Universidade Estadual de Londrina

DIEGO APARECIDO MARONESE

TÓPICOS DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA: UMA PROPOSTA DE ATIVIDADES

Londrina
2016

DIEGO APARECIDO MARONESE

TÓPICOS DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA: UMA PROPOSTA DE ATIVIDADES

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientadora: Prof.ª Dr.ª Ana Márcia Fernandes Tucci de Carvalho

Londrina
2016

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

Maronese, Diego Aparecido.
Tópicos de Aritmética Modular na Educação Básica : uma proposta de atividades / Diego Aparecido Maronese. - Londrina, 2016.
65 f.

Orientador: Ana Márcia Fernandes Tucci de Carvalho.
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Estadual de Londrina, Centro de Ciências Exatas, Programa de Pós-Graduação em Matemática em Rede Nacional, 2016.
Inclui bibliografia.

1. Matemática - Tese. 2. Aritmética Modular - Tese. 3. Educação Matemática - Tese. I. Carvalho, Ana Márcia Fernandes Tucci de. II. Universidade Estadual de Londrina. Centro de Ciências Exatas. Programa de Pós-Graduação em Matemática em Rede Nacional. III. Título.

DIEGO APARECIDO MARONESE

TÓPICOS DE ARITMÉTICA MODULAR NA EDUCAÇÃO BÁSICA: UMA PROPOSTA DE ATIVIDADES

Dissertação apresentada ao programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Mestre em Matemática.

BANCA EXAMINADORA

Prof.ª Dr.ª Ana Márcia Fernandes Tucci de Carvalho
Universidade Estadual de Londrina

Prof.ª Dr.ª Angela Marta Pereira das Dores Savioli
Universidade Estadual de Londrina

Prof. Dr. Túlio Oliveira de Carvalho
Universidade Estadual de Londrina

Londrina, 02 de setembro de 2016.

A Deus, por Sua presença constante em cada momento da minha vida; aos meus pais, Devanir e Marilsa, por terem me ajudado a construir os alicerces da minha vida; a minha irmã, Wanessa, por todo o carinho e apoio; a minha esposa, Caroline, por estar sempre ao meu lado, me dando forças para continuar; e aos meus mestres, pela dedicação e ensinamentos.

AGRADECIMENTOS

Gostaria de agradecer aos meus pais, Devanir e Marilsa, aos quais devo toda a minha vida, por me ensinarem a importância do caráter, da humildade e do esforço pessoal em cada passo da minha jornada, e à minha irmã Wanessa, por todo o carinho, amor e apoio que me deu desde a nossa infância.

Não posso deixar de agradecer à minha amada esposa Caroline, por compreender a minha ausência em algumas ocasiões devido aos compromissos do mestrado, e por estar sempre ao meu lado, me dando todo o amor e apoio que necessitava, me ajudando a enfrentar mais esse desafio.

Agradeço aos meus colegas de mestrado, companheiros de muitas horas de estudo, pelas valiosas sugestões e contribuições.

Agradeço, também, à equipe do Colégio São José de Apucarana, em especial ao coordenador do Ensino Fundamental e Médio, professor José Ferreira Leite Neto, por todo o carinho que recebi e a colaboração durante toda a realização da pesquisa.

Devo agradecer ainda à minha orientadora, Prof.ª Dr.ª Ana Márcia Fernandes Tucci de Carvalho, pelos valiosos conselhos e o apoio à realização deste trabalho, bem como, a todos os mestres que, através de seus ensinamentos, contribuíram com o aperfeiçoamento da minha formação matemática.

Finalmente, agradeço à Deus pela minha vida, por me dar saúde e forças, além de colocar todas essas pessoas no meu caminho e, dessa forma, proporcionar a realização deste trabalho, que faz parte da conclusão de mais uma etapa da minha vida.

"Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo de prazer não é o conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta."

Carl Friedrich Gauss

MARONESE, Diego Aparecido. **Tópicos de Aritmética Modular na Educação Básica:** uma proposta de atividades. 2016. 65 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual de Londrina, Londrina, 2016.

RESUMO

O presente trabalho trata de tópicos de Aritmética Modular na Educação Básica e traz uma proposta de atividades envolvendo o Teorema Chinês dos Restos. O objetivo é introduzir alguns conceitos fundamentais para o ensino da Aritmética Modular a alunos do Ensino Médio. A pesquisa foi realizada por meio da observação e análise qualitativa das resoluções das atividades aplicadas à um grupo de alunos da 2ª série do Ensino Médio de um colégio particular do norte do Paraná. Essas atividades foram aplicadas utilizando a Resolução de Problemas e a Investigação Matemática. Os resultados dessa pesquisa mostraram que, desde que respeitado o nível de conhecimento que os alunos adquiriram até esta etapa da Educação Básica, é possível inserir alguns conceitos básicos de Aritmética Modular no ensino de Matemática ainda no Ensino Médio, conseguindo participação dos alunos no desenvolvimento das atividades e a compreensão desses conceitos pela maioria deles. Também foi possível observar a importância do desenvolvimento do pensamento aritmético em conjunto com o pensamento algébrico no decorrer da Educação Básica, permitindo que os alunos interpretem de maneira adequada os problemas e saibam transcrever suas observações utilizando a notação algébrica. Além disso, o ensino de conteúdos considerados mais "avançados", como a Aritmética Modular, contribui para motivar os estudantes a buscar novas ferramentas e métodos para resolver problemas, e possibilita um maior desenvolvimento de sua capacidade interpretativa, fator fundamental para o aprimoramento do pensamento aritmético, de forma integrada ao pensamento algébrico.

Palavras-chave: Aritmética Modular. Educação Básica. Pensamento Aritmético. Pensamento Algébrico.

MARONESE, Diego Aparecido. **Topics of Modular Arithmetic in Basic Education:** a proposal for activities. 2016. 65 f. Dissertation (Professional Masters in Mathematics) – State University of Londrina, Londrina, 2016.

ABSTRACT

This work deals with topics of Modular Arithmetic in Basic Education and brings a proposal of activities involving the Chinese Remainder Theorem. The goal is to introduce some basic concepts for teaching Modular Arithmetic to high school students. The survey was conducted through observation and qualitative analysis of the resolutions of the activities applied to a group of students of the 2nd high school series of a private school in northern Paraná. These activities were implemented using the Problem-Solving Approach and Mathematical Investigation. The results of this research showed that, provided you adhere to the level of knowledge that students have acquired up to this stage of education, you can enter some basic concepts of Modular Arithmetic in teaching mathematics still in high school, getting student participation in the development of activities and understanding of these concepts by most of them. It was also noted the importance of developing the arithmetical thinking together with the algebraic thinking in the course of Basic Education, allowing students to interpret properly the problems and know how to transcribe their observations using the algebraic notation. In addition, the teaching of contents considered more "advanced" as Modular Arithmetic helps to motivate students to seek new tools and methods to solve problems and enables further development of its interpretative capacity, a key factor for improving the arithmetical thinking in an integrated manner to algebraic thinking.

Keywords: Modular Arithmetic. Basic Education. Arithmetic Thinking. Algebraic Thinking.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

PROFMAT	Mestrado Profissional em Matemática em Rede Nacional
TCR	Teorema Chinês dos Restos
UEL	Universidade Estadual de Londrina

SUMÁRIO

1 INTRODUÇÃO

Desde os primórdios da humanidade a Matemática desempenha um papel fundamental para possibilitar o desenvolvimento da sociedade, estando presente em praticamente todos os aspectos da vida humana, políticos, socioeconômicos, culturais e, em especial, no desenvolvimento de todas as tecnologias no decorrer da história. Contudo, mesmo nas últimas décadas, muitos ainda não conseguem perceber toda a sua importância e, ainda, acabam tendo certa aversão por considerá-la difícil demais ou irrelevante. Isso faz com que o ensino da Matemática seja, cada dia mais, um desafio para o professor. Conseguir obter a atenção e o interesse do aluno, despertando nele o desejo por aprender, é uma das maiores dificuldades na sala de aula.

Na busca por encontrar uma solução para essa dificuldade, ao longo dos anos foram criadas diversas metodologias que procuram desenvolver o ensino da Matemática de maneiras diferenciadas do método tradicional[1], possibilitando que o aluno desempenhe um papel mais ativo na construção de seu conhecimento. Dentre essas novas metodologias, podemos citar a Resolução de Problemas e a Investigação Matemática, como ferramentas para melhorar a aprendizagem dos alunos e desenvolver seus demais aspectos cognitivos.

Outro ponto a se observar é importância de desenvolver o pensamento aritmético dos alunos já na Educação Básica. Atualmente, os currículos de Matemática do Ensino Fundamental e Médio apenas introduzem alguns tópicos relacionados à Teoria dos Números, como os conceitos de divisibilidade, máximo divisor comum e mínimo múltiplo comum. Porém, outros conceitos, como o de congruência, são deixados de lado nessa etapa do ensino.

De acordo com Lins e Gimenez (1997, p. 34), a aritmética moderna é importante pois

> oferece respostas a problemas teóricos abertos, muito recentes. Entre eles, a chamada matemática discreta (quem sabe a "nova aritmética"), com a criptografia, os problemas de minimização e exploração máxima na economia, a análise numérica, os problemas de iteração etc. Por que reduzir então a aritmética a regras escolares? Por que reduzir a aritmética aos números naturais?

Além disso, os professores que buscam desenvolver atividades que envolvam esses tópicos mais avançados, esbarram na dificuldade em encontrar atividades didáticas aplicáveis no Ensino Básico.

[1]No ensino tradicional da matemática, o professor transmite unilateralmente os conteúdos, enquanto que os alunos recebem esse conhecimento e realizam, de forma repetitiva e mecanizada, exercícios para memorização das fórmulas e algoritmos aprendidos. Assim, neste modelo de aula, o professor não desafia, pouco interage e nem se coloca a disposição para o desenvolvimento individual do aluno, restringindo-se apenas ao que ensina (REGO, 1995).

No decorrer dos anos em que participei do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), principalmente nas disciplinas de Aritmética e História da Matemática, despertou-me um grande interesse em aprofundar meus estudos nessa área da aritmética modular, por se tratar de um tema que ainda não possuía muitos conhecimentos e pelo vasto campo de aplicações existente para essa teoria. Inserido nessa área, pude conhecer o Teorema Chinês dos Restos (TCR), um valioso resultado matemático utilizado na resolução de sistemas de congruências lineares e, com isso, busquei conhecer mais sobre a história do desenvolvimento da Matemática no oriente, em particular na China.

Outro fator motivador para a realização da presente pesquisa foi que, historicamente, o ensino de tópicos de Teoria dos Números na Educação Básica tende a focar apenas em introduzir alguns conceitos mais simples, deixando de lado diversos algoritmos e teoremas. Essa abordagem "mecanizada" do ensino de conceitos como Mínimo Múltiplo Comum, Máximo Divisor Comum e Divisibilidade, contraria o que é observado nos Parâmetros Curriculares Nacionais, os quais destacam que

> as situações de aprendizagem precisam estar centradas na construção de significados, na elaboração de estratégias e na resolução de problemas em que o aluno desenvolve processos importantes como intuição, analogia, indução e dedução, e não atividades voltadas para a memorização, desprovidas de compreensão ou de um trabalho que privilegie uma formalização precoce dos conceitos (BRASIL, 1998, p. 63)

Com isso, podemos perceber que o ensino adequado desses tópicos mais avançados da Teoria dos Números, possibilita a aquisição de novas ferramentas pelos alunos para a resolução de problemas diversos. Além disso, segundo Groenwald (2010, p. 2) o estudo de tópicos da Teoria dos Números pode ser desenvolvido, na Educação Básica, de modo a

> estimular nos alunos o interesse pela Matemática, aprimorando o raciocínio lógico e ampliando a compreensão dos conceitos básicos para o refinamento do pensamento aritmético e algébrico, fazendo com que os mesmos desenvolvam a capacidade de manipular conceitos e propriedades de forma clara e objetiva.

Assim, devido ao interesse em encontrar formas de trabalhar esses conceitos na Educação Básica, o presente trabalho apresenta uma proposta de atividades envolvendo alguns desses tópicos de Aritmética Modular, para ser aplicada a alunos do Ensino Médio, objetivando alcançar, por parte dos alunos, uma compreensão dos conceitos que fundamentam essa área tão interessante da Matemática e, dentro das possibilidades, apresentar a ideia do Teorema Chinês dos Restos.

Para isso, em um primeiro momento, foi realizada uma pesquisa bibliográfica desenvolvida em quatro capítulos: no primeiro é apresentado um breve relato histórico do desenvolvimento da Matemática desde os primórdios da China, sua importância e principais estudiosos; em seguida, são discutidas as principais ideias referentes ao conceito de pensamento aritmético e algébrico, e sua relevância para o estudo da Matemática; já no terceiro capítulo, são introduzidos alguns conceitos fundamentais da aritmética modular e os diferentes enunciados do TCR; e no quarto capítulo, as metodologias que foram utilizadas na realização da pesquisa são apresentadas, buscando explicitar a relevância para terem sido selecionadas.

Finalmente, na segunda parte do trabalho, são apresentados os principais resultados obtidos com a pesquisa, enunciando algumas das formas de resolução desenvolvidas pelos alunos durante a aplicação das atividades, sugestões para melhorar sua utilização, além das considerações finais acerca desses resultados.

2 OBJETIVOS

2.1 OBJETIVO GERAL

- Desenvolver tópicos de Aritmética Modular na Educação Básica.

2.2 OBJETIVOS ESPECÍFICOS

- Introduzir a ideia de operar com os restos da divisão euclidiana;
- Desenvolver o pensamento aritmético dos alunos, apresentando algumas noções fundamentais para a construção do conceito de congruência.

3 HISTÓRIA DA MATEMÁTICA NA CHINA

Da mesma forma que em diversas outras civilizações antigas, existem poucos registros matemáticos dos primórdios da China e os existentes não são completamente confiáveis. Há estudos que comprovam que a matemática existia desde a dinastia Han (202 a.C.), da mesma época do Império Romano, nas transações comerciais com outras regiões da Ásia.

A matemática chinesa sofreu influência dos árabes e dos indianos e também influenciou outras regiões, como o Japão, por exemplo. Estes primeiros registros são relativos à processos do cotidiano e problemas concretos de contagem e medições, porém é extremamente difícil datá-los com precisão (GARBI, 2010). Aquele que é considerado o mais antigo pergaminho clássico da matemática chinesa, o Zhoubi Suanjing (Chou Pei Suang Ching), ainda gera dúvidas entre os estudiosos acerca de sua idade, variando entre 1200 a.C. até por volta de 300 a.C., o que demonstra a dificuldade que existe em estimar as origens da matemática chinesa. Para além de uma breve explicação sobre o cálculo aritmético, este texto contém um diálogo sobre as propriedades dos triângulos retângulos, no qual o teorema de Pitágoras, conhecido por eles como teorema Gougu, é enunciado e dada uma de suas demonstrações geométricas (MIAO, 2012).

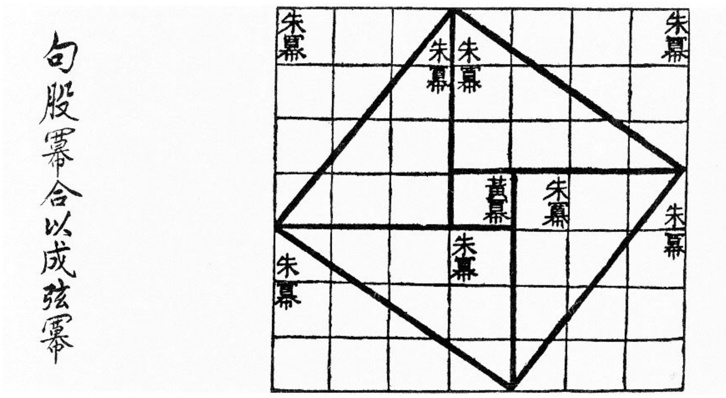

Figura 3.1: Teorema de Pitágoras (Gougu) presente no Zhoubi Suanjing
Fonte: Wikimedia Commons

Contudo, segundo Brandenburg e Nevenzeel (2007, p. 1), o mais influente livro de matemática de origem chinesa foi o Jiuzhang suanchu (Chui-chang suan-shu), ou *Nove Capítulos sobre a arte matemática*. De acordo com Garbi (2010, p. 142), o livro contém "246 problemas de diversas naturezas, como áreas de figuras geométricas, percentagens e proporções, regra de três, raízes quadradas e cúbicas, tempos e movimentos, Regra da Falsa Posição, sistemas de equações lineares e triângulos pitagóricos".

折抵地爲弦以句及股弦并求股故先令句自乘見矩
冪令如高而一凡爲高一丈爲股弦并之以除此冪得
差所得以減竹高而半其餘卽折者之高也此率與係
索之類更相返覆也亦可如上術令高自乘爲股弦并
冪去本自乘爲矩冪減之餘爲實倍高爲法則得折之
高數也

去根如勾折處
如股折梢如弦
通長如股弦和

股弦和與勾求股法曰勾自乘爲實變股弦較乘股弦
和如股弦和而一正除得股弦較以減股弦和餘二

Figura 3.2: Problema do bambu quebrado - Jiuzhang suanchu
Fonte: Wikimedia Commons

Nas obras chinesas, como nas egípcias, chama a atenção a justaposição de resultados precisos e imprecisos, primitivos e elaborados. Como exemplo, temos que as áreas de quadriláteros regulares e triângulos era calculada de forma exata, enquanto o cálculo da área do círculo ou de um setor circular era feita utilizando aproximações.

