstrados por meio de raciocínio lógico dedutivo (DOMINGUES, IEZZI, 2003).

Na educação básica muitos professores trabalham a divisão como um algoritmo para dividir inteiros em partes iguais, o que não é errado, no entanto não é suficiente, uma vez que, a divisão possui muito mais utilidades do que apenas dividir inteiros em partes iguais, com a utilização na discriminação de números por meio de propriedades fundamentadas na existência do resto, como a existência de números primos que compõe o teorema fundamental da aritmética, isto é, por meio da divisão euclidiana é possível conhecer a integridade dos números.

Em sala de aula o problema nesse algoritmo, surgi quando a divisão não é exata, a existência do resto é capaz de gerar desconforto para os estudantes, uma vez que, a partir deste momento, o estudante deve tomar uma decisão: continuar a divisão encontrando um quociente que pode não pertencer ao conjunto dos números inteiros, ou parar a divisão e registar o quociente inteiro e o resto natural.

As discussões neste trabalho estão pautadas na segunda situação, registar o quociente inteiro e o resto natural, para então, analisar as propriedades das teorias dos números fundamentadas pela existência de um resto, isto é, para conhecer a integridade dos números que tanto fascinaram grandes matemáticos e ainda atraem grandes pesquisadores principalmente na aplicação em busca de avanços na tecnologia.

2.1 NÚMEROS INTEIROS ($\mathbb{Z}$).

A discussão a seguir tem como embasamento as obras Coutinho (2014), Hefez (2014), Dutenhefner e Cadar (2016), Shokranian (2012), Domingues e Iezzi (2003) e Gonçalves (2011) para além do que for apresentado como sugestão veja as referências citadas.

Como ponto de partida desta obra, será admitir que o leitor esteja familiarizado com o conjunto dos números inteiros $\mathbb{Z}=\{\cdots -2,-1,0,1,2,\cdots\}$. Desta forma, a abordagem será essencialmente axiomática, ou seja, serão desprezadas as demonstrações das propriedades dos inteiros. Isso não implica afirmar que estas demonstrações não são importantes, apenas fica como sugestão de pesquisa para o leitor, de forma a não tornar longa a discussão do capítulo, enfatizando demonstrações de teoremas que estejam mais direcionados ao objetivo deste trabalho.

No conjunto $\mathbb{Z}$ estão bem definidas as operações de adição e multiplicação, tal que $f:\mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$, com $(x,y)=x+y$ e $(x,y)=x\cdot y$, as quais gozam das seguintes propriedades, $\forall w,x,y,z\in\mathbb{Z}$.

i. $w=x$ e $y=z \Rightarrow w+y=x+z$ e $w\cdot y=x\cdot z$.

ii. $x+y=y+x$ e $x\cdot y=y\cdot x$ (comutatividade).

iii. $(x+y)+z=x+(y+z)$ e $(x\cdot y)\cdot z=x\cdot(y\cdot z)$ (associatividade).

iv. $x+0=0+x=x$ e $x\cdot 1=1\cdot x=x$ (existência do elemento neutro).

v. $\exists -x\in\mathbb{Z}$, tal que $x+(-x)=(-x)+x=0$ (existência de inverso aditivo).

vi. $x\cdot(y+z)=x\cdot y+x\cdot z$ (distributividade do produto em relação a adição).

vii. O conjunto $\mathbb{N}$ é fechado para adição e para multiplicação, ou seja, $\forall x,y\in\mathbb{N}$ $x+y\in\mathbb{N}$ ou $x\cdot y\in\mathbb{N}$ (Fechamento de $\mathbb{N}$).

viii. (Tricotomia) Dados $x,y\in\mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verdadeira:

   I. $x=y$;

   II. $x-y\in\mathbb{N}$;

   III. $-(x-y)=y-x\in\mathbb{N}$;

Será considerado que *y é menor que x*, simbolizando por $y<x$, toda vez que a propriedade (II.) for verdadeira.

Com o objetivo de demonstrar o algoritmo da divisão euclidiana, será admitido o Princípio da Boa Ordenação (PBO) que de acordo com Gonçalves (2011) pode ser enunciado como se segue:

Diz-se que um conjunto $S \subset \mathbb{Z}$, tal que $S \neq \varnothing$ é limitado inferiormente, se existir $c \in \mathbb{Z}$, tal que $c \leq s$, $\forall s \in S$.

PROPOSIÇÃO 2.1: (Primeiro Princípio de Indução) Seja $P(n)$ uma sentença aberta em *n* e $a \in \mathbb{Z}$. Suponha que,

i. $P(a)$ é verdadeiro.

ii. $\forall n \in \mathbb{Z}$, supor $P(n)$ verdadeiro $\Rightarrow P(n+1)$ é verdadeiro.

Então, $P(n)$ é verdadeiro $\forall n \in \mathbb{Z}$.

Demonstração: Seja $S \subset \mathbb{Z}$, tal que $S \neq \varnothing$, tais que $\forall x \in S, P(x)$ é falsa. Pelo Princípio da Boa Ordenação, $\exists y_0 \in S$, tal que $y_0 \leq x, \forall x \in S$. Como $P(a)$ é verdadeiro, tem-se por hipótese que $a \notin S$, logo $y_0 \geq a$. Além disso, como $y_0 - 1 \notin S$, tem-se que $P(y_0 - 1)$ é verdadeiro. Daí, pela hipótese (ii.), isso implica $P(y_0 - 1 + 1) = P(y_0)$ verdadeiro. Isso é um absurdo, já que $y_0 \in S$. Portanto, $S = \varnothing$.

PROPOSIÇÃO 2.2: (Segundo Princípio de Indução) Seja $P(n)$ uma sentença aberta em *n* e $a \in \mathbb{Z}$. Suponha que,

i. $P(a)$ é verdadeiro.

ii. $\forall n \in \mathbb{Z}$, tal que $n > a$, supor $P(\mathrm{k})$ verdadeiro, com $0 \leq k < n \Rightarrow P(n)$ é verdadeiro.

Então, $P(n)$ é verdadeiro $\forall n \in \mathbb{Z}$.

Demonstração: Seja $S \subset \mathbb{Z}$, tal que $S \neq \varnothing$, tais que $\forall x \in S, P(x)$ é falsa. Pelo Princípio da Boa Ordenação, $\exists y_0 \in S$, tal que $y_0 \leq x, \forall x \in S$. Como $P(a)$ é verdadeiro, tem-se por hipótese que $a \notin S$, logo $y_0 \geq a$. Logo, $P(k)$ é verdadeiro $\forall a \leq k < y_0$, que pela proposição (ii.) $\Rightarrow P(y_0)$ é verdadeiro. Isso é uma contradição, logo $S = \varnothing$. Portanto, $P(n)$ é verdadeiro $\forall n \in \mathbb{Z}$.

TEOREMA 2.1. (Algoritmo da divisão Euclidiana) Sejam $a, b \in \mathbb{N}$ e $b \neq 0$, então existem $q, r \in \mathbb{N}$, tais que,

$$a = bq + r, 0 \leq r < b$$

Demonstração: A existência será provada utilizando a proposição 2.2.,isto é, por indução sobre *a*.

Se $a < b$ existem $q = 0$, $r = a$. Analisando o caso em que $a \geq b > 0$. Logo multiplicando a desigualdade por (-1) e adicionando *a,* tem-se $0 \leq a - b < a$, pela proposição (ii.) $\Rightarrow \exists q_1, r \in \mathbb{N}$ tais que, $a - b = q_1 b + r$, onde $0 \leq r < b$, de sorte $a = b(q_1 + 1) + r$, onde $0 \leq r < b$, daí $q = q_1 + 1$ e $r \in \mathbb{N}$.

Unicidade: Suponha $q_1, q_2, r_1, r_2 \in \mathbb{N}$, tais que $a = bq_1 + r_1$ e $a = bq_2 + r_2$, tais que $0 \leq r_1 < b$ e $0 \leq r_2 < b$. Daí segue que, $bq_1 + r_1 = bq_2 + r_2 \Rightarrow b(q_1 - q_2) = r_2 - r_1$, supondo $r_2 > r_1 \Rightarrow r_2 - r_1 > 0$ e $r_2 - r_1 < b \Rightarrow b(q_1 - q_2) = r_2 - r_1 < b$, o que seria um absurdo para ao caso $r_2 \neq r_1$, logo $r_1 = r_2$, daí $b(q_1 - q_2) = 0 < b \Rightarrow q_1 = q_2$.

Com o teorema da divisão euclidiana, é fácil mostrar como escrever os números no Sistema Decimal posicional, por meio de divisões sucessivas. Esse sistema é uma variante do sistema sexagesimal utilizados pelos Babilônios, desenvolvido na China e na Índia. Apenas em 1202 quando Fibonacci publica o livro *Liber Abacci* a Europa começa a aceitar o uso deste sistema (HEFEZ, 2014).

Em particular, se o resto é igual a zero é possível definir a divisibilidade em $\mathbb{Z}$. Sejam, $a, b \in \mathbb{Z}$, diz-se que *a divide b, ou a é divisor de b, ou b é múltiplo de a*, então $\exists c \in \mathbb{Z}$, tal que $b = ca$. Usa-se a notação $a \mid b$ (*a divide b)* caso contrário, $a \nmid b$.

O que acontece quando dividir um inteiro *a* qualquer por zero? Pelo teorema, consiste em encontrar $c \in \mathbb{Z}$, tal que, $a = 0 \cdot c + a$, no entanto, pelo teorema da divisão euclidiana, *c* é o quociente da divisão de *a* por zero, e pela demonstração da unicidade do quociente isso se torna um absurdo, uma vez que, *c* não pode assumir infinitos valores.

Existem quatro propriedades consideradas importantes pela literatura.

Proposição 2.3. Sejam $a, b, c, \mathrm{d} \in \mathbb{Z}$ tem-se:

I. $d \mid a$ e $d \mid b \Rightarrow d \mid ax + by$ tal que, $x, y \in \mathbb{Z}$;

II. (Limitação) $d \mid a \Rightarrow a = 0$ ou $|d| \leq |a|$;

III. (Transitividade) $a \mid b$ e $b \mid c \Rightarrow a \mid c$;

IV. $a \mid a$ (Reflexiva);

Demonstração:

I. Por hipótese, $d \mid a$ e $d \mid b$, assim pelo teorema da divisão euclidiana, $\exists q_1, q_2 \in \mathbb{Z}$, tais que $a = dq_1$ e $b = dq_2$, logo $ax + by = dq_1 x + dq_2 x$, o que implica $ax + by = d(q_1 x + q_2 y)$, como $q_1 x + q_2 y \in \mathbb{Z}$, pode-se concluir que $d \mid ax + by$.

II. Supondo $d \mid a$ e $a \neq 0$, pela divisão euclidiana, $\exists k \in \mathbb{Z}$, tal que $a = dk$, com $k \neq 0$, assim $|k| \geq 1 \Rightarrow |k||d| \geq |d| \Rightarrow |a| \geq |d|$.

III. Por hipótese, $a \mid b$ e $b \mid c$, assim pela divisão euclidiana, $\exists q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1 q_2$, portanto $a \mid c$.

A propriedade II é um caso particular da afirmação: dado um número natural a, se *b* é divisor positivo de *a,* pelo Teorema da Divisão Euclidiana, $1 \leq b \leq a$, no conjunto dos inteiros, o caso em que $b > a$, finaliza a divisão registrando o valor do quociente e do resto.

Sem perda de validade as demonstrações podem ser aplicadas aos divisores de valores estritamente positivos, uma vez que, se $d \mid x$ então $d \mid -x$. Isso é de fácil observação, já que $d \mid x$, por definição $\exists k \in \mathbb{Z}$ tal que, $x = dk$, multiplicando por (-1), tem-se $-x = d(-k)$, como $k_1 = (-1)k \in \mathbb{Z}$, então $-x = dk_1 \Rightarrow d \mid -x$. Logo, demonstrando para valores pertencentes ao conjunto dos $\mathbb{N} \subset \mathbb{Z}$, será válido para qualquer valor negativo.

Sejam dados $a, b \in \mathbb{Z}$, distintos ou não. Um número inteiro *d* será dito divisor comum de *a* e *b* se $d \mid a$ e $d \mid b$.

Proposição 2.4 Diz-se que um inteiro $d \geq 0$ é um Máximo Divisor Comum (mdc) de *a* e *b,* se possuir as seguintes propriedades:

i. d é um divisor comum de a e b;

ii. $\exists x_0, y_0 \in \mathbb{Z}$, tal que $d = ax_0 + by_0$

iii. d é divisível por todo divisor comum de a e b.

Sem perda de validade, como já foi discutido antes, será considerado $a, b \in \mathbb{N}^*$. Considerando o conjunto $S = \{ax + by \mid x, y \in \mathbb{Z}\}$. Note que, existe em S um subconjunto estritamente positivo, tal que para $x = y = 1$ tem-se pelo Princípio da Boa Ordenação um menor elemento d, tal que, $d = ax_0 + by_0$, com $x_0, y_0 \in \mathbb{Z}$.

Aplicando a divisão euclidiana, tem-se que $a = dq + r, 0 \leq r < d$, mas como já foi visto, $d = ax_0 + by_0$, daí $a = (ax_0 + by_0)q + r \Rightarrow r = a(1 - x_0 q) + b(-y_0 q)$, logo $r \in S$, por outro lado, $r < d$, o que só é possível se $r = 0 \Rightarrow a = dq \Rightarrow d \mid a$. De modo análogo, pode se concluir que $d \mid b$.

Pela proposição 2.3, se $d' \mid a$ e $d' \mid \mathrm{b}$, então $\forall x, y \in \mathbb{Z}$ tem-se $d' \mid ax + by$. De sorte, $\exists x_0, y_0 \in \mathbb{Z}$, tal que $d = ax_0 + by_0$, logo $d' \mid d$. Portanto, um $d \in \mathbb{Z}$, será dito mdc(a,b), se satisfazer as três condições.

Note que, a segunda condição afirma que se $(6,12) = 6$, então 6 é divisível por todos os divisores comuns de 6 e 12, ou seja, $1 \mid 6$, $2 \mid 6$ e $3 \mid 6$. Essa generalização é de grande importância, uma vez que, o fato de definir que o divisor é o maior elemento do conjunto de divisores comuns, não servirá para provar outras propriedades, o que só é possível com a condição iii.

O fato de supor que d é um inteiro não negativo, é resultado da observação de que, dados $a, b \in \mathbb{Z}$, se existir o mdc (a,b), então $(a,b) = (-a,b) = (a,-b) = (-a,-b)$.

A mais de dois milênios Euclides divulgou no livro XII do “Os elementos” uma demonstração de como encontrar o mdc de dois números usando o algoritmo estendido, que se baseia em aplicações de divisões sucessivas.

A demonstração do algoritmo estendido de Euclides é baseada nas discussões de Domingues e Iezzi (2003), como mostra o exemplo, abaixo.

Exemplo 2.1. Sejam $a, b, n \in \mathbb{Z}$. Mostre que se existe (a,b-na), então, (a,b) existe e (a,b)=(a,b-na).

Solução: Por hipótese existe um inteiro $d \geq 0$, tal que $d = mdc(a, b - na)$, logo $d \mid a$ e $d \mid b - na$. Logo, $\exists k_1, \mathrm{k}_2 \in \mathbb{Z}$, tal que, $a = dk_1$ e $b - na = dk_2$, o que implica $b = dk_2 + na \Rightarrow b = dk_2 + ndk_1 \Rightarrow b = d(k_2 + nd)$, portanto $d \mid b$.

Como $d = mdc(a, b - na)$, pela proposição 2.3, $\exists x, y \in \mathbb{Z}$, tal que $d = ax + (b - an)y \Rightarrow d = a(x - ny) + by$, o que satisfaz o item ii da propriedade 2.3. De modo análogo, a demonstração da propriedade iii da proposição 2.3, pode se concluir que todo divisor comum de *a e b* dividem d, portanto o *mdc(a,b-na)=mdc(a,b).*

Utilizando este exemplo pode se demonstrar o lema 2.1 e observar o comportamento das divisões sucessivas na busca o mdc.

Lema 2.1. Se $a = bq + r$ *então* $\mathrm{mdc}(a, \mathrm{b}) = mdc(\mathrm{b}, r)$.

Demonstração:

Seja $a = bq + r \Rightarrow r = a - bq$. Considere $d > 0, \mathrm{d} = \mathrm{mdc}(\mathrm{b}, \mathrm{r})$, daí é o mesmo que $d = mdc(\mathrm{b}, a - qb)$, pelo o que foi discutido no exemplo 2.1 isso implica $mdc(\mathrm{a}, \mathrm{b}) = \mathrm{mdc}(\mathrm{b}, \mathrm{r})$.

De acordo com Domingues e Iezzi (2003) encontrar o mdc(a,d) pelo algoritmo estendido de Euclides é aplicar as divisões euclidianas sucessivas vezes. Logo tem-se, $a = bq + r, 0 \leq r < b$, caso $r = 0$, então teríamos $b \mid a$, o que implica $mdc(a, b) = b = mdc(b, 0)$

Caso, $r \neq 0$ aplica-se o algoritmo em b e r, obtendo $b = rq_1 + r_1$, caso $r_1 = 0$ então o $mdc(b, r) = mdc(r, r_1)$. Caso, $r_1 \neq 0$, aplica-se novamente a divisão euclidiana. De modo geral, o processo fica descrito como a seguir.

$$
\begin{aligned}
&a = bq_0 + r_0; 0 \leq r_0 < b \\
&b = r_0 q_1 + r_1; 0 \leq r_1 < r_0 \\
&r_0 = r_1 q_2 + r_2; 0 \leq r_2 < r_1 \\
&r_1 = r_2 q_3 + r_3; 0 \leq r_3 < r_2 \\
&\cdots \\
&r_{n-2} = r_{n-1} q_n + r_n; 0 \leq r_n < r_{n-1}
\end{aligned}
$$

Como $0 \leq r_n < r_{n-1} < r_{n-2} < \cdots < r_0 < b$, o algoritmo para algum índice n chega-se ao resto igual a zero, finalizando as etapas. Pelo lema 2.1 $mdc(a, b) = mdc(b, r_0) = mdc(r_0, r_1) = \cdots = mdc(r_{n-1}, r_n) = r_{n-1}$, para $r_n = 0$.

Por exemplo, para calcular o (1030, 37), basta aplicar a divisão euclidiana sucessivas vezes.

$$
\begin{aligned}
&1030 = 37 \cdot 27 + 31 \\
&37 = 31 \cdot 1 + 6 \\
&31 = 6 \cdot 5 + 1 \\
&6 = 6 \cdot 1 + 0
\end{aligned}
$$

Assim, tem-se $(1030, 37) = (37, 31) = (31, 6) = (6, 1) = (1, 0) = 1$.

De forma mais simples, esse processo pode ser realizado em um diagrama semelhante ao “jogo da velha”, veja como segue na figura 4.

	27	1	5	6
1030	37	31	6	1
31	6	1	0	

Figura 4. Algoritmo estendido de Euclides, método de diagramas.

Existe uma interpretação geométrica muito interessante para o mdc, considere o mdc(16,7)=1, como mostra a figura 5.

	2	3	2	
16	7	2	1	
2	1	0	0	

Figura 5. Algoritmo estendido de Euclides mdc(35,3)

Imagine um retângulo 16x7, calcular o mdc, é preencher o retângulo com quadrados menores, a começar com o quadrado 7x7, em seguida 2x2 e por fim 1x1, ou seja, quadrados de lados iguais aos quocientes de cada divisão do algoritmo estendido. De acordo, com a figura 6, o mdc(16,7)=1 é o lado do menor quadrado utilizado para preencher todo o retângulo.

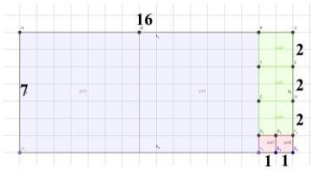


Figura 6. Representação Geométrica do mdc (16,7)

Veja que este é o único quadrado capaz de preencher um quadrado 7x7 e o 16x16 de forma exata. Desta forma, na geometria a definição poderia ser: Encontrar o mdc dos quadrados 7x7 e 16x16, é achar a maior medida comum deles.

Esta interpretação geométrica permite observar que a sequência de Fibonacci, definhada por 1,1,2,3,5,8,... onde cada termo da sequência é definido pela soma de dois termos anteriores, ou seja, $a_0, a_0, a_1, a_2, a_3, \cdots, a_n$, tal que $a_i = a_{i-2} + a_{i-1}, i = 0,1,2,3,4...$, geometricamente a sequência de Fibonacci é representada como mostra a figura 7.

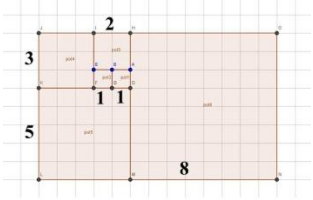


Figura 7. Representação geométrica da sequência de Fibonacci.

Tem-se também uma sequência de números que $mdc(a_{n-1}, a_n) = 1$, uma vez que todos, finalizam em uma quadrado 1x1.

Dados $a, b \in \mathbb{Z}$, serão ditos primos entre si, ou coprimos, se $(a,b) = 1$, ou seja, se o único divisor comum positivo de ambos é 1. No caso anterior, pode se afirmar que a sequência de Fibonacci é formada por números coprimos dois a dois.

Exemplo 2.2. Se a e b são inteiros não simultaneamente nulos e se $d = mdc(a,b)$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Solução: Sendo $d = mdc(a,b)$, pela proposição 2.2, $\exists x_0, y_0 \in \mathbb{Z}$, tal que $d = ax_0 + by_0 \Rightarrow 1 = \frac{a}{d}x_0 + \frac{b}{d}y_0$, ainda pela proposição 2.2, pode-se afirmar que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

2.2 NÚMEROS PRIMOS

Seja um número $p > 1$, tal que, os divisores de *p* são ± 1 e $\pm p$, diz-se que p é número primo. Esta definição permitiu concluir que dado, *p e q* primos, os seguintes fatos serão válidos.

I. $p \mid q \Rightarrow p = q$

É fácil observar considerando os divisores positivos e será trivial para os negativos. Note que, se $p \mid q$ com *q* primo, então só possui os divisores $p = 1$ ou $p = p$, por outro lado, *p* também é primo, logo por definição $p > 1 \Rightarrow p = q$.

II. $p \nmid \mathrm{a} \Rightarrow (\mathrm{p}, \mathrm{a}) = 1$

De fato, se $\mathrm{mdc}(p,a) = d$, então $d \mid p$ e $d \mid a$, como *p* é primo, então $d = 1$ ou $d = p$, por outro lado, $p \nmid a$, logo $p \neq d$. Portanto $d = 1$.

A propriedade II e a proposição 2.4 permite concluir que, $\exists x_0, y_0 \in \mathbb{Z}$, tal que $px_0 + ax_0 = 1$, sempre que $mdc(a, p) = 1$.

Exemplo 2.3 (lema de Euclides) Sejam $a, b, p \in \mathbb{Z}$. Se *p* é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Solução: Suponha que $p \nmid a$, pela propriedade II $mdc(a,\mathrm{p})=1$, daí $\exists x_0, y_0 \in \mathbb{Z}$, tal que $px_0 + ay_0 = 1 \Rightarrow (pb)x_0 + (ab)\,\mathrm{y}_0 = b$. Por hipótese, $p \mid ab$, logo $\exists k \in \mathbb{Z}$, tal que $ab = kp$. Daí, $(pb)x_0 + (ab)\,\mathrm{y}_0 = b \Rightarrow (pb)x_0 + kpy_0 = b \Rightarrow p(bx_0 + ky_0) = b$, logo $p \mid b$.

Além disso, todo número $a > 1$, que não seja primo é dito número composto. Desta forma, existe, $b \in \mathbb{Z}$, com $b \mid a$, logo pela definição de divisores $\exists k \in \mathbb{Z}$, tal que $a = bk$, com $1 < k < a$ e $1 < b < a$. Portanto, além de 1 e ele mesmo, o *a* apresenta *k* e *b* como possiblidade de divisores. Assim sendo, os número 2, 3, 5 e 7 são exemplos de números primos, e os número 4, 6, 8 e 9 são exemplos de números compostos.

O teorema fundamental da aritmética apresenta uma relação entre estes dois tipos de números, afirmando que os números compostos são escritos univocamente como um produto de primos.

Teorema 2.3. (Teorema Fundamental da Aritmética) Seja $n \geq 2$ um número natural. Podemos escrever n de uma única forma com um produto de fatores primos

$$n = p_1, p_2, \cdots, p_m$$

onde $m \in \mathbb{N}$ e $p_1 \leq \cdots \leq p_m$ são primos.

Demonstração:

De acordo com Domingues e Iezzi (2003) e Hefez (2014) a rigor essa demonstração deve-se racionar por indução. Desta forma, este teorema será demonstrado pela aplicação da proposição 2.2 o segundo princípio de indução.

O caso é trivial para $n = 2$.

Seja $n \geq 2$, se o número n é primo nada se tem a demonstrar. Para n composto, suponha ser verdadeiro para $\mathrm{k} \in \mathbb{N}; 0 \leq k < n$. Como *n* é composto, $\exists k_1, k_2 \in \mathbb{N}$, tal que $n = k_1 \cdot k_2$, com $1 < k_1 < n$ e $1 < k_2 < n$. Pela hipótese de indução, existem números primos $p_1, \cdots, p_s$ e $q_1, \cdots, q_r$, tais que $k_1 = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ e $k_2 = q_1 \cdot q_2 \cdot \ldots \cdot q_r$, o que implica afirmar que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_r$.

Para demonstrar a unicidade da escrita, suponha que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_s$ e $n = q_1 \cdot q_2 \cdot \ldots \cdot q_r$, com $p_i, i = 1,..,s$ e $q_i, i = 1,..,\mathrm{r}$ números primos. Como $q_1 \cdot q_2 \cdot \ldots \cdot q_r = p_1 \cdot p_2 \cdot \ldots \cdot p_s$, pode-se afirmar que $q_1 \mid p_1 \cdot p_2 \cdot \ldots \cdot p_s$, pelo exemplo 2.3 q_1 divide algum $p_i, \mathrm{i} = 1,...,\mathrm{s}$ e pela propriedade I da definição de números primos, pode-

se supor $p_1 = q_1$. Isso permite reescrever a igualdade como $q_2 \cdot \ldots \cdot q_r = p_2 \cdot \ldots \cdot p_s$ e repetir a análise, o que leva a concluir que $r = s$, logo $p_i = q_i, \forall i = 1,...,r = s$.

De modo geral, o teorema fundamental da aritmética afirma que existem dois tipos de números naturais, os que são primos e os que são escritos como um produto de primos, dito números compostos.

A mais de 2000 anos, Euclides mostrou que existem infinitos primos, argumentando que se o conjunto S de números primos fosse finito, então S seria limitado superiormente e $\exists n \in \mathbb{N}$ e $n \in S$, tal que, para algum $p \in S$ deveria ser válido que $p \mid n$. O que se torna uma contradição ao teorema fundamental da aritmética, uma vez que, se $n \in S$, então *n* é primo e pela definição de primos $n = p$.

2.3 EQUAÇÕES DIOFANTINAS LINEARES

Segundo Eves (2004), Hefez (2014) e Domingues e Iezzi (2003) as equações diofantinas estão presentes na obra de Diofanto *Arithmetica,* se trata de equações com coeficientes inteiros com incógnitas elevadas a expoentes inteiros, cujo estudo se baseia em encontrar soluções no universo dos inteiros. Diofanto estudava se as equações possuíam ou não soluções inteiras.

Conforme esta definição, permite afirmar que o ultimo teorema de Fermat, é uma equação Diofantina do tipo $a^n + b^n = c^n, n > 2$, que não possui soluções.

Nesta obra é de interesse apenas as equações diofantinas lineares de duas incógnitas, isto é, equações do tipo $ax + by = c, x, y \in \mathbb{Z}$ e sua solução será um par de inteiros (x_0, y_0) que satisfaça a igualdade. No entanto, como ocorre com o ultimo teorema de Fermat, nem todo equação diofantina possui solução. A proposição 2.5 mostra uma forma de identificar se uma equação possui solução nos inteiros.

Proposição 2.5 Seja $ax + by = c, x, y \in \mathbb{Z}$ tem solução se, e somente se, $d = mdc(a,b) \mid c$.

$\rightarrow \exists x_0, y_0 \in \mathbb{Z},\ ax_0 + by_0 = c \Rightarrow d = mdc(a,b) \mid c$.

Suponha $\exists x_0, y_0 \in \mathbb{Z},$ uma solução, logo $ax_0 + by_0 = c$, como $d \mid a$ e $d \mid b$, pela proposição 2.3, $d \mid c$.

$\leftarrow d = mdc(a,b) \mid c \Rightarrow \exists x_0, y_0 \in \mathbb{Z}, ax_0 + by_0 = c$

Como $d = mdc(a,b)$, pela proposição 2.3, $\exists x_0, y_0 \in \mathbb{Z}$, tal que $d = ax_0 + by_0$, mas por hipótese $d \mid c$ e portanto $c = dq$, daí $c = (ax_0 + by_0)q \Rightarrow c = a(x_0 q) + \mathrm{b}(y_0 q)$, logo $(x_0 q, y_0 q)$ é uma solução no universo dos inteiros.

Essa discussão será de grande importância nas estratégias de criptografia que serão discutidas no capítulo 4.

2.4 ARITMÉTICA MODULAR

Nesta sessão, serão presentadas umas das noções mais importantes desta pesquisa, resultado da existência de restos não nulos, que impulsionou os avanços nos estudos na teoria dos números. Introduzido por Gauss, trata-se de uma aritmética com os restos da divisão em eventos cíclicos (HEFEZ, 2014).

Definição: Seja $m \in \mathbb{N}$, diz-se que dois números *a* e *b* são congruentes módulo m, se os restos na divisão euclidiana por *m* forem iguais. Denota-se por,

$$a \equiv b \bmod m$$

diz-se que *a* é congruente a *b* módulo *m*, caso contrário $a \not\equiv b \bmod m$, ou seja, *a* não é congruente a *b* modulo *m*.

Por exemplo, $25 \equiv 37 \bmod 12$, já que, 25 e 37 deixam resto 1 quando dividido por 12.

Decorre da definição que a congruência módulo *m* é uma relação de equivalência.

