UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Câmpus de Bauru

Mateus José Locali

Aritmética na BNCC: Uma proposta para os anos finais do Ensino Fundamental

BAURU
2024

Mateus José Locali

Aritmética na BNCC: Uma proposta para os anos finais do Ensino Fundamental

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre, junto ao Programa de Pós-Graduação PROFMAT - Mestrado Profissional em Matemática em Rede Nacional, do departamento de Matemática da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Bauru.

Orientador: Prof. Dr. Agnaldo José Ferrari

BAURU
2024

L811a

Locali, Mateus José
Aritmética na BNCC: uma proposta para os anos finais do Ensino Fundamental / Mateus José Locali. -- Bauru, 2024
64 f.

Dissertação (mestrado) - Universidade Estadual Paulista (UNESP), Faculdade de Ciências, Bauru
Orientador: Agnaldo José Ferrari

1. Matemática (Ensino fundamental). 2. Aritmética. 3. Base Nacional Comum Curricular. 4. Congruências e restos. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Dados fornecidos pelo autor(a).

ATA DA DEFESA PÚBLICA DA DISSERTAÇÃO DE MESTRADO DE MATEUS JOSÉ LOCALI, DISCENTE DO PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL, DO INSTITUTO DE BIOCIÊNCIAS, LETRAS E CIÊNCIAS EXATAS - CÂMPUS DE SÃO JOSÉ DO RIO PRETO.

Aos 09 dias do mês de dezembro do ano de 2024, às 09:00 horas, por meio de Videoconferência, realizou-se a defesa de DISSERTAÇÃO DE MESTRADO de MATEUS JOSÉ LOCALI, intitulada **Aritmética na BNCC: Uma proposta para os anos finais do Ensino Fundamental**. A Comissão Examinadora foi constituida pelos seguintes membros: Prof. Dr. AGNALDO JOSÉ FERRARI (Orientador - Participação Presencial) do Departamento de Matemática / UNESP/Câmpus de Bauru, Profa. Dra. TATIANA MIGUEL RODRIGUES DE SOUZA (Participação Presencial) do Departamento de Matemática / UNESP/Câmpus de Bauru, Prof. Dr. JOÃO ELOIR STRAPASSON (Participação Virtual) da Faculdade de Ciências Aplicadas / Universidade Estadual de Campinas. Após a exposição pelo mestrando e arguição pelos membros da Comissão Examinadora que participaram do ato, de forma presencial e/ou virtual, o discente recebeu o conceito final: **APROVADO**. Nada mais havendo, foi lavrada a presente ata, que após lida e aprovada, foi assinada pelo Presidente da Comissão Examinadora.

Prof. Dr. AGNALDO JOSÉ FERRARI

Mateus José Locali

Aritmética na BNCC: Uma proposta para os anos finais do Ensino Fundamental

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre, junto ao Programa de Pós-Graduação PROFMAT - Mestrado Profissional em Matemática em Rede Nacional, do departamento de Matemática da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de Bauru.

Comissão Examinadora

Prof. Dr. Agnaldo José Ferrari
UNESP – Câmpus de Bauru
Orientador

Profa. Dra. Tatiana Miguel Rodrigues
UNESP - Bauru

Prof. Dr. João Eloir Strapasson
UNICAMP – Campinas

BAURU
2024

Dedico este trabalho a São José, Esposo da Mãe de Deus e Protetor da Santa Igreja.

AGRADECIMENTOS

Agradeço:

À Sagrada Família de Nazaré, Jesus, Maria e José.

À minha esposa Maria Clara.

Aos meus pais Marta e Sebastião.

Ao meu orientador Prof. Dr. Agnaldo José Ferrari.

Aos meus professores do PROFMAT, em especial a Profa. Dra. Tatiana Miguel Rodrigues.

À todos que direta ou indiretamente contribuíram para a realização deste trabalho.

"Quem não deixa de caminhar, mesmo que tarde, afinal chega. Para mim, perder o caminho é abandonar a Oração."

Trecho do Livro da Vida - Santa Teresa D'Àvila

RESUMO

Este trabalho tem como objetivo propor a inclusão da Aritmética como uma nova unidade temática na Base Nacional Comum Curricular (BNCC) para os anos finais do Ensino Fundamental. Inicialmente, é feita uma análise detalhada da BNCC, abordando as competências, habilidades e unidades temáticas previstas no documento, com especial atenção à Matemática. É destacada a ausência de uma unidade dedicada à Aritmética, apesar de sua importância no desenvolvimento do pensamento lógico-matemático. A partir dessa constatação, o estudo sugere a criação de uma unidade temática específica para Aritmética, que inclui tópicos como Congruência Modular e introdução à Criptografia. Além disso, são propostas habilidades que possam ser trabalhadas dentro dessa nova unidade, considerando a relevância desses conceitos para a formação matemática dos estudantes. Para apoiar a implementação dessa proposta, o trabalho apresenta sequências didáticas voltadas para professores do Ensino Fundamental, oferecendo orientações práticas de como abordar os novos temas em sala de aula. Com isso, espera-se contribuir para o fortalecimento do ensino da Aritmética e enriquecer o currículo escolar com conteúdos que dialoguem com a realidade contemporânea e seus desafios matemáticos.

Palavras–chave: Aritmética; Base Nacional Comum Curricular - BNCC; Ensino Fundamental Anos Finais; Congruência Modular.

ABSTRACT

This work aims to propose the inclusion of Arithmetic as a new thematic unit in the National Common Curricular Base (BNCC) for the final years of elementary school. Initially, a detailed analysis of the BNCC is conducted, addressing the competencies, skills, and thematic units outlined in the document, with special attention to Mathematics. The absence of a unit dedicated to Arithmetic is highlighted, despite its importance in the development of logical-mathematical thinking. Based on this observation, the study suggests the creation of a specific thematic unit for Arithmetic, which includes topics such as Modular Congruence and an introduction to Cryptography. Additionally, skills that can be developed within this new unit are proposed, considering the relevance of these concepts for students' mathematical education. To support the implementation of this proposal, the work presents didactic sequences aimed at elementary school teachers, offering practical guidance on how to address the new topics in the classroom. It is hoped that this contribution will strengthen the teaching of Arithmetic and enrich the school curriculum with content that connects to contemporary realities and their mathematical challenges.

Keywords: Arithmetic; National Common Curricular Base - BNCC; Final Years of Elementary School; Modular Congruence.

LISTA DE FIGURAS

SUMÁRIO

1 Introdução

A Base Nacional Comum Curricular (BNCC), instituída com o objetivo de uniformizar os conteúdos a serem abordados nas escolas brasileiras, trouxe um novo direcionamento para o Ensino Fundamental, destacando-se em cinco áreas do conhecimento, incluindo a Matemática. Dentro do documento, cada área do conhecimento é dividida em unidades temáticas, que trazem um arranjo de objetos de conhecimento e este, por sua vez, se relaciona com as habilidades a serem desenvolvidas.

A Aritmética, também conhecida como Teoria dos Números, é um dos ramos mais antigos e fundamentais da Matemática, tendo como grandes estudiosos dessa área matemáticos como Euclides, Fermat, Euler e Gauss. Apesar de sua importância histórica e da contribuição no desenvolvimento do raciocínio lógico, este campo não recebe o destaque merecido na BNCC. O documento trata de conceitos relacionados à Aritmética dentro da unidade temática de Números, mas sem uma abordagem sistemática, o que pode resultar em um ensino fragmentado e descontextualizado.

A ausência de uma abordagem sólida e contínua da Aritmética nos anos finais do Ensino Fundamental pode impactar negativamente o desenvolvimento das competências matemáticas dos alunos. A Aritmética está na base de conceitos mais complexos que surgem em fases posteriores, além de ser essencial para o raciocínio lógico e a resolução de problemas. Além disso, conteúdos como congruências modulares e criptografia, amplamente usados em áreas como ciência da computação e segurança digital, poderiam ser introduzidos de forma gradual, permitindo que os estudantes façam conexões entre os conceitos matemáticos e sua aplicação no mundo moderno. Assim, a falta de ênfase nesse campo da Matemática pode comprometer tanto o aprendizado futuro quanto a formação de cidadãos críticos e preparados para enfrentar desafios tecnológicos.

Esse fato reflete a falta de ênfase em Aritmética nos anos finais, onde o conteúdo é abordado apenas de forma limitada entre o sexto e sétimo ano. Além disso, o termo "Aritmética" aparece apenas duas vezes em todo o documento, o que resulta em pouco conhecimento sobre este campo tanto entre professores quanto alunos, contrastando com outros campos da Matemática, como Álgebra, Geometria, Probabilidade e Estatística, que recebem mais destaque. A ausência de uma unidade temática dedicada à Aritmética pode comprometer o desenvolvimento integral das competências matemáticas, fundamentais para a resolução de problemas e para o pensamento lógico dos estudantes.

Além disso, ao ser realizada uma busca no banco de dissertações do programa PROFMAT, encontramos uma vasta gama de trabalhos com "Aritmética" no título, mas em nenhum deles o termo "BNCC" também estava presente. Visto que a análise e revisão do documento sob a perspectiva aritmética é algo inovador para a área e que, deste modo, poderíamos contribuir para a ampliação do conhecimento e popularização da Aritmética na Educação Básica brasileira, atesta-se a importância deste trabalho.

Este trabalho está estruturado em cinco capítulos. O primeiro é destinado a apresentar o documento da Base Nacional Comum Curricular (BNCC), explicando sua estrutura e como a Matemática é abordada nos anos finais do Ensino Fundamental, com destaque para a Aritmética. No segundo capítulo, abordamos os fundamentos teóricos de Aritmética. No terceiro capítulo, apresentamos uma proposta de revisão do documento da BNCC, com foco

na inclusão de conteúdos como congruência modular e introdução à criptografia. O quarto capítulo sugere sequências didáticas que auxiliem o professor no ensino dos novos tópicos de Aritmética propostos nos dois últimos anos do Ensino Fundamental. E no último capítulo apresentamos as considerações finais.

2 A Aritmética na Base Nacional Comum Curricular

Neste capítulo será apresentada a Base Nacional Comum Curricular (BNCC), com ênfase em como a Matemática está apresentada no documento para os anos finais do Ensino Fundamental, e indicaremos quais destas habilidades estão relacionadas à Aritmética.

Esperamos que o conteúdo aqui apresentado mostre como a Aritmética está "esquecida" pela BNCC, pois apesar de prever o ensino de alguns tópicos de Teoria dos Números como as operações com números inteiros, os múltiplos e divisores de um número, números primos e compostos, o cálculo do máximo divisor comum e do mínimo múltiplo comum, outros tópicos estão deixados de lado e, mais a frente neste trabalho, apresentaremos uma proposta de mudança em relação a isso com a introdução na BNCC de novas habilidades, objetos de conhecimento e unidade temática. Além disso, pretendemos expor uma abordagem de como esses conteúdos a serem adicionados podem ser trabalhados nos dois últimos anos do Ensino Fundamental.

2.1 Uma breve explicação sobre a BNCC

A Base Nacional Comum Curricular (BNCC) é um documento normativo que orienta os currículos das escolas brasileiras, homologada em 20 de dezembro de 2017 pelo então ministro da Educação, Mendonça Filho, e em 14 de dezembro de 2018 teve sua parte destinada ao Ensino Médio também homologada, desta vez pela então ministra da Educação, Roseli Soares, estabelecendo os conhecimentos essenciais que todos os alunos, tanto da rede pública quanto privada, devem aprender durante a Educação Básica.

A BNCC estabelece que, ao longo da Educação Básica, as aprendizagens essenciais devem contribuir para o desenvolvimento de dez competências gerais. Estas competências sintetizam, no âmbito pedagógico, os direitos de aprendizagem e desenvolvimento dos estudantes. Segundo a BNCC, competência é definida como:

> a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas, cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas da vida cotidiana, do pleno exercício da cidadania e do mundo do trabalho (Brasil, 2018, p. 8).

As competências de cada componente curricular se originam das dez competências gerais da BNCC que são:

> 1. Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.
> 2. Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.

> 3. Valorizar e fruir as diversas manifestações artísticas e culturais, das locais às mundiais, e também participar de práticas diversificadas da produção artístico-cultural.
>
> 4. Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos e produzir sentidos que levem ao entendimento mútuo.
>
> 5. Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva.
>
> 6. Valorizar a diversidade de saberes e vivências culturais e apropriar-se de conhecimentos e experiências que lhe possibilitem entender as relações próprias do mundo do trabalho e fazer escolhas alinhadas ao exercício da cidadania e ao seu projeto de vida, com liberdade, autonomia, consciência crítica e responsabilidade.
>
> 7. Argumentar com base em fatos, dados e informações confiáveis, para formular, negociar e defender ideias, pontos de vista e decisões comuns que respeitem e promovam os direitos humanos, a consciência socioambiental e o consumo responsável em âmbito local, regional e global, com posicionamento ético em relação ao cuidado de si mesmo, dos outros e do planeta.
>
> 8. Conhecer-se, apreciar-se e cuidar de sua saúde física e emocional, compreendendo-se na diversidade humana e reconhecendo suas emoções e as dos outros, com autocrítica e capacidade para lidar com elas.
>
> 9. Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da diversidade de indivíduos e de grupos sociais, seus saberes, identidades, culturas e potencialidades, sem preconceitos de qualquer natureza.
>
> 10. Agir pessoal e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação, tomando decisões com base em princípios éticos, democráticos, inclusivos, sustentáveis e solidários. (Brasil, 2018, p. 9 e 10).

A BNCC detalha como as aprendizagens são organizadas em cada etapa da escolaridade e explica a composição dos códigos alfanuméricos utilizados para identificar essas aprendizagens. As competências são especificadas para as três etapas da Educação Básica: Educação Infantil (EI), Ensino Fundamental (EF) e Ensino Médio (EM).

No Ensino Fundamental, está organizado em cinco áreas do conhecimento, sendo elas: Linguagens, Matemática, Ciências da Natureza, Ciências Humanas e Ensino Religioso. Que por sua vez são divididas em nove componentes curriculares: Língua Portuguesa (LP), Arte (AR), Educação Física (EF), Língua Inglesa (LI), Matemática (MA), Ciências (CI), Geografia (GE), História (HI) e Ensino Religioso (ER).

