UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Renato Machado de Sousa

UMA PROPOSTA DE ENSINO DA ARITMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS: UM PASSEIO PELA HISTÓRIA, CONCEITOS E APLICAÇÕES

Campina Grande - PB
Agosto/2024

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UFCG

Renato Machado de Sousa

UMA PROPOSTA DE ENSINO DA ARITMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS: UM PASSEIO PELA HISTÓRIA, CONCEITOS E APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Orientador: Dr. José Fernando Leite Aires
Coorientador: Dr. Leomaques Francisco Silva Bernardo

Campina Grande - PB
Agosto/2024

S725p Sousa, Renato Machado de.

Uma proposta de ensino da aritmética por meio de sequências didáticas: um passeio pela história, conceitos e aplicações / Renato Machado de Sousa. – Campina Grande, 2024.

136 f. : il. color.

Dissertação (Mestrado em Matemática) – Universidade Federal de Campina Grande, Centro de Ciências e Tecnologia, 2024.

"Orientação: Prof. Dr. José Fernando Leite Aires, Prof. Dr. Leomaques Francisco Silva Bernardo".

Referências.

1. Aritmética. 2. Matemática Aplicada. 3. Sequências Didáticas. 4. Cifras de Hill. 5. Jogos. I. Aires, José Fernando Leite. II. Bernardo, Leomaques Francisco Silva. III. Título.

CDU 511.1(043)

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECÁRIA SEVERINA SUELI DA SILVA OLIVEIRA CRB-15/225

Renato Machado de Sousa

UMA PROPOSTA DE ENSINO DA ARITMÉTICA POR MEIO DE SEQUÊNCIAS DIDÁTICAS: UM PASSEIO PELA HISTÓRIA, CONCEITOS E APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UFCG, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Trabalho aprovado. Campina Grande - PB, 22 de Agosto de 2024:

Documento assinado digitalmente
gov.br
LEOMAQUES FRANCISCO SILVA BERNARDO
Data: 19/09/2024 10:04:13-0300
Verifique em https://validar.iti.gov.br

Dr. Leomaques Francisco Silva Bernardo
Coorientador -UFCG

Documento assinado digitalmente
gov.br
RODRIGO COHEN MOTA NEMER
Data: 19/09/2024 13:55:00-0300
Verifique em https://validar.iti.gov.br

Dr. Rodrigo Cohen Mota Nemer
Membro Interno, UFCG

Documento assinado digitalmente
gov.br
PRISCILA SANTOS RAMOS
Data: 19/09/2024 12:53:58-0300
Verifique em https://validar.iti.gov.br

Dra. Priscila Santos Ramos
Membro Externo, UFOB

Campina Grande - PB
Agosto/2024

Dedico este trabalho primeiramente a Deus, por se fazer presente em todos os momentos difíceis e bons em minha vida, sempre me dando esperança e iluminando meus pensamentos, para que eu pudesse vencer todos os obstáculos.

Agradecimentos

Ao meus orientadores Dr. José Fernando Leite Aires e Dr. Leomaques Francisco Silva Bernardo, que conduziram o trabalho com paciência e dedicação, sempre disponíveis a compartilhar todo o seu vasto conhecimento.

Aos professores Dra. Priscila Santos Ramos e Dr. Rodrigo Cohen Mota Nemer, por aceitarem o convite para participar da banca examinadora, com correções, sugestões e ensinamentos imprescindíveis para conclusão deste trabalho.

Aos meus amigos Geovane Tavares Nogueira, Lucivaldo José de Andrade Pereira e Tiago Emanoel Melo Pereira e aos professores Dr. Luiz Antônio da Silva Medeiros e Dr. Leomaques Francisco Silva Bernardo que foram pilares fundamentais para construção do meu conhecimento que adquiri durante o curso.

A todos os professores que fazem parte deste programa, em especial, aos que contribuíram com a minha formação: Arimatéia, Daniel Cordeiro, Fernando, Jaime, Leomaques, Luiz Antônio, Marcelo e Romildo.

À instituição de ensino UFCG, por possibilitar esse período de estudos e desenvolvimento profissional.

Aos meus amigos de turma: Alexandre, Antônio, Emídio, Fabrícia, Flávia, Mozart, Pedro, Rejane, Renan, Ruth, Silvana e Thiago, por compartilharem comigo tantos momentos de descobertas e aprendizado e por todo o companheirismo ao longo deste percurso.

Às minhas amigas Isabela e Ana que sempre apoiaram e ajudaram a turma com uma dedicação impressionante.

Ao meu amigo Me. Emerson Fittipaldi Suassuna de Oliveira que tanto me ajudou neste período de tantas dificuldades e descobertas.

A todos os alunos da minha turma, pelo ambiente amistoso no qual convivemos e solidificamos os nossos conhecimentos, o que foi fundamental na elaboração deste trabalho de conclusão de curso.

A todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado.

"*Não vos amoldeis às estruturas deste mundo,*
mas transformai-vos pela renovação da mente,
a fim de distinguir qual é a vontade de Deus:
o que é bom, o que Lhe é agradável, o que é perfeito".
(Bíblia Sagrada, Romanos 12, 2)

Resumo

Este trabalho propõe uma abordagem de ensino da Aritmética por meio de sequências didáticas explorando conceitos, História da Matemática, aplicações e jogos, visando desenvolver alternativas metodológicas e teóricas inovadoras para melhorar a compreensão e o engajamento dos alunos em relação aos tópicos da Aritmética. A metodologia adotada nesta pesquisa envolve uma abordagem qualitativa, implementação de sequências didáticas e jogos como a "Trilha da Aritmética". Os resultados esperados incluem maior participação dos alunos, melhor compreensão dos conceitos abordados e um ambiente de aprendizagem mais dinâmico e interativo. Concluindo, este estudo visa fornecer uma contribuição significativa para o processo de ensino-aprendizagem da Matemática, demonstrando a eficácia da integração de abordagens lúdicas e práticas ao ensino da Aritmética.

Palavras-chave: Aritmética; Sequências Didáticas; Cifras de Hill; Jogos.

Abstract

This work proposes an approach to teaching Arithmetic through didactic sequences exploring concepts, History of Mathematics, applications, and games, aiming to develop innovative methodological and theoretical alternatives to improve students' understanding and engagement concerning Arithmetic topics. The methodology adopted in this research involves a qualitative approach and implementation of didactic sequences and games such as the Arithmetic Trail. The expected results include greater student participation, better understanding of the concepts covered, and a more dynamic and interactive learning environment. In conclusion, this study aims to provide a significant contribution to the Mathematics teaching-learning process, demonstrating the effectiveness of integrating playful and practical approaches to Arithmetic teaching.

Keywords: Arithmetic; Didactic Sequences; Hill Ciphers; Games. .

Lista de ilustrações

Lista de tabelas

Sumário

1 Introdução

A Aritmética desempenha um papel fundamental no currículo educacional brasileiro, sendo considerada uma base essencial para o conhecimento humano (ARAÚJO; FILHO, 2023). Mesmo sendo um dos pilares essenciais da Matemática, enfrentamos frequentemente, diversos desafios para ensinar a Aritmética no que diz respeito à sua eficácia e à promoção de uma aprendizagem significativa.

Historicamente, sua importância foi exposta nos programas escolares de 1930, enfatizando seu caráter abstrato e aplicações (AMARAL; SANT'ANA; SANT'ANA, 2019). O ensino da Aritmética tem sido influenciado por programas internacionais na época, como o Programa de Assistência Brasileiro-Americana ao Ensino Elementar (PABAEE), que circulam ideias pedagógicas no Brasil (CARVALHO; DUARTE, 2017). Apesar de sua relevância, alunos, especialmente na Educação de Jovens e Adultos, relatam dificuldades com a Aritmética, embora a reconheçam como úteis no cotidiano (ARAÚJO; FILHO, 2023).

Frente a esses desafios, torna-se essencial reconsiderar as abordagens de ensino da Aritmética, procurando por estratégias inovadoras que estimulem uma compreensão mais profunda dos conceitos. A integração desses conceitos com o contexto dos alunos é crucial, incentivando uma participação ativa e envolvente. Este desafio estimula uma reflexão contínua sobre como transcender as barreiras tradicionais, visando proporcionar uma experiência de aprendizado mais eficaz e enriquecedora para os alunos.

De acordo com a Base Nacional Comum Curricular (BNCC) (BRASIL, 2018), é importante desenvolver habilidades matemáticas essenciais, incluindo a compreensão dos números, das operações aritméticas, além de enfatizar a necessidade de promover o raciocínio lógico, a resolução de problemas e a aplicação dos conhecimentos matemáticos no cotidiano dos alunos.

Ou seja, ao ensinar Aritmética, o professor deve cultivar a habilidade dos alunos de raciocinar, resolver problemas e compreender o mundo. Além disso, deve ser uma experiência enriquecedora que capacita os alunos a aplicar conceitos de maneira prática e significativa.

Quando o professor utiliza situações-problema e estratégias que atendam às diferentes necessidades de aprendizagem, favorecendo a inclusão e a participação efetiva de todos, os alunos desenvolvem a capacidade de analisar e sintetizar os problemas de forma mais simplificada, bem como aprimorar o senso de abstração e de generalização de questões sofisticadas (HEFEZ; ARITMÉTICA, 2009).

A missão do professor consiste em orientar e ser um mediador da aprendizagem para um desenvolvimento ativo, sistemático e independente, promovendo a construção de

responsabilidade ao enfrentar desafios. Contudo, reconhecemos que transmitir conteúdos de maneira significativa é uma tarefa complexa, suscitando indagações frequentes dos alunos sobre o "como" e o "porquê".

Visando contribuir com o ensino e aprendizagem da Aritmética, neste trabalho recorremos à sequência didática que, de acordo com (ARAÚJO, 2013) e (ZABALA, 1998), é necessário organizar as atividades de forma a incluir todos nossos alunos, cumprindo todas as etapas e objetivos que devem ser alcançados. Em nosso trabalho, realizamos a sequência didática ao longo de sete encontros. Cada encontro teve um propósito específico, que será detalhado no Capítulo 5.

Neste sentido, este trabalho tem a finalidade de discutir uma abordagem alternativa no que se refere aos aspectos teórico-metodológicos sobre o ensino de Aritmética, definições e propriedades. É importante observar que esse conteúdo matemático é abordado superficialmente no Ensino Médio. Assim, nesta proposta de pesquisa, planejamos explorar esse conteúdo de forma mais aprofundada, estudando as primeiras ideias da Aritmética e aplicando esses conhecimentos em sala de aula. Buscamos analisar, coletar e verificar os resultados, de modo que o aprendizado se tornasse significativo para os alunos.

A utilização de linguagem de programação, Criptografia e materiais lúdicos foram implementados neste trabalho com o objetivo de promover um ensino e aprendizado de maior qualidade.

Consideramos que o uso da linguagem de programação foi fundamental para que os alunos entendessem os algoritmos e a aplicação do conceitos formais da Aritmética na prática. Já no campo da Criptografia abordamos algumas aplicações. Em grego, "cryptos" significa segredo, oculto. A Criptografia estuda métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-lo como afirma (COUTINHO, 2015). É a arte dos "códigos secretos". Pesquisadores propõem integrar a Criptografia em vários tópicos matemáticos, incluindo funções e matrizes, para fornecer um contexto significativo e cativar o interesse dos alunos (ROSSETO, 2018). Esta abordagem pode promover aulas de Matemática mais produtivas e preencher lacunas do conhecimento (ROSSETO, 2018).

A Criptografia vem sendo usada constantemente com objetivo de evitar violações nos sistemas eletrônicos e proteger informações sigilosas (TERADA, 1988). Por meio da Criptografia os sistemas computacionais e informações estão cada fez mais seguras, por conta da privacidade e segurança dos sistemas.

Também utilizamos recursos complementares para facilitar o processo de ensino/aprendizagem, como as Cifras de Hill. Essa abordagem visa evidenciar a interconexão e a possibilidade de trabalhar esses conteúdos de maneira integrada. Dessa forma, conseguimos demonstrar aos alunos que, a partir dos avanços matemáticos, a

Criptografia se tornou um recurso de grande relevância na sociedade moderna. Através dela, é possível transmitir e enviar mensagens de forma que somente o remetente e o destinatário possuam acesso a essa informação.

Ao trabalhar de forma lúdica, por meio de um jogo intitulado "Trilha da Aritmética", conseguimos abordar uma significativa parte dos conceitos utilizados na etapa da sequência didática. Após a aplicação da sequência didática , os alunos responderam a um questionário que buscava avaliar o grau de satisfação em relação à metodologia aplicada.

1.1 Objetivos

1.1.1 Objetivo Geral

Desenvolver alternativas metodológicas e teóricas para o ensino da Aritmética por meio de sequências didáticas, História da Matemática, conceitos e aplicações.

1.1.2 Objetivos Específicos

- Fazer um levantamento histórico e bibliográfico sobre Aritmética;
- Realizar uma abordagem investigava sobre o grau de aprendizagem da Aritmética e identificar os principais obstáculos enfrentados pelos professores e alunos ao ensinar e aprender propriedades, definições, manipulações e aplicações no intuito de participar na superação dessas dificuldades;
- Pesquisar sobre estratégias metodológicas e recursos didáticos eficazes para a compreensão e aprendizagem da Aritmética;
- Elaborar e aplicar as sequências didáticas em uma turma do 3º ano do Ensino Médio;
- Utilizar a linguagem de programação Python, com a intenção de trabalhar os algoritmos aritméticos e aplicações;
- Elaborar um jogo intitulado “Trilha da Aritmética” que tem a finalidade de auxiliar de forma lúdica a compreensão das definições e propriedades da Aritmética;
- Avaliar os resultados obtidos na aplicação dessas sequências didáticas.

1.2 Organização

Com o intuito de alcançar os objetivos apresentados na seção 1.1, a dissertação está estruturada em sete capítulos.

O Capítulo 1, fornece algumas considerações e objetivos iniciais para a elaboração da dissertação.

No Capítulo 2, apresentamos um arcabouço teórico que fundamenta a pesquisa, na qual abordaremos conceitos, habilidades e competências que estão na BNCC. E em seguida associamos a Criptografia ao estudo das matrizes e determinantes que estão na Proposta Curricular do Novo Ensino Médio da Paraíba (PCEMPB).

No Capítulo 3, incluímos alguns aspectos históricos da Aritmética, destacando a importância de conhecer o passado para entender o futuro.

Com relação ao Capítulo 4, nos dedicamos a promover a parte dos conceitos formais, definições e propriedades. Por meio destas ferramentas é possível assimilar os conteúdos de forma significativa e consistente.

Em seguida, no Capitulo 5, que teve como objetivo descrever nossa sequência didática, na qual dividimos em sete encontros. No primeiro encontro abordamos a história da Aritmética, as definições de números, múltiplos, divisores e usamos um algoritmo em linguagem de programação Python. Com relação ao segundo encontro, trabalhamos o algoritmo da divisão, critério de divisibilidade, Crivo de Eratóstenes, número primo de Mersenne e algoritmos utilizados em Python. Já no terceiro encontro dissertamos o Teorema Fundamental da Aritmética, números primos, compostos, Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC). Já no quarto encontro apresentamos problemas relacionados a relógios, calendários e congruência modular. O quinto encontro relembramos conceitos fundamentais de matrizes e determinante . Em seguida, utilizamos e aplicamos as Cifras de Hill. Por fim, aplicamos todos os conhecimentos adquiridos sobre Aritmética em um jogo intitulado “Trilha da Aritmética”.

No Capítulo 6, fizemos uma análise e obtivemos alguns resultados relevantes, com relação à aplicação do teste de sondagem sobre o conhecimento aritmético. Em seguida analisamos o questionário sobre a metodologia aplicada nos encontros.

E para finalizar, no Capítulo 7, realizamos algumas ponderações e sugestões construtivas para melhorar o nosso trabalho científico.

2 Referencial Teórico

A Aritmética que estudamos em diversas ocasiões é abordada de forma fragmentada, enfatizando ora um determinado tópico, ora outro, ignorando sua ideia fundamental que é entender definições, suas propriedades e os números inteiros. Apesar dos significativos avanços e descobertas ao longo de muitos anos de estudo sobre os números, ainda existem grandes mistérios a serem explorados (CADAR; DUTENHEFNER, 2015).

É importante ressaltar que a Aritmética desempenha um papel central como uma ferramenta essencial e fundamental na resolução de uma ampla variedade de situações-problema. Sua aplicação transcende o ambiente escolar, permeando o cotidiano e as demandas práticas da vida. Ao dominar os princípios aritméticos, os alunos adquirem uma base sólida que lhes permite enfrentar desafios e tomar decisões importantes em diversas circunstâncias, consolidando assim sua capacidade de análise crítica e resolução eficiente de problemas do mundo real. A Aritmética, portanto, não apenas enriquece a compreensão Matemática, mas também se revela como uma habilidade valiosa para a vida.

A BNCC (BRASIL, 2018), enquanto um guia normativo, desempenha um papel crucial ao apontar-nos em direção a conteúdos essenciais para o sucesso no ambiente de trabalho e no cenário da produção científica do aluno. Este documento visa não apenas fornecer uma estrutura educacional consistente, mas também orientar o processo de aprendizagem em direção as habilidades e conhecimentos que são não apenas pertinentes ao contexto acadêmico, mas também fundamentais para o êxito no mundo profissional e na contribuição para avanços científicos. Dessa forma, a BNCC(BRASIL, 2018) se posiciona como uma ferramenta orientadora que busca alinhar a formação educacional às exigências da sociedade contemporânea, preparando os alunos para os desafios e oportunidades do mundo do trabalho e da pesquisa científica.

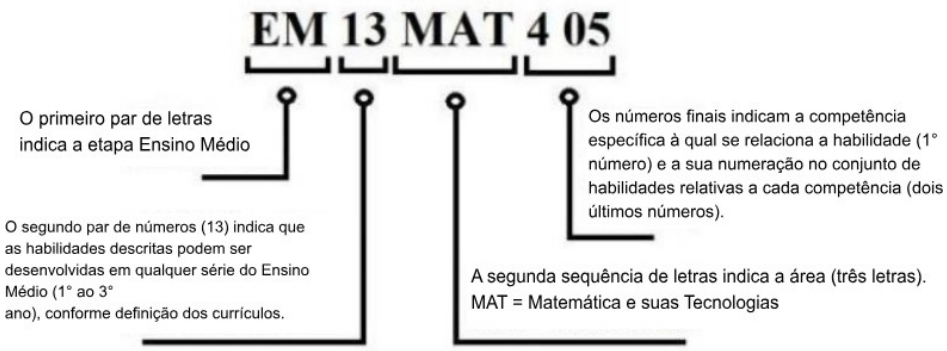
As unidades temáticas que serão abordadas neste trabalho são os números e a álgebra, e os objetos de conhecimento são operações tais como: adição, subtração, multiplicação e divisão euclidiana, a fim de auxiliar na resolução de problemas do dia a dia. Entendendo a Aritmética de forma eficiente, podemos trabalhar outros conteúdos de forma mais consistentes e abordar consequentemente, os conteúdos de forma mais dinâmica.

A BNCC(BRASIL, 2018) estabelece que ao longo da Educação Básica, 10 competências gerais devem ser desenvolvidas e aprimoradas. Estas competências abrangem áreas como conhecimento, pensamento científico, crítico e criativo, repertório cultural, habilidades de comunicação, cultura digital, além de focar em aspectos como trabalho e projeto de vida, argumentação, autoconhecimento e autocuidado, empatia, operação,

responsabilidade e cidadania. Também propõe uma abordagem holística e abrangente para o desenvolvimento integral dos alunos ao longo de sua jornada educacional.

Além das 10 competências, são necessárias habilidades que capacitam o aluno a ser independente na busca pelo conhecimento e a desempenhar um papel ativo como protagonista de sua própria trajetória. Para uma interpretação adequada dessas habilidades, é essencial contar com um código alfanumérico, estabelecidos na BNCC, conforme exemplificado a seguir:

Figura 1 – Descrição dos números e letras correspondentes às habilidades da BNCC



Fonte: (SOUZA et al., 2023, p.23)

Segue abaixo as habilidades relacionadas à Aritmética que estão contempladas na BNCC. Essas habilidades abrangem uma gama de conhecimentos essenciais para o desenvolvimento matemático dos alunos, promovendo uma compreensão aprofundada e aplicada dos conceitos aritméticos. Através dessas competências, a BNCC busca fortalecer a base Matemática dos alunos, capacitando-os para enfrentar desafios e utilizar eficazmente, as habilidades aritméticas em diversas situações práticas.

Figura 2 – Habilidades sobre Aritmética na BNCC

Unidade Temática	**Objetos de conhecimento**	**Habilidades referentes a BNCC**
Números	Fluxograma para determinar a paridade de um número natural Múltiplos e divisores de um número natural Números primos e compostos.	(EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
		(EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.
	Múltiplos e divisores de um número natural.	(EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos.
	Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações.	(EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.

Fonte: (BRASIL, 2018, p.303-309)

A partir da Figura 2 acima, podemos observar que assuntos como divisão, critérios de divisibilidade, números primos e compostos, Máximo Divisor Comum (MDC), Mínimo Múltiplo Comum (MMC), e outros tópicos como matrizes, determinantes e suas propriedades, muitas vezes são trabalhados de forma isolada.

As habilidades relacionadas à Aritmética, no âmbito da Proposta Curricular do Novo Ensino Médio da Paraíba (PCEMPB), estão apresentadas no quadro a seguir. Estas habilidades delineiam os objetivos específicos e as competências que os alunos devem adquirir no que diz respeito à Aritmética, visando aprofundar sua compreensão e capacidade de aplicação desses conceitos.

Essa abordagem específica destaca o compromisso do currículo em fornecer uma formação Matemática abrangente e relevante para os alunos, preparando-os para enfrentar os desafios acadêmicos e práticos que surgem no Ensino Médio. Vale destacar que tais habilidades serão abordadas em virtude do estudo e aplicação da Criptografia por meio da Aritmética, matrizes e determinantes.

Figura 3 – Habilidades sobre matrizes e determinantes na Proposta Curricular do Novo Ensino Médio da Paraíba (PCEMPB)

Unidade Temática	**Habilidade Especifica da Área**	**Objeto de aprendizagem**	**Objeto do Conhecimento**
Álgebra	EM13MAT410	Identificar e representar os diferentes tipos de matrizes.	Matrizes e Determinantes
		Resolver problemas utilizando as operações com matrizes e a linguagem matricial.	

Fonte: (PARAÍBA, 2021, p. 276)

A Criptografia vem sendo utilizada há muito tempo, desde do período dos antigos chineses, por espiões e até mesmo por manipuladores políticos. Mas a Criptografia ganhou mais destaque nas áreas militares e no serviço secreto, como ressalva (TERADA, 1988).

Percebe-se que a preocupação com a segurança e privacidade da informação é muito antiga. Ao longo do tempo, essas informações decidiam até batalhas um exemplo antigo de codificação e decodificação de mensagem são "Cifras de César". Era importante na época, transmitir essas informações confidenciais para os soldados aliados, pois se essas informações fossem obtidas por inimigos, os soldados aliados poderiam correr diversos tipos de riscos. Então uma maneira eficiente de proteger essas informações era por meio das "Cifras de César" ou "Cifras de Substituição": era um sistema monoalfabético, utilizado e elaborado pelo general Júlio César, em torno de 58 a.C. Este sistema consiste em trocar cada letra do alfabeto seguindo um padrão bem determinado. Acredita-se que Júlio César substituía cada letra pela terceira letra que se segue no alfabeto como comenta (ROSSETO, 2018).

As "Cifras de Hill", foram as Cifras escolhidas para manipular e aplicar com os alunos do 3º ano do Ensino Médio. Elas são baseadas em transformações matriciais e utilizam um sistema poligráfico. Foi inventada pelo matemático Lester S. Hill em 1929. Neste sentido, usamos estas cifras para fazer uma retomada nos conteúdos de matrizes e determinantes. Observamos que estes conteúdos fazem parte da PCEMPB. Este sistema de Criptografia consiste em utilizar o alfabeto com as 26 letras, onde cada letra estará associada a um valor numérico: por exemplo, A está associado a 1, B está

associado a 2 e assim sucessivamente, até chegarmos ao Z que será associado a 0. Pois, Z corresponde ao 26 e quando dividimos o número 26 por 26 obtemos o resto 0. As ideias contidas nesta dissertação sobre as "Cifras de Hill" foram retiradas do trabalho acadêmico de (ROSSETO, 2018).

Neste trabalho abordaremos algumas aplicações da Aritmética no campo da Criptografia. Em grego, "cryptos" significa segredo, oculto. A Criptografia também chamada de cifras estuda métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-lo como afirma (COUTINHO, 2015). É a arte dos "códigos secretos". Além dos tópicos da Aritmética citados anteriormente, abordamos também matrizes e determinantes.

No contexto dos desafios frequentemente encontrados no ensino da Matemática, destaca-se o papel crucial do lúdico como um recurso significativo, sobretudo no âmbito da Aritmética. A palavra Lúdico vem do latim "Ludus" que significa jogo e divertimento como afirma (ROLOFF, 2010). A utilização de abordagens lúdicas não é apenas torna o aprendizado mais envolvente, mas também promove uma compreensão mais profunda dos conceitos matemáticos, tornando o processo de ensino-aprendizagem mais acessível e estimulante para os alunos. O caráter lúdico não apenas quebra possíveis barreiras de ansiedade em relação à Matemática, mas também contribui para o desenvolvimento de habilidades cognitivas e criativas, incentivando os alunos a explorarem, experimentarem e compreenderem a Aritmética de maneira mais holística e prazerosa (MOURA, 1994).

Percebe-se que muitas vezes nossos alunos ficam muito entediados com a parte conceitual formal, pois esta conceituação na maioria das situações é transmitida de forma abstrata. Assim, as atividades lúdicas têm por finalidade proporcionar uma convivência e um interação melhor com os alunos e professor, criando um ambiente de competição saudável onde todos os envolvidos conseguem aprender e se divertir simultaneamente, como comenta (SILVA et al., 2013).

Acreditamos que por meio do lúdico podemos obter resultados mais positivos com relação ao ensino. (SILVA et al., 2013) ainda reforçam a ideia de que é possível ensinar Matemática de forma divertida sem atrapalhar a ideia dos conceitos formais, definições e propriedades.

Vale salientar também, que o lúdico será utilizado como uma forma de consolidar os conceitos da Aritmética e que isso se dará por meio de um jogo chamado "Trilha da Aritmética".

Ao abordar os tópicos aritméticos, é comum automatizar e mecanizar o ensino, tornando-o desafiador para alunos e professores. Ao enfatizar regras e soluções superficiais, muitas vezes negligenciamos a essência do processo de ensino-aprendizagem: a aquisição significativa de conhecimento. Esta pesquisa buscou transcender essa aborda-

gem, incentivando a interação entre alunos, promovendo discussões e explorando diversas estratégias de resolução. Além de contribuir para o desenvolvimento da linguagem e habilidades reflexivas, visa servir como guia para alunos e professores interessados em aprofundar seu entendimento sobre os fundamentos da Aritmética na Matemática.

Nesse sentido, a proposta deste trabalho de pesquisa é criar um elo entre estes conteúdos para que o aluno consiga estabelecer uma conexão entre eles, a fim de que a assimilação seja significativa. Dessa forma, nesta dissertação, propomos alternativas metodológicas para o ensino da Aritmética, baseando-nos em novas pesquisas e abordagens que foram adquiridas ao longo do curso de Mestrado Profissional em Matemática (PROFMAT).

3 Uma breve história sobre Arimética e o desenvolvimento da Matemática

Pode-se dizer que a Aritmética foi a primeira área da Matemática a ser criada, e mesmo ainda não sendo conhecida por este nome, surgiu juntamente com os primeiros sistemas de quantificação da humanidade. A palavra aritmética deriva do grego "arithmos", que significa número (UFABC, 2024).

A ideia de números remonta a aproximadamente 30.000 anos atrás, com o objetivo de registrar a quantidade de familiares, de animais e de objetos importantes para uma determinada comunidade tribal (HYGINO, 1991).

O Capítulo 1 do livro "Origem da Matemática", como delineada por Carl B.Boyer em sua obra seminal de 1974 (p.1-5), inicia-se pelo título "*A History of Mathematics*", que remonta aos tempos pré-históricos, onde os primeiros sinais de atividade Matemática podem ser encontrados nas práticas e na vida cotidiana das comunidades primitivas. Estas práticas rudimentares, que hoje consideraríamos como Aritmética e Geometria básicas, estavam intrinsecamente ligadas à sobrevivência e à organização social desses povos. A necessidade de contar, medir e dividir recursos como alimento, água e terra deu origem às formas mais primitivas de Matemática, que evoluíram de modo a se tornarem cada vez mais refinadas (BOYER, 1974).

Nos tempos pré-históricos, a Matemática era essencialmente uma ferramenta prática. As comunidades primitivas utilizavam métodos simples de contagem para manter registros de bens, como gado e colheitas. A contagem, inicialmente, pode ter sido feita utilizando partes do corpo humano, como os dedos, que serviram como ferramentas naturais para enumerar objetos. O conceito de números surgiu a partir dessa necessidade de quantificar. O desenvolvimento do conceito de número foi um dos primeiros e mais fundamentais avanços na história da Matemática. Os números naturais, que usamos hoje para contar, representam uma das primeiras abstrações matemáticas (BOYER, 1974).

A necessidade de contar e registrar detalhes é tão antiga quanto a própria humanidade. Os primeiros sistemas de contagem eram extremamente simples, utilizando objetos físicos como pedras, nós em cordas ou marcas em ossos. Estes métodos rudimentares de conclusão são evidências do desenvolvimento inicial da Aritmética nas primeiras civilizações, como comenta (HYGINO, 1991).

Comumente, associa-se a história dos números à noção de contagem, problemas relacionados à subsistência humana. Quando lemos problemas envolvendo contagem, o exemplo mais frequente é voltado para pastores de ovelhas, associando cada animal

com uma pedra. Neste sentido, é possível ter um certo controle sobre o rebanho. Em seguida, foram criados outros artifícios práticos associados a marcas e escritas de argila. Estas marcas estariam associadas à origem dos números. Vale ressaltar que estas fontes não são seguras, pois a maioria dos registros são muito escassos e fragmentados como pondera (ROQUE; CARVALHO, 2012).

A necessidade de medir também desempenhou um papel crucial na evolução da Matemática. A agricultura, uma das primeiras atividades econômicas a se desenvolver, exigia medições precisas de terras e a determinação dos melhores momentos para plantar e colher. Estas necessidades levaram ao desenvolvimento de técnicas básicas de Geometria. (BOYER, 1974) observou que as primeiras civilizações, como os egípcios e os babilônios, desenvolveram sistemas de medição que permitiram a construção de grandes obras de engenharia e a organização das cidades. Os egípcios, por exemplo, desenvolveram um sistema de medição baseado no cúbito, que era a distância do cotovelo à ponta do dedo médio. Esse sistema de medição era crucial para a construção de suas monumentais pirâmides e templos.

Além da medição e da contagem, a divisão de recursos era uma prática matemática fundamental nas comunidades primitivas. A divisão de terras, a distribuição de alimentos e a partilha de outros bens exigiam uma compreensão básica de frações e proporções. A necessidade de justiça e equidade na distribuição de recursos pode ter incentivado o desenvolvimento dessas ideias matemáticas. (BOYER, 1974) argumenta que a divisão de recursos não era apenas uma questão prática, mas também um aspecto essencial da vida social e política das primeiras comunidades. A Matemática, nesse contexto, surgiu como uma ferramenta para resolver problemas práticos e sociais.

A transição da Matemática prática para a Matemática teórica começou a ocorrer com o advento das primeiras civilizações, como a babilônica e a egípcia. Essas civilizações não apenas utilizavam a Matemática para fins práticos, mas também começaram a explorar conceitos matemáticos abstratos. Na Babilônia, por exemplo, o desenvolvimento de um sistema numérico baseado em 60, que ainda influencia nosso conceito de tempo e ângulos hoje, representou um avanço significativo. Os babilônios também desenvolveram tabelas de multiplicação e métodos para resolver equações quadráticas, indicando um nível avançado de pensamento matemático (BOYER, 1974).

A civilização egípcia, por outro lado, fez avanços significativos na Geometria. Os egípcios desenvolveram técnicas geométricas que lhes permitiram construir as pirâmides com uma precisão impressionante. Eles também utilizavam a Geometria para resolver problemas práticos de medição de terras e divisão de propriedades. O Papiro de Rhind, um dos documentos matemáticos mais antigos que se conhece, contém problemas aritméticos e geométricos que mostram o alto nível de conhecimento matemático dos egípcios (BOYER, 1974).

Na Grécia antiga, onde filósofos como Pitágoras e Euclides começaram a explorar a Matemática como área do estudo abstrata. Pitágoras, por exemplo, é famoso por seu teorema sobre triângulos retângulos, mas também contribuiu para o desenvolvimento da teoria dos números e a ideia de proporção. Euclides, por sua vez, organizou o conhecimento geométrico existente em sua obra "*Os Elementos*", que se tornou um dos textos mais influentes na história da Matemática (BOYER, 1974).

A Teoria dos Números, um ramo central da Matemática, tem suas raízes na escola pitagórica, fundada por Pitágoras no século VI a.C. Esta escola filosófica grega acreditava que os números eram a essência de todas as coisas e se dedicava intensamente ao estudo das propriedades numéricas. Para os pitagóricos, os números não eram apenas ferramentas matemáticas, mas também elementos fundamentais da realidade e da ordem cósmica (HYGINO, 1991).