Proposição 2.6: Seja $m \in \mathbb{N}$, $\forall a,b,c \in \mathbb{Z}$, tem-se que:

I. $a \equiv a \bmod m$.(reflexiva)

II. $a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$.(simétrica)

III. $a \equiv b \bmod m$ e $b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$.(transitiva)

Demonstração:

A demonstração de I e II é fácil de se observar. Para demonstrar III, basta aplicar a definição de congruência na hipótese. Sejam $a \equiv b \bmod m$ e $b \equiv c \bmod m$, pela definição aplica-se a divisão euclidiana por *m,* logo existem, $q_1, q_2, q_3 \in \mathbb{Z}$, tais que $a = mq_1 + r_1, 0 \le r_1 < m$, $b = mq_2 + r_2, 0 \le r_2 < m$ e $c = mq_3 + r_3, 0 \le r_3 < m$, além disso, $r_1 = r_2$ e $r_2 = r_3$, pela transitividade dos números inteiros[1], garante que $r_1 = r_3$, que pela definição de congruência permite concluir que $a \equiv c \bmod m$.

Veja que a estratégia para saber se dois números é congruente é realizar a divisão euclidiana e analisar a igualdade entre os restos, no entanto, outra relação é válida para esta análise, sem a necessidade de realizar a divisão euclidiana. É suficiente aplicar o seguinte resultado.

Proposição 2.7. Suponha que $a,b,m \in \mathbb{Z}$, com $m>1$. Tem-se que $a \equiv b \bmod m$ se, e somente, se $m \mid b-a$.

Demonstração:

Aplicando a divisão euclidiana em *m*, existem $q_{1,}q_2,r_1,r_2 \in \mathbb{Z}$, tais que, $a = mq_1 + r_1, 0 \le r_1 < m$ e $b = mq_2 + r_2, 0 \le r_2 < m$, logo

$$b-a = m(q_2 - q_1) + r_2 - r_1 \Rightarrow b-a = m(q_2 - q_1)$$

já que por hipótese *a* e *b* são congruentes. Portanto, $m \mid b-a$.

Por exemplo, o caso $25 \equiv 37 \bmod 12$, para saber se é verdade basta verificar se $12 \mid 37-25=12$.

Aplicando este resultado na divisão euclidiana de *a* por *m*, tem-se que existe $q,r \in \mathbb{Z}$, tal que $a = mq + r, 0 \le r \le m-1$. Daí, $a-r = mq \Rightarrow m \mid a-r$, logo pela proposição 2.7 $a \equiv r \bmod m$. Está análise permite concluir que todo número inteiro é congruente a um de seus restos. Logo uma forma que encontrar o resto de uma divisão de *a* por *m*, basta encontrar um dos números 0, 1, 2, 3, 4, ..., $m-1$ em que a diferença por *a* seja um múltiplo de *m.*

O fato de considerar o número é um dos 0, 1, 2, 3, 4, ..., $m-1$, é resultante da divisão euclidiana, o resto é um inteiro compreendido entre 0 e *m,* na qual ele não pode ser *m.* Por exemplo, todo número dividido por 2 só deixa resto, 0,1 ou 2. Na divisão por 3 os restos possíveis são 0, 1, 2 e 3. E assim sucessivamente.

Uma análise semelhante cabe na propriedade simétrica, dizer que $b \equiv a \bmod m$ é encontrar que $a-b = mk, \forall k \in \mathbb{Z}$ e o mesmo vale para $a \equiv b \bmod m$.

O que torna mais interessante as operações de congruência é o fato de ser uma relação de equivalências compatível as operações de adição e multiplicação.

Proposição 2.8. Sejam $a,b,c,d \in \mathbb{Z}$, com $m>1$. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$ tem-se

I. $a+c \equiv b+d \bmod m$.

II. $a \cdot c \equiv b \cdot d \bmod m$.

Demonstração:

Por hipótese, $a \equiv b \bmod m$ e $c \equiv d \bmod m$, pela proposição 2.7 tem-se que, $m \mid b-a$ e $m \mid d-c$, logo pela divisão euclidiana existem $k_1, k_2 \in \mathbb{Z}$, tais que $b-a=mk_1$ e $d-c=mk_2$.

I. Basta somar as duas igualdades, daí $(b-a)+(\mathrm{d}-\mathrm{c})=\mathrm{m}(\mathrm{k}_1+k_2)$, o que implica $(b+d)-(a+c)=m(k_1+k_2)$, portanto $a+c \equiv b+d \bmod m$.

II. Note que, $bd-ac=bd-ac+da-da$, o que implica $bd-ac=d(b-a)+a(d-c)$, pela hipótese pode-se concluir que $bd-ac=m(dk_1+ak_2)$, portanto , $m \mid bd-ac$, concluindo-se que $a \cdot c \equiv b \cdot d \bmod m$.

Por exemplo, sendo $25 \equiv 37 \bmod 12$ e $1 \equiv 13 \bmod 12 \Rightarrow 26 \equiv 50 \bmod 12$.

Na aritmética modular consideram a lei o cancelamento, o ato de cancelar termos iguais nas operações de congruência. A proposição a seguir, apresenta ser válido para a adição. Adiante a discussão será para mostrar que o mesmo não ocorre com a multiplicação. Por exemplo, $2 \cdot 15 \equiv 2 \cdot 21 \bmod 12$, no entanto $15 \not\equiv 21 \bmod 12$.

Proposição 2.9. Sejam $a,b,c,m \in \mathbb{Z}$, com $m>1$. Tem-se que

$$a+c \equiv b+c \bmod m \Leftrightarrow a \equiv b \bmod m.$$

Demonstração.

$\Rightarrow$ Considerando $a \equiv b \bmod m$ e $c \equiv c \bmod m$ segue-se da proposição 2.8 que $a+c \equiv b+c \bmod m$.

$\Leftarrow$ Se $a+c \equiv b+c \bmod m$, pela proposição 2.7, $\exists k \in \mathbb{Z}$, tal que $(b+c)-(a+c)=mk \Rightarrow b-a=mk$, portanto $a \equiv b \bmod m$.

Observe que fazer o cancelamento na adição é o mesmo que fazer a diferença de valores iguais na congruência. Ou seja, $25 \equiv 37 \bmod 12 \Rightarrow 25-5 \equiv 37-5 \bmod 12$. Já na multiplicação fazer este cancelamento é realizar a divisão de valores iguais. Antes de introduzir a multiplicação, veja a seguinte discussão que será importante no resultado do cancelamento.

De acordo com Hefez (2014), Coutinho (2014), e Moreira, Martinez e Saldanha (2012), o conjunto de números inteiros cujos elementos são os restos da divisão por *m*, ou seja, os números 0, 1, 2, 3, 4, ..., $m-1$, será chamado de *sistema completo de resíduos.* Neste caso, o sistema completo de resíduos são os primeiros estudantes da lista de cada sala. Portanto, este conjunto possui *m* elementos.

Com as propriedades da congruência é interessante apresentar ao aluno a unicidade do resto da divisão euclidiana, base considerar que, seja $a \equiv r \bmod m, 0 \leq e < m$ deve-se mostrar que *r* é único.

2.4.1 Inversos modulares

Esta subseção se trata de um dos conceitos mais importantes na criptografia, visto que, por meio destas ideias é que se define a existência das chaves. Por esse, motivo merece muita atenção, e um espaço especial.

Falar de inversos modulares se trata da operação da divisão na aritmética modular. Segundo Eves (2004) as divisões realizadas pelos povos antigos baseavam-se em uma tabela de inversos multiplicativos, o mesmo ocorre na aritmética modular, para operar divisões será necessário conhecer quais os inversos multiplicativos modulo *m.*

Define-se como $Z_m = \{1, 2, 3, ..., \mathrm{m}-1\}$ o conjunto de resíduos modulo *m*, esta discussão será pautada em analisar quais resíduos possuem inversos modulares, sendo assim, segue a definição de inversos modulares.

Definição: Sejam $r \in Z_m$, possuirá inverso modulo *m* se , existir um $r' \in \mathrm{Z}_m$, tal que,

$$r \cdot r' \equiv 1 \bmod m$$

ou seja, $r \cdot r'$ deixa resto 1 quando dividido por *m.*

Além disso, se *r* possui inverso modular, então qualquer $a \in \mathbb{Z}, a \equiv r \bmod m$, também possuirá inverso modular. Esta afirmação é possível, devido à transitividade da congruência.

Veja dois exemplos de classes residuais e quais resíduos possuem inversos modulares, perceba que nem todos os resíduos de uma classe possui inverso.

Tabela 5- Tabela dos inversos módulo 11.

Z_{11}	1	2	3	4	5	6	7	8	9	10
Inversos modulares	1	6	4	3	9	2	8	7	5	10

Fonte: próprio autor.

Tabela 6 – Tabela dos inversos módulo 12

Z_{12}	1	2	3	4	5	6	7	8	9	10	11

Inversos modulares	1	-	-	-	7	-	5	-	-	-	11

Fonte: próprio autor.

Observe que todos os resíduos de Z_{11}, possuem inversos modulares, no entanto, o Z_{12} só possui dois resíduos com inversos modulares o 1 e o 11. Além disso, zero é um resíduo, mas não aparece na tabela, isso é devido, ao fato de que o resíduo multiplicado pelo seu inverso tem que deixar resto 1 ao ser dividido por *m,* no entanto, todo inteiro multiplicado por zero, sempre deixa produto zero, e neste caso, quando dividido por *m* sempre deixará resto zero.

Em todo conjunto Z_m, o 1 sempre é inverso dele mesmo, já que 1 é elemento neutro da multiplicação. O ultimo resíduo de Z_m é o $m-1$ e seu inverso modular é ele mesmo. Note que, $(\mathrm{m}-1)(\mathrm{m}-1)$ tem que deixar resto 1 quando dividido por *m*, logo tem-se que $(m-1)(m-1)=m^2-2m+1 \Rightarrow m(m-2)+1$, ou seja, o número $(\mathrm{m}-1)(\mathrm{m}-1)$ quando dividido por *m*, deixa quociente (*m-2)* e resto 1.

Uma consideração importante ao organizar a tabela dos inversos modulares é que, cada resíduo, possui exatamente um inverso modular, ou seja, ele é único. Para provar a unicidade dos inversos modulares, basta considerarem que $\exists r', r'' \in Z_m$, tal que, $r \cdot r' \equiv 1 \bmod m$ e $r \cdot r'' \equiv 1 \bmod m$, daí pela reflexiva da congruência (proposição 2.6) e a proposição 2.7, tem-se que $r'' \cdot r \cdot r' \equiv 1 \cdot r'' \bmod m \Rightarrow r' \equiv r'' \bmod m$, por outro lado, $r' \cdot r \cdot r'' \equiv 1 \cdot r' \bmod m \Rightarrow r'' \equiv r' \bmod m$, ambos os casos, chegam ao mesmo resultado, logo pela proposição 2.2, $\exists k \in \mathbb{Z}$, tal que $r''-r'=\mathrm{mk}$. Por hipótese, $r', r'' \in Z_m$, são resíduos, o que implica, $0 \leq r' < r'' < m$ (análogo, o caso $r'' < r'$), como $r''-r'$ é múltiplo de *m*, isso só é possível se a diferença for igual a zero, daí $r''=r'$.

Ao comparar as tabelas dos inversos de Z_{11} e Z_{12} é notório que alguns resíduos não possuem inversos. Este comportamento está diretamente ligado às propriedades de existência dos inversos modulares.

Teorema 2.3. Se existir um fator primo comum entre *r* e *m,* então não tem inverso módulo *m.*

Demonstração:

Seja $m \in \mathbb{N}^*$ e $1 < r < m$, tal que *m* e *r* possuem algum fator comum *p,* $1 < p < m$. Logo, $\exists b,c \in \mathbb{N}$, tal qual $m = pb$ e $r = pc$. Além, disso $m \equiv pb \bmod m$ pela transitividade,

$$m \equiv 0 \bmod m \Rightarrow pb \equiv 0 \bmod m \qquad (2.1)$$

Por outro lado, note que $b = m/p \Rightarrow 1 < b < m$. Contudo, $b \cdot r \equiv b \cdot p \cdot c \bmod m$, da eq.(2.1) conclui-se que,

$$b \cdot r \equiv b \cdot p \cdot c \equiv 0 \bmod m \qquad (2.2)$$

Suponha que *r* possui um inverso *r'* módulo *m*, isto é, $r \cdot r' \equiv 1 \bmod m$, multiplicando por *b*¸ tem-se

$$b \cdot r \cdot r' \equiv 1 \cdot b \bmod m \Rightarrow (b \cdot r) \cdot \mathrm{r}' \equiv b \bmod m$$

Relacionando com a equação (2.2),

$$(b \cdot r) \cdot \mathrm{r}' \equiv b \bmod m \Rightarrow 0 \cdot r' \equiv b \bmod m$$
$$\Rightarrow b \equiv 0 \bmod m$$

Uma contradição, visto que, $1 < b < m$. Portanto, se existir um fator primo comum entre *r* e *m,* então não tem inverso módulo *m.*

Observe que na tabela Z_{12}, os resíduos, 2, 4, 6, 8 e 10, possuem o fator primo 2 em comum com 12, já que, são números pares. E os números 3 e 9, possuem fator comum 3. Até o momento, só é possível identificar quando um número não possui inverso modular.

Suponha que *r* tem inverso módulo *m*. Pela definição, $\exists r' \in Z_m$, tal que $r \cdot r' \equiv 1 \bmod m$. Pela proposição 2.7, $\exists k \in \mathbb{Z}$, tal que $r \cdot r' - 1 = km \Rightarrow r.r' + m(-k) = 1$, supondo $d = -k$, tem-se que $r.r' + md = 1$. De sorte, é uma equação diofantina linear, pela proposição 2.9, só possui soluções inteiras se $(r,m) \mid 1$, logo $(r,m) = 1$, isto é, se *r* possui inverso modular, então *r e m* são primos entre si. Agora, está mais claro o fato de 5 e 7 possuir inverso modulo 12.

O teorema a seguir mostra que se *r* possui inverso modular, então será válido a lei do cancelamento, ou seja, existe solução na operação de divisão.

Teorema 2.3. Seja $a,b,r,m \in \mathbb{Z}$, com $m > 1$e $(\mathrm{r},m) = 1$. Tem-se que

$$r \cdot b \equiv r \cdot c \bmod m \Leftrightarrow b \equiv c \bmod m$$

Demonstração:

Provar que $r \cdot b \equiv r \cdot c \bmod m \Rightarrow b \equiv c \bmod m$. Por hipótese, $(\mathrm{r},m) = 1$, isso implica dizer que $\exists r' \in Z_m$, tal que $r \cdot r' \equiv 1 \bmod m$. Logo, pelas proposições 2.6 e 2.7, pode se

afirmar que $r \cdot a \equiv r \cdot b \bmod m \Rightarrow r' \cdot r \cdot a \equiv r' \cdot r \cdot b \bmod m \Rightarrow a \equiv b \bmod m$. A reciproca, do teorema é fácil de observar aplicando a multiplicação entre $a \equiv b \bmod m$ e $r \equiv r \bmod m$.

Agora, ficou mais claro porque todos os resíduos de Z_{11}, possuem inversos modulares. O que permite concluir que se *m* é um número primo, então todos os elementos de sua classe residual, possui inverso modular.

Um exemplo da aplicação dos inversos modulares e o teorema 2.3 são, seja $27 \equiv 15 \bmod 12 \Leftrightarrow 3 \cdot 9 \equiv 3 \cdot 5 \bmod 12$, aplicando a lei do cancelamento, de sorte $9 \not\equiv 5 \bmod 12$, visto que, $(3,12) \neq 1$, logo não possui inverso modular. Por outro lado,

$$27 \equiv 54 \bmod 11 \Leftrightarrow 3 \cdot 9 \equiv 3 \cdot 18 \bmod 11$$

Como $(3,11) = 1$, a lei do cancelamento será válida, logo $3 \cdot 4 \equiv 1 \bmod 11$, daí tem-se que $4 \cdot 3 \cdot 9 \equiv 4 \cdot 3 \cdot 18 \bmod 11 \Rightarrow 9 \equiv 18 \bmod m$.

Para fechar este capítulo, será apresentado o resultado do teorema do Suíço Leonard Paul Euler. Desde o século XVIII Euler, mostra uma maneira de contar quantos elementos *r* existem dentro de um conjunto Z_m, tal que $(r,m) = 1$. Euler apresentou várias contribuições a teoria dos números, no entanto, daremos ênfase uma minúscula parte que será importante nas atividades propostas neste obra.

Proposição 2.10. Se *p* é um número primo e *r,* um número natural, então tem-se que

$$\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$$

Demonstração:

Note que o objetivo é contar os números que são coprimos com p^r, logo a ideia é analisar quantos números possuem fatos primo comum p^r. De 1 até p^r temos p^r números naturais, desse temos que retirar os múltiplos de p^r, daí são $p, 2p, 3p, ..., p^{r-1}p$, isto é, p^{r-1} números. Portanto $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$.

Este resultado permite analisar quantas soluções possuem a congruência $aX \equiv 1 \bmod m$, que se observar bem, se trata do inverso modular. Essas consequências geradas pelas contribuições de Euler são fundamentais em sistemas criptográficos.

2.5 MATRIZES E DETERMINANTES

O desenvolvimento das matrizes e determinantes por boa parte da história esteve relacionado à resolução de sistemas de equações lineares. Apesar de sua definição surgir apenas no século XIX, seus registros são bem antigos.

O registro mais antigo deste conhecimento está presente no mais importante texto da matemática Chinesa, o *K'ui-cb'ang Suan-sbu* (Nove capítulos sobre a Arte da Matemática) do século I a.C. De autoria desconhecida, concentra a matemática da época e supõe ser construída por vários autores. Esse conhecimento é apresentado em 246 problemas, seguido de sua resposta e processo de resolução, distribuído em nove capítulos (EVES, 2004).

Percebe a aplicação de ideias semelhante ao estudo de matrizes, no capítulo 8, na qual é aplicado o método *Fangsheng,* que consiste em solucionar problemas dispondo os dados em linhas e colunas aplicando o escalonamento, e o mais interessante é que o processo de resolução é o mesmo utilizado por Gauss, anos depois. Além disso, as equações eram dispostas em colunas, não em linhas como atualmente.

No entanto, os interesses pelo assunto só veio a surgir no século XVII impulsionados pelos estudos de matemáticos como Fermat e René Descartes sobre a geometria analítica ao resultar em equações com várias incógnitas (SANTOS, 2007).

Dedicado aos estudos das cônicas o matemático suíço Gabriel Cramer (1704-1752) apresentou em 1750 uma regra para resolução de sistemas lineares, baseado no cálculo de determinantes publicado em 1748 pelo matemático escocês Colin Maclaurin (1698-1746). Esta regra hoje é conhecida como Regra de Cramer, pelo fato de sua publicação possuir uma notação superior a de Maclaurin, provavelmente favoreceu que o mundo optasse por identificar a regra pelo nome de Cramer (EVES,2004).

Veja que o método da Regra de Cramer utilizava do conceito de determinantes, o que permite afirmar que este surgiu antes mesmo das definições de matrizes, diferente da sequência definida para estudo atualmente, na qual, primeiro se estuda os conceitos de matrizes para depois estudar os determinantes.

Foi o matemático inglês Arthur Cayley que tratou dos conceitos de matrizes como coeficientes organizados em quadrados e retângulos publicando em 1858 o

artigo *A memoir on the Theory of Matrices* onde discute as operações aritméticas possíveis de se realizar com matrizes quadradas, bem como as propriedades admitidas sobre estas operações. No entanto, o nome matriz foi utilizado pela primeira vez pelo matemático inglês James Joseph Sylvester, em 1850 (EVES, 2004; LIMA, 2011).

2.5.1 Matrizes

A discussão a seguir tem como embasamento as obras Hefez e Fernandes (2012), Howard e Rorres (2001) e Boldrini (1980) para além do que for apresentado como sugestão veja as referências citadas.

Definição: Dados $m,n \in \mathbb{N}$, a matriz real de ordem m por n $(m \times n)$ é a tabela formada por elementos (entradas da matriz) de $\mathbb{R}$ distribuídos em m linhas e n colunas.

Por exemplo a matriz,

$$\begin{bmatrix} 4 & 5 \\ x & -2 \\ 7 & 8 \end{bmatrix}$$

é uma matriz 3×2, isto é, formada por três linhas e duas colunas, na qual as entradas da primeira linha são os elementos 4 e 5.

É comum representar as entradas por meio das notações A_{ij} ou a_{ij}, na qual, os índices indicam nesta ordem a linha e a coluna. Desta forma, a matriz $m \times n$ é representada por,

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \text{ ou } A = \left[a_{ij} \right]_{m \times n}$$

Esta notação posicional foi sugerida pelos matemáticos Gottfried Wilhelm Leibiniz (1646-1716) e Alexandre-Théophile Vandermonde (1735-1796) onde deixa de lado as incógnitas e concentrasse na combinação dos coeficientes (SANTOS, 2007).

Além disso, o símbolo $M(m,n)$ denota o conjunto das matrizes $m \times n$. Veja que as entradas $a_{11}, a_{22}, a_{33}, \cdots, a_{ii}$ formam a diagonal principal.

Definição: Dada uma matriz $A=[a_{ij}]_{m\times n}$, chama-se transposta de A, e denota-se por A^t, a matriz $[b_{ij}]_{n\times m}$, tal que $b_{ij}=a_{ji}$, $\forall 1\le i\le n$ e $\forall 1\le j\le m$.

Por exemplo,

$$A=\begin{bmatrix}0 & 6\\ 3 & -1\\ 2 & 5\end{bmatrix}\Leftrightarrow A^t=\begin{bmatrix}0 & 3 & 2\\ 6 & -1 & 5\end{bmatrix}$$

Além disso, se $A^t=A$ diz que a matriz A é simétrica e chamada de antissimétrica, caso $A^t=-A$.

As operações internas definidos no conjunto das matrizes $M(m,n)$ serão discutidas a seguir, apresentando as propriedades que cada operação admite.

Definição: A soma de duas matrizes $A=\left[a_{ij}\right]_{m\times n}$ e $B=\left[b_{ij}\right]_{m\times n}$ de mesma ordem, denotada por $A+B$, é a matriz $C=\left[c_{ij}\right]_{m\times n}$ de mesma ordem, tal que $c_{ij}=a_{ij}+b_{ij}$ para todo $1\le i\le m$ e $1\le j\le m$.

Exemplo 3.1

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

Seja uma matriz $A=\left[a_{ij}\right]_{m\times n}$, a matriz oposta de A é definida como a matriz $-A=\left[-a_{ij}\right]_{m\times n}$.

A adição de matrizes possuem propriedades semelhantes à adição de números reais, como mostra o resultado a seguir.

Proposição 2.11 Se A, B e C são matrizes de mesma ordem $m\times n$, então:

I. $A+(B+C)=(A+B)+C$ (associatividade da adição)

II. $A+B=B+A$ (comutatividade da adição)

III. $A+0=A$, tal que 0 denota a matriz nula (elemento neutro)

IV. $A+(-A)=0$ (elemento simetrizável)

A operação de subtração entre duas matrizes A e B, é definida de maneira usual, por meio a adição entre a matriz A e a matriz simétrica de B, ou seja, $A+(-B)=A-B$.

O conjunto das matrizes $M(m,n)$, admite a operação multiplicação por escalar, também considerada de grande importância. Neste caso, dada a matriz $A=\left[a_{ij}\right]_{m\times n}$ e $k\in\mathbb{R}$, o produto de A por k, é definido como $kA=\left[ka_{ij}\right]_{m\times n}$.

Por exemplo,

$$2\begin{bmatrix}3 & -5\\ 1 & 3\end{bmatrix}=\begin{bmatrix}2\cdot 3 & 2\cdot(-5)\\ 2\cdot 1 & 2\cdot 3\end{bmatrix}=\begin{bmatrix}6 & -10\\ 2 & 6\end{bmatrix}$$

Proposição 2.12. A multiplicação por escalar admite as seguintes propriedades, para quaisquer $A,B\in M(m,n)$ e $k_1,k_2\in\mathbb{R}$.

I. $k\left(A+B\right)=kA+kB$

II. $\left(k_1+k_2\right)A=k_1A+k_2A$

III. $k_1\left(k_2A\right)=\left(k_1k_2\right)A$

IV. $1\cdot A=1\cdot A=A$

Estes resultados podem ser observados por meio das propriedades e operações definidas nos reais, já que o escalar é operado com cada entrada $a_{ij}\in\mathbb{R}$, com $i,j\in\mathbb{N}$ da matriz, e pela observação da definição de igualdade de matrizes.

De fato, sendo $A=\left[a_{ij}\right]$, $B=\left[b_{ij}\right]\in M(m,n)$ e $k_1,k_2\in\mathbb{R}$, então as provas dos resultados da proposição 2.12, são analisados como segue:

I. Sendo $k_1(A+B)=k_1[a_{ij}+b_{ij}]=[k_1(a_{ij}+b_{ij})]$, aplicando a distributiva dos reais, tem-se que $[k_1(a_{ij}+b_{ij})]=[k_1a_{ij}+k_1b_{ij}]=[k_1a_{ij}]+[k_1b_{ij}]$, pela definição de produto por escalar, pode-se afirmar que $[k_1a_{ij}]+[k_1b_{ij}]=k_1[a_{ij}]+k_1[b_{ij}]=k_1A+k_1B$.

II. Sejam $(k_1+k_2)A=(k_1+k_2)[a_{ij}]$, pela definição de produto de uma matriz por escalar, tem-se $[(k_1+k_2)a_{ij}]=[k_1a_{ij}+k_2a_{ij}]=[k_1a_{ij}]+[k_2a_{ij}]=k_1[a_{ij}]+k_2[a_{ij}]=k_1A+k_2A$.

III. $k_1(k_2A)=k_1(k_2[a_{ij}])=k_1[k_2a_{ij}]=[k_1k_2a_{ij}]=(k_1k_2)[a_{ij}]=(k_1k_2)A$.

IV. De modo análogo, pode se observar que $1A=A$, considerando que 1 é o elemento neutro da multiplicação nos reais.

Definição: Sejam $A=[a_{ij}]_{m\times n}$ e $B=[b_{ij}]_{n\times p}$ duas matrizes. O produto de A por B, denotado por AB, é definido como a matriz $C=[c_{ij}]_{m\times p}$ tal que

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = a_{i1} b_{1j} + \cdots + a_{in} b_{nj} \quad \forall, 1 \le i \le m \text{ e } \forall, 1 \le j \le p$$

Na prática, deve-se destacar a linha 1 da matriz A e a coluna 1 da matriz B, para que seja definido a primeira entrada da matriz AB (figura 1).

$$AB = \begin{bmatrix} \boxed{a_{11} & a_{12} & \cdots & a_{1n}} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} \boxed{b_{11}} & b_{12} & \cdots & b_{1p} \\ \boxed{b_{21}} & b_{22} & \cdots & b_{2p} \\ \boxed{\vdots} & \vdots & \ddots & \vdots \\ \boxed{b_{n1}} & b_{m2} & \cdots & b_{mp} \end{bmatrix}$$

Figura 1: Multiplicação da matriz AB.

Logo, a primeira entrada da matriz $AB = C$, será $c_{11} = a_{11} b_{11} + a_{12} b_{21} + \cdots + a_{1n} b_{n1}$, de modo, análogo determina as demais entradas da matriz produto.

Note que, o número de elementos da linha de A tem que ser igual ao número elementos da coluna de B. Sem perda de generalidade, supondo que o número de elementos da linha de A, for maior que o número de elementos da coluna de B, faltará elementos em B, para serem multiplicados com os de A. Isso, é válido para todas as linhas de A e colunas de B, logo, pode-se afirmar que para a multiplicação está bem definida, é necessário que o número de colunas de A seja igual o número de linhas de B.

Por exemplo,

$$AB = \begin{bmatrix} 1 & -2 \\ 5 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 1 \cdot 1 + (-2) \cdot 3 & 1 \cdot 2 + (-2) \cdot 4 \\ 5 \cdot 1 + 0 \cdot 3 & 5 \cdot 2 + 0 \cdot 4 \\ 0 \cdot 1 + 1 \cdot 3 & 0 \cdot 2 + 1 \cdot 4 \end{bmatrix} = \begin{bmatrix} -5 & -6 \\ 5 & 10 \\ 3 & 4 \end{bmatrix}$$

Veja que, o produto BA neste caso, não está definido, uma vez que o número de colunas de B é igual a 2 e o número de linhas de A é igual a 3.

Logo uma condição necessária para se obter $AB = BA$ é A e B serem matrizes quadradas, apesar disso, não é uma condição suficiente. Por exemplo, as matrizes A e B a seguir.

$$A = \begin{bmatrix} 1 & -2 \\ 5 & 0 \end{bmatrix} \text{ e } B = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix} \text{ tal que, } AB = \begin{bmatrix} 1 & 4 \\ 5 & 10 \end{bmatrix} \neq BA = \begin{bmatrix} 11 & -2 \\ -5 & 0 \end{bmatrix}$$

De modo mais geral, veja o que acontece com as entradas das matrizes produtos obedecendo à igualdade $AB = BA$. Pela definição de igualdade de matrizes e do produto, tem-se que a primeira entrada será,

$$a_{11} b_{11} + a_{12} b_{21} + a_{13} b_{31} + \cdots + a_{1n} b_{m1} = b_{11} a_{11} + b_{12} a_{21} + b_{13} a_{31} + \cdots + a_{1n} b_{m1}$$

$$a_{12}b_{21} + a_{13}b_{31} + \cdots + a_{1n}b_{m1} = b_{12}a_{21} + b_{13}a_{31} + \cdots + a_{m1}b_{m1}$$

Logo, para esta igualdade ser válida, em cada parcela $a_{1n}b_{m1} = a_{m1}b_{m1}$, a comutatividade entre as matrizes seria validade se $a_{ij} = a_{ji}$ ou $a_{ij} = b_{ji}$, para todo $1 \leq i \leq m$ e para todo $1 \leq j \leq n$, ou seja, se A fosse uma matriz simétrica (B fosse uma matriz simétrica) ou $AB = B^t A$ ou $AB = BA^t$.

Isso permite afirmar, que a multiplicação de matrizes não possui a propriedade comutativa. Além disso, na multiplicação de um número real qualquer por zero, o produto sempre é zero, o mesmo não pode ser afirmado na multiplicação de matrizes. Veja o que acontece com as matrizes A e B abaixo:

$$AB = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix} = 0$$

O produto entre as matrizes A e B não nulas é a matriz nula. Desta forma, a proposição 2.13 que apresenta as propriedades da multiplicação serão validadas, sempre que as operações sejam possíveis.

Proposição 2.13. Sejam as matrizes $A = [a_{ij}]$, $B = [b_{ij}]$, $C = [c_{ij}] \in M(m,n)$, desde que as operações sejam possíveis, tem-se:

I. Distributiva à esquerda da multiplicação em relação à adição.
$A(B + C) = AB + AC$

II. Distributiva à direita da multiplicação em relação a adição.
$(A + B)C = AC + BC$

III. Associatividade.
$(AB)C = A(BC)$

IV. Existência do elemento neutro.
$AI = IA = A$

Para demonstrar estes resultados basta aplicar as definições de adição e multiplicação de matrizes. Como mencionado no inicio do capítulo, as matrizes se configuram como uma ferramenta para solucionar sistemas de equações lineares. Tratando-se de uma matriz do tipo $AX = B$, chamada também de equação matricial, veja que a matriz B é o produto da matriz A por X, tal que

$$A=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix},\ X=\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}\ e\ B=\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

onde a matriz A é chamada de matriz dos coeficientes, X a matriz das incógnitas e B a matriz dos termos independentes.