Cada componente curricular define suas próprias competências específicas, alinhadas às competências gerais a serem desenvolvidas ao longo dos nove anos. Para assegurar essas competências específicas, cada componente curricular identifica um conjunto de habilidades associadas a diversos objetos de conhecimento, que por fim são organizados em unidades temáticas.

> Respeitando as muitas possibilidades de organização do conhecimento escolar, as unidades temáticas definem um arranjo dos objetos de conhecimento ao longo do

> Ensino Fundamental adequado às especificidades dos diferentes componentes curriculares. Cada unidade temática contempla uma gama maior ou menor de objetos de conhecimento, assim como cada objeto de conhecimento se relaciona a um número variável de habilidades.
>
> As habilidades expressam as aprendizagens essenciais que devem ser asseguradas aos alunos nos diferentes contextos escolares. Para tanto, elas são descritas de acordo com uma determinada estrutura. (Brasil, 2018, p.29)

Ademais, a BNCC salienta que as habilidades não determinam ações ou comportamentos específicos dos professores, nem sugerem abordagens ou metodologias. Essas decisões são responsabilidade dos currículos e projetos pedagógicos, que devem ser adaptados à realidade de cada sistema ou rede de ensino e de cada instituição escolar, considerando o contexto e as características dos alunos. Nos quadros que descrevem as unidades temáticas, os objetos de conhecimento e as habilidades para cada ano (ou conjunto de anos), cada habilidade é indicada por um código alfanumérico, cuja estrutura é semelhante ao exemplo a seguir: EF06MA03.

Este código é construído utilizando, respectivamente, duas letras que determinam a etapa da Educação Básica que a habilidade é destinada, neste caso para o Ensino Fundamental, seguido por dois algarismos que indicam o ano, neste caso é uma habilidade de 6°ano, depois novamente duas letras que determinam a componente curricular e, por fim, outros dois algarismos que indicam a posição da habilidade na numeração sequencial do ano ou bloco de anos.

É importante ressaltar que a numeração sequencial usada para identificar as habilidades de cada ano ou bloco de anos não sugere uma ordem ou hierarquia das aprendizagens. A progressão das aprendizagens, evidenciada na comparação entre os quadros de cada ano, pode estar relacionada a processos cognitivos, expressos por verbos que indicam ações mais ativas ou complexas, aos objetos de conhecimento, que podem se tornar mais sofisticados, ou aos contextos de aplicação, que podem se expandir gradualmente. A organização sequencial das habilidades na BNCC é apenas uma das formas possíveis de disposição e visa garantir a clareza sobre o que todos os alunos devem aprender na Educação Básica, servindo como diretriz para a elaboração de currículos em todo o país e adaptando esses currículos às diversas realidades.

2.2 A Matemática na BNCC

O conhecimento matemático é indispensável para todos os alunos da Educação Básica, tanto por sua vasta aplicação na sociedade moderna quanto por seu papel na formação de cidadãos críticos e conscientes de suas responsabilidades sociais. A Matemática vai além da simples quantificação de fenômenos, como contagem e medição, e das técnicas de cálculo com números e grandezas; ela também explora a incerteza associada a fenômenos aleatórios. A disciplina cria sistemas abstratos que organizam e interligam fenômenos de espaço, movimento, formas e números, relacionados ou não ao mundo físico. Esses sistemas são essenciais para entender fenômenos, construir representações significativas e desenvolver argumentações

consistentes em diversos contextos. No Ensino Fundamental, é crucial que a Matemática assegure que os alunos conectem práticas do mundo real a representações matemáticas, façam suposições e induções, desenvolvendo assim a capacidade de aplicar conceitos matemáticos na resolução de problemas.

Além disso, nesta etapa da Educação Básica é essencial focar no desenvolvimento das competências e habilidades para raciocinar, representar, comunicar e argumentar matematicamente. Esse desenvolvimento está profundamente relacionado a várias formas de organização da aprendizagem matemática, baseadas na análise de situações do cotidiano, de outras áreas do conhecimento e da própria Matemática. Os processos matemáticos, como a resolução de problemas, a investigação, o desenvolvimento de projetos e a modelagem, são considerados formas privilegiadas de atividade matemática. Por isso, eles são tanto objetos de estudo quanto estratégias de aprendizagem ao longo de todo o Ensino Fundamental.

Diante do exposto e das competências gerais da Educação Básica, a BNCC organizou as competências específicas da Matemática.

> COMPETÊNCIAS ESPECÍFICAS DE MATEMÁTICA PARA O ENSINO FUNDAMENTAL
>
> 1. Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho.
> 2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.
> 3. Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções.
> 4. Fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las crítica e eticamente, produzindo argumentos convincentes.
> 5. Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.
> 6. Enfrentar situações-problema em múltiplos contextos, incluindo-se situações imaginadas, não diretamente relacionadas com o aspecto prático-utilitário, expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas, e dados).
> 7. Desenvolver e/ou discutir projetos que abordem, sobretudo, questões de urgência social, com base em princípios éticos, democráticos, sustentáveis e solidários, valorizando a diversidade de opiniões de indivíduos e de grupos sociais, sem preconceitos de qualquer natureza.
> 8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles. (Brasil, 2018, p.267)

Para a sua criação a BNCC teve como base os currículos recentes e, devido a isso, deu importância aos diferentes campos que compõem a Matemática e suas principais ideias que estão interligadas, entre elas: proporcionalidade, ordem, interdependência, equivalência, variação e aproximação.

Por conseguinte, foi proposto pela BNCC cinco unidades temáticas que reúnem os objetos de conhecimento matemáticos em habilidades que devem ser desenvolvidas ao longo de todo o Ensino Fundamental, são elas: Números; Álgebra; Geometria; Grandezas e Medidas; Probabilidade e Estatística. A seguir veremos como a BNCC define cada uma delas.

> A unidade temática Números tem como finalidade desenvolver o pensamento numérico, que implica o conhecimento de maneiras de quantificar atributos de objetos e de julgar e interpretar argumentos baseados em quantidades. No processo da construção da noção de número, os alunos precisam desenvolver, entre outras, as ideias de aproximação, proporcionalidade, equivalência e ordem, noções fundamentais da Matemática. Para essa construção, é importante propor, por meio de situações significativas, sucessivas ampliações dos campos numéricos. No estudo desses campos numéricos, devem ser enfatizados registros, usos, significados e operações. (Brasil, 2018, p.268)

Ou seja, os alunos dos anos finais do Ensino fundamental precisam ser capazes de resolver problemas utilizando números naturais, inteiros e racionais, aplicando as operações fundamentais com diversos significados e estratégias, compreendendo os processos envolvidos. Da mesma maneira devem dominar cálculos de porcentagem, juros, descontos e acréscimos, incluindo o uso de tecnologias digitais, além de reconhecer, comparar e ordenar números reais usando a reta numérica. O pensamento numérico dos alunos se amplia ao se relacionar com conteúdos de outras unidades temáticas. Também é crucial abordar conceitos básicos de economia e finanças, como taxas de juros, inflação e investimentos, promovendo a educação financeira.

> A unidade temática Álgebra, por sua vez, tem como finalidade o desenvolvimento de um tipo especial de pensamento – pensamento algébrico – que é essencial para utilizar modelos matemáticos na compreensão, representação e análise de relações quantitativas de grandezas e, também, de situações e estruturas matemáticas, fazendo uso de letras e outros símbolos. Para esse desenvolvimento, é necessário que os alunos identifiquem regularidades e padrões de sequências numéricas e não numéricas, estabeleçam leis matemáticas que expressem a relação de interdependência entre grandezas em diferentes contextos, bem como criar, interpretar e transitar entre as diversas representações gráficas e simbólicas, para resolver problemas por meio de equações e inequações, com compreensão dos procedimentos utilizados. As ideias matemáticas fundamentais vinculadas a essa unidade são: equivalência, variação, interdependência e proporcionalidade. Em síntese, essa unidade temática deve enfatizar o desenvolvimento de uma linguagem, o estabelecimento de generalizações, a análise da interdependência de grandezas e a resolução de problemas por meio de equações ou inequações. (Brasil, 2018, p.270)

Em relação a Álgebra nos anos finais, é esperado que os alunos aprofundem e ampliem os conhecimentos adquiridos nos anos iniciais. Eles devem compreender os diversos significados das variáveis em uma expressão, generalizar propriedades, investigar a regularidade de

sequências numéricas, identificar valores desconhecidos em sentenças algébricas e estabelecer relações entre grandezas. A conexão entre variável e função, e entre incógnita e equação, é fundamental. Os alunos devem aprender a resolver equações e inequações, inclusive no plano cartesiano, como uma forma de representar e solucionar problemas. Além disso, a aprendizagem de Álgebra deve contribuir para o desenvolvimento do pensamento computacional, capacitando os alunos a traduzirem situações-problema para fórmulas, tabelas e gráficos. A importância dos algoritmos e seus fluxogramas, que podem ser estudados nas aulas de Matemática, também é destacada.

> A Geometria envolve o estudo de um amplo conjunto de conceitos e procedimentos necessários para resolver problemas do mundo físico e de diferentes áreas do conhecimento. Assim, nessa unidade temática, estudar posição e deslocamentos no espaço, formas e relações entre elementos de figuras planas e espaciais pode desenvolver o pensamento geométrico dos alunos. Esse pensamento é necessário para investigar propriedades, fazer conjecturas e produzir argumentos geométricos convincentes. É importante, também, considerar o aspecto funcional que deve estar presente no estudo da Geometria: as transformações geométricas, sobretudo as simetrias. As ideias matemáticas fundamentais associadas a essa temática são, principalmente, construção, representação e interdependência. (Brasil, 2018, p.271)

Pode-se dizer que o ensino de Geometria nos anos finais do Ensino Fundamental deve focar em tarefas que envolvam transformações e ampliações/reduções de figuras geométricas planas, destacando os conceitos de congruência e semelhança. Os alunos precisam reconhecer as condições para triângulos congruentes ou semelhantes e aplicar esse conhecimento em demonstrações simples. Além disso, é crucial integrar Álgebra e Geometria, conseguindo representações de sistemas de equações no plano cartesiano. A Geometria deve ir além da aplicação de fórmulas para cálculo de área e volume e das aplicações numéricas de teoremas, abrangendo uma compreensão mais profunda das relações geométricas e suas representações.

> As medidas quantificam grandezas do mundo físico e são fundamentais para a compreensão da realidade. Assim, a unidade temática Grandezas e medidas, ao propor o estudo das medidas e das relações entre elas – ou seja, das relações métricas –, favorece a integração da Matemática a outras áreas de conhecimento, como Ciências (densidade, grandezas e escalas do Sistema Solar, energia elétrica etc.) ou Geografia (coordenadas geográficas, densidade demográfica, escalas de mapas e guias etc.). Essa unidade temática contribui ainda para a consolidação e ampliação da noção de número, a aplicação de noções geométricas e a construção do pensamento algébrico. (Brasil, 2018, p.273)

Espera-se que os alunos dos anos finais do Ensino Fundamental sejam capazes de reconhecer grandezas como comprimento, área, volume e ângulo, associadas a figuras geométricas, e de resolver problemas que envolvam essas grandezas usando as unidades de medida padronizadas. Além do mais, devem estabelecer e utilizar relações entre essas grandezas e outras não geométricas, como densidade, velocidade, energia e potência. Também é importante que os alunos aprendam a determinar expressões para o cálculo de áreas de quadriláteros, triângulos e círculos, bem como os volumes de prismas e cilindros.

> A incerteza e o tratamento de dados são estudados na unidade temática Probabilidade e estatística. Ela propõe a abordagem de conceitos, fatos e procedimentos presentes em muitas situações- -problema da vida cotidiana, das ciências e da tecnologia. Assim, todos os cidadãos precisam desenvolver habilidades para coletar, organizar, representar, interpretar e analisar dados em uma variedade de contextos, de maneira a fazer julgamentos bem fundamentados e tomar as decisões adequadas. Isso inclui raciocinar e utilizar conceitos, representações e índices estatísticos para descrever, explicar e predizer fenômenos. (Brasil, 2018, p.274)

Nesta unidade temática, em relação aos anos finais, deseja-se que os alunos consigam utilizar as medidas de tendência central, em especial a moda, média e mediana, para a realização de pesquisas e relatórios estatísticos. Também a construção de diferentes tipos de gráficos e tabelas. Além disso, espera-se também que fique claro para o aluno a diferença entre as definições de amostra e população, com o intuito dele conseguir utilizar técnicas adequadas para realizar uma amostragem.

Em síntese, as unidades temáticas de Matemática nos anos finais do Ensino Fundamental estão interligadas de certo modo, e todas são essenciais para o desenvolvimento das habilidades matemáticas básicas, do raciocínio lógico e para a resolução de problemas, de modo que preparem o aluno para a próxima etapa da Educação Básica. Além disso, elas capacitam os alunos a entenderem a importância da Matemática em diversos contextos, possibilitando a contextualização do conteúdo com o seu cotidiano, também é possível fazer conexões com outras áreas do conhecimento e explorar a interdisciplinaridade, além do uso de tecnologias tanto para a resolução quanto para a visualização de questões matemáticas mais complexas.

2.3 Aritmética ausente na BNCC

A Aritmética é um dos principais ramos da Matemática e seu principal objeto de estudo são as propriedades dos números inteiros. Tal estudo vem ocorrendo e evoluindo ao longo dos séculos por notáveis matemáticos, dos quais podemos destacar entre eles Euclides (aprox. 300 a.C.), Pierre de Fermat (1601-1665), Leonhard Euler (1707-1783) e Carl Friedrich Gauss (1777-1855). Deste último podemos compreender a importância da Aritmética pela sua afirmação em sua obra *Disquisitiones Arithmeticae*: "A Matemática é a rainha das ciências e a Aritmética (Teoria dos Números) é a rainha da Matemática".

Infelizmente, como visto anteriormente, a BNCC não possui uma unidade temática intitulada Aritmética, porém podemos encontrar objetos de conhecimento e habilidades que fazem parte do ensino de alguns tópicos de Aritmética, todos esses estão compreendidos dentro da unidade temática Números. Como nosso foco neste trabalho são os anos finais do Ensino Fundamental, iremos abordar as habilidades concentradas apenas nesta parte da Educação Básica, e veremos nos quadros a seguir que as habilidades relacionadas diretamente à Aritmética estão concentradas apenas no sexto e sétimo ano do Ensino Fundamental.