Existem referências à regra de três, raízes quadradas e cúbicas, além de várias resoluções de problemas envolvendo equações lineares simultâneas. Os estudiosos chineses também eram especialmente admiradores de padrões matemáticos, o que possibilitou diversos estudos na área, inclusive o quadrado mágico mais antigo conhecido é de origem chinesa.

Segundo Boyer (2012, p. 144), "se a matemática chinesa tivesse tido continuidade de tradição, algumas das notáveis antecipações dos métodos modernos poderiam ter modificado substancialmente o desenvolvimento da matemática". Porém houve diversos momentos na história chinesa que culminaram em rupturas na construção deste conhecimento, inclusive causando a perda de muitos estudos já realizados. Como ocorreu no ano 213 a.C. quando o imperador Shi Huang-ti, com vistas em controlar e manipular as manifestações populares, mandou destruir todos os livros existentes na China. Este fato, entre tantos outros, fez com que o conhecimento matemático se estagnasse em alguns períodos, sendo que apenas não foram perdidos todos os registros anteriores devido à transmissão oral e algumas poucas cópias que foram mantidas em segredo por séculos (GARBI, 2010).

O ponto alto da matemática chinesa ocorreu no século XIII durante o fim do período Sung. Nesta época foi descoberta a impressão, a pólvora, o papel e a bússola. Obras chinesas desta época influenciaram fortemente a Coréia e o Japão, contudo muitas destas obras desapareceram da China neste período, reaparecendo apenas no século XIX (BRANDENBURG; NEVENZEEL, 2007).

Yang Hui (1261 - 1275) foi um matemático talentoso cuja obra inclui os mais antigos quadrados mágicos chineses de ordem maior que três, estudos com séries numéricas além de uma variação chinesa para o triângulo de Pascal. Suas obras puderam ser melhor preservadas e conhecidas devido à publicação no *Precioso espelho dos quatro elementos*.

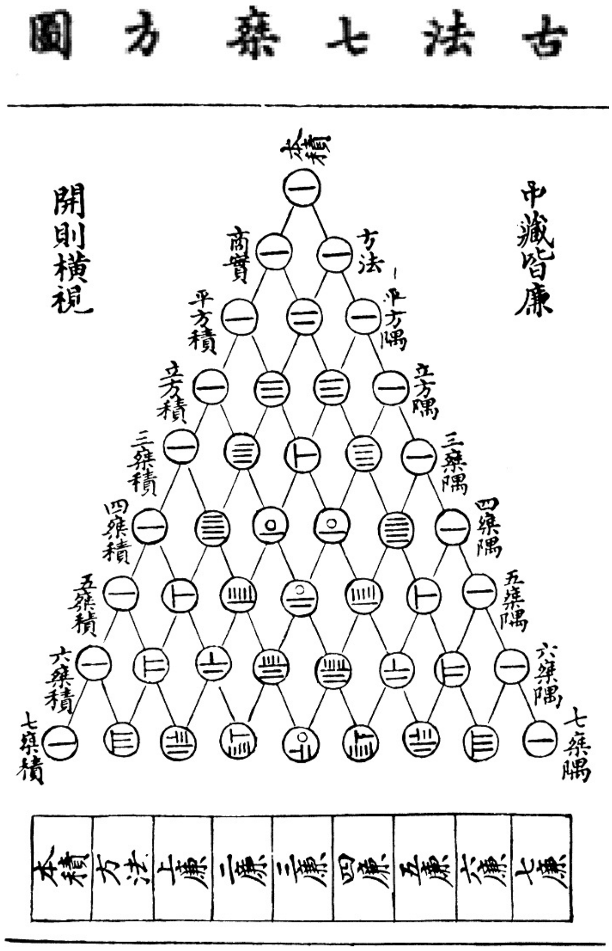

Figura 3.3: O triângulo de aritmético de Yang Hui, ilustrado na capa do *Precioso espelho dos quatro elementos*

Fonte: Wikimedia Commons

Considerado um dos mais brilhantes matemáticos da era Sung, Zhu Shijie viveu por volta de 1260 a 1320, porém pouco se sabe acerca de sua vida (BRANDENBURG; NEVENZEEL, 2007). Tem-se conhecimento de duas obras de sua autoria. A primeira, escrita em 1299, foi o Suanxue qimeng (Suan-hsueh ch'i-meng), traduzida como Introdução aos estudos matemáticos, é um livro sobre a matemática elementar com quatro problemas ilustrativos para explicar operações de aritmética e álgebra, além de 284 problemas como exercícios. O original em chinês ficou perdido mas foi reconstruído em 1839 através de um edição coreana de 1660.

Sua segunda, e mais conhecida obra, foi o Siyuan yujian (Ssu-yuan yu-chien), conhecido como *Precioso espelho dos quatro elementos*, escrita em 1303. Segundo Boyer (2012, p. 149) "O livro representa o ápice do desenvolvimento da álgebra chinesa, pois trata de equações simultâneas e de equações de grau até quatorze." A obra inicia com uma representação do triângulo aritmético dos coeficientes binomiais proposto por Yang Hui, porém ampliado até a oitava potência e apresentando um símbolo redondo para representar o zero, sendo que ele chama esta representação de "diagrama do velho método para achar potências oitavas e menores". Com isso observa-se que a origem do triângulo aritmético é chinesa, logo é impróprio depositar todo o crédito à Blaise Pascal, o qual se baseou nesta descoberta para desenvolver e estudar as propriedades existentes nele, em 1653.

Com isso, podemos perceber que, as contribuições chinesas para o desenvolvimento da matemática são muito valiosas e evidenciam como essa ciência pode ser pensada de vária formas, por diferentes culturas, mas sendo possível encontrar pontos em comum que interligam e constroem sua estrutura.

Contudo, mesmo com toda a sua riqueza e complexidade, percebemos que a história das civilizações do oriente é muito pouco abordada na Educação Básica no Brasil. Isso faz com que os alunos acreditem que nada de interessante ocorreu nestas regiões, por isso não há preocupação em estudá-las. Dessa forma, o ato de contextualizar historicamente os conceitos matemáticos que serão apresentados, oferece uma oportunidade valiosa para o professor instigar a curiosidade e o interesse dos alunos.

> Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor tem a possibilidade de desenvolver atitudes e valores mais favoráveis do aluno diante do conhecimento matemático. Em muitas situações, o recurso à História da Matemática pode esclarecer idéias (sic.) matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns "porquês" e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento. (BRASIL, 1998, p.34)

Essa ferramenta se mostra de grande importância pois, de acordo com as Diretrizes Curriculares da Educação Básica do Paraná (2008),

> a história deve ser o fio condutor que direciona as explicações dadas aos porquês da Matemática. Assim, pode promover uma aprendizagem significativa, pois propicia ao estudante entender que o conhecimento matemático é construído historicamente a partir de situações concretas e necessidades reais.

Assim, observamos a relevância da utilização da história como uma ferramenta de contextualização e "humanização" da matemática, possibilitando ao educador criar um ambiente mais propício à aprendizagem dos mais diversos conceitos, o que facilita a compreensão e a construção do conhecimento por parte dos alunos.

4 PENSAMENTO ARITMÉTICO E ALGÉBRICO

Desde os anos iniciais da Educação Básica, a aritmética é desenvolvida de maneira conjunta entre o trabalho com números e operações e o ensino do espaço e das formas, sendo que esses conceitos são os primeiros conteúdos matemáticos aprendidos pela criança. Além disso, devemos salientar que, mesmo antes de chegar à escola, a criança já possui uma certa noção de número, a qual foi sendo construída a partir de atitudes naturais de agrupamento e seriação por ela vivenciadas.

Poderíamos tentar definir a aritmética apenas como sendo os números e as operações entre eles. Porém, segundo afirmam Lins e Gimenez (1997, p. 33), a educação aritmética é muito mais que isso, ela inclui também

> a) representações e significações diversas (pontos de referencias (sic.) e núcleos, que ampliam a idéia (sic.) simples do manipulativo); b) análise do porquê dos algoritmos e divisibilidade (elementos conceituais); c) uso adequado e racional de regras (técnicas, destrezas e habilidades); e d) descobertas ou "teoremas" (descobertas, elaboração de conjecturas e processos de raciocínio).

Com isso, observamos que, de acordo com Laudares e Leite (2011, p. 53), "pensar aritmética é buscar os significados que números e suas operações podem ter na legitimidade de questões da matemática e da não matemática". Logo, o ensino da aritmética, em particular na Educação Básica, deve ter como foco desenvolver a capacidade do aluno de produzir seu próprio conhecimento aritmético com real significado, compreendendo sua importância e sabendo utilizá-lo quando necessário.

Porém, para isso, o professor deve buscar atividades e ferramentas que estimulem esse desenvolvimento em seus alunos, evitando exercícios de simples repetição que fortalecem essa abordagem tradicional e superficial da aritmética, a qual persiste até os dias atuais, pois, segundo Lins e Gimenez (1997), o currículo tradicional indica o que se deve ser ensinado, submetendo os professores a uma enorme pressão.

Ainda de acordo com Silva (2007, p. 4),

> atualmente aritmética e álgebra, no ensino fundamental, são ensinadas separadamente. Nas séries iniciais é ensinada somente a aritmética e apesar de saber que para o desenvolvimento do pensamento aritmético trabalha-se intuitivamente noções de álgebra, o ensino dessa última, em geral, é efetivado somente nas séries finais do ensino fundamental. Assim, para favorecer o ensino da álgebra e da aritmética, poderia haver um esforço entre os educadores matemáticos para que ambas pudessem ser concebidas como complementares, uma ajudando no desenvolvimento da outra.

Esse fato é facilmente percebido, segundo Cruz (2005), pois dificilmente encontramos nos livros didáticos uma articulação entre os conteúdos de aritmética e álgebra que possibilitem ao aluno compreender a ligação entre os números e as letras, o que dificulta o seu entendimento da álgebra como uma ferramenta para provar regras e relações numéricas. Isso contraria o que também propõem Lins e Gimenez (1997), que a educação Aritmética e Algébrica devem ocorrer ao mesmo tempo, não apenas integradas entre si, mas conectadas ao ambiente interno e externo à escola, desempenhando seu papel de auxiliar os alunos a construírem seu conhecimento matemático, visando a produção de significados.

> O grande objetivo da educação aritmética e algébrica hoje deve ser o de encontrar um equilíbrio em três frentes: i) o desenvolvimento da capacidade de por em jogo nossas habilidades de resolver problemas e de investigar e explorar situações; ii) o desenvolvimento de diferentes modos de produzir significado (pensar), o que poderíamos chamar de atividades de inserção e tematização; iii) o aprimoramento das habilidades técnicas, isto é, da capacidade de usar as ferramentas desenvolvidas com maior facilidade. (LINS; GIMENEZ, 1997, p. 165).

Para estes autores, não há um consenso a respeito do que seja pensar algebricamente, o que dificulta uma formalização para esse conceito. De uma forma mais superficial, a atividade algébrica costuma ser descrita como "fazer ou usar álgebra", ou mesmo "calcular com letras", o que tende a enfatizar mais a linguagem algébrica do que o pensamento algébrico em si. Para buscarmos compreender melhor esse conceito, podemos nos pautar nas definições apresentadas por Boni e Savioli (2015, p. 271) para o pensamento algébrico:

> - Kaput e Blanton (2001) defendem o pensamento algébrico como aritmética generalizada, ou seja, como a generalização de operações aritméticas e propriedades numéricas;
> - Fujii e Stephens (2001), abordam sobre o conceito de quase-variáveis, considerando que nos contextos aritméticos estão relacionadas variáveis implícitas que são utilizadas pelos estudantes;
> - Usiskin (2000) argumenta que, mesmo sem perceberem, os professores dos anos iniciais já ensinam álgebra, apresentando exemplos que mostram reconhecimento de padrões e generalização em propriedades de números e de operações aritméticas.

Dessa forma, observamos a necessidade que ocorra essa integração natural entre a álgebra e a aritmética em sala de aula, pois

> o trabalho integrado entre procedimentos de cálculos aritméticos e pensamento algébrico, além de possibilitar o desenvolvimento deste a partir da generalização de aspectos adjacentes em procedimentos de cálculo, contribui, do mesmo modo, para os estudantes reexaminarem e compreenderem o significado das operações e as diferentes formas de pensar a Matemática (RUSSELL; SCHIFFER; BASTABLE, 2011 *apud* BONI; SAVIOLI, 2015, p. 266).

Assim, podemos perceber que esse desenvolvimento conjunto do pensamento aritmético e do pensamento algébrico mostra-se fundamental para a plena compreensão do aluno quanto à forma como é constituída a Matemática. Mesmo com as dificuldades apresentadas anteriormente, é fundamental que o professor assuma seu papel de condutor dessa construção de conhecimento, possibilitando aos seus alunos não apenas um entendimento superficial dos conceitos matemáticos, mas sim que desenvolvam seu pensamento aritmético e algébrico de modo a encontrarem soluções mais facilmente para os problemas de sala de aula e de fora da escola.

Nesse contexto, o ensino de tópicos mais avançados de matemática, como a Aritmética Modular, além de permitir observar o nível de aprimoramento aritmético e algébrico dos alunos, também pode proporcionar um melhor desenvolvimento de ambos os pensamentos de uma maneira integrada, por meio de problemas que instigam o estudante à analisar e realizar essa transição entre as operações aritméticas observadas e suas conclusões, utilizando a notação algébrica.

5 ARITMÉTICA MODULAR

Mesmo sabendo que a aritmética está presente nos currículos do ensino obrigatório em todos os países, conforme afirmam Lins e Gimenez (1997), o mesmo não acontece com a aritmética desenvolvida por Gauss, conhecida como Aritmética Modular. A Aritmética Modular trabalha com os inteiros separando-o em conjuntos, chamados classes de equivalência, definidos segundo o resto da divisão por um número natural fixo, digamos n (MATTOS; PUGGIAN; LOZANO, 2011). No conjunto dos restos possíveis na divisão por n: $\{0, 1, 2, \cdots, n-1\}$, definem-se as operações de soma e multiplicação, condizentes com a multiplicação dos inteiros.

Como ilustração, podemos observar um uso mais comum da Aritmética Modular no relógio analógico, no qual analisamos o dia em dois períodos de 12 horas cada. Se em determinado momento o relógio marca 7 horas, então daqui a 8 horas estará marcando 3 horas. Porém, se seguirmos a adição usual, o horário futuro deveria ser $7 + 8 = 15$, o que não é possível no relógio analógico, pois o mesmo possui um período de 12 horas, logo não é possível que marque "15 horas". Da mesma forma, se o relógio começa em 12:00 (meio dia) e se passam 21 horas, o horário observado será 9:00 do dia seguinte, em vez de 33:00. Como a contagem das horas recomeça ao atingir 12, podemos perceber que a aritmética do relógio é uma aritmética módulo 12.

Além disso, ainda que normalmente não estejam presentes nos planos de ensino de matemática em todos os níveis, trabalhamos com os restos das divisões na resolução de diversos problemas no nosso dia a dia. Mesmo esse sendo um conceito pouco desenvolvido na Educação Básica, observamos que pode ser um grande motivador para a aprendizagem, em razão de sua boa capacidade de contextualização, o que possibilita a elaboração de diversas e desafiadoras atividades didáticas. Além disso, segundo Mattos, Puggian e Lozano (2011), o ensino da Aritmética Modular na Educação Básica auxilia a consolidação do conceito de divisibilidade, proporciona que os alunos conheçam um contexto diferente para a realização das operações aritméticas e, ainda, incentiva um maior desenvolvimento do pensamento aritmético e sua ligação com o algébrico.

Para fundamentar melhor esses conceitos que serão trabalhados durante a pesquisa, vamos apresentar alguns tópicos para compreendermos as bases da Aritmética Modular. No que se segue, estaremos seguindo as obras de Domingues e Iezzi (2003), Hefez (2014), Martinez *et al.* (2013) e Evaristo e Perdigão (2002).

5.1 Divisibilidade

Dados dois inteiros d e a, com $d \neq 0$. Dizemos que d *divide* a, ou que d é um *divisor* de a, ou ainda que a é um *múltiplo* de d, e escrevemos

$$d \mid a$$

se existir $q \in \mathbb{Z}$ com $a = qd$. Caso contrário, escrevemos $d \nmid a$.

No caso particular $a = 0$, temos que o conjunto de seus divisores $D = \{d \in \mathbb{Z} \mid d \mid a\}$ é infinito, pois, $\forall d \in \mathbb{Z}$, $\exists q \in \mathbb{Z}$, $q = 0$, tal que $0 = d \cdot 0$.

5.2 Divisão Euclidiana

A divisão euclidiana, ou divisão com resto, é uma das quatro operações fundamentais que as crianças aprendem logo nos primeiros anos da Educação Básica. Primeiramente, vamos introduzir alguns resultados que serão necessários para demonstrar o Teorema 5.6, o qual enunciaremos a seguir.

Proposição 5.1. *Seja* $x \in \mathbb{R}$*. Se* $0 < x < 1$*, então* $x^2 < x$*.*

Demonstração. Para demonstrarmos, basta multiplicar todos os termos da desigualdade por x. Como $0 < x < 1$, o sinal da desigualdade não se altera, logo

$$\begin{aligned} 0 < x < 1 \\ 0 \cdot x < x \cdot x < 1 \cdot x \\ 0 < x^2 < x \end{aligned}$$

□

A proposição a seguir estabelece que não existem elementos inteiros no intervalo entre 0 e 1.