Os gregos viam a Matemática não apenas como uma ferramenta prática, mas como uma forma de compreender o universo. Acreditavam que os princípios matemáticos subjacentes à natureza poderiam ser descobertos através da razão e da lógica. Esta abordagem teórica e abstrata levou a grandes avanços em diversas áreas da Matemática, incluindo Geometria, Aritmética e Álgebra (BOYER, 1974).

A Matemática continuou a evoluir ao longo da história, com cada civilização contribuindo de maneiras únicas para o seu desenvolvimento. Na Índia, por exemplo, matemáticos como *Aryabhata* e *Brahmagupta* fizeram avanços significativos na álgebra e na aritmética, ampliando as ideias e conceitos que seriam posteriormente utilizados por matemáticos árabes e europeus. Os matemáticos indianos introduziram o zero como um número e elaboraram métodos avançados para resolver equações quadráticas e cúbicas (BOYER, 1974).

Na China, a Matemática também progrediu de maneira significativa, especialmente na área da Aritmética e da Geometria. Matemáticos chineses, como *Liu Hui* e *Zu Chongzhi*, fizeram contribuições importantes para o cálculo do número pi e o desenvolvimento de métodos de solução de sistemas de equações lineares. O "*Livro dos Números e Computações*", escrito por *Yang Hui*, é um exemplo da sofisticação da Matemática Chinesa, contendo métodos avançados para resolver problemas aritméticos e geométricos (BOYER, 1974).

O mundo islâmico também desempenhou um papel crucial na preservação e no desenvolvimento da Matemática. Após a queda do Império Romano, muitos textos matemáticos gregos foram traduzidos para o árabe e estudados por matemáticos islâmicos. *Al-Khwarizmi*, um dos matemáticos mais influentes da época, escreveu obras sobre Álgebra e Aritmética que tiveram um impacto duradouro. Seu livro "*Kitab al-Jabr wal-Muqabala*" deu origem ao termo "*Álgebra*" e estabeleceu as bases para a resolução sistemática de equações (BOYER, 1974).

Na Europa Medieval, a matemática começou a florescer novamente com a redescoberta dos textos gregos e islâmicos. Durante o Renascimento, matemáticos como *Leonardo Fibonacci* introduziram o sistema numérico hindu-árabe na Europa, o que revolucionou a Aritmética. *Fibonacci*, em sua obra "*Liber Abaci*", demonstrou as vantagens deste sistema numérico em comparação com o sistema romano, facilitando cálculos mais rápidos e precisos (BOYER, 1974).

No início da era moderna, a Matemática continuou a evoluir rapidamente. *René Descartes*, por exemplo, desenvolveu a Geometria Analítica, que unificou a Álgebra e a Geometria e abriu caminho para o desenvolvimento do cálculo. *Isaac Newton* e *Gottfried Wilhelm Leibniz*, de forma independente, desenvolveram o Cálculo Diferencial e Integral, ferramentas fundamentais para a ciência moderna. O cálculo permitiu o estudo de mudanças contínuas e teve um impacto profundo na Física, na Engenharia e em outras ciências (BOYER, 1974).

Durante o século XVIII, a Matemática se expandiu ainda mais com os trabalhos de matemáticos como *Leonhard Euler* e *Carl Friedrich Gauss*. *Euler* fez contribuições significativas em diversas áreas da Matemática, incluindo a teoria dos números, a topologia e a análise. *Gauss*, conhecido como o "príncipe dos matemáticos", fez descobertas fundamentais na Álgebra, na teoria dos números e na Geometria Diferencial (BOYER, 1974).

O século XIX viu a Matemática se tornar cada vez mais abstrata e rigorosa. *Georg Cantor* desenvolveu a teoria dos conjuntos, que revolucionou a forma como os matemáticos pensam sobre o infinito e a estrutura dos números. A Matemática se tornou uma disciplina mais formalizada e teórica, com o desenvolvimento de novas áreas como a Álgebra Abstrata e a Topologia (BOYER, 1974).

No século XX, a Matemática continuou a se expandir em novas direções. A Teoria da Relatividade de *Albert Einstein* e a mecânica quântica exigiram novos desenvolvimentos matemáticos, levando a avanços na Geometria Diferencial e na Teoria dos Grupos. A Matemática Computacional emergiu como uma nova área de estudo, com o desenvolvimento de computadores permitindo a resolução de problemas complexos que antes eram intratáveis (BOYER, 1974).

A obra de *Carl B. Boyer* de 1974, "*A History of Mathematics*", oferece uma visão abrangente e detalhada do desenvolvimento da Matemática desde suas origens primitivas até os avanços modernos. (BOYER, 1974) argumenta que a Matemática evoluiu de uma ferramenta prática para uma ciência teórica e abstrata, impulsionada pela necessidade humana de contar, medir e dividir. Cada civilização ao longo da história contribuiu de maneira única para o desenvolvimento da Matemática, refletindo suas próprias necessidades e interesses (BOYER, 1974).

A história da Matemática é uma narrativa de progresso contínuo e inovação. Desde

as origens primitivas nas comunidades pré-históricas até os avanços complexos da era moderna, a Matemática tem sido uma ferramenta essencial para a compreensão e a organização do mundo ao nosso redor. O desenvolvimento da Matemática é um testemunho do engenho humano e da capacidade de abstrair e generalizar conceitos a partir de necessidades práticas. Como Boyer destaca, a Matemática não é apenas uma coleção de técnicas e fórmulas, mas uma disciplina profundamente enraizada na história e na cultura humana, refletindo as aspirações, as necessidades e as conquistas das civilizações ao longo do tempo. A evolução da Matemática continua a ser uma narrativa de inovação e progresso, moldando e sendo moldada pela história da humanidade. A trajetória da Matemática, como descrita por Carl B. Boyer, não é apenas uma sequência de descobertas e avanços técnicos, mas também uma história rica de interações culturais, intercâmbios intelectuais e contextos sociais (BOYER, 1974).

No século XX, a Matemática experimentou uma expansão significativa em várias direções, refletindo as demandas de novas áreas do conhecimento e as revoluções tecnológicas. A teoria da relatividade de *Albert Einstein* e a mecânica quântica transformaram nossa compreensão do universo, exigindo desenvolvimentos matemáticos em áreas como a geometria diferencial e a teoria dos grupos. A Matemática computacional surgiu como uma nova área de estudo, com o advento dos computadores permitindo a resolução de problemas complexos que antes eram intratáveis (BOYER, 1974).

Uma das inovações mais significativas do século XX foi o desenvolvimento da teoria dos conjuntos por *Georg Cantor*, que revolucionou a forma como os matemáticos pensam sobre o infinito e a estrutura dos números. A teoria dos conjuntos tornou-se a base para muitas áreas da Matemática Moderna, proporcionando uma linguagem comum e um *framework* unificador para várias disciplinas matemáticas. Além disso, a teoria dos jogos, desenvolvida por *John von Neumann* e *Oskar Morgenstern*, trouxe uma nova perspectiva para a tomada de decisões e a economia, demonstrando a aplicabilidade da Matemática em ciências sociais (BOYER, 1974).

O campo da Matemática aplicada também experimentou uma enorme expansão. As técnicas matemáticas foram essenciais para o desenvolvimento da engenharia, da física, da economia e das ciências biológicas. Modelos matemáticos tornaram-se ferramentas cruciais na análise de sistemas complexos, desde o comportamento das partículas subatômicas até as dinâmicas dos ecossistemas. A modelagem Matemática e a simulação computacional permitem a previsão de fenômenos naturais e a otimização de processos industriais, destacando a relevância prática e o impacto da Matemática no mundo contemporâneo (BOYER, 1974).

No entanto, a Matemática não evoluiu apenas em resposta às necessidades práticas. O desenvolvimento da Matemática pura, que busca explorar conceitos abstratos e resolver problemas teóricos sem uma aplicação imediata em mente, também floresceu. A

teoria dos números, a Topologia, a Álgebra Abstrata e a Análise Funcional são apenas algumas das áreas que se desenvolveram significativamente no século XX e continuam a avançar no século XXI. Essas áreas, embora muitas vezes afastadas das aplicações práticas diretas, têm profundas implicações para o entendimento fundamental da estrutura e da lógica (BOYER, 1974).

A globalização e o intercâmbio de ideias aceleraram o progresso matemático. Colaborações internacionais e o acesso a uma vasta gama de recursos através da internet permitiram que os matemáticos de todo o mundo compartilhassem suas descobertas e insights mais rapidamente do que nunca. Esta conectividade global também trouxe à luz contribuições matemáticas de culturas e civilizações que anteriormente poderiam ter sido negligenciadas ou subestimadas, ampliando a compreensão da Matemática como uma disciplina verdadeiramente universal (BOYER, 1974).

Além disso, a Educação Matemática tem evoluído, com novas abordagens pedagógicas sendo desenvolvidas para engajar alunos e incentivar o pensamento crítico. A Matemática, muitas vezes considerada difícil e abstrata, é incentivada a tornar-se mais acessível e relevante através do uso de tecnologias educacionais, abordagens interativas e uma ênfase renovada na resolução de problemas do mundo real (BOYER, 1974).

O impacto da Matemática na sociedade moderna não pode ser subestimado. As finanças, a medicina, a tecnologia da informação, a engenharia e muitas outras áreas dependem profundamente de técnicas e conceitos matemáticos. A Criptografia, por exemplo, é fundamental para a segurança das comunicações digitais, enquanto algoritmos matemáticos são essenciais para a inteligência artificial e o aprendizado de máquina, que estão transformando indústrias inteiras e a forma como vivemos nossas vidas (BOYER, 1974).

A Matemática também desempenha um papel vital na abordagem dos desafios globais contemporâneos. Questões como a mudança climática, a gestão de recursos naturais, a saúde pública e a sustentabilidade econômica exigem análises matemáticas sofisticadas e modelos preditivos para desenvolver soluções eficazes. A capacidade da Matemática de abstrair e generalizar permite que os cientistas e engenheiros compreendam e enfrentem esses desafios complexos com rigor e precisão (BOYER, 1974).

No entanto, a História da Matemática também nos ensina sobre os desafios e as limitações do conhecimento humano. A busca pela verdade Matemática é frequentemente marcada por controvérsias e debates intensos. Questões como a natureza dos infinitos, a lógica subjacente à Matemática e a validade dos sistemas axiomáticos continuam a ser temas de discussão e investigação. A Matemática é uma ciência viva, em constante evolução, que se beneficia de uma diversidade de perspectivas e abordagens (BOYER, 1974).

Em resumo, a obra de Carl B. Boyer, “A History of Mathematics”, nos oferece

uma visão rica e detalhada da evolução da Matemática desde suas origens primitivas até os avanços contemporâneos. A Matemática, inicialmente uma ferramenta prática para contagem, medição e divisão, transformou-se ao longo dos séculos em uma ciência teórica e abstrata, essencial para a compreensão e a organização do mundo. Cada civilização ao longo da história contribuiu de maneira única para o desenvolvimento da Matemática, refletindo suas próprias necessidades, interesses e contextos culturais (BOYER, 1974).

A evolução da Matemática é um testemunho do engenho humano e da capacidade de abstrair e generalizar conceitos a partir de necessidades práticas. A Matemática não é apenas uma coleção de técnicas e fórmulas, mas uma ciência profundamente enraizada na história e na cultura humana, refletindo as aspirações, as necessidades e as conquistas das civilizações ao longo do tempo. Como Boyer destaca, a Matemática continua a ser uma narrativa de progresso contínuo e inovação, moldando e sendo moldada pela história da humanidade. O desenvolvimento da Matemática é um processo dinâmico, impulsionado tanto pela curiosidade intelectual quanto pelas demandas práticas, e continuará a evoluir à medida que enfrentamos novos desafios e exploramos novas fronteiras do conhecimento (BOYER, 1974).

4 Aritmética e alguns de seus importantes resultados

Neste capítulo, daremos início à formalização dos conceitos e propriedades da Aritmética, acreditamos que por meio das definições formais podemos trabalhar a resolução de situações-problemas de modo mais eficiente e coerente.

Vale salientar que as definições são ferramentes importantes para demonstrar propriedades significativas para o desenvolvimento do pensamento crítico e o raciocínio lógico.

As definições, propriedades e resultados aqui tratados encontram-se nos livros utilizados na disciplina de Aritmética do curso de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT: (HEFEZ; ARITMÉTICA, 2009); (OLIVEIRA; PINHEIRO, 2010), assim como no livro do Programa de Iniciação Científica da OBMEP (HEFEZ, 2009).

A ideia de números inteiros originou-se da ideia de números naturais, que por sua vez se desenvolveu graças à ideia de números que se tinha como objetivo principal a resolução de pequenos problemas envolvendo contagem.

Desde da antiguidade, os números negativos eram trabalhados de forma abstrata, mas com o tempo e o desenvolvimento mercantil no final da idade média, os números negativos começaram a ter um papel de relevância maior.

A evolução dos números inteiros foi de certa forma elaborado de maneira muito lenta. Mas a partir do século XIX com diversos questionamentos, a noção de números passou a ser fundamentada em conceitos e propriedades (HEFEZ; ARITMÉTICA, 2009).

Assumiremos que o leitor já está familiarizado com os conceitos, notações e convenções destacados a seguir:

- $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$: denota o conjunto dos números naturais;
- $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$: denota o conjunto dos números inteiros;
- $D(n)$: o conjunto dos divisores de um número natural n;
- Todo número inteiro possui uma única representação decimal, ou seja, um número inteiro n admite uma única representação da forma:

  $n = \pm\ a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$, onde os $a_{i's}$ são números naturais tais que $0 \leq a_i \leq 9$ e $i \in \{0, 1, 2, \cdots, m-1, m\}$;

- (a, b): denota Máximo Divisor Comum de a e b, ou seja, $(a, b) = MDC(a, b)$.

Os termos a_i, $0 \leq a_i \leq 9$, são chamados de algarismos, dígitos ou cifras. Se for informado que um número inteiro possui, por exemplo, n dígitos, o dígito mais a esquerda (também conhecido como mais significativo) não pode valer zero. Os dígitos recebem nomes de acordo com a sua ordem. O dígito a_0 é chamado de dígito das unidades, a_1 de dígito das dezenas, a_2 de dígito das centenas, a_3 de dígito dos milhares, a_4 de dígito dos milhões e assim por diante. A ordem de cada dígito, por sua vez, é igual ao expoente da potência de 10 de cada dígito. por exemplo: o dígito das unidades é o de ordem zero, e o dígito das centenas é o de ordem dois.

Através destas convenções, definições e das propriedades das operações como adição e multiplicação, podemos demonstrar outras propriedade importantes para Aritmética.

A adição e a multiplicação são definidas pelas seguintes propriedades:

Propriedade 1. Para quaisquer $a, a', b, b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

Propriedade 2. A adição e a multiplicação são comutativas:

- $\forall\ a, b \in \mathbb{Z}$ tem-se: $a + b = b + a$ e $a \cdot b = b \cdot a$.

Propriedade 3. A adição e a multiplicação são associativas:

- $\forall\ a, b, c \in \mathbb{Z}$ tem-se: $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Propriedade 4. A adição e a multiplicação possuem elementos neutros:

- $\forall\ a \in \mathbb{Z}$ tem-se: $a + 0 = a$ e $a \cdot 1 = a$.

Propriedade 5. A adição possuem elementos simétricos:

- $\forall\ a \in \mathbb{Z}$ existe $b = -a$ tal que $a + b = 0$.

Propriedade 6. A multiplicação é distributiva em relação à adição:

- $\forall\ a, b, c \in \mathbb{Z}$ tem-se: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Utilizando as propriedades acima podemos demonstrar a seguinte proposição:

Proposição 4.1. *A adição é compatível e cancelativa com respeito à igualdade: Para todos $a, b, c \in \mathbb{Z}$, $a = b$ se, e somente se, $a + c = b + c$.*

Demonstração.
A implicação $a = b \Rightarrow a + c = b + c$ é consequência do fato de a adição ser bem definida **(Propriedade 1).**

Se $a = b$ e $c = c$, então $a + c = b + c$.

Suponhamos agora $a + c = b + c$. Pela **Propriedade 5,** existe $c \in \mathbb{Z}$ tal que $c + (-c) = 0$. Assim, Desde que $a + c = b + c$, somando $(-c)$ a ambos membros e aplicando a **Propriedade 1,** Tem-se:

$$\begin{aligned} & a + (c + (-c)) = b + (c + (-c)) \\ \Rightarrow \quad & a + 0 = b + 0 \\ \Rightarrow \quad & a = b. \end{aligned}$$

■

Podemos observar que estas propriedades não são válidas para outras operações como a subtração e divisão que estudaremos posteriormente. Definições bastante importante são as de múltiplos, múltiplos comuns, divisores e divisores comuns que veremos abaixo:

Definição 4.1. *Dado um número inteiro a, consideremos o conjunto dos múltiplos naturais de a:*

$$a\mathbb{N} = \{a \cdot d \ \mid \ d \in \mathbb{N}\}.$$

Os números que pertencem simultaneamente ao conjunto dos múltiplos de dois ou mais números dados serão chamados de múltiplos comuns destes números dados.

Observação 4.1. *Se a e b são números naturais não nulos, sabemos que o número $a \cdot b$ é um múltiplo de a. Por outro lado, pela propriedade comutativa da multiplicação, tem-se que ele também um múltiplo de b. Assim, o conjunto dos múltiplos comuns de a e b, além de conter o número 0, contém também o número $a \cdot b \neq 0$.*

A partir deste momento iremos abordar a definição de divisibilidade e demonstrar algumas propriedades.

Definição 4.2. *Dados dois números inteiros a e b, diremos que a divide b, denota-se por $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = c \cdot a$. Nesse caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a ou que b é divisível por a.*

Observação 4.2. *$a \mid b$ não representa uma operação e podemos representar por meio dos símbolos.Assim,*

$$a \mid b \Leftrightarrow b = c \cdot a, \text{ para algum } c \in \mathbb{Z}.$$

Já a negação dessa sentença pode ser escrito da seguinte forma: $a \nmid b$, ou seja, não existe nenhum número c inteiro tal que $b = c \cdot a$.

Após definirmos a divisibilidade, vamos demonstrar algumas propriedades. Sejam $a, b, c \in \mathbb{Z}$, tem-se:

1. $a \mid a$, $1 \mid a$ e $a \mid 0$.

   Demonstração.
   $a \mid a$, pois $a = 1 \cdot a$.
   $1 \mid a$, pois $a = a \cdot 1$.
   $a \mid 0$, pois $0 = 0 \cdot a$.

   ■

2. $0 \mid a$ se, e somente se, $a = 0$.

   Proposição 4.2. *$a \cdot 0 = 0$ para todo $a \in \mathbb{Z}$*

   A **Proposição 4.2.** A demonstração está na bibliografia (HEFEZ; ARITMÉTICA, 2009)

   Demonstração.
   Suponhamos que $0 \mid a$, se existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$
   Pela **Proposição 4.2.** Conclui-se que $a = 0$, implica que $a = 0 \cdot 0$, o que nos diz que $0|a$. ■

3. a divide b se, e somente se, $|a|$ divide $|b|$.

   Demonstração.
   $a \mid b$ se, e somente se, existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$.
   Ora,

   $$\begin{aligned} b &= c \cdot a \\ |b| &= |c \cdot a| \\ |b| &= |c||a|, \end{aligned}$$

   o que implica que $|a| \mid |b|$.
   $|a| \mid |b|$ se, e somente se, existe $p \in \mathbb{Z}$ tal que $|b| = p \cdot |a|$. Assim teremos que analisar 4 casos:

1º caso: $a \geq 0$ e $b \geq 0$.
$b = p \cdot a$, implica que $a|b$.

2º caso: $a \geq 0$ e $b < 0$.
$-b = p \cdot a$, implica que $b = -p \cdot a$, ou ainda, que $a \mid b$.

3º caso: $a < 0$ e $b < 0$.
$-b = p \cdot (-a)$, implica que $b = p \cdot a$, ou ainda, que $a \mid b$.

4º caso: $a < 0$ e $b \geq 0$.
$b = p \cdot (-a)$, implica que $b = -p \cdot a$, ou ainda, que $a \mid b$.

■

4. Se $a \mid b$ e $b \mid c$, então $a \mid c$.

   Demonstração.

   Se $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$.

   Se $b \mid c$, então existe $m \in \mathbb{Z}$ tal que $c = m \cdot b$.
   Substituindo $b = k \cdot a$ em $c = m \cdot b$, obtemos: $c = m \cdot (k \cdot a) = (m \cdot k) \cdot a$, o que implica que $a \mid c$. ■

5. Sejam $a, b, c, d \in \mathbb{Z}$, se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.

   Demonstração.

   Se $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$.

   Se $c \mid d$, então existe $m \in \mathbb{Z}$ tal que $d = m \cdot c$.

   Multiplicando b por d e fazendo a devida substituição obtemos:

   $$b \cdot d = (k \cdot a) \cdot (m \cdot c) = (m \cdot k) \cdot (a \cdot c),$$

   o que implica que $a \cdot c \mid b \cdot d$. ■

6. Sejam $a, b, c, d \in \mathbb{Z}$, tais que $a \mid (b + c)$. Então $a \mid b$ se, e somente se, $a \mid c$.

   Demonstração.
   Se $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$.
   Se $a \mid (b + c)$, então existe $t \in \mathbb{Z}$ tal que $b + c = a \cdot t$, ou ainda, $c = a \cdot t - b$.
   Assim, substituindo $b = a \cdot k$ em $c = a \cdot t - b$, obtemos:

   $$c = a \cdot t - a \cdot k = a \cdot (t - k),$$

ou seja, $a \mid c$.

Se $a \mid c$, então existe $k \in \mathbb{Z}$, tal que $c = k \cdot a$, e Se $a \mid (b + c)$, então existe $t \in \mathbb{Z}$, tal que $b + c = t \cdot a$, ou ainda, $b = t \cdot a - c$.

Substiuindo $c = k \cdot a$ em $b = t \cdot a - c$, obtemos:

$$b = t \cdot a - k \cdot a = (t - k) \cdot a,$$

ou seja, $a \mid b$.

■

7. Sejam $a, b, c, \in \mathbb{Z}$, tais que $a \mid b$ e $a \mid c$. Então $\forall x, y \in \mathbb{Z}, a \mid (xb + yc)$.

   Demonstração. Ora,

   Se $a \mid b$, então existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$, ou ainda, $xb = x(k \cdot a)$.

   Se $a \mid c$, então existe $m \in \mathbb{Z}$ tal que $c = m \cdot a$, ou ainda, $yc = y(m \cdot a)$.

   Assim, temos pela propriedade associativa,

   $$bx + cy = (kx)a + (my)a = (kx + my)a,$$

   ou seja, $a \mid (xb + yc)$. ■

8. Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, se $a \mid b$, então $|a| \leq |b|$.

   Demonstração.

   $a \mid b$ implica que $|a| \leq |b|$.

   $a \mid b$ logo existe $k \in \mathbb{Z}$ tal que $b = k \cdot a$. O que implica que $|b| = |k \cdot a| = |k| \cdot |a|$.

   O fato de $b \neq 0$ implica que $|k| \neq 0$, ou ainda $|k| \geq 1$, donde, $|k| \cdot |a| \geq 1 \cdot |a|$.
   Ora, $|k| \cdot |a| = |b|$, logo:

   $$|b| \geq |a|.$$

   ■

4.1 Algoritmo da Divisão Euclidiana

Uma das propriedades mais importantes dos números inteiros é a possibilidade de dividir um número por outro, essa divisão é a chamada divisão euclidiana.

Definição 4.3. *Sejam a e b números inteiros com $b \neq 0$. Existem dois únicos números inteiros q e r tais que $a = b \cdot q + r$, com $0 \leq r < |b|$. Chamamos a, b, q e r de dividendo, divisor, quociente e resto, respectivamente.*

O algoritmo da divisão euclidiana fornece uma importante ferramenta no estudo de questões em que determinada propriedade deve ser analisada para todos os inteiros. Por exemplo, como na divisão euclidiana por 3 temos apenas os restos 0, 1 e 2, todos os inteiros podem ser escritos da seguinte maneira: $3 \cdot k$, $3 \cdot k + 1$ e $3 \cdot k + 2$ para todo $k \in \mathbb{Z}$. Mas para demonstrar a existência e a unicidade da divisão euclidiana a propriedade acima não é suficiente, precisamos de algumas ferramentas poderosas como Princípio da Boa Ordenação e a Propriedade Arquimediana conforme abaixo respectivamente:

Definição 4.4. *Diremos que um subconjunto S de $\mathbb{Z}$ é limitado inferiormente, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in S$. Diremos que $a \in S$ é um menor elemento de S se $a \leq x$ para todo $x \in S$.*

Teorema 4.3. *Princípio da Boa Ordenação: Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então possui um menor elemento.*

Corolário 4.4. ***(Propriedade Arquimediana)*** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.*

As demonstrações desses resultados podem ser encontradas no livro (HEFEZ; ARITMÉTICA, 2009). Portanto, por meio destes resultados apresentados anteriormente podemos demonstrar a existência e a unicidade do algoritmo da divisão euclidiana.

Demonstração. (**Existência**) Vamos demonstrar a princípio a existência do quociente e do resto. Considere o conjunto: $S = \{x = a - by; y \in \mathbb{Z}\} \bigcap \mathbb{N}$, veremos no decorrer da demonstração que x será o r e y será q.

Lembrando que S é um conjunto e S é limitado inferiormente por 0. Pela Propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$ o que implica que $a - b \cdot n > 0$, podemos concluir que o conjunto S é não vazio.

Portanto, com estas duas propriedades, percebe-se que pelo Princípio da Boa Ordenação, S possui um menor elemento r, logo $r \geq 0$.

Suponhamos então que $r = a - b \cdot q$, pois $r \in S$ e $r \geq 0$. Vamos demonstrar que $r < |b|$, suponhamos por absurdo que $r \geq |b|$, isto é, que existe $s \in \mathbb{N}$ tal que $r = |b| + s$, portanto pela divisão euclidiana, $0 \leq s < r$. Mas isto contradiz o fato de r ser o menor elemento de S.

Substituindo, $r = |b| + s$ em $r = a - b \cdot q$, obtemos:

$$\begin{aligned} r = a - b \cdot q &\Rightarrow |b| + s = a - b \cdot q \\ &\Rightarrow s = a - b \cdot q - |b| \\ &\Rightarrow s = a - b \cdot (q \pm 1) \in S, \end{aligned}$$

absurdo, logo $r < |b|$.

Portanto, verificamos a existência do quociente e do resto, ou seja, $0 \leq r < |b|$.

Unicidade: Demonstraremos a unicidade do quociente e do resto:

Suponha que $a = b \cdot q + r = b \cdot q' + r'$, onde $q, q', r, r' \in \mathbb{Z}$. Portanto, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica que

$|b||q - q'| = |r' - r| < |b|$.

O que só é possível se $q = q'$ e consequentemente, $r' = r$. Portanto, r e q são únicos.

■

4.2 Critérios de divisibilidade

Nesta seção, apresentamos alguns critérios de divisibilidade importantes. Mas, antes destes critérios, vamos precisar de algumas definições, como a de números primos e compostos abordadas por (CADAR; DUTENHEFNER, 2015).

Definição 4.5. *Um número natural maior que 1 é **primo** quando ele é divisível apenas por 1 e por ele mesmo.*

Definição 4.6. *Quando um número não é primo, ele é chamado de **composto**.*

Estes critérios compreendem apenas os casos de divisibilidade por números primos (número que só tem como divisores 1 e ele próprio) (2, 3, 5, 7, 11, 13, $\cdots$) ou potências de primos (4, 9, 16, $\cdots$). No caso da análise da divisibilidade de determinado inteiro por um número composto, que não seja uma potência de um primo, deve-se fatorar este número composto como a multiplicação de termos com Máximo Divisor Comum (MDC) igual a 1 e aplicar os critérios por cada um destes termos. Por exemplo, para a análise da divisibilidade de um inteiro por 18, deve-se aplicar os critérios de divisibilidade por 2 e 9.

4.2.1 Divisibilidade por 2

Proposição 4.5. *Um número inteiro é divisível por 2 se seu último algarismo for divisível por 2.*

Demonstração.
Seja $n = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 0 + a_0$

$$= 10(a_n a_{n-1} a_{n-2} \cdots a_2 a_1) + a_0.$$

O valor de n é um número inteiro. Como $10(a_n a_{n-1} a_{n-2} \cdots a_2 a_1)$ é par, n é par se, e somente se, a_0 (que é o algarismo das unidades de n) é par. ■

4.2.2 Divisibilidade por 3

Proposição 4.6. *Um número inteiro é divisível por 3 se a soma dos seus algarismos for divisível por 3.*

Demonstração.
Seja um número natural n na sua representação decimal dado por:

$$\begin{aligned}
n &= a_n a_{n-1} \cdots a_2 a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 \cdot 10 + a_0 \\
&= \left(\underbrace{9999\cdots9}_{n} + 1 \right) a_n + \left(\underbrace{9999\cdots9}_{n-1} + 1 \right) a_{n-1} + \cdots + (9+1)a_1 + a_0 \\
&= \underbrace{99\cdots9}_{n} a_n + \underbrace{99\cdots9}_{n-1} a_{n-1} + \cdots + 9a_2 + 9a_1 + a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \\
&= 3\left(\underbrace{33\cdots3}_{n} a_n + \underbrace{33\cdots3}_{n-1} a_{n-1} + \cdots + 3a_2 + 3a_1 \right) + a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0.
\end{aligned}$$

Como o primeiro termo é multiplo de 3, para que n seja múltiplo de 3, devemos ter que $a_n + a_{n-1} + a_{n-2} + \cdots + a_3 + a_2 + a_1 + a_0$ (que é a soma dos dígitos de n) seja múltiplo de 3. ■

4.2.3 Divisibilidade por 4

Proposição 4.7. *Um número inteiro é divisível por 4 se o número formado por seus dois últimos algarismos for divisível por 4.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned}
n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2 00 + (a_1 a_0) \\
&= 100 a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2 + a_1 a_0
\end{aligned}$$

Como $100 a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2$ é divisível por 4, n é divisível por 4 se, e somente se, $a_1 a_0$ (que é o número formado pelos dois últimos algarismos de n) é divisível por 4. ■

4.2.4 Divisibilidade por 5

Proposição 4.8. *Um número inteiro é divisível por* 5 *se o último algarismo for igual a* 0 *ou* 5.