Quadro 1 – Objetos de conhecimento e habilidades relacionadas à Aritmética no 6°ano

Objetos de conhecimento	**Habilidades**
Operações (adição, subtração, multiplicação, divisão e potenciação) com números naturais Divisão euclidiana	(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora.
Fluxograma para determinar a paridade de um número natural Múltiplos e divisores de um número natural Números primos e compostos	(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). (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.

Fonte: Brasil, 2018, p.300 e 301

Como podemos observar no sexto ano do Ensino Fundamental as primeiras habilidades da BNCC que iniciam a abordagem de tópicos de Aritmética são as quatro operações básicas envolvendo os números naturais, a paridade de um número natural, as ideias introdutórias do conceito de múltiplos e divisores de um número natural, números primos e compostos e critérios de divisibilidade. Vale ressaltar aqui que em nenhum momento o termo "Teorema Fundamental da Aritmética" é utilizado.

Quadro 2 – Objetos de conhecimento e habilidades relacionadas à Aritmética no 7°ano

Objetos de conhecimento	**Habilidades**
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	(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. (EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.

Fonte: Brasil, 2018, p.306 e 307

Já no sétimo ano do Ensino Fundamental as habilidades trabalhadas que envolvem os tó-

picos de Aritmética são o cálculo do Máximo Divisor Comum e do Mínimo Múltiplo Comum, a ordenação dos números inteiros e as operações com números inteiros.

Percebemos que mesmo que essas habilidades sejam todas da área de Aritmética, não encontramos a palavra "Aritmética" citada em nenhuma delas, na realidade, em toda a BNCC ela aparece somente duas vezes e com o mesmo propósito, especificar um dos campos da Matemática, como podemos observar. "por meio da articulação de seus diversos campos – Aritmética, Álgebra, Geometria, Estatística e Probabilidade" (Brasil, 2018, p.265) e "Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade)" (Brasil, 2018, p.267).

Notamos que os outros três campos da Matemática que são citados (Álgebra, Geometria e Estatística e Probabilidade) intitulam três das cinco unidades temáticas - um adendo ao terceiro termo que muda de ordem para ser título da unidade temática – e deixam o questionamento de pôr qual motivo a Aritmética não pode também ter a sua própria unidade temática, por isso no capítulo 4 iremos propor uma mudança na BNCC com a implementação dela, além dos objetos de conhecimentos e habilidades que poderiam ser acrescentados para serem trabalhados no oitavo e nono ano do Ensino Fundamental.

3 Tópicos de Aritmética

Neste capítulo iremos apresentar os conteúdos relacionados a Aritmética que também são trabalhados, de maneira simplificada, na Educação Básica. Além de expor o conteúdo necessário para o desenvolvimento e aplicação da nossa proposta de plano de aula a ser apresentada no decorrer deste trabalho. As definições, resultados e propriedades enunciadas neste capítulo encontram-se no livro Aritmética (HEFEZ, 2022).

3.1 Números Inteiros

Os números inteiros têm sua origem nos números naturais, criados para resolver problemas de contagem. Desde a antiguidade, a introdução dos números negativos foi recebida com desconfiança tanto pelos matemáticos quanto pelas atividades mercantis da época. No entanto, surgiu a necessidade de realizar operações de adição e multiplicação com esses números inteiros.

O conjunto dos números inteiros é denotado pela letra $\mathbb{Z}$ e representado por:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$$

Nesta seção iremos explorar as operações de adição e multiplicação no conjunto dos inteiros e a ordenação deste conjunto.

3.1.1 Adição e multiplicação

As operações de adição $(+)$ e multiplicação $(.)$ no conjunto dos números inteiros $(\mathbb{Z})$ possuem algumas propriedades que as definem. Para isso, consideremos a, a', b, b' e $c \in \mathbb{Z}$, e em relação a multiplicação vamos suprimir o seu símbolo para efeito de simplificação, por exemplo, ao invés de "$a.b$" escreveremos "ab":

1. São operações bem definidas: Se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $ab = a'b'$.
2. São operações comutativas, indicando que a ordem dos números nessas operações não altera o resultado: $a + b = b + a$ e $ab = ba$.
3. São operações associativas, indicando que a maneira como os números são agrupados nessas operações não altera o resultado: $(a + b) + c = a + (b + c)$ e $(ab)c = a(bc)$.
4. Possuem elemento neutro, sendo 0 o elemento neutro da adição e 1 o elemento neutro da multiplicação: $a + 0 = a$ e $a1 = a$.
5. A adição possui elementos simétricos: Existe $b(= -a)$ tal que $a + b = 0$.

6. A multiplicação é distributiva em relação à adição: Tem-se $a(b+c) = ab + ac$.

Essas propriedades são fundamentais para a compreensão e a manipulação das operações aritméticas no conjunto dos números inteiros. Elas não apenas fornecem uma base sólida para cálculos simples, mas também são essenciais em áreas mais avançadas da Matemática, já que qualquer conjunto em que as operações de adição e multiplicação possuem as seis propriedades listadas são chamados de anel.

Além disso, podemos particionar o conjunto dos números inteiros em três subconjuntos dele: o conjunto dos números naturais, o conjunto unitário zero e o conjunto dos simétricos de $\mathbb{N}$ $(-\mathbb{N})$. Assim,

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N}).$$

Ainda em relação as propriedades da adição, podemos definir uma outra operação básica, a subtração.

Define-se a menos b, denotado por $a - b$ como sendo

$$a - b = a + (-b).$$

A partir dos seis axiomas, iremos destacar as proposições 3.1 e 3.2, sendo que esta só será apresentada depois da definição de ordenação dos inteiros.

Proposição 3.1. $a0 = 0$ para todo $a \in \mathbb{Z}$.

Demonstração. Temos que $0a = 0$, pois $0a = (0+0)a = 0a + 0a$, o que implica que $0a - 0a = (0a + 0a) - 0a = 0a + (0a - 0a) = 0a$. Assim, $0 = 0a$.

3.1.2 Ordenação dos inteiros

Para que possamos ordenar os números inteiros, precisamos de características únicas que somente eles possuem, como o Princípio da Boa Ordenação.

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

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

Além disso, admitiremos que em $\mathbb{Z}$ também valem as seguintes propriedades:

7) $\forall a, b \in \mathbb{Z}$, tem-se que $a + b \in \mathbb{Z}$ e $ab \in \mathbb{Z}$. Chamada de fechamento de $\mathbb{Z}$, ou seja, o conjunto é fechado para toda adição e multiplicação.

8) Tricotomia: Dados a, $b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

   (i) $a = b$;

   (ii) $b - a \in \mathbb{N}$;

(iii) $a - b \in \mathbb{N}$.

Dizemos que a é menor do que b, simbolizado por $a < b$, toda vez que a propriedade (ii) for verificada. Assim, segue da propriedade (iii) que $b < a$.

Podemos reescrever a propriedade (8) usando a notação $<$:

(i) $a = b$;

(ii) $a < b$;

(iii) $b < a$.

Utilizando a notação $b > a$, que se lê b é maior do que a, para representar $a < b$. Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z}; x > 0\} = \mathbb{N} \quad \text{e} \quad \{x \in \mathbb{Z}; x < 0\} = -\mathbb{N}.$$

Daí decorre que $a > 0$ se, e somente se, $-a < 0$.

A seguir, enunciaremos algumas proposições.

Proposição 3.2. A adição é compatível e cancelativa com respeito à igualdade:

$$\forall a, b, c \in \mathbb{Z}, a = b \iff a + c = b + c.$$

Demonstração. A implicação $a + c = b + c$ é consequência do fato da adição ser bem definida. Suponha agora que $a + c = b + c$. Temos três possibilidades:

(i) $a < b$. Temos que $a + c < b + c$, o que é um absurdo.

(ii) $b < a$. Pelo mesmo argumento acima, $b + c < a + c$, o que também é um absurdo.

(iii) $a = b$. Esta é a única alternativa válida.

Em outras palavras, podemos somar $-c$ aos dois lados da igualdade para obter o desejado.

Proposição 3.3. A relação menor do que é transitiva

$$\forall a, b, c \in \mathbb{Z}; a < b \text{ e } b < c \Rightarrow a < c.$$

Demonstração. Suponha que $a < b$ e $b < c$, então temos que $b - a > 0$ e $c - b > 0$. Logo ambos são resultados naturais e $\mathbb{N}$ é aditivamente fechado, temos que:

$$c - a = (b - a) + (c - b) \in \mathbb{N};$$

portanto $a < c$.

Proposição 3.4. A adição é compatível e cancelativa com respeito à relação "menor do que"

$$\forall a, b, c \in \mathbb{Z}; a < b \iff a + c < b + c.$$

Demonstração. ($\Rightarrow$) Supondo que $a < b$. Temos que $b - a \in \mathbb{N}$. Logo,

$$(b + c) - (a + c) = b - a \in \mathbb{N}.$$

Portanto $a + c < b + c$.

($\Leftarrow$) Supondo que $a + c < b + c$. Podemos somar $(-c)$ a ambos os lados da desigualdade, devido à primeira parte da proposição, logo $a < b$, como queríamos demonstrar.

Proposição 3.5. A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que"

$$\forall a, b \in \mathbb{Z}; \forall c \in \mathbb{N}, a < b \iff ac < bc.$$

($\Rightarrow$) Supondo $a < b$. Temos $b - a \in \mathbb{N}$, e se $c \in \mathbb{N}$, como $\mathbb{N}$ é multiplicativamente fechado, segue que

$$bc - ac = (b - a)c \in \mathbb{N}.$$

Portanto $ac < bc$.

($\Leftarrow$) Supondo que $ac < bc$, com $c \in \mathbb{N}$. Temos, pela tricotomia:

(i) $a = b$. Que resulta em $ac = bc$. Falso.

(ii) $b < a$. Pela primeira parte da demonstração isso resulta em $bc < ac$. Falso.

(iii) $a < b$. Única possibilidade válida.

Proposição 3.6. A multiplicação é compatível e cancelativa com respeito à igualdade

$$\forall a, b \in \mathbb{Z}; \forall c \in \mathbb{Z} - \{0\}, a = b \iff ac = bc.$$

($\Rightarrow$) É consequência imediata do fato da multiplicação ser bem definida.

($\Leftarrow$) Supondo $ac = bc$, temos três possibilidades:

(i) $a < b$. Que resulta em $ac < bc$. Absurdo.

(ii) $b < a$. Que resulta em $bc < ac$. Absurdo.

(iii) $a = b$. Única possibilidade válida.

Com o intuito de visualizar a ordenação do conjunto dos inteiros, podemos organizá-los em uma linha, geralmente chamada de reta numérica, onde o zero é o ponto central, à sua direita estão os números inteiros positivos, e à esquerda estão os números inteiros negativos.

3.2 Divisão nos Inteiros

A divisão no conjunto dos números inteiros é uma operação que não é sempre fechada, o que significa que o quociente de dois inteiros pode não ser um número inteiro. Em casos em que a divisão não é exata, usamos o conceito de quociente e resto para representar a operação, a chamada Divisão Euclidiana. Quando for possível efetuar a divisão de um número inteiro por outro utilizaremos o termo divisibilidade.

3.2.1 Divisibilidade

Definição 3.7. (Divisibilidade) Sejam dois números inteiros a e b, diz-se que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Assim, neste caso, a é um divisor de b, ou a é um fator de b ou, ainda, que b é um múltiplo de a. Observe que a notação $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade a existência de um inteiro c tal que $b = ca$. A negação dessa sentença é representada por $a \nmid b$, que pode ser lida como "a não divide b", significando que inexiste número inteiro c tal que $b = ca$.

Exemplo 3.8. $7 \mid 105$, pois $105 = 15 \cdot 7$.

Exemplo 3.9. $6 \nmid 23$, pois não existe um inteiro c tal que $23 = 6c$.

Proposição 3.10.
Consideremos $a, b, c, d, m, n \in \mathbb{Z}$. Tem-se que:

1. $1 \mid a$;
2. $a \mid a$;
3. $a \mid 0$;
4. $0 \mid a$ se, e somente se, $a = 0$;
5. Se $a \mid b$ e $b \mid c$, então $a \mid c$;
6. Se $a \mid b$ e $c \mid d$, então $(ac) \mid (bd)$;
7. Se $a \mid b$ e $a \mid c$, então $a \mid (b \pm c)$;
8. Se $a \mid b$, então $a \mid (bc)$;
9. Se $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$;
10. Se $a \mid b$, então $|a| \leq |b|$;

11. Se $b \mid a$ e $a \mid b$, então $a = \pm b$;

12. Se $a \mid 1$, então $a = \pm 1$.

Demonstrações:

1. Decorre da igualdade $a = a1$.

2. Decorre da igualdade $a = 1a$.

3. Decorre da igualdade $0 = 0a$.

4. Suponhamos que $0 \mid a$; logo existe $c \in \mathbb{Z}$ tal que $a = c0$, e, portanto, $a = 0$. Para a recíproca, basta observarmos que $0 \mid 0$, demonstrado no item anterior.

5. Se $a \mid b$, então existe um inteiro m tal que $b = am$, e se $b \mid c$, então existe um inteiro n tal que $c = bn$. Substituindo b em c, temos $c = (am)n = a(mn)$. Portanto, $a \mid c$.

6. Se $a \mid b$, então existe um inteiro m tal que $b = am$, e se $c \mid d$, então existe um inteiro n tal que $d = cn$. Multiplicando estas duas equações, obtemos $bd = (am)(cn) = (ac)(mn)$. Portanto, $(ac) \mid (bd)$.

7. Se $a \mid b$, então existe um inteiro m tal que $b = am$. Se $a \mid c$, então existe um inteiro n tal que $c = an$. Somando e subtraindo obtemos $b + c = am + an = a(m + n)$ e $b - c = am - an = a(m - n)$. Portanto, $a \mid (b \pm c)$.

8. Se $a \mid b$, então existe um inteiro m tal que $b = am$. Logo, $bc = (am)c = a(mc)$. Portanto, $a \mid (bc)$.

9. Se $a \mid b$, então existe um inteiro k tal que $b = ak$, e se $a \mid c$, então existe um inteiro l tal que $c = al$. Multiplicando e somando temos, $mb + nc = m(ak) + n(al) = a(mk + nl)$. Portanto, $a \mid (mb + nc)$.