Proposição 5.2. *Dado* $x \in \mathbb{Z}$*. Se* $x > 0$*, então* $x \geq 1$*.*

Demonstração. Seja o conjunto $S = \{y \in \mathbb{Z} \mid 0 < y < 1\}$. Devemos mostrar que $S = \varnothing$. Se $S \neq \varnothing$, pelo Princípio da Boa Ordenação[1], S possui um elemento mínimo b. Como $0 < b < 1$ (pela definição do conjunto S), segue que, pela proposição 5.1, $b^2 < b$, o que implica, por transitividade, que $b^2 < 1$. Além disso, como $b > 0$, segue que $b^2 > 0$. Assim, $0 < b^2 < 1$ e, portanto, $b^2 \in S$. Porém, esta pertinência contraria o fato de que b é o elemento mínimo de S, já que $b^2 < b$. Assim, $S = \varnothing$ e a proposição 5.2 está demonstrada. □

[1] **Princípio da Boa Ordenação.** Todo subconjunto de $\mathbb{Z}$ não vazio limitado inferiormente possui elemento mínimo.

É uma consequência imediata da Proposição 5.2 o fato de que, no conjunto dos números inteiros, não existe um inteiro entre dois inteiros y e $y+1$, por isto se diz que estes são inteiros consecutivos.

Definição 5.3 (Valor Absoluto ou módulo). *Dado um número inteiro z, o valor absoluto ou módulo é definido por*

$$|z| = \begin{cases} z, & se\ z \geq 0 \\ -z, & se\ z < 0 \end{cases}$$

Por exemplo, $|1| = 1$, $|0| = 0$ e $|-1| = 1$.

Lema 5.4 (Propriedades da divisibilidade)**.** *Sejam $a, b, c, d \in \mathbb{Z}$. Temos:*

(i) ("d divide") Se $d \mid a$ e $d \mid b$, então $d \mid ax + by$ para qualquer combinação linear $ax + by$ de a e b com coeficientes $x, y \in \mathbb{Z}$.

(ii) (Limitação) Se $d \mid a$, então $a = 0$ ou $|d| \leq |a|$.

(iii) (Transitividade) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. [2] Se $d \mid a$ e $d \mid b$, então podemos escrever $a = dq_1$ e $b = dq_2$, com $q_1, q_2 \in \mathbb{Z}$. Logo, $ax + by = d(q_1x + q_2y), \forall x, y \in \mathbb{Z}$. Como $q_1x + q_2y \in \mathbb{Z}$, temos $d \mid ax + by$.

Para demonstrar *(ii)*, suponha que $d \mid a$ e $a \neq 0$. Neste caso, $a = dq$ com $q \neq 0$ (pois supomos que $a \neq 0$). Pela Proposição 5.2 assim $|q| \geq 1$ e $|a| = |d||q| \geq |d|$.

Finalmente, se $a \mid b$ e $b \mid c$, então existem $q_1, q_2 \in \mathbb{Z}$ tais que $b = aq_1$ e $c = bq_2$, logo $c = aq_1q_2$ e, portanto, $a \mid c$. □

Proposição 5.5 (Propriedades do Valor Absoluto). *Seja D um domínio ordenado*[3]*. Então, dados $z, y \in D$,*

a) $|z| \geq 0$ e $|z| = 0$ se, e somente se, $z = 0$;

b) $|z \cdot y| = |z| \cdot |y|$;

c) $-|z| \leq z \leq |z|$;

d) $|z| \leq y$ se, e somente se, $-y \leq z \leq y$.

---

[2] MARTINEZ *et al.*, 2013, p. 15

[3] **Domínio ordenado.** Seja A um anel. Diz-se que A é um domínio de integridade se a multiplicação do anel satisfizer à seguinte propriedade.

Quaisquer que sejam $a, b \in A$, se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Um domínio de integridade A é dito *domínio bem ordenado* se satisfizer ao Princípio da Boa Ordenação.

Demonstração. a) Decorre imediatamente da definição 5.3, pois se $z > 0$, $|z| = z > 0$ e se $z < 0$, então $|z| = -z > 0$.

b) A demonstração desta igualdade pode ser feita analisando-se os quatro casos possíveis de combinações de positividade e negatividade de y e z:

(i) se $z \geq 0$ e $y \geq 0$, temos, pela compatibilidade da relação de ordem com a multiplicação, que $z \cdot y \geq 0$ e a igualdade a ser provada decorre da definição.

(ii) se $z \geq 0$ e $y \leq 0$, temos, pelas regras de sinais da multiplicação[4], que $z \cdot y \leq 0$, e então

$$\begin{aligned} |z \cdot y| &= -(z \cdot y) \\ &= z \cdot (-y) \\ &= |z| \cdot |y| \end{aligned}$$

A primeira e a terceira igualdades são obtidas pela própria definição 5.3, enquanto que a segunda igualdade é obtida utilizando o item *(b)* da regra de sinais[5].

(iii) se $z \leq 0$ e $y \geq 0$, a demonstração é análoga a anterior, sendo que, neste caso, $z \cdot y \leq 0$.

(iv) se $z \leq 0$ e $y \leq 0$, temos, $z \cdot y \geq 0$ e $|z \cdot y| = z \cdot y = (-z) \cdot (-y) = |z| \cdot |y|$.

c) Se $z \geq 0$, então $|z| = z \geq -|z|$, pois $-|z|$ é sempre negativo. Logo, $-|z| \leq z \leq |z|$. Agora, se $z \leq 0$, então $|z| = -z$. Além disso, como $|z|$ é sempre positivo e supomos que z é negativo, então $-|z| = z \leq |z|$. Dessa forma, verifica-se a afirmação.

d) Suponhamos, inicialmente, que $|z| < y$. Assim, utilizando o item *(c)* anterior, temos que $-y < -|z| \leq z \leq |z| < y$. Reciprocamente, suponhamos que $-y \leq z \leq y$. Se $z \geq 0$, então $|z| = z$ e, assim, $|z| < y$. De modo semelhante, se $z \leq 0$, temos $|z| = -z$. Como $-y < z$, então, $-z < y$ e, portanto, $|z| > -y$.

□

[4]**Regras de sinais da multiplicação.** Sejam A um anel ordenado e a e b dois elementos de A.
a) se $a \geq 0$, então $-a \leq 0$;
b) se $a \leq 0$, então $-a \geq 0$;
c) se $a \geq 0$ e $b \geq 0$, então $a \cdot b \geq 0$;
d) se $a \geq 0$ e $b \leq 0$, então $a \cdot b \leq 0$;
e) se $a \leq 0$ e $b \leq 0$, então $a \cdot b \geq 0$.

[5]**Regra de sinais.** Seja A um anel. Para todos $a, b \in A$,
a) $(-1) \cdot a = -a$;
b) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$;
c) $(-a) \cdot (-b) = a \cdot b$.

Após a apresentação dos resultados acima, o conceito de ***divisão euclidiana*** pode ser formalmente apresentado, de acordo com Martinez *et al.* (2013, p. 18), como:

Teorema 5.6. *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r \ \ e \ \ 0 \leq r < |b|.$$

Demonstração. [6] Considere o conjunto

$$S = \{y \in \mathbb{Z} \mid y \geq 0 \ \ e \ \ y = a - bn\}.$$

Existência: Pela Propriedade Arquimediana[7], existe um inteiro n tal que $n(-b) \geq -a$, logo $a - bn \geq 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação[8], temos que S possui um menor elemento r. Como $r \in S$, $r \geq 0$ e $r = a - bq$, para algum inteiro q. Vamos mostrar que $r < |b|$.

Suponhamos por absurdo que $r \geq |b|$. Assim, $r > r - |b| \geq 0$ e, então, $r - |b| \in S$, pois, como $a = b(q+1) + (r - |b|)$ ou $a = b(q-1) + (r - |b|)$, temos que $r - |b| = a - b(q+1)$ ou $r - |b| = a - b(q-1)$. Mas isto é um absurdo, pois r é o elemento mínimo de S. Logo, $r < |b|$.

Unicidade: Para provar que q e r são únicos, suponhamos que $a = bq_1 + r_1 = bq_2 + r_2$, em que $q_1, q_2, r_1, r_2 \in \mathbb{Z}$, $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$.

De $r_2 < |b|$, segue que $-|b| < -r_2$ e, desta desigualdade e do fato de que $0 \leq r_1$, segue, por adição, que $-|b| < r_1 - r_2$. Por outro lado, de $r_1 < |b|$ segue, pela compatibilidade da relação de ordem com a adição, que $r_1 - r_2 < |b| - r_2$. Como de $r_2 \geq 0$ segue que $-r_2 \leq 0$, temos que $|b| - r_2 \leq |b|$ e então $r_1 - r_2 \leq |b|$. Assim, $-|b| < r_1 - r_2 < |b|$ e, portanto, pela propriedade *(d)* do Valor Absoluto (proposição 5.5), $|r_1 - r_2| < |b|$.

Agora, de $bq_1 + r_1 = bq_2 + r_2$, temos que $b(q_1 - q_2) = r_2 - r_1$ e, como consequência da propriedade *(b)* do Valor Absoluto (proposição 5.5), $|b| \cdot |q_1 - q_2| = |r_2 - r_1|$. Logo, utilizando a desigualdade $|r_1 - r_2| < |b|$, mostrada acima, $0 \leq |b| \cdot |q_1 - q_2| < |b|$ e então, considerando que $\mathbb{Z}$ é um domínio de integridade[9] e que $|b| > 0$, temos $|q_1 - q_2| < 1$. Como a proposição 5.2 garante que não há inteiros entre 0 e 1, temos que $|q_1 - q_2| \geq 0$, o que implica que $|q_1 - q_2| = 0$, resultando em $q_1 = q_2$. Da igualdade $b(q_1 - q_2) = r_2 - r_1$ apresentada acima, segue que $r_2 = r_1$, o que conclui a demonstração. □

[6] EVARISTO; PERDIGÃO, 2002, pp. 93,94

[7] **Propriedade Arquimediana.** Se $z, y \in \mathbb{Z}$ e $y \neq 0$, então existe um inteiro n tal que $ny \geq z$.

[8] **Princípio da Boa Ordenação.** Todo subconjunto de $\mathbb{Z}$ não vazio limitado inferiormente possui elemento mínimo.

[9] **Domínio de integridade.** Seja A um anel. Diz-se que A é um domínio de integridade se a multiplicação do anel satisfazer à seguinte propriedade:
Quaisquer que sejam $a, b \in A$, se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Tais inteiros q e r são determinados unicamente pelas duas condições apresentadas no teorema 5.6 e são chamados, respectivamente, de **quociente** e **resto** da divisão de a por b.

5.3 MÁXIMO DIVISOR COMUM

Dados dois números $a, b \in \mathbb{Z}$, podemos dizer que o número inteiro $d \in \mathbb{Z}$ é um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Definição 5.7 (Máximo divisor comum)**.** [10] *Sejam a e b dois números inteiros, não simultaneamente nulos. Dizemos que o elemento $d \in \mathbb{Z}$ é o máximo divisor comum (mdc) de a e b, e o denotamos $d = (a, b)$, se possuir as seguintes propriedades:*

(i) $d \geq 0$*;*

(ii) d é um divisor comum de a e de b; e

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

A condição (ii) *acima pode ser reenunciada como segue:*

(iii') Se c é um divisor comum de a e b, então $c \mid d$.

Portanto, se d é o mdc de a e b, e c é um divisor comum desses números, então, pelo item *(iii')*, $d = c \cdot k$, com $k \in \mathbb{Z}$. Logo $c \leq d$. Isto nos mostra que o máximo divisor comum de dois números é efetivamente o maior dentre todos os divisores comuns desses números.

Em particular, isto nos mostra que, se d e d' são dois mdc de um mesmo par de números, então $d \leq d'$ e $d' \leq d$, e, consequentemente, $d = d'$. Ou seja, o mdc de dois números é único.

Em relação ao caso específico do $mdc(0, 0)$, podemos observar que o mesmo não é definido. Como foi apresentado anteriormente, o mdc de dois números é o elemento máximo do conjunto formado pelos seus divisores comuns. Pela definição de divisibilidade, o 0 é divisível por todos os números, logo o conjunto de seus divisores é infinito e, portanto, não possui um máximo.

Teorema 5.8 (Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{Z}$, não ambos nulos. Então existem $x, y \in \mathbb{Z}$ com*

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

Portanto, se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $c \mid mdc(a, b)$.

[10] DOMINGUES; IEZZI, 2003, pp. 39-40

Demonstração. [11] Se $a = 0$, tome $y = 1$ e x qualquer. Se $b = 0$, tome $x = 1$ e y qualquer. Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$I(a, b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Sabemos que $I(a, b)$ possui pelo menos um elemento positivo. De fato, $|b| \in I(a, b)$ (basta tomarmos $x = 0$ e $y = 1$, caso $b \geq 0$, ou $y = -1$, se $b < 0$). Assim, seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$. Afirmamos que d divide todos os elementos de $I(a, b)$. De fato, dado $m = ax + by \in I(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Temos

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a, b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a, b)$, segue que $r = 0$ e, portanto, $d \mid m$.

Em particular, como $a, b \in I(a, b)$ temos que $d \mid a$ e $d \mid b$, logo $d \leq mdc(a, b)$. Finalmente, note que se $c \mid a$ e $c \mid b$, então $c \mid ax_0 + by_0 \Leftrightarrow c \mid d$. Tomando $c = mdc(a, b)$, temos que $mdc(a, b) \mid d$ o que, juntamente com a desigualdade $d \leq mdc(a, b)$, mostra que $d = mdc(a, b)$. E também que todo divisor comum de a e b divide d. $\square$

Lema 5.9. *Seja m um inteiro positivo e seja a um inteiro tal que $mdc(a, m) = 1$. Então, existe um inteiro x tal que*

$$ax \equiv 1 \ (mod\, m).$$

Tal inteiro é único módulo m. Além disso, se $mdc(a, m) > 1$, não existe x que satisfaça tal equação.

Demonstração. Pelo teorema de Bachet-Bézout (5.8), existem inteiros x e y tais que $ax+my = 1$. Analisando essa equação módulo m, obtemos $ax = m(-y) + 1$, ou seja, $ax \equiv 1 \ (mod\, m)$. Se x' é outro inteiro que satisfaz a mesma congruência, temos $ax \equiv ax' \ (mod\ m)$. Isto é equivalente a $a(x - x') \equiv 0 \ (mod\, m)$, isto é, para algum $k \in \mathbb{Z}$,

$$a(x - x') = km$$

Como a e m não têm divisores comuns, segue que $m|(x - x')$, isto é $x = x' \ (mod\, m)$.

Por outro lado, se $d = mdc(a, m) > 1$, não podemos ter $d \mid m$ e $m \mid ax - 1$, pois $d \nmid -1$. $\square$

[11] MARTINEZ *et al.*, 2013, p. 20

Proposição 5.10. *Se $mdc(a, b) = 1$ e $a \mid bc$, então $a \mid c$.*

Demonstração. Como $mdc(a, b) = 1$, pelo teorema de Bachet-Bézout (5.8), existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Logo, $a \cdot cx + (bc) \cdot y = c$. Do fato de a dividir cada termo do lado esquerdo, temos que $a \mid c$. □

5.4 Congruência Modular

Um dos tópicos da Teoria dos Números, a aritmética dos restos, denominada de Aritmética Modular, foi introduzida por Gauss, no ano de 1801, em seu livro *Disquisitiones Arithmeticae*, sendo a ideia de congruência um dos conceitos envolvidos nos estudos dessa área. Além disso, também credita-se a Gauss a criação da simbologia utilizada nesta teoria. Segundo Barbosa Junior (2013, p. 26), este ramo da aritmética "tornou-se uma importante ferramenta nas resoluções de problemas que estão associados a fatos periódicos".

Definição 5.11 (Congruência modular)**.** *Sejam **a** e **b** inteiros quaisquer e seja **m** > 1 um inteiro positivo fixo. Diz-se que **a** é congruente a **b** módulo **m**, representado por $a \equiv b \ (mod\, m)$, se, e somente se, **m** divide a diferença $a - b$. Em outros termos, **a** é congruente a **b** módulo **m** se, e somente se, existe um inteiro **k** tal que $a - b = km$.*

Definição 5.12 (Congruência linear)**.** *Sejam $a, b, m, x \in \mathbb{Z}$, com $m > 1$. Chamamos de congruência linear módulo m toda congruência da forma*

$$ax \equiv b \ (mod\, m).$$

Além disso, um inteiro x_0 é chamado uma solução da congruência, caso $ax_0 \equiv b \ (mod\, M)$.

Por exemplo, $x_0 = 15$ é uma solução da congruência $3x \equiv 5 \ (mod\ 8)$, pois $45 \equiv 5 \ (mod\, 8)$.

A seguir, apresentamos algumas propriedades das congruências.

Proposição 5.13. [12] *Para quaisquer $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$, temos:*

1. *(Reflexividade) $a \equiv a\ (mod\ m)$;*

2. *(Simetria) se $a \equiv b\ (mod\ m)$, então $b \equiv a\ (mod\ m)$;*

3. *(Transitividade) se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então $a \equiv c\ (mod\ m)$;*

4. *(Compatibilidade com a soma e diferença) Podemos somar e subtrair "membro a membro":*
$$\begin{cases} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d\ (mod\ m) \\ a - c \equiv b - d\ (mod\ m) \end{cases}$$
Em particular, se $a \equiv b\ (mod\ m)$, então $ka \equiv kb\ (mod\ m)$ para todo $k \in \mathbb{Z}$.