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2 a_1 0 + a_0 \\ &= 10 a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2 a_1 + a_0 \end{aligned}$$

Como $10 a_n a_{n-1} a_{n-2} a_{n-3} a_{n-4} \cdots a_4 a_3 a_2 a_1$ é divisível por 5, n é divisível por 5 se, e somente se, a_0 (que é algarismo das unidades de n) é divisível por 5, ou seja, se é igual a 0 ou 5. ■

4.2.5 Divisibilidade por 7

Proposição 4.9. *Um número inteiro* $n = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0$ *é divisível por 7 quando o inteiro* $a_0 + 3a_1 + 2a_2 + 6a_3 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + \cdots$ *for divisível por 7.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} \cdots a_2 a_1 a_0 = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k + \cdots + 10^n a_n + \cdots \\ &= a_0 + (7+3)a_1 + (98+2)a_2 + (994+6)a_3 + (9996+4)a_4 + (99995+5)a_5 + \\ &\quad (999999+1)a_6 + (9999997+3)a_7 + (99999998+2)a_8 + (999999994+6)a_9 + \cdots \\ &= 7(a_1 + 14a_2 + 142a_3 + 1428a_4 + 14285a_5 + 142857a_6 + 1428571a_7 + \cdots) \\ &\quad a_0 + 3a_1 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + \cdots \end{aligned}$$

Como o primeiro termo é múltiplo de 7, para que n seja múltiplo de 7 devemos ter que a expressão $a_0 + 3a_1 + 4a_4 + 5a_5 + a_6 + 3a_7 + 2a_8 + 6a_9 + \cdots$ seja múltipla de 7. ■

4.2.6 Divisibilidade por 8

Proposição 4.10. *Um número inteiro é divisível por 8 se o número formado por seus três últimos algarismos for divisível por 8.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = a_n a_{n-1} a_{n-2} \cdots a_4 a_3 000 + a_2 a_1 a_0 \\ &= 1000(a_n a_{n-1} a_{n-2} \cdots a_4 a_3) + a_2 a_1 a_0 \end{aligned}$$

Como $1000(a_n a_{n-1} a_{n-2} \cdots a_4 a_3)$ é divisível por 8, n é divisível por 8 se, e somente se, $a_2 a_1 a_0$ (que é o número formado pelo três últimos algarismos de n) é divisível por 8. ■

4.2.7 Divisibilidade por 9

Proposição 4.11. *Um número inteiro é divisível por 9 se a soma dos seus algarismos for divisível por 9.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 \cdot 10 + a_0 \\ &= \left(\underbrace{9999 \cdots 9}_{n} + 1 \right) a_n + \left(\underbrace{9999 \cdots 9}_{n-1} + 1 \right) a_{n-1} + \cdots + (9+1) a_1 + a_0 \\ &= \underbrace{99 \cdots 9}_{n} a_n + \underbrace{99 \cdots 9}_{n-1} a_{n-1} + \cdots + 9a_2 + 9a_1 + a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \\ &= 9 \left(\underbrace{11 \cdots 1}_{n} a_n + \underbrace{11 \cdots 1}_{n-1} a_{n-1} + \cdots + a_2 + a_1 \right) + a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0. \end{aligned}$$

Como o primeiro termo é múltiplo de 9, para que n seja múltiplo de 9, devemos ter que a expressão $a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0$ seja múltipla de 9. ■

4.2.8 Divisibilidade por 10

Proposição 4.12. *Um número inteiro é divisível por 10 se seu último algarismo for igual a 0.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$n = a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = 10(a_n a_{n-1} a_{n-2} \cdots a_2 a_1) + a_0$$

Como $10(a_n a_{n-1} a_{n-2} \cdots a_2 a_1)$ é divisível por 10, n é divisível por 10 se, e somente se, a_0 (que é o algarismo das unidades de n) é divisível por 10, ou seja, se é igual a 0. ■

4.2.9 Divisibilidade por 11

Proposição 4.13. *Um número inteiro $n = a_n a_{n-1} a_{n-2} \cdots a_3 a_2 a_1 a_0$ é divisível por 11 quando o inteiro $a_0 - a_1 + a_2 - a_3 + a_4 + \cdots + (-1)^n a_n$ for divisível por 11.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = 10(a_n a_{n-1} a_{n-2} \cdots a_2 a_1) + a_0 \\ &= a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 \cdot 10 + a_0 \\ &= (100 \cdots 00 \pm 1)^n a_n + \cdots + (100001 - 1)a_5 + (9999 + 1)a_4 + (1001 - 1)a_3 + \\ &\quad (99 + 1)a_2 + (11 - 1)a_1 + a_0 \\ &= 11\,[a_1 + 9a_2 + 91a_3 + 909a_4 + \cdots +] + a_0 - a_1 + a_2 - a_3 + a_4 \cdots + (-1)^n a_n \end{aligned}$$

Como o primeiro termo é múltiplo de 11, para que n seja múltiplo de 11, devemos ter que a expressão $a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + \cdots + (-1)^n a_n$ seja múltipla de 11. ■

4.2.10 Divisibilidade por 2^m ou 5^m, $m \geq 1 \in \mathbb{N}$.

Proposição 4.14. *Um número inteiro de n algarismos é divisível por 2^m ou 5^m, $n \geq m \geq 1$, se o número formado por seus últimos m algarismos for divisível por 2^m ou 5^m, respectivamente.*

Demonstração.
Seja um número inteiro n na sua representação decimal dado por:

$$\begin{aligned} n &= a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0 = (a_n a_{n-1} a_{n-2} \cdots a_{n-m} 000 \cdots 0) + (a_{n-m-1} \cdots a_1 a_0) \\ &= 10^m (a_n a_{n-1} \cdots a_{n-m}) + (a_{n-m-1} \cdots a_1 a_0) \\ &= (2 \cdot 5)^m (a_n a_{n-1} \cdots a_{n-m}) + (a_{n-m-1} \cdots a_1 a_0) \\ &= 2^m \cdot 5^m (a_n a_{n-1} \cdots a_{n-m}) + (a_{n-m-1} \cdots a_1 a_0) \end{aligned}$$

Como $2^m \cdot 5^m (a_n a_{n-1} \cdots a_{n-m})$ é divisível por 2^m ou por 5^m, n é divisível por 2^m ou 5^m se, e somente se, $(a_{n-m-1} \cdots a_1 a_0)$ (que é o número formado pelos últimos m algarismos de n) é divisível por 2^m ou 5^m, respectivamente. ■

4.3 (MDC) e (MMC) : Definições e propriedades relevantes

Nesta seção, abordaremos alguns conceitos e resultados necessários sobre máximo divisor comum (MDC) e mínimo múltiplo comum (MMC).

Definição 4.7. *Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d será dito um divisor comum de a e b , se $d \mid a$ e $d \mid b$.*

Por exemplo, 3 é divisor comum de 6 e 9. De fato, $3 \mid 6$ e $3 \mid 9$.

A seguir tem-se a definição abordada no livro VII dos Elementos de Euclides um dos pilares fundamentais da Aritmética.

Definição 4.8. *Diremos que um número d é máximo divisor comum de (MDC) de a e b, se possuir as seguintes propriedades.*

i) *d é um divisor comum de a e b, e*

ii) *d é divisível por todo divisor comum de a e b.*

A propriedade **ii)** pode ser reescrita da seguinte forma:

$$c \mid a \text{ e } c \mid b \Rightarrow c \mid d.$$

Para demonstrar a existência do máximo divisor comum de dois números inteiros não negativos, Euclides recorreu, ao lema abaixo, lembrando que denotaremos o (MDC) por meio de parênteses ( ): por exemplo, o máximo divisor comum de 4 e 8, denota-se $(4, 8) = 4$.

Lema 4.15. *Sejam $a, b, n \in \mathbb{Z}$. Se existe $(a, b - na)$, então (a, b) existe e*

$$(a, b) = (a, b - na).$$

Demonstração. Considere $d = (a, b - na)$, logo $d \mid a$ e $d \mid (b - na)$ e também $d \mid na$. Pela proposição 7. $d \mid (b - na) + na$, que implica que $d \mid b$. Portanto, d é um divisor comum de a e b.

Suponhamos que c seja divisor comum de a e b, ou seja, Se $c \mid a$, $c \mid b$ e $c \mid b - na$, então $c \mid d$. Isso demostra que $d = (a, b)$. ■

Definição 4.9. *Diremos que um número inteiro é um múltiplo comum de dois números inteiros dados se ele é simultaneamente múltiplo de ambos os números.*

Definição 4.10. *Diremos que um número inteiro $m \geq 0$ é um mínimo múltiplo comum (MMC) do números a e b, se possuir as seguintes propriedades:*

(i) *m é um múltiplo comum de a e b, e*

(ii) *se c é um múltiplo comum de a e b, então $m \mid c$.*

4.4 Teorema Fundamental da Aritmética

Nesta seção apresentamos alguns conceitos e propriedades relevantes para Aritmética, tais como os números primos, compostos e o Teorema Fundamental da Aritmética (TFA). Tais tópicos constituem as bases fundamentais para demonstrar diversas proposições significativas na Aritmética e têm aplicações interessantes na sociedade moderna.

Teorema 4.16. ***Teorema Fundamental da Aritmética :*** *Todo número natural maior do que* 1 *ou é primo ou se escreve de modo único(a menos da ordem dos fatores) como um produto de números primos.*

A demonstração deste teorema é encontrado no livro (HEFEZ; ARITMÉTICA, 2009).

Definição 4.11. ***(Número Primo):*** *Um número natural maior do que* 1 *que só possui como divisores positivos* 1 *e ele próprio é chamado de número primo.*

Proposição 4.17. *Sejam p e q primos e a um número inteiro qualquer. Tem-se as seguintes propriedades:*

I) *Se $p \mid q$, então $p = q$.*

Demonstração. Como q é primo, então o mesmo possui dois divisores o 1 e ele próprio(q). Logo, $p = 1$ ou $p = q$, p é primo, portanto, $p \neq 1$, o que acarreta $p = q$.

■

II) *Se $p \nmid a$, então $(p, a) = 1$.*

Demonstração. De fato, seja $d = (p, a)$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Vamos supor, por absurdo, que $d \neq 1$. Portanto, $d = p$, então $p \mid a$. Absurdo pois, pela hipótese, $p \nmid a$, e consequentemente, $d = 1$. ■

Definição 4.12. ***(Número Composto):*** *Um número maior do que* 1 *e que não é primo será dito composto.*

Proposição 4.18. *Seja $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se $p \mid ab$ e $p \nmid a$, então $p \mid b$. Mas , se $p \nmid a$, temos que $(p, a) = 1$.

Teorema 4.19. ***(Teorema de Bézout)*** *Dados a e b inteiros positivos, existem inteiros x, y tais que :*

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

Teorema 4.20. *Se $(p, a) = 1$, então pelo Teorema de Bezout dois números inteiros a e b são primos entre si, se, e somente se, existem números inteiros m e n tais que $mp + na = 1$.*

A demonstração do **Teorema 4.19**, encontra-se no livro (HEFEZ; ARITMÉTICA, 2009). Multiplicando ambos os membros por b tem-se: $mpb + nba = b$.

Se $p \mid ab$, então existe $e \in \mathbb{Z}$ tal que $ab = ep$.

Substituindo ab por ep e colocando em evidência p , teremos $p(mb + ne) = b$, portanto, $p \mid b$. A recíproca é verdadeira.

■

4.5 Congruência e suas propriedades importantes

Nesta seção, mostramos uma das noções mais interessantes da Aritmética, trata-se da aritmética dos resto da divisão euclidiana por um número natural maior que 1. Introduzida por Gaus no livro Disquisitiones Arithmeticae, em 1801. As definições, propriedades e demonstrações apresentadas a seguir foram baseadas no livro (HEFEZ; ARITMÉTICA, 2009).

Definição 4.13. *Seja $m > 1$ um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b \pmod{m}.$$

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escrevemos, nesse caso, $a \not\equiv b \pmod{m}$.

Vale salientar que quando $m = 1$, $a \equiv b \pmod{1}$ deixa sempre resto igual a 0 para quaisquer$a$, $b \in \mathbb{Z}$. Logo, consideramos sempre $m > 1$.

Reescrevendo a definição da aritmética dos restos tem-se:

Proposição 4.21. *Sejam $a, b, n \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \pmod{m}$ se, e somente se, $m \mid b - a$.*

Demonstração. De fato, pelo algoritmo da divisão, podemos escrever

$a = m \cdot q_1 + r_1$, com r_1 , $q_1 \in \mathbb{Z}$, $0 \leq r_1 < m$.

$b = m \cdot q_2 + r_2$, com r_2 , $q_2 \in \mathbb{Z}$, $0 \leq r_2 < m$.

Sem perda de generalidade, podemos supor que $r_1 \leq r_2$ (se o contrário ocorrer, basta trocar os papéis de r_1 e r_2). Assim, podemos escrever

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

Logo, m divide $b-a$ se, e somente se, m divide r_1-r_2. Por ser $0 \leq r_1-r_2 < m$, segue que m divide $b - a$ se, e somente se, $r_1 - r_2 = 0$, ou seja, se e somente se $r_1 = r_2$. ■

Vamos demonstrar algumas propriedades importantes no estudo referente a Aritmética dos Restos.

Sejam $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.

i) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.

Demonstração. Suponhamos que

$a \equiv b \pmod{m} \Rightarrow m \mid b - a$.

$c \equiv d \pmod{m} \Rightarrow m \mid d - c$.

Logo, temos que $m \mid (b + d) - (a + c) \Rightarrow a + c \equiv b + d \pmod{m}$. ■

ii) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração. Nota-se m divide a combinação linear como veremos abaixo.

$m \mid x \cdot (b+d) - y \cdot (a+c)$.

Substituindo $x = d$ e $y = a$ temos:

$m \mid d{\cdot}(b-a)+a{\cdot}(d-c) \Rightarrow m \mid db-da+ad-ac \Rightarrow m \mid db-da+ad-ac \Rightarrow m \mid db-ac \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$. ■

iii) Para todo $n \geq 1$, a, $b \in \mathbb{Z}$, se $a \equiv b \pmod{m}$, então tem-se : $a^n \equiv b^n \pmod{m}$.

Demonstração. Vamos provar por indução que $a^n \equiv b^n \pmod{m}$ para todo inteiro $n \geq 1$.

i) Como por hipótese, $a \equiv b \pmod{m}$, então o resultado é válido para $n = 1$.

ii) Suponhamos por hipótese de indução que, $a^n \equiv b^n \pmod{m}$ para $n \geq 1$.

Multiplicando i) por ii) temos:

$a \equiv b \pmod{m}$ e $a^n \equiv b^n \pmod{m} \Rightarrow a^n \cdot a \equiv b^n \cdot b \pmod{m} \Rightarrow a^{n+1} \equiv b^{n+1} \pmod{m}$. Logo, $a^{n+1} \equiv b^{n+1} \pmod{m}$ para todo $n \geq 1$.

Portanto, pelo Princípio da Indução Finita podemos concluir que $a^n \equiv b^n \pmod{m}$ para $n \geq 1$ é verdadeiro. ■

4.6 Classes residuais

Nesta seção, abordamos as classes residuais e o conjunto quociente $\mathbb{Z}_m$. Temos como base os livros (HEFEZ; ARITMÉTICA, 2009) e (VIEIRA, 2015). A seguir apresentamos algumas definições e propriedades relevantes associados à relação congruência módulo m.

Definição 4.14. *Sejam $a, m \in \mathbb{Z}$ $m > 1$. O conjunto $\bar{a} = \{x \in \mathbb{Z};\ x \equiv a \pmod{m}\}$ é chamado classe residual módulo m.*

Ou seja, $\bar{a}$ é o conjunto os inteiros que deixam o mesmo resto que na divisão por m.

A demonstração a seguir, faz-se necessário a proposição da transitividade.

Proposição 4.22. *Seja $m \in \mathbb{N} - \{0\}$. Para todos a, b, $c \in \mathbb{Z}$, tem-se que*
se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$

Proposição 4.23. *Para quaisquer $a, b, x, m \in \mathbb{Z}$ e $m > 1$,*
$\bar{a} = \bar{b}$ se, e somente se, $a \equiv b \pmod{m}$.

Demonstração. Por definição 4.14. $\bar{a} = \bar{b} \Rightarrow \{x \in \mathbb{Z};\ x \equiv a \pmod{m}\} =$
$\{x \in \mathbb{Z}\ ;\ x \equiv b \pmod{m}\} \Rightarrow x \equiv a \pmod{m}$ e $x \equiv b \pmod{m}$, por **Proposição 4.21.** temos que: $a \equiv b \pmod{m}$.

$\Leftarrow$) $a \equiv b \pmod{m} \Rightarrow \bar{a} = \bar{b}$.

$x \in \bar{a} \Rightarrow x \equiv a \pmod{m}$. Por hipótese $a \equiv b \pmod{m}$. Aplicando a **Proposição 4.21.** $x \equiv b \pmod{m} \Rightarrow x \in \bar{b}$. Logo $\bar{a} \subset \bar{b}$.

$x \in \bar{b} \Rightarrow x \equiv$ b $\pmod{m}$. Por hipótese $a \equiv b \pmod{m}$. Aplicando a **Proposição 4.21.** $x \equiv a \pmod{m} \Rightarrow x \in \bar{a}$. Logo $\bar{b} \subset \bar{a}$.

Portanto, se $\bar{a} \subset \bar{b}$ e $\bar{b} \subset \bar{a}$, então $\bar{a} = \bar{b}$.

■

Lembrando que estes resultados são ferramentas importantes para outras demonstrações, a seguir tem-se as definições de adição $\oplus$ e multiplicação $\odot$ em $\mathbb{Z}_m$ bem como algumas propriedades relacionadas a tais operações.

Definição 4.15. *O conjunto das classes residuais módulo m será denotado por* $\mathbb{Z}_m$ *:*

$$\mathbb{Z}_m = \{\bar{0},\ \bar{1},\ \bar{2},\ \ldots,\ \overline{m-1}\}$$

Definição 4.16. *Seja m um natural e* $m > 1$*. Então,*

$$\bar{a} \oplus \bar{b} = \overline{a+b} \text{ e } \bar{a} \odot \bar{b} = \overline{a \cdot b}$$

Definem as operações de adição $\oplus$ e multiplicação $\odot$ em $\mathbb{Z}_m$.

Sejam $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d} \in \mathbb{Z}_m$ tais que:

$\bar{a} = \bar{b}$ e $\bar{c} = \bar{d}$.

Devemos mostrar que:

$\bar{a} \oplus \bar{c} = \bar{b} \oplus \bar{d}$ e $\bar{a} \odot \bar{c} = \bar{b} \odot \bar{d}$.

Por definição 3.8. $\bar{a} = \bar{b}$ e $\bar{c} = \bar{d} \Leftrightarrow a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$.

Pela propriedade da congruência temos:

$a + c \equiv b + d \pmod{m}$ e $a \cdot c \equiv b \cdot d \pmod{m}$, de modo que em $\mathbb{Z}_m$ temos:

$\overline{a+c} = \overline{b+d}$ e $\overline{a \cdot c} = \overline{b \cdot d}$,

ou seja, $\bar{a} \oplus \bar{c} = \bar{b} \oplus \bar{d}$ e $\bar{a} \odot \bar{c} = \bar{b} \odot \bar{d}$. Isso prova o resultado.

Teorema 4.24. *A operação* $\oplus$ *de adição sobre* $\mathbb{Z}_m$ *tem as propriedades :*

(1) $\bar{a} \oplus (\bar{b} \oplus \bar{c}) = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$. $\forall\ \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_m$ *(* $\oplus$ *é associativa).*

(2) $\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a}$. $\forall\ \bar{a}, \bar{b}, \in \mathbb{Z}_m$ *(*$\oplus$ *é comutativa).*

(3) $\bar{a} \oplus \bar{0} = \bar{a}$. $\forall\ \bar{a} \in \mathbb{Z}_m$ *(*$\oplus$ *tem o elemento neutro).*

(4) *Dado* $\bar{a} \in \mathbb{Z}_m$*, existe um* $\bar{b} \in \mathbb{Z}_m$*, com* $\bar{a} \oplus \bar{b} = 0$ *(existência do simétrico sob* $\oplus$ *).*

Demonstração. **(1)** ($\oplus$ é associativa).

Consideremos $\bar{a}$, $\bar{b}$, $\bar{c} \in \mathbb{Z}_m$ e o fato de a adição em $\mathbb{Z}_m$ ser asssociativa tem-se:
$\bar{a} \oplus(\ \bar{b} \oplus \bar{c}) = \bar{a} \oplus(\ \overline{b+c}) = \overline{a+(b+c)} = \overline{(a+b)+c} = \overline{(a+b)} \oplus \bar{c} = (\bar{a} \oplus \bar{b}) \oplus \bar{c}$.
Portanto, a adição é asssociativa em $\mathbb{Z}_m$. ■

Demonstração. **(2)** ($\oplus$ é comutativa).

Sejam $\bar{a}$, $\bar{b} \in \mathbb{Z}_m$ e o fato de a adição em $\mathbb{Z}_m$ ser comutativa obtemos:
$\bar{a} \oplus \bar{b} = \bar{b} \oplus \bar{a} = \bar{a} \oplus \bar{b} = \overline{a+b} = \overline{b+a} = \bar{b} \oplus \bar{a}$.
Portanto, a adição é comutativa em $\mathbb{Z}_m$. ■

Demonstração. **(3)**($\oplus$ tem o elemento neutro).

Dado $\bar{a} \in \mathbb{Z}_m$ e o fato de a adição em $\mathbb{Z}_m$ ter um elemento neutro na adição obtemos:
$\bar{a} \oplus \bar{0} = \overline{a+0} = \bar{a}$.
Portanto, tem um elemento neutro sob $\oplus$ em $\mathbb{Z}_m$. ■

Demonstração. **(4)**(existe inverso sob $\oplus$).

Dado $\bar{a} \in \mathbb{Z}_m$, existe $\bar{b} \in \mathbb{Z}_m$, como $\bar{a} \oplus \bar{b} = \bar{0}$ se, e somente se, $\overline{a+b} = \bar{0}$. Ou seja, se, e somente se, $\overline{a+b} = \bar{m}$, pois $m \equiv 0 \pmod{m}$. Mas, $\overline{a+b} = \bar{m} \Leftrightarrow a+b = m \cdot k$, para algum $k \in \mathbb{Z}$.

.

■

Teorema 4.25. *A operação $\odot$ de multiplicação sobre $\mathbb{Z}_m$ tem as propriedades :*

(1) *$\bar{a} \odot(\ \bar{b} \odot \bar{c}) = (\bar{a} \odot \bar{b}) \odot \bar{c}$. $\forall\ \bar{a}$, $\bar{b}$, $\bar{c} \in \mathbb{Z}_m$ ($\odot$ é associativa).*

(2) *$\bar{a} \odot \bar{b} = \bar{b} \odot \bar{a}$. $\forall\ \bar{a}$, $\bar{b}$, $\in \mathbb{Z}_m$ ($\odot$ é comutativa).*

(3) *$\bar{a} \odot \bar{1} = \bar{a}$. $\forall\ \bar{a} \in \mathbb{Z}_m$ ($\odot$ tem o elemento neutro).*

(4) *$\bar{a} \odot(\ \bar{b} \oplus \bar{c}) = (\bar{a} \odot \bar{b}) \oplus(\bar{a} \odot \bar{c})$. $\forall\ \bar{a}$, $\bar{b}$, $\bar{c} \in \mathbb{Z}_m$ ($\odot$ é distributiva em relação a $\oplus$).*

Provaremos apenas os itens **(3)** e **(4)**.

Demonstração. **(3)**($\odot$ tem o elemento neutro).

$\bar{a} \odot \bar{1} = \overline{a \cdot 1} = \bar{a}$. ■

Demonstração. **(4)**($\odot$ é distributiva em relação a $\oplus$).

$\bar{a} \odot(\ \bar{b} \oplus \bar{c}) = \bar{a} \odot \overline{(b+c)} = \overline{a \cdot (b+c)} = \overline{a \cdot b + a \cdot c} = \overline{(a \cdot b)} \oplus \overline{(a \cdot c)} = (\bar{a} \odot \bar{b}) \oplus(\bar{a} \odot \bar{c})$. Portanto, $\odot$ é distributiva com relação a $\oplus$. ■

Para compreendermos melhor estas propriedades podemos utilizar as tábuas de $\oplus$ e $\odot$ em $\mathbb{Z}_4$.

Efetuando algumas operações temos: $\bar{2} \odot \bar{3} = \bar{6} = \bar{2}$; $\bar{2} \odot \bar{2} = \bar{4} = \bar{0}$; $\bar{2} \oplus \bar{3} = \bar{5} = \bar{1}$ e $\bar{1} \oplus \bar{3} = \bar{4} = \bar{0}$.

Para concluir a seção das classes residuais, vamos abordar uma proposição fundamental que estabelece condições para que um elemento tenha inverso multiplicativo.

Tabela 1 – Adição em $\mathbb{Z}_4$

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Fonte: Elaborado pelo autor (2024)

Tabela 2 – Multiplicação em $\mathbb{Z}_4$

$\odot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Fonte: Elaborado pelo autor (2024)

Proposição 4.26. *Temos que $\bar{a} \in \mathbb{Z}$ é invertível se, e somente se, $(a, m) = 1$.*

Demonstração. $\bar{a}$ é invertível, implica que existe $\bar{b} \in \mathbb{Z}_m$ tal que $\bar{a} \cdot \bar{b} = \bar{1}$. Desde que $a \cdot b \equiv 1 \pmod{m}$, tem-se, $a \cdot b = m \cdot q + 1$. Reescrevendo temos que, $a \cdot b - m \cdot q = 1$, $q \in \mathbb{Z}$, implicando que $(a, m) = 1$.

Suponhamos que $(a, m) = 1$, logo existem $x, y \in \mathbb{Z}$ tais que $a \cdot x + m \cdot y = 1$. Pela **Poposição 4.23**, e considerando $x = b$ e $y = (-q)$ tem-se: $\overline{a \cdot b + m \cdot (-q)} = \bar{1}$, logo, $\overline{a \cdot b} + \overline{m \cdot (-q)} = \bar{1}$, tem-se: $\bar{a} \cdot \bar{b} + \bar{m} \cdot \overline{(-q)} = \bar{1}$. Portanto, $\bar{a} \cdot \bar{b} + \bar{0} \cdot \overline{(-q)} = \bar{1}$, concluindo que, $\bar{a} \cdot \bar{b} = \bar{1}$, e portanto $\bar{a}$ é inversível em $\mathbb{Z}_m$.

■

Indicaremos o inverso de $\bar{a}$ por $\bar{a}^{-1}$ e o conjunto dos elementos invertível de $\mathbb{Z}_m$ por U($\mathbb{Z}_m$), isto é,

$$\text{U}(\ \mathbb{Z}_m) = \{\ \bar{a} \in \mathbb{Z} : (a, m) = 1\ \}\ .$$

Por exemplo, U($\mathbb{Z}_7$) =$\{\ \bar{1}, \bar{2}\ , \bar{3}, \bar{4}, \bar{5}, \bar{6}\ \}$, pois $(a, 7) = 1$ para $a = 1, 2, 3, 4, 5$ e 6. Temos:

$$\bar{1} \cdot \bar{1} = \bar{1} \Rightarrow \bar{1}^{-1} = \bar{1} \text{ e } \bar{1} = \bar{1}^{-1};$$
$$\bar{2} \cdot \bar{4} = \bar{1} \Rightarrow \bar{4}^{-1} = \bar{2} \text{ e } \bar{2}^{-1} = \bar{4};$$
$$\bar{3} \cdot \bar{5} = \bar{1} \Rightarrow \bar{5}^{-1} = \bar{3} \text{ e } \bar{3}^{-1} = \bar{5};$$
$$\bar{6} \cdot \bar{6} = \bar{1} \Rightarrow \bar{6}^{-1} = \bar{6} \text{ e } \bar{6} = \bar{6}^{-1}.$$

Percebe-se que trabalhando as classes residuais, desenvolve-se uma estrutura importante nos elementos da álgebra que são os anéis como define(GARCIA; LEQUAIN, 2006).

Definição 4.17. *Um anel ou anel comutativo $(A, +, \cdot)$ é um conjunto A com pelo menos dois elementos, munidos de uma operação denotada por $+$ (chamada adição) e de uma operação denotada por $\cdot$(chamada multiplicação) que satisfazem as condições:*

Comutativa, associativa, elemento neutro e elemento simétrico com relação à adição. Mas, com relação à multiplicação temos as seguintes propriedades válidas, comutativa, associativa, elemente neutro e distributiva.

Portanto, com estas propriedades da adição $\oplus$ e da multiplicação $\odot$ em $\mathbb{Z}_m$, temos que $\mathbb{Z}_m$ é anel, denominado das classes residuais módulo m.

5 SEQUÊNCIA DIDÁTICA

Neste capítulo, apresentamos como foi organizada nossa sequência didática, a qual foi dividida em sete encontros envolvendo conteúdos da Aritmética, onde abordamos um breve contexto histórico da temática assim como algumas aplicações relacionadas com o tema. O principal objetivo em uma sala de aula é agregar novos conhecimentos aos alunos.

> Por educar entendemos atuar junto ao sujeito visando seu integral desenvolvimento; já ensinar para nós é agir de forma a possibilitar ao educando o acesso ao conhecimento, intermediando sua busca por novos horizontes em direção à cidadania.(BALESTRA, 2012, p.24)

De acordo com (ARAÚJO, 2013), as Sequências Didáticas são modos do professor organizar suas atividades educacionais por meio de temas e procedimentos a serem aplicados. Dessa forma, o professor precisa buscar formas de incluir os alunos em todos os âmbitos da aprendizagem, desde a elaboração de uma aula até o seu resultado, que é o aprendizado do conteúdo estudado. O aluno precisa enxergar o que aquele aprendizado terá de útil em sua vida, pois assim terá cada vez mais interesse em aprender. Com isso, é muito importante que o professor ouça os seus educandos, e assim busque alternativas para estimular o interesse e a busca por conhecimento.

Corroborando com esse pensamento, (ZABALA, 1998, p.18) afirma que sequência didática é "um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecido tanto pelos professores como pelos alunos". Assim, compreendemos que a sequência didática se refere à organização de atividades bem planejadas com o intuito de tornar as aulas mais atraentes para os alunos e assim instiguem-os a vivenciar essas práticas no seu próprio cotidiano.

Sabemos que o conhecimento matemático é essencial para todo aluno da educação Infantil, Fundamental e Médio, pois fornece recursos fundamentais na sociedade contemporânea para que o aluno seja um cidadão crítico e responsável por suas ações na comunidade em que se encontra inserido.

Vale salientar que os ensinos Infantil, Fundamental e Médio tem a responsabilidade do desenvolvimento do letramento matemático, processos matemáticos que envolve resolução de problemas, habilidades e competências (específicas e gerais) que serão orientadas por meio dos documentos normativos como a **BNCC**(BRASIL, 2018) e pela **PCEMPB**(PARAÍBA, 2021). Estes documentos também determinam que essas competências, habilidades e conteúdos devem ser os mesmos, independentemente de onde as crianças, os adolescentes e os alunos moram ou estudam.

Nessa linha, a Lei de Diretrizes e Bases da Educação Nacional **(LDB)** de nº 9.394, de 20 de dezembro de 1996, no Art. 26 retoma a necessidade de uma Base Comum Curricular a ser complementada em cada sistema de ensino e em cada estabelecimento escolar, como é comentado na (LDB, 2017).

Diante disso, desenvolvemos uma sequência didática composta por sete encontros e aplicado em uma turma de 3º ano do Ensino Médio da Escola Estadual de Ensino Fundamental e Médio Major Veneziano Vital do Rêgo na cidade de Campina Grande-PB, as quais planejamos os objetivos e procedimentos necessários para alcançá-los. Sendo assim, a cada encontro apresentamos a unidade temática, modalidade/nível de Ensino, objetos de conhecimento, habilidades, objetivos/expectativas de Aprendizagem, estratégia de ensino, materiais utilizados e a duração das atividades em cada encontro da sequência desenvolvida.

Para estes encontros, utilizamos alguns recursos que consideramos fundamentais para ensino/aprendizagem do aluno, como a Criptografia, a utilização de algoritmos matemáticos associados à linguagem de programação Python e também recorremos ao lúdico na criação de um jogo intitulado "Trilha da Aritmética". As fontes principais que usamos foram o livro do Programa de Iniciação Científica da OBMEP **(PIC)**, Criptografia (COUTINHO, 2015), (MEDINA; FERTING, 2006), o Complemento da **BNCC** da Computação (BRASIL, 2022) e (GRANDO, 2004).

A Criptografia em grego, "crytos" significa secreto, oculto que estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos" secretos como afirma (COUTINHO, 2015).

Em nosso trabalho aplicamos a Criptografia com as Cifras de Hill, e os alunos por meio do conhecimentos de matrizes e determinantes conseguiam codificar e decodificar algumas palavras simples. Mas existem duas condições fundamentais para ocorrer a Criptografia: haja reversibilidade e o receptor detenha uma chave. Com estes elementos os alunos tiveram uma experiência incrível sobre como funciona o processo de codificar e decodificar mensagens secreta.

Outro ponto relevante abordado em nossos encontros, foram o uso de algoritmos relacionados à linguagem de programação Python. Neste tópico trabalhamos a aplicação dos algoritmos matemáticos na computação. As definições de algoritmos segundo (MEDINA; FERTING, 2006) são:

- Um procedimento passo a passo para solução de um problema;
- Uma sequência detalhada de ações a serem executadas para realizar alguma tarefa.

A escolha pela linguagem Python foi por conta de ser uma linguagem de programação com forte apelo e conhecida por muitos programadores, como comenta (MCKINNEY, 2018). Surgiu por volta de 1991, e possui o código aberto (pode ser modificado por programadores) podendo ser usado de forma comercial ou acadêmica.

A utilização desta linguagem de programação foi com objetivo pedagógico e usual, a nossa intenção foi apenas de apresentar o aplicativo e não programar (criar e desenvolver programas), pois, ensinar programação de forma completa demandaria muito tempo, por isso os programas utilizados são apenas exemplos de aplicação e uso de algoritmos.

É comum a nós professores associarmos a ideia de jogo como um instrumento motivacional, mas na verdade o jogo é mais do que isso, é uma atividade lúdica. Definir o jogo é um desafio, pois existem diversas vantagens e desvantagens (GRANDO, 2004). Mas o professor (mediador) deve planejar as estratégias mais convenientes para que o processo de ensino/aprendizagem seja significativo.

Percebe-se que muitas vezes nossos alunos ficam muito entediados com a parte conceitual formal, pois esta conceituação na maioria das situações é transmitida de forma abstrata. A palavra Lúdico vem do latim "Ludus" que significa jogo e divertimento, como afirma (ROLOFF, 2010). Assim, as atividades lúdicas têm por finalidade proporcionar uma convivência e um interação melhor com os alunos e professor, criando um ambiente de competição saudável onde todos os envolvidos conseguem aprender e se divertir simultaneamente, como comenta (SILVA et al., 2013).

Acreditamos que por meio do lúdico podemos obter resultados mais positivos com relação ao ensino. Estes autores ainda reforçam a ideia de que é possível ensinar Matemática de forma divertida sem atrapalhar o entendimento dos conceitos formais, definições e propriedades.

A sequência didática aplicada foi organizada da seguinte forma: nos sábados das 9 h às 12 h, com tempo estimado de cada encontro de 3 h. Cada encontro é representado no quadro abaixo.