10. Se $a \mid b$, então existe um inteiro k tal que $b = ak$. Se $b = 0$, então a também deve ser 0, e $|a| = |b| = 0$. Se $b \neq 0$, então $|b| = |ak| = |a||k|$. Como $|k|$ é pelo menos 1, temos $|a| \leq |b|$.

11. Se $b \mid a$, então existe um inteiro m tal que $a = bm$ e se $a \mid b$, então existe um inteiro n tal que $b = an$. Substituindo a primeira equação na segunda, temos $b = (bm)n = b(mn)$. Se $b \neq 0$, então $mn = 1$, o que implica que m e n são ± 1. Portanto, $a = \pm b$.

12. Se $a \mid 1$, então existe um inteiro k tal que $1 = ak$. Logo, para que a igualdade seja verdadeira a e k devem ser ± 1. Portanto, $a = \pm 1$.

Exemplo 3.11. $1 \mid 13$, pois $13 = 1 \cdot 13$.

Exemplo 3.12. $5 \mid 5$, pois $5 = 1 \cdot 5$.

Exemplo 3.13. $16 \mid 0$, pois $0 = 16 \cdot 0$.

Exemplo 3.14. $2 \mid 8$ e $8 \mid 48$, segue que, $8 = 2 \cdot 4$ e $48 = 8 \cdot 6$, daí $48 = (4 \cdot 2) \cdot 6 = 2 \cdot (4 \cdot 6)$. Logo, $2 \mid 48$.

Exemplo 3.15. $3 \mid 15$ e $4 \mid 16$, temos que $15 = 3 \cdot 5$ e $16 = 4 \cdot 4$. Portanto, $15 \cdot 16 = (3 \cdot 5) \cdot (4 \cdot 4) = (3 \cdot 4) \cdot (5 \cdot 4)$. Logo, $3 \cdot 4 \mid 15 \cdot 16$.

Exemplo 3.16. $5 \mid 15$ e $5 \mid 25$, com isso temos que $15 = 5 \cdot 3$ e $25 = 5 \cdot 5$. Somando as duas equações resulta que $15 + 25 = 5 \cdot (3 + 5)$. Logo, $5 \mid 15 + 25$.

3.2.2 Divisão Euclidiana

Mesmo que tenhamos dois números inteiros a e b, sendo que nem a divide b e nem b divide a, podemos fazer a divisão entre eles a partir da Divisão Euclidiana.

Teorema 3.17. Dados dois números inteiros a e b (com $b \neq 0$), existem únicos inteiros q e r tais que:

$$a = bq + r \quad \text{e} \quad 0 \leq r < |b|,$$

onde q é o quociente e r é o resto da divisão de a por b.

Demonstração. Seja o conjunto

$$S = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Existência:

Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |b|$.

Suponhamos por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de S, pois $s = a - (q \pm 1)b$, com $s < r$.

Unicidade:

Suponha que $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ 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, $r = r'$.

Exemplo 3.18. Considere os inteiros $a = 17$ e $b = 5$. Aplicando a divisão euclidiana, temos:

$$17 = 5 \cdot 3 + 2.$$

Aqui, o quociente $q = 3$ e o resto $r = 2$, cumprindo as condições $0 \leq r < |5|$.

Observação. Utilizaremos a notação $[\frac{a}{b}]$ para indicar a parte inteira do número racional $\frac{a}{b}$, ou seja, $[\frac{a}{b}]$ é o quociente da divisão euclidiana de a por b.

3.3 Algoritmo de Euclides

Nesta seção iremos apresentar os conceitos de Máximo Divisor Comum e Mínimo Múltiplo Comum, denotados respectivamente por mdc e mmc, além do Algoritmo de Euclides como forma para calcular o mdc a partir de repetidas divisões euclidianas.

3.3.1 Máximo Divisor Comum

Dados dois inteiros a e b, sejam eles distintos ou não, um número inteiro $d \in \mathbb{Z}$ será dito um divisor comum de a e b se $d \mid a$ e $d \mid b$. Por exemplo, $\pm 1, \pm 2, \pm 5, \pm 10$ são os divisores comuns de 20 e 30. Utilizando agora a definição dada por Euclides no livro Elementos, que se constitui em um dos pilares da sua Aritmética, diremos que um número inteiro $d \geq 0$ é o máximo divisor comum de a e b, denotamos por $\text{mdc}(a, b)$, 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, ou seja, se c é um divisor comum de a e b, então $c \mid d$.

Exemplo 3.19. O $\text{mdc}(20, 30)$ é 10.

Em determinadas situações específicas, o cálculo do mdc é direto. Por exemplo, se a é um número inteiro não nulo, é claro que:

(i) $\text{mdc}(0, a) = |a|$;

(ii) $\text{mdc}(1, a) = 1$;

(iii) $\text{mdc}(a, a) = |a|$;

(iv) Se $b \in \mathbb{Z}$, então $a \mid b \Leftrightarrow \text{mdc}(a, b) = |a|$;

(v) $\text{mdc}(a, b) = \text{mdc}(-a, b) = \text{mdc}(-a, -b) = \text{mdc}(a, -b)$.

Observe que os itens mencionados acima seguem diretamente da definição de máximo divisor comum juntamente com a definição de divisibilidade. Além disso, o item (v) nos permite assumir, sem perda de generalidade, que o $\text{mdc}(a, b)$ é igual ao $\text{mdc}(|a|, |b|)$, isso simplificará o processo de encontrar o máximo divisor comum de dois inteiros quaisquer.

Teorema 3.20. Se $a = bq + r$, então $\text{mdc}(a, b) = \text{mdc}(b, r)$.

Demonstração. Supondo que $d = \text{mdc}(a, b)$, queremos mostrar que $d = \text{mdc}(b, r)$. Como $d = \text{mdc}(a, b)$, segue que $d \mid a$ e $d \mid b$. Assim, pela Proposição 3.10, $d \mid (a - bq)$. Mas como $a - bq = r$, segue que $d \mid r$. Logo, d é um divisor comum de b e r.

Considerando c um inteiro, tal que $c \mid b$ e $c \mid r$. Assim, $c \mid (bq + r)$ e, consequentemente, $c \mid a$. Como $d = \text{mdc}(a, b)$ e c também é um divisor comum de a e b, segue da definição de máximo divisor comum, que $c \mid d$. Portanto $d = \text{mdc}(b, r) \Rightarrow \text{mdc}(a, b) = \text{mdc}(b, r)$.

Teorema 3.21. (Algoritmo de Euclides) Para todos $a, b \in \mathbb{Z}$, existe $\text{mdc}(a, b) = d$.

Demonstração. Observe que é equivalente mostrar para $a, b \in \mathbb{N}$, pois, como vimos, $\text{mdc}(a, b) = \text{mdc}(|a|, |b|)$. Além disso, como $\text{mdc}(a, b) = a$ quando $a \mid b$, resta analisar o caso em que $1 < a < b$ e $a \nmid b$. Assim, aplicando o Algoritmo da Divisão, temos que:

$$b = aq_1 + r_1 \quad \text{com} \quad 0 < r_1 < a.$$

Assim, se $r_1 \mid a$, então

$$\text{mdc}(a, b) = \text{mdc}(a, b - aq_1) = \text{mdc}(a, r_1) = r_1.$$

Se $r_1 \nmid a$, então

$$a = r_1q_2 + r_2 \quad \text{com} \quad 0 < r_2 < r_1 \quad (\text{onde } r_2 = a - r_1q_2).$$

Assim, se $r_2 \mid r_1$, então

$$\text{mdc}(a, b) = \text{mdc}(a, r_1) = \text{mdc}(a - r_1q_2, r_1) = \text{mdc}(r_2, r_1) = r_2.$$

Caso contrário, se $r_2 \nmid r_1$, então

$$r_1 = r_2q_3 + r_3 \quad \text{com} \quad 0 < r_3 < r_2 \quad (\text{onde } r_3 = r_1 - r_2q_3).$$

E assim continuamos o procedimento até que pare (quando encontrarmos o máximo divisor comum). Note que isso sempre ocorre, pois, caso contrário, teríamos uma sequência de números naturais $a > r_1 > r_2 > \ldots$ que não possui menor elemento, o que é um absurdo pelo Princípio da Boa Ordenação. Sendo assim, para algum k, temos que $r_k \mid r_{k-1}$, o que nos dá $\text{mdc}(a, b) = r_k$.

De modo simples, podemos dizer que $\text{mdc}(a, b) = r_k$, onde r_k é o último resto não nulo das divisões sucessivas mencionadas anteriormente.

Exemplo 3.22. Calculemos o mdc de 252 e 200.

$$
\begin{aligned}
252 &= 200 \cdot 1 + 52 \\
200 &= 52 \cdot 3 + 44 \\
52 &= 44 \cdot 1 + 8 \\
44 &= 8 \cdot 5 + \mathbf{4} \\
8 &= 4 \cdot 2 + 0
\end{aligned}
$$

Assim, o $\mathrm{mdc}(252, 200)$ é o último resto não nulo, que é 4.

3.3.2 Mínimo Múltiplo Comum

Podemos afirmar que um número inteiro é um múltiplo comum de dois ou mais números inteiros dados se ele for, simultaneamente, um múltiplo de todos esses números. Sempre serão múltiplos comuns de a e b o produto ab (e suas variantes negativas) e o zero.

Um número inteiro positivo m é considerado o mínimo múltiplo comum (mmc) dos números inteiros a e b se m for o menor inteiro positivo que é múltiplo de a e de b.

Para inteiros a e b diferentes de zero, dizemos que o número $m \in \mathbb{N}$ é o mínimo múltiplo comum (mmc) entre a e b se m satisfizer as seguintes condições:

i) m é um múltiplo de a e b, isto é, $a \mid m$ e $b \mid m$;

ii) Se c é um múltiplo comum de a e b, ou seja, $a \mid c$ e $b \mid c$, então $m \mid c$.

Denotaremos o mínimo múltiplo comum entre a e b por $m = \mathrm{mmc}(a, b)$.

Por exemplo, 30 é múltiplo de 3 e 5, mas não é $\mathrm{mmc}(3, 5)$, o mínimo múltiplo comum nesse caso é 15.

Proposição 3.23. Dados dois números inteiros a e b, temos que $\mathrm{mmc}(a, b)$ existe e

$$\mathrm{mmc}(a, b)\mathrm{mdc}(a, b) = |ab|.$$

Demonstração. Se a=0 ou b=0, a igualdade é trivialmente satisfeita, então iremos verificar a igualdade para a e b não nulos, e, sem perda de generalidade, consideraremos a e b positivos

Existência de $\mathrm{mmc}(a, b)$:

O mínimo múltiplo comum $\mathrm{mmc}(a, b)$ de a e b é o menor inteiro positivo que é múltiplo de ambos. A existência de $\mathrm{mmc}(a, b)$ é garantida, pois o conjunto de múltiplos comuns positivos de a e b não é vazio (por exemplo, $|ab|$ é um múltiplo comum de a e b). Portanto, $\mathrm{mmc}(a, b)$ sempre existe.

Agora, o mínimo múltiplo comum $\mathrm{mmc}(a, b)$ é o menor número positivo que é múltiplo de a e b, e o máximo divisor comum $\mathrm{mdc}(a, b)$ é o maior número positivo que divide tanto a quanto b.

Seja $d = \text{mdc}(a, b)$. Então, por definição:

$$d \mid a \quad \text{e} \quad d \mid b.$$

Podemos escrever a e b em termos de d:

$$a = da' \quad \text{e} \quad b = db',$$

onde a' e b' são inteiros que não têm fatores comuns (isto é, $\text{mdc}(a', b') = 1$).

O mínimo múltiplo comum $\text{mmc}(a, b)$ deve ser um múltiplo de ambos a e b. Assim, podemos escrever:

$$\text{mmc}(a, b) = da'b'.$$

Portanto, o produto $\text{mmc}(a, b)\text{mdc}(a, b)$ é:

$$\text{mmc}(a, b)\text{mdc}(a, b) = (da'b')d = d^2a'b'.$$

Note que:

$$ab = (da')(db') = d^2a'b'.$$

Portanto:

$$\text{mmc}(a, b)\text{mdc}(a, b) = |ab|.$$

Assim, $\text{mmc}(a, b)\text{mdc}(a, b) = |ab|$, como queríamos demonstrar.

A partir da Proposição 3.23. podemos utilizar o Algoritmo de Euclides para calcular o mínimo múltiplo comum entre dois números inteiros não nulos, dividindo o módulo do produto dos dois números pelo seu máximo divisor comum.

Exemplo 3.24. Calculemos o $\text{mmc}(252, 200)$.

Sabemos pelo Exemplo 3.22 que $\text{mdc}(252, 200) = 4$.

Logo,

$$\text{mmc}(252, 200) = \frac{252 \cdot 200}{4} = 12600.$$

3.4 Números Primos

Nesta seção abordaremos um dos conceitos mais importantes da Matemática, os números primos. O principal resultado dessa seção é o Teorema Fundamental da Aritmética. Os números primos estão atrelados a diversos problemas que, apesar de esforços de diferentes gerações de matemáticos, continuam sem solução.

3.4.1 Teorema Fundamental da Aritmética

Definição 3.25. Qualquer número natural maior do que 1, que possui apenas dois divisores positivos, sendo eles o 1 e ele próprio é chamado de número primo.

A partir dessa definição, podemos inferir os seguintes fatos para dois números primos p e q e um número inteiro qualquer a:

(i) Se $p \mid q$, então $p = q$. De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

(ii) Se $p \nmid a$, então $\text{mdc}(p, a) = 1$. De fato, se $\text{mdc}(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$.

Se um número inteiro $n > 1$ possui mais de dois divisores positivos ele é chamado de composto. Assim, n é composto, se existem $n_1, n_2 \in \mathbb{N}$, $1 < n_2 \leq n_1 < n$ com $n = n_1 n_2$.

Exemplos de números primos: 2, 3, 5, 7, 11, 13, 17.

Exemplos de números compostos: 4, 6, 8, 9, 10, 12, 14.

Definição 3.26. Dois números inteiros serão chamados de primos entre si, ou coprimos, quando o máximo divisor comum entre eles for igual a 1.

Exemplos de pares de coprimos: (4, 9), (7, 12), (35, 88).

Corolário 3.27. Se $p, p_1, \ldots, p_n$ são números primos e, se $p \mid p_1 \cdots p_n$, então $p = p_i$ para algum $i = 1, \ldots, n$.