5. *(Compatibilidade com o produto) Podemos multiplicar "membro a membro":*
$$\begin{cases} a \equiv b\ (mod\ m) \\ c \equiv d\ (mod\ m) \end{cases} \Rightarrow ac \equiv bd\ (mod\ m)$$
Em particular, se $a \equiv b\ (mod\ m)$, então $a^k \equiv b^k\ (mod\ m)$ para todo $k \in \mathbb{Z}$.

6. *(Cancelamento) Se $mdc(c, m) = 1$, então*
$$ac \equiv bc\ (mod\ m) \Leftrightarrow a \equiv b\ (mod\ m).$$

***Demonstração**.* Para o item *(1)* basta observar que $m \mid a - a = 0$.

Em *(2)*, se $m \mid a - b$, então $m \mid -(a - b) \Leftrightarrow m \mid b - a$.

Em *(3)*, se $m \mid a - b$ e $m \mid b - c$, então, pelo item *(i)* do lema 5.4, $m \mid (a - b) + (b - c)$. Logo, $m \mid a - b + b - c$ e, portanto, $m \mid a - c$.

Em *(4)* e *(5)*, se $m \mid a - b$ e $m \mid c - d$, então $m \mid (a - b) + (c - d) \Leftrightarrow m \mid (a+c)-(b+d)$, $m \mid (a-b)-(c-d) \Leftrightarrow m \mid (a-c)-(b-d)$ e $m \mid (a-b)c+(c-d)b \Leftrightarrow m \mid ac-bd$.

Finalmente, como $mdc(c, m) = 1$, temos que $m \mid ac-bc \leftrightarrow m \mid a-b$, pela proposição 5.10. □

[12] MARTINEZ *et al.*, 2013, p. 34

5.5 Teorema Chinês dos Restos

Teorema 5.14 (Teorema Chinês dos Restos - *versão fraca*)**.** *Dados dois inteiros $m_1, m_2 \geq 2$, primos entre si (isto é, $mdc(m_1, m_2) = 1$), e dados outros dois inteiros quaisquer a_1, a_2, o sistema*

$$\begin{cases} x \equiv a_1 \ (mod\, m_1) \\ x \equiv a_2 \ (mod\, m_2) \end{cases}$$

possui uma solução $x = x_0$. Além disso, um inteiro x é solução do sistema se, e somente se,

$$x \equiv x_0 \ (mod\, m_1 m_2).$$

Tal solução será obtida na forma:

$$x_0 = M_1 x_1 a_1 + M_2 x_2 a_2,$$

em que $M_i = \frac{M}{m_i}$ e x_i é solução de $M_i X \equiv 1 \ (mod\, M_i)$, $i \in \{1, 2\}$.

Demonstração. A primeira parte da demonstração é verificar que *existe* pelo menos uma solução para o sistema

$$\begin{cases} x \equiv a_1 \ (mod\, m_1) \\ x \equiv a_2 \ (mod\, m_2) \end{cases}$$

Sabemos que, um inteiro x satisfaz o sistema acima se, e somente se, existirem $y_1, y_2 \in \mathbb{Z}$ tais que

$$x = m_1 y_1 + a_1 \tag{5.1}$$

$$x = m_2 y_2 + a_2 \tag{5.2}$$

Subtraindo essas equações e reordenando seus termos, temos

$$m_1 y_1 - m_2 y_2 = a_2 - a_1 \tag{5.3}$$

Então, como $mdc(m_1, m_2) = 1$, pelo Teorema de Bachet-Bézout (5.8) e pelo Lema 5.9 sabemos que a equação acima possui alguma solução $(y_1, y_2) \in \mathbb{Z}^2$. Fixando uma solução arbitrária, definimos $x = x_0$ pela equação (5.1) e, usando a equação (5.3), verificamos que a equação (5.2) também é válida. Portanto, este $x = x_0$ é uma solução do sistema.

Agora que encontramos uma solução x_0, vamos provar que qualquer $x \equiv x_0 \ (mod\, m_1 m_2)$ também é solução do sistema. De fato,

$$x = x_0 + k m_1 m_2 \ \Rightarrow \ x \equiv x_0 \ (mod\, m_1) \quad e \quad x \equiv x_0 \ (mod\, m_2).$$

Finalmente, vamos demonstrar que todas as soluções do sistema são da forma $x \equiv x_0\ (mod\ m_1m_2)$. Supondo um inteiro x solução do sistema, como x_0 também é solução, temos que $y = x - x_0$ satisfaz

$$y \equiv a_1 - a_1 \equiv 0\ (mod\, m_1) \tag{5.4}$$

$$y \equiv a_2 - a_2 \equiv 0\ (mod\, m_2) \tag{5.5}$$

Pela equação (5.4), temos que m_1 divide y, ou seja, existe um inteiro q tal que $y = qm_1$. De maneira análoga, por (5.5) temos que m_2 divide $y = qm_1$. Como m_1 e m_2 são primos entre si, m_2 divide q e, com isso, existe $k \in \mathbb{Z}$ tal que $q = km_2$. Portanto, $y = km_1m_2 \equiv 0\ (mod\, m_1m_2)$, ou seja, $x \equiv x_0\ (mod\, m_1m_2)$, como queríamos demonstrar. □

Essa versão do Teorema Chinês dos Restos, limitada a um sistema de apenas duas congruências lineares, também pode ser enunciada da seguinte forma:

Teorema 5.15 (Teorema Chinês dos Restos - *simplificado*)**.** *Sejam m e n dois inteiros positivos primos entre si. Dados inteiros i e j com $0 \leq i < m$ e $0 \leq j < n$, existe exatamente um inteiro a, com $0 \leq a < m \cdot n$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j.*

Contudo, nos casos em que o sistema possui mais de duas congruências lineares, essa versão do teorema se mostra insuficiente. Assim, é necessário utilizar a versão completa do Teorema Chinês dos Restos, também chamada de *versão forte*, que expande a aplicação do teorema para sistemas que contém um número finito, porém ilimitado de congruências.

Teorema 5.16 (Teorema Chinês dos Restos - *versão forte*)**.** *Sejam $m_1, \cdots m_k$ inteiros ≥ 2, dois a dois primos entre si (isto é, $mdc(m_i, m_j) = 1$, para $i \neq j$), e sejam $a_1, \cdots, a_k \in \mathbb{Z}$. Assim, o sistema*

$$\begin{cases} x \equiv a_1\ (mod\, m_1) \\ x \equiv a_2\ (mod\, m_2) \\ \vdots \\ x \equiv a_k\ (mod\, m_k) \end{cases}$$

possui uma solução $x = x_0$. Além disso, um inteiro x é solução do sistema se, e somente se,

$$x \equiv x_0\ (mod\ M),$$

com $M = m_1m_2 \cdots m_k$.

Tal solução será obtida na forma:

$$x_0 = M_1x_1a_1 + M_2x_2a_2 + \cdots + M_kx_ka_k,$$

em que $M_i = \frac{M}{m_i}$ e x_i é solução de $M_iX \equiv 1\ (mod\ M_i)$, $i = 1, \cdots, k$.

Demonstração. Queremos provar que o TCR também é válido para mais de duas equações. Como o teorema já foi demonstrado para 2 equações, vamos provar por indução, que ele também vale para um número $k > 2$ de equações.

Suponha que o teorema vale para $k - 1$ equações. Dados $m_1, \cdots, m_k$ dois a dois primos entre si, e $a_1, \cdots, a_k$ inteiros quaisquer. Consideremos o sistema formado apenas pelas $k - 1$ primeiras equações

$$\begin{cases} x \equiv a_1 \ (mod\, m_1) \\ x \equiv a_2 \ (mod\, m_2) \\ x \equiv a_3 \ (mod\, m_3) \\ \vdots \\ x \equiv a_{k-1} \ (mod\, m_{k-1}) \end{cases}$$

Pela hipótese de indução, existe um inteiro b tal que este subsistema é equivalente a uma única equação

$$x \equiv b \ (mod\, M), \quad onde \ \ M = m_1 \cdots m_{k-1}.$$

Portanto, o sistema formado com k equações é equivalente ao sistema

$$\begin{cases} x \equiv b \ (mod\, M) \\ x \equiv a_k \ (mod\, m_k) \end{cases}$$

Sabendo que M e m_k são primos entre si e que o TCR vale para duas equações, temos que existe uma solução x_0 para o sistema acima. Além disso, um x será solução do sistema se, e somente se, $x \equiv x_0 \ (mod\ M \cdot m_k)$. Como $M \cdot m_k = m_1 \cdot ... \cdot m_{k-1} m_k$, a demonstração está concluída. $\square$

Prova dinâmica do Teorema Chinês dos Restos. [13] Sejam m_1 e m_2 inteiros ≥ 2 quaisquer. Considere um retângulo de lados m_1 e m_2, dividido em quadrados 1x1. Cada quadrado é descrito por coordenadas (x, y) onde x e y são inteiros com $0 \leq x \leq m_1 - 1$ e $0 \leq y \leq m_2 - 1$; veja a Figura 3.1. Considere o seguinte passeio no retângulo:

- No tempo $t = 0$ começamos no quadrado $(0, 0)$.
- Se no tempo (inteiro não-negativo) t estamos no quadrado $(x(t), y(t))$, então no tempo $t+1$ pulamos para o quadrado $(x(t+1), y(t+1))$ no retângulo m_1xm_2, cujas coordenadas satisfazem

$$x(t+1) \equiv x(t) + 1 \ (mod\, m_1) \ \text{ e } \ y(t+1) \equiv y(t) + 1 \ (mod\, m_2).$$

[13] BOCHI, 2009, p. 3

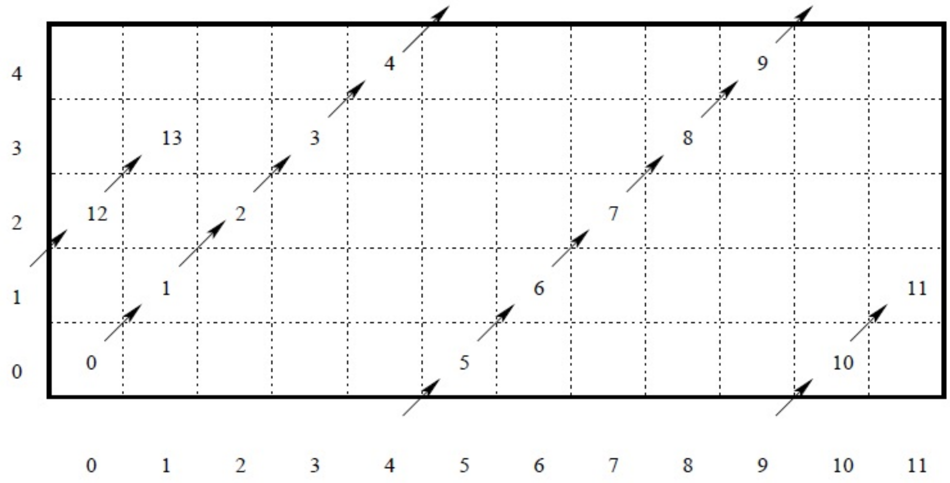

Figura 5.1: Passeio no retângulo 12x5. No tempo $t = 13$ estamos no quadrado $(1, 3)$

Equivalentemente, $x(t) \equiv t\ (mod\, m_1)$ e $y(t) \equiv t\ (mod\, m_2)$. Quando retornamos pela primeira vez ao quadrado $(0, 0)$? Isso acontece no menor tempo t que é congruente a 0 módulo m_1 e m_2, isto é, no mínimo múltiplo comum de m_1 e m_2. Chamemos $p = mmc(m_1, m_2)$ e observe, também, que o tempo $t = p$ é a primeira vez que visitamos um quadrado que já tinha sido visitado antes. (Isso acontece pois não há dois quadrados diferentes que pulem para um mesmo quadrado.) A partir do tempo p, visitaremos os mesmos quadrados de novo, e na mesma ordem. Além disso, cada um desses quadrados é visitado periodicamente uma vez a cada p unidades de tempo.

No caso em que m_1 e m_2 são primos entre si, temos $p = m_1m_2$. Mas esse é o número total de quadrados no retângulo; portanto visitaremos todos os quadrados. Isto prova o Teorema Chinês dos Restos: dados quaisquer x_0, y_0, o sistema $t \equiv x_0\ (mod\ m_1)$ e $t \equiv y_0\ (mod\ m_2)$ tem uma solução t_0, e as outras soluções são exatamente os t tais que $t \equiv t_0\ (mod\, p)$. Podemos pensar que o passeio se estende indefinidamente no passado para incluir t negativos. $\square$

Caso m_1 e m_2 não sejam primos entre si, temos $p < m_1m_2$ e, portanto, alguns quadrados jamais serão visitados.

Para atingir o objetivo central desse trabalho – desenvolver alguns dos conceitos de Aritmética Modular na Educação Básica, por meio da proposta de algumas atividades que possibilitassem essa compreensão pelos alunos – buscamos selecionar as metodologias de ensino e de pesquisa que mais se adequaram à essa proposta, na aplicação das atividades e na realização da pesquisa, as quais serão apresentadas no próximo capítulo.

6 PROCEDIMENTOS METODOLÓGICOS

De modo geral, observa-se que a forma como a Matemática é ensinada, em particular na Educação Básica, tende a perpetuar um modelo tradicionalista, não buscando acompanhar a evolução sociocultural e tecnológica da sociedade. Na tentativa de melhorar esse processo de ensino e aprendizagem da Matemática, surgiram algumas novas propostas metodológicas, dentre as quais escolhemos a Resolução de Problemas e a Investigação Matemática, que, em virtude dos objetivos do presente trabalho e das características do PROFMAT, consideramos as mais adequadas, pois permitem que os alunos participem mais ativamente do desenvolvimento das atividades, buscando soluções para os problemas sem a interferência direta do professor e, com isso, possibilitando uma compreensão mais prática dos conceitos da Aritmética Modular.

6.1 Resolução de Problemas

Historicamente o professor de Matemática tende, ao desenvolver determinado problema ou atividade em sala de aula, a se limitar à ideia de que o mesmo possui apenas uma solução, ou seja, pode ser resolvido seguindo apenas um método. Porém, ao trabalharmos com problemas que apresentam diversas soluções é possível analisar mais a fundo os conhecimentos que os alunos já possuem, auxiliando na compreensão dos novos conteúdos que estão sendo trabalhados, e sua capacidade de interpretar matematicamente as mais diversas situações propostas.

De acordo com D'Ambrosio (1989, p. 17), a resolução de problemas

> [...] visa a construção de conceitos matemáticos pelo aluno através de situações que estimulam a sua curiosidade matemática. Através de suas experiências com problemas de naturezas diferentes o aluno interpreta o fenômeno matemático e procura explicá-lo dentro de sua concepção da matemática envolvida.

Também podemos observar a contribuição de Poffo (2011, p. 3), ao afirmar que

> [...] a resolução de problemas consiste em permitir que os alunos utilizem seus conhecimentos e desenvolvam a capacidade de administrar as informações ao seu redor. Dessa forma, os alunos adquirem a oportunidade de ampliar seu conhecimento, desenvolver seu raciocínio lógico, enfrentar novas situações e conhecer as aplicações da matemática.

Desse modo, o aluno deixa de ser apenas um ouvinte passivo diante da simples apresentação do conteúdo e passa a envolver-se ativamente na criação dos conceitos matemáticos através da formulação de hipóteses, baseadas em seus conhecimentos anteriores e de suas observações em relação ao problema proposto.

Com isso, o professor fica diante de uma sala de aula formada por alunos que buscam conhecimentos através de abordagens diferentes, alguns procuram uma solução direta e simples, enquanto outros trabalham analisando várias soluções. Esta diferença de visão talvez possa justificar, em parte, o fato de alguns alunos afirmarem que um problema simples é um problema complexo.

Segundo Polya (1978 *apud* FLEMMING; LUZ; MELLO, 2005, p. 73), o processo de resolução de problemas pode ser realizado através de questionamentos e sugestões, e baseado em quatro etapas:

> Primeiro, temos de **compreender** o problema, temos de perceber claramente o que é necessário. Segundo, temos de ver como os diversos itens estão inter-relacionados, como a incógnita está ligada aos dados, para termos a idéia (sic.) da resolução, para estabelecermos um **plano**. Terceiro, **executamos** o nosso plano. Quarto, fazemos um **retrospecto** da resolução completa, revendo-a e discutindo-a. [Grifos no original]

De acordo com a descrição acima, podemos perceber que a estratégia proposta por Polya se baseia no processo de interação entre professor-aluno e aluno-aluno. Assim, além de promover um amadurecimento acadêmico e pessoal de cada aluno, também acarreta um maior desenvolvimento do professor que precisa agir como mediador e incentivador de seus educandos, proporcionando uma melhor qualidade de aprendizagem para todos os envolvidos e um maior desenvolvimento da capacidade de trabalhar em equipe, ou seja, de desenvolver tarefas em conjunto através do compartilhamento de conhecimentos visando um objetivo comum, sendo neste caso encontrar métodos de solucionar o problema.