Quadro 01: Organização dos Encontros

Encontro 01: 06/04/2024	**Questionário de Sondagem, História da Aritmética, Algoritmo da Divisão, Múltiplos, Divisores e Linguagem de Programação Python.**
Encontro 02: 13/04/2024	**Algoritmo da Divisão, Critério de Divisibilidade, Crivo de Eratóstenes, Números Primos de Mersenne e Linguagem de Programação Python.**
Encontro 03: 20/04/2024	**Teorema Fundamental da Aritmética, Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC). Apresentação de exemplos simples e problemas contextualizados de Olimpíadas (OBMEP).**
Encontro 04: 27/04/2024	**Ideias de Congruência e construção das tábuas de operação (Adição e Multiplicação). Aplicação de alguns problemas envolvendo a Aritmética, Calendários e Relógios.**
Encontro 05: 04/05/2024	**Cifras de Hill (Retomando alguns conceitos e definições importantes de Matrizes e Determinantes).**
Encontro 06: 11/05/2024	**Cifras de Hill (Apresentando a ideia de Criptografia e Cifras em questão).**
Encontro 07: 18/05/2024	**Aplicação do Jogo intitulado "Trilha da Aritmética" e do questionário de avaliação da metodologia utilizada em sala de aula.**

Fonte: Elaborado pelo autor (2024)

A sequência didática foi planejada para ser executada em 7 encontros. Vale ressaltar que o tempo pedagógico pode ser ajustado de acordo com a necessidade e o nível de cada turma.

5.1 Descrição dos encontros da sequência didática

5.1.1 1º ENCONTRO

1. **Unidade Temática BNCC: Números.**
2. **Modalidade/Nível de Ensino: 3º do Ensino Médio.**

3. **Objetos de Conhecimento BNCC:**

   - Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações;
   - Operações (adição, subtração, multiplicação, divisão e potenciação) com números naturais;
   - Fluxograma para determinar a paridade de um número natural;
   - Múltiplos e divisores de um número natural.

4. **Habilidades BNCC:**

   - **(EF06MA04)** Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par);
   - **(EF06MA06)** - Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor;
   - **(EM13MAT406)** - Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.

     Vale ressaltar que o item **(EM13MAT406)** foi retirado do documento da BNCC, mas a mesma habilidade se encontra no documento normativo PCEMPB.

5. **Objetivos/Expectativas de Aprendizagem:**

   - Abordar os princípios que deram origem aos números, processo de contagem e a sua evolução;
   - Apresentar os múltiplos e divisores de um número natural.

6. **Estratégia de Ensino e materiais utilizados:**

   - Aulas expositivas;
   - Quadro, pincel, apagador, livro didático e retroprojetor;
   - Material obtido no site da OBMEP;
   - Algoritmos envolvendo à linguagem de programação Python.

7. **Duração da atividade:** 3 horas (aos sábados das 9 h às 12 h).

Sequência Didática I – Encontro 01

Neste primeiro momento, introduziremos a história da Aritmética, mas especificamente, na Pré-História em que o homem passar a ter contato com a ideia de contagem, e consequentemente, passando a associar número com objetos, a fim de promover uma sociedade mais desenvolvida.

A ideia de números remonta a aproximadamente 30.000 anos atrás com a preocupação de registrar a quantidade de familiares, de animais e de objetos importantes para uma determinada comunidade tribal (HYGINO, 1991).

Um dos principais recursos para a contagem eram pedras, galhos, dedos das mãos, e as vezes até dos pés, para indicar a quantidade de elementos e posteriormente veio uma escrita rudimentar em paredes associando números com objetos. Este fato foi muito relevante para que estas informações fossem armazenadas e transmitidas para as gerações seguintes.

Mas o avanço do conceito de contagem de número ocorreu de forma lenta e em etapas difíceis de estipular. Por exemplo, o símbolo ou o som que foi empregado primeiro? Segundo (HYGINO, 1991), provavelmente, os símbolos surgiram primeiro com a intenção de representar os objetos, pessoas e animais para depois os sons serem utilizados e abordados para cada situação.

A primeira civilização a aplicar estes símbolos foram as pessoas que viviam nos vales dos Rio Nilo, Tigres e Eufrades. Mas temos registros também nos vales Indo e Yangtse Kiang na China a cerca de 6000 anos.

Podemos observar que estes símbolos foram fundamentais para a criação dos números naturais, inteiros, operações e suas propriedades.

Figura 4 – Rio Nilo

Fonte:<https://escolakids.uol.com.br/geografia/rio-nilo.htm>

Figura 5 – Rio Indo

Fonte:<https://blogcatedranaval.com/tag/rio-indo>

Figura 6 – Rio Yangtse

Fonte:<https://kids.britannica.com/kids/article/Yangtze-River/353943>.

Os números naturais foram representados ao longo da história de diversas formas diferentes, mas para este trabalho, convencionaremos o conjunto dos números naturais da seguinte forma:

$\mathbb{N} = \{0, 1, 2, \cdots\}$.

Já o conjunto dos números inteiros da seguinte maneira:

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

As definições apresentadas a seguir estão baseadas nos livros Programa de Iniciação Científica da OBMEP e o Livro de Aritmética utilizado no programa PROFMAT. Para maiores detalhes veja (HEFEZ, 2009) e (HEFEZ; ARITMÉTICA, 2009).

Definição de múltiplo de um número natural:

Dado um número natural a, consideremos o conjunto dos múltiplos naturais de a:

$$a\mathbb{N} = \{a \cdot d \mid d \in \mathbb{N}\}.$$

Múltiplos Comuns:

Considere o conjunto dos múltiplos de $3 = \{0, 3, 6, 9, 12, \cdots\}$ e o conjunto dos múltiplos $5 = \{0, 5, 10, 15, 20 \cdots\}$.

Portanto, o conjunto que representa os múltiplos comuns de 3 e 5 é mostrado abaixo: $\{0, 15, 30, 45, 60, \cdots\}$.

Definição de Múltiplos Comuns:

Os números que pertencem simultaneamente ao conjunto dos múltiplos de dois ou mais números dados será chamado de múltiplos comuns destes números.

Observação: Se a e b são números naturais não nulos, sabemos que o número $a \cdot b$ é um múltiplo de a; por outro lado, pela propriedade comutativa da multiplicação, tem-se que ele também um múltiplo de b. Assim, o conjunto dos múltiplos comuns de a e b, além de conter o número 0, contém também o número $a \cdot b \neq 0$.

Exercício 01: Determine os múltiplos comuns de 3 e 4.

Definição de divisores de um número natural:

Diremos que um número natural d é um divisor de outro natural a, se a é múltiplo de d, ou seja, se $a = d \cdot c$, para algum natural a. Representamos o conjunto dos divisores de um número natural n por $D(n)$.

Exercício 02: Determinar todos os divisores de 20.

Definição de divisores comuns:

São números que são divisores simultaneamente de dois ou mais números dados.

Exercício 03: Determine os divisores naturais comuns dos números 18 e 3.

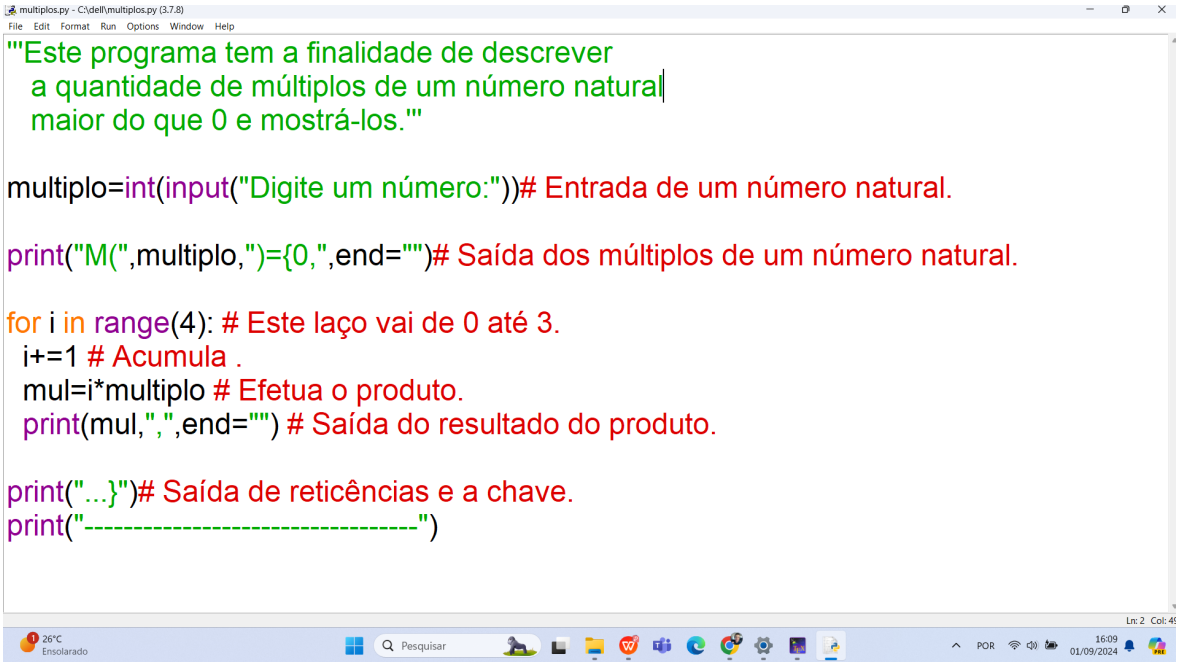
Vale ressaltar que após a aula expositiva, tivemos um momento utilizando e aplicando a linguagem Python, neste primeiro momento verificamos alguns exemplos de múltiplos.

Esta linguagem de programação foi executada pelo professor em computador pessoal, os alunos participavam sugerindo exemplos, em sala de aula, com o objetivo de mostrar como a programação é uma ferramenta interessante para o desenvolvimento do conhecimento matemático dos alunos. Como mostra a **BNCC Complementar**

em Computação (BRASIL, 2022).

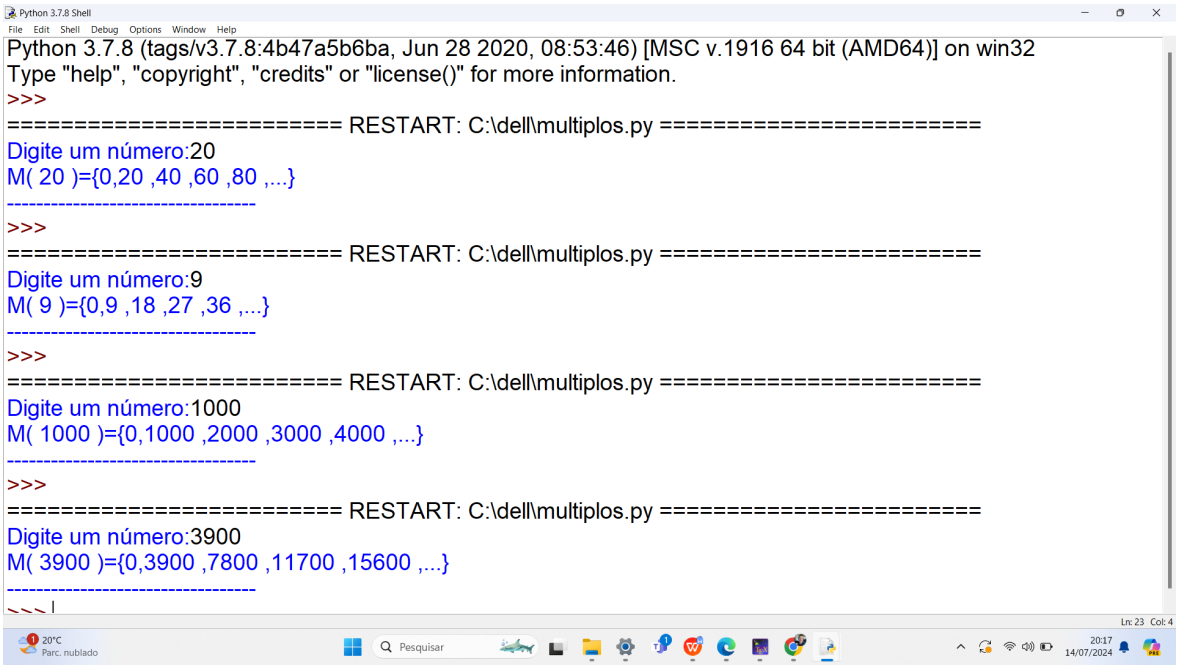
Obs.: Percebe-se que, nos códigos fontes tem-se a presença das aspas triplas abrindo "'*e aspas triplas fechando* "', esta parte do comando significa comentários em blocos, já com relação ao símbolo # (cerquilha), significa comentários em linha. O restante do código faz parte do corpo do programa.

Figura 7 – Código fonte 01: Múltiplos de um número natural



Fonte: Elaborado pelo Autor (2024)

Figura 8 – Execução do código fonte 01: Múltiplos de um número natural



Fonte: Elaborado pelo Autor (2024)

5.1.2 2º ENCONTRO

1. **Unidade Temática BNCC:** Números.
2. **Modalidade/Nível de Ensino:** 3º do Ensino Médio.
3. **Objetos de Conhecimento BNCC:**
   - Divisão euclidiana;
   - Fluxograma para determinar a paridade de um número natural;
   - Números primos e composto.
4. **Habilidades BNCC:**
   - **(EF06MA05)** - Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos “é múltiplo de”, “é divisor de”, “é fator de”, e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6,7, 8, 9, 10,11 e assim por diante;
   - **(EF06MA04)** Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par);

- **(EM13MAT406)** - Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.
  Vale ressaltar que o item **(EM13MAT406)** foi retirado do documento da BNCC, mas esta habilidade se encontra no documento normativo PCEMPB.

5. **Objetivos/Expectativas de Aprendizagem:**

   - Trabalhar com os números primos e compostos;
   - Investigar e discutir o Crivo de Eratóstenes.

6. **Estratégia de Ensino e materiais utilizados:**

   - Aulas expositivas;
   - Atividades sobre os critérios de divisibilidade;
   - Quadro, pincel, apagador, livro didático e retroprojetor;
   - Material obtido no site da OBMEP.

7. **Duração da atividade:** 3 horas (aos sábados das 9 h às 12 h).

Sequência Didática I – Encontro 02

Neste encontro, abordaremos os conceitos de Divisão euclidiana, Critérios de Divisibilidades, Crivo de Eratóstenes e Números Primos de Mersenne.

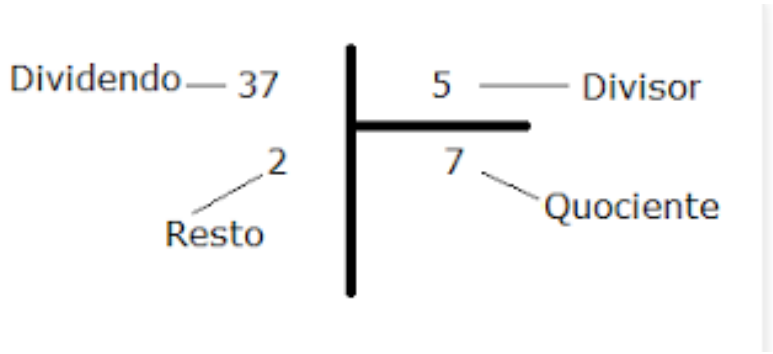
Algoritmo da Divisão

Uma das propriedades mais importantes dos números naturais é a possibilidade de dividir um número por outro com resto pequeno. Essa divisão é a chamada divisão euclidiana. Dados dois números naturais a e b, com $b \neq 0$, existem números naturais q e r tais que $a = b \cdot q + r$, onde $0 \leq r < b$. Chamamos a, b, q e r de dividendo, divisor, quociente e resto, respectivamente.

$$\begin{array}{r|l} \text{a} & \text{b} \\ \hline r & q \end{array}$$

Vamos verificar como funciona o algoritmo da divisão euclidiana em um caso particular.

Figura 9 – Divisão de 37 por 5



Fonte:<https://sempreamathematicarcommusica.blogspot.com/2011/01/identidade-fundamental-da-divisao.html>

Temos, $37 = 5 \cdot 7 + 2$, portanto a divisão foi efetuada de forma correta.

Exercício 04: Usando o Algoritmo da Divisão efetue a divisão de 1436 por 7.

A seguir relembraremos alguns critérios importantes de divisibilidade que foram estudados em séries anteriores.

Critério de divisibilidade por 2

Um número N é divisível por 2 quando seu algarismo das unidades for divisível por 2.

Critério de divisibilidade por 3

Um número N é divisível por 3 se a soma dos seus algarismos for um número divisível por 3.

Critério de divisibilidade por 4

Um número N é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4, ou seja, quando o número formado pelos algarismos das dezenas e das unidades de N é divisível por 4.

Critério de divisibilidade por 5

Um número é divisível por 5 se seu algarismo das unidades é 0 ou 5.

Critério de divisibilidade por 6

Um número N é divisível por 6 quando N é divisível por 3 e por 2.

Critério de divisibilidade por 7

Dado um número natural N, considere $N = 10 \cdot b + a$, onde a é o algarismo das unidades de N. Se $b - 2 \cdot a$ é divisível por 7, então N é divisível por 7.

Exemplo 01: Para decidir se o número $N = 86415$ é divisível por 7, devemos aplicar o critério de divisibilidade por 7 diversas vezes até percebemos que o número é divisível por 7 ou não.

86415 $\rightarrow$ 8641 - $2 \cdot 5 = 8631 \rightarrow$ 863 - $2 \cdot 1 = 861 \rightarrow$ 86 - $2 \cdot 1 = 84 \rightarrow$ 8 - $2 \cdot 4 = 0$.

Usando o critério, temos:

0 é múltiplo de 7 $\rightarrow$ 84 é múltiplo de 7 $\rightarrow$ 861 é múltiplo de 7 $\rightarrow$ 8631 é múltiplo de 7 $\rightarrow$ 86415 é múltiplo de 7.

Critério de divisibilidade por 9

Um número N é divisível por 9 se a soma dos seus algarismos for um número divisível por 9.

Critério de divisibilidade por 10

Um número é divisível por 10 se seu algarismo das unidades é 0.

Critério de divisibilidade por 11

Um número natural N é divisível por 11 quando a diferença não negativa entre a soma dos algarismos de ordem ímpar (Soi) e a soma dos algarismos de ordem par (Sop) for um número divisível por 11.

Exemplo 02: Considere o número $N = 3767632$. Temos:

7^a	6^a	5^a	4^a	3^a	2^a	1^a
3	7	6	7	6	3	2

Assim, S_{oi} = 2+6+6+3 = 17 e S_{op} = 3+7+7 = 17. Agora observe que S_{oi} -S_{op} = 17-17= 0 é divisível por 11, o número N é divisível por 11.Aqui, o significado de "diferença não negativa" é semelhante ao que aparece no primeiro critério de divisibilidade por 7. Lembrando que S_{oi} é o somatório dos números das classes ímpares e S_{op} é o somatório dos números das classes pares.

Exercício 05: Classifique as seguintes afirmações em verdadeira (V) ou falsa (F):

a) ( ) 2374160 é divisível por 2

b) ( ) 202428 é divisível por 3

c) ( ) 3263612 é divisível por 11

d) ( ) 14777 é divisível por 7

e) ( ) 20025 é divisível por 9

f) ( ) 20002 é divisível por 5

g) ( ) 32147800003 é divisível por 10

Questão para pensar: Em grupos estabeleçam um critério de divisibilidade por 16, isto é, quando um número é divisível por 16?

A seguir, apresentaremos um conceito de grande importância na Matemática: o fato de um número ser primo ou não. Esses números desempenham um papel fundamental e a eles estão associados muitos problemas famosos cujas soluções tem resistido aos esforços de várias gerações de matemáticos (HEFEZ; ARITMÉTICA, 2009).

Definição de números primos: Um número natural maior do que 1 que possui como divisores positivos 1 e ele próprio é chamado número primo.

Exemplo 03: São exemplos de números primos: 2, 3, 5, $\cdots$.

Definição de números compostos: Um número maior que 1 e que não é primo será dito composto.

Exemplo 04: São exemplos de números compostos: 4, 6, 9, 10, 12, $\cdots$.

Crivo de Eratóstenes

Eratóstenes foi um estudioso que viveu no século III a.C. Nasceu em Cirene, na África, e morreu em Alexandria, na Grécia. Teve um destaque muito grande na comunidade científica da época com diversos trabalhos em matemática, ciência, filosofia, geografia e em outras áreas.

Figura 10 – Eratóstenes

Fonte:<http://www.geografia.seed.pr.gov.br/modules/galeria/detalhe.php?foto=1063&evento=1>

Mas, o trabalho que mais teve destaque foi o Crivo de Eratóstenes, que explicaremos a seguir. Considere um número natural n. Por exemplo, $n = 32$. Agora, listamos todos

os números de 1 a 32 em um quadro. Nosso objetivo é determinar quais são todos os números primos de 1 até 32.

Tabela 01 - Números de 1 até 32

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	26	27	28	29	30	31	32

Fonte: Elaborado pelo autor (2024)

A princípio poderíamos fazer uma varredura com todos os números, mas este processo seria muito exaustivo. Porém, graças ao Crivo de Eratóstenes, podemos realizar o processo de eliminação, onde em cada passo descartamos da tabela alguns números dos quais temos certeza de que são compostos. Fazemos isso várias vezes de um modo bem específico para que, ao final do processo, tenhamos certeza de que os números que sobrarem sejam todos primos (HEFEZ, 2009).

Iniciaremos o processo retirando os números 1 e os múltiplos de 2. Pois, por definição, os números primos são maiores do que 1 e o 2 é o único primo par. Já os múltiplos de 2 são compostos. Logo, eles não são primos e devemos descartá-los.

Tabela 02 - Etapa 2 do Crivo de Eratóstenes

~~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	~~26~~	27	~~28~~	29	~~30~~	31	~~32~~

Fonte: Elaborado pelo autor (2024)

Continuando com este processo temos que o 3 é primo. Logo, todos os múltiplos de 3 são compostos e, portanto, riscamos todos. E ficamos fazendo este processo sucessivamente, até riscarmos todos os números compostos que desejamos 1 até N.

Tabela 03 - Etapa 3 do Crivo Eratóstenes

~~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	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~

Fonte: Elaborado pelo autor (2024)

Percebe-se que, no final deste processo, os números que não foram riscados são os números primos, como mostra a Tabela 04.

Tabela 04 - Etapa Final do Crivo Eratóstenes

~~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~~	~~26~~	~~27~~	~~28~~	29	~~30~~	31	~~32~~

Fonte: Elaborado pelo autor (2024)

Números Primos de Mersenne

Introduziremos, neste momento, alguns tipos de números primos especiais, que são denominados de números de Mersenne, uma homenagem a Marin Mersenne.

O projeto Great Internet Mersenne Prime Search (GIMPS) foi criado em 1996 por George Woltman, formado em Ciência da Computação pelo Instituto de Tecnologia de Massachusetts (MIT), é um projeto voluntário de computação distribuída, que como o próprio nome já indica, seu objetivo é encontrar números primos conhecidos como primos de Mersenne (WOLTMAN, 1996), isto é, conforme a **definição** de (HEFEZ; ARITMÉTICA, 2009), temos:

Os números de Mersenne são os números da forma

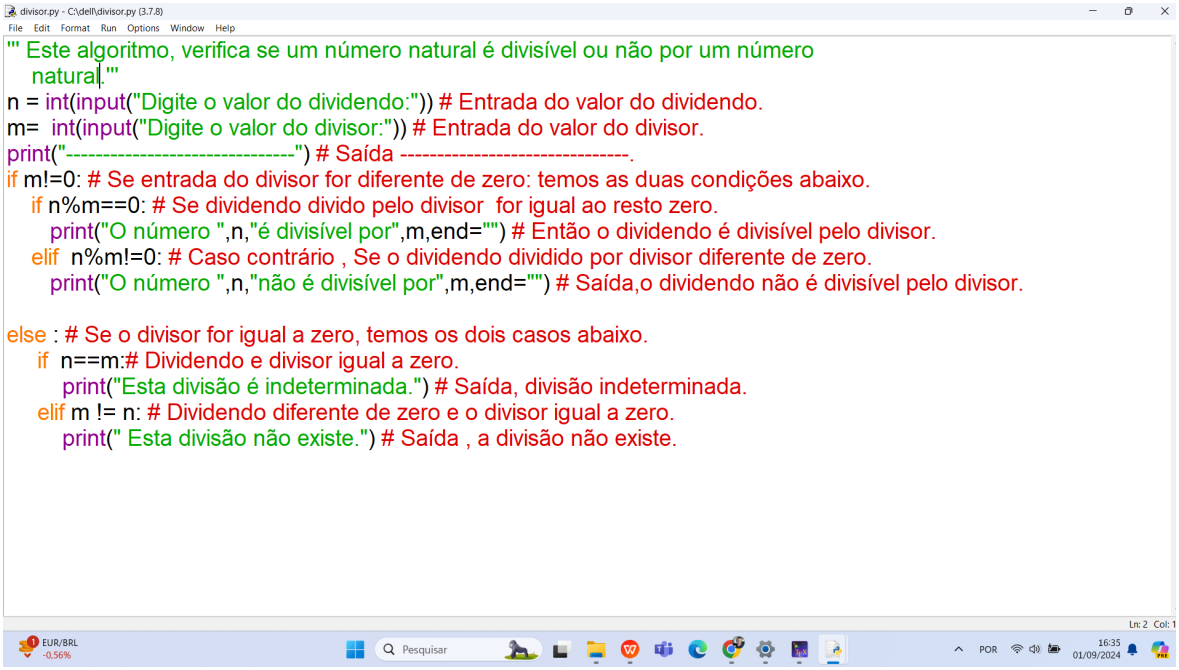
$$M_p = 2^p - 1,$$

para algum p natural maior do que 1. Onde p é um número primo.

Curiosidade: O GIMPS descobriu o maior número primo conhecido até o momento, $2^{82.589.933} - 1$, com 24.862.048 dígitos. Um computador oferecido por Patrick Laroche de Ocala, Flórida, fez a descoberta em 7 de dezembro de 2018 (WOLTMAN, 1996). Essa descoberta encontra-se no site oficial do GIMPS.

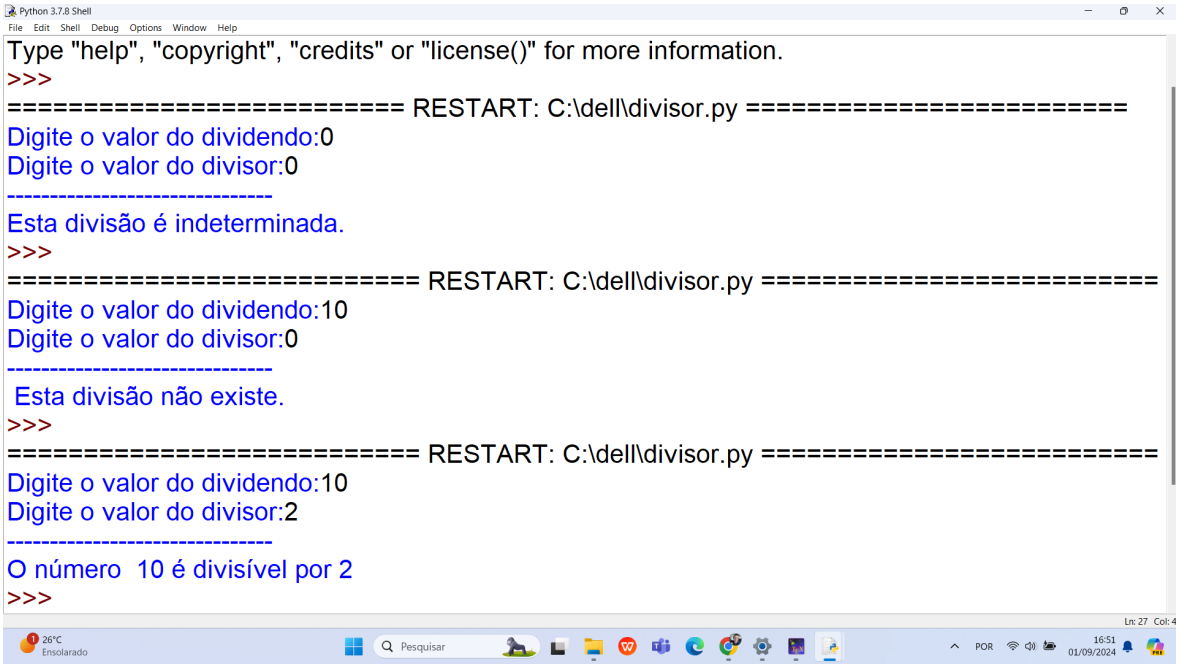
Vale ressaltar que após a aula expositiva, tivemos um momento utilizando e aplicando algoritmos à linguagem de programação Python, abaixo temos um programa que aborda o algoritmo da divisão euclidiana.

Figura 11 – Código fonte 02: Divisão euclidiana



Fonte: Elaborado pelo Autor(2024)

Figura 12 – Execução do código fonte 02: Divisão euclidiana



Fonte: Elaborado pelo Autor(2024)

5.1.3 3º ENCONTRO

1. **Unidade Temática BNCC: Números.**

2. **Modalidade/Nível de Ensino: 3º do Ensino Médio.**

3. **Objetos de Conhecimento BNCC:**

   - Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações;
   - Números primos e compostos;
   - Divisão euclidiana.

4. **Habilidades BNCC:**

   - **(EF07MA01)** - Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos;
   - **(EF07MA04)** - Resolver e elaborar problemas que envolvam operações com números inteiros;

- **(EF07MA05)** - Resolver um mesmo problema utilizando diferentes algoritmos;
- **(EM13MAT406)** - Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.

5. **Objetivos/Expectativas de Aprendizagem:**

   - Identificar que números inteiros podem ser decompostos em fatores primos;
   - Identificar que a fatoração em fatores primos é única (Teorema Fundamental da aritmética);
   - Usar o Teorema Fundamental da Aritmética e a decomposição em fatores primos além da determinação do Mínimo Múltiplo Comum (MMC) e do Máximo Divisor Comum (MDC) de números inteiro;
   - Aplicar o resultado do (MMC) e do (MDC);
   - Utilizar o algoritmo de Euclides para o cálculo do (MDC).

6. **Estratégia de Ensino e materiais utilizados:**

   - Aulas expositivas;
   - Atividades sobre Teorema Fundamental da Aritmética,(MDC) e (MMC);
   - Quadro, pincel, apagador, livro didático e retroprojetor.

7. **Duração da atividade:** 3 horas (aos sábados das 9 h às 12 h).

Sequência Didática I – Encontro 03

Neste terceiro encontro, trabalharemos o processo de fatoração, o Teorema Fundamental da Aritmética e suas aplicações. Fatorar um número significa transformá-lo em uma multiplicação (TELÁRIS, 2012). Também pode ser definido como decompor um número em um produto de fatores primos (DOLCE; IEZZI; MACHADO, 2009). O processo de fatoração é muito importante para a Matemática, pois através dele podemos simplificar e facilitar a resolução de situações-problema.

Exemplo 1: Escreva o número 1820 como um produto de números primos (CADAR; DUTENHEFNER, 2015). Pelo algoritmo da decomposição do número em fatores primos, temos:

Figura 13 – Decomposição do 1820 em fatores primos

1820	2
910	2
455	5
91	7
13	13
1	

Fonte: Elaborado pelo autor (2024)

Multiplicando os números do lado direito da barra vertical obtemos a fatoração de 1820 como produto de números primos: $1820 = 2^2 \cdot 5 \cdot 7 \cdot 13$

Teorema Fundamental da Aritmética: Todo número natural $a > 1$, ou é primo, ou se escreve como produto de números primos. E além disso, está escrita é única (HEFEZ; ARITMÉTICA, 2009).

Exemplo 2: $60 = 2^2 \cdot 3 \cdot 5$.

Quantidade de divisores: Vamos representar por $q(n)$ a quantidade de divisores do número natural n. E n pode ser escrito da seguinte forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r} .$$

Onde p_1, p_2, p_3, $\cdots$, p_r são primos e α_1, α_2, α_3,$\cdots$, α_r. São números naturais maiores que 1, então :

$q(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdots (\alpha_r + 1)$.

Exemplo 3: Determine a quantidade de divisores de 18.

Uma vez que $18 = 2^1.3^2$, tem-se $q(18) = (1+1) \cdot (1+2) = 2 \cdot 3 = 6$; portanto, existem 6 números que são divisores por 18.

O Mínimo Múltiplo Comum (MMC) de dois ou mais números naturais é o menor número, excluindo o zero, que é múltiplo desses números (DOLCE; IEZZI; MACHADO, 2009).

O MMC é o produto dos fatores primos comuns e não comuns, cada um com o maior expoente que apresenta nas formas fatoradas dos números dados (DOLCE; IEZZI; MACHADO, 2009).

Exemplo 4: Vamos calcular o MMC de 10, 15 e 21, para a resolução desta questão podemos usar três métodos distintos.

Primeiro método: listagem de múltiplos. Esse método é o que utilizaremos no **Exemplo 4**. Listamos os múltiplos de cada um dos números dados e procuramos identificar o menor número que é múltiplo de todos, isto é, que pertence a todas as listas de múltiplos. O MMC de uma lista de números naturais não nulos existe e é

único. No entanto, esse método pode ser muito trabalhoso se tivermos que lidar com números grandes.

Sejam $M(10)$, $M(15)$ e $M(21)$ os conjuntos dos múltiplos, respectivamente, de 10, 15 e 21.

$M(10) = \{0, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, \cdots, 160, 170, 180, 190, 200, 210, \cdots\}$.

$M(15) = \{0, 15, 30, 45, 60, 75, 90, 105, 120, 135, 150, 165, 180, 195, 210, \cdots\}$.

$M(21) = \{0, 21, 42, 63, 84, 105, 126, 147, 168, 189, 210, \cdots\}$.

Com exceção do zero, o menor múltiplo comum de 10, 15 e 21 é exatamente 210. Logo, $\text{MMC}(10, 15, 21) = 210$.