Demonstração. Utilizando o Princípio de Indução: Sejam p, p_1, $\ldots$, p_n, p_{n+1} números primos.

Se $p \mid p_1$, como p e p_1 são primos, por hipótese, então $p = p_1$.

Suponha que $p \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n$, então $p = p_i$, para algum $i = 1, 2, \ldots, n$.

Logo, se $p \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n$, então $p \mid p_1 \cdot p_2 \cdot \cdots \cdot p_n \cdot p_{n+1}$ e, portanto, $p = p_i$, para algum $i = 1, 2, 3, \ldots, n, n+1$.

Teorema 3.28. 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.

Demonstração. Utilizaremos a segunda forma do Princípio de Indução.

Se $n = 2$, o resultado é claramente verificado. Supondo agora que o resultado seja válido para todo número natural menor do que n, vamos mostrar que também é válido para n.

Se n é primo, não há o que demonstrar. Então, vamos supor que n seja composto. Assim, existem números $n_1, n_2 \in \mathbb{N}$ tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Por hipótese de indução, existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Logo, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Agora, vamos mostrar a unicidade da escrita. Supondo que $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p_1 \mid q_1 \cdots q_s$, pelo Corolário 3.27, então $p_1 = q_j$ para algum j, que após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

$p_2 \cdots p_r = q_2 \cdots q_s$. Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

Teorema 3.29. Dado um número inteiro n não nulo e diferente de 1 e -1, existem primos $p_1 < \ldots < p_r$ e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que

$$n = \pm p_1^{\alpha_1} \ldots p_r^{\alpha_r}.$$

Ao utilizar a decomposição em fatores primos de dois ou mais números naturais, podemos dispor da convenção de incluir fatores na forma $p^0 = 1$, onde p é qualquer número primo. Assim, dados $n, m \in \mathbb{N}$ com $n > 1$ e $m > 1$, podemos escrever

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \quad \text{e} \quad m = p_1^{\beta_1} \ldots p_r^{\beta_r},$$

usando o mesmo conjunto de primos $p_1, \ldots, p_r$. Nessa representação, permitimos que os expoentes $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r$ variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$.

Um processo muito utilizado na Educação Básica para a decomposição de um número em primos é a chamada fatoração em números primos, que consiste na divisão sucessiva pelo menor primo divisor do número em questão, como mostra o exemplo a seguir:

Exemplo 3.30. Decomponha o número 84 em fatores primos

84	2
42	2
21	3
7	7
1	

Portanto,

$$84 = 2^2 \cdot 3 \cdot 7.$$

Com a decomposição em números primos é possível obter o mínimo múltiplo comum e o máximo divisor comum entre dois ou mais números, encontrar a quantidade de divisores e quem são os divisores de um número natural, extrair ou simplificar uma radiciação.

3.4.2 Um Pouco Sobre a Distribuição dos Números Primos

Teorema 3.31. Existem infinitos números primos.

Demonstração. Vamos supor, por absurdo, que existem finitos números primos, sendo eles $p_1, \ldots, p_r$. Vamos considerar o número $a = p_1 \cdot \ldots \cdot p_r + 1$.

Por hipótese, a não pode ser primo. Mas, pelo Teorema 3.28, a possui um fator primo p, tal que $p \mid p_1 \cdot \ldots \cdot p_r + 1$ e por hipótese $p = p_i$ para algum $i = 1, 2, \ldots, r$, o que resulta em $p \mid p_1 \cdot \ldots \cdot p_r$ e consequentemente $p \mid 1$, o que é um absurdo. Portanto, existem infinitos números primos.

Lema 3.32. Se um número natural $n > 1$ não é divisível por nenhum primo p tal que $p^2 \leq n$, então ele é primo.

Demonstração. Supondo, por absurdo, que n não é primo e também não é divisível por nenhum primo p tal que $p^2 \leq n$. Seja q o menor primo que divide n, então $n = qn'$, com $q \leq n'$. Acontece que $q^2 \leq qn'$. Logo, n é divisível por um primo q tal que $q^2 \leq n$, o que é um absurdo.

Vamos utilizar esse resultado para a construção do *Crivo de Eratóstenes*, um dos métodos mais antigos e ainda utilizado na Educação Básica para elaborar uma tabela com números primos.

O método consiste em escrever os números naturais de 2 até algum número desejado e depois ir riscando os números que são múltiplos dos primos, como veremos na sequência. Por não ser eficiente para ordens elevadas e como queremos mostrar a aplicação do Lema 3.32, vamos escrever até o número 150 ($< 13^2$).

Depois de escritos, devemos começar riscando todos os múltiplos de 2, com exceção do 2, que é primo. Com isso, partimos para o segundo número que não está riscado, que é o 3 e é primo, então riscamos todos os múltiplos dele, pois não são primos. O próximo não riscado que aparece é o 5; faremos o mesmo processo de riscar seus múltiplos. E continuamos com o mesmo processo até o número primo 11, não sendo necessário verificar o 13, pois, como foi visto no Lema 3.32, nosso $n < 13^2$. Com isso, todos os números que não estão riscados são números primos.

	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~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	119	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	127	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	137	~~138~~	139	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	149	~~150~~

Mesmo sendo antigo e trabalhoso, este processo ainda é útil para um aluno da Educação Básica, pois ele fornece uma boa quantidade de números primos que ajudam na fatoração e, como foi dito anteriormente, o processo de decomposição em fatores primos proporciona diversos resultados.

3.5 Congruências

A teoria das congruências modulares é um campo central na teoria dos números, focado na análise dos restos das divisões euclidianas. As congruências módulo m desempenham um papel crucial na verificação da divisibilidade de números e são fundamentais para os sistemas de criptografia modernos. Nesta seção, exploraremos a definição e algumas propriedades essenciais das congruências modulares, acompanhadas de suas respectivas demonstrações. Ilustraremos como dois números inteiros são considerados congruentes quando apresentam o mesmo resto ao serem divididos por um número inteiro positivo.

3.5.1 Aritmética dos Restos

Seja $m \in \mathbb{N}$. Quando dois números inteiros a e b apresentam o mesmo resto na divisão euclidiana por m, chamamos esses dois números de congruentes módulo m, e utilizamos a notação:

$$a \equiv b \mod m.$$

Porém, quando os seus restos na divisão por m são diferentes, então chamamos eles de não congruentes módulo m, e escrevemos:

$$a \not\equiv b \mod m.$$

Por exemplo, $27 \equiv 22 \mod 5$, pois os restos da divisão de 27 e de 22 por 5 são iguais a 2. Por outro lado, $27 \not\equiv 22 \mod 4$, pois o resto da divisão de 27 por 4 é 3 e de 22 por 4 é 2.

Observação: O resto da divisão de qualquer número inteiro por 1 é sempre 0, logo todos os números inteiros são congruentes módulo 1, o que torna seu estudo desinteressante. Devido a isso, sempre iremos considerar $m > 1$ para nossos estudos.

Proposição 3.33. Suponha que $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \mod m$ se, e somente se, $m \mid (b - a)$.

Demonstração. ($\Rightarrow$) Supondo que $a \equiv b \mod m$. Pela Divisão Euclidiana, existem inteiros q, q' e r, tais que $a = mq + r$ e $b = mq' + r$, onde $0 \leq r < m$. Temos que

$$b - a = mq' + r - (mq + r) = m(q' - q).$$

Logo, $m \mid (b - a)$.

($\Leftarrow$) Supondo que $m \mid (b - a)$. Então, existe $q \in \mathbb{Z}$ tal que $b - a = mq$. Portanto, $b = mq + a$. E sejam q' e r o quociente e o resto da divisão de a por m, respectivamente. Assim,

$$a = mq' + r,$$

com $q', r \in \mathbb{Z}$ e $0 \leq r < m$. Logo, segue que

$$b = mq + a = mq + (mq' + r) = m(q + q') + r,$$

ou seja,

$$b = m(q + q') + r,$$

onde $0 \leq r < m$. Pela unicidade na Divisão Euclidiana, concluímos que r é também o resto da divisão de b por m. Portanto, $a \equiv b \mod m$.

Proposição 3.34. Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que:

(i) $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, então $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$.

Não é necessário efetuar a divisão euclidiana em ambos os números para verificar se são congruentes. O resultado obtido na Proposição 3.33 é suficiente. Além disso, com ele demonstramos todos os itens anteriores.

Demonstração.

(i) Observe que $m \mid 0 \implies m \mid (a - a)$ e, portanto, $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, então temos que $m \mid (a - b)$. Assim, $a - b = mq$ para algum número inteiro q. Multiplicando por -1 a igualdade, obtemos $b - a = m(-q)$, que significa que $m \mid (b - a)$. Portanto, $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $m \mid (b - a)$ e $m \mid (c - b)$. Agora, pelo item 7 da proposição 3.10, temos que $m \mid [(b - a) + (c - b)]$, ou seja, $m \mid (c - a)$. Logo, $a \equiv c \mod m$.

Proposição 3.35. Sejam $a, b, c, d \in \mathbb{Z}$, com $m > 1$.

(i) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.

(ii) Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $ac \equiv bd \mod m$.

Demonstração. Supondo que $a \equiv b \mod m$ e $c \equiv d \mod m$. Temos que $m \mid (b - a)$ e $m \mid (d - c)$.

(i) $m \mid (b - a) + (d - c)$, portanto, $m \mid (b + d) - (a + c)$.

(ii) Observe que $bd - ac = d(b - a) + a(d - c)$, logo $m \mid (bd - ac)$.

Corolário 3.36. Para todos $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \mod m$, então tem-se que $a^n \equiv b^n \mod m$.

Demonstração. Vamos analisar por meio da indução matemática:

Consideremos $p(n)$: $a \equiv b \mod m \implies a^n \equiv b^n \mod m$.

Para $n = 0$, temos $a^0 - b^0 = 1 - 1 = 0 = 0m \implies m \mid (a^0 - b^0) \implies a^0 \equiv b^0 \mod m$. Então, $p(n)$ é válida para $n = 0$.

Agora, suponhamos que $p(n)$ vale para algum $n \in \mathbb{N}$, assim sendo,
Hipótese de indução: $a \equiv b \mod m \implies a^n \equiv b^n \mod m$.
Vamos mostrar que $p(n+1)$ também vale,
Tese: $a \equiv b \mod m \implies a^{n+1} \equiv b^{n+1} \mod m$.
Como $a \equiv b \mod m$ e, por hipótese de indução, $a^n \equiv b^n \mod m$, pela Proposição 3.35, temos que $aa^n \equiv bb^n \mod m \implies a^{n+1} \equiv b^{n+1} \mod m$, como queríamos demonstrar.
Portanto, a sentença $p(n)$ é válida para todo $n \in \mathbb{N}$.

Proposição 3.37. Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que

$$a + c \equiv b + c \mod m \iff a \equiv b \mod m.$$

Demonstração. ($\Rightarrow$) Se $a + c \equiv b + c \mod m$, então $m \mid (b + c - (a + c))$, o que implica que $m \mid (b - a)$ e, por consequência, $a \equiv b \mod m$.
($\Leftarrow$) Se $a \equiv b \mod m$, pela Proposição 3.35, temos que $a + c \equiv b + c \mod m$, pois $c \equiv c \mod m$.

A última proposição traz como consequência o cancelamento de parcelas em relação à adição nas congruências. Porém, isso não vale, de modo geral, para a multiplicação, como se pode ver a seguir.

Exemplo 3.38. Como $4 \cdot 7 - 4 \cdot 3 = 16$ e $8 \mid 16$, temos que $4 \cdot 7 \equiv 4 \cdot 3 \mod 8$, e, por outro lado, $7 \not\equiv 3 \mod 8$.

Proposição 3.39. Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Temos que

$$ac \equiv bc \mod m \iff a \equiv b \mod \frac{m}{\text{mdc}(c, m)}.$$

Demonstração. Sabemos que $\frac{m}{\text{mdc}(c,m)}$ e $\frac{c}{\text{mdc}(c,m)}$ não possuem fator em comum, ou seja, são coprimos, e com isso temos:

$$ac \equiv bc \mod m \iff m \mid (b - a)c$$
$$\iff \frac{m}{\text{mdc}(c, m)} \mid \frac{(b - a)c}{\text{mdc}(c, m)} \iff \frac{m}{\text{mdc}(c, m)} \mid (b - a) \iff a \equiv b \mod \frac{m}{\text{mdc}(c, m)}.$$

Exemplo 3.40. Já vimos pelo Exemplo 3.38 que $4 \cdot 7 \equiv 4 \cdot 3 \mod 8$, aplicando a proposição 3.39, temos $7 \equiv 3 \mod \frac{8}{\text{mdc}(4,8)}$. Ou seja $7 \equiv 3 \mod 2$.

3.5.2 Uma aplicação de Congruência

Como aplicação prática do conceito de congruência, podemos utilizar o algoritmo de Zeller, uma fórmula desenvolvida pelo reverendo Julius Christian Johannes Zeller (1822 - 1899), utilizada para definir o dia da semana de determinada data. Este algoritmo é válido a partir do ano 1601 e, devido à irregularidade do mês de fevereiro, adotaremos a convenção de considerá-lo como o último mês do ano. Dessa forma, março será considerado como o primeiro mês (mês 1), abril como o segundo mês (mês 2), e assim sucessivamente, até chegar aos meses 11 e 12, que correspondem a janeiro e fevereiro do ano seguinte. Portanto, janeiro e fevereiro de um determinado ano serão tratados como os meses 11 e 12 do ano anterior. Como notação para o dia da semana de determinada data utilizaremos s(d,m,A), sendo d o dia do mês, m o número do mês como foi definido anteriormente começando por março até fevereiro e A o ano. Por exemplo a data 10 de janeiro de 1958, consideraremos o dia 10, o mês 11 e o ano 1957 para os cálculos, logo utilizaremos a notação s(10,11,1957), já para o dia 31 de agosto de 1963, temos s(31,6,1963). Essa reorganização dos meses facilita o uso do algoritmo de Zeller e melhora a consistência dos cálculos ao lidar com a variação no número de dias de fevereiro.

O dia da semana será determinado a partir da congruência módulo 7, onde os dias são definidos da seguinte maneira: sábado é congruente a 0, domingo é congruente a 1, e assim sucessivamente até sexta-feira, que é congruente a 6.