Conforme consta nos Parâmetros Curriculares Nacionais (BRASIL, 1998, p. 40),

> a prática mais frequente na Resolução de Problemas, consiste em ensinar um conceito, um procedimento ou técnica e depois apresentar um problema para avaliar se os alunos são capazes de empregar o que lhes foi ensinado. Para a maioria dos alunos, resolver um problema significa fazer cálculos com números do enunciado ou aplicar algo que aprendam nas aulas. Desse modo o que o professor explora na atividade matemática não é mais a atividade, ela mesma, mas seus resultados, técnicas e demonstrações.

Com isso podemos perceber que, segundo Onuchic (1999), o foco central do ensino da matemática não deve estar em encontrar a solução dos problemas propostos e, para isso, a função da resolução de problemas no currículo seria um caminho do aluno obter novos conhecimentos e aperfeiçoar aqueles que este já possui, ou seja, o principal objetivo do ensino deve ser compreender, para assim adquirir um novo conhecimento ou processo através do qual pode ser aplicado tudo aquilo que previamente havia sido desenvolvido.

6.2 INVESTIGAÇÃO MATEMÁTICA

De acordo com os Parâmetros Curriculares Nacionais (BRASIL, 1998, p. 27), a sociedade atual exige “trabalhadores mais criativos e versáteis, capazes de entender o processo de trabalho como um todo, dotados de autonomia e iniciativa para resolver problemas em equipe e para utilizar diferentes tecnologias e linguagens”. Contudo, pode-se observar que, muitas vezes, o ensino da Matemática é baseado na repetição e treino de algoritmos, normalmente sem que os alunos possam refletir ou discutir sobre suas regras e características, e utilizando situações-problema que desempenham o papel de simples exercício, visto que não se mostram desafiadoras aos alunos e não possibilitam que estes busquem diferentes estratégias de resolução.

Na maioria dos casos, as aulas de Matemática, principalmente na Educação Básica, estão voltadas para a resolução de problemas e exercícios, os quais são diferentes em sua definição, sendo que, de acordo com Bertini e Passos (2008, p. 2), “um problema é uma questão para a qual o aluno não dispõe de um método imediato de resolução. Já um exercício pode ser resolvido usando um método ou algoritmo já conhecido”. Porém, em ambos os casos, o enunciado define de maneira clara os dados que são fornecidos e o que se espera encontrar, ou seja, o problema ou exercício, mesmo que permita formas diferentes de resolução, possui uma resposta única e fechada.

Neste ponto encontra-se a principal diferença na utilização da investigação como metodologia de ensino de Matemática: nela o aluno parte de uma situação aberta, não completamente definida ou com apenas uma única resposta correta, o que possibilita a construção de diversos conhecimentos no decorrer do processo de investigação, até mesmo alguns não previstos pelo professor ao propor a atividade.

Segundo Ponte, Brocardo e Oliveira (2003 *apud* DICK *et al.*, 2014, p. 8),

> desenvolver o ensino e a aprendizagem da Matemática utilizando a investigação significa considerar ou elaborar questões relacionadas a essa área do conhecimento e para as quais a pessoa que investiga não dispõe de uma resolução imediata, com o objetivo de que se sinta motivada a procurá-la, valendo-se dos conhecimentos prévios matemáticos e lógicos necessários.

Ainda de acordo com Ponte, Brocardo e Oliveira (2003, p. 20), o desenvolvimento do processo de investigação matemática é dividido em quatro momentos:

> O primeiro abrange o reconhecimento da situação, a sua exploração preliminar e a formulação de questões. O segundo momento refere-se ao processo de formulação de conjecturas. O terceiro inclui a realização de testes e o eventual refinamento das conjecturas. E, finalmente, o último diz respeito à argumentação, à demonstração e à avaliação do trabalho realizado.

Com isso, o professor deixa de ser um simples “transmissor” de conteúdos, devendo proporcionar aos alunos um ambiente adequado para que possam investigar a situação proposta.

Nesse sentido, Skovsmose (2000, p. 6) afirma que "um cenário para investigação é aquele que convida os alunos a formularem questões e procurarem explicações", ou seja, o papel do professor passa a ser de organizar o ambiente, dar encaminhamento às atividades, inserindo os conhecimentos e recursos que se mostrem necessários no decorrer do processo de investigação, buscando constantemente estimular a autonomia dos alunos na resolução das questões.

6.3 Caracterização da pesquisa

Dentro do universo das Ciências, a pesquisa possui papel central, sendo o elo de ligação entre as conjecturas criadas e a realidade a ser investigada. Segundo Gil (2007, p. 17), pesquisa é definida como o

> (...) procedimento racional e sistemático que tem como objetivo proporcionar respostas aos problemas que são propostos. A pesquisa desenvolve-se por um processo constituído de várias fases, desde a formulação do problema até a apresentação e discussão dos resultados.

De modo semelhante, Lehfeld (1991 *apud* GERHARDT; SILVEIRA, 2009, p. 31) define a pesquisa como "a inquisição, o procedimento sistemático e intensivo, que tem por objetivo descobrir e interpretar os fatos que estão inseridos em uma determinada realidade".

Dentro desse contexto, a pesquisa científica pode ser classificada, quanto à sua abordagem, em pesquisa qualitativa e pesquisa quantitativa. Para o presente trabalho, vamos nos focar em apresentar as principais características e conceitos que permeiam a pesquisa qualitativa, abordagem que foi escolhida para direcionar a pesquisa realizada.

A pesquisa qualitativa busca analisar de forma descritiva o fenômeno ou o meio que está sendo observado, não se preocupando em quantificar numericamente os resultados. De acordo com Gerhardt e Silveira (2009), os pesquisadores que utilizam a pesquisa qualitativa buscam encontrar respostas não quantificáveis, as razões que levam à determinada situação, buscando apresentar soluções ou ideias que possam modificar positivamente o meio estudado. Os dados obtidos com esse tipo de pesquisa não seguem um padrão métrico, sendo resultados da interação do pesquisador com o objeto, por meio de diferentes abordagens e, não necessariamente utilizando instrumentos formais e estruturados para sua captura.

> Na pesquisa qualitativa, o cientista é ao mesmo tempo o sujeito e o objeto de suas pesquisas. O desenvolvimento da pesquisa é imprevisível. O conhecimento do pesquisador é parcial e limitado. O objetivo da amostra é de produzir informações aprofundadas e ilustrativas: seja ela pequena ou grande, o que importa é que ela seja capaz de produzir novas informações (DESLAURIERS, 1991 *apud* GERHARDT; SILVEIRA, 2009, p. 32).

Dessa forma, a pesquisa qualitativa foca-se nos aspectos da realidade que não podem ser quantificados, aspectos subjetivos nas relações sociais, sendo criticada, principalmente, em razão dessa subjetividade na obtenção das informações e na possibilidade de envolvimento emocional do pesquisador (MINAYO, 2001).

Segundo Gerhardt e Silveira (2009, p. 32), as características da pesquisa qualitativa são:

> objetivação do fenômeno; hierarquização das ações de descrever, compreender, explicar, precisão das relações entre o global e o local em determinado fenômeno; observância das diferenças entre o mundo social e o mundo natural; respeito ao caráter interativo entre os objetivos buscados pelos investigadores, suas orientações teóricas e seus dados empíricos; busca de resultados os mais fidedignos possíveis; oposição ao pressuposto que defende um modelo único de pesquisa para todas as ciências.

Contudo, ao se utilizar desses métodos qualitativos em sua pesquisa, o pesquisador deve atuar de maneira consciente, evitando exercer demasiada influência sobre os objetos estudados, podendo causar alterações nos resultados finais. O pesquisador, também, deve estar ciente de detalhar bem a forma como a pesquisa foi desenvolvida, em razão da falta de ferramentas padronizadas para a coleta e análise dos dados.

Nesse contexto, acreditamos que a pesquisa desenvolvida neste trabalho se enquadra no modelo qualitativo por não estar focada apenas no ensino dos conteúdos da Aritmética Modular, mas sim em observar os caminhos seguidos pelos alunos durante a sua realização. Ao aplicar as atividades, buscou-se analisar o comportamento do estudante ao se deparar com os conceitos apresentados, observar sua capacidade de lidar com esse tipo de problemas e sua maturidade intelectual para buscar soluções dentro do conjunto de conhecimentos que já possuía.

A pesquisa foi realizada por meio da aplicação de atividades, adaptadas e elaboradas por nós, a uma turma de 19 alunos da 2ª série do Ensino Médio de um colégio particular do norte do Paraná. Para podermos utilizar os dados obtidos com a aplicação, foi encaminhado aos responsáveis de cada um dos alunos o Termo de Consentimento Livre e Esclarecido, no qual foram explicados os objetivos, métodos e resultados que esperávamos obter com a pesquisa.

No decorrer deste trabalho, em razão do sigilo dos nomes reais dos participantes da pesquisa, cada aluno será identificado por uma letra do alfabeto latino. Também justificamos, previamente, a ausência do material escrito produzido por alguns alunos nos exemplos apresentados, pois, como as atividades foram realizadas em grupos, algumas resoluções e observações ficaram iguais. Assim, acreditamos não ser interessante inseri-las no corpo do trabalho.

A opção por não aplicar as atividades em uma instituição de ensino pública ocorreu, principalmente, devido às turmas do Ensino Médio possuírem apenas duas aulas de Matemática semanais, o que dificultou que as coordenações disponibilizassem o tempo necessário para realizar a pesquisa, pois como o tema não está incluído no currículo normal, o ensino dos conteúdos previstos poderia ser prejudicado. Também, em decorrência do período em que os professores das escolas estaduais estiveram em greve, na época em que a pesquisa seria realizada os colégios estavam realizando aulas de revisão e aplicando as provas trimestrais, impossibilitando a entrada do pesquisador em sala de aula para desenvolver a pesquisa.

Durante todo o processo, que teve uma duração de, aproximadamente, uma hora e trinta minutos, os alunos foram instigados a buscar formas de resolver as atividades com o conhecimento que já possuíam, o que se mostrou bastante efetivo em alguns dos problemas propostos. Além disso, buscou-se encaminhar o seu pensamento para que pudessem compreender os fatos relacionados à Aritmética Modular inerentes às atividades, que muitos perceberam, mesmo que não formalmente.

Na sequência, apresentamos as atividades que foram propostas, juntamente com a resolução e a análise dos resultados obtidos, a qual será fundamentada nos conceitos que envolvem o pensamento aritmético e algébrico (capítulo 4), e as metodologias de ensino e pesquisa utilizadas (capítulo 6).

7 ATIVIDADES PROPOSTAS E RESULTADOS

7.1 Problema 1 - Descobrir o dia da semana

A copa do mundo de futebol foi realizada no Brasil no ano de 2014. O jogo de abertura ocorreu no dia 12 de junho. Supondo que não haja um calendário em mãos, e sabendo que o dia 1º de janeiro de 2014 foi uma quarta-feira, determine em que dia da semana ocorreu o jogo de abertura.[1]

Tabela 7.1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

7.1.1 Sugestão de resposta

Primeiramente podemos determinar quantos dias se passaram do início do ano até o dia 12 de junho. Para isso, basta somarmos os dias dos meses de Janeiro à Maio e os 12 dias de Junho:

$$31 + 28 + 31 + 30 + 31 + 12 = 163$$

Assim, temos que a abertura ocorreu no 163º dia do ano de 2014.

Agora vamos pensar em como esses dias estarão relacionados com os dias da semana. Para tentar observar isso, podemos construir uma tabela com os primeiros dias de Janeiro:

Tabela 7.2: Primeiros dias de Janeiro

QUA	QUI	SEX	SAB	DOM	SEG	TER
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

Vamos observar quais dias se relacionam com cada dia da semana:

- Terça-feira: 7, 14, 21, 28, ... são múltiplos de 7, ou seja, quando divididos por 7 deixam resto igual a 0 ($7n$, com $n \in \mathbb{N}$).
- Quarta-feira: 1, 8, 15, 22, ... são múltiplos de 7, mais 1, ou seja, quando divididos por 7 deixam resto igual a 1 ($7n + 1$, com $n \in \mathbb{N}$).

[1] BARROS, 2014

- Quinta-feira: 2, 9, 16, 23, ... são múltiplos de 7, mais 2, ou seja, quando divididos por 7 deixam resto igual a 2 ($7n + 2$, com $n \in \mathbb{N}$).
- Sexta-feira: 3, 10, 17, 24, ... são múltiplos de 7, mais 3, ou seja, quando divididos por 7 deixam resto igual a 3 ($7n + 3$, com $n \in \mathbb{N}$).
- Sábado: 4, 11, 18, 25, ... são múltiplos de 7, mais 4, ou seja, quando divididos por 7 deixam resto igual a 4 ($7n + 4$, com $n \in \mathbb{N}$).
- Domingo: 5, 12, 19, 26, ... são múltiplos de 7, mais 5, ou seja, quando divididos por 7 deixam resto igual a 5 ($7n + 5$, com $n \in \mathbb{N}$).
- Segunda-feira: 6, 13, 20, 27, ... são múltiplos de 7, mais 6, ou seja, quando divididos por 7 deixam resto igual a 6 ($7n + 6$, com $n \in \mathbb{N}$).

Assim, se continuarmos colocando os dias na tabela até o 163º, vamos descobrir em qual dia da semana caiu o dia 12 de junho. Porém, como temos 7 opções para o dia cair na semana, podemos agilizar o processo dividindo 163 por 7 e verificando qual o resto dessa divisão.

Efetuando a divisão de 163 por 7, obtemos quociente 23 e resto 2, ou seja: $163 = 7 \cdot 23 + 2$.

Portanto, a abertura da copa do mundo ocorreu em uma **quinta-feira**.

7.1.2 Análise da resolução dos alunos

O objetivo principal dessa atividade era permitir que os alunos percebessem que a resposta não seria encontrada no resultado "normal" das operações, mas sim na análise dos restos obtidos, proporcionando esse primeiro contato com o pensamento básico da Aritmética Modular. Para isso, foi utilizada a metodologia de Resolução de Problemas no desenvolvimento dessa primeira atividade, permitindo que os alunos buscassem a solução por meio dos conhecimentos que já possuíam.

Para a resolução, foi permitido que os alunos compartilhassem ideias entre si, o que proporcionou um momento interessante de troca de conhecimentos e debate acerca das melhores formas de resolver os problemas. Todo esse processo foi acompanhado pelo responsável pela pesquisa, o qual deu liberdade aos alunos apresentarem suas resoluções, orientando nos pontos onde houve dúvidas.

Nesse primeiro momento, foi possível observar que a grande maioria dos alunos conseguiu encontrar a resposta de maneiras similares a que se esperava. Alguns alunos buscaram analisar o que ocorria no primeiro e último dia de cada mês, até chegar no final de maio, para assim encontrar o dia da semana em que caiu o dia 12 de junho.

Essa maneira também estava correta, sendo que apenas a aluna C encontrou a resposta incorreta pois errou ao iniciar sua tabela na segunda semana, ao colocar que a quarta-feira seguinte seria dia 07/01 e não dia 08/01. Contudo, os alunos que seguiram essa linha de raciocínio tiveram maior dificuldade em conseguir perceber a ideia dos restos, inerente a esse problema.

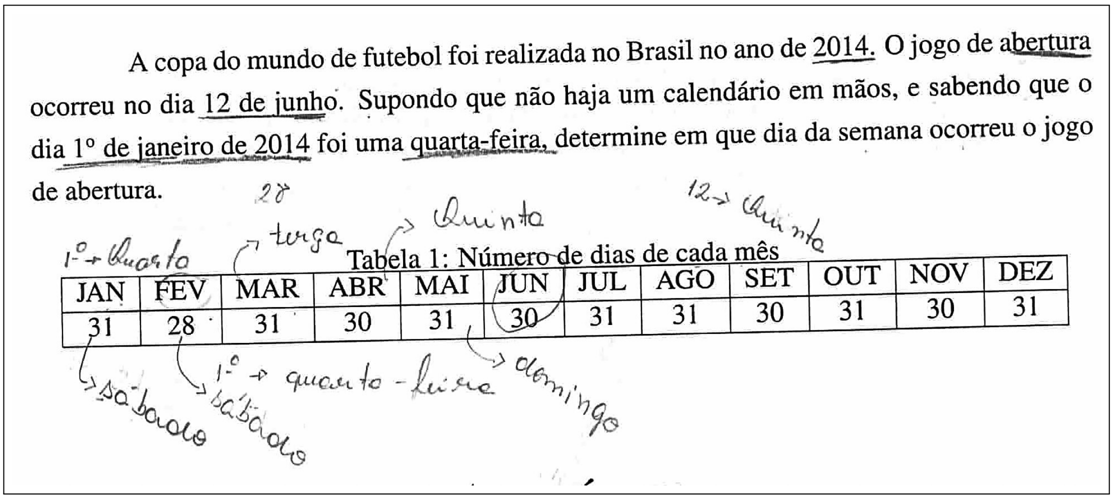
A copa do mundo de futebol foi realizada no Brasil no ano de 2014. O jogo de abertura ocorreu no dia 12 de junho. Supondo que não haja um calendário em mãos, e sabendo que o dia 1º de janeiro de 2014 foi uma quarta-feira, determine em que dia da semana ocorreu o jogo de abertura.