Segundo método: decomposição simultânea. Como o próprio nome já diz, esse método consiste em decompor simultaneamente, como produtos de fatores primos, os números dos quais queremos calcular o MMC.

Figura 14 – Decomposição simultaneamente dos números 10 , 15 e 21

10	15	21	2
5	15	21	3
5	5	7	5
1	1	7	7
1	1	1	2.3.5.7=210

Fonte: Elaborado pelo autor (2024)

Terceiro método: decomposição de fatores primos.

$10 = 2 \cdot 5$

$15 = 3 \cdot 5$

$21 = 3 \cdot 7$

Vamos retirar todos os números primos da decomposição de cada número em fatores primos e considerar os maiores expoentes de cada número primo. Logo, teremos:

MMC (10, 15, 21) $= 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

Exercício 1 (PUC MG/2001): O Mínimo Múltiplo Comum dos números 2^3, 3^n e 7 é 1512. O valor de n é:

A) 3

B) 4

C) 5

D) 6

E) 7

Exercício 2 (IFCE 2020): Um relógio A bate a cada 15 minutos, outro relógio B bate a cada 20 minutos, e um terceiro relógio C, a cada 25 minutos. O menor intervalo de tempo decorrido entre duas batidas simultâneas dos três relógios, em horas, é igual:

A) 3

B) 4

C) 5

D) 6

E) 7

O Máximo Divisor Comum de dois ou mais números naturais é o maior número que é divisor de todos esses números (DOLCE; IEZZI; MACHADO, 2009). O MDC é o produto dos fatores primos comuns, cada um com o menor expoente que apresenta nas fatorações dos números dados (DOLCE; IEZZI; MACHADO, 2009) .

Exemplo 5: Os números 12, 18 e 30 têm conjuntos de divisores, respectivamente, dados por:

$D(12) = \{1, 2, 3, 4, 6, 12\}$;

$D(18) = \{1, 2, 3, 6, 9, 18\}$;

$D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

O maior número divisor comum entre 12, 18 e 30 é exatamente 6.

Portanto, MDC (12, 18, 30)= 6.

Primeiro método: listagem de divisores. Consiste no que já foi feito no **Exemplo 5**. Listamos os divisores de cada número e procuramos o maior dentre os divisores comuns a todos. Esse método não será eficaz se os números dados tiverem muitos divisores.

Segundo método: divisões sucessivas. Esse método, também conhecido como algoritmo de Euclides, pode ser aplicado para o cálculo do MDC entre dois números naturais. Mais adiante veremos que, aplicando-o várias vezes, também é possível usá-lo para o cálculo do MDC de mais de dois números. O método se baseia nas duas observações a seguir.

O método consiste nos seguintes passos:

1. Se os dois números são iguais a zero, o MDC não existe.

2. Se um dos números for igual a zero, o MDC será o outro número.

3. Se os dois números são diferentes de zero, mas são iguais, o MDC será qualquer um dos dois.

4. Se os dois números são diferentes de zero e diferentes um do outro, divida o maior pelo menor.

5. Se o resto da divisão for igual a zero, o MDC é o menor dos números.

6. Se o resto da divisão for diferente de zero, retorne ao passo 4, substituindo o maior número pelo menor e o menor número pelo resto.

7. Repita os passos 4, 5 e 6 até o resto da divisão ser igual a zero.

Geralmente, usamos uma grade para facilitar a compreensão, um bom exemplo, esta na Figura 11.

Exemplo 6: Usando agora o algoritmo de Euclides calcularemos o MDC(124, 48). De início, colocamos os dois números na linha do meio da grade, sendo o maior número (124) colocado na primeira casa à esquerda e o menor número (48) colocado na segunda casa, ao lado do maior número.

Figura 15 – Algoritmo de Euclides (MDC)

Quocientes:	2	1	1	2	2
124	48	28	20	8	4
Restos: 28	20	8	4	0	

Fonte: Elaborado pelo autor (2024)

O algoritmo de Euclides é uma ferramenta muito eficiente para encontrar o Máximo Divisor Comum de dois números quaisquer diferente de zero de maneira rápida e objetiva.

O método consiste em efetuar sucessivas divisões entre os dois números seguidos que constam na segunda linha, da seguinte forma. Neste processo colocamos o quociente de cada divisão na primeira linha, acima do divisor, e o resto correspondente na terceira linha abaixo do dividendo.

Inicialmente dividimos 124 por 48, obtendo quociente 2 e resto 28. Uma vez que o resto da divisão é não-nula, adicionamos o resto 28 após o 48 na segunda linha. Agora dividimos 48 por 28, obtendo quociente 1 e resto 20, como mostra a Figura 15. Continuamos este processo até que o resto da divisão seja iguala zero. Neste caso, o máximo divisor comum será o último resto não nulo da terceira linha, ou seja, MDC (124, 48)= 4.

Terceiro método: decomposição em fatores primos. Sejam a_1, a_2, $\cdots$, a_n números naturais diferentes de zero. Se um deles for igual a 1, o (MDC) de todos esses números também será igual a 1. Caso contrário, podemos escrever cada um deles como

produto de números primos e em seguida considerar o produto dos primos em comum nas fatorações, com os maiores expoentes de cada número primo comum.

Exemplo 7: Determine o Máximo Divisor Comum MDC (12, 18, 30) fatorando os três números.

$12 = 2^2 \cdot 3$.

$18 = 2 \cdot 3^2$.

$30 = 2 \cdot 3 \cdot 5$.

Para encontrar o Máximo Divisor Comum de três números quaisquer basta observarmos os primos que dividem simultaneamente, os três números fatorados dados, logo sao 2 e 3. O primo 2 aparece com expoente 1 na decomposição de 12, 18 e 30 e o número primo 3 aparece com expoente 1 na decomposição de 12, 18 e 30. Devemos escolher o menor expoente e os números primos que dividem simultaneamente os três número, para enfim encontrar o (MDC).

Portanto, o Máximo Divisor Comum dos três números será $2 \cdot 3 = 6$.

Este recurso pode se realizar com dois ou mais números, tornando-se um artifício muito eficiente e utilizado.

Exercício 3 (Vunesp 2023): Um ajudante de uma loja de ferragens precisa distribuir, em saquinhos de plásticos, três tipos diferentes de parafusos, de agora em diante identificados com tipo A, B e C. Todos os saquinhos devem conter a mesma quantidade de parafusos e sempre parafusos de um mesmo tipo. Também foi pedido ao ajudante que cada saquinho tivesse a maior quantidade possível de parafusos. Sabendo que são 132 parafusos do tipo A, 180 parafusos do tipo B e 228 parafusos do tipo C, o número de saquinhos necessários para cumprir essa tarefa é:

A) 30

B) 34

C) 42

D) 45

E) 48

Obs.: Podemos também relacionar o Máximo Divisor Comum com o Mínimo Múltiplo Comum. Esta relação é muito fácil, mas o leitor não deve ter a ilusão de que este recurso pode ser utilizado com números grandes, pois teremos um trabalho muito desgastante. Para estes números grandes é mais eficiente utilizarmos o algoritmo de Euclides (HEFEZ, 2009).

Sejam a e b dois números naturais não nulos. Então:
MMC $(a, b)\cdot$ MDC $(a, b) = a \cdot b$.

Exercício 4 (Aprendiz de Marinheiro - 2016): Sejam $A = 120$, $B = 160$, $x =$ MMC (A, B) e $y =$MDC (A, B), então o valor de $x + y$ é igual a:

A) 460

B) 480

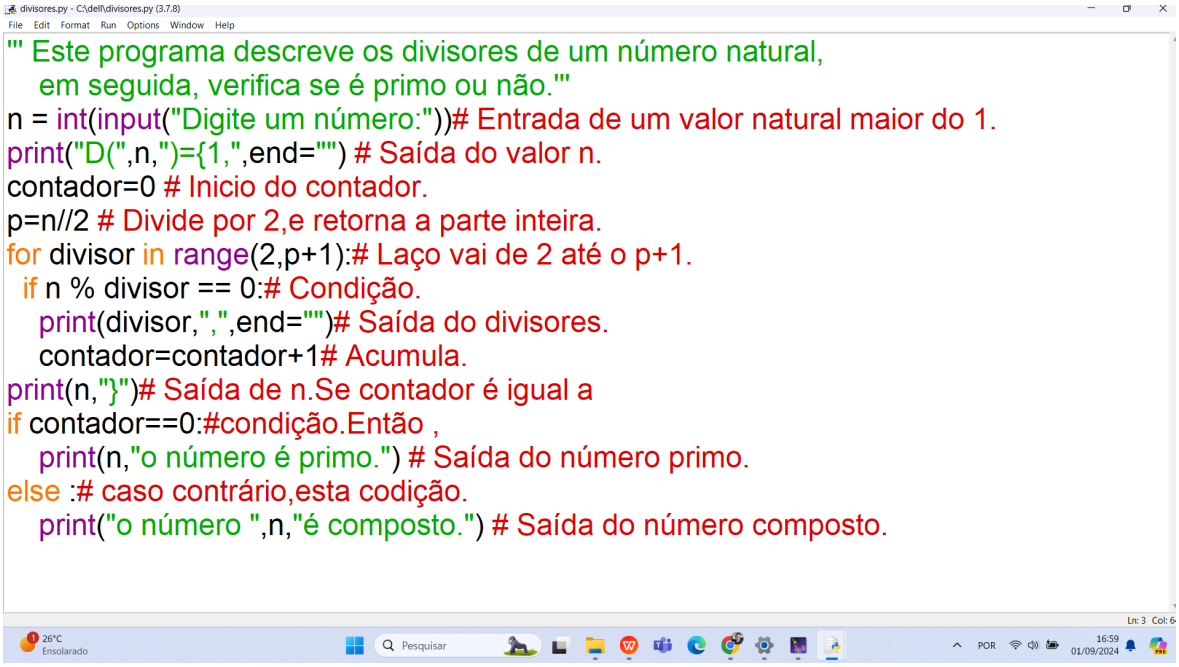
C) 500

D) 520

E) 540

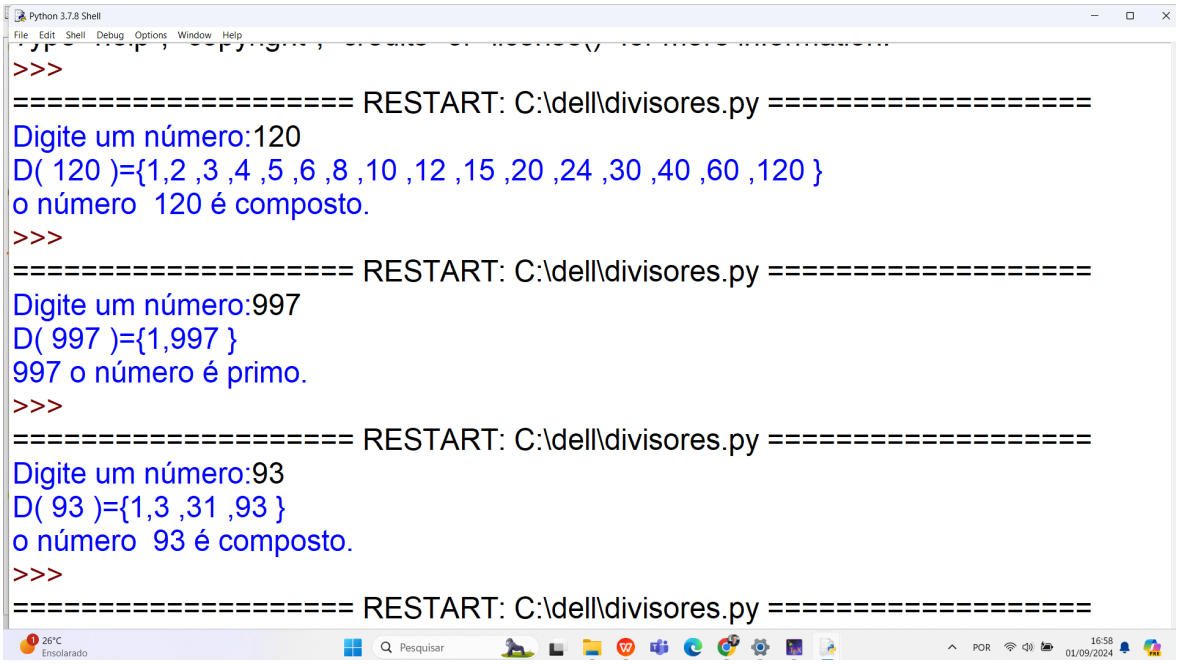
Observe que, os programas tem a finalidade de ser aplicados, pois segundo o documento da BNCC complementar da computação, podemos utilizar a linguagem de programação Python e associar com os conteúdos transversais ou por meio da interdisciplinaridade. Vejamos dois programas um que aborda os divisores de um número e verifica se ele é primo ou não. E outro programa que utiliza o algoritmo de Euclides para encontrar o (MDC) e (MMC). Vejamos os programas a seguir.

Figura 16 – Código fonte 03: Divisores, primos e compostos



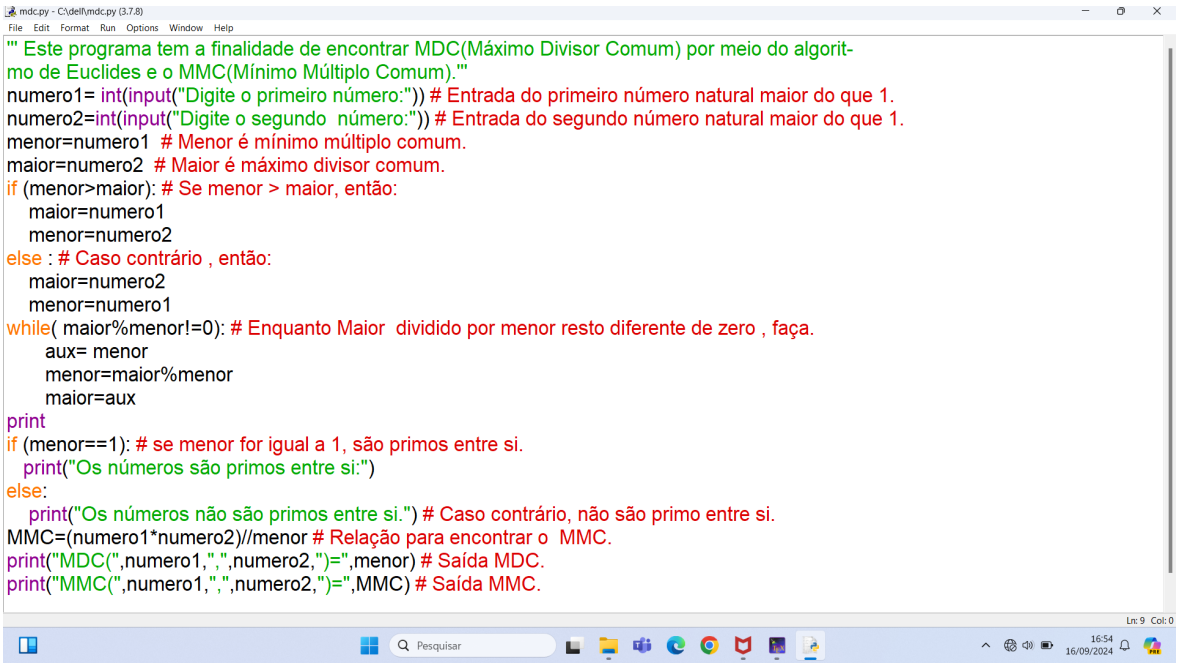
Fonte: Elaborado pelo Autor (2024)

Figura 17 – Execução do código fonte 03: Divisores, primos e compostos



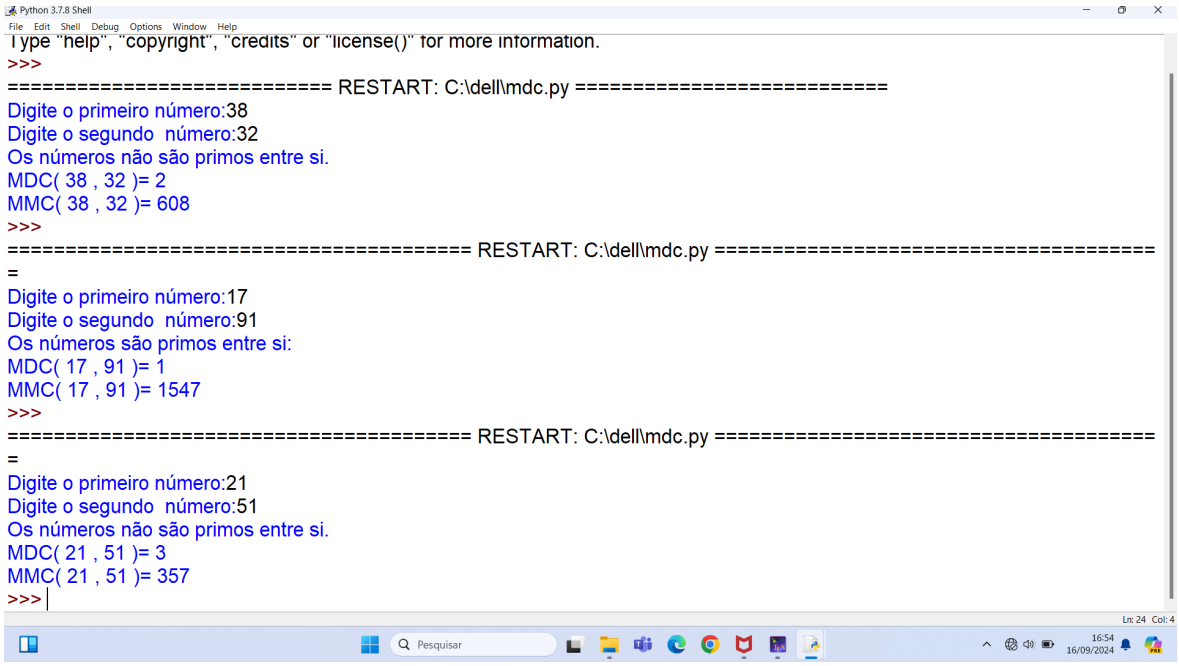
Fonte: Elaborado pelo Autor (2024)

Figura 18 – Código fonte 04: (MDC) e (MMC)



Fonte: Elaborado pelo Autor (2024)

Figura 19 – Execução do código-fonte 04: (MDC) e (MMC)



Fonte: Elaborado pelo Autor (2024)

5.1.4 4º ENCONTRO

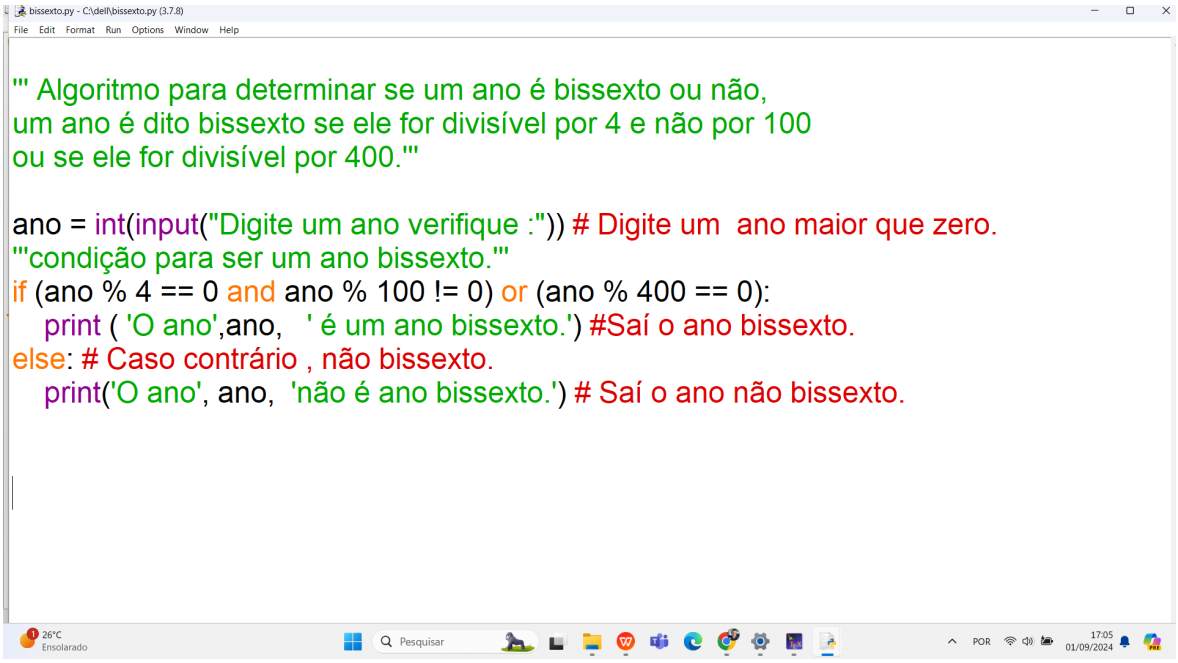
1. **Unidade Temática:** Números.
2. **Modalidade/Nível de Ensino:** 3º do Ensino Médio.
3. **Objetos de Conhecimento:**
   - Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações.
4. **Habilidades BNCC:**
   - **(EF07MA04)** - Resolver e elaborar problemas que envolvam operações com números inteiros;
   - **(EF07MA03)** - Comparar e ordenar números inteiros em diferentes contextos, incluindo o histórico, associá-los a pontos da reta numérica e utilizá-los em situações que envolvam adição e subtração;
   - **(EM13MAT406)** - Utilizar os conceitos básicos de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática.
5. **Objetivos/Expectativas de Aprendizagem:**

- Abordamos neste encontro, as sementes da Congruência, o alicerce da aritmética dos restos, conteúdo este que é desconhecido por muitos, em particular pelos discentes do Ensino Fundamental e Ensino Médio;
- Destacamos que estes conceitos são imprescindíveis na Aritmética e mostraremos algumas aplicações na Matemática do cotidiano;
  item Apresentar problemas que envolvam as congruências modulares, por exemplo, como podemos trabalhar os diferentes calendários.

6. **Estratégia de Ensino e materiais utilizados:**
   - Aulas expositivas;
   - Atividades sobre calendários , relógios e tábuas Aritméticas;
   - Quadro, pincel, apagador, livro didático e retroprojetor.
7. **Duração da atividade:** 3 horas (aos sábados das 9 h às 12 h).

Neste encontro 04, inciamos a aula com o instigante algoritmo do ano bissexto, que verifica se um ano é bissexto ou não, percebemos um interesse muito motivador entre os alunos, na hora de aplicar os conhecimentos matemáticos na linguagem de programação. O código fonte e o executável encontre-se a seguir:

Figura 20 – Código fonte: Algoritmo do ano bissexto



Fonte: Elaborado pelo Autor (2024)

Figura 21 – Execução do código fonte: Algoritmo do ano bissexto

Fonte: Elaborado pelo Autor (2024)

Sequência Didática I – Encontro 04

Uma das ideias mais importantes e fortes na Teoria dos Números é a de congruência que foi introduzida por Karl Friedrich Gauss (1777 – 1855) (HYGINO, 1991).

Neste encontro trabalharemos a aritmética dos fenômenos periódicos e a ideia de congruência, recurso importante para resolução de problemas envolvendo estes eventos, ou seja, aquelas situações em que há uma repetição regular de intervalos.

Estes fenômenos acontecem, diariamente, quando precisamos tomar um medicamento no horário regular, quando olhamos o relógio e percebemos que os dias são obtidos através dos segundos, minutos e horas. Que as semanas são formadas por 7 dias, os meses por 28, 29, 30 ou 31 dias, e os anos são formados por 365 dias e 6 horas aproximadamente ou 366 dias quando são bissextos.

Movimentos periódicos ocorrem em diversas situações do nosso cotidiano, por exemplo, o movimento que a Terra leva para dar uma volta em torno de si, representa 24h (movimento de rotação), já o movimento que a terra dá em torno do sol corresponde a 365 dias e 6 horas aproximadamente (movimento de translação) (COUTINHO, 2015).

Um outro exemplo que podemos introduzir é referente ao calendário escolar, suponhamos que um pai pergunte ao filho: filho dia 23 vai ter aula de Física? O filho verifica que hoje é dia 11 (segunda-feira), utilizando a tabela abaixo:

Figura 22 – Dias da semana

Restos	0	1	2	3	4	5	6
Dia	Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo

Fonte: (COUTINHO, 2015)

Sabe-se que hoje é dia 11 e que o dia que se deseja saber é dia 23, portanto, a diferença do dia que se quer e hoje é dado por $23 - 11 = 12$, podemos rescrever o 12 da seguinte forma: $12 = 7 + 5$, onde este 5 seria o resto da divisão de 12 por 7. Portanto, o dia 23 vai cair em um sábado, conforme a Figura 21. Logo, sábado não tem aula.

Exercício 01: O ano de 2019 começou em um terça-feira, em que dia da semana caíra o último dia do ano de 2019 ?

Exercício 02: O ano de 2023 começou em um domingo, em que dia da semana caíra o 1^o dia de 2026?

É importante salientar que nos calendários existem anos que são bissextos. Há alguns critérios que precisamos identificar para que seja classificado um ano bissexto.

Se o ano for um múltiplo de 4, o ano é bissexto, mas se o ano for múltiplo de 4 e múltiplo de 100 simultaneamente o ano não será bissexto e por fim se o ano for múltiplo de 4, múltiplo de 100 e múltiplo de 400 teremos um ano bissexto, é relevante saber destas informações para que haja uma classificação do ano de forma adequada. Fonte: <https://www.youtube.com/watch?v=Gj5uopyMoKc>.

Exercício 03: Quantos calendários anuais diferentes existem?

Em algum momento nos deparamos com a seguinte situação: "$7 + 8 = 3$". Para que esta situação tenha sentido é necessário contextualizarmos. Um relógio seria um exemplo significativo, pois 15 horas representa 3 horas da tarde. Como isso temos a ideia da aritmética dos restos. Que podemos representar da seguinte forma:

$7 + 8 \equiv 3 \pmod{12}$ (lê-se: sete mais oito é congruente a três módulo doze).

A seguir iremos explicar de forma mais detalhada essa operação. Antes disso, definiremos formalmente a ideia de congruência módulo m. A definição apresentada a seguir consta em (HEFEZ; ARITMÉTICA, 2009).

Seja m um número natural. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se: $a \equiv b \pmod{m}$

Quando a relação $a \equiv b \pmod{m}$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, nesse caso:

Exercício 04: Vamos verificar se são verdadeiras (V) ou falsas (F) as seguintes congruências:

a) $11 + 2 \equiv 1 \pmod{12}$ ( )

b) $10 + 10 \equiv 8 \pmod{12}$( )

c) $20 \equiv 0 \pmod{4}$ ( )

d) $21 \equiv 9 \pmod{12}$ ( )

e) $8 \equiv 2 \pmod{3}$( )

A ideia primária da aritmética modular é bem simples. Fixado um inteiro m, todos os demais números inteiros a são substituídos pelo resto de sua divisão euclidiana por m. Desse modo, o conjunto $\mathbb{Z}$ dos números inteiros se transforma no conjunto $\mathbb{Z}_m = \{0,\ 1,\ 2,\ \ldots,\ m-1\}$, denominado conjunto dos inteiros módulo m (cujos elementos são os restos possíveis da divisão de um inteiro qualquer por m). Fonte: <https://sca.profmatsbm.org.br/profmat_tcc.php?id1=6047&id2=171053443>.

No conjunto $\mathbb{Z}$ apresentado anteriormente definiremos duas operações: adição e multiplicação, as quais serão detalhadas a seguir. A soma será denotada pelo símbolo $\oplus$ e o produto será denotado pelo símbolo $\odot$.

$$a \oplus b = \text{resto da divisão de } a + b \text{ por } m.$$
$$a \odot b = \text{resto da divisão de } a \cdot b \text{ por } m.$$

Exemplo 01: Observe que em $\mathbb{Z}_4$ temos as seguintes operaçãos.

$2 \oplus 3 =$ resto da divisão de $2 + 3$ por $4 =$ resto da divisão de 5 por $4 = 1$.

$2 \odot 3 =$ resto da divisão de $2 \cdot 3$ por $4 =$ resto da divisão de 6 por $4 = 2$.

As tabelas apresentadas a seguir representam as tábuas das operações de adição e multiplicação em $\mathbb{Z}_4$.

Tabela 05 -Tábua de operação $\oplus$ em $\mathbb{Z}_4$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Fonte: Elaborado pelo autor (2024)

Tabela 06 -Tábua de operação $\odot$ em $\mathbb{Z}_4$

$\odot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Fonte: Elaborado pelo autor (2024)

Exercício 05: Construa as tábuas das operações de adição e multiplicação em $\mathbb{Z}_7$.

5.1.5 5º ENCONTRO

1. **Unidade Temática:** Números e Álgebra.
2. **Modalidade/Nível de Ensino:** 3º do Ensino Médio.
3. **Objetos de Conhecimento:** BNCC(BRASIL, 2018) e PCEMPB(PARAÍBA, 2021).
   - Matrizes;
   - Determinantes.
4. **Habilidades BNCC e PCEMPB:**
   - **(EM13MAT405)** Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática;
   - **(EM13MAT410)** - Associar o conceito de matrizes, determinantes e sistemas de equações lineares às situações nas quais são utilizadas planilhas eletrônicas;
   - **(EM13MAT411)** - Reconhecer um sistema de equações associado a uma matriz com o intuito de resolver situações problemas.

   Vale salientar que as habilidades **(EM13MAT405)**, **(EM13MAT410)** e **(EM13MAT411)** foram retiradas da BNCC, porém elas continuam fazendo parte da PCEMPB, portanto achamos conveniente trabalhar com os alunos, tais habilidade que é de suma importância no desenvolvimento do ensino/aprendizagem das Cifras de Hill.
5. **Objetivos/Expectativas de Aprendizagem:**
   - Trabalha a ideia de matrizes, tipos de matrizes, operações envolvendo matrizes e matrizes inversas;
   - Conceituar determinantes; e aprender a calcular determinantes de ordem 2, 3 e como calcular seu valor numérico.
6. **Estratégia de Ensino e materiais utilizados:**
   - Retroprojetor,computador, lousa, lápis, aulas expositivas e dialogadas.
7. **Duração da atividade:** 3 horas (Aos sábados das 9 h às 12 h).

Sequência Didática I - Encontro 05

Neste encontro, faremos uma abordagem relembrando alguns conceitos fundamentais de matrizes, suas operações e determinantes, pois esses conteúdos serão importantes para o Encontro 06, no qual trabalharemos a Criptografia e as Cifras de Hill.

Uma matriz nada mais é do que uma tabela disposta em linhas e colunas, e é bastante usada para organizar dados em empresas, jornais, calendários e planilhas. Historicamente, o surgimento de tabelas para resolver situações-problema tem indícios na China por volta de 2500 a.C., apresentados em um dos capítulos do livro chinês "Chui-Chang Suan-Shu". Mas quem introduziu a ideia de configurar dados em tabelas foi o matemático francês Augustin-Louis Cauchy (1789-1857), como é mostrado no livro (DANTE, 2013).

Vamos definir as matrizes conforme (IEZZI; HAZZAN, 2004). Dados dois números m e n naturais não-nulos, chama-se matriz m por n (indica-se m x n) toda tabela M formada por números reais distribuídos em m linhas e n colunas.

Em uma matriz M qualquer, cada elemento é indicado por a_{ij}. O índice i indica a linha e o índice j indica a coluna. Por convenção $i = 1,\cdots, m$ e $j = 1,\cdots, n$.

Exemplo 01:

$$M = (a_{ij})_{m\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

Após relembrarmos a definição de matriz, vamos abordar a operação de multiplicação de matrizes, que será de extrema importância para o próximo encontro. Uma condição para que o produto $A \cdot B$ seja definido é que o número de colunas de A seja igual ao número de linhas de B (IEZZI et al., 2001).

A matriz produto $C = A \cdot B$ é uma matriz cujo o número de linhas é igual ao número de linhas de A e o número de colunas é igual ao número de colunas de B. Observemos o esquema abaixo:

$$A_{m\times n} \cdot B_{n\times p} = C_{m\times p}$$

Podemos observar que a condição de existência do produto é válida, pois o número de colunas da matriz A é igual ao número de linhas da matriz B. Logo, este produto existe e o resultado do mesmo é uma matriz cujo número de linhas corresponde ao mesmo da matriz A e o número de colunas corresponde ao mesmo da matriz B.

Exemplo 02:

$$\begin{pmatrix} 1 & 4 & 0 \\ \text{-2} & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 0 & 2 \\ \text{-3} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 10 \\ \text{-11} & 7 \end{pmatrix}$$

Como a condição de existência para a multiplicação de matrizes é válida, ou seja, o número de colunas da primeira matriz é igual ao número de linhas da segunda matriz, logo o resultado desta multiplicação de matrizes será uma matriz de ordem 2.

Vejamos o processo: Sejam $C = A \cdot B$, onde A é representada pela primeira matriz, B a segunda matriz e C a matriz resultado do produto de A por B. A seguir ilustraremos como calcular os elementos da matriz produto C. Percebe-se que as letras minúsculas representam os elementos de cada matriz e suas respectivas posições; por exemplo, a_{11} seria o elemento da matriz A na primeira linha e primeira coluna. O elemento c_{11} da matriz C é obtido pela soma dos produtos dos elementos correspondentes da primeira linha da matriz A pelos elementos da primeira coluna de B.