Teorema 3.41 - Zeller.

$$s(d,m,A) = d + 1 + \left[\frac{13m-1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

Exemplo 3.42. Encontremos qual foi o dia da semana em 6 de setembro de 2000
Temos:

$$\begin{aligned} d &= 6 \\ m &= 7 \\ A &= 2000 \end{aligned}$$

Substituindo:

$$\begin{aligned} s(6,7,2000) &= 6 + 1 + \left[\frac{13\cdot 7-1}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7 \\ s(6,7,2000) &= 6 + 1 + \left[\frac{91-1}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7 \\ s(6,7,2000) &= 6 + 1 + \left[\frac{90}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7 \\ s(6,7,2000) &= 6 + 1 + 18 + 2000 + 500 - 20 + 5 \mod 7 \\ s(6,7,2000) &= 2510 \mod 7 \\ 2510 &\equiv 4 \mod 7 \end{aligned}$$

Logo, $s(6,7,2000)$ representa uma quarta-feira.

4 Proposta de inclusão da unidade temática Aritmética na BNCC

Neste capítulo, apresentaremos uma proposta de como a Aritmética poderia ser inserida na Base Nacional Comum Curricular (BNCC) como unidade temática nos anos finais do Ensino Fundamental. A ideia central dessa proposta é que a Aritmética, como um dos principais campos da Matemática, tenha maior reconhecimento por parte dos alunos e professores da Educação Básica, além da própria BNCC, assim como já é visto nos outros campos, como Álgebra, Geometria, Estatística e Probabilidade.

A introdução da Aritmética como unidade temática visa proporcionar aos alunos uma compreensão mais profunda dos conceitos fundamentais que sustentam grande parte da Matemática. A aritmética, com seu foco em operações básicas, divisibilidade, números primos e teoria dos números, oferece uma base sólida que é essencial para o desenvolvimento do raciocínio lógico e do pensamento crítico. Ao reconhecer a importância da Aritmética, espera-se que os alunos se sintam mais motivados a explorar e entender outros campos da Matemática.

Primeiramente, nenhuma unidade temática existente deve ser excluída e a única a sofrer alguma alteração nesta proposta seria a intitulada Números. Neste caso, sugerimos transferir os objetos de conhecimento e habilidades citados nos quadros 1 e 2 da seção 2.3 deste trabalho para a nova unidade temática de Aritmética. Contudo, como foi observado anteriormente, dessa maneira apenas os sexto e sétimo anos seriam contemplados com a nova unidade temática. Por isso, é necessário que outros conceitos de Aritmética sejam introduzidos para alcançar também os dois últimos anos finais do Ensino Fundamental.

Um exemplo de conceito que poderia ser introduzido é a aritmética modular ou aritmética dos restos. Este campo, além de ser uma ferramenta importante na matemática avançada, também tem aplicações práticas, como na criptografia. A criptografia é um tópico relevante e atual, que pode despertar o interesse dos alunos ao mostrar como a matemática é utilizada para proteger informações na internet, nos cartões de crédito e em muitas outras áreas do cotidiano. A introdução da aritmética dos restos pode ser feita de maneira lúdica e contextualizada, utilizando problemas e exemplos que mostrem sua aplicação prática.

Para os conceitos que desejamos incluir na BNCC, serão apresentados planos de aula no próximo capítulo para servirem de base e sugestão. A proposta será constituída em duas partes: uma introdução sobre o que deve ser trabalhado e a importância da nova unidade temática, seguida por um quadro de como ficariam divididos os objetos de conhecimento e habilidades. As habilidades já existentes não sofrerão alteração no seu código alfanumérico, e as habilidades acrescentadas seguirão a numeração de acordo com a última já existente com seu respectivo ano na BNCC. Por exemplo, a última habilidade listada para o oitavo ano tem como código EF08MA27, continuaremos com a EF08MA28 e assim por diante.

Este trabalho se concentrará apenas nos conteúdos destinados aos anos finais do Ensino Fundamental. No entanto, a proposta apresentada pode servir como uma base sólida para a construção de outras habilidades de Aritmética para o Ensino Médio. Ao estabelecer um fundamento robusto no Ensino Fundamental, os alunos estarão melhor preparados para aprofundar seus estudos na Aritmética e explorar suas aplicações mais complexas, como a criptografia, em níveis mais avançados de ensino. A continuidade e o aprofundamento desses

estudos no Ensino Médio poderiam promover uma compreensão mais abrangente e integrada da Matemática, beneficiando o desenvolvimento acadêmico dos alunos e preparando-os para futuros desafios educacionais e profissionais.

Em resumo, a proposta de incluir a Aritmética como unidade temática nos anos finais do Ensino Fundamental visa dar maior reconhecimento a este importante campo da Matemática, proporcionando uma base sólida para os alunos e preparando-os para conceitos mais avançados e aplicações práticas, como a criptografia. Esta abordagem não só enriquece o currículo, mas também torna a aprendizagem mais relevante e interessante para os alunos, promovendo um maior engajamento e compreensão da Matemática como um todo.

4.1 Unidade Temática Aritmética

A unidade temática Aritmética tem como finalidade desenvolver a compreensão dos números inteiros e das operações básicas entre eles, que são fundamentais para a construção de habilidades matemáticas mais complexas. Nesse processo, os alunos precisam explorar a relação das operações aritméticas (adição, subtração, multiplicação e divisão), além de compreender as propriedades dos números primos. É crucial que os estudantes sejam incentivados a usar a aritmética em situações práticas e cotidianas, para que possam apreciar sua relevância e aplicabilidade, com destaque para o máximo divisor comum e o mínimo múltiplo comum.

Além disso, devem ser promovidas atividades que estimulem a estimativa, o cálculo mental e a resolução de problemas, facilitando uma compreensão profunda e intuitiva dos conceitos aritméticos. As ideias matemáticas fundamentais associadas a essa unidade incluem a estruturação do pensamento lógico, a análise crítica e a capacidade de argumentação baseada em quantidades e operações. A abordagem integrada desses conceitos é essencial para preparar os alunos para desafios mais avançados na Matemática e em outras disciplinas.

Outro aspecto importante da Aritmética que deve ser abordado é a aritmética dos restos, ou aritmética modular. Esse ramo da Matemática, que envolve a divisão de inteiros e a observação dos restos, possui aplicações práticas significativas, incluindo na área da criptografia. A aritmética modular não apenas enriquece o entendimento dos alunos sobre divisibilidade e congruências, mas também fornece uma ponte para a exploração de tópicos mais complexos e interessantes.

A introdução à criptografia, por meio da aritmética dos restos, pode ser uma maneira fascinante de mostrar aos alunos como a Matemática é aplicada na proteção de informações em nosso mundo digital. A criptografia utiliza princípios matemáticos para garantir a segurança de dados em transações bancárias, comunicações eletrônicas e muitas outras áreas. Ensinar os fundamentos da criptografia pode despertar o interesse dos alunos e demonstrar a importância da Matemática em contextos reais e modernos.

Para alcançar esses objetivos, é essencial que as atividades propostas sejam desafiadoras e ao mesmo tempo acessíveis, incentivando os alunos a pensar criticamente e a aplicar suas habilidades de forma criativa. A inclusão de projetos e problemas práticos que envolvam a aritmética modular e a criptografia podem tornar o aprendizado mais dinâmico e envolvente,

promovendo uma maior compreensão e apreciação das aplicações da Aritmética.

Em suma, a unidade temática Aritmética deve proporcionar aos alunos uma base sólida nos conceitos fundamentais dos números inteiros e das operações básicas, além de introduzi-los à aritmética dos restos e à criptografia. Essa abordagem abrangente e prática não só enriquece o currículo, mas também prepara os alunos para os desafios futuros, desenvolvendo habilidades essenciais de pensamento lógico, análise crítica e resolução de problemas. Ao integrar essas áreas, os alunos terão uma experiência de aprendizado mais completa e significativa, que os motivará a continuar explorando e aplicando a Matemática em diversas situações

Quadro 3 – Objetos de conhecimento e habilidades da unidade temática Aritmética

Ano	**Objetos de conhecimento**	**Habilidades**
6°	Operações (adição, subtração, multiplicação, divisão e potenciação) com números naturais Divisão euclidiana Fluxograma para determinar a paridade de um número natural Múltiplos e divisores de um número natural Números primos e compostos	(EF06MA03) Resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora. (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). (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.

7°	Múltiplos e divisores de um número natural Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações	(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. (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. (EF07MA04) Resolver e elaborar problemas que envolvam operações com números inteiros.
8°	Congruência modular Operações com os restos da divisão euclidiana: adição, multiplicação e potenciação	(EF08MA28) Compreender a ideia de igualdade nos restos da divisão euclidiana de dois números inteiros distintos por um mesmo número (módulo) e utilizar a representação de congruência. (EF08MA29) Verificar e classificar dois números como congruentes, ou não congruentes, módulo m. (EF08MA30) Resolver e elaborar problemas que envolvam congruência modular, utilizando as propriedades das operações de adição, multiplicação e potenciação.
9°	Algoritmo de Zeller: verificações experimentais Noções de criptografia: o código de César	(EF09MA24) Determinar o dia da semana de uma data passada ou futura utilizando o Algoritmo de Zeller. (EF09MA25) Compreender a importância da criptografia e, conhecer e utilizar um dos métodos mais famosos utilizado na antiguidade conhecido como código de César.

Fonte: autor (2024)

5 Sugestão de sequências didáticas para o ensino de Aritmética para alunos do 8° e 9°anos do Ensino Fundamental

Como no capítulo anterior foi feita uma proposta para a inserção da Aritmética como unidade temática na BNCC, e para isso seriam acrescentadas novas habilidades para serem trabalhadas com o aluno do Ensino Fundamental, neste capítulo vamos trazer uma proposta de sequências didáticas para servir de orientação ou exemplo para um professor que precisaria desenvolver essas novas habilidades com seus alunos nos anos finais do Ensino Fundamental.

5.1 1° Sequência Didática

Público: Alunos do 8° ano do Ensino Fundamental.

Habilidades:

- (EF08MA28) Compreender a ideia de igualdade nos restos da divisão euclidiana de dois números inteiros distintos por um mesmo número (módulo) e utilizar a representação de congruência.
- (EF08MA29) Verificar e classificar dois números como congruentes, ou não congruentes, módulo m.

Objetivos:

- Entender o conceito de congruência em aritmética.
- Aplicar a congruência para resolver problemas matemáticos.
- Desenvolver habilidades de raciocínio lógico e resolução de problemas.
- Verificar e classificar números como congruentes, ou não congruentes, módulo m.

Recursos didáticos: Quadro, giz, folhas de exercícios impressas, cartolina.

Tempo previsto: Três horas aulas.

Desenvolvimento:

1ª Hora Aula: Retomada à Divisão Euclidiana e ao Conceito de Resto

1. **Sugestão para o professor(a):** Retome a divisão euclidiana, explicando a forma geral $a = bq + r$, onde a e b são números inteiros, q é o quociente e r é o resto.

2. **Exemplos:** Resolva exemplos de divisões euclidianas no quadro, destacando os restos. Mostre aos alunos que todos os números que deixam resto zero estão na tabuada do divisor, e questione se números que deixam o mesmo resto não podem ser encaixados em um mesmo grupo.

   Neste momento pode-se usar tabelas que tenham como número de colunas o divisor em questão. Desta maneira todos os números que possuem o mesmo resto quando divididos por este divisor ficaram na mesma coluna.

   Por exemplo uma tabela para o divisor 7:

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

   Todos os números da primeira coluna são múltiplos de 7, todos da segunda deixam resto 1 ao serem divididos por 7, na terceira deixam resto 2 e assim por diante até a última coluna em que temos os números que deixam resto 6.

3. **Atividade Prática:** Os alunos realizam divisões euclidianas, anotando os restos, como por exemplo:

   - $23 \div 5$
   - $18 \div 5$
   - $53 \div 5$
   - $41 \div 6$
   - $47 \div 6$
   - $11 \div 6$
   - $34 \div 7$
   - $20 \div 7$

- $97 \div 7$

Nesta atividade é recomendado que haja uma separação na lousa entre as divisões com o mesmo divisor, para facilitar a implementação da ideia de módulo.

Também utilize exercícios mais elaborados, como:

- Encontre o número natural que ao ser dividido por 7 resulta um quociente 4 e resto o maior possível.
- Encontre os números naturais que, quando divididos por 8 deixam o resto igual ao dobro do quociente.

Além disso, pode-se dividir a sala em grupos e pedir a construção de tabelas como a que foi utilizada no exemplo.

Sugestão: Divida a sala em grupos de 3 alunos. De acordo com o número de grupos formados, designe um divisor n para cada um dos grupos, oriente a montarem uma tabela em cartolina com 8 linhas e n colunas, preenchendo-a com números inteiros em ordem crescente e começando pelo 0.

4. **Discussão:** Discuta as respostas com a turma, garantindo que todos retomaram o conceito de resto na divisão euclidiana. Aqui também é importante que tenha ficado claro para o aluno que os restos podem repetir quando dividimos diferentes números por um mesmo divisor, além de que o resto de uma divisão é sempre menor que o divisor.

   Deixe os trabalhos com cartolina expostos em sala de aula, as tabelas são um ótimo recurso visual para compreender a ideia de congruência modular.

2ª Hora Aula: Introdução à Congruência Módulo m

1. **Sugestão para o professor(a):** Introduza o conceito de congruência, explicando que dois números a e b são congruentes módulo m se tiverem o mesmo resto quando divididos por m. Escreva a notação: $a \equiv b \mod m$. Chame a atenção do aluno para o símbolo usado em congruência, reforce para que não seja confundido com o símbolo de igualdade.

2. **Exemplos:** Mostre exemplos no quadro, como $23 \equiv 2 \mod 3$ e $45 \equiv 3 \mod 6$. Os exercícios deixados na aula anterior são ótimos para serem usados como exemplos agora e, principalmente, as tabelas que foram construídas pelos alunos.

   Escolha uma das tabelas, como por exemplo a do divisor 8, que deve ter ficado assim:

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

Neste momento, retome o conceito que estava sendo construído na primeira aula, observe com os estudantes a disposição dos números na tabela de acordo com o resto que deixam ao serem divididos por 8, mostre que todos os números que se encontram na mesma coluna possuem o mesmo módulo 8.

Agora levante questionamentos sobre números que não estão presentes na tabela.