No entanto, o objetivo de toda equação é determinar os valores para as incógnitas, desta forma, existe uma outra operação de matrizes presente nas resoluções de sistemas lineares matriciais.

$$X = BA^{-1}$$

No conjunto dos reais, multiplicar um real por um simétrico é chamado de quociente de A e B, ou seja, configura a operação da divisão. Portanto, para solucionar o sistema é necessário operar a divisão entre matrizes. Mas para isso, Cayley mostrou no século 19 que é necessário determinar a matriz A^{-1}, conhecida como matriz inversa de A.

Assim como na multiplicação dos reais, determinar a matriz inversa na multiplicação de matrizes trata-se em determinar a matriz A^{-1}, tal que $AA^{-1} = A^{-1}A = I_n$, onde A é uma matriz quadrada de ordem n.

Por exemplo, dada a matriz

$A=\begin{bmatrix} 7 & 4 \\ 1 & 2 \end{bmatrix}$, tem-se que a matriz inversa será $A^{-1}=\begin{bmatrix} 2 & -4 \\ -1 & 7 \end{bmatrix}$, já que $AA^{-1} = A^{-1}A = I_2$.

No entanto, nem toda matriz quadrada possui uma inversa, a título de exemplo a matriz nula, não possui inversa, pois não existe mais matriz de ordem n, tal que o produto entre as duas gere uma matriz identidade de ordem n, ou seja, sendo A à matriz nula e B uma matriz quadrada de ordem n, então $AB \neq I_n$. Outro exemplo é a matriz,

$C=\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, pois não existe C^{-1}, tal que $CC^{-1} = I_2$.

Portanto, se A admite inversa, então A é dita invertível e é válida a proposição a seguir:

Proposição 2.14. Seja A uma matriz quadrada de ordem n, se A é invertível, então sua inversa é única.

Demonstração: Para provar a unicidade das matriz inversa, basta supor que existem duas matrizes B e C inversas de A, logo será válido que $AB = I_n$ e $AC = I_n$, daí considerando

$$B = BI_n = B(AC) = (BA)C = I_nC = C$$

Portanto, $B = C$ implicando a unicidade da inversa de A.

A proposição a seguir, apresenta as propriedades admitidas pelas matrizes inversas.

Proposição 2.15. Sejam A e B matrizes quadradas de ordem n.

I. Se A é invertível então A^{-1} também é invertível e $(A^{-1})^{-1} = A$.

II. Se A e B são invertíveis, então AB também é invertível e $(AB)^{-1} = A^{-1}B^{-1}$.

Demonstração:

I. Seja A uma matriz quadrada invertível de ordem n e A^{-1} a sua inversa, tal que $AA^{-1} = A^{-1}A = I_n$. Afirmar que A^{-1} implica existe $B = \left(A^{-1}\right)^{-1}$ uma matriz quadrada de ordem n, tal que $A^{-1}B = BA^{-1} = I_n$.

   Daí, $A^{-1}A = BA^{-1} \Rightarrow AA^{-1}A = BA^{-1}A \Rightarrow I_nA = BI_n \Rightarrow A = B.$ Portanto, $\left(A^{-1}\right)^{-1} = A.$

II. Sejam A e B matrizes quadradas invertíveis de ordem n, então existem A^{-1} e B^{-1}, tal que $AA^{-1} = A^{-1}A = I_n$ e $BB^{-1} = B^{-1}B = I_n$. Da igualdade

   $BB^{-1} = I_n \Rightarrow BB^{-1}A^{-1} = I_nA^{-1} \Rightarrow ABB^{-1}A^{-1} = AA^{-1} \Rightarrow \left(AB\right)B^{-1}A^{-1} = I_n$, logo a matriz $\left(AB\right)^{-1} = A^{-1}B^{-1}$.

Quando se estuda matrizes invertíveis, geralmente se questionam os métodos de definir quando uma matriz pode ser considerada invertível e os métodos que aperfeiçoam os cálculos dessas inversas. Este problema será tratado nas próximas seções por meio do uso do determinante. Para os leitores que desejam aprofundar e conhecer outros métodos, fica a sugestão das obras citadas durante o texto.

2.5.2 Determinantes

A definição de determinantes apresentada neste trabalhado é baseado nas definições encontradas em Kolman e Hill (2006), Anton e Rorres (2001) e Boldrini e

Figueiredo (1980), que usam a ideia das permutações, para apresentar uma definição geral. Sendo assim, inicialmente será brevemente tratado das permutações.

Definição: Dado um conjunto $A \neq \varnothing$ finito, tal que $A = \{1, 2, 3, \cdots, \mathrm{n}\}$, uma reordenação de $j_1, j_2, j_3, \cdots, j_n$ dos elementos de A é chamada permutação de A.

Isso corresponde a uma função bijetora $f : A \to A$, que associa a cada elemento de A, um elemento do próprio conjunto A. Por exemplo, considerando o conjunto $A = \{1, 2, 3\}$, então 213 é uma permutação de A, tal que

$$f(1) = 2$$
$$f(2) = 1$$
$$f(3) = 3$$

Seja $A_3 = \{(1,2,3); (1,3,2); (3,1,2); (3,2,1); (2,3,1); (2,1,3)\}$, o conjunto das permutações de A, o seu número de elementos é definido, observando que, em uma permutação o elemento 1 do domínio de f, pode ser associado 1 dos n elementos, logo existem n possibilidades para $f(1)$, como a função é bijetora, ao definir a imagem de $f(1)$, a imagem de $f(2)$ pode ser definida escolhendo um dos $n-1$ elementos restantes, da mesma forma, $f(3)$ pode ser escolhido entre $n-2$ elementos, sucessivamente restando apenas uma possibilidade para $f(n)$.

Logo, existem $n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1$ permutações de A. Veja que para o conjunto A com três elementos, o conjunto das permutações será composto por $3 \cdot 2 \cdot 1 = 6$ elementos, ou seja, $n(A_3) = 6$. De modo geral, $n(\mathrm{A}_n) = n!$.

No entanto, é importante observar que uma permutação $j_1, j_2, j_3, \cdots, j_n$ de A, tem uma inversão se um inteiro j_n precede um inteiro menor j_{n-1}. Assim, uma permutação chamada de par ou ímpar de acordo com o número total de inversões, caso tenha um número par de inversões a permutação é chamada de permutação par, caso contrário, diz-se permutação impar. Observe a tabela 7 com as permutações do conjunto A_3.

Tabela 7: Número de inversões em uma permutação.

PERMUTAÇÕES	NÚMERO DE INVERSÕES
(1,2,3)	0
(1,3,2)	1

(2,1,3)	1
(3,1,2)	2
(2,3,1)	2
(3,2,1)	3

Fonte: Próprio autor.

Observe que a permutação 132 tem apenas uma inversão o 3 antes do 2, já a permutação 312 tem a inversão 3 antes do 1 e 3 antes do 2, logo são duas inversões. Neste caso, a permutação 132 é impar e a 312 é par.

A partir deste momento é possível definir o determinante de uma matriz B.

Definição: Seja a matriz $B=[\mathrm{b}_{ij}]$ de ordem n, diz-se determinante de B denotado por $\det(B)$ um número real tal que,

$$\det(B)=\sum_{p}(-1)^{j}b_{1j_1}b_{2j_2}\ldots b_{nj_n}$$

onde, j é o número de inversões da permutação $(j_1, j_2,\ldots, j_n)$ e p indica que a soma é estendida a todas as $n!$ permutações.

Note que, se o número de inversões de uma permutação for ímpar o sinal do coeficiente do somatório será negativo, caso contrário será par. Por exemplo, seja a matriz

III. $$A=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Daí, $\det(\mathrm{A})=a_{11}a_{22}a_{33}-a_{11}a_{21}a_{33}-a_{12}a_{21}a_{31}+a_{12}a_{23}a_{31}+a_{13}a_{21}a_{32}-a_{13}a_{22}a_{31}$.

Por exemplo, seja a matriz A, definhada por

$$A=\begin{bmatrix} 3 & 2 & 5 \\ 1 & 3 & 3 \\ 0 & -2 & -3 \end{bmatrix}$$

O seu determinante pode ser calculado como acima, fazendo

$$\det(\mathrm{A})=3\cdot3\cdot(-3)-3\cdot1\cdot(-3)-2\cdot1\cdot0+2\cdot3\cdot0+5\cdot1\cdot(-2)-5\cdot3\cdot0$$
$$\det(\mathrm{A})=-27+9-10$$
$$\det(A)=-28$$

Observe que em cada termo do somatório existe um e apenas um elemento de cada linha, bem como um e apenas um elemento de cada coluna da matriz. Esta

observação permite demonstrar a primeira propriedade dos determinantes que serão discutidos a seguir.

Teorema 2.4 Se todos os elementos de uma linha (coluna) de uma matriz A são nulos, $\det(\mathrm{A}) = 0$.

Demonstração:

Basta observa a firmação anterior, uma vez que, uma linha ou coluna seja nula, em cada parcela do somatório do determinante possui pelo menos uma das entradas desta linha (coluna), ao realizar o produto, todas as parcelas serão nulas. Portanto $\det(A) = 0$.

Teorema 2.5 O determinante de uma matriz e sua transposta são iguais, isto é, $\det(\mathrm{A}) = \det(\mathrm{A}^t)$.

Demonstração:

Seja a matriz $A = [a_{ij}]$ e a matriz $B = [b_{ij}]$, tal que $B = A^t$ o que implica afirmar $a_{ij} = b_{ij}$. Pela definição de determinantes tem-se

$$\det(\mathrm{A}) = \sum_p (-1)^j a_{1j_1} a_{2j_2} \ldots a_{nj_n} \Leftrightarrow \det(A) = \sum_p (-1)^j b_{1j_1} b_{2j_2} \ldots b_{nj_n} \Leftrightarrow \det(A) = \det(B).$$

Teorema 2.6 Se B é obtida de A pela multiplicação de uma linha (coluna) de A por uma constante k, então $\det(B) = k \det(A)$.

Demonstração:

Seja a matriz,

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

ao multiplicar uma linha por uma constante real k, tem-se

$$B = \begin{bmatrix} ka_{11} & ka_{12} & \cdots & ka_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

O determinante de A é igual a,

$$\det(\mathrm{B}) = \sum_{p} (-1)^{j} k a_{1j_1} a_{2j_2} \ldots a_{nj_n} \Rightarrow \det(\mathrm{B}) = k \sum_{p} (-1)^{j} a_{1j_1} a_{2j_2} \ldots a_{nj_n} \Rightarrow \det(\mathrm{B}) = k \det(A)$$

Teorema 2.6 Se uma matriz B é obtida da matriz A trocando-se de posição duas linhas (colunas) de A, então $\det(B) = -\det(A)$.

Demonstração

Dado a matriz B obtida da matriz A trocando-se a posição de duas linhas, suponhas $1 \le r < s \le i,$ com $i = 1,2,3,4,...,n$, tem-se que as entradas da linha r da matriz A são as entradas da linha s na matriz B, ou seja, $a_{rj} = b_{sj}$, o mesmo ocorre com $a_{sj} = b_{rj}$. Aplicando o determinante na matriz B, obtêm-se $\det(B) = \sum_{p} (-1)^{j} b_{1j_1} b_{2j_2} \ldots b_{rj_r} \ldots b_{sj_s} \ldots b_{nj_n}$, isso implica que $\det(\mathrm{B}) = \sum_{p} (-1)^{j} a_{1j_1} a_{2j_2} \ldots a_{sj_s} \ldots a_{rj_r} \ldots a_{nj_n}$. Note que, se a permutação $(j_1, j_2, \ldots, j_r, \ldots, \mathrm{j}_s, \ldots, j_n)$ possuir n inversões, a permutação $(j_1, j_2, \ldots, j_s, \ldots, \mathrm{j}_r, \ldots, j_n)$ possui $n+1$ inversões, assim as parcelas do somatório do determinante de B, possui sinais trocados, logo $\det(B) = -\det(A)$.

Supondo que B seja obtido de A, por meio da troca de colunas, então B^t é obtido da A^t. Pelo que foi concluído anteriormente, $\det(B^t) = -\det(A^t)$, pelo teorema 3.2, $\det(B) = -\det(A)$.

Teorema 2.7 O determinante de uma matriz que tem duas linhas (colunas) iguais, é igual a zero, ou seja, $\det(A) = 0$.

Demonstração

Supondo que na matriz A as linhas r e s sejam iguais e B é obtido de A pela troca de posição das linhas r e s. Pelo teorema 3.4 $\det(B) = -\det(A)$. Por outro lado, $B = A$, logo $\det(B) = \det(A) \Rightarrow \det(\mathrm{A}) = -\det(\mathrm{A})$, isso só é possível se $\det(A) = 0$.

Na definição de determinantes, foi visto que para determinar o $\det(A)$, tal que A é uma matriz de ordem n, realizava-se o processo a seguir,

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Logo, $\det(\mathrm{A}) = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}$, veja que pode-se reescrever como,

$$\det(\mathrm{A}) = a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}),$$

veja que na primeira parcela aparece o determinante da matriz formada pelas entradas da matriz A, excluindo a linhas 1 e coluna 1, ou seja,

$$A_{11} = \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix} \Rightarrow \det(A_{11}) = a_{22}a_{33} - a_{32}a_{23}$$

Daí, $\det(\mathrm{A}) = a_{11}\det(A_{11}) - a_{12}\det(A_{12}) + a_{13}\det(A_{13})$. Este método de calcular determinantes é conhecido como Teorema de Laplace, cuja demonstração pode ser consultada em Hefez e Fernandez (2012). A demonstração apresentada por Laplace foi publicado em 1772, no mesmo volume onde se encontra a publicação de Vandermonde sobre os determinantes (SANTOS, 2007).

Observe que em cada parcela do $\det(A)$, a linha 1 da matriz A sempre é excluída, alternando a retirada das colunas. De modo geral, considerando que sempre se retire a linha i, o determinante de uma matriz A de ordem n, pode ser calculado aplicando

$$\det(A) = a_{i1}(-1)^{i+1}A_{i1} + a_{i2}(-1)^{i+2}A_{i2} + \cdots + a_{ij}(-1)^{i+j}A_{ij}$$

Exemplo 3.1

Seja a matriz

$$A = \begin{bmatrix} 3 & -1 & 2 \\ 4 & 5 & 6 \\ 7 & 1 & 2 \end{bmatrix}$$

Logo, $\det(A) = 3(-1)^{1+1}(5\cdot 2 - 1\cdot 6) + (-1)(-1)^{1+2}(4\cdot 2 - 7\cdot 6) + 2(-1)^{1+3}(4\cdot 1 - 7\cdot 5)$, o que implica $\det(\mathrm{A}) = 3\cdot 4 - 1\cdot(-34) - 2\cdot(-31) = 108$, como o determinante é diferente de zero, é possível afirmar que esta matriz é invertível.

Seja $\Delta_{ij} = (-1)^{i+j}A_{ij}$ diz-se que Δ_{ij} é cofator da matriz A de ordem n. Além disso, com estes cofatores é possível formar uma nova matriz $\overline{A}$, chamada matriz dos cofatores de A. Logo, a matriz dos cofatores da matriz do exemplo 3.1 é:

$$\overline{A} = \begin{bmatrix} 4 & -34 & -31 \\ 4 & -8 & -10 \\ -16 & -10 & 11 \end{bmatrix}$$

Veja que as entradas e os cofatores multiplicados no cálculo do determinante são da mesma linha. O que se pode afirmar se as entradas e cofatores fossem de

linhas diferentes? Considere uma matriz B, encontrada de A, tal que a linha 1 e linha 3 sejam iguais, ou seja,

$$B=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{(n-1)1} & a_{(n-1)2} & \cdots & a_{(n-1)n} \\ a_{11} & a_{12} & \cdots & a_{1n} \end{bmatrix}$$

Sejam $\Delta'_{n1},\Delta'_{n2},\cdots,\Delta'_{nn}$ os cofatores da n-ésima linha da matriz B, além disso as $n-1$ linhas das matrizes A e B são iguais. Note que, para obter os cofatores da n-ésima linhas das matrizes A e B, utiliza-se apenas as entradas as $n-1$ linhas. Logos os cofatores de A e B da n-ésima linhas são iguais, ou seja, $\Delta'_{n1}=\Delta_{n1},\Delta'_{n2}=\Delta_{n2},\cdots,\Delta'_{nn}=\Delta_{nn}$.

Por outro lado, a matriz B tem duas linhas idênticas, pelo teorema 2.7 $\det(B)=0$, além disso, os cofatores da linha 1 e linha n são iguais, logo encontrando o determinante pela extensão dos cofatores ao longo da primeira linha, tem-se

$$\det(B)=a_{11}\Delta_{n1}+a_{12}\Delta_{n2}+\cdots+a_{1n}\Delta_{nn}=0\Rightarrow$$

$$a_{11}\Delta_{n1}+a_{12}\Delta_{n2}+\cdots+a_{1n}\Delta_{nn}=0$$

Logo, o determinante sempre seria nulo. Portanto, este resultado mostra a importância da atenção quanto a escolha das entradas e dos cofatores.

Definição: Dada uma matriz quadrada A, diz-se matriz adjunta de A à transposta da matriz dos cofatores de A, ou seja, $adjA=\bar{A}^t$.

Exemplo 3.2: Seja A uma matriz quadrada de ordem 2, encontre a matriz adjunta de A.

Solução: Seja a matriz A de ordem 2, definida por

$A=\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, a matriz dos cofatores serão definidos por $\bar{A}=\begin{bmatrix} \Delta_{11} & \Delta_{12} \\ \Delta_{21} & \Delta_{22} \end{bmatrix}$ tal que, $\Delta_{11}=(-1)^2\det(A_{11})$ veja que $A_{11}=[a_{11}]$ uma matriz de ordem $n=1$, o determinante de uma matriz unitária é sempre o próprio elemento que a compõe, ou seja, $\det(A_{11})=a_{11}$. Logo os demais cofatores serão, $\Delta_{11}=a_{11}$, $\Delta_{12}=-a_{12}$, $\Delta_{21}=-a_{21}$ e $\Delta_{22}=a_{22}$, assim

$$\bar{A}=\begin{bmatrix} a_{11} & -a_{12} \\ -a_{21} & a_{22} \end{bmatrix}\Rightarrow \bar{A}^t=\begin{bmatrix} a_{11} & -a_{21} \\ -a_{12} & a_{22} \end{bmatrix}=adjA$$

Este exemplo, mostra um método prático de encontrar a matriz adjunta de uma matriz de ordem 2, por exemplo se a matriz for definida pelos elementos

$$A=\begin{bmatrix}2 & 5\\ 4 & 3\end{bmatrix}$$

Pelo exemplo 3.2, a matriz inversa adjunta de A será,

$$adjA=\begin{bmatrix}2 & -4\\ -5 & 3\end{bmatrix}$$

Para concluir objetivo deste capítulo, observe que se A é uma matriz quadrada invertível, então sua inversa existe tal que $A^{-1}A=AA^{-1}=I_n$. Aplicando o determinante tem-se que $\det(A\cdot A^{-1})=\det(A)\cdot\det(A^{-1})\Rightarrow \det(\mathrm{I}_m)=\det(A)\cdot\det(A^{-1})$, logo $\det(A)\cdot\det(A^{-1})=1$, deste modo, conclui-se que se A tem inversa então $\det(A)\neq 0$ o que implica $\det(A^{-1})=\dfrac{1}{\det A}$.

O teorema a seguir, apresenta como encontrar a matriz inversa, por meio da matriz adjunta.

Teorema 2.8 Se A é uma matriz invertível, então

$$A^{-1}=\frac{1}{\det A}adj\left(A\right)$$

Demonstração:

Primeiro é necessário chegar a conclusão de que $A\cdot adj\left(A\right)=\det\left(A\right)\cdot I_n$. Considere o produto

$$A\cdot adj\left(A\right)=\begin{bmatrix}a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & \cdots & \vdots\\ a_{i1} & a_{i2} & \cdots & a_{in}\\ \vdots & \vdots & \cdots & \vdots\\ a_{11} & a_{12} & \cdots & a_{1n}\end{bmatrix}\cdot\begin{bmatrix}\Delta_{11} & \cdots & \Delta_{1j} & \cdots & \Delta_{1n}\\ \Delta_{21} & \cdots & \Delta_{2j} & \cdots & \Delta_{2n}\\ \vdots & \cdots & \vdots & \cdots & \vdots\\ \Delta_{n1} & \cdots & \Delta_{nj} & \cdots & \Delta_{nn}\end{bmatrix}$$

Desta forma a entrada da primeira linha e primeira coluna é defina pelo valor do somatório $a_{11}\Delta_{11}+a_{12}\Delta_{21}+\cdots+a_{1n}\Delta_{n1}$. Como já foi visto, expansão de entradas e cofatores de linhas diferentes é igual a zero, logo $\det\left(A\right)=a_{11}\Delta_{11}+a_{12}\Delta_{21}+\cdots+a_{1n}\Delta_{n1}=a_{11}\Delta_{11}+0$, o que implica afirmar $\det\left(A\right)=a_{11}\Delta_{11}$.

Veja que a entrada da i-ésima linha e j-ésima coluna do produto $A \cdot adj(A)$ é definido pelo valor $a_{i1}\Delta_{1j} + a_{i2}\Delta_{2j} + \cdots + a_{in}\Delta_{nj}$, na qual se pode concluir que para o caso $i = j$, tem-se $\det(A) = a_{ii}\Delta_{ii}$, o que caracteriza as entradas da diagonal principal da matriz $A \cdot adj(A)$. Portanto,

$$A \cdot adj(A) = \begin{bmatrix} \det(A) & 0 & 0 & 0 \\ 0 & \det(A) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \det(A) \end{bmatrix} = \det(A) \cdot \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

Logo, $A \cdot adj(A) = \det(A) \cdot I_n$. Como A é invertível pode-se afirmar que $\det(A) \neq 0$, Daí, multiplicando a igualdade pela inversa de A, tem-se $A \cdot A^{-1} \cdot adj(A) = \det(A) \cdot I_n \cdot A^{-1} \Rightarrow adj(A) = \det(A) \cdot A^{-1} \Rightarrow A^{-1} = \frac{1}{\det(A)} \cdot adj(A)$.

O estudo de determinantes é algo bastante importante no estudo da álgebra linear, de tal forma, que os autores das referencias citadas dedicaram um capítulo de sua obra especialmente para este estudo. No entanto, não se considera necessário fazer o mesmo neste trabalho, uma vez que, os conceitos discorridos neste capítulo são suficientes para o acompanhamento nas atividades propostas. Para além, o que foi abordado, fica como sugestão as referências citadas durante o texto.

CAPÍTULO 3.

PROCEDIMENTOS METODOLOGICOS

3.1 MOTIVAÇÃO

A prática docente em matemática na educação básica, bem como a participação em eventos com a finalidade de refletir a prática pedagógica e os desafios encontrados na socialização do conhecimento na área de exatas são fatores que impulsionaram os estudos deste trabalho.

A experiência que apresenta mais influência nesta pesquisa é a vivenciada no projeto Descobrindo Talentos em Matemática (DTM), do Núcleo de Pesquisa e Ensino em Matemática (NUPEMAT/UNIVASF) da Universidade Federal do Vale do São Francisco (Univasf).

O projeto DTM com o objetivo de descobrir talentos em matemática possui uma metodologia fundamentada nas resoluções de problemas presentes em provas de olímpiadas de matemática de anos anteriores, além de oficinas ofertadas nos meses finais de cada ano, com atividades distintas e principal objetivo de promover uma matemática divertida. As experiências são socializadas em eventos voltados para o ensino da matemática, bem como a publicação de artigos.

As aulas são ofertadas por professores da educação básica e superior e estudantes de graduação e pós-graduação. É um projeto que valoriza as capacidades cognitivas dos sujeitos envolvidos (docentes e discentes), onde a prática pedagógica é realizada com o desenvolvimento de pesquisas que possibilitam a recriação de conhecimentos e inovação dos processos pedagógicos.

No DTM os problemas a serem trabalhados em sala de aula, são divididos em aritmética, geometria e contagem, sendo assim cada sábado são dedicadas a um desses três ramos da matemática, sendo repetidos periodicamente, por exemplo, aritmética é trabalhada a cada três sábados.

As indagações que motivaram esta pesquisa manifestaram-se em uma dessas aulas, em que se trabalhavam questões com o objetivo de identificar padrões na matemática, aplicando-se conceitos de sequências de números, em particular aritmética modular. A cada questão trabalhada, identificava-se o quanto esse tipo de problema era novo para o estudante.

Naquele momento os estudantes figurava indicar estar em um mesmo nível cognitivo, quanto às habilidades em analisar padrões nos números, por outro lado, se trata de uma turma multiseriada com estudantes oriundos de distintas escolas públicas, desde as que apresentam bons resultados em provas externas, até as que apresentam menor rendimento nas avaliações.

Está experiência gerou várias indagações, sobre como esses conteúdos são abordados nos livros didáticos? Que tipo de formação o professor recebe para lidar com estes conteúdos? Quais os desafios encontrados pelos sujeitos (docente e discente) ao se deparar com problemas deste tipo? Porém, são questionamentos que demanda um longo tempo de pesquisa, desta forma, este trabalho se limitou em tentar analisar de que forma estes conteúdos estão presentes em sala de aula, para desta observação, analisar a viabilidade de uma abordagem que auxilia os professores da educação básica a socializarem os conceitos presentes neste tipo de problema.

Em conversas com orientador desta pesquisa, o mesmo levantou como sugestão analisar uma forma de abordar estes conceitos evitando uma prática pedagógica meramente discursiva, mas que seja utilizada com significado, onde o estudante possa aplicar o conhecimento que está sendo produzido, concluindo que, possivelmente uma forma divertida seria usando nas criptografias primitivas.

Em pesquisas já publicadas, como a dissertação produzida por Jesus (2013), apresenta-se uma proposta de implementação de uma sequência didática para o desenvolvimento do tema criptografia aliado aos conteúdos de matrizes para turmas do ensino médio com aplicação na prática. Para isso, o autor ressalta que a motivação da pesquisa foi gerada por notar que os livros didáticos não apresentavam uma sequência lógica da organização dos conteúdos aplicados ao contexto do aluno.

Por outro lado, a dissertação de Carvalho (2016) investiga como abordar os conteúdos das teorias dos números e da álgebra, por meio da aplicação na criptografia, no entanto, está proposta faz uso de uma troca de conversas criptografadas por meio do *Whatsap* e construção de dispositivos de encriptação e decriptação com copos descartáveis.

Após as análises de trabalhos já publicados, para tornar o estudo da matemática mais divertido, observa-se, o que torna esta pesquisa diferente das demais é a ideia de analisar a possibilidade de esta abordagem ser aplicada dentro

de um jogo dinâmico, que simule a aplicação direta da criptografia em agências secretas, onde manter informações criptografadas é o segredo para vencer o jogo.

Portanto, fundamentadas nas ideias de Prodanov e Freitas (2013) esta é uma pesquisa de natureza aplicada, um a vez que, o autor define este tipo de pesquisa, como a que visa produzir conhecimentos a serem aplicados na prática, com foco na solução de problemas específicos.

3.2 METODOLOGIA: ESTUDO DE CASO

O delineamento deste processo metodológico caracteriza esta pesquisa de natureza aplicada, que dos pontos de vista dos objetivos geral e específicos se fundamenta como pesquisa explicativa.

Andrade (2010) salienta que esse tipo de pesquisa além de “registrar, analisar e interpretar os fenômenos estudados procura identificar seus fatores determinantes, ou seja, suas causas”, o que evidencia o objetivo geral deste trabalho, delimitado em analisar a viabilidade do uso do jogo Caça ao Tesouro como uma ferramenta de auxilio na socialização de conhecimentos aritméticos e algébricos aplicados à criptografia primitiva.

A pesquisa será fundamenta pelo método indutivo, já que o objetivo geral visa alcançar um resultado generalizado por meio da observação de um grupo específico de sujeitos. Desta forma, por meio de uma análise de fenômenos em um pequeno grupo, conclusões foram inferidas a um público mais amplo (LAKATOS, MARCONI, 2003).

Para alcançar o objetivo geral, foram traçados como objetivos específicos: Investigar a matemática elementar presente nas criptografias primitivas; viabilizar uma proposta de abordagem de alguns conteúdos de aritmética modular e matrizes, aplicado a criptografia; desenvolver e implementar um jogo capaz de trabalhar os conceitos de aritmética e matrizes de forma divertida.

O procedimento adotado para alcançar os objetivos específicos é o estudo de caso, por se tratar de uma investigação de um caso específico, bem delimitado dentro do contexto da realidade atual, em uma busca detalhada de informações (GIL, 2008). Por outro lado, Ventura (2007) salienta que este tipo de pesquisa é aplicado quando se deseja investigar casos com uma variedade de fatores e relacionamentos que podem ser diretamente observados, mas sem estratégias para

definir quais são importantes, se caracterizando assim, um processo empírico onde é importante contato direto do pesquisador com os sujeitos a serem observados.

Quanto às etapas da pesquisa, Gil (1995, apud, VENTURA, p.385, 2007) destaca que “o estudo de caso, não aceita um roteiro rígido para a sua delimitação, mas é possível definir quatro fases que mostram o seu delineamento”, logo, o processo sistemático adotado neste procedimento foi sustentado nas quatro etapas sugeridas pelo autor: 1) delimitação do caso; 2) coleta de dados; 3) seleção, análise e interpretação dos dados; 4) elaboração do relatório.

Para delimitar o caso a ser estudado, fez uso da pesquisa bibliográfica de fontes secundárias, como artigos, monografias, dissertações e teses publicadas em periódicos, e livros (ANDRADE, 2010).

Nesta etapa da pesquisa, a análise bibliográfica foi realizada com objetivo de levantar dados em relação à matemática presente nos processos de criptografias primitivas, bem como conhecer o seu desenvolvimento histórico. Os dados levantados permitiram estabelecer os conteúdos de matemática a ser observado e estudado, para isso, o primeiro passo foi identificar de que forma estão presentes no livro-texto utilizado nas escolas, Paramentos Curriculares Nacionais (PCN) e matriz curricular do estado do Pernambuco.