$c_{11} = a_{11} \cdot b_{11} + a_{12} \cdot b_{21} + a_{13} \cdot b_{31} \Rightarrow c_{11} = 1 \cdot 1 + 4 \cdot 0 + 0 \cdot (-3) = 1.$

$c_{12} = a_{11} \cdot b_{12} + a_{12} \cdot b_{22} + a_{13} \cdot b_{32} \Rightarrow c_{12} = 1 \cdot 2 + 4 \cdot 2 + 0 \cdot 1 = 10.$

$c_{21} = a_{21} \cdot b_{11} + a_{22} \cdot b_{21} + a_{23} \cdot b_{31} \Rightarrow c_{21} = (-2) \cdot 1 + 4 \cdot 0 + 3 \cdot (-3) = -11.$

$c_{22} = a_{21} \cdot b_{12} + a_{22} \cdot b_{22} + a_{23} \cdot b_{32} \Rightarrow c_{22} = (-2) \cdot 2 + 4 \cdot 2 + 3 \cdot 1 = 7.$

Vale salientar que esses conceitos já foram abordados no 2^o ano do Ensino Médio, mas é importante relembrá-los para garantir uma aprendizagem significativa quando forem apresentados a Criptografia e as Cifras de Hill.

Exercício 01: Dadas as matrizes:

$$D_2 = (d_{ij})_{2\times 2} = \begin{pmatrix} 1 & -2 \\ 3 & 4 \end{pmatrix}$$

$$B = (b_{ij})_{2\times 2} = \begin{pmatrix} -1 & 2 \\ 1 & 3 \end{pmatrix}$$

Verifique se a propriedade comutativa é válida, ou seja, se $D_2 \cdot B = B \cdot D_2$.

Existem matrizes que são especiais e importantes para efetuar operações; uma delas é a matriz unidade (ou matriz identidade) de ordem n (indicada por I_n). Tal matriz é toda matriz diagonal em que os elementos da diagonal principal são iguais a 1, e o restante dos elementos que fazem parte da matriz são iguais a zero (IEZZI; HAZZAN, 2004).

$$I_2 = (i_{ij})_{2\times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$I_3 = (i_{ij})_{3\times 3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\vdots$$

$$I_{\mathrm{n}} = (i_{ij})_{n\times n} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Outro conceito importante na teoria de matrizes é o de matriz inversível. Por definição, uma matriz quadrada A de ordem n é inversível se existir uma matriz B tal que $A \cdot B = B \cdot A = I_n$ (I_n é a matriz identidade). Se A não é inversível, então dizemos que A é uma matriz singular (IEZZI; HAZZAN, 2004).

Exercício 02: Considere a matriz

$$A_1 = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

Determine a inversa de A_1.

Com relação à teoria dos determinantes, sua origem remonta por volta do século XVII, quando eram estudados os processos de resolução de sistemas lineares. Embora não seja um método muito prático, era possível resolver alguns sistemas através do Teorema de Cramer (IEZZI; HAZZAN, 2004)
.

Vamos relembrar agora a definição de determinantes para os casos $n = 1$, 2, 3. Consideremos o conjunto de matrizes quadradas de elementos reais. Seja M uma matriz de ordem n desse conjunto. Chamamos de determinante da matriz M (e indicamos por det M) o número obtido operando com os elementos de M da seguinte forma:

1º Caso: Se M é de ordem $n = 1$, então detM_1 é o único elemento de M_1.

$$M_1 = (a_{ij})_{1\times 1} = \begin{pmatrix} a_{11} \end{pmatrix}$$

Portanto, o determinante de M_1, Det $M_1 = a_{11}$.

2º Caso: Se M é de ordem $n = 2$, então o determinante de M_2 é o produto dos elementos da diagonal principal menos o produto dos elementos da diagonal secundária.

$$M_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Portanto, o determinante de M_2, pode ser calculado da seguinte forma:

Det $M_2 = a_{11} \cdot a_{22} - a_{21} \cdot a_{12}$.

3º Caso: Se M é de ordem $n = 3$, isto é :

$$M_3 = (a_{ij})_{3\times 3} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Definimos,

Det $M_3 = a_{11} \cdot a_{22} \cdot a_{33} + a_{12} \cdot a_{23} \cdot a_{31} + a_{13} \cdot a_{21} \cdot a_{32} - a_{13} \cdot a_{22} \cdot a_{31} - a_{11} \cdot a_{23} \cdot a_{32} - a_{12} \cdot a_{21} \cdot a_{33}$.

Podemos memorizar este cálculo da seguinte forma:

$$M_3 = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \end{vmatrix}$$

a) Repetimos ao lado da matriz as duas primeiras colunas;

b) Os termos precedidos pelo sinal + são obtidos multiplicando-se os elementos segundo na direção das diagonais principais, isto é, são os termos:

$a_{11} \cdot a_{22} \cdot a_{33}$, $a_{12} \cdot a_{23} \cdot a_{31}$ e $a_{13} \cdot a_{21} \cdot a_{32}$.

c) Os termos precedidos pelo sinal − são obtidos multiplicando-se os elementos segundo na direção das diagonais secundárias:

$-a_{13} \cdot a_{22} \cdot a_{31}$, $-a_{11} \cdot a_{23} \cdot a_{32}$ e $-a_{12} \cdot a_{21} \cdot a_{33}$.

Este método pode ser visto com mais detalhes no livro "Fundamentos de Matemática Elementar", volume 4 (IEZZI; HAZZAN, 2004).

Exercício 03: Calcule o determinante das seguintes matrizes.

$$a) P_1 = (p_{ij})_{1\times 1} = \begin{pmatrix} 2 \end{pmatrix}$$

$$b) P_2 = (p_{ij})_{2\times 2} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

$$c) P_3 = (p_{ij})_{3\times 3} = \begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 2 \\ 4 & 1 & 2 \end{pmatrix}$$

Observação: É possível verificar que uma matriz admite inversa somente quando ela for quadrada e o seu determinante for não nulo.

Método para o Cálculo do Inverso de uma Matriz de ordem 2.

A seguir, descrevemos um método para o cálculo da inversa de uma matriz A de ordem 2. Tal método encontra-se em (BOLDRINI et al., 1980). Em primeiro lugar, precisamos entender o que é uma matriz adjunta Observação: É possível verificar que uma matriz admite inversa somente quando ela for quadrada e o seu determinante for não nulo.

Método para o Cálculo do Inverso de uma Matriz de ordem 2.

A seguir, descrevemos um método para o cálculo da inversa de uma matriz A de ordem 2. Tal método encontra-se em (BOLDRINI et al., 1980). Em primeiro lugar, precisamos entender o que é uma matriz adjunta (PACCOLA, 1995).

A matriz adjunta de uma matriz quadrada M é a transposta da matriz dos cofatores de A. Indicamos a matriz adjunta de M por:

$$\text{Adj } M = (cofM)^t.$$

Vamos obter a matriz dos cofatores de M.

$$M_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

O elemento c_{ij} da matriz dos cofatores de M_2 é calculo por $(-1)^{i+j}$ vezes o determinante da matriz obtida após eliminarmos a linha i e a coluna j de M_2. Vamos determinar os elementos da matriz dos cofatores da matriz M_2 de ordem 2, conforme descrito acima.

$c_{11} = (-1)^{1+1} \cdot a_{22} = a_{22}$.
$c_{12} = (-1)^{1+2} \cdot a_{21} = -a_{21}$.
$c_{21} = (-1)^{2+1} \cdot a_{12} = -a_{12}$.
$c_{22} = (-1)^{2+2} \cdot a_{11} = a_{11}$.
Logo, a matriz dos cofatores de M_2, isto é, Cof M_2 é :

$$CofM_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{22} & -a_{21} \\ -a_{12} & a_{11} \end{pmatrix}$$

Portanto, de acordo com a definição da matriz Adj $M_2 = (CofM_2)^t$:

$$AdjM_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Por fim, podemos calcular a matriz inversa como sendo a fórmula:

$$A^{-1} = \frac{1}{DetM_2} \cdot (AdjM_2) = \frac{1}{DetM_2} \cdot \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Iremos considerar esta fórmula como verdadeira sem demonstração.

Exercício 04: Calcule, se existir, a inversa da matriz R_2.

$$R_2 = (r_{ij})_{2\times 2} = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

5.1.6 6º ENCONTRO

1. **Unidade Temática BNCC(BRASIL, 2022):** Mundo Digital.
2. **Modalidade/Nível de Ensino:** 3º do Ensino Médio.
3. **Objetos de Conhecimento BNCC:**
   - Segurança e cibernética.
4. **Habilidades BNCC:**
   - **(EF09CO05)** - Analisar técnicas de criptografia para armazenamento e transmissão de dados.
5. **Objetivos/Expectativas de Aprendizagem:**
   - Efetuar cálculos de operações envolvendo matrizes e as Cifras de Hill;
   - Utilização de matrizes e matrizes inversas para codificar e decodificar mensagens.
6. **Estratégia de Ensino e materiais utilizados:**
   - Aulas expositivas e dialogadas.
7. **Duração da atividade:** 3 horas (Aos sábados das 9 h às 12 h).

Sequência Didática I - Encontro 06

Nesta sequência didática vamos abordar um assunto de extrema relevância para o mundo moderno, a Criptografia, a qual pode ser implementada em diversos contextos tanto no Ensino Fundamental quanto no Ensino Médio. Nossa abordagem será voltada para o Ensino Médio e requer conhecimentos de Aritmética, bem como ideias envolvendo matrizes e determinantes, que foram apresentados em encontros anteriores.

Em grego, cryptos significa secreto, oculto. A Criptografia estuda os métodos para codificar uma mensagem de modo que seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos", que todos já praticamos quando criança. O mais simples desses códigos consiste em substituir uma letra para a seguinte, isto é, transladar o alfabeto uma casa para diante. Um código semelhante foi usado por César para comunicar-se com legiões em combate pela Europa. Este parece ter sido o primeiro exemplo de um código secreto de que se tem notícia (COUTINHO, 2015).

Nota-se que para um sistema criptográfico funcionar é preciso cumprir duas condições,o primeiro que ele seja reversível,ou seja ,que a mensagem possa ser codificada e decodificada com precisão e o segundo, o receptor tenha uma chave para realizar esta codificação e decodificação com eficiência. Fonte: <https://www.youtube.com/watch?v=pgEV9XjOQ6I&t=134s>.

Atualmente, a Criptografia é uma ferramenta muito importante para sociedade moderna, utilizamos em trocas de e-mails, transações bancárias, compra e venda de produtos na internet, permitindo que estas informações sejam transmitidas de acordo com os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade (KIM; SOLOMON, 2014).

Antes de apresentar o método de Criptografia que será estudado, faremos uma retomada ao conjunto $\mathbb{Z}_m$, por ser importante para identificar o inverso multiplicativo de um conjunto. Vamos utilizar um exemplo prático para discutir essa ideia. Considere a seguir a tábua de multiplicação em $\mathbb{Z}_5$.

Tabela 07 -Tábua de operação $\odot$ em $\mathbb{Z}_5$

$\odot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Fonte: Elaborado pelo autor (2024)

Percebe-se que 1 funciona como elemento neutro da multiplicação em $\mathbb{Z}_5$. Observe, que:
$2 \odot 3 =$ resto da divisão de $2 \cdot 3$ por $5 =$ resto da divisão de 6 por $5 = 1$.
Por isso, dizemos que 2 é o inverso multiplicativo de 3 módulo 5.
Exemplo 01: Qual o inverso multiplicativo em $\mathbb{Z}_5$.

a) 1;

b) 2;

c) 2;

d) 3;

E) 0 tem inverso multiplicativo?

Uma das ferramentas importantes que temos para associar os estudos de matrizes e determinantes com a Criptografia são as Cifras de Hill que é um sistema poligráfico, ou seja, cada letra é representada por um número módulo 26. Inventado por Lester S.Hill, matemático americano em 1929 (ROSSETO, 2018).

As ideias contidas aqui constam em (ROSSETO, 2018). A princípio utilizaremos o alfabeto com as 26 letras, onde cada letra estará associada a um valor numérico: por exemplo A está associado a 1, B está associado a 2 e assim sucessivamente, até chegarmos ao Z que será associado a 0 (pois, Z corresponde a última letra do nosso alfabeto (posição 26) e quando dividimos o número 26 por 26 obtemos o resto 0). A princípio vamos atribuir um número a cada letra como podemos observar abaixo:

Figura 23 – Blocos de substituição de letras por números e vice-versa

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

Fonte: (ROSSETO, 2018)

Em seguida, dividiremos em blocos a palavra ou frase a ser decifrada. Cada bloco é formado por duas letras, logo estas letras serão associadas a dois números formando um vetor, com 2 linhas e 1 coluna. Pois este vetor é que vai garantir a condição de multiplicação de matrizes. Criamos uma matriz de ordem 2 para facilitar os cálculos, desde que esta matriz seja inversível, pois para codificar

precisamos da matriz criada e para decodificar precisamos da matriz inversa. Lembrando que para termos uma matriz inversa é necessário que o determinante seja diferente de zero. Para entendermos melhor vejamos a seguinte situação.

Para criptografar uma mensagem, cada bloco de duas letras, considerando como vetor de dois componentes, é multiplicado por uma matriz de ordem 2 invertível módulo 26. Para descriptografar a mensagem, cada bloco é multiplicado pela inversa da matriz usada no processo de codificação.

A matriz utilizada para criptografia é a chave de cifra, e deve ser escolhida aleatoriamente do conjunto de matrizes de ordem 2 invertíveis módulo 26. A cifra pode, é claro, ser adaptada a um alfabeto com qualquer número de letras; toda aritmética só precisa ser feita módulo o número de letras em vez de módulo 26 (ROSSETO, 2018).

Sejam A uma matriz de ordem 2, A^{-1} a matriz inversa de ordem 2 de A, V a matriz que representa vetor coluna a ser codificado, M_c a matriz de codificação e M_d a matriz de decodificação. Então:

Processo de codificação

$$\boxed{A_{2\times2} \cdot V_{2\times1} = M_c(_{2\times1})}$$

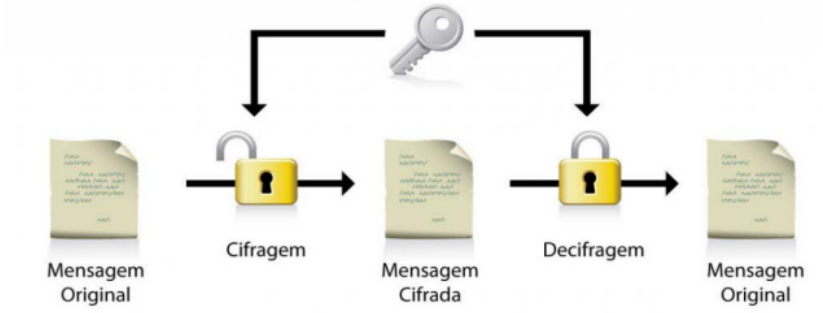
Fonte: Elaborado pelo autor (2024)

Processo de decodificação

$$\boxed{A^{-1}_{2\times2} \cdot (A_{2\times2} \cdot V_{2\times1}) = A^{-1}_{2\times2} \cdot M_c(_{2\times1}) = M_d(_{2\times1})}$$

Fonte: Elaborado pelo autor (2024)

Figura 24 – Esquema de ciframento e deciframento



Fonte:<https://www.cin.ufpe.br/~flash/ais98/cripto/criptografia.htm>

Codificaremos a seguir a palavra GALO.

A princípio colocaremos a palavra GALO em blocos, ou seja, separemos em sílabas e em seguida colocaremos seus respectivos valores.

Figura 25 – Bloco de vetores

G	A	L	O
7	1	12	15

Fonte: Elaborado pelo autor (2024)

Logo, em seguida escolhemos uma matriz quadrada de ordem 2 e inversível para facilitar os cálculos. Para que ela seja inversível, uma condição necessária é que ela seja não-singular, ou seja, o determinante da mesma tem de ser diferente zero.

$$A_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$$

Observe que o determinante da matriz A é que é inversível módulo 26.

Vamos converter cada bloco em um vetor-coluna, pois assim podemos multiplicar a matriz pelo vetor de modo que a condição de existência de multiplicação de matrizes seja válida, condição esta que trabalhamos no **Encontro 5**. Vamos cifrar o par G A da seguinte maneira, segundo o Processo de Codificação apresentado anteriormente:

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 31 \\ 8 \end{pmatrix}$$

Sempre que ocorrer um número inteiro maior que 25, ele será substituído pelo resto da divisão deste inteiro por 26. Faremos sempre isso, pois estamos trabalhando com a aritmética dos inteiros módulo 26, uma vez que estamos considerando o alfabeto constituído de 26 letras. No cálculo anterior substituiremos 31 por 5, pois o resto da divisão de 31 por 26 é 5.

Assim,

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 1 \end{pmatrix} = \begin{pmatrix} 31 \\ 8 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \end{pmatrix} \pmod{26}$$

Portanto, o bloco G A cifrado será E H, pois o 5 está associado a letra E e o 8 está associado a letra H.

Por fim, vamos cifrar o último bloco, o par L O da seguinte maneira:

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 93 \\ 27 \end{pmatrix}$$

Como 93 e o 27 são maiores que 25, vamos substituir 93 pelo resto da divisão deste inteiro por 26, no caso 93 dividido por 26 deixa resto 15. E substituir o 27 pelo resto da divisão deste número inteiro por 26, logo 27 dividido por 26 deixa resto 1.

Assim,

$$\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 15 \end{pmatrix} = \begin{pmatrix} 93 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 15 \\ 1 \end{pmatrix} \pmod{26}$$

Logo, o bloco L O cifrado será O A. Percebe-se que a mensagem codificada será EHOA. Para decodificar esta mensagem, precisaremos encontrar a matriz inversa de A e multiplicar pelos vetores que formam o bloco codificado. Relembrando o **Encontro 5** que a inversa da matriz A pode ser calculada da seguinte forma:

$$A^{-1} = \frac{1}{DetM_2} \cdot (AdjM_2) = \frac{1}{DetM_2} \cdot \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

$$A_2 = (a_{ij})_{2\times 2} = \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}$$

$$\text{Det } A_2 = a_{11} \cdot a_{22} - a_{21} \cdot a_{12} = 4 \cdot 1 - 1 \cdot 3 = 1.$$

$$A_2{}^{-1} = \tfrac{1}{1} \cdot \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$$

Figura 26 – Bloco de vetores da mensagem codificada

E	H	O	A
5	8	15	1

Fonte: Elaborado pelo autor (2024)

Vamos converter cada bloco em vetor coluna, pois assim podemos multiplicar a matriz inversa pelo vetor de modo que a condição de existência de multiplicação de matrizes seja válida.

Vamos decodificar o par E H efetuando os seguintes cálculos, segundo o Processo de Decodificação apresentado anteriormente:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 8 \end{pmatrix} = \begin{pmatrix} -19 \\ 27 \end{pmatrix}$$

Sempre que ocorrer um número inteiro negativo, vamos realizar a seguinte operação $26 - 9 = 7$, portanto o resto da divisão de -19 por 26 será 7. No caso de 27 dividimos o mesmo por 26, teremos o resto 1. Como mostra o cálculo abaixo:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 8 \end{pmatrix} = \begin{pmatrix} -19 \\ 27 \end{pmatrix} \equiv \begin{pmatrix} 7 \\ 1 \end{pmatrix} \pmod{26}$$

Portanto, o bloco E H decodificado será G A.

Vamos decodificar o par O A da seguinte maneira:

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ -11 \end{pmatrix}$$

Percebe-se que novamente o número negativo apareceu, logo basta subtrairmos 26 de 11: obtendo 15 como resultado. Logo, teremos a seguinte conclusão.

$$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 15 \\ 1 \end{pmatrix} = \begin{pmatrix} 12 \\ -11 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 15 \end{pmatrix} \pmod{26}$$

Por fim, o bloco O A decodificado será L O. Portanto, quando juntamos a decodificação dos dois blocos obtemos a palavra G A L O.

Vale salientar que $\frac{1}{DetA}$ é o inverso multiplicativo de Det A $\pmod{26}$. A tabela seguir mostra o inverso multiplicativo para alguns valores de a $\pmod{26}$:

Figura 27 – Elementos inversos multiplicativo $\pmod{26}$

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

Fonte: (ROSSETO, 2018)

EXERCÍCIO 02: Dada a matriz utilizada para codificar e decodificar a palavra galo, encontre a codificação e decodificação da palavra EU.

EXERCÍCIO 03: Dada a matriz utilizada para codificar e decodificar a palavra galo, encontre a codificação e decodificação da palavra SAPO.

5.1.7 7º ENCONTRO

1. **Unidade Temática BNCC:** Números.
2. **Modalidade/Nível de Ensino:** 3º do Ensino Médio.
3. **Objetos de Conhecimento BNCC:**
   - Todos os objetos já estudados anteriormente.
4. **Habilidades da BNCC:** Retomar todas habilidades que foram trabalhadas nos encontros anteriores, fazendo o uso do jogo intitulado a "Trilha da Aritmética".
5. **Objetivos/Expectativas de Aprendizagem:**
   - Utilizar por meio do jogo, as definições, propriedades e conceitos trabalhados nos encontros anteriores;
   - Trazer uma nova maneira lúdica de trabalhar conceitos que muitas das vezes não se tem costume de serem abordados na educação básica.
6. **Estratégia de Ensino e materiais utilizados:**
   - Aulas expositivas e dialogadas;
   - Jogos;
   - Tabuleiro.
7. **Duração da atividade:** 3 horas (Aos sábados das 9 às 12 horas).

Sequência Didática I – Encontro 07

Nesta sequência didática, faremos uma reapresentação dos tópicos que foram abordados nos encontros anteriores, desde definições, propriedades e resultados importantes, através de um jogo lúdico, que será denominado de **"Trilha da Aritmética"**.

Vamos criar um tabuleiro com o propósito de tornar a Matemática mais atrativa e significativa para o aluno. Nossa intenção é mostrar de maneira clara e direta que por meio dos jogos podemos desenvolver um pensamento criativo e crítico (GRANDO, 2004).

É muito comum associarmos a ideia de jogo com o material concreto, que muitas vezes utilizamos em sala de aula, mas na verdade o jogo é mais do que isso, pode proporcionar uma interação social, um desenvolvimento maior cognitivo e estratégias lúdicas essenciais para processo de ensino/aprendizagem dos alunos.

Mas, é extremamente relevante o professor analisar as vantagens e desvantagens de um determinado jogo, de modo que as vantagens se sobressaiam mais que as desvantagens, o mediador deve organizar o trabalho pedagógico de forma que ele consiga transmitir os conceitos e definições de modo que alunos se sintam motivados e tenham o prazer de aprender (GRANDO, 2004).

Para elaborar a estratégia do jogo vamos definir quatro etapas, segundo (GRANDO, 2004):

- Familiarização com o jogo;
- Exploração inicial com objetivo de relembrar conceitos e definições já trabalhadas em aulas anteriores;
- Aplicação de uma estratégia vencedora, ou seja, trabalhar em equipe com o pensamento coletivo;

- Validar as concepções trabalhadas nos encontros anteriores.

Para isto, construímos uma trilha no tabuleiro enumerada de 1 até 30, onde o primeiro aluno ou equipe que alcançar a chegada da trilha será o vencedor. Cada aluno ou equipe participante da "Trilha da Aritmética" será representado por um peão. Será definido a ordem da largada do jogo que poderá ser através de um sorteio por meio dos dados ou de um acordo prévio entre os participantes. O primeiro jogador lançará o dado e o peão será movido no tabuleiro de acordo com o número sorteado.

Por exemplo, se o número sorteado no dado for o 4, o peão que corresponde o aluno ou equipe deverá ser movido no tabuleiro 4 casas. Quando ele chegar nessa casa haverá uma pergunta, caso o jogador acerte ele permanecerá na casa e caso ele erre ele voltará para a casa de onde ele partiu. O tabuleiro será composto também de **"casas surpresas"**: as quais podem apresentar um bônus ou um ônus. Na nossa Trilha essas casas serão identificadas com os números **2, 5, 8, 12, 16, 18, 24 e 29**. A casa de número 2 terá o seguinte bônus: "avance duas casas".

Já a casa 5 terá o seguinte ônus: **"volte ao início"**. Com relação a casa 8 teremos o seguinte ônus: "Volte uma casa". Já a casa 12 terá o seguinte bônus: "avance duas casas". Com relação a casa 16 teremos o seguinte ônus: **"Volte duas casas"**. Já a casa 18 terá o seguinte ônus **"Volte ao início"**.

Já na casa 24 teremos o seguinte bônus: **"Avance duas casas"** e Por fim, a última casa surpresa, a 29 terá o seguinte ônus: **"recue três casas"**. É importante destacar que o jogo aqui sugerido pode ser adaptado e modificado a depender da intenção de cada professor e de cada turma que irá participar da atividade. Destacamos ainda que esse jogo ele poderá ser adaptado para trabalhar diferentes conteúdos da Matemática. Acreditamos que essa experiência de atividade se bem planejada e organizada pode representar uma importante metodologia de ensino-aprendizagem para o ensino da Matemática.

6 ANÁLISE E RESULTADOS

Neste capítulo, apresentamos uma breve análise dos resultados obtidos na nossa pesquisa, mas especificamente, uma análise do teste de sondagem e do questionário de avaliação das sequências didáticas.

Ao longo dos meus dez anos como professor na Escola Estadual de Ensino Fundamental e Médio Major Veneziano Vital do Rêgo, em Campina Grande, observei uma notável falta de interesse por parte dos alunos ao abordar a resolução de problemas relacionados à Aritmética. Além disso, é evidente que essa dificuldade na Aritmética repercute em desafios adicionais em outros conteúdos para os alunos.

A pesquisa adota uma perspectiva qualitativa, conforme delineado por (PRODANOV; FREITAS, 2013). A principal fonte de investigação e pesquisa se desenvolveu no ambiente escolar, com foco especial na sala de aula de Matemática. Nesse contexto, desempenharei o papel de professor-pesquisador-mediador, orientando e facilitando o desenvolvimento da experiência deste trabalho junto aos alunos.

A pesquisa foi aplicada em uma turma do Ensino Médio com um grupo de 10 alunos da Escola Estadual de Ensino Fundamental e Médio Major Veneziano Vital do Rêgo, no bairro Acácio Figueiredo, localizada em Campina Grande-PB.

Inicialmente, nossa proposta consiste em realizar uma pesquisa abrangente, tanto dentro como fora da sala de aula, com o intuito de promover uma avaliação reflexiva por parte dos alunos e até mesmo do professor. Essa autoavaliação pretendeu identificar áreas passíveis de aprimoramento no conhecimento aritmético, com o objetivo de tornar o processo de ensino e aprendizado mais envolvente e significativo. Para alcançar esse propósito, elaboramos um questionário de sondagem.

O questionário de sondagem foi composto de 08 questões que tinha por objetivo avaliar o conhecimento sobre alguns tópicos da Aritmética, mas especificamente: a ideia de números primos, compostos, múltiplos, algoritmo da divisão, propriedades dos números inteiros, fatoração e Teorema Fundamental da Aritmética.

A princípio, vamos analisar as questões 1, 5, 6 e 7 referentes ao conhecimento aritmético.

1-**(Portal da OBMEP)** Número primo é aquele que possui exatamente quantos divisores naturais?

A) 1

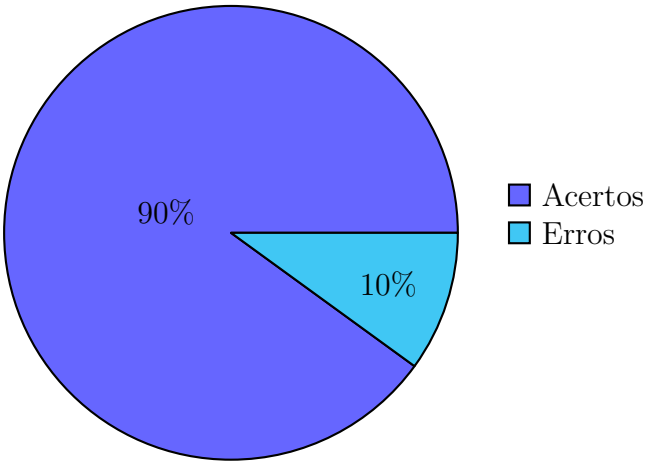
B) 2

C) 3

D) 4

E) nenhum

Figura 28 – Resultados da Questão 1 do teste de sondagem



Fonte: Elaborado pelo autor (2024)

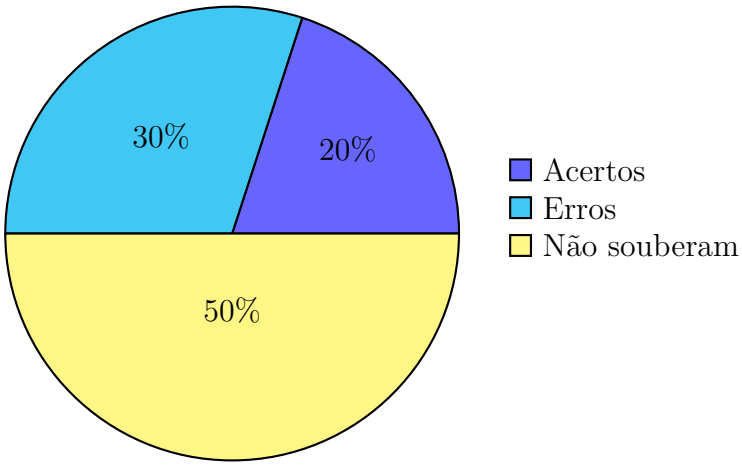
Percebemos que a definição de número primo, a maioria dos alunos acertaram. Esta definição é uma das mais importantes da Aritmética por conta de ter uma aplicação geral em diversas situações como a fatoração, Mínimo Múltiplo Comum, Máximo Divisor Comum e outros resultados. Apenas um aluno do grupo de 10 errou a questão.

Lembrando que na BNCC (BRASIL, 2018) esta habilidade corresponde ao código **(EF06MA05)** - Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por $2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ e assim por diante.

Em seguida, vamos analisar a questão 5 e o desempenho da turma ao tentar resolvê-la.

5**-(Portal da OBMEP)** Um número ao ser dividido por 3, deixa resto 1 e ao ser dividido por 4, deixa resto 1, que número é este?

Figura 29 – Resultados da Questão 5 do teste de sondagem



Fonte: Elaborado pelo autor (2024)

Observamos que em relação a esta questão subjetiva, os alunos tiveram dificuldade em responder, argumentar é uma atividade difícil e exige um certo grau de conhecimento com relação a questão.

Nosso objetivo neste trabalho também é auxiliar o desenvolvimento de habilidades de acordo com a BNCC (BRASIL, 2018), tal habilidade pode ser encontrada no código **(EF06MA06)** - Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor e **(EM13MAT315)** - Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

A seguir apresentaremos a questão 6 do teste de sondagem bem como o desempenho obtido pelos alunos.

6-**(OBM)** Um litro de álcool custa $R\$0,75$. O carro de Henrique percorre 25 km com 3 litros de álcool. Quantos reais serão gastos de álcool para percorrer 600 km?

A) 54

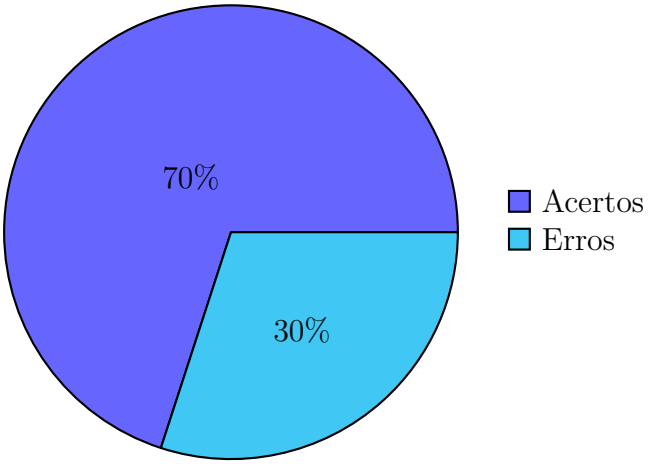
B) 72

C) 50

D) 52

E) 45

Figura 30 – Resultados da Questão 6 do teste de sondagem



Fonte: Elaborado pelo autor (2024)

Nesta questão 6, tivemos o seguinte resultado: 7 pessoas acertaram e 3 erraram. A escolha dessa questão para o teste teve por objetivo explorar a contextualização de conceitos aritméticos: os objetos de estudos que abordamos nela são multiplicação com números naturais e divisão euclidiana que são operações imprescindíveis para qualquer habilidade da BNCC (BRASIL, 2018). A habilidade esperada que os alunos desenvolvam é **(EM13MAT314)** - Resolver e elaborar problemas que envolvem grandezas determinadas pela razão ou pelo produto de outras (velocidade, densidade demográfica, energia elétrica etc.).

Para finalizar a análise do teste de sondagem apresentaremos a questão 07, bem como os resultados obtidos pelos alunos.

7-(OBM) Qual o menor número inteiro positivo pelo qual se deve multiplicar o número $7 \cdot 3^3 \cdot 2^4$ para obter um quadrado perfeito?