"Se prolongarmos a tabela em qual coluna estaria o número 80? e o 92? e o 175?"

Escolha uma outra tabela e repita o processo.

3. **Atividade Prática:** Retome as divisões euclidianas, procure utilizar diferentes divisores como por exemplo:

   - $26 \div 4$
   - $18 \div 7$
   - $53 \div 6$
   - $41 \div 5$
   - $47 \div 9$
   - $11 \div 3$
   - $34 \div 2$
   - $25 \div 8$

   Depois, instrua os alunos a utilizarem os restos encontrados nas divisões anteriores para completarem as congruências, como por exemplo:

   - $26 \equiv \mod 4$
   - $18 \equiv \mod 7$
   - $53 \equiv \mod 6$
   - $41 \equiv \mod 5$
   - $47 \equiv \mod 9$
   - $11 \equiv \mod 3$

- $34 \equiv \mod 2$
- $25 \equiv \mod 8$

Algumas questões contextualizadas:

- Uma empresa de coleta de material reciclável dividiu o município de Bauru em 46 áreas para realizar pontualmente a coleta nas residências. Foi feito um cronograma para a coleta de acordo com o quadro abaixo:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	...	...	...	...

  Em qual dia da semana a coleta será feita na área número 20? E na área número 32? E na número 46?

- (FUVEST) Os números inteiros positivos são dispostos em "quadrados" da seguinte maneira:

1	2	3	10	11	12	19	...	...
4	5	6	13	14	15	...	...	...
7	8	9	16	17	18	...	...	...

  O número 500 se encontra em um desses "quadrados". Determine em qual "quadrado" está, linha e coluna.

4. **Discussão:** Revisem as respostas em conjunto retirando as dúvidas que ficaram. Caso perceba que não ficou claro para o aluno retome os exemplos, utilize o mesmo módulo algumas vezes, mostre novamente que os restos são limitados.

   O principal neste momento é a compreensão de que números que deixam o mesmo resto ao serem divididos por um mesmo divisor podem ser encaixados em um "subgrupo". Se for necessário, retorne as colunas das tabelas construídas.

3ª Hora Aula: Verificação da Congruência Módulo m

1. **Sugestão para o professor(a):** Reforce o conceito de congruência, relembrando que dois números a e b são congruentes módulo m se tiverem o mesmo resto quando divididos por m. Agora mostre como fazer essa verificação sem precisar dividir os dois números pelo módulo, realizando a divisão de $a - b$ por m, temos que eles serão congruentes quando essa divisão for exata, e não serão quando ela não for, pois $a - b$ é divisível por m se, e somente se, $a \equiv b \mod m$. (A demonstração desse resultado se encontra

nesse trabalho na demonstração da proposição 3.33, a primeira parte é de certa forma simples e pode ser apresentada em sala de aula)

2. **Exemplos:** Mostre exemplos numéricos no quadro verificando se as congruências existem ou não, como "verifique se 36 é congruente a 22 módulo 7"e "verifique se 46 é congruente a 32 módulo 4".

   Recomenda-se também, depois de realizar os exemplos para verificação, mostrar os mesmos exemplos numéricos na demonstração feita anteriormente.

   Por exemplo:

   $$36 - 22 = 7 \cdot 5 + 1 - (7 \cdot 3 + 1) = 7(5 - 3) + (1 - 1) = 7 \cdot 2.$$

   (múltiplo de 7)

   $$46 - 32 = 4 \cdot 11 + 2 - (4 \cdot 8 + 0) = 4(11 - 8) + (2 - 0) = 4 \cdot 3 + 2.$$

   (não é múltiplo de 4)

3. **Atividade Prática:** Utilize exercícios parecidos com os exemplos, peça a verificação da congruência entre dois números, instrua o aluno a fazer a conferência na demonstração (caso tenha sido apresentada).

   - Verifique se há congruência entre os números:
     - 83 e 67 módulo 4
     - 30 e 18 módulo 3
     - 178 e 73 módulo 7
     - 1045 e 386 módulo 9
     - 94 e 34 módulo 5
     - 367 e 147 módulo 11
     - 763 e 481 módulo 6
     - 921 e 382 módulo 3

   - Os números 32 e 17 são congruentes em quais módulos? (considere apenas inteiros positivos)

   - Em qual módulo positivo os números 143 e 113 são congruentes?

4. **Discussão:** Revisem as respostas em conjunto retirando as dúvidas que ficaram. Incentive os alunos a refletirem sobre a operação efetuada e a perceberem como os restos se cancelam na operação de subtração, comece uma introdução para a próxima habilidade a ser trabalhada (as operações de adição e multiplicação com os restos).

5.2 2ª Sequência Didática

Público: Alunos do 8° ano do Ensino Fundamental.

Habilidade:

- (EF08MA30) Resolver e elaborar problemas que envolvam congruência modular, utilizando as propriedades das operações de adição, multiplicação e potenciação.

Objetivos:

- Entender as propriedades das operações de adição, multiplicação e potenciação no contexto da congruência modular.
- Aplicar essas propriedades para resolver problemas.
- Desenvolver habilidades de raciocínio lógico e resolução de problemas.

Recursos didáticos: Quadro, giz, folhas de exercícios impressas, caderno de exercícios do portal da OBMEP.

Tempo previsto: Três horas aulas.

Desenvolvimento:

1ª Hora Aula: Propriedades da Adição, Multiplicação e potenciação em Congruências

1. **Sugestão para o professor(a):**
   - Relembre rapidamente o conceito de congruência módulo m.
   - Explique as propriedades da adição, multiplicação e potenciação em congruências. Diga que, se $a \equiv b \mod m$ e $c \equiv d \mod m$, então:
     * $a + c \equiv b + d \mod m$
     * $ac \equiv bd \mod m$

$*$ $a^n \equiv b^n \mod m$

2. **Exemplos:**

   - Mostre exemplos numéricos no quadro para ilustrar essas propriedades:
     $*$ $23 \equiv 2 \mod 7$ e $16 \equiv 2 \mod 7$, então $23 + 16 \equiv 2 + 2 \equiv 4 \mod 7$
     $*$ $6 \equiv 2 \mod 4$ e $14 \equiv 2 \mod 4$, então $6 \cdot 14 \equiv 2 \cdot 2 \equiv 4 \mod 4$
     $*$ $7 \equiv 1 \mod 3$, então $7^6 \equiv 1^6 \mod 3$. Logo $7^6 \div 3$ vai deixar resto 1

   Neste momento é importante que o professor mostre para o aluno que ele pode testar numericamente a congruência de um número elevado a determinado expoente e verificar como o resto da divisão por um mesmo módulo se comporta. Também é preciso mostrar para o aluno que ao encontrar uma potência congruente a 1 módulo m obtemos uma grande "vantagem matemática", pois podemos elevar essa potência a qualquer expoente e ela ainda será congruente a 1 módulo m.

   Para uma exemplificação visual utilize novamente as tabelas construídas nas aulas anteriores, vamos utilizar por exemplo a tabela do divisor 5. (Lembre que os números da primeira coluna são múltiplos de 5, os da segunda são congruentes a 1 módulo 5, os da terceira coluna congruentes a 2 módulo 5 e assim por diante.)

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

   Questione em qual coluna se encontra o resultado da soma $10+25$ que são dois números que estão na primeira coluna e portanto são múltiplos de 5, ou ao somar $7+12$ que são números que são congruentes a 2 módulo 5 na coluna de qual congruência o resultado vai estar. Faça os mesmos questionamentos para os produtos entre números de diferentes colunas, observando sempre aonde se encontra o resultado.

3. **Atividade Prática:** Alguns exercícios para trabalhar as operações com módulos:

   - (Colégio Militar de Fortaleza - Adaptada) Dois números inteiros positivos são tais que a divisão do primeiro por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será?

- Sejam a e b dois números inteiros positivos cujos restos da divisão por 5 são respectivamente 3 e 2. Determine:
  - O resto da divisão de $a + b$ por 5.
  - O resto da divisão de ab por 5.
  - O resto da divisão de a^4 por 5.
  - O resto da divisão de b^6 por 5.
  - O resto da divisão de $a^4 + b^6$ por 5.
- (FUVEST - Adaptada) Sabendo que os anos bissextos são múltiplos de 4 e que o primeiro dia de 2024 foi segunda-feira, o próximo ano a começar também em uma segunda feira será? (Lembre-se $365 \equiv 1 \mod 7$ e $366 \equiv 2 \mod 7$)
- Nas divisões de 123656 e 456789 por 6 obtemos, respectivamente, restos 2 e 3. Qual o resto da divisão de $123656 \cdot 456789$ por 6?
- Sejam a e b dois números inteiros positivos cujos restos da divisão por 8 são respectivamente 3 e 2. Determine:
  - O resto da divisão de $4a$ por 8.
  - O resto da divisão de $4b$ por 8.
  - O resto da divisão de a^{20} por 8.
  - O resto da divisão de b^{20} por 8.
  - O resto da divisão de $(ab)^3$ por 8.

4. **Discussão:**

- Revisem as respostas juntos, garantindo que todos entenderam como aplicar as propriedades das operações com congruências.
- Reforce a importância de verificar os restos antes de aplicar as operações.

2ª e 3ª Horas Aulas: Problemas Envolvendo Congruência Modular

1. **Sugestão para o professor(a):**

- Explique como resolver problemas práticos usando congruência modular e as propriedades aprendidas.
- Diga que esses conceitos são úteis em diversas áreas, como criptografia e computação. (Pode citar também o CPF e o código de barras como aplicações da Aritmética Modular)

2. **Exemplos e Atividade Prática:**

- Recomenda-se que o docente acesse o portal disponível no seguinte endereço eletrônico:

  https://portaldaobmep.impa.br/index.php/modulo/ver?modulo=63. Ao entrar na página, deve-se localizar e acessar a aba intitulada "Caderno de Exercícios", situada na parte inferior esquerda da tela. Nesse local, o professor encontrará e poderá fazer o download das apostilas de exercícios intituladas "Aritmética dos Restos"e "Aritmética Modular".

  Essas duas apostilas, somadas, contêm um total de 52 exercícios, classificados em categorias de introdutórios, de fixação e de aprofundamento, todos acompanhados de suas respectivas resoluções. Cabe ao professor a tarefa de selecionar alguns desses exercícios para serem utilizados como exemplos durante a explicação dos conteúdos, bem como outros exercícios para serem empregados em atividades práticas. Considerando que a aula é destinada aos alunos do 8° ano do Ensino Fundamental, é aconselhável evitar a utilização de exercícios que envolvam provas e demonstrações formais.

  Para a realização da atividade prática, sugere-se dividir a turma em duplas, promovendo a resolução de exercícios objetivos. Esta abordagem colaborativa visa fomentar o aprendizado ativo e a consolidação dos conceitos matemáticos apresentados.

3. **Discussão:**

   - Revisem atentamente as soluções dos problemas, assegurando-se de que os alunos compreendem cada etapa do processo de resolução. É fundamental reforçar a ideia de que a aritmética modular pode ser uma ferramenta eficaz para a solução de exercícios que envolvem números muito grandes. Além disso, destacar a importância de considerar o resto em uma divisão euclidiana como uma estratégia viável para resolver esse tipo de exercício é igualmente crucial. Essa abordagem não só facilita a compreensão dos conceitos matemáticos, mas também demonstra a aplicabilidade prática da aritmética modular em situações complexas.

5.3 3ª Sequência Didática

Público: Alunos do 9° ano do Ensino Fundamental.

Habilidade:

- (EF09MA24) Determinar o dia da semana de uma data passada ou futura utilizando o Algoritmo de Zeller.

Objetivos:

- Compreender o Algoritmo de Zeller.
- Aplicar o Algoritmo de Zeller para determinar o dia da semana de uma data específica.
- Desenvolver habilidades de raciocínio lógico e resolução de problemas.

Recursos didáticos: Quadro, giz, folhas de exercícios impressas.

Tempo previsto: Duas horas aulas.

Desenvolvimento:

1ª e 2ª Horas Aulas: Algoritmo de Zeller e sua aplicação

1. **Sugestão para o professor(a):**
   - Introduza o Algoritmo de Zeller, explicando que ele é usado para calcular o dia da semana de uma data específica. (Utilize a subseção 3.5.2 deste trabalho.)
   - Caso julgue necessário, faça uma revisão do conteúdo de Congruência Modular que foi trabalhado no 8° ano.
   - Apresente a fórmula do Algoritmo de Zeller para o calendário gregoriano:

$$s(d, m, A) = d + 1 + \left[\frac{13m - 1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7.$$

     Onde:
     - s é o dia da semana (0 = sábado, 1 = domingo, 2 = segunda-feira, ..., 6 = sexta-feira)
     - d é o dia do mês
     - m é o mês (1 = março, 2 = abril, ..., 12 = fevereiro; janeiro e fevereiro são tratados como meses 11 e 12 do ano anterior)
     - A é o ano (Reforce que a fórmula só é válida para anos posteriores a 1600)

2. **Exemplos:** Calcule alguns exemplos no quadro para ilustrar a aplicação do algoritmo. Por exemplo:
   - Vamos calcular em que dia da semana caiu a data 31 de agosto de 1963.

Temos:

$$\begin{aligned} d &= 31 \\ m &= 6 \\ A &= 1963 \end{aligned}$$

Substituindo:

$$s(31,6,1963) = 31 + 1 + \left[\frac{13 \cdot 6 - 1}{5}\right] + 1963 + \left[\frac{1963}{4}\right] - \left[\frac{1963}{100}\right] + \left[\frac{1963}{400}\right] \mod 7$$
$$s(31,6,1963) = 31 + 1 + \left[\frac{78 - 1}{5}\right] + 1963 + \left[\frac{1963}{4}\right] - \left[\frac{1963}{100}\right] + \left[\frac{1963}{400}\right] \mod 7$$
$$s(31,6,1963) = 31 + 1 + \left[\frac{77}{5}\right] + 1963 + \left[\frac{1963}{4}\right] - \left[\frac{1963}{100}\right] + \left[\frac{1963}{400}\right] \mod 7$$
$$s(31,6,1963) = 31 + 1 + 15 + 1963 + 490 - 19 + 4 \mod 7$$
$$s(31,6,1963) = 2485 \mod 7$$
$$2485 \equiv 0 \mod 7$$

Logo, $s(31,6,1963)$ representa um sábado.