Durante a análise desses dados, definiram-se os procedimentos para coleta de dados. A coleta dos dados foi realizada durante as aulas da oficina de criptografia aplicada no projeto DTM, durante os sábados, com aulas ministradas em um tempo de duração de três horas, por um período de dois meses. Os meses de aplicação foram novembro de 2016 e fevereiro de 2017, períodos de termino e início dos anos letivos, o que desfavoreceu a coleta de dados ser realizada no ambiente escolar dos estudantes.

O minicurso de criptografia ministrado em uma sala de aula da Univasf campus Petrolina, teve como sujeitos de pesquisa 45 estudantes de uma escola pública da Gerencia Regional de Educação de Petrolina no estado de Pernambuco. A turma tinha uma característica multiseriada, uma vez que, era composto por alunos do 6º ao 9º ano do ensino fundamental.

A sequência didática do curso é realizada em três etapas, inicia por uma discussão sobre a história da criptografia e a sua influência nos dias atuais. Esta aula foi importante para atrair o interesse do estudante em participar do curso, caso contrário, a evasão poderia prejudicar a coleta dos dados, uma vez que, demandaria

mais tempo para a realização da pesquisa, ao se pensar em buscar outros meios de coleta de dados.

A segunda etapa consiste na socialização dos processos de criptografar, discutindo simultaneamente os conceitos de aritmética modular e álgebra linear presente nas criptografias. A terceira etapa se caracteriza pela aplicação do jogo Caça ao Tesouro.

Em cada etapa a coleta de dados foi por meio da documentação direta extensiva com a aplicação de questionários auto aplicados e intensiva por meio da observação participante assistemática. Segundo Prodanov e Freitas (2013) a observação participante ocorre quando o observador se torna um membro do grupo observado, no caso desta pesquisa, o observador que assume o papel de professor, participa da situação, mantendo o máximo de cuidado para não interferir na qualidade dos dados, deixando que os sujeitos realizem suas atividades de forma independente.

Por outro lado, não foi elaborado um plano de observação, desta forma se caracteriza por assistemática. No entanto, os dados coletados simultaneamente com a observação assistemática, foram levantados por meio da aplicação de questionários propostos por escrito, ou seja, auto aplicados composto por questões fechadas e abertas. Além dos questionários e da observação, coletou por meio de imagens fotográficas as soluções a questões sobre o conteúdo de matemática trabalhado no dia da aula.

Além da coleta de dados no ambiente de pesquisa, aplicaram-se questionários aos professores de matemática das escolas que participam do DTM, com o objetivo de levantar dados possíveis de obter uma descrição desse público, para uma análise que permita levantar conclusões que justifiquem o comportamento de fenômenos registrados durante a aplicação do curso.

Seguindo esta perspectiva, permite afirmar que esta pesquisa faz uso de duas abordagens, a qualitativa e quantitativa. Ventura (2007) salienta que no estudo de caso, é frequente a descrição qualitativa, no entanto, existem pesquisas que podem realizar um estudo de caso com abordagem qualitativa e quantitativa.

Além disso, Prodanov e Freitas (2013) afirma que na abordagem qualitativa os dados são utilizados no direcionamento de coleta, análise e interpretação de dados, que no caso desta pesquisa, foi coletado por meio da observação assistemática, que ao adotar a descrição quantitativa dos dados por meio da

aplicação de questionários, contribui em uma melhor qualidade dos dados, permitindo uma análise comparativa de dados qualitativos e quantitativos.

A análise dos dados foi realizada de forma sistematizada fundamentado nas ideias de Prodanov e Freitas (2013), Gil (2008) e Lakatos, Marconi (2003) por meio das evidências observadas de acordo com a metodologia, além de relações feitas entre o referencial teórico e os dados coletados.

A análise consiste em três processos definidos pelos autores: A seleção dos dados, para identificar os dados que serão úteis; Codificação dos dados, que neste caso são separados por assunto abordado, pela data de coleta, e a série/ano do sujeito, dentro de cada grupo, haverá dois subconjuntos de dados, os qualitativos e quantitativos; Tabulação e interpretação dos dados na qual foram dispostos em tabelas e gráficos, para serem confrontados e analisados, para em seguida apresentar seus resultados e conclusões por meio de um texto cientifico, que neste caso, é o capítulo 4 desta obra.

CAPÍTULO 4.

DISCUSSÕES DOS RESULTADOS

As discussões acerca da educação e a ratificação da importância dela na Constituição Federal de 1988 colocaram a necessidade da universalização da educação básica em evidência. A partir desse marco legal, havia a necessidade de reformulação na Lei de Diretrizes e Bases da Educação Nacional, culminada com a aprovação da Lei 9.394 de 20 de dezembro de 1996. Nela, a oferta do ensino fundamental passa a ser de responsabilidade prioritária dos municípios, entretanto, estes terão apoio do estado e da União (BRASIL, 1996).

Desta forma, durante o século XX maior parte da população teve acesso ao ensino fundamental, impulsionado pela oferta do ensino gratuito junto com a obrigatoriedade da matricula de crianças a partir dos seis anos (BRASIL, 2013).

Durante este período, como resultado de discussões realizadas em fóruns, simpósios e congressos, alguns documentos foram elaborados com o objetivo de nortear a educação básica. Entre estes documentos, podem ser citadas a Lei de Diretrizes e Bases da Educação Nacional, de 20 de dezembro de 1996 – LDB 9394/96 (BRASIL, 1996) e as Diretrizes Curriculares Nacionais para a Educação Básica – DCNEB (BRASIL, 2013), que definem o ensino fundamental como a etapa mais longa da educação básica, com uma duração de nove anos, atendendo crianças e adolescentes entre seis e 14 anos, tendo como o objetivo a formação básica dos cidadãos.

Para tanto, o ensino fundamental é dividido em duas fases, os anos iniciais compostos pelas turmas do 1º ao 5º ano e os anos finais compostos pelas turmas do 6º ao 9º ano, a transição entre as fases merece uma atenção especial, uma vez que, o estudante sai de um ambiente que possui um professor com atendimento generalizado e passa para um ambiente com professores especialistas por área, desta forma, a Base Nacional Curricular Comum (BNCC) enfatiza a importância das abordagens dos conteúdos levar em consideração esta transição, caso contrário haverá uma desconexão no processo de aprendizagem do estudante (BRASIL, 2017).

Além disso, os anos finais é uma consolidação dos conceitos adquiridos nos anos iniciais e uma preparação para o ingresso no ensino médio, etapa final da educação básica. Desta forma, os conteúdos nesta etapa são abordados de forma

mais abrangente, na qual não basta apenas saber o processo das quatro operações, mas por meio delas, descrever fenômenos e observar sequências e eventos.

Considerando que o processo de aprendizagem é continua, acredita-se que a cada etapa o estudante possui estrutura cognitiva mais complexa referente à anterior. Por outro lado, quando se observa os dados referentes ao Índice de Desenvolvimento da Educação Básica (IDEB) do Brasil em quase uma década, a cada etapa da educação básica os dados são sempre menores, sendo em 2015 o ano com maior diferença. De outro ponto de vista, às metas previstas para cada etapa, foram todas atingidas.

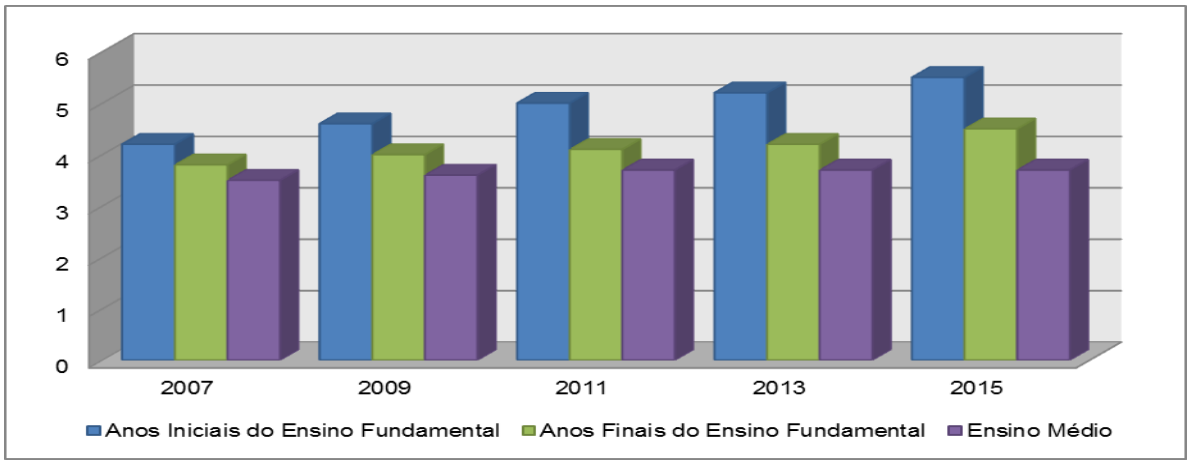


Gráfico 1: Resultados do IDEB da educação básica no Brasil. 2007- 2015.
Fonte: Saeb e Censo Escolar.

Observando estes dados, permite inferir a possibilidade da transição de etapa ser um dos fatores que influenciam na queda destes dados. O cenário não é diferente quando se refere ao município de Petrolina no Estado do Pernambuco, como mostra do gráfico 2.

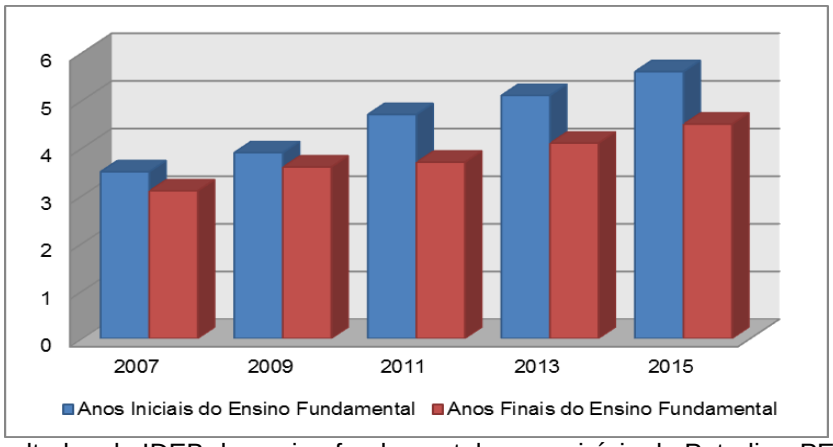


Gráfico 2: Resultados do IDEB do ensino fundamental no município de Petrolina-PE. 2007- 2015.
Fonte: Saeb e Censo Escolar.

Diante deste cenário e dos desafios encontrados na educação básica, discussões são geradas a fim de analisar, compreender e diagnosticar os possíveis motivos na queda destes dados para então, estabelecer metas e estratégias que possibilitem mudanças no ensino, atendendo os anseios da sociedade atual.

Com isso, tanto a rede municipal como a estadual, realiza formações continuadas com seus professores, além de utilizarem um sistema de avaliação externa, como uma ferramenta para diagnosticar problemas sanando-os antes das avaliações externas nacionais e internacionais serem aplicadas, acreditando assim, em uma mudança nos dados da educação básica.

A título de exemplo, existe o Sistema de Avaliação Educacional de Pernambuco (SAEPE), na qual realiza avaliações anuais em todo estado, descrevendo os níveis de aprendizagem dos estudantes, como uma forma de garantir o direito a educação.

A leitura dos dados é realizada com base em uma média de proficiência, calculada sobre os percentuais de desempenho apresentados em quatro níveis: Elementar I, composto por estudantes que apresentam características distantes da esperada em sua etapa de ensino, na qual não é capaz de realizar trabalhos em grupos; Elementar II, estudantes com aprendizagem inferior ao previsto, no entanto, são capazes de realizarem trabalhos em grupo; Básico, estudantes com desempenho mínimo, mas compatíveis ao esperado na sua etapa de ensino; Desejável, estudantes com características que se enquadram no desempenho considerado satisfatório na sua etapa de ensino (BRASIL, 2012).

De acordo com os dados do SAEPE (gráfico 3), mais de 50% dos estudantes do estado de Pernambuco nos anos finais do ensino fundamental, ainda não alcançaram as habilidades mínimas em matemática para esta etapa da educação básica. Veja que este percentual está distribuído entre os níveis elementar I e elementar II.

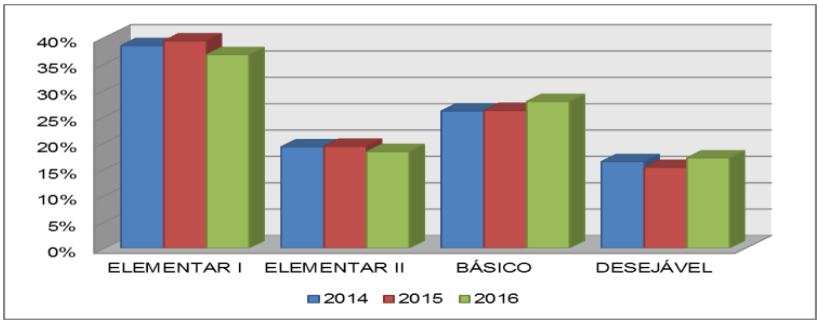


Gráfico 3: Resultados do SAEPE em matemática dos anos finais do ensino fundamental do estado de Pernambuco. (2014 – 2015).
Fonte: SAEPE, Secretaria de Educação do Estado de Pernambuco.

A secretaria de educação do Estado de Pernambuco realiza suas atividades em articulação com 16 Gerencias Regionais de Educação (GRE) distribuídas pelo estado. Entre elas a GRE Sertão do Médio São Francisco localizado em Petrolina-PE, é responsável por gerir as escolas de sete municípios que compõe o Sertão do São Francisco. Observando o gráfico 4, a GRE Sertão do Médio São Francisco apresenta dados mais satisfatórios em comparação aos dados do estado, uma vez que, o percentual dos estudantes que não atingiram as características mínimas esperadas em sua etapa de ensino, esta abaixo de 50%.

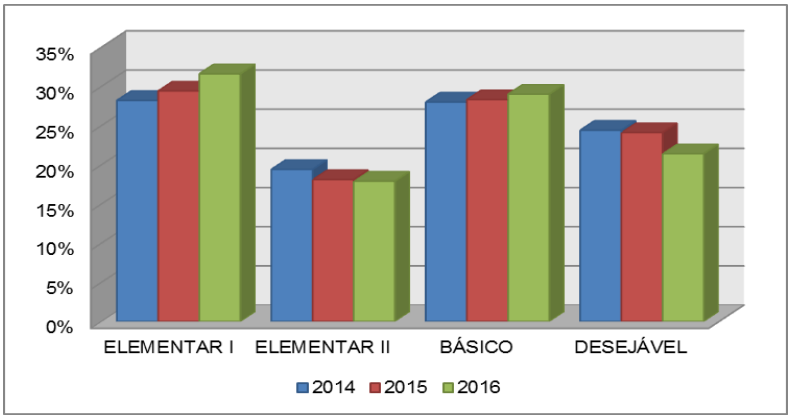


Gráfico 4: Resultados do SAEPE em matemática dos anos finais do ensino fundamental da GRE Sertão do Médio São Francisco (2014 – 2015).
Fonte: SAEPE, Secretaria de Educação do Estado de Pernambuco.

Mas, para realmente gerar resultados, não se resume apenas em aplicar avaliações e quantificar, outros fatores merecem ser analisados e discutidos, como por exemplo, as práticas pedagógicas e o currículo trabalhado em sala de aula capaz de atender as necessidades do público. Cada geração realiza o mesmo percurso realizado por gerações anteriores de forma modificada, adequada a suas necessidades atuais, desta forma, se torna imprescindível às discussões voltadas para uma prática e um currículo inovador (SANTOS, OLIVEIRA, PAZ, 2016).

A BNCC (2017) evidencia em sua proposta uma mudança no que diz respeito aos currículos de cada etapa da educação básica, por considerar ser necessário manter uma ponte de comunicação entre as etapas, defendendo a ideia da aprendizagem do estudante ser um processo contínuo, ameaçado pela a mudança grotesca no processo de ensino aprendizagem de uma etapa para outra.

Analisando esses dados e o ponto de vista da BNCC (2017), sustenta o fato de esta pesquisa direcionar seu foco para os anos finais do ensino fundamental, visto que, as contribuições deste trabalho poderão servir de ferramenta para professores

de matemática da educação básica, nos planejamentos de aulas que gerem uma aprendizagem significativa.

3.1 DESCRIÇÕES: SUJEITOS DA PESQUISA

De acordo com os dados do SAEPE (2016) fornecidos no site da Secretaria de Educação do Estado de Pernambuco, um percentual considerável de estudantes dos anos finais do ensino fundamental da GRE de Petrolina-PE, apresentam dificuldades em solucionar problemas com as quatro operações, além de situações que envolvam equações do 1º e 2º grau.

Os estudantes dos anos finais do ensino fundamental que participaram do projeto DTM em 2016 são oriundos de 25 escolas de Petrolina. Em análise aos dados destas escolas, é possível observar que no DTM a realidade não é diferente, em relação à GRE.

Os últimos dados do SAEPE mostram que das 25 escolas, 17 escolas retém mais de 40% dos estudantes abaixo das expectativas para os anos finais do ensino fundamental no ano de 2014. No ano seguinte o número de escolas nestas condições, reduziu para 13. Em 2016 este número volta a subir, sendo 16 escolas com mais de 40% dos estudantes abaixo das expectativas (SAEPE, 2016).

Esta estatística mostra que o público do DTM apresenta uma característica diversificada, composto por estudantes de escolas que enfrentam maiores dificuldades com o ensino da matemática e outras que apresentam melhores índices. Isto é, pelo quantitativo de escolas, dispõe uma amostra considerável de estudantes das escolas públicas do município de Petrolina.

No entanto, esta pesquisa analisou uma pequena parcela desta amostra, composta por 45 estudantes das escolas públicas de Petrolina que estão entre as 16 escolas que participam no DTM e apresentam um alto percentual de estudantes com dificuldades em aprender matemática. Logo, a turma não era composta por estudantes de altas habilidades em matemática, mas alunos com necessidades semelhantes às de turmas de escolas padrão.

Além dos dados do SAEPE, uma pesquisa de opinião, permitiu inferir a semelhança do perfil da turma ao de uma escola padrão. Para isso, o questionário (APÊNDICE B) foi aplicado a dois públicos, um formado pelos sujeitos da pesquisa e outro formado por estudantes de uma escola municipal de Petrolina que atende aos padrões das escolas do município. Desta forma, o confronto dos dados dos 45

sujeitos da pesquisa (Grupo A) com os dos 120 estudantes da escola municipal (Grupo B), permitiu analisar se existe uma divergência acentuada, entre o perfil da turma e o perfil desta escola.

Tabela 8: Resultado da pesquisa de opinião. Comparativo entre o grupo A e Grupo B.

Descrição das perguntas	GRUPO A	GRUPO B
Gosta de estudar matemática.	45% afirmaram gostar de estudar matemática.	30% afirmaram gostar de estudar matemática.
Existência de laboratório de Informática (LI) na escola.	87% afirmou que possui (LI)	90% afirmou que possui (LI)
Uso de laboratório de informática durante as aulas.	42% confirmou ter em algum momento aulas no LI.	80% confirmou ter em algum momento aulas no LI.
Disciplinas que utilizam o laboratório.	Geografia, artes e língua portuguesa.	Geografia, ciências e língua portuguesa.
Uso de jogos na sala de aula.	45% confirma o uso de jogos na sala de aula	67% confirma o uso de jogos na sala de aula
Jogos que exigem conhecimento matemático.	48% afirma que não conhece.	50% afirma que não conhece.
Uso de jogos	54% pratica algum tipo de jogo.	Mais de 90% pratica algum tipo de jogo.
Definição de Criptografia	Apenas 4% afirma conhecer, dos quais dois conseguem definir.	Apenas 1% afirma conhecer, mas não consegue descrever a definição.

Fonte: Próprio autor.

Note na tabela 8, que existe uma divergência pequena entre os percentuais, permitindo concluir que os dois grupos é composto por alunos em que maioria afirma não gostar de estudar matemática. Além disso, um bom percentual possui laboratório de informática, mas poucos professores realizam atividades com o uso desta tecnologia.

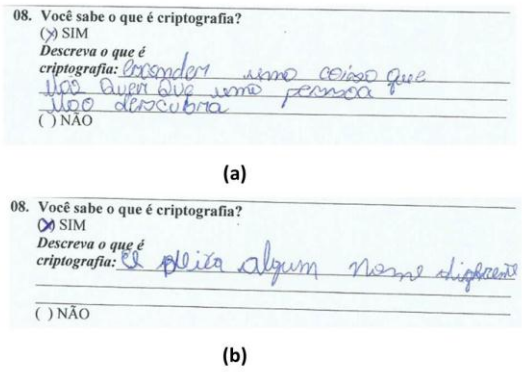


Figura 8: Resposta da pesquisa de opinião de dois sujeitos do grupo A. (a) aluno do 7º ano; (b) aluno do 8º ano.
Fonte: Próprio autor

Uma quantidade considerável nos dois grupos confirma o uso de jogos em sala de aula, em contrapartida, um bom percentual mencionou que esta atividade era realizada pelo professor de educação física, e metade salienta não conhecer jogos que envolvam conhecimentos de matemática. Quanto à definição de criptografia apenas dois estudantes apresentam uma definição, como mostra a figura 8.

Os dois estudantes demonstram em sua resposta, conhecer de forma superficial a definição de criptografia, uma vez que a criptografia é uma prática para esconder conteúdos secretos, e muitas vezes para isso, utilizam a técnica de modificar o conteúdo da mensagem para garantir uma melhor segurança da informação.

3.2 PROPOSTA PEDAGÓGICA DA PESQUISA.

Aprender matemática não é apenas acumular conteúdos, esse processo de aprendizagem vai muito mais além, o estudante deve ser estimulado a fazer matemática, a realizar descobertas de acordo com suas experiências, para isso são discutidos diversos caminhos que direcionem a este tipo de ensino, e a presente proposta didática é uma sugestão desta prática de ensino, onde o professor é mediador do conhecimento.

Para isso, o processo de aprendizagem desta proposta está fundamentado nos teóricos construtivistas Lev Vygotsky (MOREIRA, 2011, FINO, 2001) e David Ausubel (ARAGÃO, 1976; MOREIRA, 2010; COSTA, MOREIRA, 2001), uma vez que, as discussões serão pautadas na importância da estrutura cognitiva do estudante, bem como na interação durante a mediação do conhecimento. Tratam-se apenas dos pontos mais pertinentes à realidade desta pesquisa, acreditando que as teorias se complementam, ao identificar que para Vygotsky o foco é a interação social, enquanto que Ausubel focaliza o individuo como unidade de análise.

A teoria de Vygotsky parte da premissa de que o desenvolvimento cognitivo ocorre na interação social, para isso tem influência de instrumentos físicos como bola e abstratos como crenças e valores, bem como o domínio de signos, como a fala. Além disso, define o homem como um ser histórico na qual o seu desenvolvimento não depende unicamente de sua estrutura biológica, mas de uma interação social, que em termos históricos vai se evoluindo (FINO, 2001)

O que existe em comum entre as teorias é a consideração de que o estudante possui uma estrutura cognitiva pré-organizada, isto é, o educando, quando chega à escola, já possui algum tipo de inteligência. Assim, os teóricos argumentam a necessidade de identificar os conhecimentos prévios, para que se promova uma aprendizagem significativa.

A partir daí, Vygotsky define uma Zona de Desenvolvimento Proximal, como uma distância entre o desenvolvimento cognitivo real, indicado pelas habilidades e competências que o estudante é capaz de realizar sem a ajuda de uma adulto e o nível de desenvolvimento potencial, pontuado pelas habilidades realizadas com a ajuda e orientação de um adulto. Desta forma, está zona define as possíveis habilidades que o estudante será capaz de realizar após a interação com um ser de estrutura cognitiva mais desenvolvida (MOREIRA, 2011).

Na sala de aula, essa interação social foi gerada por meio do contato entre o pesquisador e os sujeitos, bem como em atividades propostas, onde os estudantes com habilidades já desenvolvidas interagiam com colegas que ainda estavam em desenvolvimento.

Por outro lado, para que o desenvolvimento ocorra é necessário que o educador gere esta zona de desenvolvimento proximal. Para isso, uma alternativa, foi à utilização de um organizador prévio que será discutido com mais detalhes na seção 3.2.

A preocupação desta pesquisa em gerar esta zona de desenvolvimento proximal, encontra mais respaldo em Fino (2001) e Moreira (2011) ao afirmarem que a aprendizagem é provocada dentro da zona de desenvolvimento proximal, por este motivo os autores levantam a importância de estabelecer os limites desta zona de desenvolvimento, definindo o inferior fixado pelo nível de desenvolvimento real e o superior pelas habilidades e competências que o estudante pode ser capaz de desenvolver por influência da interação.

Assim, esta pesquisa além de analisar a interação social durante a aplicação da proposta, busca-se em Ausubel fundamentar a aprendizagem como um caso particular de cada sujeito, pois compreendendo este processo o educador terá suporte para planejar aulas capazes de promover uma aprendizagem significativa.

David Ausubel (1968, apud MOREIRA, 2010) apresenta em sua teoria o termo aprendizagem significativa como algo ocorre quando novas informações são interiorizadas, por meio de uma espécie de ancoragem em conhecimentos prévios

relevantes na estrutura cognitiva, na qual o conhecimento já existente e o novo se modificam durante a interação, moldando uma estrutura cognitiva mais complexa.

Os conhecimentos prévios relevantes durante a interação das informações formam o subsunçor, isto é, o novo conhecimento deve se relacionar com os conhecimentos presente na estrutura cognitiva (ARAGÃO, 1976; COSTA, MOREIRA, 2001). Com esta definição, Ausubel (200, apud MOREIRA, 2010) entende que existem dois tipos de aprendizagem, a significativa indicada pela interação do novo conhecimento com o subsunçor e a mecânica indicada pela absorção do novo conhecimento sem interação com o subsunçor.

Na falta da interação com o subsunçor, ou seja, na aprendizagem mecânica não significa que o educando não aprendeu. O que ocorre é uma absorção de conhecimento sem significado para o estudante.

A interação do conhecimento pode ser realizada de três formas, a subordinada caracterizada pela absorção de informações com significados subordinados ao que o estudante já conhece, a supeordenada indicada pela informação que ao ser absorvida pode modificar a ordem de hierarquia das informações e a combinatória indicada pela combinação com informações prévias do estudante (ARAGÃO, 1976).

Veja alguns exemplos de cada interação. Subordinada: o estudante conhece os números naturais, e a nova informação é a definição de número par, veja que na estrutura cognitiva do estudante já está formada a ideia mais geral de número, agora ele conhecerá uma ideia particular que é a diferenciação entre os números par e ímpar.

Supeordenada: O estudante conhece a ideia de números naturais e agora vai conhecer outros tipos de números os inteiros, racionais, irracionais e reais, veja que na sua estrutura cognitiva os números naturais era uma informação hierarquicamente mais relevante, agora os números reais assume a posição antes ocupada pelos naturais. Veja o esquema representado na figura 9.

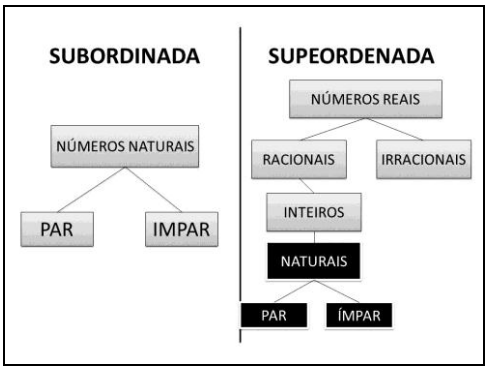


Figura 9: Esquema da estrutura cognitiva após a interação subordinada e supeordenada.
Fonte: Próprio autor

Combinatória: a criança conhece uma caixa de sapato, mas não conhece um paralelepípedo, desta forma o professor utiliza da caixa para combinar esta informação que estar estruturada no cognitivo, com as propriedades do paralelepípedo.

Outra diferença marcante entre a aprendizagem significativa e a mecânica é reforçada pela assimilação obliteradora, na qual o resultado final é o esquecimento, ou seja, mesmo que tenha estudado de forma significativa o conceito de números racionais e não aplicar em situações problemas o resultado será o esquecimento, no entanto, será de fácil reaprendizagem (MOREIRA, 2010; COSTA, MOREIRA, 2001).

Veja que na aprendizagem significativa a retenção é maior e o estudante será capaz de relembrar os conceitos facilmente. Por outro lado, na aprendizagem mecânica existe uma menor retenção e o esquecimento é total, ou seja, o estudante precisará de uma nova interação social para interiorizar a informação.

Além da relevante importância do interacionismo proposto por Vygotsky, a sequência didática desta proposta seguiu as ações sistemáticas, que Moreira (2010) baseado nas ideias de Ausubel (1968, 2000), apresenta como uma proposta para que ocorra a aprendizagem significativa: 1) identifica uma estrutura de significados no contexto da aula ou curso; 2) Identificar os subsunçores necessários (pré-requisitos); 3) Identificar os significados preexistentes na estrutura cognitiva do estudante; 4) Organizar sequencialmente os conteúdos e selecionar os materiais curriculares; 5) Ensinar usando organizadores prévios, para fazer pontes entre os significados que os estudantes já possuem e os que ele precisaria ter para aprender significativamente.

Atualmente alguns teóricos identifica uma estrutura de significados no contexto da aula ou curso, por meio de mapas conceituais que auxiliam nas etapas

seguintes, no entanto, Ausubel não utiliza mapas conceituais em sua teoria, esta técnica foi apresentada em meados da década de setenta por Joseph Novak e seus colaboradores na Universidade de Cornell, nos Estados Unidos (MOREIRA, 2011).

Nesta pesquisa não será relevante discutir mapas conceituais, no entanto, o apêndice A, é um modelo de mapa conceitual utilizado pelo pesquisador como auxilio no planejamento e identificação dos subsunçores necessários para que ocorra a aprendizagem significativa.

3.2.1 Discussão da proposta didática

A proposta trabalhada em três etapas caracteriza a etapa A como o momento de análise da matemática presente na criptografia como criação humanada, apresentando as necessidades e preocupações das diferentes culturas, discutindo a evolução dos conceitos em épocas distintas até a sua importância nos dias atuais, como por exemplo, a criação do computador. Usar a história da matemática como um recurso didático permite esclarecer ideias que estão sendo construídas pelos alunos, contribuindo para um olhar mais crítico dos conceitos matemático (PCN, 1997).

A história apresentada no primeiro capítulo deste trabalho foi fundamental para o estimulo a curiosidade do estudante, na medida em que descobria a presença da criptografia no seu contexto social, a atenção era atraída durante a aula e várias indagações foram levantadas por parte dos estudantes, que cada vez mais, demostravam interesse em conhecer o processo para criptografar mensagens.