A) 7

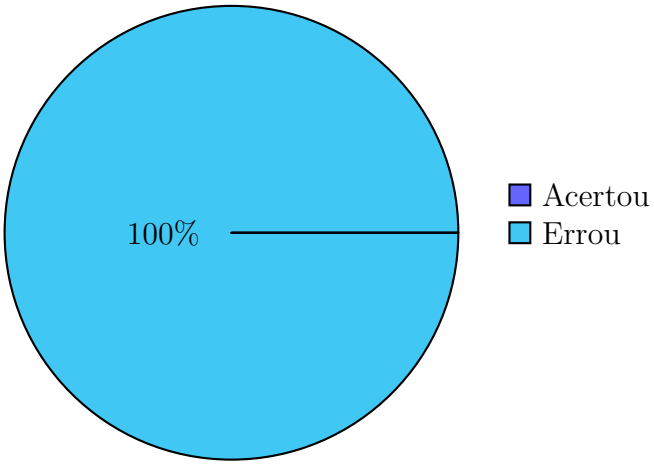
B) 84

C) 0

D) 1

E) 21

Figura 31 – Resultados da Questão 7 do teste de sondagem



Fonte: Elaborado pelo autor (2024)

A questão 7, percebe-se que houve bastante dificuldade de resolvê-la, por abordar muitos detalhes como quadrado perfeito, multiplicação e Teorema Fundamental da Aritmética (TFA).

Acreditamos que todos os alunos erraram, por desconhecer alguns requisitos fundamentais da Aritmética na questão. Estes requisitos estão associados a forma como tais conteúdos são explorados na Educação Básica. Estudar os conteúdos de forma insolada pode trazer diversos problemas, com relação a interpretação das questões, como este problema envolve diversos conhecimentos preliminares torno-se mais difícil para os alunos.

Escolhemos esta questão, bem como as outras, pelo motivo de trabalhar a seguinte habilidade da BNCC (BRASIL, 2018) **(EF07MA04)** - Resolver e elaborar problemas que envolvam operações com números inteiros.

A análise dos resultados obtidos com a aplicação desse teste mostra a relevância de fazer uma retomada desses conceitos, devido à grande notabilidade que a Aritmética possui na Matemática. É importante destacar que essa retomada pode ser adaptada de acordo com cada turma. Nesta turma especificamente, decidimos reapresentar tais conteúdos por meio de sequências didáticas.

Acreditamos que as sequências didáticas quando bem planejadas maximiza muita aprendizagem.

Logo após a aplicação das sequências didáticas, coletamos todas as informações obtidas antes e depois da experiência trabalhada na pesquisa. Ao término da aplicação da sequência proposta também aplicamos aos alunos um questionário que visa avaliar o grau de satisfação com relação a metodologia aplicada, serão 10 questões e as estatísticas da avaliação foram realizadas também com os 10 alunos. Vale ressaltar que durante aplicação deste questionário deixamos bem claro para eles serem o mais imparcial possível com relação as respostas.

Estas perguntas foram importantes para que este trabalho fosse melhorado servindo de reflexão sobre a sequência didática. Percebemos os entusiamos dos alunos en relação a metodologia, tivemos

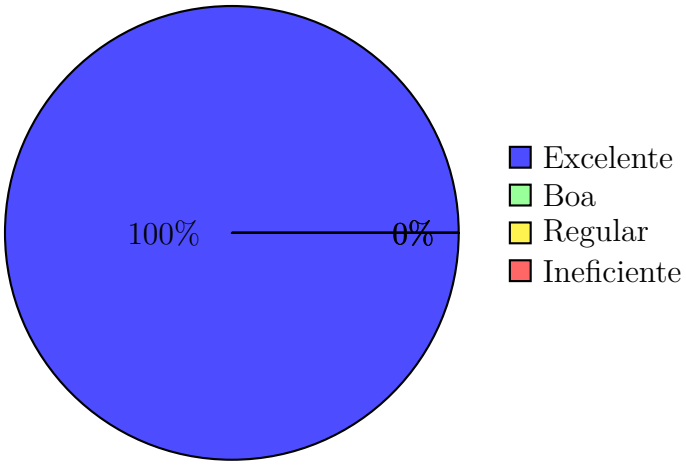
algumas dificuldades com relação ao espaço estrutural da escola (iluminação e calor), mas produzimos bem apesar de todas as dificuldades.

Vejamos agora algumas opiniões e observações sobre a metodologia das sequências didáticas, vamos analisar os resultados das questões implementadas 1, 3, 6, 7 e 10.

Questão 01- Como você avalia a proposta aplicada com relação ao ensino/aprendizagem da Aritmética nos encontros durante o curso:

- Excelente.
- Boa.
- Regular.
- Ineficiente.

Figura 32 – Resultados obtidos na Questão 01 sobre a metodologia da sequência didática



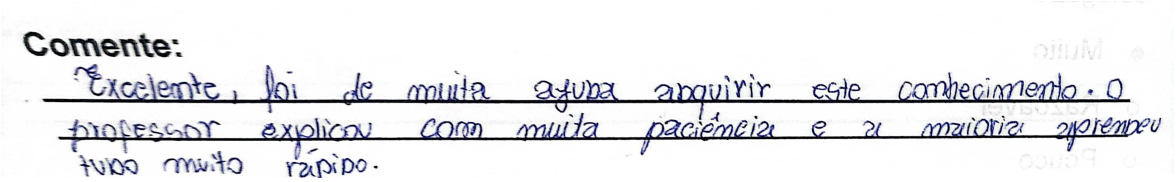
Fonte: Elaborado pelo autor (2024)

A questão 01, abordou a metodologia utilizada na elaboração da nossa sequência didática. Observamos que durante os nossos encontros, os objetivos, habilidades e competências foram trabalhas no sentido de tornar Aritmética mais acessível aos alunos.

De acordo com as respostas e comentários dos alunos tivemos resultados positivos. Tentamos proporcionar um material de qualidade para que o nosso objetivo fosse alcançado, que era de tornar a Aritmética mais significativa para nossos alunos.

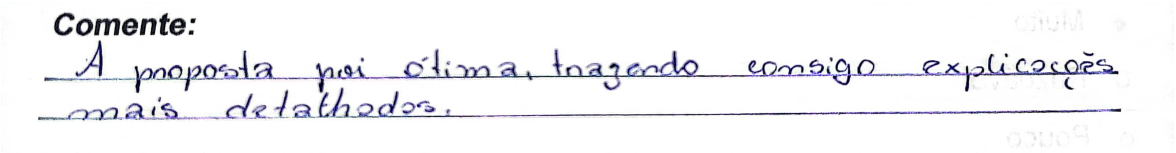
Lembrando que pedimos aos alunos que fossem o mais verdadeiro possível com relação as respostas. Vejamos alguns comentários sobre a metodologia das sequências didáticas, feitas pelos alunos.

Figura 33 – Comentário da Questão 01 sobre a metodologia da sequência didática: Aluno 01



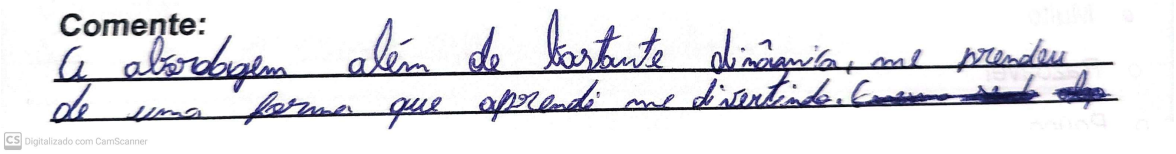
Fonte: Elaborado pelo Autor (2024)

Figura 34 – Comentário da Questão 01 sobre a metodologia da sequência didática: Aluno 02



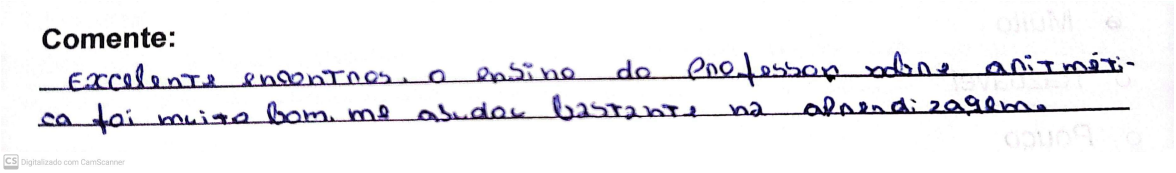
Fonte: Elaborado pelo Autor (2024)

Figura 35 – Comentário da Questão 01 sobre a metodologia da sequência didática: Aluno 03



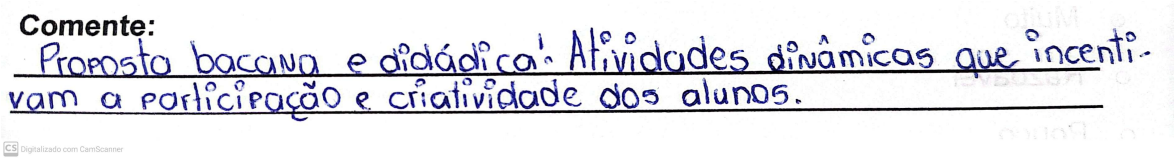
Fonte: Elaborado pelo Autor (2024)

Figura 36 – Comentário da Questão 01 sobre a metodologia da sequência didática: Aluno 04



Fonte: Elaborado pelo Autor (2024)

Figura 37 – Comentário da Questão 01 sobre a metodologia da sequência didática: Aluno 05

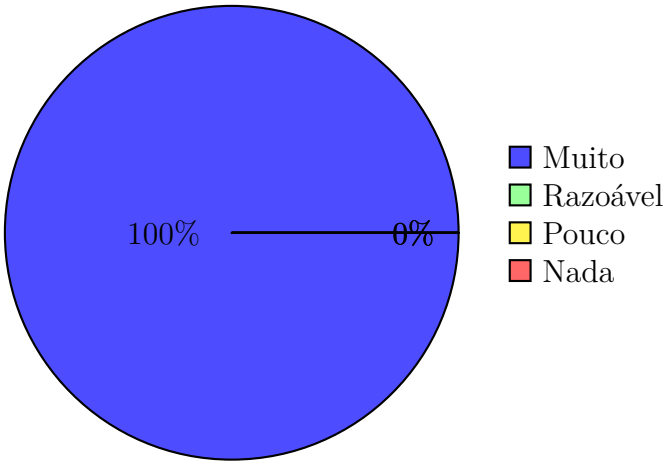


Fonte: Elaborado pelo Autor (2024)

Questão 03- Os recursos utilizados nos encontros (como retroprojetor, apostilas, lousa, lápis, linguagem de programação Python, etc.) contribuíram para uma aprendizagem significativa?

- Muito.
- Razoável.
- Pouco.
- Nada.

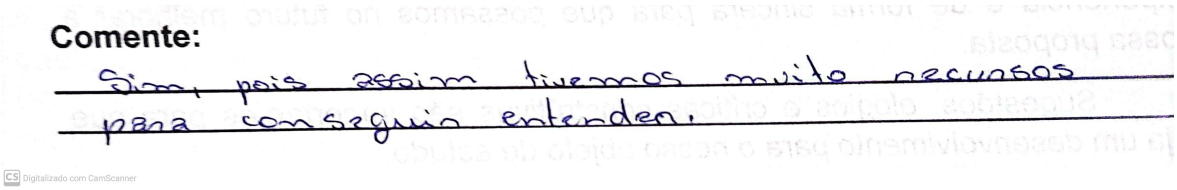
Figura 38 – Resultados obtidos na Questão 03 sobre a metodologia da sequência didática



Fonte: Elaborado pelo autor (2024)

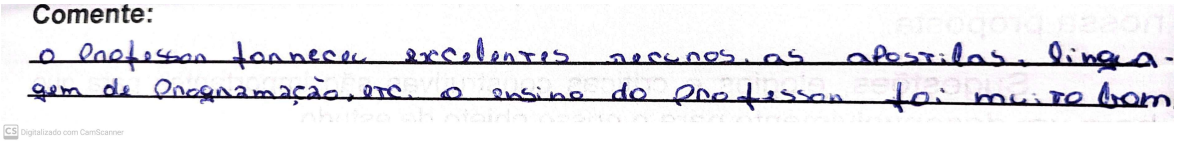
A questão 03, abordou os recursos didáticos utilizados nos encontros, percebemos que os alunos tiveram uma boa receptividade com relação ao material didático, trabalhamos com apostilas, retroprojetor com slides explicando de maneira resumida as apostilas, trabalhamos a resolução de situações-problema no quadro e também houve o uso da linguagem de programação Python que foi importante para aplicação de algoritmos. Vejamos alguns comentários, percebe-se que a maioria dos alunos gostaram dos recursos implementados nas aulas.

Figura 39 – Comentário da Questão 03 sobre a metodologia da sequência didática: Aluno 02



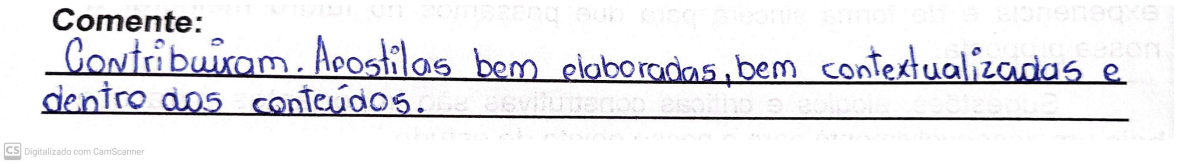
Fonte: Elaborado pelo autor (2024)

Figura 40 – Comentário da Questão 03 sobre a metodologia da sequência didática: Aluno 04



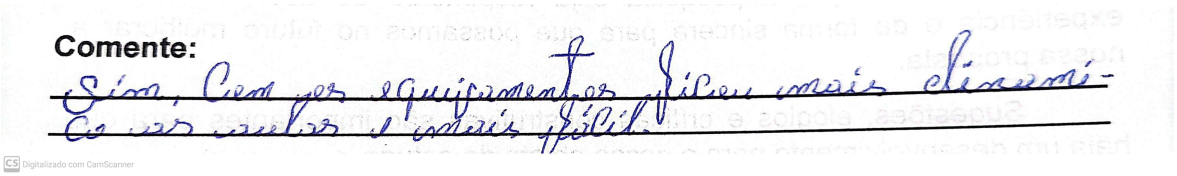
Fonte: Elaborado pelo Autor (2024)

Figura 41 – Comentário da Questão 03 sobre a metodologia da sequência didática: Aluno 05



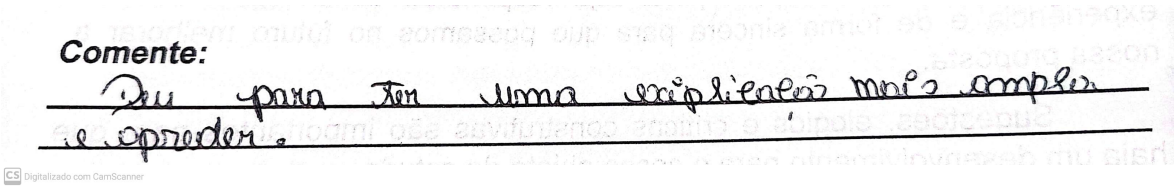
Fonte: Elaborado pelo Autor (2024)

Figura 42 – Comentário da Questão 03 sobre a metodologia da sequência didática: Aluno 06



Fonte: Elaborado pelo Autor (2024)

Figura 43 – Comentário da Questão 03 sobre a metodologia da sequência didática: Aluno 08

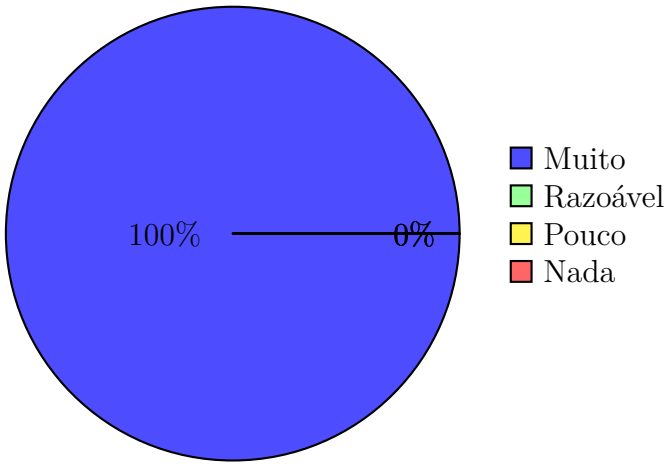


Fonte: Elaborado pelo Autor (2024)

Questão 06 - Você acredita que a metodologia aplicada durante os encontros contribuiu mais no processo de aprendizagem da Aritmética do que as aulas trabalhadas em anos anteriores sobre os mesmos conteúdos abordados nas sequências?

- Muito.
- Razoável.
- Pouco.
- Nada.

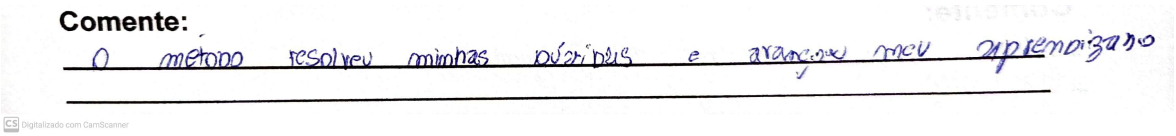
Figura 44 – Resultados obtidos na Questão 06 sobre a metodologia da sequência didática



Fonte: Elaborado pelo autor (2024)

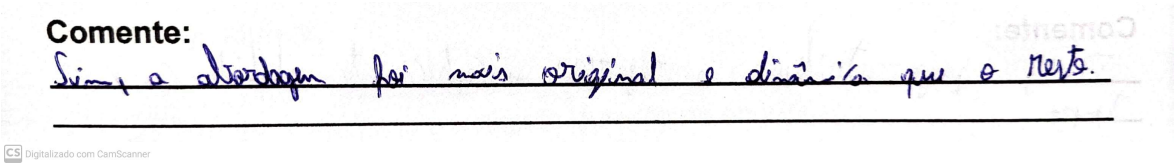
Nesta questão 06, fizemos uma pergunta voltada para as metodologias abordadas nos anos anteriores, se era mais produtiva que as metodologias implementadas nesta sequência didática, Obtemos uma reposta positiva com relação as sequências didáticas, os alunos se sentiram mais motivados na proposta dos encontros, percebemos este fato por meio da participação e compromisso dos alunos durante o encontro. A seguir mostramos alguns comentários dos alunos.

Figura 45 – Comentário da Questão 06 sobre a metodologia da sequência didática: Aluno 01



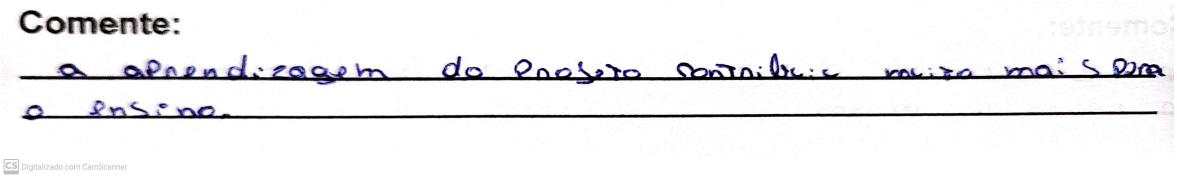
Fonte: Elaborado pelo Autor (2024)

Figura 46 – Comentário da Questão 06 sobre a metodologia da sequência didática: Aluno 03



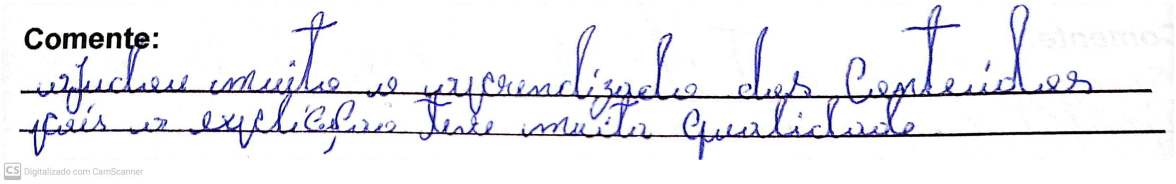
Fonte: Elaborado pelo Autor (2024)

Figura 47 – Comentário da Questão 06 sobre a metodologia da sequência didática: Aluno 04



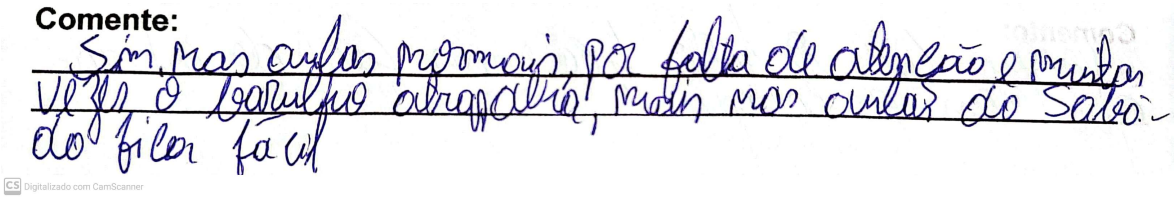
Fonte: Elaborado pelo Autor (2024)

Figura 48 – Comentário da Questão 06 sobre a metodologia da sequência didática: Aluno 06



Fonte: Elaborado pelo Autor (2024)

Figura 49 – Comentário da Questão 06 sobre a metodologia da sequência didática: Aluno 07

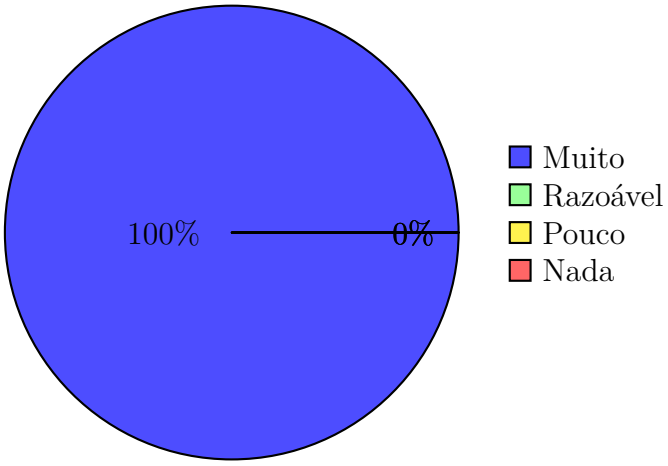


Fonte: Elaborado pelo Autor (2024)

Questão 07-O professor foi flexível e objetivo no momento em que sugiram dúvidas nos encontros?

- Muito.
- Razoável.
- Pouco.
- Nada.

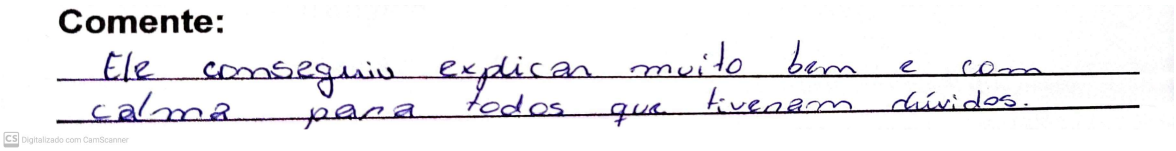
Figura 50 – Resultados obtidos na Questão 07 sobre a metodologia da sequência didática



Fonte: Elaborado pelo autor (2024)

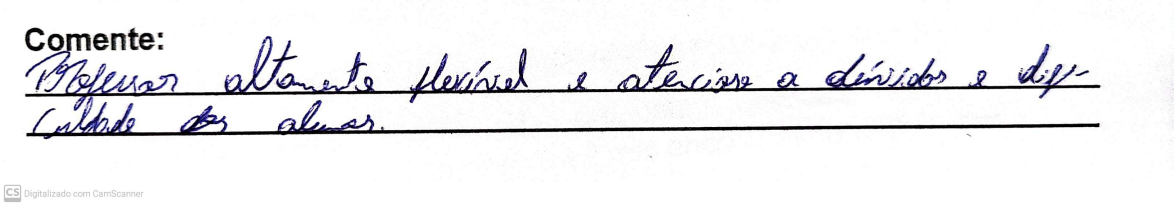
Na questão 07, solicitamos aos alunos que opinassem com relação a didática e a flexibilidade do professor em tirar dúvidas durante os encontros. Nota-se que a maioria gostou, pois não estava familiarizado com esta abordagem dos conteúdos, na maioria das vezes temos dificuldades de ensinar uma sala com 30 ou 40 alunos, já uma sala com 10 alunos podemos nos concentrar em tirar dúvidas e focar nas dificuldades para tentar resolvê-las. A seguir podemos observar alguns comentários.

Figura 51 – Comentário da Questão 07 sobre a metodologia da sequência didática: Aluno 02



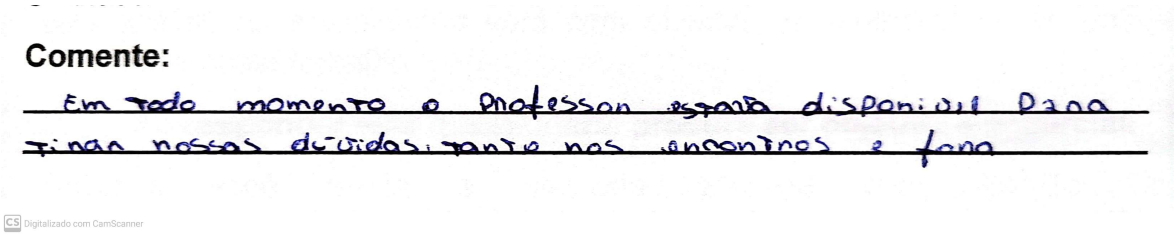
Fonte: Elaborado pelo Autor (2024)

Figura 52 – Comentário da Questão 07 sobre a metodologia da sequência didática: Aluno 03



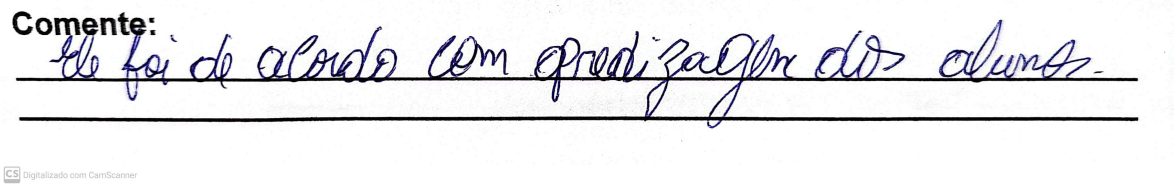
Fonte: Elaborado pelo Autor (2024)

Figura 53 – Comentário da Questão 07 sobre a metodologia da sequência didática: Aluno 04



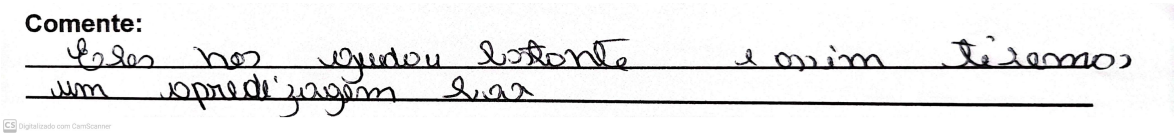
Fonte: Elaborado pelo Autor (2024)

Figura 54 – Comentário da Questão 07 sobre a metodologia da sequência didática: Aluno 07



Fonte: Elaborado pelo Autor (2024)

Figura 55 – Comentário da Questão 07 sobre a metodologia da sequência didática: Aluno 08

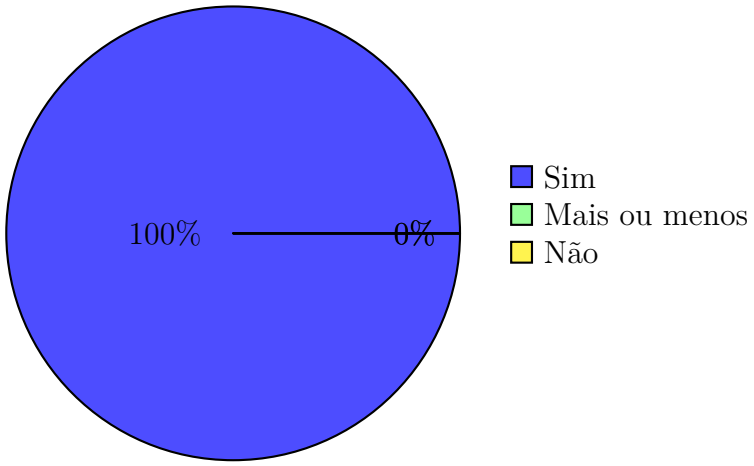


Fonte: Elaborado pelo Autor (2024)

Questão 10- Você acha que o Jogo intitulado **"Trilha da Aritmética"** contribuiu com a aprendizagem dos conteúdos da Aritmética abordados nos Encontros?

- Sim.
- Mais ou menos.
- Não.

Figura 56 – Resultados obtidos na Questão 10 sobre a sequência didática



Fonte: Elaborado pelo autor (2024)

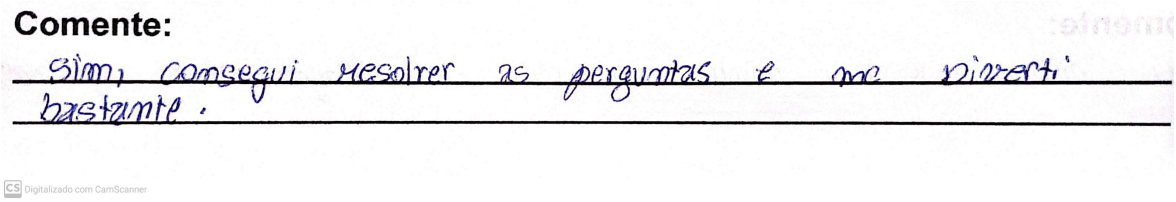
Por fim, a questão 10, avalia-se o jogo lúdico com relação a importância para aprendizagem, todos os alunos responderam que sim, por meio do jogo podemos aprender se divertindo e interagindo com os amigos e professor.

Vale salientar que este recurso lúdico é apenas mais uma ferramenta que pode contribuir para ensino/aprendizagem, neste caso, trabalhamos a maioria dos conceitos e propriedades tornando o ensino mais significativo para o aluno.

O nosso objetivo foi abordar o lúdico para fixar as ideias envolvendo a Aritmética.

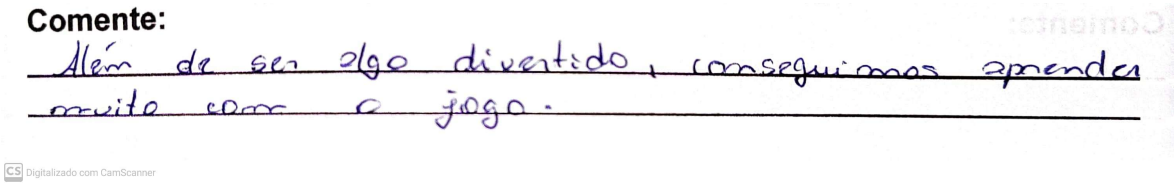
A seguir, temos alguns comentários relevantes com relação a aplicação do jogo em sala de aula.

Figura 57 – Comentário da Questão 10 sobre a metodologia da sequência didática: Aluno 01



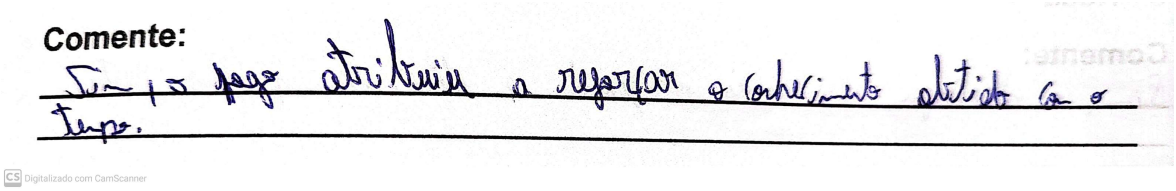
Fonte: Elaborado pelo Autor (2024)

Figura 58 – Comentário da Questão 10 sobre a metodologia da sequência didática: Aluno 02



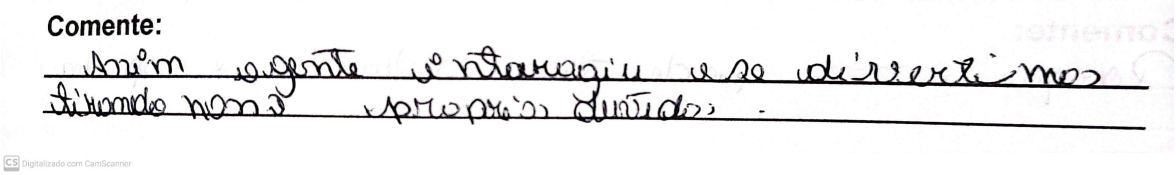
Fonte: Elaborado pelo Autor (2024)

Figura 59 – Comentário da Questão 10 sobre a metodologia da sequência didática: Aluno 03



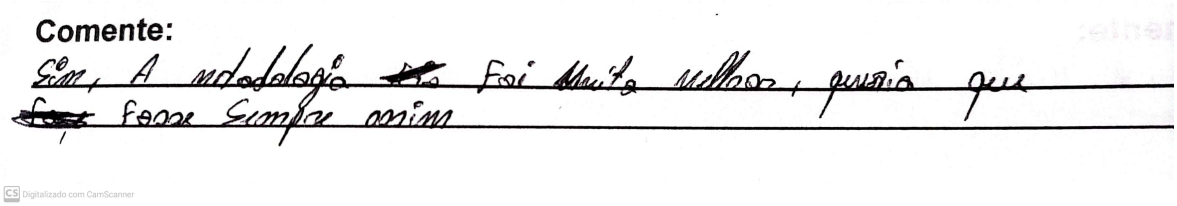
Fonte: Elaborado pelo Autor (2024)

Figura 60 – Comentário da Questão 10 sobre a metodologia da sequência didática: Aluno 08



Fonte: Elaborado pelo Autor (2024)

Figura 61 – Comentário da Questão 10 sobre a metodologia da sequência didática: Aluno 09



Fonte: Elaborado pelo Autor (2024)

No final do sétimo encontro tivemos um momento de agradecimentos a todos envolvidos nesta pesquisa, e por meio destas opiniões podemos identificar os pontos fortes e as dificuldades na prática de ensino/aprendizagem procurando assim, promover uma educação de qualidade e relevante para nossos alunos.