- O primeiro dia deste século foi em qual dia da semana?
  Primeiro dia do século foi 1 de janeiro de 2001.
  Temos:

$$\begin{aligned} d &= 1 \\ m &= 11 \\ A &= 2000 \end{aligned}$$

Substituindo:

$$s(1,11,2000) = 1 + 1 + \left[\frac{13 \cdot 11 - 1}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7$$
$$s(1,11,2000) = 1 + 1 + \left[\frac{143 - 1}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7$$
$$s(1,11,2000) = 1 + 1 + \left[\frac{142}{5}\right] + 2000 + \left[\frac{2000}{4}\right] - \left[\frac{2000}{100}\right] + \left[\frac{2000}{400}\right] \mod 7$$
$$s(1,11,2000) = 1 + 1 + 28 + 2000 + 500 - 20 + 5 \mod 7$$
$$s(1,11,2000) = 2515 \mod 7$$
$$2515 \equiv 2 \mod 7$$

Logo, $s(1,11,2000)$ representa uma segunda-feira.

3. **Atividade Prática:** Alguns exercícios para que os alunos trabalhem com o Algoritmo de Zeller:

   - Utilizando o Algoritmo de Zeller, calcule em que dia da semana ocorreram, ou ocorrerão, as seguintes datas:
     - 15 de janeiro de 1932
     - 22 de fevereiro de 2050
     - 5 de maio de 1995
     - 20 de dezembro de 1989
     - 31 de dezembro de 2100
   - Em que dia da semana você nasceu?
   - Em que dia da semana ocorreu a Proclamação da República do Brasil (15 de novembro de 1889)?
   - No dia 7 de setembro de 2072 o Brasil comemorará 250 anos de sua independência. Em que dia da semana cairá essa data? E em que dia da semana foi declarada a independência?
   - O matemático alemão Carl Friedrich Gauss nasceu no dia 30 de abril de 1777 e morreu no dia 23 de fevereiro de 1855, devido a suas grandes contribuições ele ficou conhecido como o "Príncipe da Matemática". Determine em que dia da semana ocorreu o seu nascimento e o seu falecimento.

4. **Discussão:**

   - Revise as soluções dos problemas em conjunto, garantindo que os alunos compreenderam cada passo da aplicação do algoritmo.
   - Destaque a utilização da Congruência Modular nos exercícios.
   - Conclua a aula dissertando sobre a importância da matemática na resolução de problemas do dia a dia e na compreensão de eventos históricos.

5.4 4ª Sequência Didática

Público: Alunos do 9° ano do Ensino Fundamental.

Habilidade:

- (EF09MA25) Compreender a importância da criptografia e, conhecer e utilizar um dos métodos mais famosos utilizado na antiguidade conhecido como código de César.

Objetivos:

- Entender a importância da criptografia na proteção de informações.
- Compreender o funcionamento do código de César.
- Aplicar o código de César para codificar e decodificar mensagens.

Recursos didáticos: Quadro, giz, folhas de exercícios impressas, cartolina e outros recursos para confecção de trabalhos, computadores ou outro aparelho que promova o acesso a internet.

Tempo previsto: Três horas aulas.

Desenvolvimento:

1ª Hora Aula: Apresentação de trabalhos sobre a Criptografia

1. **Trabalho em grupo:** Previamente a esta aula (recomenda-se ao menos 4 semanas) organize a turma em grupos de 4 a 6 alunos de maneira que se tenha pelo menos 5 grupos, para cada grupo defina um tema, caso seja necessário repita o tema, mas não deixe nenhum deles de fora, utilize os temas a seguir:

   - Cítala
   - Código de César
   - Cifra de Vigenère
   - Cifra de substituição
   - Enigma (máquina)

   Cada grupo deve apresentar um trabalho final, em forma de cartaz, e fazer a apresentação do seu tema para o restante da turma com informações sobre a história, o período em que foi utilizado, a segurança do método, como ele funciona e respondendo ao seguinte questionamento que será comum a todos os grupos "Atualmente, qual a importância da criptografia?".

   Defina o tempo de apresentação de acordo com a quantidade de grupos e a duração da aula disponível.

2. **Discussão:**

   - Após as apresentações, promova uma discussão sobre os métodos que foram utilizados, sobre as adaptações que ocorreram ao longo da história e a importância da criptografia nos dias atuais, especialmente em transações bancárias e comunicações online. Além disso, comente sobre a utilização de números primos e congruência modular em sistemas de criptografia modernos.

2ª Hora Aula: O Código de César

1. **Sugestão para o professor(a):**

   - Retome o código de César, explicando que é um dos métodos de criptografia mais antigos, utilizado por Júlio César.
   - Explique o funcionamento do código de César: cada letra da mensagem original é deslocada um número fixo de posições no alfabeto.

2. **Exemplos:** Faça alguns exemplos de codificação e decodificação utilizando o código de César com diferentes deslocamentos. Por exemplo:

   - Codifique a palavra MATEMATICA com um deslocamento de 3:
     - Mensagem original: **MATEMATICA**
     - Passo a passo do deslocamento:
       - M $\xrightarrow{3}$ P
       - A $\xrightarrow{3}$ D
       - T $\xrightarrow{3}$ W
       - E $\xrightarrow{3}$ H
       - M $\xrightarrow{3}$ P
       - A $\xrightarrow{3}$ D
       - T $\xrightarrow{3}$ W
       - I $\xrightarrow{3}$ L
       - C $\xrightarrow{3}$ F
       - A $\xrightarrow{3}$ D
     - Mensagem codificada: **PDWHPDWLFD**
   - Sabendo que o código de César foi utilizado para codificar uma mensagem com um deslocamento de 8 posições, decodifique a seguinte mensagem: I IZQBUMBQKI M I ZIQVPI LI UIBMUIBQKI
     - Mensagem codificada: **I IZQBUMBQKI M I ZIQVPI LI UIBMUIBQKI**
     - Passo a passo do deslocamento:
       - I $\xrightarrow{-8}$ A
       - I $\xrightarrow{-8}$ A
       - Z $\xrightarrow{-8}$ R
       - Q $\xrightarrow{-8}$ I
       - B $\xrightarrow{-8}$ T
       - U $\xrightarrow{-8}$ M
       - M $\xrightarrow{-8}$ E

    * B $\xrightarrow{-8}$ T
    * Q $\xrightarrow{-8}$ I
    * K $\xrightarrow{-8}$ C
    * I $\xrightarrow{-8}$ A
    * M $\xrightarrow{-8}$ E
    * I $\xrightarrow{-8}$ A
    * Z $\xrightarrow{-8}$ R
    * I $\xrightarrow{-8}$ A
    * Q $\xrightarrow{-8}$ I
    * V $\xrightarrow{-8}$ N
    * P $\xrightarrow{-8}$ H
    * I $\xrightarrow{-8}$ A
    * L $\xrightarrow{-8}$ D
    * I $\xrightarrow{-8}$ A
    * U $\xrightarrow{-8}$ M
    * I $\xrightarrow{-8}$ A
    * B $\xrightarrow{-8}$ T
    * M $\xrightarrow{-8}$ E
    * U $\xrightarrow{-8}$ M
    * I $\xrightarrow{-8}$ A
    * B $\xrightarrow{-8}$ T
    * Q $\xrightarrow{-8}$ I
    * K $\xrightarrow{-8}$ C
    * I $\xrightarrow{-8}$ A
  - Mensagem decodificada: **A ARITMETICA E A RAINHA DA MATEMATICA**

3. **Atividade Prática:** Distribua folhas de exercícios com mensagens para serem codificadas e decodificadas usando o código de César (Nesta atividade o importante é que o aluno apenas compreenda o funcionamento deste método de criptografia, então já deixe indicado o deslocamento para ele quando for decodificar uma mensagem).

   - Utilizando o código de César, codifique as palavras ESCOLA e ALUNO, utilizando um deslocamento 2:
   - Decodifique as palavras a seguir, sabendo que foi utilizado um deslocamento 3 para escreve-las:
     - HVWRMR
     - FROD
     - OLYUR

- Henrique e Antônio trocam bilhetes com mensagens codificadas durante a aula utilizando o código de César, cada um utiliza como deslocamento a quantidade de letras do nome do amigo.
  - Nesta manhã, Henrique enviou um bilhete a seu amigo com a seguinte mensagem: "CHTVZ HUKHY KL IPIPISLAH OVQL?". E o bilhete de resposta de Antônio foi: "VIW XWAAW, BMVPW LMVBQABI."
    Decifre as mensagens trocadas pelos amigos.
  - Antônio deseja mandar um novo bilhete com a pergunta "podemos fazer isso amanhã?". Como deverá ficar a mensagem escrita no bilhete?

4. **Discussão:**

- Revise as respostas com a turma, discutindo quaisquer dificuldades ou dúvidas que surgirem durante os exercícios.

3ª Hora Aula: Prática com o Código de César utilizando Material Eletrônico

1. **Sugestão para o professor(a):**

- Para essa aula é necessário material com acesso a internet, utilize a sala de informática ou tablets se forem disponibilizados pela escola.
  Divida a turma em duplas para realizarem essa atividade.
  Instrua para que cada aluno individualmente acesse o site:
  mathcryptosite.wixsite.com/mathcrypto para criar mensagens criptografadas usando o código de César. (Este site foi desenvolvido como parte de uma dissertação de mestrado do PROFMAT).

2. **Atividade Prática:**

- Peça que os alunos criem mensagens criptografadas utilizando o site. Para isso oriente eles a escreverem a mensagem com letras minúsculas no campo indicado, sem colocar acentos nas palavras e colocarem um número inteiro no intervalo de 1 a 26, no outro campo, que será o número de posições que cada letra será deslocada no alfabeto, para que a mensagem seja criptografada.
- Depois, instrua os alunos a trocarem as mensagens criptografadas entre suas duplas e a decifrarem as mensagens um do outro. Nesta atividade o deslocamento que foi feito deve ser decifrado pelo próprio aluno, o professor pode orientar algum tipo de estratégia, como procurar pelas letras que mais se repetem e tentar identificar as vogais primeiro.

3. **Discussão:**

   - Revise as soluções das mensagens decifradas em conjunto, garantindo que os alunos compreendem cada passo da aplicação do código de César, além disso discuta como cada um pensou para começar a decifrar a mensagem, busque encontrar com eles qual era a melhor estratégia.
   - Discuta a importância de compreender métodos básicos de criptografia e a dificuldade que tiveram em decifrar suas mensagens.

6 Considerações finais

Este estudo propôs a inclusão de uma unidade temática de Aritmética na Base Nacional Comum Curricular (BNCC) para os anos finais do Ensino Fundamental, destacando que a ausência de uma abordagem estruturada para essa área se diferencia dos outros campos da Matemática, como Álgebra, Geometria, Probabilidade e Estatística, que contam com tratamento próprio e bem delimitado na BNCC. A Aritmética possui um corpo de conceitos próprios e aplicações significativas que merecem maior destaque. Essa negligência compromete não apenas o desenvolvimento do raciocínio lógico, mas também a compreensão de temas atuais e interdisciplinares, como a segurança digital.

A implementação da unidade temática de Aritmética no Ensino Fundamental é também um passo inicial para que seu ensino possa se expandir ao Ensino Médio. A abordagem introdutória de temas como congruências modulares no Ensino Fundamental possibilita que, em etapas posteriores, os alunos explorem tópicos mais avançados, como criptografia e segurança da informação. Essas áreas, cada vez mais relevantes no contexto tecnológico contemporâneo, podem se tornar um ponto de conexão entre a Matemática e as demandas da sociedade atual, despertando o interesse dos estudantes e valorizando a Matemática como ferramenta prática e indispensável.

É importante enfatizar que este trabalho, assim como a própria BNCC, busca servir de base. As habilidades e objetos de conhecimento propostos para a unidade temática de Aritmética foram planejados considerando o desenvolvimento cognitivo esperado para alunos dos anos finais do Ensino Fundamental. Não se trata de uma lista exaustiva ou definitiva de conteúdos, mas sim de um ponto de partida, que pode e deve ser enriquecido pelos professores de acordo com as necessidades, os interesses e o contexto de seus alunos. Garantindo que a Aritmética seja uma oportunidade para os alunos desenvolverem habilidades críticas e conectarem os conceitos matemáticos ao seu cotidiano.

As sequências didáticas apresentadas ao longo deste trabalho foram pensadas para facilitar a implementação da proposta, oferecendo aos professores exemplos práticos de como abordar os novos conteúdos em sala de aula. Contudo, são apenas sugestões que podem ser adaptadas, ampliadas e personalizadas, respeitando a realidade de cada turma e promovendo um ensino mais significativo.

Por fim, espera-se que este trabalho contribua para a valorização da Aritmética na Educação Básica e inspire futuras discussões sobre a ampliação de seu papel no currículo escolar. Que ela se torne, assim, não apenas um tema de discussão acadêmica, mas uma prática efetiva no cotidiano das escolas brasileiras.

Referências

BARROS, M. A. O. **Aritmética Modular: Aplicações no Ensino Médio**. Dissertação (PROFMAT) - Instituto de Ciências Exatas e da Terra, Universidade Federal de Mato Grosso. Cuiabá, p.100. 2014.

BRASIL. Ministério da Educação. **Base Nacional Comum Curricular**. Brasília, 600 páginas, 2018.

CADAR, L; DUTENHEFNER, F. **Encontros de Aritmética**. Rio de Janeiro: SBM, 2016

FERREIRA, R. B. **Congruência Modular no Ensino Básico**. Dissertação (PROFMAT) - Centro de Ciências Exatas e Tecnologia, Universidade Federal do Maranhão. São Luís, p.49. 2018.

HEFEZ, Abramo. **Aritmética**. 3 ed. Rio de Janeiro: SBM, 2022.

JURKIEWICZ, Samuel. **Divisibilidade e Números Inteiros: Introdução à Aritmética Modular**. Apostila do PIC, OBMEP. 2006.

Portal da OBMEP. Tópicos adicionais - Módulo: Aritmética dos Restos. Disponível em: https://portaldaobmep.impa.br/index.php/modulo/ver?modulo=63 . Acesso em: 01 de agosto de 2024.

REIS, M. A. M. **Criptografia: A teoria e a prática em sala de aula**. Dissertação (PROFMAT) - Faculdade de Matemática, Universidade Federal de Uberlândia. Uberlândia, p.74. 2023.