Esta discussão gerou uma zona de desenvolvimento proximal, mediada pela interação do educador com o educando, marcada pela pré-disposição em aprender os conceitos mediados pelo professor. A tabela 1 permitiu identificar para esta etapa se os estudantes detinham como conhecimento prévio a definição de criptografia, observando que mais de 90% do público não conhecia este conceito. Este foi um fator importante e de grande relevância no planejamento da primeira etapa.

As próximas etapas adotam a identificação dos conhecimentos prévios defendidos por Ausubel e o interacionaismo de Vygotsky com ênfase na ideia de que não se trata de realizar um acumulo de conteúdos, mas de uma situação problema onde os conteúdos apareçam naturalmente (MOREIRA, 2011). Desta forma, à medida que se realiza um método de criptografar, surge o conteúdo e a sistematização é realizada simultaneamente.

Esta pesquisa esta centrada em uma forma diferente de compreensão da divisão euclidiana estudada nos anos iniciais do ensino fundamental, e compreende-se que seu conceito deve ser consolidado nos anos finais, assim, buscou-se abordar segundo os conceitos presentes na aritmética modular, como mostra o capítulo 3.

A primeira criptografia a ser trabalhada foi à cifra de César, mas para isso, a atividade de sondagem no apêndice C foi fundamental para uma identificação dos conhecimentos prévios dos estudantes.

A atividade, composta por sete questões abertas, foi aplicada no final da primeira etapa, uma vez que, a etapa B seria planejada com base nos resultados da sondagem. Todas as questões envolviam as operações de divisão e multiplicação, e exigia do estudante a habilidade de tratar as operações de divisão e multiplicação como inversas uma da outra, além disso, permite identificar se as crianças dominam os conceitos de dividendo, divisor, quociente e resto.

Na questão um, o estudante deve dominar o conceito de divisão exata, para então perceber que o dividendo pode ser encontrado por meio da multiplicação entre o divisor e o quociente. A questão quatro e sete, também se espera como resultado o valor do dividendo, mas para isso, o conceito do resto será fundamental.

As questões dois, três e cinco envolve o cálculo inverso da divisão, ou seja, a multiplicação uma vez que, pretende-se encontrar o divisor de um número. Já na questão 6, o objetivo é apenas identificar se o estudante possui em sua estrutura cognitiva a visão de que o resto de uma divisão são valores maiores que zero e menores que o divisor.

Observe que nesta abordagem o importante não é apenas saber operar a divisão ou a multiplicação, mas conhecer a estrutura dos números quando se realiza este tipo de análise. Estes são os conceitos que se espera estarem definidos nos subsunçores do estudante, para então compreender os conceitos da aritmética modular.

Na primeira aplicação da atividade, isto é, antes da abordagem, somente as questões dois, três, quatro e cinco apresentaram índices de acertos com um processo lógico correto, como mostra o gráfico (a) (gráfico 5), por outro lado, as questões quatro, cinco, seis e sete apresentaram o maior percentual de estudantes que nem chegou a tentar solucionar, um percentual acima de 60%.

A questão três cujo enunciado é “*Pensei em um número, multipliquei-o por 17 e obtive 1836. Em qual número eu pensei?”* apresentou o maior índice de acertos,

na qual era analisada a habilidade de realizar o cálculo inverso das operações, além disso, permitia o estudante pensar na questão como a definição de múltiplos de um número.

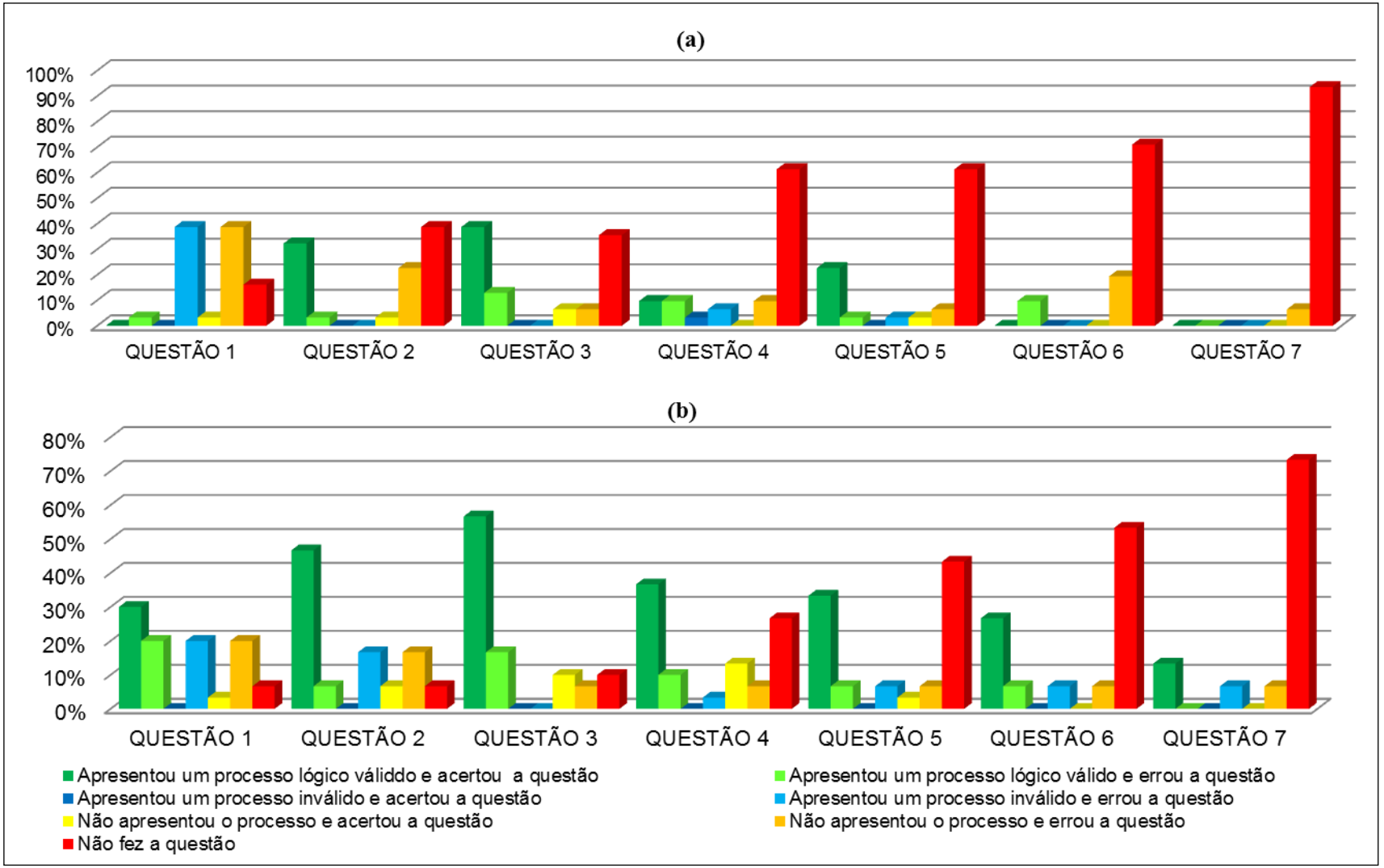
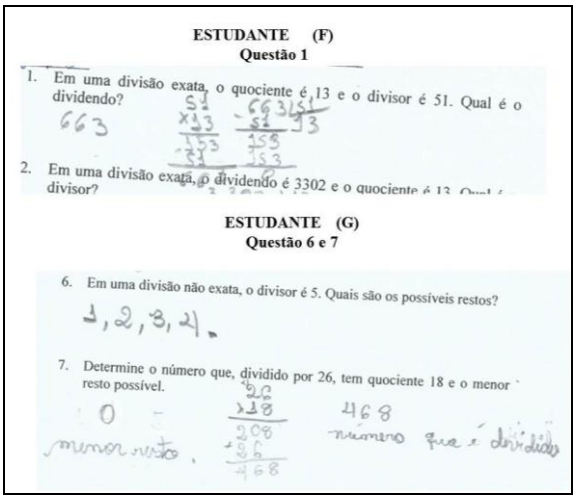


GRÁFICO 5: Resultados da atividade de sondagem: (a) antes da abordagem; (b) depois da abordagem;
Fonte: Próprio Autor

Com o objetivo de gerar uma interação significativa das novas informações com o subsunçor dos estudantes, fez se o uso de um organizador prévio. Logo após, aplicou se novamente a atividade do apêndice C, a fim de identificar se a nova abordagem influenciou na aprendizagem dos estudantes quanto aos conceitos de dividendo, divisor, quociente e resto, caso isso tenha acontecido de forma positiva, então o subsunçor do estudante estaria preparado para interagir com novos conhecimentos.

Pelos resultados apresentados no gráfico 5 (b), é possível perceber uma avanço significativo dos dados. Questões como a um, seis e sete que não apresentaram acertos na primeira aplicação, nesta segunda foi perceptível um índice de acertos considerável, reduzindo significativamente o número de questões não resolvidas, bem como o aumento de acertos nas demais questões.


ESTUDANTE (F)
Questão 1

1. Em uma divisão exata, o quociente é 13 e o divisor é 51. Qual é o dividendo?

663

2. Em uma divisão exata, o dividendo é 3302 e o quociente é 13. Qual é o divisor?

ESTUDANTE (G)
Questão 6 e 7

6. Em uma divisão não exata, o divisor é 5. Quais são os possíveis restos?

1, 2, 3, 4.

7. Determine o número que, dividido por 26, tem quociente 18 e o menor resto possível.

0

menor resto.

468

número que é dividido

Figura 10: Solução apresentada pelos estudantes, questão dois, após abordagem.
Fonte: Próprio autor

Na figura 10, é possível perceber que as questões que não foram solucionadas na primeira aplicação, após o organizador prévio houve uma assimilação significativa que ajudou os estudantes a relembrarem conceitos e compreenderem os novos. A questão um, chama a atenção, pois maior parte dos estudantes que a solucionavam, sempre realizavam a multiplicação, como uma forma de se certificar da validade da solução.

As questões seis e sete solucionadas pelo estudante G, exemplifica o pensamento dos demais estudantes sobre a questão 6, na qual escreviam direto o resultado, como uma sequência de valores de 1 até o antecessor do divisor. A questão

sete o estudante consegue na segunda aplicação identificar que o menor resto possível é o zero, apesar de que algumas soluções consideravam o natural 1 como menor resto possível.

A figura 11 mostra uma dos erros mais comuns nas duas aplicações.

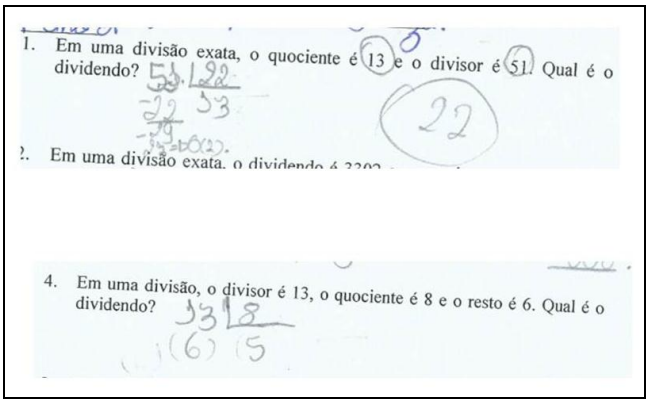


Figura 11: Erros mais frequentes na atividade de sondagem.
Fonte: Própio autor

Os erros mais identificados estavam na realização das operações erradas, ou seja, a operação era escrita de forma correta, mas os resultados estavam errados. Outro erro estava na decisão da operação a ser realizada, quando era necessário aplicar a divisão, adotavam a multiplicação, e o inverso também ocorria.

3.2.2 Organizador Prévio

Como uma forma de facilitar a aprendizagem significativa, por meio de estratégias que manipulem a estrutura cognitiva do estudante, Ausubel propôs o uso de organizadores prévios, definidos como materiais introdutórios apresentados antes da aprendizagem do material programado (MOREIRA, 2011). O organizador prévio pode ser definido por questionamentos a serem levantados na turma, que deve ser capaz de gerar teses, sendo elas verdadeiras ou falsas (ARAGÃO, 1976).

Seguindo esta perspectiva, utilizou-se de organizador prévio para introduzir conceitos gerais em relação ao conteúdo que será estudado. Consiste em realizar uma divisão da turma em grupos, de tal forma que, o nome de cada estudante será representado por um número. Para isso, foi estabelecido um acordo: “*nesta aula será realizada a divisão dos grupos, e durante todo o curso as atividades deverão ser realizadas com os mesmos integrantes de cada equipe*”.

Com a turma formada por 45 alunos, o problema inicial foi dividi-la em dois grupos? Ao levantar este questionamento aos estudantes, foram apresentadas diversas ideias, entre elas, uma possibilidade de resposta é dividir a sala como mostra a tabela 9.

Tabela 9: Modelo da organização dos estudantes em dois grupos.

GRUPO 1	**0**	**2**	**4**	**6**	**8**	**10**	**12**	**14**	**16**	**18**	**20**	**22**	**24**	**26**	**28**	**30**	**32**	**34**	**36**	**38**	**40**	**42**	**44**
GRUPO 2	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	X

Fonte: próprio autor

O grupo 1 formado com 23 estudantes pares e o grupo 2 formado com 22 estudantes impares, definindo grupos com quantidades diferentes de membros. Sendo assim, o professor decide seguir a mesma ordenação dos estudantes, no entanto, dividindo em três grupos. A tabela 10 apresenta a composição dos grupos.

Tabela 10: Modelo organização dos estudantes em três grupos.

GRUPO 1	**0**	**3**	**6**	**9**	**12**	**15**	**18**	**21**	**24**	**27**	**30**	**33**	**36**	**39**	**42**
GRUPO 2	**1**	**4**	**7**	**10**	**13**	**16**	**19**	**22**	**25**	**28**	**31**	**34**	**37**	**40**	**43**
GRUPO 3	2	5	8	11	14	17	20	23	26	29	32	35	38	41	44

Fonte: próprio autor.

Agora os estudantes estão satisfeitos com esta divisão por apresentar uma quantidade justa para os três grupos. Durante a formação dos grupos, o professor solicita a ajuda dos estudantes e vai escrevendo esta divisão no quadro branco. Os alunos mais espertos, podem observar o comportamento dos números e concluir que para decidir qual será o próximo estudante a incluir no grupo, basta somar 3 ao ultimo incluído. Por exemplo, no grupo 1, o primeiro aluno a ser membro foi o zero, os próximos serão $0+3=3$, $3+3=6$, $6+3=9$ assim sucessivamente.

Para deixar o problema mais interessante, o professor levanta a seguinte situação-problema: informa aos estudantes que haverá um evento na escola, na qual, serão realizadas 12 palestras diferentes, uma em cada sala da escola. Para evitar, grandes aglomerações em umas salas e evitar que outras fiquem sem plateia, decide divulgar um dia antes, 12 listas com o nome de cada estudante direcionando a palestra que ele deverá assistir.

Dessa forma, propõe aos estudantes realizar esta divisão, no entanto, são muitos nomes para serem escritos, sendo assim: como divulgar a informação, de forma que, não seja preciso escrever os nomes de todos os estudantes? Isso é possível?

Percebendo a incredulidade dos estudantes na possibilidade de encontrar uma solução para este problema, convida os estudantes para analisar o comportamento dos números durante a divisão das salas em grupo.

Note que, na divisão da sala em três grupos, o primeiro aluno é o zero, o segundo é $3=3+0$, o terceiro é $6=3+3\Rightarrow 6=3+3+0\Rightarrow 6=3\cdot 2+0$, o quarto membro é $9=3+6\Leftrightarrow 9=3+3\cdot 2+0\Leftrightarrow 9=3\cdot 3+0$. Observando os estudantes do grupo dois, notou se que os membros são 1, depois $4=3+1$, em seguida $7=3+4\Leftrightarrow 7=3+3+1\Leftrightarrow 7=3\cdot 2+1$.

Logo, com base no teorema da divisão euclidiana, o professor aproveita da oportunidade e mostra para os estudantes que esta é uma forma diferente de escrever uma divisão. Cada estudante era o dividendo, o divisor era a quantidade de grupos e o resto é representado pelo primeiro estudante de cada grupo. Então, montaram a seguinte tabela para o grupo 1 e em seguida para os demais.

Tabela 11: Tabela com dados das divisões euclidianas de cada estudante por 3, especificando as entradas e saídas encontradas durante a operação.

ESTUDANTES	DIVISÃO	DIVISOR	QUOCIENTE	RESTO
3	$3=3+0$	3	1	0
6	$6=3\cdot 2+0$	3	2	0
9	$9=3\cdot 3+0$	3	3	0
12	$12=3\cdot 4+0$	3	4	0

Fonte: Próprio autor.

Com esta análise, os estudantes observaram que todos os membros do grupo 1, tinha resto zero quando dividido por três, o grupo 2 deixavam resto 1 quando dividido por 3 e o grupo 3 deixavam resto dois quando dividido por três.

A partir deste ponto, fica perceptível a zona de desenvolvimento proximal começando a ser gerada, uma vez que, a divisão euclidiana é o limite inferior deste nível de desenvolvimento, já que se trata de uma operação estudada nos anos iniciais do ensino fundamental.

Seguindo adiante, os estudantes pensam em começar a distribuir os estudantes nas 12 salas. Começa colocando um estudante em cada grupo, seguindo a sequência 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11 perceberam que o estudante 12 será o segundo estudante a entrar no grupo 1, e continua a distribuição finalizando em 3 estudantes por grupo, considerando uma amostra suficiente para analisar o comportamento desta distribuição.

De sorte, o comportamento dos números é o mesmo da divisão da sala em três grupos. Então, o estudante propõe como solução divulgar a seguinte informação: os estudantes compreendidos de 0 até 11, deve assistir as palestras das salas correspondentes as suas numerações, os estudantes maiores que 11 devem dividir o seu número por 12 e ocupar a sala representada pelo resto da divisão.

Outro estudante em sala concluiu que ao colocar os estudantes em ordem, crescente, em uma lista por sala, o quociente informa a posição do estudante nesta lista. Por exemplo, o estudante 235, será o 19º da lista e deverá assistir a palestra na sala 7, pois $235 = 12 \cdot 19 + 7$. Isso considerando que a lista começa a contagem do zero.

Estas são situações em que a aritmética modular está presente. Para causar, curiosidade o professor escreve no quadro que será divulgado a seguinte informação: Cada estudante deverá realizar a operação $estudante \equiv sala \bmod 12$.

A partir daí, a cifra de César passa a ser abordada com a ideia de divisão de estudantes em salas. Uma das frases solicitadas para ser cifrada foi, ATAQUEM AO AMANHECER, assim cada letra da frase original que é representada por um número de acordo com sua ordem no alfabeto brasileiro (capítulo 1), será o estudante e cada sala é representada pelo alfabeto original. Mas para isso, é necessário compreender como criptografar usando a cifra de César.

3.2.3 Criptografias Primitivas em sala de aula

Em dezembro de 2016 no Instituto Federal de Educação Ciências e Tecnologia do Piauí no município de Foriano-PI, a equipe do Nupemat com participação da autoria desta pesquisa, ministrou um curso no 2º Simpósio da Formação do Professor de Matemática da Região Nordeste, com título "*Reciclamatica – confecção de objetos pedagógicos com recursos recicláveis em um ensino interdisciplinar"*, na qual uma das

atividades era a confecção de artefatos criptográficos com materiais recicláveis (figura 12).

Figura 12: Objetos criptográficos com produtos recicláveis
Fonte: Reciclamática/Nupemat

Durante o curso foi realizada a confecção e análise de sequências didáticas possíveis de utilizar deste material como auxilio no ensino da matemática, no entanto, o foco de estudo está direcionado a aprendizagem por manipulação dos objetos durante o processo de confecção. Desta forma, se o objetivo é trabalhar os conceitos de matemática durante o processo de criptografar, o processo de divisão pode ser evitado pelos estudantes, uma vez que basta mover discos nos objetos e substituir letras que a cifra será criptografada com sucesso.

Foi pensando nisso, que o uso destes objetos só foi apresentado à turma durante a realização do jogo “Caça ao Tesouro”, etapa onde os conceitos de matemática envolvidos já tinham sido apresentados em sala.

Nestes artefatos, a cifra mais pertinente é a de César, considerada por vários autores como Faleiro (2011), Malagutti (2015), Shokranian (2012) e Singh (2002), a cifra mais antiga que se conhece, utilizada pelo Imperador Júlio César na Roma Antiga. Trata-se de uma cifra por substituição, na qual as letras do texto original são substituídas por letras de um alfabeto cifrado.

Seguindo esta perspectiva, a sequência didática desta etapa inicia com a Cifra de César, para isso, considerou-se o alfabeto de 26 letras e a cada letra foi atribuído um valor numérico, como mostra a tabela 12.

Tabela 12: Alfabeto utilizado na Cifra de César

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Próprio autor

Cifrar a mensagem, é utilizar a equação $y = x + chave$, tal que as variáveis *x* e *y* são respectivamente, o valor da letra no texto original e o valor da letra do texto cifrado, isto é, considerando a chave 3 para cifrar a mensagem *NUPEMAT*, a letra N deverá ser cifrada pela letra Q, pois o valor de N na tabela 12, é igual a 13, aplicando na equação tem-se $y = 13 + 3 = 16$, observe na tabela 12, que o número 16 corresponde a letra Q.

Portanto, conclui-se que para cifrar as demais letras do texto original, basta adicionar 3 unidades ao valor de cada letra, logo a letra U será cifrada por $y = 20 + 3 = 23$, o que implica ser a letra X, de modo análogo, as demais letras serão cifras obtendo a cifra *QXSHPDW*. A mensagem pode ser enviada em letras ou em números, como 16-23-18-7-15-3-22.

Para ler a mensagem, o destinatário em posse da chave realiza o processo inverso, ou seja, para ler a letra Q, observa que o valor numérico correspondente é o 16, então basta fazer $x = 16 - 3 = 13$, que de sorte é o valor da letra N. Repete-se o processo com todas as letras, obtendo a mensagem original.

O uso de uma chave pequena é fundamental para introdução do conteúdo, visto que, o processo de cifrar e decifra se torna simples e de fácil compreensão. Após esta atividade, os estudantes manifesta interesse em criptografar outras mensagens com chaves diferentes. Assim, pode-se solicitar que os estudantes troquem mensagens e combinem uma chave a ser utilizada.

Para a mensagem NUPEMAT, uma das possíveis chaves a ser escolhida é a 10. Por outro lado, esta escolha gera um questionamento, fundamental para começar a introduzir os conceitos de aritmética modular, posto que, a letra U deverá ser cifrada pela letra de valor 30, já que, $y = 20 + 10 = 30$.

É neste momento, que o organizador prévio será utilizado como uma ponte de assimilação dos conceitos. Veja que, a letra U na frase original será o estudante 20, e deverá ser cifrado por $20 + 10 = 30$, porém só existem 26 salas. Então, qual a sala correspondente a este estudante? Aplicando, os conceitos do organizador prévio, o estudante deverá ocupar a sala 4, tal que, $30 = 26 * 1 + 4$, logo, a sala de cada estudante, será a letra utilizada para cifrar a mensagem, assim, a o estudante U está na sala E, portanto a cifra para letra U será a letra E.

Além disso, é nesta análise que começa a introduzir os conceitos de congruência modular. Considerando *k* a chave para cifrar a mensagem, pode-se afirmar que a cifra de César é uma congruência do tipo $Y \equiv X + k(\mathrm{mod}\,26)$, ou seja, a posição da letra da mensagem cifrada é o resto da divisão de $x+k$ por 26, que pela definição da divisão euclidiana $0 \le y < 26$. Se $k = 0$, então a cifra será a própria mensagem original.

Aplicando a proposição 2.8, é possível concluir que para decifrar basta realizar a congruência $Y - k \equiv X(\mathrm{mod}\,26)$, isto é, agora se procura o resto da divisão de $y-k$ por 26, tal que $0 \le x < 26$.

Durante a abordagem, foi solicitado aos estudantes que verificassem se as congruências na figura 13 são verdadeiras ou falsas. Para isso, os estudantes realizavam a divisão e em seguida comparavam os restos.

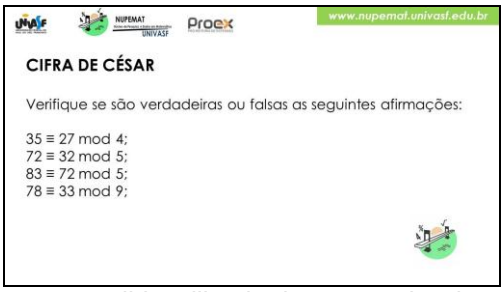


Figura 13: *Slide* utilizado durante a abordagem
Fonte: Próprio autor

No entanto, um dos estudantes (7º ano) se manifestou falando que não precisava realizar a divisão e exemplificou argumentando que: *"para a congruência* $35 \equiv 27(\mathrm{mod}\,4)$ *basta fazer* $35-27=8$ *e 8 é divisível por 4, logo são congruentes, por outro lado,* $72 \equiv 32(\mathrm{mod}\,5)$*, temos* $72-32=40 \to 40-32=8$*, mas 5 não divide 8, portanto não são congruentes".*

O que o estudante percebeu, na realidade foi à proposição 2.7, na qual de forma significativa está propriedade foi de fácil descoberta.

Para tornar a criptografia mais interessante, consideraram-se dois valores *a* e *b* com $y \equiv ax + b(\mathrm{mod}\,26)$, tal que *a* e *b* são as chaves para cifrar. Quando isso acontece, diz que utilizou a Cifra Afim. Por exemplo, cifrar a mensagem NUPEMAT, utilizando as chaves $a = 10$ e $b = 23$, a letra N de valor 13 deverá ser cifrado pela letra X, visto que, $y \equiv 10 * 13 + 23(\mathrm{mod}\,26) \to \mathrm{y} \equiv 23(\mathrm{mod}\,26)$. Repetindo o processo em todas as letras da mensagem, a cifra será *XVRLNXF* ou 23-21-17-11-13-23-5.

Para decifrar, basta aplicar o processo inverso, obtido por meio da proposição 2.8 e a definição de inversos modulares, isto é, $(y-b)a^{-1} \equiv x(\mathrm{mod}\,26)$. No entanto, este processo exige do estudante o domínio dos conceitos de inversos modulares para que seja possível, realizar a divisão na congruência.

De início, alguns estudantes na tentativa de realizar o processo inverso, procederam realizando o processo inverso da adição e da multiplicação, isto é, para decifrar a letra V, faziam $(21-23)*3^{-1} \equiv x(\mathrm{mod}\,26)$ o que implica $2*3^{-1} \equiv x(\mathrm{mod}\,26)$ o que considerava impossível, uma vez que, $2*3^{-1} \notin \mathbb{Z}$, no entanto, o processo a ser realizado não é a divisão nos inteiros.

Daí surge à necessidade de abordar os conceitos de inversos modulares e equações diofantinas, com atenção a utilização de uma linguagem compreensível pelos estudantes, para que a assimilação dos conceitos seja algo possível.

Para isso, utilizou de exemplos mais simples para chegar aos mais complexos. Por se tratar de estudantes do ensino fundamental, utilizou de organizador prévio a ideia do cancelamento na adição e multiplicação dos inteiros, a fim de que fosse possível compreender cancelamento de valores iguais, observando que se trata de realizar a operação entre um número inteiro e o seu inverso. Desta forma, na congruência não será diferente. Mas, para isso precisam-se conhecer os inversos modulares.

Quando se trata do conjunto dos números inteiros, encontrar o inverso de um número em relação à operação de adição basta analisar qual o número x^{-1} que somado com x gera o elemento neutro da adição, caso seja possível encontrar este número x^{-1} será chamado de inverso de x na adição. De modo análogo, define-se o inverso de um inteiro na multiplicação.

Para a congruência modulo 26, considera que o conjunto é o $Z_{26} = \{0,1,2,3,\cdots,25\}$, ou seja, todos os possíveis restos de uma divisão por 26. Este conjunto recebe o nome de resíduos módulo 26. Pela definição dos inteiros, encontrar um inverso de qualquer elemento de Z_{26} é analisar qual o valor $a^{-1} \in Z_{26}$ aplicado à

operação de multiplicação com algum elemento $a \in Z_{26}$, gere o elemento neutro da multiplicação. Isto é, $a * a^{-1} \equiv 1 (\mathrm{mod}\, 26)$.

Daí, encontrar este valor é fazer $aa^{-1} - 1 = 26k$, com $k \in \mathbb{Z}$, o que implica solucionar a equação diofantina $aa^{-1} + 26(-k) = 1$, pela seção 2.3 isso só é possível se $mdc(a, 26) = 1$, portanto isso, reproduz uma limitação para escola dos valores de *a.* Aplicando a proposição 2.10, a decomposição prima de $26 = 2 \cdot 13$, com isso o conjunto Z_{26}, possui $\varphi(26) = 26\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12$ inversos modulares, sendo eles representados na tabela 13.

Tabela 13: Inversos modulares de Z_{26}

Resídusos	1	3	5	7	9	11	15	17	19	21	23	25
Inversos modulares	1	9	21	15	3	19	7	23	11	5	17	25

Fonte: Próprio autor.

Se você possui uma informação bem sigilosa e pretende criptografar de forma que seja o mais segura possível, qual das duas Cifras deve-se utilizar? No capítulo 1, uma das discussões esta pautada na segurança de uma cifra. Veja que a cifra de César é um caso particular da cifra afim, isso por que, a cifra considera $a = 1$ e apenas o valor de *b* é variável. Desta forma, pela divisão euclidiana, $0 \leq b \leq 25$, onde 0 não é uma escolha segura, já que não altera o conteúdo da mensagem, sendo assim existem 25 possibilidades de escolhas para *b,* por tanto existe 25 chaves possíveis.

Por outro lado, apesar da cifra afim, apresentar uma limitação para as escolhas dos valores de *a,* ela é considerada mais segura do que a cifra de César, uma vez que, é necessário escolher duas chaves, onde para escolha de a existem 12 possibilidades e para a escolha de b existem 25 possibilidades, logo para a cifra afim existem 300 chaves possíveis.

Durante o processo de socialização destes conceitos, foram aplicados uma sequência de questões como mostra o apêndice D. O objetivo é identificar se os estudantes assimilaram as ideias das escolhas da chave, uma vez que será fundamental o domínio deste conceito durante o jogo Caça ao Tesouro, que será detalhado na subseção 3.2.4.

As questões um e dois foram utilizadas para identificar se houve uma boa compreensão sobre as escolhas das chaves a e b. Onde na questão um, 58% responderam ser possível escolher qualquer valor inteiro e os demais afirmaram ser possível apenas valores menores que 26.