Tabela 1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

Figura 7.1: Resposta da aluna A para o problema 1

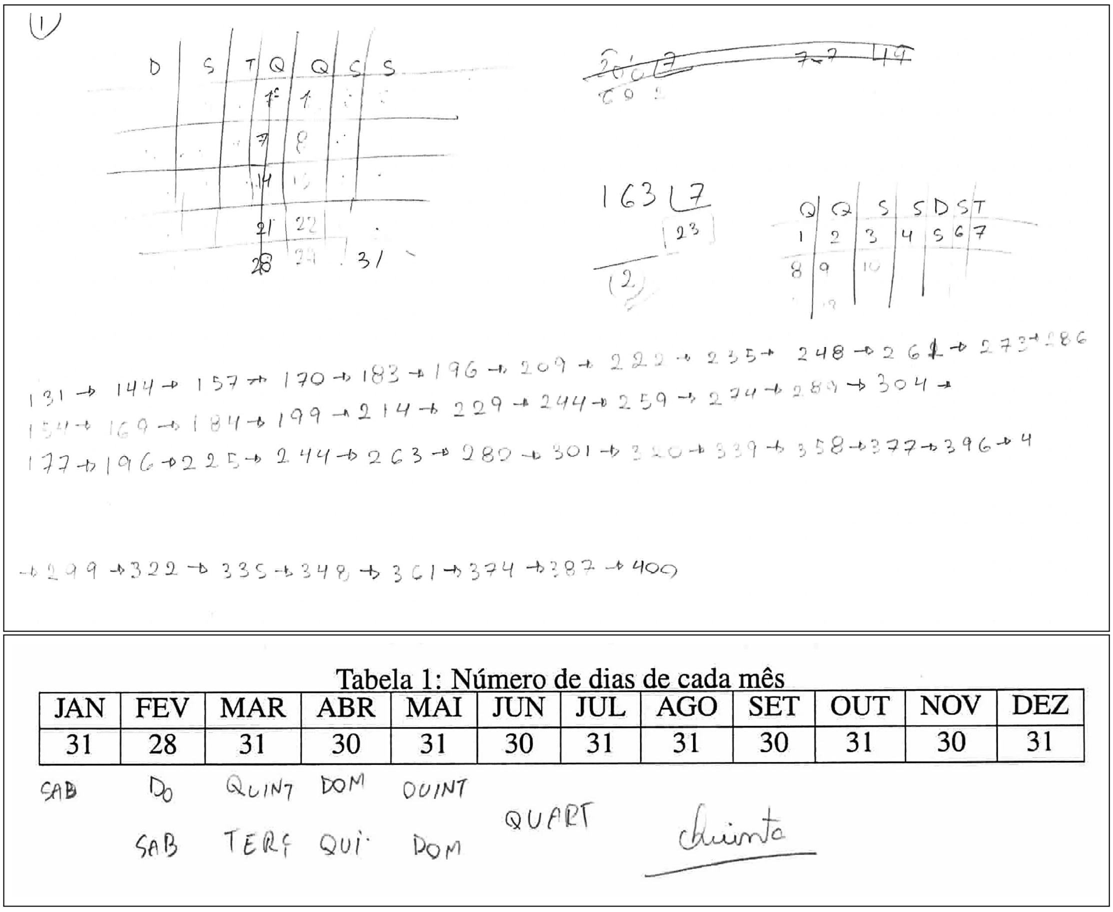
Tabela 1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

Figura 7.2: Resposta da aluna C para o problema 1

Enquanto isso, outros alunos utilizaram o raciocínio de somar a quantidade de dias de cada mês até maio e os doze dias de junho, para encontrar quantos dias haviam se passado entre o dia 01 de janeiro e 12 de junho. Em seguida, dividiram o resultado por 7 e obtiveram o número de semanas completas, 23, e também um resto 2. Como o dia 01 de janeiro foi uma quarta-feira, a análise das semanas estava sendo feita de quarta a terça-feira. Portanto, como o resto obtido foi 2, encontraram que o dia da semana em que caiu o dia 12 de junho foi uma quinta-feira.

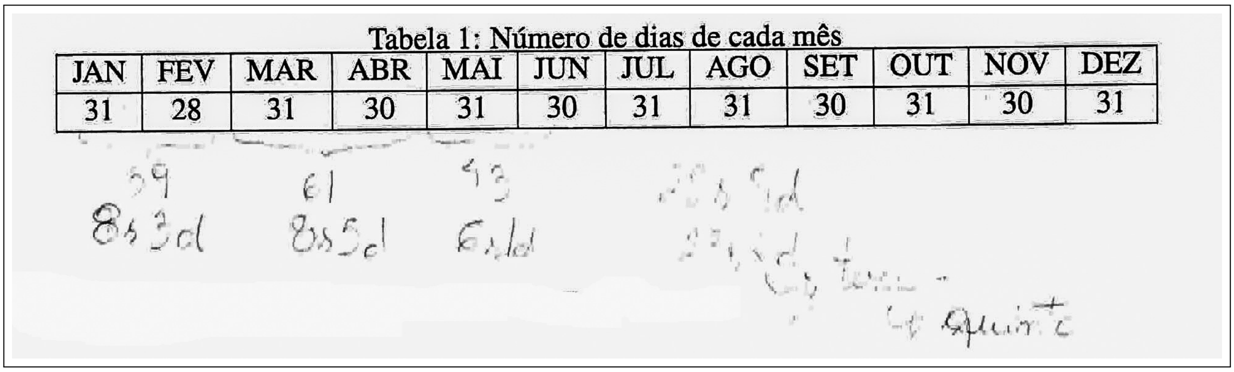
Tabela 1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

Figura 7.3: Resposta do aluno E para o problema 1

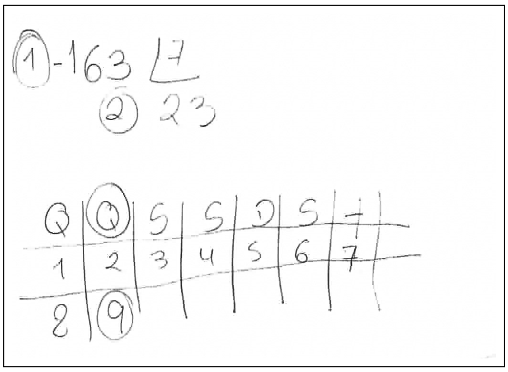

Figura 7.4: Resposta do aluno B para o problema 1

Esse era o ponto chave desta atividade: os alunos perceberem que não importava quantas semanas completas fossem encontradas, mas sim que a resposta para o problema estava no resto da divisão do número de dias por 7. Com isso, seria possível que, sabendo o dia em que caiu um dos dias do ano, encontrassem qualquer outro.

Dessa forma, foi possível perceber como pode ser interessante para o professor desenvolver problemas que envolvem conceitos de Aritmética Modular, mesmo que sejam os mais básicos como a ideia de trabalhar com os restos. Os alunos demonstraram um grande interesse no problema, por se tratar de um tema que fez parte de seu cotidiano e por se mostrar um desafio, diferente de grande parte dos problemas que integram os materiais didáticos na Educação Básica.

Isso reforça o que já foi comentado anteriormente sobre a relevância de trabalhar tópicos de Aritmética Modular na Educação Básica, pois estes possibilitam ao professor

> estimular nos alunos o interesse pela Matemática, aprimorando o raciocínio lógico e ampliando a compreensão dos conceitos básicos para o refinamento do pensamento aritmético e algébrico, fazendo com que os mesmos desenvolvam a capacidade de manipular conceitos e propriedades de forma clara e objetiva. (GROENWALD, 2010, p. 2).

Um dos alunos, inclusive, realizou uma mudança curiosa no problema para sua resolução: ele mudou o dia 01 de janeiro para um domingo e realizou toda a análise a partir desse dia. Ao encontrar a resposta, uma segunda-feira, ele retornou a situação para os parâmetros iniciais, ou seja, acrescentou os três dias que havia diminuído anteriormente, obtendo a resposta correta, quinta-feira. Ao ser questionado sobre as razões que o levaram a fazer essa mudança, o aluno afirmou que, como estava acostumado a observar os dias da semana no calendário sempre iniciando pelo domingo, achou mais fácil fazer a análise dessa forma e deixar para "transformar" a resposta no final.

Nesse ponto, percebemos como o pensamento matemático de cada indivíduo se desenvolve de maneiras e em ritmos diferentes. No caso do aluno citado acima, observamos que o seu raciocínio para a resolução do problema foi análogo ao dos demais. Contudo, como é costume observar os dias da semana iniciando no domingo, ele sentiu a necessidade de fazer essa "mudança" no problema para conseguir compreender sua resolução.

Esse fato ilustra um problema que muitos alunos enfrentam na Educação Básica, em especial no início dos anos finais do Ensino Fundamental, quando iniciam a transição entre a aritmética e a álgebra. Alguns estudantes sentem dificuldade em realizar essa transição, não apenas devido a notação, na qual são utilizadas outros símbolos para representar incógnitas e variáveis numéricas, mas também em razão dessa nova forma de pensar a matemática de uma maneira mais generalizada. A dificuldade se encontra em perceber que diversas situações problemas, mesmo que aparentem ser diferentes, podem ser solucionadas de modo similar, ou seja, existem ferramentas de resolução que não são aplicáveis a apenas um problema. Um bom exemplo disso é o aluno aprender a resolver uma equação cuja incógnita é um x e, quando o professor apresenta uma outra equação semelhante, mas com uma incógnita y, o aluno não consegue perceber que o modo de resolver também é semelhante.

Dessa forma, fica evidente a necessidade de desenvolver a capacidade dos alunos de pensar aritmética e algebricamente, de modo que sejam capazes de perceber a matemática, não como um conjunto de problemas, fórmulas e equações, mas sim, como um conjunto de ferramentas que podem ser adaptadas e aplicadas às mais diversas situações.

Outra aluna, também, comentou que agora entendia o "segredo" de uma pessoa que apareceu em um programa de televisão que conseguia "adivinhar" o dia da semana de qualquer data que lhe perguntavam. Segundo suas palavras, "parecia mágica, ou que ele tinha decorado, mas era tudo Matemática!".

7.2 PROBLEMA 2 - DADO OS RESTOS, ENCONTRE O NÚMERO

O objetivo dessa atividade[2] foi possibilitar que os estudantes observassem, através da Investigação Matemática, as relações existentes entre os restos e os resultados encontrados, permitindo que compreendessem de maneira prática a versão mais simples do Teorema Chinês dos Restos, enunciado no teorema 5.15.

Para realizar a atividade, cada dupla de alunos recebeu um dado. Como o dado possui seis faces, cada vez que ele é jogado podemos obter como resultado o valor 1, 2, 3, 4, 5 ou 6. Assim, podemos tomar quaisquer números maiores que 6 de tal forma que os resultados dos lançamentos sempre serão menores que m e n.

No caso da atividade aplicada nessa pesquisa, foram definidos os valores $m = 7$ e $n = 8$, para reduzir a quantidade de números que os alunos precisariam analisar para verificar a existência e a unicidade do inteiro que procuravam.

Foi solicitado que os alunos seguissem os seguintes passos para realizar a atividade:

1º) Lance o dado algumas vezes e anote os resultados obtidos na tabela abaixo:

2º) Encontre um número inteiro a menor que $(m \cdot n = 56)$ de tal modo que quando dividirmos a por $m = 7$ vamos obter resto i e quando dividirmos a por $n = 8$ vamos obter resto j.

i	j	a

3º) O que você pôde observar em relação aos valores de a encontrados para cada lançamento?

7.2.1 Análise da resolução dos alunos

Dentre as três atividades propostas, esta foi a que mais possibilitou observar que os alunos no Ensino Médio já possuem uma maturidade de conhecimento matemático suficiente para compreender os conceitos que se buscava analisar.

Inicialmente, foi feita uma breve explicação sobre a atividade, sem apresentar diretamente os objetivos almejados. No decorrer da realização das tarefas, os alunos se mostraram muito participativos e, mesmo tendo algumas dúvidas no início em relação às etapas que deviam ser realizadas, todos conseguiram efetuar ao menos algumas etapas da atividade.

[2]Elaborada a partir de uma questão da Olimpíada Brasileira de Matemática de 2009.

Algumas observações que eles levantaram durante o processo se mostraram muito relevantes, sendo inclusive mais aprofundadas do que o esperado como resultados da atividade. Os alunos C e E, conforme as imagens abaixo, perceberam um padrão que ocorria na hora de descobrir o número a: após fazerem o teste e encontrarem um inteiro que satisfazia o que foi pedido para a divisão por 7, ao tentarem por 8 perceberam que não dava certo. Contudo, se adicionassem 7 a esse número, o resto na divisão por 8 diminuía 1 unidade. Assim, conseguiram encontrar mais facilmente os demais números, apenas acrescentando ou diminuindo 7 unidades ao primeiro número encontrado.

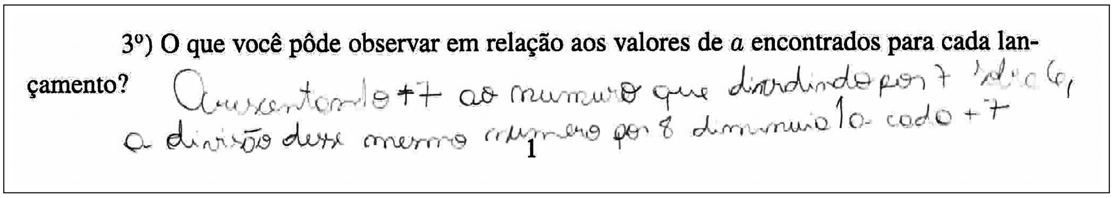

Figura 7.5: Resposta da aluna C para a letra c do problema 2

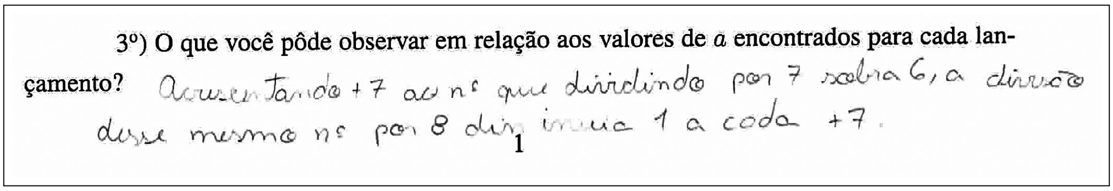

Figura 7.6: Resposta do aluno E para a letra c do problema 2

De maneira semelhante, o aluno D observou esse mesmo fato analisando a divisão por 8, percebendo que ocorria o inverso: quando acrescentava 8 unidades no número a encontrado, o resto da divisão desse a por 7 aumentava em 1 unidade.

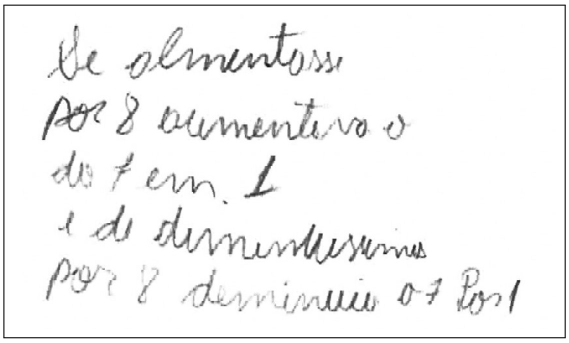

Figura 7.7: Resposta do aluno D para a letra c do problema 2

Essas observações demonstram que os alunos compreenderam a relação existente entre os restos das duas divisões, encontrando um padrão que se repetia para cada dupla de resultados obtidos nos lançamentos. Mesmo alguns alunos que não conseguiram observar esse ponto facilmente, por meio do auxílio dos demais colegas e do pesquisador, conseguiram perceber que, ao encontrar esse padrão, a resolução da tarefa ficava muito mais simples.

Alguns outros alunos, como é o caso do aluno B, explicitaram a relação existente entre as duas propriedades que o número a deveria possuir na forma de uma equação, o que demonstra uma forma de raciocínio lógico ainda mais maduro e adaptado a buscar “escrever matematicamente” o que compreenderam na linguagem escrita, facilitando a resolução de diversos problemas.

3º) O que você pôde observar em relação aos valores de a encontrados para cada lançamento? $7 \cdot n + 1 = 8 \cdot m + \gamma$

Figura 7.8: Resposta do aluno B para a letra c do problema 2

Nesse ponto, podemos observar aquilo que já foi afirmado por Lins e Gimenez (1997) e Boni e Savioli (2015), em relação à importância do desenvolvimento simultâneo do pensamento aritmético e algébrico dos estudantes, possibilitando que estes compreendam de maneira adequada os conceitos matemáticos, saibam interpretar aquilo que o problema está pedindo e, principalmente, “transcrever” isso que compreenderam para a “linguagem matemática”, ou seja, transcrever aquilo que perceberam por meio da análise aritmética do problema para a linguagem algébrica, por meio de símbolos e equações que exprimam o mesmo significado.

Isso se mostra fundamental na aprendizagem da Aritmética Modular, pois os alunos conseguiram observar esses conceitos de operações e relações com os restos da divisão euclidiana por meio de exemplos numéricos, mais fáceis de serem analisados, e, a partir disso, podem generalizar os resultados dos casos estudados e compreender como se dá a construção do conceito formal que buscamos apresentar.

7.3 Problema 3 - Encontro dos satélites

O objetivo dessa terceira atividade era apresentar aos alunos um problema que envolve diretamente o conceito de congruências modulares, até então desconhecido por eles, para verificar os métodos que poderiam utilizar para a sua resolução. Além disso, objetivou-se realizar a apresentação formal do Teorema Chinês dos Restos e, dentro das possibilidades, utilizá-lo para a resolução do problema.