7 Considerações Finais

Este trabalho buscou demonstrar a relevância do uso de aspectos históricos da Aritmética, bem como seus conceitos e aplicações, além de propor uma sequência didática, o uso da linguagem de programação e um jogo lúdico. A escolha dessa estrutura se deu pela convicção de que seria possível abordar os tópicos de maneira significativa e fundamentada.

O objetivo deste trabalho foi de evidenciar as sequências didáticas, aos alunos, aos professores e futuros professores o quanto as sequências são ferramentas relevantes para as aulas de Aritmética.

Os encontros com os alunos, realizados aos sábados, mostrou o quanto é importante o professor conhecer a realidade e a estrutura da escola para que o ensino seja consistente.

Para nós professores é fundamental planejar, organizar e estruturar os encontros para que haja um aprendizagem e estratégia pedagógica eficiente.

Durante estes encontros obtivemos resultados positivos e também dificuldades, que tivemos que superar. Foi neste ambiente que sentimos a necessidade de colocar em prática nosso trabalho acadêmico e abordar alguns tópicos relevantes estudados na disciplina MA 14 - Aritmética do curso de Mestrado Profissional em Matemática (PROFMAT), na intenção de promover um ensino/aprendizagem de qualidade.

A proposta de fazer uma retomada dos conteúdos iniciais de Aritmética oferece a oportunidade especial para os alunos buscarem esses conceitos detalhadamente, melhorando e desenvolvendo suas habilidades e competências em diversas áreas da Matemática.

Com isto, a nossa intenção é tornar o aluno protagonista do seu conhecimento, deixando o mesmo a vontade para esclarecer dúvidas e propor novos caminhos para responder uma determinada questão.

Vale ressaltar que propomos algumas atividades para escutar o aluno, deixando sempre a liberdade de opinar e discutir sobre suas inquietações, afim de melhorar o processo de ensino/aprendizagem. Fizemos uma abordagem sobre o conhecimento aritmético do aluno deixando bem claro que não haveria a exposição da nota e nem críticas sobre o seu conhecimento.

Em seguida, nos encontros trabalhamos diversos conceitos formais retirados principalmente da página das Olimpíadas Brasileira de Matemática das Escolas Públicas (OBMEP), Programa de Iniciação Científica (PIC), Revista do Professor de Matemática (RPM) e outras fontes que consideramos imprescindíveis para a formação do conhecimento matemático.

Durante os encontros também implementamos a linguagem de programação Python, no sentido de aplicação de algoritmos. A utilização desta ferramenta foi importante para mostrar alguns resultados. Percebemos que os alunos ficaram bem motivados e curiosos, mas infelizmente, não foi possível mostrar como cada comando funcionava, por levar muito tempo na introdução deste conhecimento. Nosso objetivo era apenas mostrar que a Computação e Matemática estavam interligados.

A inserção do jogo intitulado “Trilha da Aritmética” foi muito interessante aplicar, por meio do tabuleiro e cartas contendo diversas perguntas, 150 aproximadamente, obtivemos alguns resultados importantes, como a memorização dos conceitos, o cálculo, a interação e as perguntas foram relevantes para os alunos aprenderem de maneira divertida as propriedades e definições. Este recurso foi muito prazeroso de aplicar, pois os alunos se sentiram confiantes e entusiasmados com os prêmios para quem vencesse e para quem perdesse, o importante era a participação de todos.

Por fim, depois da competição no tabuleiro, aplicamos um questionário metodológico, no qual o aluno teria a liberdade de responder as questões de forma livre e sem pressão. Onde deixamos bem claro que era importante os alunos comentarem as questões de forma verdadeira podendo criticar e

argumentar sobre suas dificuldades para que o nosso trabalho fosse melhorado. Após eles responderem, percebemos um nível muito bom de satisfação.

Esta dissertação representa apenas uma pequena fração do vasto campo que a Aritmética oferece para exploração. A riqueza de conceitos, aplicações e abordagens metodológicas da Aritmética permite que o estudo se expanda para diversas áreas, desde a História da Matemática até aplicações modernas em Criptografia e programação. Embora o foco deste trabalho tenha sido desenvolver uma abordagem didática para facilitar a compreensão dos conceitos fundamentais, ainda há muito a ser investigado e explorado. Novas metodologias, ferramentas e perspectivas podem continuar a enriquecer o ensino da Aritmética, abrindo portas para avanços tanto no aprendizado quanto na pesquisa Matemática.

Referências

AMARAL, R. dos S.; SANT'ANA, I. P.; SANT'ANA, C. de C. História do ensino de aritmética no brasil: análise do manual"metodologia do ensino primário-1932. *Com a Palavra, o Professor*, v. 4, n. 8, p. 357–400, 2019. Citado na página 15.

ARAÚJO, D. L. de. O que é (e como faz) sequência didática? *Entrepalavras*, v. 3, n. 1, p. 322–334, 2013. Citado 2 vezes nas páginas 16 e 52.

ARAÚJO, G. C. de; FILHO, P. P. C. Aprendizagem da aritmética na educação de jovens e adultos em uma escola pública tocantinense. *Revista Profissão Docente*, v. 23, n. 48, p. 01–30, 2023. Citado na página 15.

BALESTRA, M. M. M. *A psicopedagogia em Piaget: uma ponte para a educação da liberdade*. [S.l.]: Editora Ibpex, 2012. Citado na página 52.

BOLDRINI, J. L. et al. Álgebra linear, 3a edição. *Sao Paulo: Editora Harbra Ltda*, 1980. Citado 2 vezes nas páginas 85 e 86.

BOYER, C. B. História da matemática; tradução: Elza f. *Gomide. São Paulo, Edgard Blücher, Ed. da Universidade de São Paulo*, 1974. Citado 7 vezes nas páginas 25, 26, 27, 28, 29, 30 e 31.

BRASIL. *Base Nacional Comum Curricular*. 2018. <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 12 jul. 2023. Citado 8 vezes nas páginas 15, 19, 21, 52, 82, 96, 97 e 98.

BRASIL. *Base Nacional Comum Curricular*. 2022. <http://portal.mec.gov.br/docman/fevereiro-2022-pdf/236791-anexo-ao-parecer-cneceb-n-2-2022-bncc-computacao/file>. Acesso em: 12 jul. 2023. Citado 3 vezes nas páginas 53, 59 e 87.

CADAR, L.; DUTENHEFNER, F. Encontros de aritmética. *Apostila do PICOBMEP*, 2015. Citado 3 vezes nas páginas 19, 39 e 69.

CARVALHO, R. P. F. de; DUARTE, A. R. S. A aritmética no ensino primário de brasília: Circulação e apropriações de ideias advindas do pabaee. In: *VII CONGRESSO INTERNACIONAL DE ENSINO DE MATEMÁTICA-2017*. [S.l.: s.n.], 2017. Citado na página 15.

COUTINHO, S. C. Criptografia. *Rio de Janeiro, Programa de Iniciação Científica da OBMEP (PIC-OBMEP)*, 2015. Citado 6 vezes nas páginas 16, 23, 53, 79, 80 e 87.

DANTE, L. R. Matemática: contexto & aplicações. v. 2. *São Paulo: Ática*, 2013. Citado na página 82.

DOLCE, O.; IEZZI, G.; MACHADO, A. *Matemática e Realidade. 6º ao 9º ano*. [S.l.]: São Paulo: Atual, 2009. Citado 3 vezes nas páginas 69, 70 e 72.

GARCIA, A.; LEQUAIN, Y. *Elementos de álgebra*. [S.l.]: Instituto de Matemática Pura e Aplicada, 2006. Citado na página 51.

GRANDO, R. C. O jogo e a matemática no contexto da sala de aula. *São Paulo: Paulus*, p. 07–38, 2004. Citado 3 vezes nas páginas 53, 54 e 93.

HEFEZ, A. Iniciação à aritmética. *Sociedade Brasileira de Matemática*, 2009. Citado 4 vezes nas páginas 32, 58, 65 e 74.

HEFEZ, A.; ARITMÉTICA, C. P. Sociedade brasileira de matemática. 2009. Citado 12 vezes nas páginas 15, 32, 35, 38, 45, 46, 47, 58, 64, 66, 70 e 80.

HYGINO, D. Fundamentos da aritmética. *S. Paulo: Atual*, 1991. Citado 4 vezes nas páginas 25, 27, 57 e 79.

IEZZI, G. et al. *Matemática: ciência e aplicações*. [S.l.]: Atual, 2001. Citado na página 83.

IEZZI, G.; HAZZAN, S. *Fundamentos de matemática elementar, 4: sequências, matrizes, determinantes, sistemas*. [S.l.]: Atual, 2004. Citado 3 vezes nas páginas 83, 84 e 85.

KIM, D.; SOLOMON, M. G. Fundamentos de segurança de sistemas de informação. *Rio de Janeiro: LTC*, p. 653–659, 2014. Citado na página 87.

LDB. *Lei de Diretrizes e Bases da Educação Nacional*. 2017. Diponível em <https://www2.senado.leg.br/bdsf/bitstream/handle/id/529732/lei_de_diretrizes_e_bases_1ed.pdf>. Acesso em: 08 ago. 2024. Citado na página 53.

MCKINNEY, W. *Python para análise de dados: Tratamento de dados com Pandas, NumPy e IPython*. [S.l.]: Novatec Editora, 2018. Citado na página 54.

MEDINA, M.; FERTING, C. *Algoritmos e programação: teoria e prática*. [S.l.]: Novatec Editora, 2006. Citado na página 53.

MOURA, M. O. d. A séria busca no jogo: do lúdico na matemática. *Educação Matemática em Revista*, Sociedade Brasileira de Educação Matemática, v. 2, n. 3, p. 17–24, 1994. Citado na página 23.

OLIVEIRA, M. R. d.; PINHEIRO, M. R. d. R. *Coleçao Elementos da Matemática: Conjuntos e Funçoes Aritmética*. [S.l.]: Fortaleza: Editora VesteSeller, 2010. Citado na página 32.

PACCOLA, E. B. e H. *Matemática*: Versão beta - 2 grau. [S.l.]: Moderna, 1995. ISBN 85-16-01359-6. Citado na página 86.

PARAÍBA. *Proposta Curricular do Novo Ensino Médio da Paraiba*. 2021. Diponível em <https://paraiba.pb.gov.br/arquivos/pdfs/PropostaCurriculardoEnsinoMdiodaParabaPCEMPB23.pdf>. Acesso em: 12 jul. 2023. Citado 3 vezes nas páginas 22, 52 e 82.

PRODANOV, C. C.; FREITAS, E. C. D. *Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico-2ª Edição*. [S.l.]: Editora Feevale, 2013. Citado na página 95.

ROLOFF, E. M. A importância do lúdico em sala de aula. *X Semana de Letras*, v. 70, p. 1–9, 2010. Citado 2 vezes nas páginas 23 e 54.

ROQUE, T.; CARVALHO, J. B. P. de. *Tópicos de história da matemática*. [S.l.]: Sociedade Brasileira de Matemática, 2012. Citado na página 26.

ROSSETO, C. K. Criptografia como recurso didático: uma proposta metodológica aos professores de matemática. Universidade Estadual Paulista (Unesp), 2018. Citado 6 vezes nas páginas 16, 22, 23, 88, 89 e 91.

SILVA, J. L. S. da et al. Matemática lúdica ensino fundamental e médio. *Educação em foco*, 2013. Citado 2 vezes nas páginas 23 e 54.

SOUZA, J. E. d. et al. O uso da linguagem de programação python na resolução de problemas matemáticos do ensino médio. Universidade Federal de Campina Grande, 2023. Citado na página 20.

TELÁRIS, P. *Matemática/Luiz Roberto Dante.–*. [S.l.]: São Paulo, 2012. Citado na página 69.

TERADA, R. Criptografia e a importância das suas aplicações. *Revista do Professor de Matematica*, 1988. Citado 2 vezes nas páginas 16 e 22.

UFABC. *Origem da palavra Aritmética*. 2024. Diponível em <https://lirte.pesquisa.ufabc.edu.br/matreematica/a-matematica-do-cotidiano/ramos/aritmetica/>. Acesso em: 29 jul. 2024. Citado na página 25.

VIEIRA, V. L. *Um Curso Básicio em Teoria dos Números*. [S.l.]: EDUEPB, 2015. Citado na página 47.

WOLTMAN, G. *GIMPS: Great Internet Mersenne Primes Search.[S. l.]*. 1996. Diponível em <https://www.mersenne.org/>. Acesso em: 26 mar. 2023. Citado 2 vezes nas páginas 66 e 67.

ZABALA, A. *A prática educativa: como ensinar*. [S.l.]: Penso Editora, 1998. Citado 2 vezes nas páginas 16 e 52.

Apêndices

APÊNDICE A – Questionário de sondagem sobre o nível de conhecimento aritmético

QUESTIONÁRIO DE AVALIAÇÃO DO NÍVEL DE APRENDIZAGEM DA ARITMÉTICA EM UM GRUPO DE ALUNOS DE UMA TURMA DO 3º DO ENSINO MÉDIO

1- (Portal da OBMEP) Numero primo é aquele que possui exatamente quantos divisores naturais?

a) 1 b) 2 c) 3 d) 4 e) nenhum

Fonte:<https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material/d5slrp7xnz4kg.pdf>. Acesso 19/03/2024.

2-(Portal da OBMEP)Um sapo salta sobre uma régua numerada em centímetros. Se ele inicia no ponto zero e salta de 6 em 6 centímetros. Entre 100 cm e 200 cm ele pisa em quantos números?

Fonte:<https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material/d5slrp7xnz4kg.pdf>. Acesso 19/03/2024.

3-(Portal da OBMEP) No quadro abaixo, marque um X nas casas correspondentes aos divisores (que estão na linha superior) de cada número (que estão na coluna da esquerda)

Divisores	2	3	5	6	9
264					
315					
1461					
3258					

Fonte:<https://cdnportaldaobmep.impa.br/portaldaobmep/uploads/material/diwprpqrh80sw.pdf>. Acesso 19/03/2024

4-(OBMEP-2018) Miguel tinha em sua carteira várias notas de 2, 5, 10, 20 e 50 reais. Ele pagou 63 reais por um livro com seis dessas notas, sem ter troco a receber. Quantas notas de 2 reais ele usou?
a) 0 b) 1 c) 2 d) 3 e) 4

5-(Portal da OBMEP) Um número ao ser dividido por 3, deixa resto 1 e ao ser dividido por 4, deixa resto 1, que número é este?

6-(OBM) Um litro de álcool custa R$0,75. O carro de Henrique percorre 25 km com 3 litros de álcool. Quantos reais serão gastos de álcool para percorrer 600 km?

a) 54 b) 72 c) 50 d) 52 e) 45

7-(OBM) Qual o menor número inteiro positivo pelo qual se deve multiplicar o número $7.3^3.2^4$ para obter um quadrado perfeito?
a) 7 b) 84 c) 0 d) 1 e) 21

8-(Adaptado do portal da OBMEP) No quadro abaixo, marque um X nos números compostos de 1 a 100.

Tabela: Números de 1 a 100

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	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Fonte: Elaborado pelo autor (2024)

APÊNDICE B – Questionário sobre a avaliação metodológica da sequência didática

Questionário para Avaliação de Aplicação das Sequências Didáticas elaboradas para o trabalho de Dissertação "Uma Proposta de Ensino da Aritmética por meio da Criptografia e do Uso de Jogos"

Estimados alunos,

Este questionário tem por objetivo proporcionar aos alunos uma avaliação da metodologia utilizada durante os encontros.

Almejamos que a pesquisa seja respondida de acordo com sua experiência e de forma sincera para que possamos no futuro melhorar a nossa proposta.

Sugestões, elogios e críticas construtivas são importantes para que haja um desenvolvimento para o nosso objeto de estudo.

Lembrando que este questionário será analisado para fins educativos e para melhorar a qualidade da educação. Não precisa se identificar, pois esta análise do questionário será com objetivo de melhorar os encontros abordados neste trabalho.

Ao responder este questionário procure ser objetivo e imparcial.

1- Como você avalia a proposta aplicada com relação ao ensino/aprendizagem da Aritmética nos encontros durante o curso:

- Excelente
- Boa
- Regular
- Ineficiente

Comente:

_____

_____

2- Em que medida a metodologia aplicada ajudou você a entender as definições, propriedades e conceitos abordados na sala de aula:

- Muito
- Razoável
- Pouco
- Nada

Comente:

_____

_____

3- Os recursos utilizados nos encontros (como retroprojetor, apostilas, lousa, lápis, linguagem de programação Python, etc.) contribuíram para uma aprendizagem significativa?

- Muito
- Razoável
- Pouco
- Nada

Comente:

_____
_____

4- Você se sentiu motivado e engajado durante os encontros?

- Muito
- Razoável
- Pouco
- Nada

Comente:

_____
_____

5- A metodologia aplicada ajudou sua participação e interação com os colegas?

- Muito
- Razoável
- Pouco
- Nada

Comente:

_____
_____

6- Você acredita que a metodologia aplicada durante os encontros contribuiu mais no processo de aprendizagem da Aritmética do que as aulas trabalhadas em anos anteriores sobre os mesmos conteúdos abordados nas sequências?

- Muito
- Razoável

- Pouco
- Nada

Comente:

_____

_____

7-O professor foi flexível e objetivo no momento em que sugiram dúvidas nos encontros?

- Muito
- Razoável
- Pouco
- Nada

Comente:

_____

_____

8- Os exercícios e os exemplos contribuíram para melhorar suas habilidades de resolução de situações-problema e raciocínio lógico?

- Sim
- Mais ou menos
- Não

Comente:

_____

_____

9- Você gostaria que esta metodologia fosse aplicada mais vezes durante o ano?

- Sim
- Não

Comente:

_____

_____

10- Você acha que o Jogo intitulado **"Trilha da Aritmética"** contribuiu coma aprendizagem dos conteúdos da Aritmética abordados nos Encontros?

- Sim

- Mais ou menos
- Não

Comente:

_____

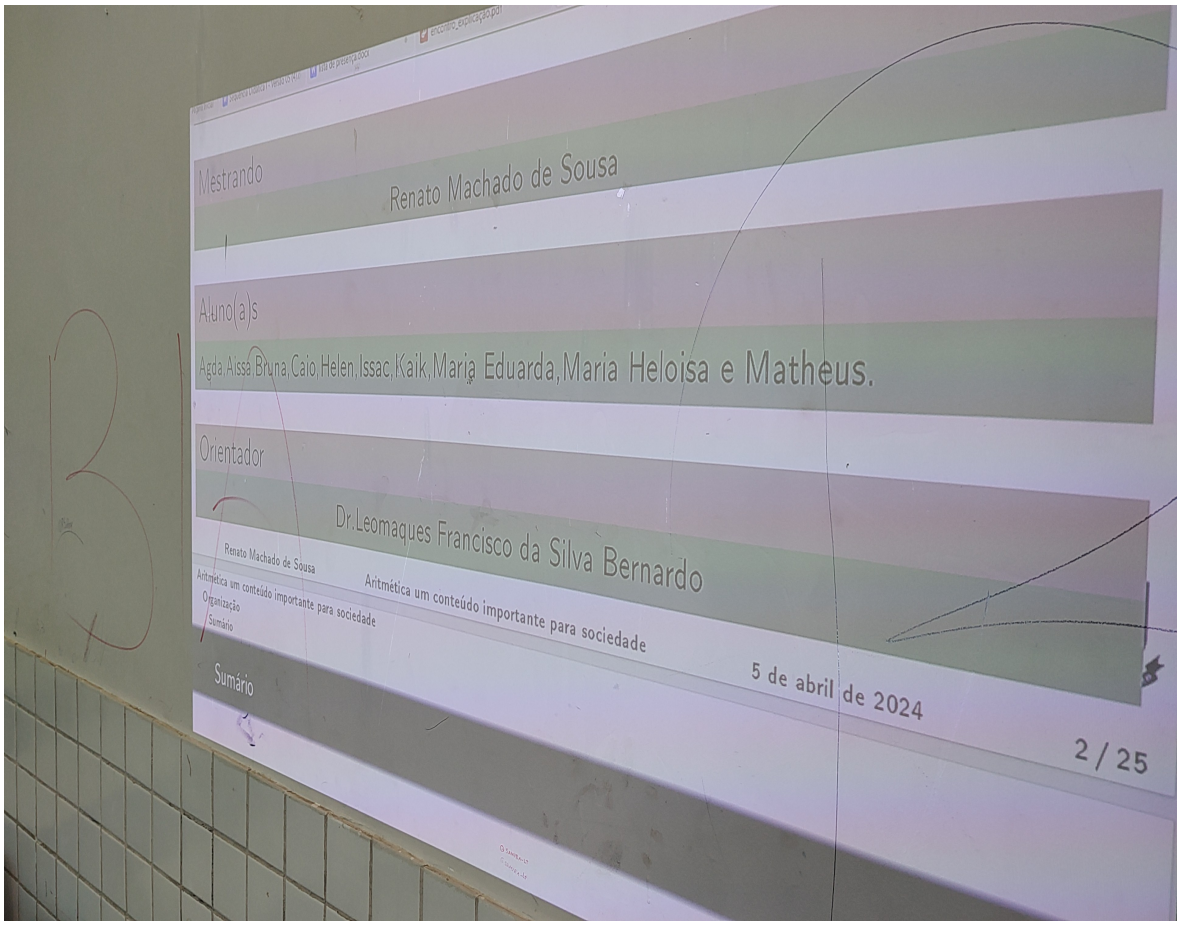
_____

Estas perguntas são importantes para que este trabalho seja melhorado e que sirva de reflexão sobre a abordagem do ensino/aprendizagem. Agradecemos a todos envolvidos nesta pesquisa, pois por meio deste feedback poderemos identificar os pontos fortes e melhorar a prática de ensino/aprendizagem promovendo assim uma educação de qualidade e significativa.

Anexos

ANEXO A – Fotos retiradas durante a sequência didática

Figura 62 – Início dos Encontros

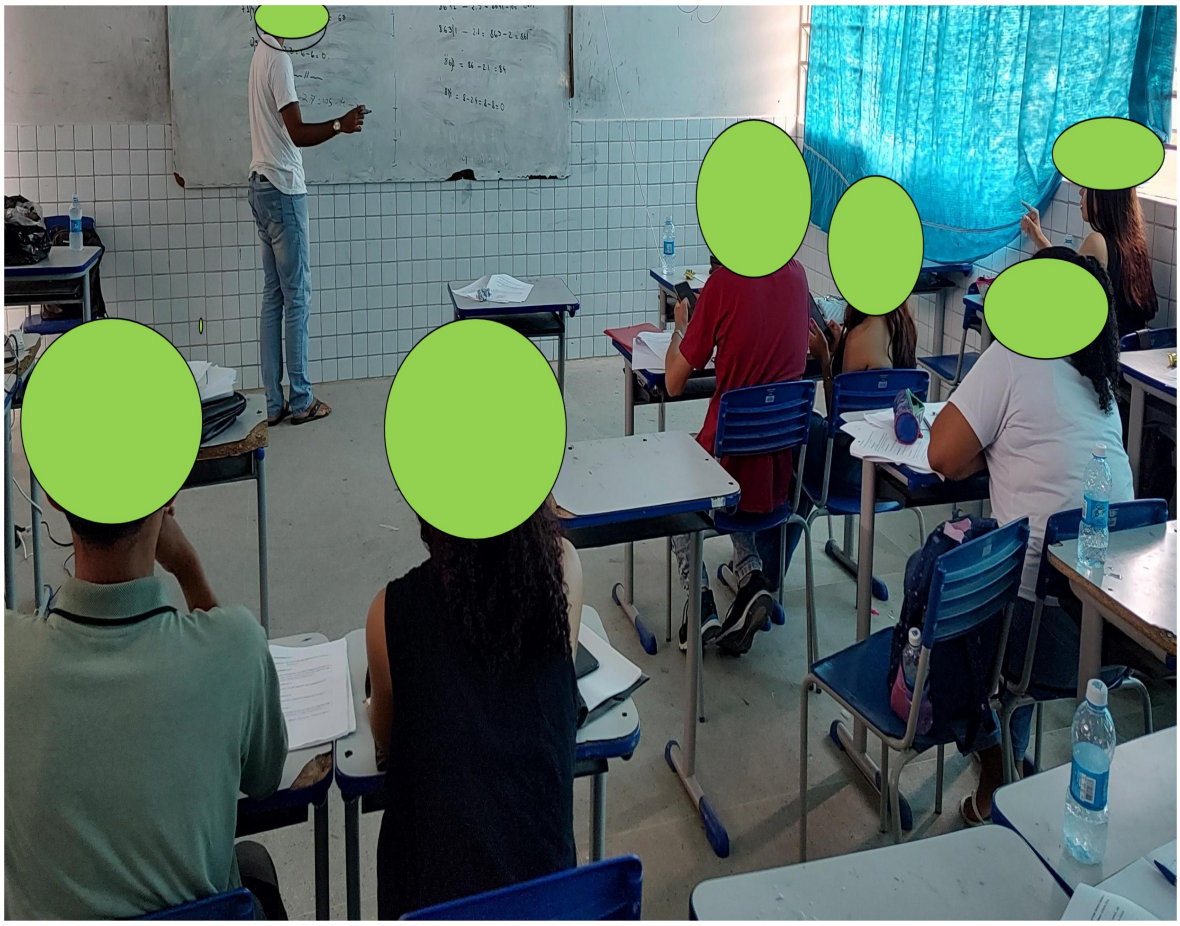


Fonte: Elaborado pelo Autor (2024)

Figura 63 – Teste de sondagem sobre o conhecimento aritmético

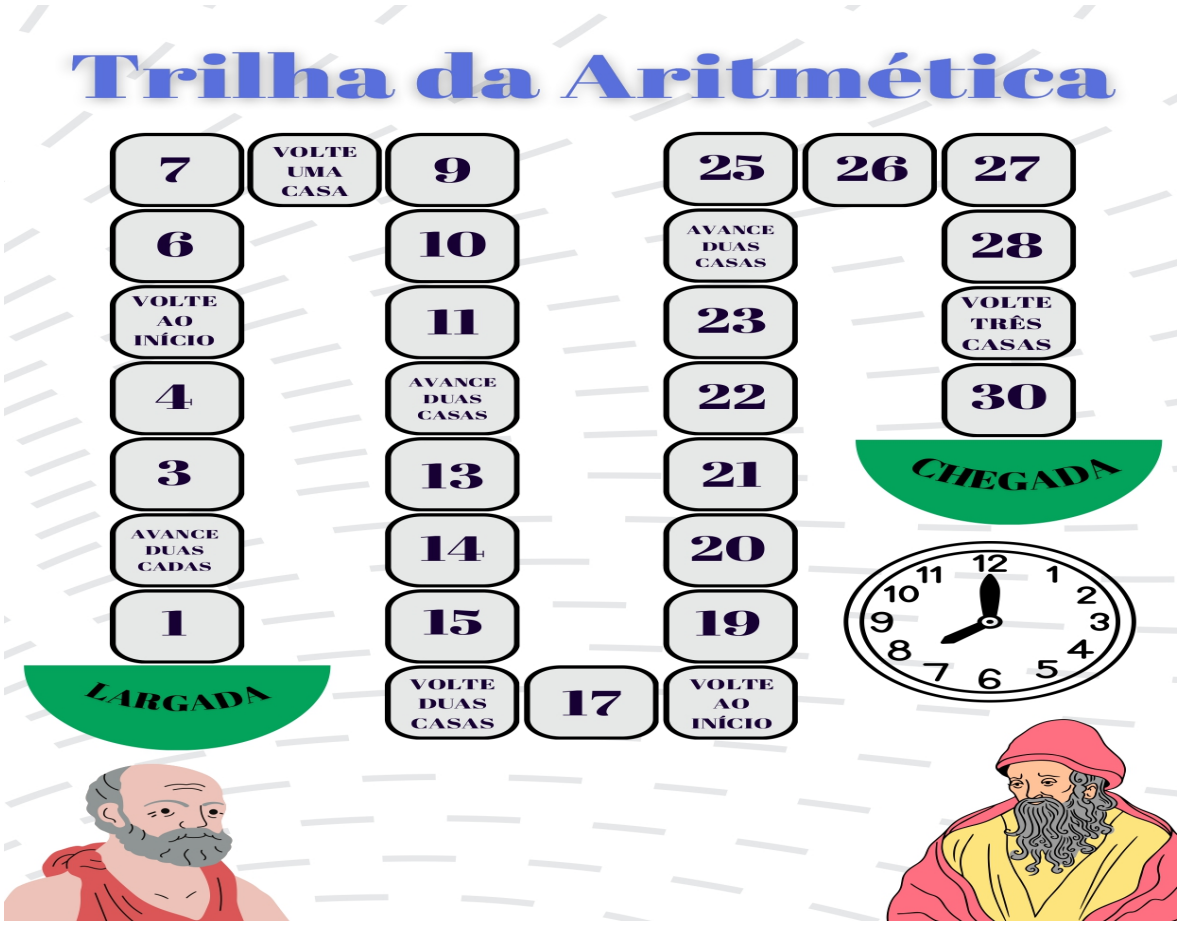
Fonte: Elaborado pelo Autor (2024)

Figura 64 – Aluno aplicando o critérios de divisibilidade por 7



Fonte: Elaborado pelo Autor (2024)

Figura 65 – Trilha da Aritmética arquivo



Fonte: Elaborado pelo Autor (2024)

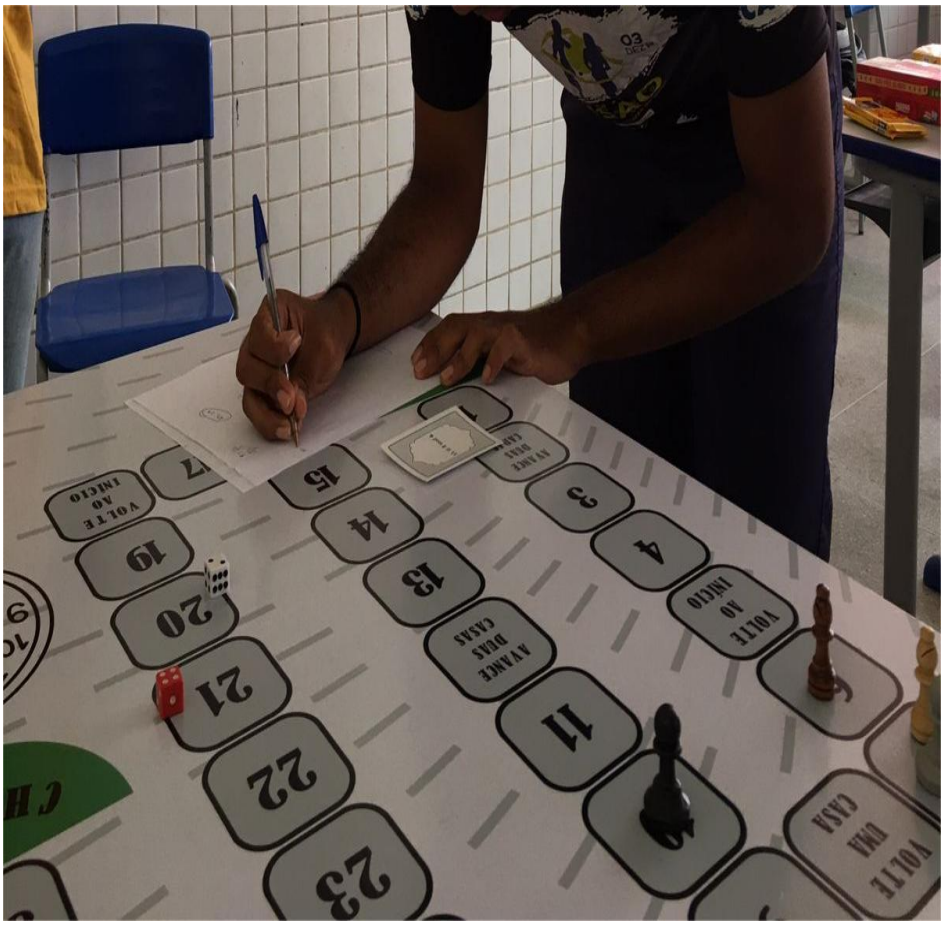
Figura 66 – Cartas

Fonte: Elaborado pelo Autor (2024)

Figura 67 – Trilha

Fonte: Elaborado pelo Autor (2024)

Figura 68 – Alunos utilizando a trilha



Fonte: Elaborado pelo Autor (2024)

Figura 69 – Alunos competindo

Fonte: Elaborado pelo Autor (2024)

Figura 70 – Alunos interagindo

Fonte: Elaborado pelo Autor (2024)

Figura 71 – Os alunos respondendo o questionário

Fonte: Elaborado pelo Autor (2024)