Por este motivo, foi realizada outra discussão acerca da escolha da chave *b,* desta vez com objetivo de justificar que b pode assumir qualquer valor inteiro, no entanto, existem conjuntos de valores que geram a mesma cifra.

Sejam $a,b \in \mathbb{Z}$, tal que $c \in A = \left\{ c = a^{-1} \mid aa^{-1} \equiv 1 (\mathrm{mod}\, 26); \mathrm{a, c} \in \mathrm{Z}_{26} \right\}$, daí $y = cx + b (\mathrm{mod}\, 26)$, para o caso $0 \le b < 26$, garante que *b* será um resíduo módulo 26. Para o caso, $26 \le b$, tal que $b = 26q + r$, com $0 \le r < 26$. Logo, a congruência será $y \equiv cx + 26q + r (\mathrm{mod}\, 26)$ o que implica $y \equiv \left(cx + r\right) + 26q (\mathrm{mod}\, 26)$, note que $cx + r$ é o resto da divisão de um inteiro $d = 26q + (cx + r)$ por 26. Logo, pode-se afirmar pela definição de congruência que $d \equiv cx + r (\mathrm{mod}\, 26)$ e $y \equiv d (\mathrm{mod}\, 26)$, por transitividade $y \equiv cx + r (\mathrm{mod}\, 26)$, com $0 \le r < 26$. Portanto, $b \in Z_{26} - \{0\}$, com 25 possibilidades de escolas.

A questão dois, referente aos valores de a todos os estudantes afirmaram ser valores primos menores que 26, o que não está errado, no entanto o valores de a, podem não ser primos e admitir inverso, a exemplo do 9. Ou seja, o correto é afirmar que os valores *a,* são os co-primos de 26, que sejam maiores ou iguais a 26. Na discussão em sala, a resposta foi esclarecida (figura 14), os alunos entendiam que era necessário que $mdc(a, 26) = 1$, o que não conseguiram foi transcrever esta informação, na qual acreditavam que afirmar ser primo menor que 26 representava a mesma ideia de ser co-primos.

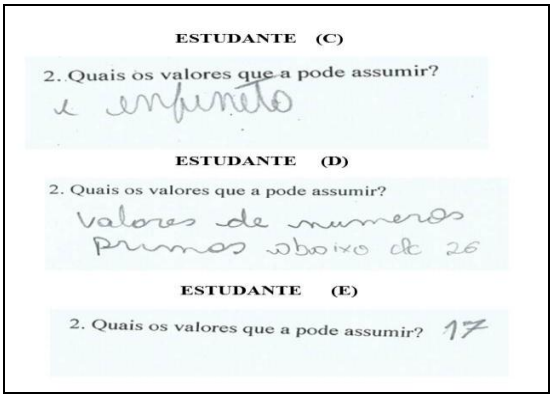


Figura 14: Soluções da questão 2 da atividade da cifra de César (apêndice D).
Fonte: Próprio autor

O estudante (C) afirma poder ser utilizado infinitos valores, o que não está errado, no entanto, mostra não ter assimilado a ideia de chaves que geram as mesmas cifras. O estudante (D), afirma que o possível são valores primos menores que 26. Em conversa na sala de aula, foi possível perceber que os estudantes que apresentaram esta solução, acreditavam que para serem primos entre si, os números precisam ser primos, o que não é verdade, porém, demonstraram compreender a ideia das chaves que apresentam cifras iguais. O estudante (E) apresentou um pensamento semelhante ao estudante (D), com a diferença de ao invés de apresentar todos os possíveis valores, optou por apresentar um exemplo.

Na questão três, todos afirmaram que para o caso $a = b$, retornamos a cifra de César, no entanto, não deixaram uma justificativa da resposta. Esperava-se que os estudantes registrassem que o único caso possível seria se $a = b = 1$. A escolha de outras igualdades pode implicar na invalidade de chaves para *a*.

A questão quatro foi influenciada pela questão 1 apresentando que 58% afirmaram existir ser infinitas chaves. Cerca de 10% não respondeu a questão e um estudante respondeu existir duas chaves para cada número primo *a*. Os demais, afirmaram existir 300 chaves.

A questão com maior êxito foi a cinco, induzindo os estudantes a cifrar e decifrar mensagens. Durante esta atividade, foi possível perceber o estimulo, a participação voluntária em realizar as atividades, uma vez que, para eles se tratava de uma diversão. Assim, as operações eram realizadas durante a atividade e consideradas prazerosas.

Outra cifra estudada, foi à famosa Cifra de Hill, criada pelo americano Lester S. Hill durante a década de 20, sua valiosa contribuição impulsionou os estudos no uso da álgebra na criptografia (FALEIROS, 2011).

Trata-se de uma criptografia por substituição com o uso de matrizes quadradas $n\times n$, chamada n-Cifra de Hill. Por ser um conceito, abordado com estudantes do ensino fundamental e considerar que sua estrutura cognitiva não dispõe de subsunçores suficientes para que ocorra uma aprendizagem significativa com matrizes superiores, nesta pesquisa foram abordadas apenas as ideias de matrizes quadrada 2×2, isto é, a 2-Cifra de Hill.

Para criptografar uma mensagem, utiliza-se o mesmo alfabeto utilizado na cifra afim (tabela 5), de tal forma, que $X,Y\in M_{2\times 2}\left(Z_{26}\right)$. Com isso define-se a Cifra de Hill como uma congruência entre matrizes, tal que

$$Y\equiv AX\,(\mathrm{mod}\,26)$$

Onde, X é a matrizes da mensagem original, Y as matrizes da mensagem cifrada e A é a chave da Cifra. Assim, suponha que a mensagem que se deseja cifrar seja $x_1x_2x_3\cdots x_n$ e a chave é a matriz quadrada $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Como na congruência é necessário realizar a multiplicação de matrizes *AX,* pela definição de multiplicação de matrizes, $X\in M_{2\times n}\left(Z_{26}\right)$, com $x_i\in Z_{26}$, e $i=1,2,3,4,...,n$. Logo, organizando a mensagem em uma matriz do tipo,

$$X=\begin{pmatrix} x_1 & \cdots & x_{n-1} \\ x_2 & \cdots & x_n \end{pmatrix}$$

Será obtida a congruência,

$$\begin{pmatrix} y_1 & \cdots & y_{n-1} \\ y_2 & \cdots & y_{\tilde{n}} \end{pmatrix}\equiv\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} x_1 & x_3 & \cdots & x_{n-1} \\ x_2 & x_4 & \cdots & x_n \end{pmatrix}(\mathrm{mod}\,26).$$

Encontrando a mensagem cifrada $y_1y_2y_3\cdots y_n$. Note que, para este caso, n é um número par. Para o caso de, *n* ser ímpar merece uma atenção especial. Veja que para escrever a matriz *X*, você precisa decidir como preencher a ultima entrada.

$$X=\begin{pmatrix} x_1 & x_3 & \cdots & x_n \\ x_2 & x_4 & \cdots & x_i \end{pmatrix}$$

Uma alternativa para este problema é escolher um $x_i \in Z_{26}$ de forma arbitrária, assim à congruência não se altera, e na leitura da mensagem original, basta eliminar o ultimo elemento da sequência.

Outra forma de pensar é acrescentar um novo símbolo ao alfabeto, no entanto, o alfabeto não será mais composto por 26 caracteres, mas 27. Logo, considerando o @ como sendo o novo caractere, a congruência será,

$$\begin{pmatrix} y_1 & y_3 & \cdots & y_n \\ y_2 & y_4 & \cdots & y_{n+1} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_1 & x_3 & \cdots & x_n \\ x_2 & x_4 & \cdots & @ \end{pmatrix} (\mathrm{mod}\, 27)$$

Desta forma, a cada símbolo acrescentado, o módulo da congruência se modifica, bem como a quantidade de chaves possíveis, uma vez que, a análise para as chaves é análoga à realizada na cifra afim, isto é, na congruência módulo 26 existem 12 inversos modulares capazes de gerar matrizes chaves, no Z_{27} esse valor aumenta para 18 inversos modulares. De acordo, com a definição de inversos modulares, para o conjunto Z_p com *p* primo existem $p-1$ inversos modulares.

Ao trabalhar com turmas do ensino fundamental, optou por dividir a matriz *X* em matriz coluna de ordem 2, e realizar as congruências separadas. Assim, a mensagem deve ser dividida em matrizes do tipo,

$$X_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}; X_2 = \begin{pmatrix} x_2 \\ x_3 \end{pmatrix}; \cdots; X_{\frac{n}{2}} = \begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix}$$

Reduzindo a congruência $\begin{pmatrix} y_{n-1} \\ y_n \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_n \end{pmatrix} (\mathrm{mod}\, 26)$.

Sendo assim, ao cifrar a palavra *NUPEMAT*, utilizando a chave $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix}$, as entradas da matriz *X* serão os $x_i \in Z_{26}$, correspondentes as suas respectivas letras como mostra a tabela 10. Daí, a palavra NUPEMAT corresponde à sequência $13-20-15-4-12-0-19$, mas como possui uma quantidade ímpar de elementos, uma escolha aleatória será a letra B, cujo valor é 1, portanto a sequencia será $13-20-15-4-12-0-19-1$, deste modo, as matrizes do texto original são,

$$X_1 = \begin{pmatrix} 13 \\ 20 \end{pmatrix}; X_2 = \begin{pmatrix} 15 \\ 4 \end{pmatrix}; X_3 = \begin{pmatrix} 12 \\ 0 \end{pmatrix} e\ X_4 = \begin{pmatrix} 19 \\ 1 \end{pmatrix}.$$

Aplicando a congruência em cada matriz, tem-se para X_1 o seguinte resultado:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 13 \\ 20 \end{pmatrix} (\text{mod } 26) \Rightarrow \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \equiv \begin{pmatrix} 73 \\ 46 \end{pmatrix} (\text{mod } 26)$$

Logo, $y_1 = 73$ e $y_2 = 46$, mas não existem letras com estes valores, com isso, aplica-se congruência modulo 26 em cada valor de y, isto é, $y_1 \equiv 73 (\text{mod } 26) \Rightarrow y_1 = 21$ e $y_2 \equiv 46 (\text{mod } 26) \Rightarrow y_2 = 20$, portanto a letra N será substituída pela letra V e a letra U permanece sendo a letra U.

Repetindo o processo com as matrizes X_2, X_3 e X_4 a cifra da mensagem *NUPEMAT* será *VUBIMYWY*.

Aplicando a propriedade 2.7, na congruência abaixo, obtêm-se como resultado o processo para decifrar a cifra de Hill.

$$Y \equiv AX (\text{mod } 26) \Rightarrow YA^{-1} \equiv X (\text{mod } 26)$$

Logo, para decifrar é necessário encontrar a matriz inversa da chave. Pelo teorema 2.8, a matriz inversa pode ser definida fazendo, $A^{-1} = \det(A)^{-1} adj(A)$. Além disso, suponha a matriz A de ordem 2, possui inversa, então existe A^{-1}, tal que $AA^{-1} = I_2$.

Aplicando o determinante, tem-se que $AA^{-1} = I_2 \Rightarrow \det(A) \cdot \det(A^{-1}) = \det(I_2)$, logo $\det(A) \cdot \det(A^{-1}) = 1$. Aplicando congruência, tem-se que $\det(A) \cdot \det(A^{-1}) \equiv 1 (\text{mod } 26)$. Pela definição de inversos modulares, é possível afirmar que o inverso do determinante de A, é o determinante da matriz inversa de A, modulo 26, isto é, $\det(A)^{-1} = \det(A^{-1})$.

Desta forma, para que uma chave possa ser válida na cifra de Hill, a sua matriz precisa admitir uma inversa, ou seja, $\det(A) \neq 0$, além disso, o determinante precisa possuir um inverso módulo 26, caso contrário, não será possível decifrar a mensagem.

Veja que, no exemplo da mensagem *NUPEMAT*, a chave A utilizada é válida, uma vez que, $A = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \Rightarrow \det(A) = -5 \neq 0$. Além disso, possui inverso $\det(A)^{-1} = 5$ módulo 26, já que, $(-5) \cdot 5 \equiv 1 (\text{mod } 26) \Leftrightarrow 26 \mid -25 - 1 = -26$.

Para determinar a matriz inversa, precisa-se determinar a adjunta, que pelo exemplo 3.2, por se tratar de uma matriz quadrada de ordem 2, a sua adjunta será:

$$adj(A) = \begin{pmatrix} 1 & -3 \\ -2 & 1 \end{pmatrix}$$

Logo, a matriz inversa será $A^{-1} = 5\begin{pmatrix} 1 & -3 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 5 & -15 \\ -10 & 5 \end{pmatrix}$. Assim, para decifrar a mensagem *VUBIMYWY*, representada pela sequência numérica $21-20-1-8-12-24-22-13$, aplica na congruência obtendo:

$$\begin{pmatrix} 21 & 1 & 12 & 22 \\ 20 & 8 & 24 & 13 \end{pmatrix}\begin{pmatrix} 5 & -15 \\ -10 & 5 \end{pmatrix} \equiv \begin{pmatrix} x_1 & x_3 & x_5 & x_7 \\ x_2 & x_4 & x_6 & x_8 \end{pmatrix} (\text{mod } 26)$$

Definindo assim, a mensagem original *NUPEMAT*.

Veja que de acordo com o que foi discutido até este ponto, mostra que a criptografia pode ser utilizada como uma ferramenta, de auxilio no ensino e aprendizagens de conceitos nas séries finais do ensino fundamental. Além disso, essa é uma forma de consolidar os conceitos de divisão aprendidos nos anos iniciais.

Além disso, no que diz respeito aos conteúdos de matrizes e determinantes a possibilidade se serem trabalhados no ensino fundamental estar diretamente relacionada à linguagem de abordagem. Ou seja, não se pode tratar de determinantes como se aborda no ensino médio, no entanto, não impede de ser utilizado com estudantes do 6º ao 9º ano.

Sendo assim, isso exige que o professor tenha conhecimento no ramo da álgebra e das teorias dos números, quando se trabalha com aritmética modular. Com isso, pensou-se em levantar dados por meio do questionário no apêndice E, sobre o perfil do professor em relação à forma de abordagem dos conceitos de divisões com os anos finais do ensino fundamental.

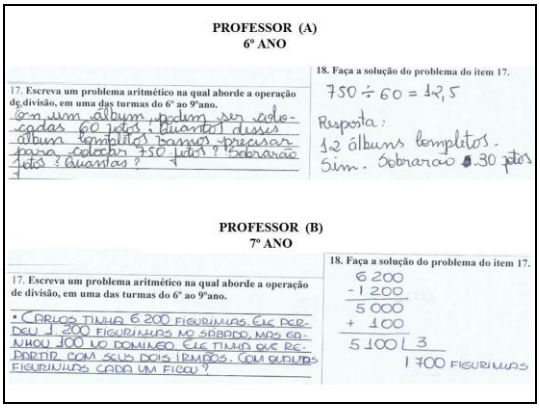
Pesquisou-se a opinião dos professores das escolas públicas, em especial as escolas a qual pertence o público do DTM. Os estudantes do ensino fundamental que participam do DTM são oriundos de 25 escolas públicas de Petrolina, no entanto, devido ao difícil acesso, o questionário foi aplicado a apenas uma escola da área rural, e sete escolas da área urbana, um total de 20 professores de matemática que lecionam no ensino fundamental.

Dos entrevistados, menos de 1% atuam em sala de aula a menos de um ano, 18% estão em sala de aula a mais de quatro anos e menos de seis anos, e mais de 70% estão em sala de aula a mais de seis anos. Todos são licenciados em matemática, exceto uma professora que é licenciada em Biologia e outra que está em processo de conclusão, no entanto, atua como professora de matemática nos anos finais do ensino fundamental, além disso, com exceção da professora que está concluindo o ensino superior, os demais possuem especialização lato sensu, sendo 80% em metodologia no ensino da matemática, 2% em outra área e 18% não informaram a área do curso.

Todos esses professores já lecionaram outras disciplinas. No questionário (Apêndice E), solicita que se possível informe quais são essas disciplinas, os nomes citados foram: matemática, física, química, biologia, artes, religião e um professor que atuou com disciplinas no ensino superior. Desses profissionais apenas três professores atuam somente em uma escola, os demais atuam em mais de um local.

Em primeiro momento foi solicitado que escrevessem um problema aritmético na qual aborde a operação de divisão, em uma das turmas do 6º ao 9º ano. Apenas dois professores não responderam a esta questão. Ao escrever o problema, o professor precisava em seguida informar a solução e em qual turma ele abordaria problemas deste tipo.

Os problemas foram todos seguindo pensamentos semelhantes, dividir quantidades em partes iguais, analisar se sobram quantidades, uso de frações e sistemas de equações. Não houve problemas, relacionados à análise padrão de comportamento dos números e problemas em eventos cíclicos. Veja alguns exemplos das repostas dadas pelos professores nas figuras 15 e 16.



PROFESSOR (A)
6º ANO

17. Escreva um problema aritmético na qual aborde a operação de divisão, em uma das turmas do 6º ao 9ºano.

Em um álbum podem ser colocadas 60 fotos. Laurentt disse álbum completo bastaria precisar para colocar 750 fotos? Sobrarão fotos? Quantas?

18. Faça a solução do problema do item 17.

750 ÷ 60 = 12,5

Resposta:
12 álbuns completos.
Sim. Sobrarão 30 fotos

PROFESSOR (B)
7º ANO

17. Escreva um problema aritmético na qual aborde a operação de divisão, em uma das turmas do 6º ao 9ºano.

• CARLOS TINHA 6.200 FIGURINHAS ELE PERDEU 1.200 FIGURINHAS NO SÁBADO, MAS GANHOU 100 NO DOMINGO. ELE TINHA QUE REPARTIR COM SEUS DOIS IRMÃOS. COM QUANTAS FIGURINHAS CADA UM FICA?

18. Faça a solução do problema do item 17.

6 200
-1 200
5 000
+ 100
5 100 | 3
1 700 FIGURINHAS

Figura 15: Solução dos professores referentes às questões de divisão.
Fonte: Próprio autor

Vejam que as questões do professor A e B na figura 15 mostram que a abordagem sugerida pelos docentes é o conceito de divisão em partes iguais, onde seja possível sobrar resto ou não. Na figura 16, os professores apresentam uma sugestão de questões a serem trabalhadas com o 8º de 9º anos, onde as ideias da operação de divisão aparecem como ferramenta para solucionar o problema, mas é vista como uma etapa da resolução das equações, onde não permite ao estudante afirmar se trata de um problema de divisão ou não.

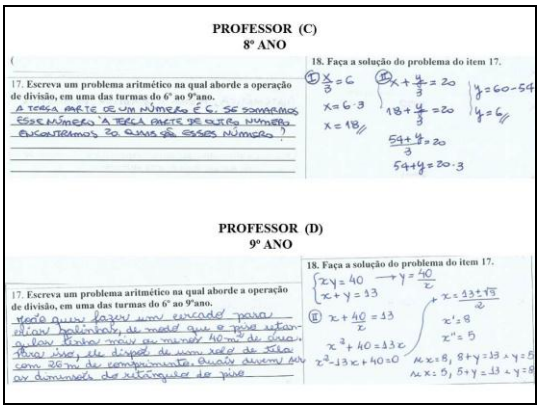


Figura 16: Solução dos professores referentes às questões de divisão.
Fonte: Próprio autor

Em seguida, questionou-se sobre opinião deles em relação às operações que os estudantes possuem maior dificuldades. Cerca de, 61% dos professores afirmam ser a divisão a operação que os estudantes apresentam maior dificuldade, em seguida a multiplicação. Isso mostra a necessidade de maior atenção a esta operação, uma vez que, é necessário identificar os motivos geradores.

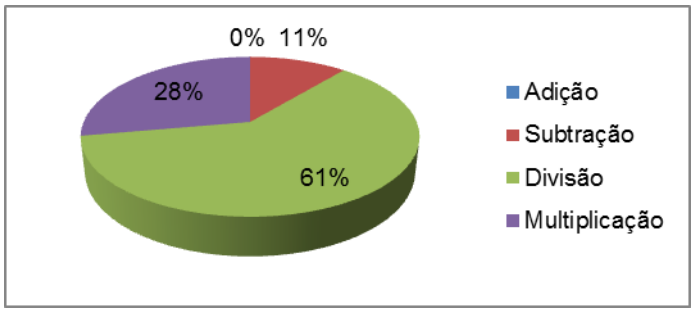


Gráfico 6: Operações que os estudantes apresentam maior dificuldade
Fonte: Próprio autor

Como mostram dos dados do gráfico 1, a transição entre os anos iniciais e finais, pode ser um motivo para esta dificuldade, na qual a continuidade da aprendizagem do

estudante pode sofrer rompimentos, impedindo de progredir. Daí, buscar recursos que gerem atividades lúdicas, pode ser uma alternativa para manter a conexão do processo de aprendizagem.

Como esta proposta propõe utilizar a criptografia como auxilio no planejamento de atividades que gerem uma aprendizagem significativa, as próximas questões aplicadas aos professores, levantou dados sobre o que eles entendem por criptografia.

Mais de 50% dos professores afirmaram já ter ouvido fala em criptografia, porém somente dois professores descreveram o que é criptografia. Isso permite, inferir que estes profissionais, conhecem a palavra por ter em algum momento visto em filmes ou texto, mas sem atentar para seu significado.

Além disso, mais de 60% afirmaram não ser possível trabalhar criptografia em sala de aula, por ser complexa para o aluno, ou por não conhecer uma forma de abordar este conceito em sala de aula. Em relação aos conteúdos abordados na criptografia, apenas dois professores apresentaram sugestões, sendo uma com o uso de aritmética modular e outra com o uso de funções. Esses professores informaram ter aprendido estes conceitos no curso do mestrado do Profmat na Univasf.

Em relação aos conceitos de matrizes mais de 50% acredita ser possível aplicar conceitos de matrizes nas turmas do 6º ao 9º ano. Assim, esses dados revelam que a falta de conhecimento por parte dos professores, impedem de utilizar esta abordagem em sala de aula.

Por outro lado, mostra que esta pesquisa pode ser uma oportunidade desses profissionais estudarem uma forma diferente de aplicar os conceitos de divisão e multiplicação ligados às ideias de aritmética modular e determinantes, percebendo que em qualquer abordagem é necessário adaptar os conceitos a estrutura cognitiva no educando.

3.3 USO DE JOGOS NO ENSINO DA MATEMÁTICA: CAÇA AO TESOURO

A discussão sobre jogos apesar de ser bem antiga, no âmbito da educação suas contribuições mais importantes são datadas da metade do século XX. Além disso, com o advento da tecnologia e a grande participação dos jogos eletrônicos na realidade

sociocultural dos estudantes, falar de jogos se tornou um assunto amplo e de grande importância na educação das crianças (DALARMI, 2013; BRASIL, 2012).

Desta forma, a escola não pode se manter isolada desse processo evolutivo da tecnologia, ela precisa estar atenta às necessidades do público atual (GRANDO, 2000). As mudanças curriculares é uma manifestação de adaptação às necessidades do público, elaborada a partir de discussões e análises de publicações e práticas pedagógicas.

Assim, a estrutura dos parâmetros curriculares, apresentam discussões sobre os conteúdos a serem trabalhados, os métodos de avaliação e novas formas de abordagem dos conteúdos, como uma forma de ajudar a escola no seu planejamento (BRASIL, 2013;BRASIL,2012).

Huizinga (1990, p. 33, apoud, LIMA, 2008, p. 40) apresenta uma definição de jogo, sintetizando os seus principais fenômenos.

> O jogo é uma atividade ou ocupação voluntária, exercida dentro de certos limites de tempo e espaço, segundo regras livremente consentidas, mas absolutamente obrigatórias, dotado de um fim em si mesmo, acompanhado de um sentimento de tensão e alegria e de uma consciência de ser diferente da vida cotidiana.

Reforçando a importância do jogo, na vida do homem, Callois (1990, apud LIMA, 2008) afirma que o jogo, é uma escola capaz de trabalhar no jogador certos costumes e valores sociais, e recuar a cobiça e o ódio, lembrando que é princípio do jogo aprender a aceitar a derrota como contratempo e a vitória sem vaidade.

Uma das abordagens, discutidas estão voltadas para o uso de jogos e Tecnologias da Informação e Comunicação (TIC's). Tanto os Parâmetros Curriculares do Estado de Pernambuco (BRASIL, 2012), como os Parâmetros Curriculares Nacionais (BRASIL, 1997) tratam, como formas de abordagens, capazes de estimular a capacidade do estudante de levantar, hipóteses, testarem, argumentar a sua validade e apresentar conclusões, por meio do raciocínio lógico presente, além da interação na produção de conhecimento.

Dentre as críticas mais comuns quanto ao ensino da matemática tradicional, destacam-se: o aluno passivo, acúmulo de informações, pouca experimentação, altos índices de reprovação em matemática e a grande dificuldade dos estudantes em

estabelecer uma lógica matemática. Isso são consequências de abordagens onde a nova informação não interage com o que o educando já conhece. Assim, os jogos e tecnologias são vistos como oportunidades de gerar uma aprendizagem significativa, na qual o estudante seja ativo na construção de seu conhecimento, adquirindo autonomia em sua aprendizagem (GRANDO, 2000).

Seguindo este princípio, ainda no questionário aplicado aos 20 professores do DTM, levantou-se dados a respeito do uso de tecnologia e jogos em sala de aula.

A primeira pergunta a respeito à prática pedagógica do professor estava relacionada à frequência do uso de tecnologia em sala de aula durante as aulas de matemática. O gráfico 7 mostra que todos utilizam tecnologia em sala de aula, apenas 35% utilizam com mais frequência.

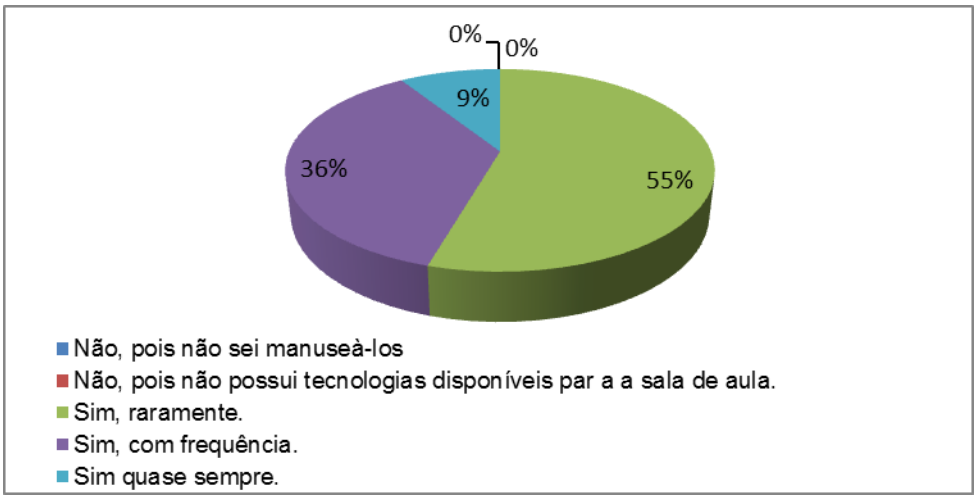


Gráfico 7: Frequência do uso de tecnologias na sala de aula.
Fonte: Próprio autor

O tipo de tecnologia utilizada por mais de 36% dos professores são o computador e data show, os demais afirmaram usar outros tipos de tecnologias. Apesar destes resultados, apresentarem que os professores estão atentos aos usos das tecnologias como auxilio o ensino da matemática, isso não garante inferir se possuem formação adequada para o uso desta ferramenta, o que pode ser o motivo de 55% raramente usarem este recurso.

Por outro lado, outros fatores podem influenciar no uso da tecnologia, como por exemplo, o fato de mais da metade dos professores lecionarem em mais de uma

escola, na qual, dependendo da jornada de trabalho, esses profissionais não tenham tempo suficiente para se dedicar a um planejamento com atividades lúdicas.

A falta da tecnologia na escola, também pode ser encarada como um obstáculo para o profissional. Para isso, a segunda questão, pergunta se quando esses profissionais utilizam a tecnologia em sala de aula, se é em quantidade suficiente para a turma.

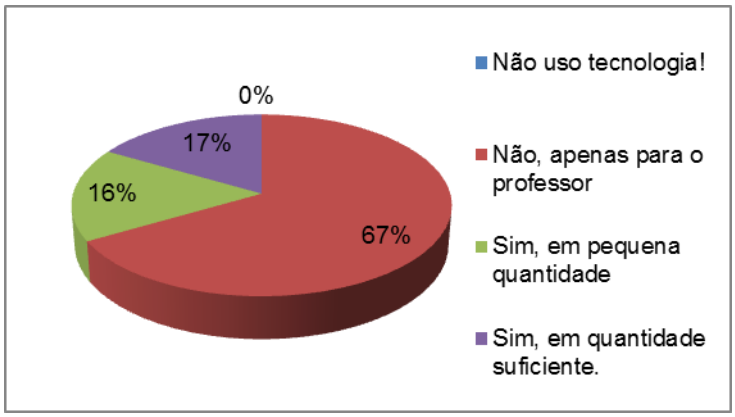


Gráfico 8: Quantidade de tecnologia suficiente para a quantidade de estudantes.
Fonte: Próprio autor

Veja que no gráfico 8, apenas 17% dos profissionais atuam em escolas na qual a quantidade de tecnologia é suficiente para toda a turma. Infelizmente 67% possui apenas a quantidade para o professor. Esses dados, só reforçam as hipóteses levantadas em relação aos obstáculos ao uso de tecnologia.

Em relação à tecnologia computacional, inserir o computador na escola não significa que, os profissionais e estudantes estão sendo informatizados, para que isso aconteça, o profissional deve está preparado para utilizar este recurso de forma que atenda aos objetivos de sua disciplina, saber planejar como avaliar o estudante que realizará suas atividades com um computador.

Borba e Penteado (2012) ressalta que os cursos de ensino superior e as formações continuadas devem dar estes suportes aos profissionais da educação básica, pois além da falta de formação, existe a saída de uma zona de conforto, onde o novo assusta. Porém a escola não pode fugir dessa realidade.

Além do uso, da tecnologia, outro recurso utilizado em atividades lúdicas são os jogos, sejam eles eletrônicos ou não.