Três satélites passarão sobre Londrina esta noite. O primeiro à 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra; o segundo, 15 horas e, o terceiro, 19 horas. Determine após quantas horas, a partir da meia-noite, os três satélites passarão ao mesmo tempo sobre Londrina.[3]

[3] COUTINHO, 1997, p. 116, *adaptado*

7.3.1 Sugestão de resposta

Podemos denotar de x_i o número de horas que se passaram, a partir da meia-noite. Sabe-se que o primeiro satélite passa a cada 13 horas, a contar da 1 da madrugada. Então podemos escrever essa informação na forma da equação $x_a = 13a + 1$, para algum inteiro a. Da mesma forma, podemos utilizar esse pensamento para os outros três satélites, obtendo o seguinte sistema:

$$\begin{cases} x_a = 13a + 1 \\ x_b = 15b + 4 \\ x_c = 19c + 8 \end{cases}$$

Podemos analisar as situação acima como um sistema formado por três progressões aritméticas, cujos termos iniciais são 1, 4 e 8, e as razões 13, 15 e 19, respectivamente.

$$\begin{array}{l} (1, 14, 27, 40, \cdots) \\ (4, 19, 34, 49, \cdots) \\ (8, 27, 46, 65, \cdots) \end{array}$$

Assim, queremos encontrar todos os termos que pertençam simultaneamente às três sequências, em especial o menor termo.

Observamos que o termo geral de cada PA é dado por:

$$\begin{array}{l} a_n = 1 + (n-1)13 = 13n - 12 \\ b_m = 4 + (m-1)15 = 15m - 11 \\ c_p = 8 + (p-1)19 = 19p - 11 \end{array}$$

Desta forma, teremos $c_p = b_m$ sempre que

$$\begin{aligned} c_p &= b_m \\ 19p - 11 &= 15m - 11 \\ 19p &= 15m \\ p &= \frac{15m}{19} \end{aligned} \tag{7.1}$$

Logo, teremos $c_p = b_m$ sempre que $(15m)/19$ for inteiro, para $m \in \{1, 2, 3, \cdots\}$. Isto ocorre se, e somente se, m for múltiplo de 19, ou seja,

$$m = 19k, \ k \in \mathbb{Z} \tag{7.2}$$

De modo análogo, temos que p é múltiplo de 15.
Analisando, agora, a primeira PA em relação às demais, temos:

$$\begin{aligned} a_n &= b_m \\ 13n - 12 &= 15m - 11 \\ 13n &= 15m + 1 \\ n &= \frac{15m+1}{13} \end{aligned} \tag{7.3}$$

$$\begin{aligned} a_n &= c_p \\ 13n - 12 &= 19p - 11 \\ 13n &= 19p + 1 \\ n &= \frac{19p+1}{13} \end{aligned} \tag{7.4}$$

Como $k \in \mathbb{Z}$, $k \geq 1$ e $a, b, c \geq 0$, então podemos assumir valores para k e encontrar valores inteiros para n, m, p que satisfaçam o sistema.
Tomando $k = 1$, obtemos pela equação 7.2 que $m = 19$.
Substituindo esse valor na equação 7.1, temos

$$\begin{aligned} p &= \frac{15m}{19} \\ p &= \frac{15 \cdot 19}{19} \\ p &= 15 \end{aligned}$$

E, finalmente, substituindo o valor de m na equação 7.3, temos

$$\begin{aligned} n &= \frac{15m+1}{13} \\ n &= \frac{15 \cdot 19 + 1}{13} \\ n &= 22 \end{aligned}$$

Como os três valores encontrados são inteiros, podemos encontrar o termo das PAs desejado:

$$a_n = 13n - 12 = 274$$
$$b_m = 15m - 11 = 274$$
$$c_p = 19p - 11 = 274$$

Portanto, o primeiro momento em que os três satélites irão passar juntos sobre Londrina ocorrerá **274 horas** após a meia-noite.

A resposta encontrada pode ser verificada por meio da aplicação do Teorema Chinês dos Restos (teorema 5.16).

Para encontrar o tempo que irá demorar para os três satélites se encontrarem novamente sobre Londrina, basta resolver o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 1 \ (mod\ 13) \\ x \equiv 4 \ (mod\ 15) \\ x \equiv 8 \ (mod\ 19) \end{cases}$$

De acordo com o teorema 5.16, primeiramente encontramos os valores de M, M_1, M_2 e M_3.

$$\begin{aligned} M &= 13 \cdot 15 \cdot 19 = 3705 \\ M_1 &= 15 \cdot 19 = 285 \\ M_2 &= 13 \cdot 19 = 247 \\ M_3 &= 13 \cdot 15 = 195 \end{aligned}$$

Com isso, temos que $x_1 = 12$, $x_2 = 13$ e $x_3 = 4$ são, respectivamente, soluções particulares das congruências

$$\begin{cases} 285X \equiv 1 \ (mod\ 13) \\ 247X \equiv 1 \ (mod\ 15) \\ 195X \equiv 1 \ (mod\ 19) \end{cases}$$

Logo, a solução particular x_0, do sistema inicial, é dada por

$$\begin{aligned} x_0 &= 285 \cdot 12 \cdot 1 + 247 \cdot 13 \cdot 4 + 195 \cdot 4 \cdot 8 \ (mod\ 3705) \\ &= 3420 + 12844 + 6240 \ (mod\ 3705) \\ &= 22504 \ (mod\ 3705) \end{aligned}$$

Porém, como $22504 \equiv 274 \ (mod\ 3705)$, temos que as soluções do problema são

$$x \equiv 274 \ (mod\ 3705).$$

Portanto, os encontros dos três satélites ocorrerão após $(274 + 3705k)$ horas, com $k \in \mathbb{Z}$ e $k \geq 0$. Com isso, verificamos que o primeiro encontro ($k = 0$) ocorrerá *274* horas após o início da observação.

7.3.2 Análise da resolução dos alunos

Esta atividade se mostrou a mais complexa para que os alunos conseguissem resolver, principalmente por se tratar de um problema que envolve um sistema de congruências modulares. Essa dificuldade já ficou evidente nas primeiras tentativas que realizaram, pois alguns alunos buscaram descrever o problema na forma de equações algébricas e resolver o sistema com as ferramentas por eles já conhecidas. Ao seguir por esse caminho, alguns cometeram o erro de não considerar que cada equação deveria ter uma segunda incógnita diferente, pois não necessariamente os satélites se cruzariam após um mesmo número de voltas.

O aluno B foi o que chegou mais próximo da resposta sem auxílio, pois ele observou que cada equação do sistema deveria ter uma incógnita diferente e, assim, conseguiu chegar a algumas relações envolvendo essas três incógnitas, conforme a imagem abaixo.

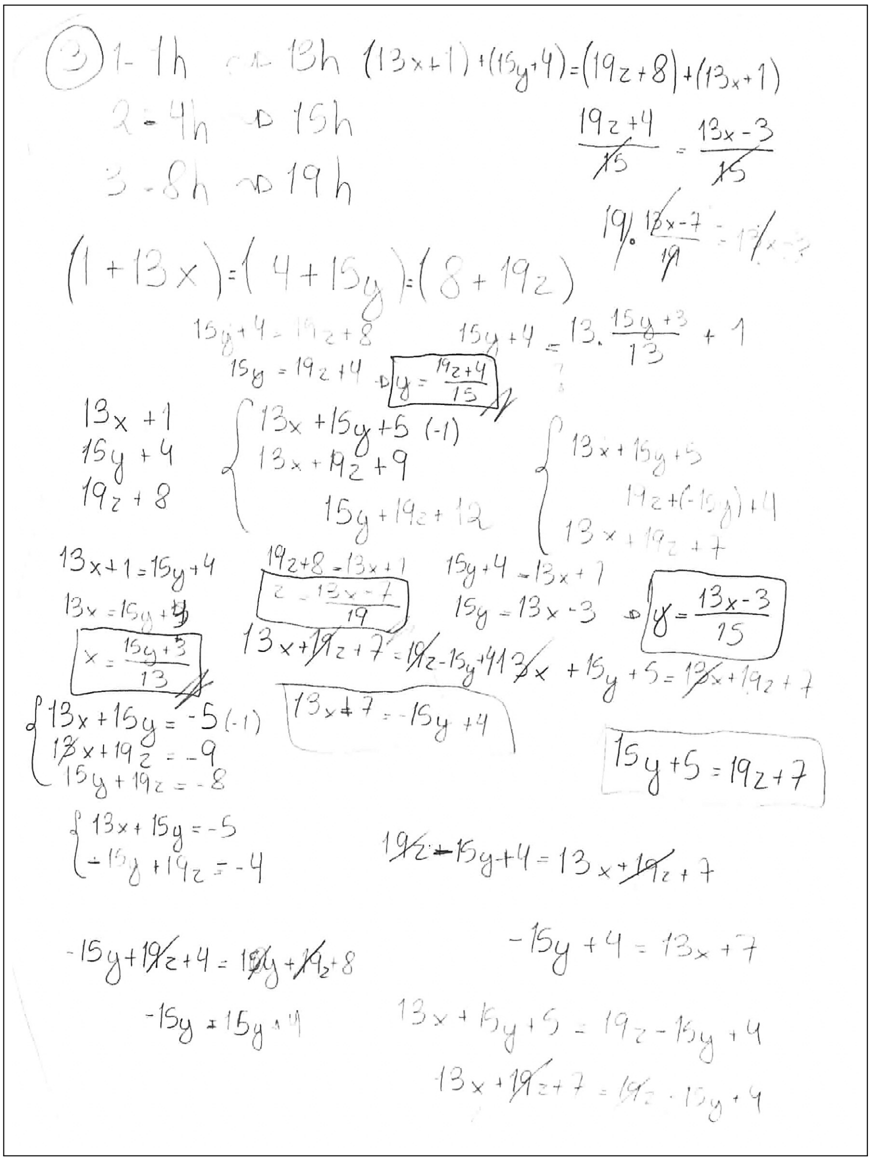

Figura 7.9: Resposta do aluno B para o problema 3

Para dar continuidade à resolução, foi necessário desenvolver com os alunos no quadro as sequências dos horários em que cada satélite sobrevoava Londrina, o que levou um grupo a observar que cada uma dessas sequências forma uma Progressão Aritmética (P.A.). Contudo, nesse ponto foi possível perceber que a atividade havia se desviado da metodologia de resolução de problemas, escolhida para sua aplicação, e de seu objetivo, que era analisar as possíveis formas de resolução que os alunos encontrariam sozinhos, verificando se estariam preparados para resolver um problema deste nível apenas com o conhecimento que possuem até então. Assim, percebemos que, da forma em que foi apresentada, sem atividades prévias correlatas, essa terceira atividade ficou muito difícil.

Esse nível de dificuldade já estava previsto quando da elaboração da pesquisa pois, como se trata de um problema que envolve a utilização do Teorema Chinês dos Restos para sua resolução, foram realizadas várias tentativas por diferentes caminhos para encontrar uma forma de resolvê-lo sem utilizar o teorema, ou seja, um caminho para resolvê-lo que os alunos, que ainda não conheciam o TCR, poderiam seguir. Como foi necessário quase um mês para nós encontrarmos essa solução completa, iniciando com a ideia de P.A., era possível que os alunos não conseguissem encontrá-la tão facilmente durante o pouco tempo que tínhamos disponível para realizar a aplicação da atividade.

Uma forma para facilitar que os alunos conseguissem observar esse caminho de resolução sem auxílio do pesquisador, seria inserir algumas atividades prévias, envolvendo problemas em que possam observar mais facilmente a possibilidade de utilizar a ideia da P.A. Por exemplo, o problema a seguir:

Uma indústria de confecções produziu, em janeiro de 2015, 1000 camisetas e 700 calças. Sabendo que a cada mês a empresa aumenta sua produção em 10 camisetas e 20 calças, quanto será sua produção total naquele ano?

Com isso, os alunos podem ter a oportunidade de relembrar e aplicar alguns conceitos que envolvem a Progressão Aritmética em problemas, aparentemente, mais simples. Acreditamos que, assim, os alunos estarão mais aptos à perceberem que podem utilizar um caminho semelhante para iniciar a resolução da terceira atividade proposta (satélites).

Na sequência do desenvolvimento da atividade 3 com os alunos, como essa atividade se mostrou mais complexa para eles resolverem sozinhos, assim como foi explicitado anteriormente, o processo foi sendo acompanhado pelo pesquisador, o qual permitiu que os alunos indicassem o passo seguinte, interferindo apenas quando solicitado, por meio de questionamentos, os instigando a encontrar os erros, quando estes existiam, e perceberem que nem sempre existia apenas uma forma de realizar determinada etapa da resolução. Desta forma, os alunos foram desenvolvendo juntos a resolução, seguindo um processo semelhante ao previsto, sendo que a grande maioria demonstrou compreender todo o desenvolvimento.

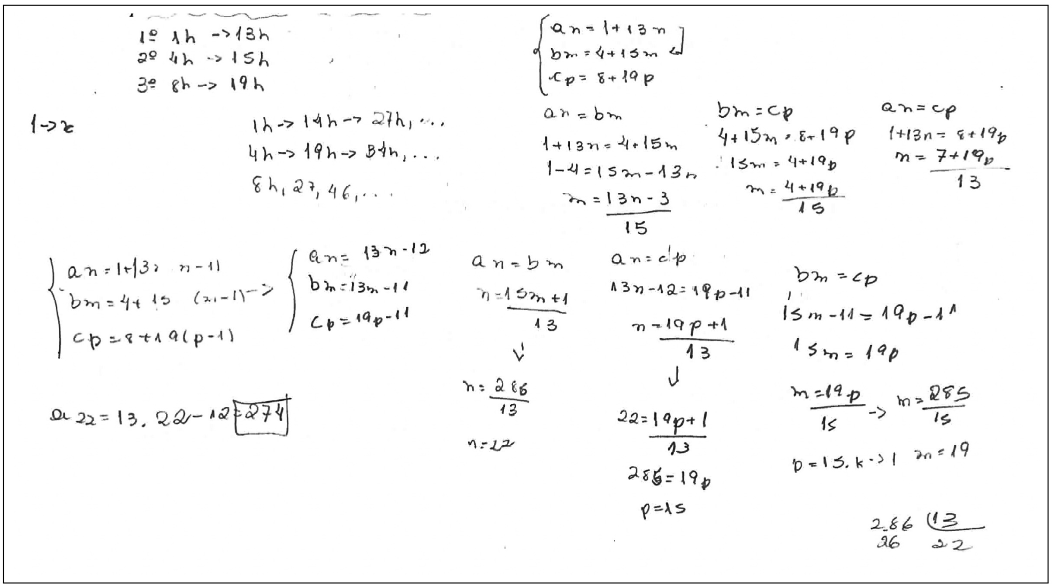

Figura 7.10: Resposta da aluna F para o problema 3

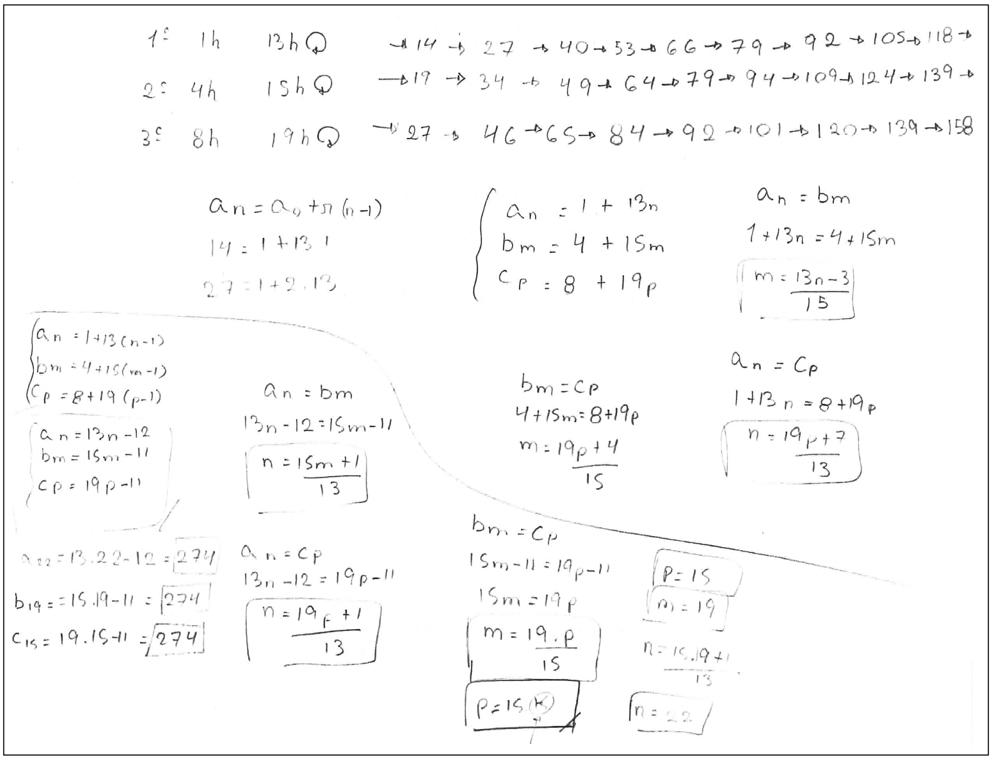

Figura 7.11: Resposta da aluna C para o problema 3

Após o término dessa atividade, alguns alunos disseram que não seriam capazes de resolver esse problema sozinhos, principalmente devido à análise que deveria ser feita para entender os "detalhes" existentes na resolução que a diferenciam da "matemática normal" que eles estão acostumados. Neste momento, aproveitou-se para explicar que a matemática possui diversos campos de estudo, alguns muito diferentes dos ensinados durante a Educação Básica, mas que essas áreas podem ser aprendidas também por eles. Por exemplo, foi explicado que eles conseguiram observar sozinhos algumas ideias básicas que fundamentam a aritmética modular nas primeiras atividades, quando trabalharam com os restos das operações e fizeram diversas observações muito interessantes, algumas até mesmo inesperadas pelo pesquisador, as quais já foram citadas nas análises anteriores.

Finalmente, foi apresentado o conceito do Teorema Chinês dos Restos, explicando que seria muito mais rápido resolver um problema como esse visto na terceira atividade utilizando essa ferramenta matemática. Contudo, não foi possível desenvolver completamente o teorema e demonstrá-lo, pois os alunos ainda não conheciam, de maneira formal, alguns conceitos e a simbologia relacionada às congruências. Assim, explicou-se a ideia geral e a origem do teorema, ressaltando a importância da matemática oriental e de todo o conhecimento por eles produzido ao longo dos séculos.

Ao observar tudo que foi realizado durante a aplicação dessas atividades, fica evidente como a participação dos alunos foi fundamental para que conseguissem desenvolver e compreender todas as etapas. Além disso, a maneira como trabalharam em conjunto para encontrar as melhores formas de resolver os problemas contribui para despertar nos alunos sua curiosidade, sua vontade de aprender e compartilhar seu conhecimento, buscando compreender as situações a partir de pontos de vista diferentes.

Isso mostrou-se ainda mais relevante quando observamos como a aplicação dessas atividades serviu para reforçar nos alunos, não apenas o uso da simbologia algébrica, mas a maneira de pensar um problema algebricamente. Ficou evidente que alguns estudantes ainda possuíam dificuldade em transcrever o que compreenderam dos problemas usando a notação da álgebra. Porém, foi possível observar que, mesmo apresentando essa dificuldade na simbologia, a ideia de pensar algebricamente estava presente em quase todas as resoluções, em especial na segunda atividade. Pensar algebricamente não é apenas descrever uma situação em notação algébrica, escrever algo usando letras e números, mas sim compreender os conceitos matemáticos existentes naquele problema, reconhecendo os padrões já observados em outros casos. Com isso, o aluno consegue descrever suas observações sobre o problema, mesmo sendo com suas palavras, e propor caminhos para chegar à solução.

8 CONSIDERAÇÕES FINAIS

A utilização de atividades em sala de aula cujos temas não estão incluídos no currículo tradicional, como foi o caso deste trabalho, tende a dar mais liberdade aos alunos em procurar soluções diferentes, motivando sua busca por ferramentas que eles já conhecem, ou novas, para solucionar problemas, até então, inéditos para eles. Essa abordagem acabou incentivando a maior parte dos estudantes que participou da pesquisa a querer resolver os problemas; e mais, a querer aprender os diferentes caminhos, em especial os mais simples e rápidos, para chegar nos resultados esperados.

O modo como as atividades foram planejadas visou preparar os alunos para compreenderem alguns conceitos essenciais para o ensino formal da Aritmética Modular, como trabalhar utilizando os restos das operações, analisar o significado desses restos dentro dos problemas, observar a existência de sistemas de equações “diferentes” dos que já estudaram, entre outros. Dessa forma, foi possível observar que esses conceitos puderam ser bem compreendidos pelos estudantes, em particular nas duas primeiras atividades, durante as quais eles conseguiram realizar o que foi pedido quase sem nenhum auxílio e, se utilizando de diferentes métodos, puderam “enxergar” a matemática sob um outro ponto de vista, percebendo como esse trabalho envolvendo os restos pode ser uma valiosa ferramenta na resolução dos mais diversos problemas.

Além disso, essa proposta desafia o professor a inovar suas aulas, tanto em metodologia como no conteúdo, uma vez que a Aritmética Modular não é um assunto normalmente abordado na Educação Básica.

Assim, observamos que o objetivo do presente trabalho é algo que pode ser realizado de uma maneira muito satisfatória com alunos do Ensino Médio, pois o nível de conhecimento matemático que estes já possuem se mostra suficiente para acompanhar as atividades da forma que foram apresentadas, salvo o caso da terceira atividade, na qual se mostra necessária a inclusão de atividades prévias para facilitar que sejam dados os passos iniciais em sua resolução.

Em razão de seu caráter introdutório, recomendamos a utilização dessas atividades como uma aula preparatória para o professor desenvolver formalmente a Aritmética Modular na Educação Básica, pois, após a compreensão dessas ideias fundamentais que foram desenvolvidas durante sua aplicação, os alunos estarão mais preparados para compreenderem os conceitos e trabalharem com as notações que fazem parte dessa área tão rica da Matemática.

Por fim, este trabalho visa contribuir para o entendimento de como se daria a inserção de tópicos de Aritmética Modular na Educação Básica, uma vez que a importância do assunto é notória e seus principais conceitos se dão em níveis relativamente fáceis de compreensão. Dada a relevância do tema, consideramos que há muito mais a ser abordado e, portanto, há também um vasto campo de trabalho para estudos posteriores nesta área. Esperamos que as atividades e resultados apresentados acima, bem como nossas referências, possam servir de subsídios para futuros trabalhos teóricos e práticos.

REFERÊNCIAS

ALLEVATO, N. S. G.; ONUCHIC, L. R. Ensinando matemática na sala de aula através da resolução de problemas. **Boletim GEPEM**, Rio de Janeiro, ano 33, n. 55, p. 133-156, jul./dez. 2009.

BARBOSA JUNIOR, J. H. **Congruências modulares:** construindo um conceito e as suas aplicações no ensino médio. 2013. 51 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Sergipe, São Cristóvão, 2013.

BARROS, M. A. de O. **Aritmética Modular:** Aplicações no Ensino Médio. 2014. 90 f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Mato Grosso, Cuiabá, 2014.

BERTINI, L. F.; PASSOS, C. L. B. Uso da Investigação Matemática no Processo de Ensino e Aprendizagem nas Séries Iniciais do Ensino Fundamental. In: XII Encontro Brasileiro de Estudantes de Pós-Graduação em Educação Matemática, 2008, Rio Claro. **Anais.** Rio Claro: UNESP, 2008.

BOCHI, J. **Teorema Chinês dos Restos:** notas de aula. Rio de Janeiro: Pontifícia Universidade Católica, 2009.

BONI, K. T.; SAVIOLI, A. M. P. D. Contribuições para o Desenvolvimento do Pensamento Algébrico. **Perspectivas da Educação Matemática**, Brasília, v.8, n.17, p. 265-286, 2015.

BOYER, C. B.; MERZBACH, U. C. **História da Matemática.** Tradução de Helena Castro. São Paulo: Blucher, 2012. Tradução de: A History of Mathematics.

BRANDENBURG, R.; NEVENZEEL, K. **The Nine Chapters on the History of Chinese Mathematics.** Groningen, Holanda: University of Groningen, 2007. Disponível em: <http://www.astro.rug.nl/ nevenzeel/Study/PGvdW_t=9C_HCM_a=RB,KN.pdf> Acesso em: 02 set. 2015.

BRASIL. **Parâmetros Curriculares Nacionais:** terceiro e quarto ciclos do ensino fundamental: matemática. Brasília: MEC/SEF, 1998.

CHEMLA, K. Reading proofs in Chinese commentaries: algebraic proofs in an algorithmic context. In: CHEMLA, K. (Org.) **The History of Mathematical Proof in Ancient Traditions.** Nova Iorque: Cambridge University Press, 2012.

COUTINHO, S. C. **Números inteiros e criptografia RSA.** Rio de Janeiro: IMPA/SBM, 1997.

D'AMBROSIO, B. S. Como ensinar matemática hoje? Temas e Debates. **SBEM**, Brasília, ano II, n. 2, p. 15-19, 1989.

DICK, A. P.; PALIOZA, L. H.; HAUSCHILD, C. A.; DULLIUS, M. M. Investigação Matemática: Uma metodologia para o Ensino Fundamental. **Destaques Acadêmicos**, Lajeado, v. 6, n. 4, p. 7-18, dez. 2014.

DOMINGUES, H. H.; IEZZI, G. **Álgebra moderna:** volume único. São Paulo: Atual, 4.ed., 2003.

EVARISTO, J; PERDIGÃO, E. **Introdução à Álgebra Abstrata.** Maceió: EDUFAL, 2002.

FLEMMING, D. M.; LUZ, E. F.; MELLO, A. C. C. de. **Tendências em educação matemática.** Palhoça: UnisulVirtual, 2.ed., 2005.

GARBI, G. G. **A Rainha das Ciências.** São Paulo: Livraria da Física, 3.ed., 2006.

GERHARDT, T. E.; SILVEIRA, D. T. (Org.). **Métodos de Pesquisa.** Porto Alegre: Editora da UFRGS, 2009.

GILL, A. C. **Métodos e técnicas de pesquisa social.** São Paulo: Atlas, 1999.

GROENWALD, C. G. O. Pensamento Aritmético, a Resolução de Problemas e o Processo de Ensino-Aprendizagem. In: X Encontro Nacional de Educação Matemática, 2010, Salvador. **Anais.** Salvador: SBEM, 2010.

HEFEZ, A. **Aritmética.** (Notas de aula PROFMAT). Rio de Janeiro: SBM, 2014.

História da Civilização Chinesa. Disponível em: <http://www.historiadomundo.com.br/chinesa/civilizacao-chinesa.htm>. Acesso em: 12 ago. 2015.

History of Chinese Mathematics. Disponível em: <http://www1.chinaculture.org/created/created_mathematic.html> Acesso em: 15 ago. 2015.

LAUDARES, J. B.; LEITE, J. R. M. O Desenvolvimento do Pensamento Aritmético a Partir de Experiência Matemática. **Educação Matemática em Revista**, Brasília, ano 16, n. 34, p. 52-61, nov. 2011.

LINS, R. C.; GIMENEZ, J. **Perspectivas em aritmética e álgebra para o século XXI.** São Paulo: Papirus, 1997.

MARTINEZ, F. E. B.; MOREIRA, C. G. T. A.; SALDANHA, N. C; TENGAN, E. **Teoria dos números:** um passeio com primos e outros números familiares pelo mundo inteiro. Rio de Janeiro: IMPA, 2.ed., 2013.

MATTOS, S. R. P.; PUGGIAN, C.; LOZANO, A. R. G. Aritmética modular e suas possibilidades na formação continuada de professores de Matemática. In: XIII Conferência Interamericana de Educação Matemática, 2011, Recife. **Anais.** Recife: CIAEM, 2010.

MIAO, T. A formal system of the Gougu method: a study on Li Rui's Detailed Outline of Mathematical Procedures for the Right-Angled Triangle. In: CHEMLA, K. (Org.) **The History of Mathematical Proof in Ancient Traditions.** Nova Iorque: Cambridge University Press, 2012.

MINAYO, M. C. S. (Org.). **Pesquisa social:** teoria, método e criatividade. Petrópolis: Vozes, 2001.

ONUCHIC, L. de la R. Ensino-aprendizagem de Matemática através da Resolução de Problemas. In: BICUDO, M. A. V. (Org.) **Pesquisa em Educação Matemática:** Concepção & Perspectivas. São Paulo: UNESP, 1999.

PARANÁ, Secretaria de Estado da Educação. **Diretrizes Curriculares da Educação Básica.** Curitiba: SEED, 2008.

POFFO, E. M. A resolução de problemas como metodologia de ensino: uma análise a partir das contribuições de Vygotsky. In: II Seminário em Resolução de Problemas, 2011, Rio Claro. **Anais.** Rio Claro: UNESP, 2011.

PONTE, J. P.; BROCARDO, J.; OLIVEIRA, H. **Investigações matemáticas na sala de aula.** Belo Horizonte: Autentica, 2003.

PORTANOVA, R. (Org.). **Um currículo de matemática em movimento.** Porto Alegre: Edipucrs, 2005.

REGO, T. C. V. **Uma perspectiva histórico-cultural da educação.** 2.ed. Petrópolis: Vozes, 1995.

ROQUE, T. **História da Matemática.** Uma visão crítica, desfazendo mitos e lendas. Rio de Janeiro: Zahar, 2012.

SILVA, R. N. **Álgebra e Aritmética no Ensino Fundamental:** um estudo de como ensiná-las de forma integrada e com base em significados. 2007. 20 f. Trabalho de Conclusão de Curso (Licenciatura em Matemática) – Universidade Católica de Brasília, Brasília, 2007.

SKOVSMOSE, O. Cenários para investigação. **BOLEMA**, Rio Claro, v. 13, n. 14, p. 66-91, 2000.

Sociedade Brasileira de Matemática - SBM. **Banco de Questões da XXXI Olimpíada Brasileira de Matemática.** Rio de Janeiro: IMPA, 2009.

A ATIVIDADES PROPOSTAS

1 Descobrir o dia da semana

A copa do mundo de futebol foi realizada no Brasil no ano de 2014. O jogo de abertura ocorreu no dia 12 de junho. Supondo que não haja um calendário em mãos, e sabendo que o dia 1º de janeiro de 2014 foi uma quarta-feira, determine em que dia da semana ocorreu o jogo de abertura.

Tabela 1: Número de dias de cada mês

JAN	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
31	28	31	30	31	30	31	31	30	31	30	31

2 Dado os restos, encontre o número

Para realizar a atividade, cada dupla de alunos irá receber um dado.

Obs.: Como o dado possui seis faces, cada vez que ele for jogado poderemos obter como resultado o valor 1, 2, 3, 4, 5 ou 6. Assim, podemos tomar quaisquer números maiores que 6, por exemplo $m = 7$ e $n = 8$, de tal forma que os resultados dos lançamentos sempre serão menores que m e n.

1º) Lance o dado algumas vezes e anote os resultados obtidos na tabela abaixo: 2º)

i	j	a

Encontre um número inteiro a menor que $(m \cdot n = 56)$ de tal modo que quando dividirmos a por $m = 7$ vamos obter resto i e quando dividirmos a por $n = 8$ vamos obter resto j.

3º) O que você pôde observar em relação aos valores de a encontrados para cada lançamento?

3 Encontro dos satélites

Três satélites passarão sobre Londrina esta noite. O primeiro a 1 hora da madrugada, o segundo às 4 horas e o terceiro às 8 horas da manhã. Cada satélite tem um período diferente. O primeiro leva 13 horas para completar uma volta em torno da Terra; o segundo, 15 horas e, o terceiro, 19 horas. Determine após quantas horas, a partir da meia-noite, os três satélites passarão ao mesmo tempo sobre Londrina. (COUTINHO, 1997, p.116, *adaptado*)

B TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Termo de Consentimento Livre e Esclarecido

Título da pesquisa:
"Tópicos de Aritmética Modular na Educação Básica"

Prezado(a) Senhor(a), responsável pelo menor ___________________________________

Gostaríamos de convidar seu(sua) filho(a) a participar da pesquisa **"Tópicos de Aritmética Modular na Educação Básica"**, realizada no Colégio São José. O objetivo da pesquisa é **desenvolver algumas atividades matemáticas com os alunos da Educação Básica, buscando introduzir alguns conceitos básicos de aritmética modular.** A sua participação é muito importante e ela se daria por meio da resolução de alguns problemas matemáticos em sala de aula, sob a orientação e com o acompanhamento do responsável pela pesquisa**.**
Gostaríamos de esclarecer que a participação é totalmente voluntária, podendo o menor: recusar-se a participar, ou mesmo desistir a qualquer momento sem que isto acarrete qualquer ônus ou prejuízo à sua pessoa. Informamos ainda que as informações serão utilizadas somente para os fins desta pesquisa e serão tratadas com o mais absoluto sigilo e confidencialidade, de modo a preservar a sua identidade.
Os benefícios esperados com essa pesquisa são compreender formas melhores de ensinar alguns conceitos mais avançados de matemática para os alunos do Ensino Médio, além de incentivar um maior desenvolvimento do pensamento algébrico (matemático) dos alunos, o que é muito importante, principalmente, para a realização de exames, como o ENEM, vestibulares e concursos públicos.
Informamos que o(a) senhor(a) não pagará nem será remunerado pela participação de seu(sua) filho(a). Garantimos, no entanto, que todas as despesas decorrentes da pesquisa serão ressarcidas, quando devidas e decorrentes especificamente de sua participação na pesquisa.
Caso você tenha dúvidas ou necessite de maiores esclarecimentos pode nos contatar: **Diego Aparecido Maronese, (43) 8807-9080, diegomaronese@msn.com**, ou procurar o Comitê de Ética em Pesquisa Envolvendo Seres Humanos da Universidade Estadual de Londrina, na Avenida Robert Kock, nº 60, ou no telefone (43) 3371-2490. Este termo deverá ser preenchido em duas vias de igual teor, sendo uma delas, devidamente preenchida e assinada entregue a você.

Londrina, 18 de maio de 2016.

Pesquisador Responsável: Diego Aparecido Maronese
RG: 10.707.855-0 Telefone: (43) 8807-9080

EU, ______________________________________, CPF: ___________________, responsável pelo menor____, tendo sido devidamente esclarecido sobre os procedimentos da pesquisa, concordo que ele (ela) participe **voluntariamente** da pesquisa descrita acima.

Assinatura do menor: ______________________________

Assinatura do responsável: ________________________