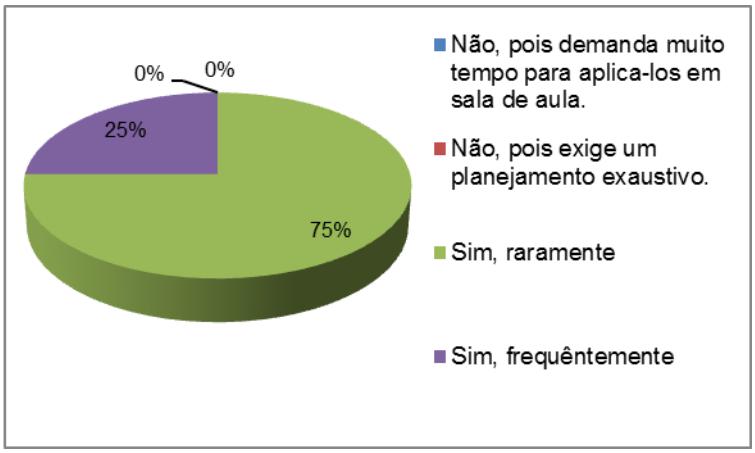


Gráfico 9: Frequência do uso de jogos na sala de aula
Fonte: Próprio autor

Veja que todos os professores mencionaram utilizar jogos em sala de aula, no entanto, 75% raramente utiliza esta ferramenta. Mas esses dados mostram que o público de professores está atento ao uso de ferramentas que promovam atividades lúdicas. Essas são abordagem que são cobradas pelo estado de Pernambuco por meio dos PCN, e formações continuadas. Por acreditarem que, por meio dos jogos é possível promover a aprendizagem do estudante de forma divertida.

Dalarmi (2013) realizou uma pesquisa semelhante a este questionário, com o objetivo de levantar as possíveis dificuldades pelos professores no uso de jogos em sala de aula. Os questionários foram aplicados a um público de 20 professores do ensino médio e fundamental. Os dados revelam que em relação ao uso de jogos em sala de aula: apesar de todos assumirem o uso, 67% dos profissionais raramente utilizam esta ferramenta; 57% acredita que o interesse do estudante pela disciplina aumenta; 58% conseguem identificar as dificuldades dos estudantes com a disciplina, durante as jogadas; 92% acreditam que existe uma melhoria na aprendizagem dos alunos.

Apesar de serem aplicados em local e tempos diferentes, os resultados não são divergentes, os profissionais utilizam os jogos e acreditam neles como ferramentas que auxiliam no ensino aprendizagem do estudante.

Geralmente o uso de tecnologia e jogos gera um ambiente onde a aprendizagem ocorre por descoberta, os estudantes são agentes ativos no processo de

ensino/aprendizagem, se bem planejado, os conceitos estudados em sala de aula, podem ser assimilados de forma significativa.

A próxima questão estava relacionada a identificar quanto ao uso de jogos sem tecnologias, na qual 66% afirmam utilizar jogos sem tecnologias, os demais utilizam apenas jogos eletrônicos. Dentre os jogos, citados estão o tangram, dominós, baralhos, desafios, jogos de cartas e bingo.

De acordo, com esses dados, permite inferir que o jogo Caça ao Tesouro pode ser uma ferramenta aceita pelos professores, uma vez que, se trata de um jogo que pode ser utilizado com tecnologia ou não. Além disso, pode ser adaptado para ser utilizada em qualquer disciplina, pode assim, profissionais realizarem um trabalho em conjunto, como uma atividade interdisciplinar.

3.3.1 **Caça ao tesouro**

O jogo Caça ao Tesouro, foi criado com objetivo de estimular a aprendizagem de matemática de forma divertia, além disso, sua estrutura foi pensada com a preocupação de deixar o mais próximo possível da realidade do uso de criptografias com a ideia de proteção de informações sigilosas.

Espera-se que durante o jogo, o estudante seja capaz de aplicar os conhecimentos abordados durante as aulas, neste âmbito se trata de uma ferramenta de auxilio na fixação dos conceitos estudados.

Para a realização do jogo, pensou-se em um cenário que pode ser criado na imaginação da criança, influenciada pelos nomes dados ao ambiente. Geralmente o ambiente físico a ser utilizado é a escola, onde a sala de aula recebe o nome de *Bletchley Park* , esse nome é em homenagem ao local onde o matemático Alan Turing decifrou a Enigma durante a Segunda Guerra Mundial na Inglaterra.

Na sala de aula, os estudantes devem ser divididos em grupos, na qual cada um será uma agencia secreta, para identifica-los os grupos podem receber nomes que podem ser escolhidos pelos próprios integrantes. Em cada agência, deve ser indicado quem será o líder, os criptógrafos e criptoanalistas. O líder será o intermediário entre o juiz (professor) e sua agencia secreta. As regras do jogo se encontram no apêndice H,

na qual cada equipe recebe uma cópia e antes do inicio do jogo, o juiz faz uma leitura para todas as agencias, sanando as dúvidas antes das jogadas começarem.

O objetivo principal do jogo é encontrar um tesouro perdido, para isso, as agências vão à busca de pergaminhos direcionando-os, a cada pergaminho seguinte. O jogo finaliza quando uma das equipes encontrar o tesouro. No entanto, para conseguir realizar a leitura da mensagem contida em cada pergaminho, os agentes devem decifrar a mensagem e por meio dela, tentar identificar onde encontrar o próximo pergaminho.

Como já se sabe, para decifrar a mensagem é necessário conhecer a cifra utilizada e a chave. Com isso, em cada pergaminho estar especificada a cifra que foi utilizada, por outro lado, a chave é a solução de uma questão de matemática solucionada no *Bletchley Park.* Isto é, o jogo inicia com uma questão relacionada ao conteúdo que se deseja revisar, a solução será a chave para decifrar o pergaminho.

Cada pergaminho foi produzido em quantidade igual ao das equipes, assim o Juiz inicia o jogo, entregando para cada líder o pergaminho referente à primeira pista, que vai informar onde estar localizado o pergaminho 2.

Por outro lado, cada agencia só pode sair do *Bletchley Park* , quando encontrar a solução da questão que contém a chave para a leitura do pergaminho dois. Em busca de cada pergaminho, só foi permitido sair dois integrantes, a fim de evitar muitas aglomerações na escola, evitando atrapalhar as demais aulas.

Enquanto os agentes estão procurando o pergaminho, o juiz já expõe na lousa a questão que contem a chave do pergaminho três, assim as agencias vão tentando solucionar enquanto chega à informação com a localização encontrada.

A primeira equipe que encontrar o pergaminho retorna para sua agencia onde deverão ler a mensagem. Após a leitura e em posse da chave do pergaminho 3, a agencia deve enviar dois agentes em busca da nova pista, no entanto, não poderão ser os mesmos da jogada anterior, ou seja, a dois estudantes, nunca vão em busca de um pergaminho em jogadas consecutivas.

Cada agência dispõe de um computador com o programa de criptografia que foi criado especialmente para ser utilizado neste jogo. Assim, veja que a informação da localização que chega ao *Bletchley Park* é uma mensagem cifrada que pode ser lida

com a ajuda do programa. Essas jogadas se repetem até encontrar o ultimo pergaminho.

Note que se trata de um jogo interativo, onde todos participam das jogadas permitindo uma interação dentro das equipes. O que chama a atenção na aplicação do jogo é à participação voluntária de todos e o companheirismo, aqueles que apresentavam mais dificuldades para cifrar e aplicar os conceitos estudados participava de discussões com os colegas que apresentavam mais habilidades, gerando uma zona de desenvolvimento proximal, entre os integrantes das equipes.

No dia, da aplicação do jogo, foi realizada uma discussão inicial sobre a importância do Rio São Francisco para as cidades de Juazeiro-BA e Petrolina-PE, com isso, pensou-se em elaborar os pergaminhos com mensagens que reflitam a discussão realizada sobre os impactos ambientais sofridos pelo rio.

O pergaminho um (Apêndice H), foi entregue pelo juiz a cada equipe, como uma forma de iniciar o jogo. A chave para decifrar, é a solução da seguinte questão: "*A chave é o número natural que ao ser dividido por 7 resulta um quociente 4 e resto o maior possível". Cuja solução é: Pela divisão euclidiana se um inteiro a for dividido por um inteiro b, então existem* $q, r \in \mathbb{Z}$ *tal que,* $a = bq + r$ *com* $0 \leq r \leq b-1$*. Daí, o problema pode ser escrito na divisão euclidiana como* $chave = 7 \cdot 4 + 6 = 34$*, isto é, a chave é o dividendo, gerado pelo divisor 7, quociente 4 e o maior resto possível igual a 6. Portanto, a chave é igual a 34.*

Os estudantes não apresentaram dificuldades em solucionar esta questão, de tal forma, todas as equipes foram em busca do pergaminho dois, em intervalos de tempo bem pequenos.

No pergaminho dois (Apêndice I), a cifra a ser utilizada também é a de César, na qual a chave está na solução da questão de enunciado: "*O ano de 2014 começou em uma quarta-feira. Em que dia da semana cairá o último dia deste ano?"* (DUTENHEFNER, CADAR, 2016, p. 34). Para solucionar o juiz deu a dica de quê o ano deve conter 365 dias e a chave será a quantidade de letras do dia da semana.

Neste problema, devem-se distribuir os dias do ano, nos dias da semana para compor as semanas e os meses, desta forma, tem-se uma divisão em grupos. È Como se a semana fosse uma escola de sete salas (sete dias). Em cada sala existe um

representante de turma, representados pelos sete primeiros dias, como 2014 inicia na quarta-feira, termos a distribuição a seguir.

Tabela 14: Distribuição dos primeiros dias do ano.

D	S	T	Q	Q	S	S
5	6	7	1	2	3	4

Fonte: Próprio autor

Logo, cada líder são os possíveis restos na divisão por sete. Lembre-se que, no caso da divisão ser exata o resto é igual a zero e diz-se que o dividendo é múltiplo do divisor, logo a terça-feira representa o resto zero. Como são sete grupos, então pela divisão euclidiana $365 = 7 \cdot 52 + 1$, como o resto é 1, podemos concluir que o estudante 365 frequenta a sala do líder 1, portanto, se o ano é de 365 dias, e iniciou na quarta-feira, então o ultimo dia, também será em uma quarta-feira.

Nesta questão, uma equipe não conseguiu encontrar a solução, o que gerou uma preocupação, visto que, apesar do jogo ser um instrumento capaz de manter o foco do aluno, estimulando a participar das jogadas até o final, movido pela tensão do jogo e pelas mudanças de fase que transmite a ideia de ser capaz de enfrentar os desafios de cada nível, tem o problema, das tentativas frustradas em mudar de níveis durante um jogo, levar a desistência pelo jogador (LIMA, 2008).

Com isso, foi importante a intervenção do professor, ao realizar uma revisão com os estudantes deste grupo, enquanto os demais estavam em busca dos pergaminhos. Esta foi uma forma de manter a equipe no jogo, pois uma vez, que não conseguissem solucionar os problemas, poderia resultar na desistência em participar das atividades, por se considerarem incapazes de competir.

O Pergaminho três (Apêndice J), com mensagem escrita com a cifra afim, possui sua chave na solução do problema. “*A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118 ?*” encontrada no Banco de questões de 2010 da Olímpiada Brasileira das Escolas Públicas.

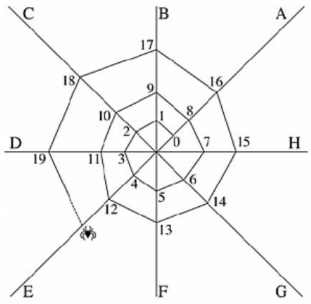


Figura 17: Ilustração do enunciado usado para solucionar o problema.
Fonte: Banco de questões de 2010 da OBMEP.

A chave é a decomposição prima do primeiro número do fio de apoio que será solução do problema. Para tanto, Observe que a aranha começa a tecer do fio de apoio A e vai até o fio de apoio H, assim retornando para o A logo em seguida, repedindo o ciclo. Considerando que cada fio de apoio seja uma sala de aula, e em cada uma delas a aranha deixa um estudante, então no primeiro ciclo a aranha colocou o estudante zero na sala A, o estudante um na sala B, o estudante dois na sala C e assim sucessivamente.

Desta forma, veja que existem oito salas de aula representadas pelas letras de A até H e lideres de turma respectivamente de 0 a 7, assim para saber onde o estudante 118 vai ficar, deve-se dividir este número pelo total de salas, logo tem-se $118 = 8 \cdot 14 + 6$, assim, o estudante 118 ficará na sala G, cujo líder de turma é o 6.

Para definir a chave, veja que o líder da turma será o valor escolhido, já que é o primeiro número no fio G, logo, decompondo obtêm-se $6 = 2 \cdot 3$. Por se tratar, da cifra afim, sabe-se que é necessário duas senhas, daí os candidatos são os números 2 e 3, por outro lado, não foi informado quem será a senha *a* e *b,* para identificar o estudante deve se recordar quais as restrições de cada senha. A conclusão obtida será que, o 2, só poderá ser a senha de *b,* uma vez que, $mdc(2,26) = 2 \neq 1$, portanto as senhas serão $a = 3$ e $b = 2$, tal que $mdc(3,26) = 1$.

Pergaminho quatro (Apêndice K), considerado o ultimo pergaminho, estava cifrada sob a cifra de Hill. A chave para decifrar a mensagem estava na solução da seguinte questão.

“Estrelix, um habitante de Geometrix, decidiu colocar os inteiros positivos seguindo a disposição indicada na figura. Em quais estrelas aparece o número 2011? Posicione

todos os números que aparecem nas referidas estrelas." (DUTENHEFNER, CADAR, 2016, p. 36)

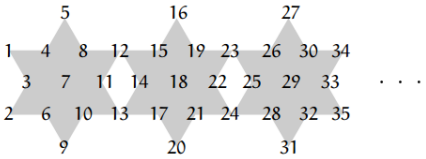


Figura 18: Ilustração do enunciado da questão, considera necessária para resolução.
Fonte: (DUTENHEFNER, CADAR, 2016, p. 36)

A chave para decifrar é 2X11, tal que $\mathrm{X} = \text{A posição do número } 2011$. Para solucionar Separe as estrelas deixando os números compartilhados sempre na estrela à direita. Fazendo isto, como indicado na figura a seguir, vemos que em cada estrela ficam escritos 11 números.

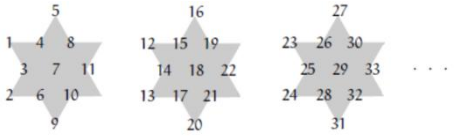


Figura 19: Ilustração para solução.
Fonte: (DUTENHEFNER, CADAR, 2016, p. 36)

Imagine que 2011 seja a quantidade de pessoas de um grupo formado apenas por professores, e precisamos distribuir os professores colocando um em cada sala nas diversas escolas, desta forma, cada estrela é uma escola e os números de 1 a 11 são as salas de aula de cada escola. Temos um grupo de professores que ficarão sempre na primeira sala de cada escola, são eles os professores $\{1,12,23,\cdots\}$, o mesmo acontece com a sala dois, representada por $\{2,13,24,\cdots\}$ e assim sucessivamente.

Considerando que os professores de 1 a 11, são os representantes de cada grupo, como foi discutido no organizador prévio, basta fazer $2011 = 11 \cdot 182 + 9$, logo o professor 2011 ficará na sala referente ao grupo que contém o líder 9, portanto, a sala 9 da escola. Além disso, veja que faltam duas unidades para a divisão por 11 ser exata e dar quociente 183, isso porque a sala nove esta na escola 183 e se continuarmos contanto, completamos esta escola. Portanto, a solução para a senha é x=9.

Para esta questão, a dificuldade dos estudantes foi em separar as estrelas como foi sugerido na solução, sendo desta forma, o problema que exigiu mais tempo da atividade. Houve a necessidade de o professor sugerir a separação das estrelas, após a sugestão os estudantes começaram a estabelecer estratégias para solução. Outra

dica dada foi que eles tentassem analisar semelhanças entre as duas questões anteriores. Após um intervalo de tempo, apenas duas equipes encontraram a solução e um delas foi à vencedora.

Apesar da proposta está direcionada ao ensino da matemática, ao interagir com o tema transversal meio ambiente, além de ser, uma exigência dos PCN, foi uma forma de mostrar que o Caça ao Tesouro, pode ser adaptado a qualquer disciplina. Bastam modificar as mensagens dos pergaminhos que podem ser feitas facilmente com a ajuda do programa de criptografia e as questões com as soluções das chaves podem ser substituídas, por aquelas direcionadas a disciplina.

Com o objetivo de avaliar a eficiência do jogo, além da observação realizada pelo professor, aplicou-se um questionário, cujo modelo se encontra no apêndice E. A primeira questão pergunta se o estudante considera o jogo Caça ao Tesouro um jogo, chato, cansativo, divertido ou estimulante.

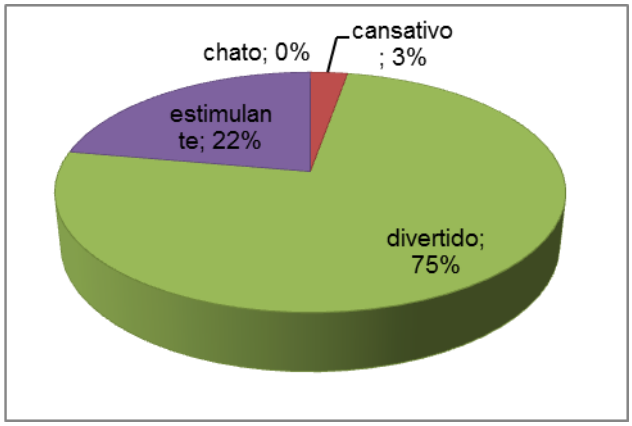


Gráfico 10: Opinião dos estudantes quanto ao jogo Caça ao Tesouro.
Fonte: Próprio autor.

Veja que, 87% dos estudantes demonstraram uma boa aceitação do jogo, de tal forma que 75%, afirma ser um jogo divertido e 22% considera estimulante. Esta é uma característica fundamental dos jogos, a participação voluntária é estimulada pelo prazer sentido em participar do jogo. Este prazer pode ser estimulado pelos desafios apresentados durante o jogo e pela sensação de ser capaz de competir (LIMA, 2008).

A segunda questão tem como objetivo identificar na opinião dos estudantes quanto à dificuldade presentes nas criptografias dos pergaminhos.

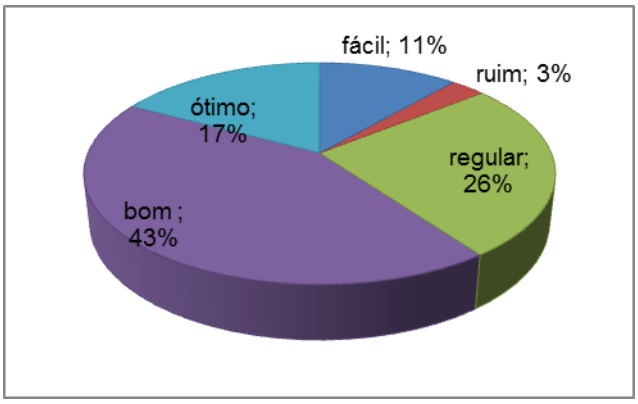


Gráfico 11: Opinião dos estudantes quanto ao nível de dificuldade do jogo Caça ao Tesouro.
Fonte: Próprio autor.

Estes resultados permitem analisar que a forma como foi apresentada as criptografias nos pergaminhos 11% consideraram fácil, o ótimo e o bom, são níveis em que os estudantes conseguem decifrar, no entanto, apresentam algumas dificultadas ou precisam de mais tempo para decifrar. Apenas 29% dos estudantes afirmaram ser ou ruim ou regular.

Lembrando que, se o professor de outra disciplina decidir utilizar do jogo como auxilio na revisão de seus conteúdos, mas não apresentar para o estudante os conceitos de criptografia, o interessante é utilizar o programa como ferramenta do jogo, optando pelas cifras mais simples. Mas, fazendo uma exposição bem geral de como ocorre o processo da escolha da chave. Caso, contrário o estudante não consegue participar do jogo, levando-o a desistência e recusa em fazer parte da atividade.

A terceira questão tem como objetivo identificar na opinião do estudante se ele considera um jogo, na qual foi capaz de aprender mais sobre o conteúdo trabalhado, ou seja, se facilitou a assimilação dos conceitos durante a experiência.

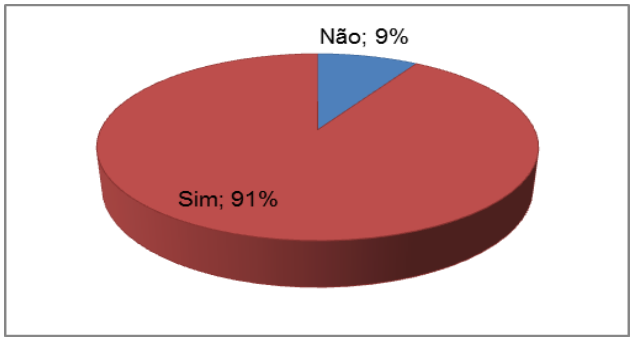


Gráfico 12: Opinião dos estudantes quanto a contribuição do jogo na sua aprendizagem.
Fonte: Próprio autor.

Identificar se houve algum tipo de aprendizagem na aplicação do jogo, é uma forma de avaliar se é possível considera-lo um jogo educativo ou não. Durante as jogadas, a observação na interação dos estudantes, permitiu perceber nas equipes com oito estudantes cerca de 4 a 5 integrantes dominavam o conceito, e os demais apresentavam dificuldades distintas, alguns durante as cifras outros durante as soluções das questões.

No entanto, a aprendizagem não ocorre apenas quando o aluno chega a um resultado correto, a partir do momento que estudante consegue chegar a uma tese, o professor deve ajuda-lo a identificar se é válida ou não, sendo válido ótimo, não sendo válido ótimo também, uma vez que, agora o estudo e análise serão sobre o erro que tornou a tese inválida até torna-la válida.

A ultima questão tem como objetivo identificar se as regras do jogo estão bem definidas e claras para os estudantes.

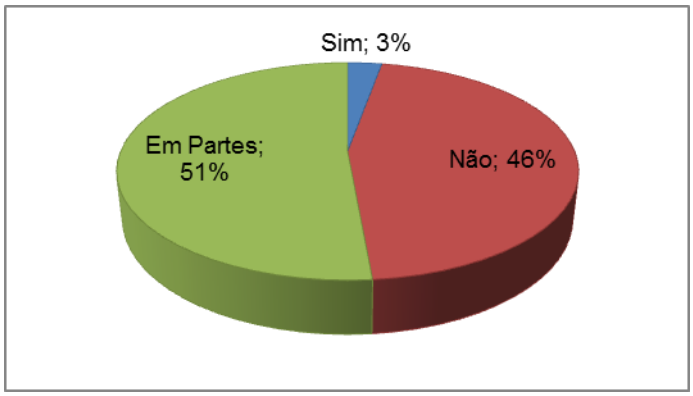


Gráfico 13: Resultado da questão 4, do questionário (apêndice G)
Fonte: Próprio autor.

Perguntava-se: “*Você sentiu dificuldades em compreender as regras do Jogo?*”, assim, o resultado obtido foi que apenas 3% sentiram dificuldades, essa dificuldade pode ter sido gerada pela falta de leitura as regras, ou pela falta de atenção durante as explicações. O que permite inferir estes fatores é a afirmação de mais de 90% dos estudantes em que compreenderam as regras.

Desta forma, estes dados permitem concluir que o jogo quando bem planejado oferece várias possibilidades, uma vez que, o próprio estudante é quem realiza os cálculos, já que, encontrar o resultado é fundamental para progredir no jogo,

desenvolvendo assim a autonomia, já que, são eles que levantam hipótese, testam os cálculos e chegam a uma tese.

Além disso, gera uma aprendizagem significativa, já que geralmente é utilizado como revisão de conteúdos, e os jogos que são aplicados no inicio como um gerador de problema a ser discutido, dependendo da abordagem pode ser visto como um organizador prévio, e da mesma forma gerar um ambiente de aprendizagem significativa.

CAPÍTULO 5

CONSIDERAÇÕES FINAIS

Os baixos índices do IDEB sobre o desempenho dos estudantes do ensino fundamental em matemática refletem as dificuldades encontradas pelo sistema de ensino em promover uma oferta que atenda as necessidades e expectativas do público atual.

Dentre as possíveis falhas da educação básica, a BNCC enfatiza a falta de conexão entre as etapas de ensino. Salientando que o ensino aprendizagem deve ser visto como um processo contínuo, sendo necessário que os currículos e práticas pedagógicas dos anos iniciais e finais do ensino fundamental estejam conectados, de forma que esses profissionais se conversem, isto é, o professor dos anos iniciais e o professor dos anos finais, ambos devem definir em conjunto o produto final que se deseja obter, ou seja, que perfil de estudante os anos iniciais devem moldar para que possa chegar aos anos finais com a base necessária.

A título de exemplo, o estudo da divisão euclidiana esta presente no currículo dos anos iniciais, no 6º ano quando tratado de números naturais e no 7º ano quando tratado dos números inteiros. No entanto, os dados desta pesquisa permitiu inferir que os conceitos de divisão são sempre tratados com o mesmo olhar. Dividir objetos em quantidades iguais, ou como ferramenta para determinar números primos, divisores e no uso de frações. Tratando o resto apenas como uma sobra com pouca importância.

Tratar de dividir objetos em partes iguais faz parte das habilidades e competências dos anos iniciais, nos anos finais este conceito deveria ser tratado como subsunçor para abordar a divisão em um âmbito mais complexo, como em eventos cíclicos, permitindo ao estudante atribuir um significado maior ao resto da divisão.

Para isso, não basta apenas apresentar os conceitos na lousa e sugerir exercícios. É necessário que o profissional reflita suas práticas pedagógicas afim de, utilizar diversos recursos que auxiliam em um planejamento capaz de promover uma aprendizagem significativa.

A experiência com a Cifra de Hill permitiu observar que a complexidade do conteúdo depende da forma e linguagem na abordagem, uma vez que, nele foram

necessários os conceitos de matrizes e determinantes, abordados de forma que estudantes dos anos finais do ensino fundamental assimilassem os conceitos necessários para operar com determinantes. Desta forma, o subsunçor destes estudantes, estão previamente preparados para absorver os conceitos quando for tratado no ensino médio.

As ferramentas utilizadas, como o programa de criptografia e o jogo Caça ao Tesouro foram de grande contribuição na assimilação destes conceitos, já que, motivaram os estudantes a participarem de forma voluntária e instigou a curiosidade em aprender.

Por outro lado, é importante salientar que não se trata de uma tarefa fácil, são muitos os obstáculos descritos pelos professores em levar para sala de aula, atividades mais interativas e que motivem a aprendizagem. Dentre elas, existe a falta ou quantidade insuficiente de recursos pedagógicos na escola. Assim, o sistema de ensino que tanto almeja o aumento dos índices de desempenho precisa dar subsídios aos seus profissionais para que exerçam sua função com êxito.

Logo, o sistema deve enviar para suas escolas recursos tecnológico e materiais concretos que fortaleçam o trabalho do professor, no entanto, deve atender a quantidade de estudantes de cada escola. Além disso, é necessário realizar uma formação com os educadores, a fim de orientá-los quanto ao uso dos materiais discutindo como avaliar o estudante durante o uso desses recursos.

Contudo, a proposta desta pesquisa permite que o educador utilize de um recurso que não exigirá tantos investimentos, mas um pouco de tempo para planejar sua aula e adaptar ao jogo Caça ao Tesouro.

O Caça ao Tesouro foi criado com o objetivo de estudar a matemática de forma divertida, permitindo que os estudantes simulassem o trabalho de agentes secretos em agências de espionagem, dentre os quais, 75% consideraram a atividade divertida e 91% afirmaram ter contribuído na sua aprendizagem durante o curso.

Portanto, sair em busca de um tesouro perdido foi realmente uma grande diversão para os sujeitos desta pesquisa, que de forma prazerosa assimilaram conceitos de aritmética modular e álgebra linear como algo necessário para desempenhar com êxito as tarefas do jogo, se tornando o vencedor.

Com isso, a complexidade dos conteúdos e as dificuldades em assimilar os conceitos são consequências das práticas pedagógicas, que são influenciadas pela valorização do profissional, e os investimentos em recursos pedagógicos que auxiliem os educadores.

REFERÊNCIAS

ANDRADE, M. M. **Introdução à metodologia do trabalho científico: elaboração de trabalhos na graduação.** 10 ed. São Paulo: Atlas, 2010.

ARAGÃO, R. M. R. **Teoria da Aprendizagem significativa de David P. Ausubel: sistematização dos aspectos teóricos fundamentais.** 1976. Dissertação de doutorado em Educação. Universidade Estadual de Campinas. Disponível em: < http://www.reposip.unicamp.br/xmlui/bitstream/handle/REPOSIP/253230/Aragao_RosaliaMariaRibeirode_D.pdf?sequence=1&isAllowed=y>. Acesso em: 23 de maio de 2017.

ANTON, H; RORRES, C. **Álgebra Linear com aplicações.** Tradução Claus Ivo Doering. 8.ed. Porto Alegre: Bookman, 2001.

BORBA, M. C; PENTEADO, M. G. **Informática e Educação Matemática**. 5.ed. Belo Horizonte: Autêntica Editora, 2012.

BRASIL, **Lei de Diretrizes e B. Lei nº 9.394/96, de 20 de dezembro de 1996**.

BRASIL, Secretaria de Educação Fundamental**. Parâmetros curriculares nacionais: matemática.** Brasília: MEC/SEF, 1997.

_____, Secretaria de Educação do Estado de Pernambuco. **Parâmetros para Educação Básica do Estado de Pernambuco.** 2012.

_____, Ministério da Educação. Secretaria de Educação Básica. Diretoria de Currículos e Educação Integral. **Diretrizes Curriculares Nacionais Gerais da Educação Básica**. Brasília:MEC, SEB, DICEI, 2013.

_____. Ministério da Educação. **Base Nacional Comum Curricular**. Proposta preliminar. Terceira versão revista. Brasília: MEC, 2017. Disponívelem:<http://basenacional comum.mec.gov.br/images/BNCC_publicacao.pdf> . Acesso em: 18 jun. 2017.

CARVALHO, L. R. **Uso de elementos da criptografia como estímulo matemático na sala de aula.** 2016. 78 f. Dissertação-(Mestrado Profissional em Matemática em Rede Nacional)-Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas. Rio Claro-SP, 2016.

CAYLEY, A. **A Memoir on the Theory of Matrices.** Philosophical Transactions of the Royal Society of London. Londo: Royal Society. Vol 148, 1858. pp 17-37. Disponível em:< http://www.jstor.org/stable/108649>. Acesso em: 21 maio 2017.

COSTA, S. S. C; MOREIRA, M. A. **A resolução de problemas como um tipo especial de aprendizagem significativa.** Caderno Brasileiro de Ensino de Física. Universidade de São Carlos. v. 18, n. 13. P. 263-277, 2001. Disponível em:< https://periodicos.ufsc.br/index.php/fisica/article/view/6663/19039>. Acesso em: 4 de maio de 2017.

COUTINHO, S. C. **Números inteiros e Criptografia RSA**. Rio de Janeiro, IMPA, 2014.

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

CRUZ, Edilson Fernandes da. **A criptografia e seu papel na segurança da informação e das comunicações (sic) – retrospectiva, atualidade e perspectiva.** 2009. 84 f. Monografia-(Especialização em Gestão de Segurança da Informação e Comunicações)-Instituto de Ciências Exatas, Universidade de Brasília.

DALARMI, T. T. **O uso de jogos nas aulas de matemática**. Encontro Nacional de Educação Matemática – ENEM, Curitiba-PR, jul 2013.
DANZIGER, M.; HENRIQUES, M. A. A. **Computational Intelligence Applied on Cryptology: a Brief Review**. IEEE Latin America Transactions, vol. 10, nº 3, abr 2012.

DOMINGUES, H.; IEZZI, G. **Álgebra Moderna: volume único.** 4 ed. Reform. São Paulo: Atual 2003.

DUTENHEFNER, F; CADAR, L. **Encontros de Aritmética**. Rio de Janeiro: IMPA, 2016.
ELLIS, Claire. **Exploring the Enigma**. Plus magazine: 2005. Disponível em: <https://plus.maths.org/content/os/issue34/features/ellis/index >. Acesso em 19 de jan. de 2017.

EVES, H. **Introdução à história da matemática.** Tradução: Hygino H. Domingues Campinas, SP: Editora da Unicamp, 2004.

FALEIRO, A. C. **Criptografia.** Notas em Matemática Aplicada. v.52. São Carlos-SP:SBMAC, 2011, 138p.

FINO, C. N. **Vygotsky e a Zona de desenvolvimento proximal (ZDP): três implicações pedagógicas.** Revista portuguesa de Educação. Universidade do Minho. v. 14. n. 02, pp. 273-291. set./dez. 2001.Disponível em: < http://www3.uma.pt/carlosfino/publicacoes/11.pdf>. Acesso em: 23 de maio de 2017.

GIL, A. C. **Métodos e técnicas de pesquisa social.** 6 ed. São Paulo: Atlas, 2008.

GONÇALVES, A. **Introdução a álgebra.** 5 ed. Rio de Janeiro: IMPA, 2011.

GRANDO, R. C. **O conhecimento matemático e o uso de jogos na sala de aula.** 2000. Tese de doutorado - Universidade de Campinas, Campinas-SP, 2000.

HEFEZ, A. FERNANDEZ, C. S. **Introdução a Álgebra Linear.** Rio de Janeiro: SBM, 2012.

HEFEZ, A**. Aritmética**. SBM: Rio de Janeiro, 2014.

JESUS, A. L. N. **Criptografia na educação básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes**. 2013. 70 f. Dissertação-(Mestrado Profissional em Matemática em Rede Nacional)-Universidade Federal do Vale do São Francisco, campus Juazeiro. Juazeiro-BA, 2013.

KOLMAN. B; HILL, D.R. **Introdução à álgebra linear: com aplicações**. Tradução Alessandra Bosquilha; revisão técnica Rafael José Iorio Júnior. Rio de Janeiro: LTC, 2006.

LAKATOS, E. M; MARCONI, M. A. **Fundamentos de Metodologia Científica**. 5 ed. São Paulo: Atlas, 2003.

LIMA, J. M. **O jogo como recurso pedagógico no contexto educacional.** São Paulo: Cultura Acadêmica: Universidade Estadual de Paulista, Pró reitoria de Educação, 2008.
MALAGUTTI, P. Atividades de contagem a partir da criptografia. Rio de Janeiro, IMPA, 2015. 77p.

LIMA, G. L. **Matrizes e algumas de suas aplicações.** 37 f. Trabalho de conclusão de curso. Graduação em Matemática. Universidade Estadual da Paraíba, 2011.

MALAGUTTI, P. **Atividades de contagem a partir da criptografia.** Rio de Janeiro, IMPA, 2015. 77p.

MOREIRA, C. G. T. de A.; MARTÍNEZ, F. E. B.; SALDANHA, N. C. **Tópicos de Teoria dos Números.** Rio de Janeiro:SBM, 2012.

MOREIRA, M. A. **Mapas conceituais e Aprendizagem Significativa**. 2 ed. São Paulo: EPU, 2010.

_____, M. A. **Teorias da Aprendizagem**. 2 ed. São Paulo: EPU, 2011.

PRODANOV, C. C; FREITAS, E. C. **Metodologia do Trabalho Científico: Métodos e técnicas da pesquisa e do trabalho acadêmico.** 2 ed. Novo Hamburgo: Freevale, 2013.

PROVOS, N.; HONEYMAN, P. **Hide and Seek: An Introduction to Steganography**, IEEE Security & Privacy, 1(3): 32-44, maio/junho 2003. Disponível em:<http://www.citi.umich.edu/u/provos/papers/practical.pdf>. Acesso em: 18 de janeiro de 2017.

ROQUE, T.. **História da Matemática: uma visão crítica, desfazendo mitos e lendas.** Rio de Janeiro: Zahar, 2012.

SANTOS, R. N. **Uma breve história do desenvolvimento das teorias dos determinantes e das matrizes.** 42 f. dissertação. Projeto de ensino de matemática do curso de licenciatura em Matemática. Instituto de Matemática e Estatística da Universidade de São Paulo, 2007.

SANTOS, J. M. C. T; OLIVEIRA, M. B; PAZ, S. R. (org.). **Reinvenções do Currículo: sentidos e reconfigurações no contexto escolar**. Fortaleza: Edições UFC, 2016.

SHOKRANIAN, Salahoddin. **Criptografia para iniciantes.** 2.ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

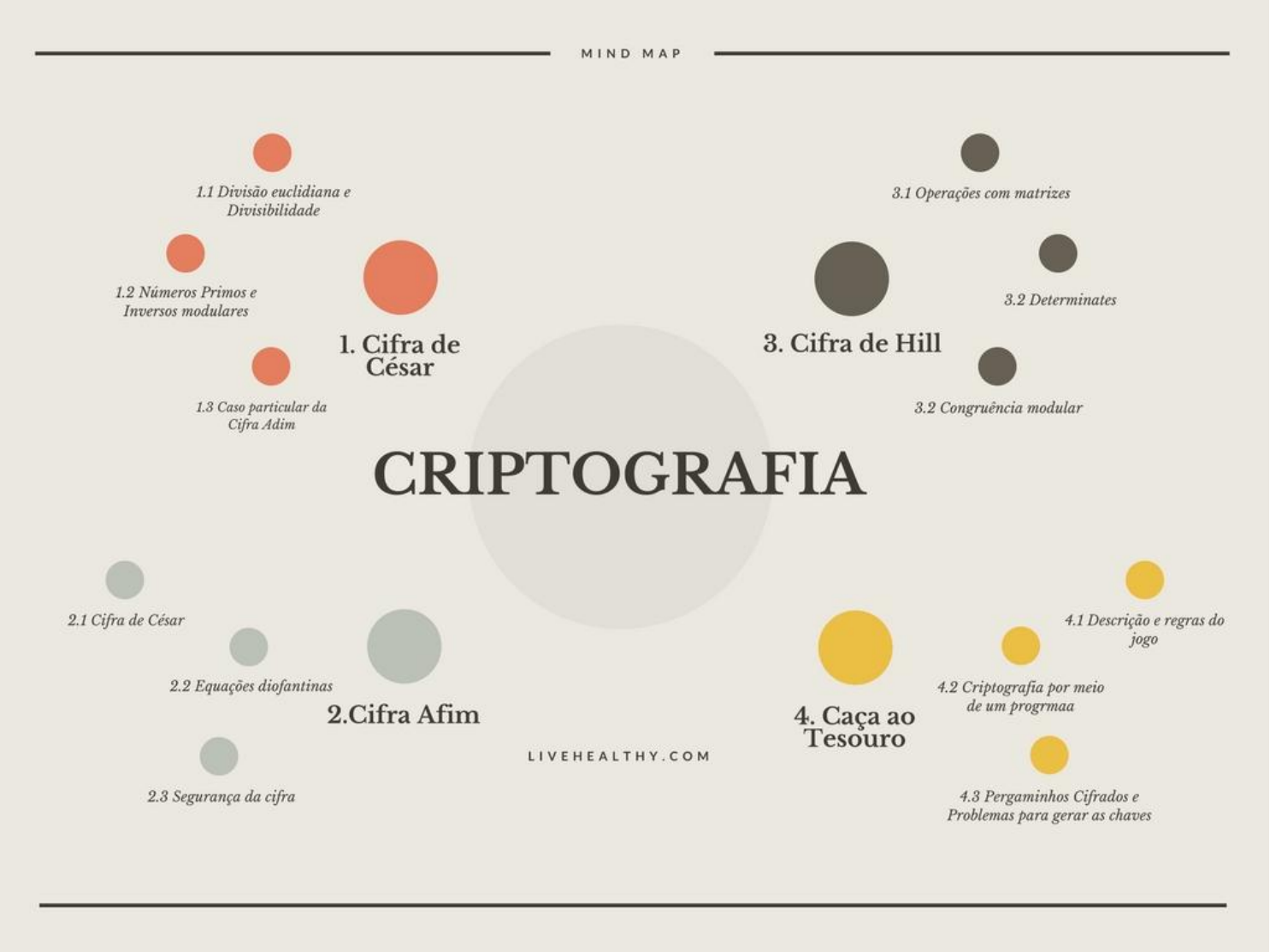
SINGH, S. **O livro dos códigos**. Tradução de Jorge Calife. 2.ed. Rio de Janeiro: Record, 2002.

SINGH, S. **O último teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos.** Tradução de Jorge Luiz Calife. 17 ed. Rio de Janeiro: Record, 2010.

STRATHERN, P. **Turing e o computador em 90 minutos**. Traduzido por Mara Luiza X. de A. Borges. Jorge Zahar Editor. 2000.

VENTURA, M. M. **O Estudo de Caso como Modalidade de Pesquisa**. Revista da SOCERj. Rio de Janeiro, 382-386 p. 2007. Disponível em: < http://www.rbconline.org.br/wp-content/uploads/a2007_v20_n05_art10.pdf> . Acesso em: 20 jun 2017.

APÊNDICE A – Mapa mental



APÊNDICE B - Questionário A (Pesquisa de Opinião)

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

Desde já, agradeço pela sua colaboração em oferecer informações por meio deste questionário.

Pesquisa de Opinião

Idade:_____
Nome de sua escola:_____
Série/ano:_____

01. **Você gosta de estudar matemática:** ( )SIM ( ) NÃO
02. **Na sua escola possui laboratório de informática?** ( )SIM ( ) NÃO
03. **Você já assistiu alguma aula no laboratório de informática de sua escola?**
( ) SIM
( ) NÃO
( ) MINHA ESCOLA NÃO POSSUI LABORATÓRIO DE INFORMÁTICA
04. **Qual o nome da disciplina do professor que levou a sua turma para assistir uma aula no laboratório de informática?**
Nome da disciplina:_____
( ) MINHA ESCOLA NÃO POSSUI LABORATÓRIO DE INFORMÁTICA
05. **Alguma vez o seu professor utilizou jogos na sala de aula, como reforço de algum conteúdo?**
( ) SIM Nome da disciplina do professor:_____
( ) NÃO
06. **Você conhece algum tipo de jogo, na qual é necessário o conhecimento de conteúdos da matemática para realizar as jogadas?**
( ) SIM Nome do conteúdo:_____
( ) NÃO
07. **Você costuma praticar algum tipo de jogo?**
( ) SIM
( ) NÃO

Por que, você pratica este jogo?

_____
_____
_____

08. **Você sabe o que é criptografia?**
( ) SIM
Descreva o que é criptografia:_____
_____
_____

( ) NÃO

APÊNDICE C – Questionário de sondagem

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

Avaliação de Sondagem

Idade:_____
Nome: _____
Série/ano:_____

1. Em uma divisão exata, o quociente é 13 e o divisor é 51. Qual é o dividendo?

2. Em uma divisão exata, o dividendo é 3302 e o quociente é 13. Qual é o divisor?

3. Pensei em um número, multipliquei-o por 17 e obtive 1836. Em qual número eu pensei?

4. Em uma divisão, o divisor é 13, o quociente é 8 e o resto é 6. Qual é o dividendo?

5. Em uma divisão, o dividendo é 78, o quociente é 5 e o resto é 3. Qual é o divisor?

6. Em uma divisão não exata, o divisor é 5. Quais são os possíveis restos?

7. Determine o número que, dividido por 26, tem quociente 18 e o menor resto possível.

APÊNDICE D – Atividade Cifra de César

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

CIFRA DE CESAR

1. Quais os valores que b pode assumir?

2. Quais os valores que a pode assumir?

3. Quando a = b, pode se afirmar que a cifra volta a ser um caso particular, ou seja, a Cifra de Júlio César?

4. Existem quantas chaves possíveis na Cifra Afim?

5. Escolha um amigo na sala e envie uma mensagem com a cifra afim. Descreva qual/quais a(s) chave(s) você escolheu.

APÊNDICE E – Pesquisa de opinião dos docentes

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

Desde já, agradeço pela sua colaboração em oferecer informações por meio deste questionário.

1.Sexo: ( ) feminino ( ) masculino

2.Idade: marque um x se sua idade for:
( ) 18 ou menor que 20;
( ) 20 ou menor que 25;
( ) 25 ou menor que 30;
( ) 30 ou menor que 35;
( ) 35 ou mais.

3.Há quanto tempo atua em sala de aula como professor?
( ) menos de 1 ano;
( ) mais de 1 ano e menos de 2 anos;
( ) mais de 2 anos e menos de 4 anos;
( ) mais de 4 anos menos de 6 anos;
( ) mais de 6 anos;

4.Quais as disciplinas você já lecionou? Descreva todas, se possível.
_____
_____
_____
_____

5.Marque a alternativa que melhor represente a sua formação.
Se necessário marque mais de uma alternativa.
( ) Licenciado em Matemática;
( ) Bacharelado em Matemática;
( ) Licenciado ou Bacharelado em outra área.
Qual?_____
( ) Especialização (Pós –graduação lato sensu)
Qual?_____
( ) Mestrado.
Qual?_____
( ) Doutorado.
Qual?_____

6.Já finalizou algum curso de ensino superior?
( ) Sim. Quando (ano)?_____
( ) Não.
( ) Não, e estou cursando.
Qual o ano de previsão de termino?_____

7.Já finalizou algum curso de pós - graduação?
( ) Sim. Quando (ano)?_____
( ) Não.
( ) Não, e estou cursando.
Qual o ano de previsão de termino?_____

8.Já finalizou algum curso de doutorado?
( ) Sim. Quando (ano)?_____
( ) Não.
( ) Não, e estou cursando.
Qual o ano de previsão de termino?_____

9.Você é professor(a) efetivo(a) em alguma escola pública?
( ) não
( ) Sim ⟶ ( ) da rede estadual ( ) da rede municipal ( ) da rede federal Ano de íncio?_____

10.Você já atuou ou atua como professor(a) contratado(a) na rede pública?
( ) Já atuei. Durante quanto tempo?_____ Desde qual ano? _____
( ) Nunca.
( ) Estou atuando. Desde quando?_____

11.Nesta escola, você é professor contratado ou efetivo?
( ) Contratado
( ) efetivo

12.Além dessa escola, você é professor em outro lugar?
( ) Não
( ) Sim. ( ) Contratado ( ) efetivo

Se atua em mais lugares, descreva sua situação. (descreva se a instituição é pública ou privada; atua como apoio secretariado, monitor em algum curso etc.)

_____
_____
_____

13.Nas suas aulas de matemática, você utiliza a tecnologia como recurso pedagógico?

( ) Não, pois não sei manuseá-los.
( ) Não. Demanda muito tempo de planejamento.
( ) Não, pois não possui tecnologias disponíveis para a sala de aula.
( ) Sim, raramente.
( ) Sim, com frequência.
( ) Sim quase sempre.

→ Quais? ( ) computador ( ) Datashow ( ) tablet ( ) outros

14.Quando você utiliza tecnologia em sala de aula, é em quantidade suficiente para a turma?

( ) Não uso tecnologia!
( ) Não, apenas para o professor .
( ) Sim, em pequena quantidade.
( ) Sim, em quantidade suficiente.

15.Você costuma utilizar jogos em sala de aula, no ensino da matemática?

( ) Não, pois demanda muito tempo para aplica-los em sala de aula.
( ) Não, pois exige um planejamento exaustivo.
( ) Sim, raramente.
( ) Sim, frequentemente.

16.Você utiliza jogos SEM tecnologia?

( ) Não
( ) Sim.
Quais?_____
_____

17. **Escreva um problema aritmético na qual aborde a operação de divisão, em uma das turmas do 6º ao 9ºano.**

_____
_____
_____
_____
_____
_____

18. Faça a solução do problema do item 17.

19.Para qual turma você aplicaria este tipo de problema?

( ) 6º ano
( ) 7º ano
( ) 8º ano
( ) 9º ano

20.Entre as operações a seguir, qual você julga que seu aluno possui maior dificuldade?

( ) adição
( ) subtração
( ) divisão
( ) multiplicação

21.Você já ouviu falar em Criptografia?

( ) Não
( ) Sim

Caso, tenha respondido SIM, descreva o que é criptografia dentro da sua opinião?

_____
_____
_____
_____

22. Na sua opinião, é possível trabalhar a criptografia nas aulas de matemática?

( ) Não, pois é bastante complexo para o aluno.
( ) Não, pois eu não conheço uma forma de abordar este conceito em sala de aula.
( ) Sim, mas eu não conheço uma forma de abordar este conceito em sala de aula.
( ) Sim, e conheço uma forma de aplicar em sala de aula.

23.Caso tenha respondido SIM no item 22, descreva quais os conteúdos de matemática estão aplicados na criptografia.

_____
_____
_____

( ) Apesar de conhecer, não sei descrever os conteúdos aplicados à criptografia.

24.Você já estudou ou ouviu falar sobre aritmética dos restos ou aritmética modular?

( ) Não
( )Sim Onde?_____

25. Caso tenha respondido SIM no item 24, descreva o que é aritmética dos restos.

_____
_____
_____

26.Na sua opinião, é possível trabalhar conceitos de matrizes e determinantes com turmas do 6º ao 9º ano do ensino fundamental?

( ) Não, pois estes estudantes não possuem maturidade para assimilar estes conceitos.
( ) Não, pois não conheço uma forma de trabalhar estes conceitos com alunos com esta maturidade.
( ) Sim.

APÊNDICE F – Pesquisa de opinião Caça ao Tesouro

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

Desde já, agradeço pela sua colaboração em oferecer informações por meio deste questionário.

JOGO CAÇA AO TESOURO

Idade:_____
ALUNO:_____
Nome de sua escola:_____
Série/ano:_____

1. Você considera o jogo CAÇA AO TESOURO.
   ( ) Chato ( ) cansativo ( ) divertido ( ) estimulante
2. Você considera que a criptografia utilizada nos pergaminhos, apresentava um nível de dificuldade:
   ( ) Fácil ( ) Ruim ( ) Regular ( ) Bom ( ) Ótimo
3. Você acredita que o jogo CAÇA AO TESOURO contribuiu na sua aprendizagem?
   ( ) NÃO ( ) SIM
4. Quais as suas dificuldades durante o jogo?
   _____
   _____
   _____
5. Se você gostou do jogo, descreva por quê?
   _____
   _____
   _____
6. Você sentiu dificuldades em compreender as regras do jogo?
   ( ) SIM ( ) NÃO ( ) EM PARTES

APÊNDICE G – Descrição do jogo Caça ao Tesouro

UNIVERSIDADE FEDERAL DO VALE DO SÃO FRANCISCO - UNIVASF
NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA - NUPEMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

DESCRIÇÃO DO JOGO

A "Caça ao Tesouro" é um jogo cooperativo de estratégia e raciocínio lógico. Consiste em uma batalha entre agências de inteligências formadas por criptógrafos e criptoanalistas.

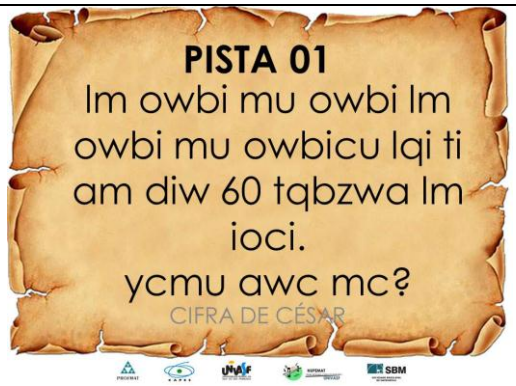
OBJETIVO DO JOGO:
Por meio de pistas criptografadas, encontrar o tesouro perdido.

CENÁRIO DO JOGO:
- **Campo de batalha**: Ambiente Escola
- ***Bletchley Park***[2]: Sala de aula
- **Agencias de inteligência**: Times

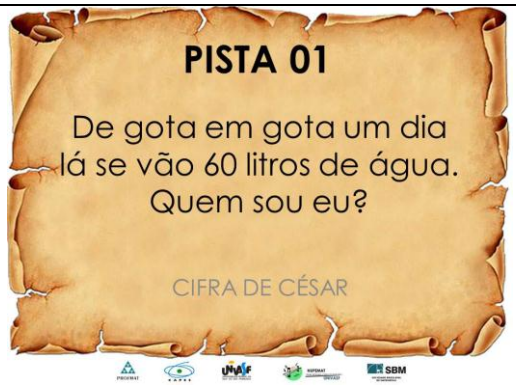
REGRAS DO JOGO:

- As agências permanecerão no *Bletchley Park*, e cada integrante só poderá sair e entrar com a autorização do juiz.
- Cada agência deverá informar quais são os criptógrafos e criptoanalistas;
- O jogo tem sete pistas criptografadas, escondidas no campo de batalha. Cada agência deverá enviar dois integrantes à procura de cada pista.
- A chave para criptografar a pista será disponibilizada por meio de uma questão de matemática apresentada no *Bletchley Park*. A chave será a solução da questão.
- A dupla que encontrar a pista deverá retornar ao *Bletchley Park* onde será decifrada mensagem.
- A quantidade de pergaminhos de cada pista e de agencias, são as mesmas, ou seja, se existem 4 equipes então vai existir quatro pergaminhos de cada pista.
- A cada pista a ser procurada, o Juiz apresentará a questão que informa a chave para decifrar a pista.
- Só é permite a saída para a procura do pergaminho, a dupla da agência que já tenha descoberto a chave para decifrar a mensagem.
- O jogo finaliza quando uma das equipes encontrar o tesouro perdido.

APÊNDICE H: Primeiro pergaminho



(a)



(b)

Figura 14: Ilustração do primeiro pergaminho: (a) Cifrado; (b) Decifrado.
Fonte: Próprio autor

Questão chave

1) A chave é o número natural que ao ser dividido por 7 resulta um quociente 4 e resto o maior possível.

SOLUÇÃO:

Pela divisão euclidiana se um inteiro a for dividido por um inteiro b, então existem $q, r \in \mathbb{Z}$ *tal que,* $a = bq + r$ *com* $0 \leq r \leq b-1$*. Daí, o problema pode ser escrito na divisão euclidiana como* $chave = 7 \cdot 4 + 6 = 34$*, isto é, a chave é o dividendo, gerado pelo divisor 7, quociente 4 e o maior resto possível igual a 6. Portanto, a chave é igual a 34.*

Fonte: Próprio autor

APÊNDICE I: Segundo pergaminho

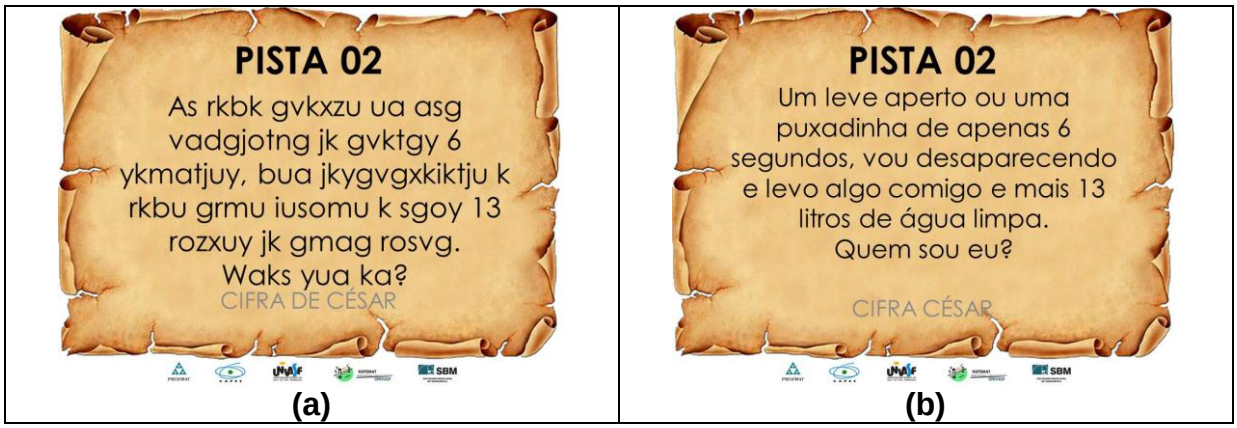


Figura 15: Ilustração do segundo pergaminho: (a) Cifrado; (b) Decifrado.
Fonte: Próprio autor

Questão chave:

O ano de 2014 começou em uma quarta-feira. Em que dia da semana cairá o último dia deste ano?
Dica: o ano tem 365 dias

CHAVE: A QUANTIDADE DE LETRAS DO DIA DA SEMANA

UMA SOLUÇÃO:

Neste problema, devemos distribuir os dias do ano, nos dias da semana para compor as semanas e os meses, desta forma, como devemos dividir nos dias da semana, então temos uma divisão em grupos.

Como a semana possui sete dias, então os sete primeiros dias, serão os representantes de cada grupo, logo como 2014 inicia na quarta-feira, termos a distribuição a seguir.

D	*S*	*T*	*Q*	*Q*	*S*	*S*
5	*6*	*7*	*1*	*2*	*3*	*4*

Logo, dada líder são os possíveis restos na divisão por sete. Lembre-se que, no caso da divisão ser exata o resto é igual a zero e dizemos que o dividendo é múltiplo do divisor, logo a terça-feira representa o resto zero.

Como são sete grupos, então pela divisão euclidiana $365 = 7 \cdot 52 + 1$ *, como o resto é 1, podemos concluir que o 365 pertence ao grupo do líder 1, portanto, se o ano é de 365 dias, e iniciou na quarta-feira, então o ultimo dia, também será em uma quarta-feira.*

Fonte: Enunciado da questão: DUTENHEFNER, F; CADAR, L. Encontros de Aritmética. Rio de Janeiro: IMPA, 2016. Solução da questão: Próprio autor.

APÊNDICE J: Terceiro pergaminho

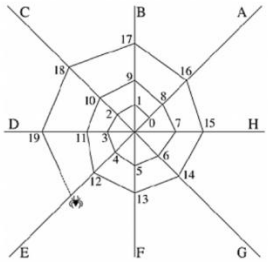
(a)

(b)

Figura 16: Ilustração do terceiro pergaminho: (a) Cifrado; (b) Decifrado.
Fonte: Próprio autor

Questão chave:

A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118 ?



CHAVE: DECOMPOSIÇÃO PRIMA DO PRIMEIRO NÚMERO DA DO FIO DE APOIO DA SOLUÇÃO.

UMA SOLUÇÃO:
Observe que a aranha começa a tecer do fio de apoio A e vai até o fio de apoio H, retornando para o A logo em seguida, repedindo o ciclo. Considerando que cada fio de apoio seja uma sala de aula, e em cada uma delas aranha deixa um estudante, então no primeiro ciclo a aranho colocou o estudante 0 na sala A, o estudante 1 na sala B, o estudante e na sala C e assim sucessivamente.

Desta forma, veja que temos oito salas de aula representadas pelas letras de A até H e lideres de turma respectivamente de 0 a 7, assim para saber onde o estudante 118 vai ficar, devemos dividir este número pelo total de salas, logo temos $118 = 8 \cdot 14 + 6$*, assim, o estudante 118 ficará na sala G, cujo líder de turma é o 6.*

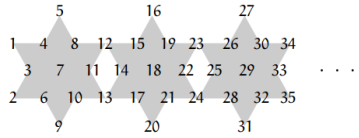
Fonte: Banco de questões 2010, da OBMEP.

APÊNDICE K: Quarto pergaminho

Figura 17: Ilustração do terceiro pergaminho: (a) Cifrado; (b) Decifrado.
Fonte: Próprio autor

Questão chave:

Estrelix, um habitante de Geometrix, decidiu colocar os inteiros positivos seguindo a disposição indicada na figura.

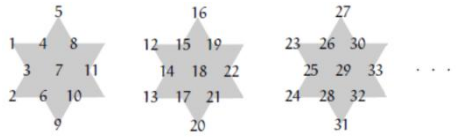


Em quais estrelas aparece o número 2011? Posicione todos os números que aparecem nas referidas estrelas.

CHAVE: 2X11, tal que $X = \text{A posição do número 2011}$

SOLUÇÃO:

Separe as estrelas deixando os números compartilhados sempre na estrela à direita. Fazendo isto, como indicado na figura a seguir, vemos que em cada estrela ficam escritos 11 números.



Imagine que 2011 sejam quantidade de pessoas de um grupo formado apenas por professores, e precisamos distribuir os professores colocando um em cada sala nas diversas escolas, desta forma, cada estrela é uma escola e os números de 1 a 11 são as salas de aula de cada escola. Temos um grupo de professores que ficarão sempre na primeira sala de cada escola, são eles os professores $1,12,23,\cdots$ *o mesmo acontece com a sala dois, representada por* $2,13,24,\cdots$ *e assim sucessivamente.*

Considerando que os professores de 1 a 11, são os representantes de cada grupos, como foi discutido no organizador prévio, basta fazer $2011 = 11 \cdot 182 + 9$*, logo o professor 2011 ficará na sala referente ao grupo que contém o líder 9, portanto, a sala 9 da escola. Além, disso veja que falta 2 unidades para a divisão por 11 ser exata e dar quociente 183, isso porque a sala nove esta na escola 183 e se continuarmos contanto, completamos esta escola.*

Portanto, a solução para a senha é x=9.

APÊNDICE L – Certificado de participação do curso de criptografia

NÚCLEO DE PESQUISA E ENSINO EM MATEMÁTICA
NUPEMAT/UNIVASF

Certificamos que

(NOME DO ESTUDANTE)

participou do curso de extensão

Introdução à Criptografia

ministrado pela professora *Sumaia Almeida Ramos*, no período de novembro a dezembro de 2016, totalizando a carga horária de 40 h.

Profº. Dr. Severino Cirino de Lima Neto
Coordenador do Nupemat/prof. Orientador

Esp. Sumaia Almeida Ramos
Professora

PROFMAT CAPES UNIVASF NUPEMAT UNIVASF SBM