

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO ACADÊMICO DO AGRESTE
NÚCLEO DE FORMAÇÃO DOCENTE
MATEMÁTICA-LICENCIATURA

**INVESTIGANDO O USO DE APLICAÇÕES DE ARITMÉTICA MODULAR
EM LIVROS DIDÁTICOS DO ENSINO SUPERIOR**

JOSÉ ALEX DOS SANTOS

CARUARU, 2015

JOSÉ ALEX DOS SANTOS.

**INVESTIGANDO O USO DE APLICAÇÕES DE ARITMÉTICA MODULAR
EM LIVROS DIDÁTICOS DO ENSINO SUPERIOR**

Trabalho de Conclusão de Curso,
apresentado à disciplina TCC II como
requisito obrigatório para obtenção do
título de licenciado em Matemática pela
Universidade Federal de Pernambuco-
Centro Acadêmico do Agreste.

Orientador: MARIA DO DESTERRO AZEVEDO DA SILVA

Coorientador: EDELWEIS JOSÉ TAVARES BARBOSA

CARUARU, 2015

Catálogo na fonte:
Bibliotecária - Simone Xavier CRB/4-1242

S237i Santos, José Alex dos.
Investigando o uso de aplicações de aritmética modular em livros didáticos do ensino superior. / José Alex dos Santos. - Caruaru: O Autor, 2015.
77f. il. ; 30 cm.

Orientadora: Maria do Desterro Azevedo da Silva
Coorientador: Edelweis José Tavares Barbosa
Monografia (Trabalho de Conclusão de Curso) – Universidade Federal de Pernambuco, CAA, Licenciatura em Matemática, 2015.
Inclui referências bibliográficas

1. Ensino. 2. Aprendizagem. 3. Aritmética modular. 4. Livro didático. I. Silva, Maria do Desterro Azevedo. (Orientadora). II. Barbosa, Edelweis José Tavares. III. Título

371.12 CDD (23. ed.) UFPE (CAA 2015-205)



**Universidade Federal de Pernambuco
Centro Acadêmico do Agreste
Núcleo de Formação Docente
Matemática-Licenciatura**

**INVESTIGANDO O USO DE APLICAÇÕES DE ARITMÉTICA MODULAR
EM LIVROS DIDÁTICOS DO ENSINO SUPERIOR.**

JOSÉ ALEX DOS SANTOS

Monografia submetida ao corpo docente do curso de MATEMÁTICA-Licenciatura do Centro Acadêmico do Agreste da Universidade Federal de Pernambuco e aprovada em 31 de julho de 2015.

Banca examinadora:

Prof^a. Maria do Desterro Azevedo da Silva (CAA-UFPE)
Orientadora

Prof. Edelweis José Tavares Barbsa (CAA-UFPE)
Co-orientador

Prof. José Marcos da Silva (IFPB)
Examinador Externo

Prof^a. Cristiane de Arimatéia Rocha (CAA-UFPE)
Examinadora Interna

Dedico este trabalho aos meus familiares, em especial a minha mãe Josefa (rainha), que sempre foi meu porto seguro me incentivando a alçar grandes voos.

AGRADECIMENTOS

Aqui fica expressa minha gratidão, para todos que contribuíram direta ou indiretamente no processo de construção deste trabalho.

Primeiramente a DEUS, por ser meu refúgio em todos os momentos da minha vida, além de me proporcionar a certeza que me dar forças para continuar sempre.

A minha orientadora, Maria do Desterro Azevedo da Silva, pela orientação competente, incentivo, dedicação, paciência e valiosas contribuições para que este trabalho se concretizasse.

Ao professor, Edelweis José Tavares Barbosa, pelo grande apoio e comentários dando sua importante contribuição como coorientador deste trabalho.

A professora Cristiane de Arimatéa Rocha, pelos puxões de orelha e incentivos enquanto professora da disciplina de TCC2.

A todos os docentes do curso de Matemática- Licenciatura da UFPE-CAA, por fazerem com que eu me apaixonasse pelo curso e por me proporcionarem grandes fontes de conhecimento.

Aos meus companheiros de curso, pela troca de experiências e discussões enriquecedoras. Além da união que perpassa todos os ambientes nos quais estamos juntos.

Aos meus familiares por toda forma de carinho e compreensão demonstrados durante a realização deste trabalho, em especial a minha mãe, por todo amor e dedicação dados durante sua vida.

E por fim, porém não menos importantes, agradeço aos meus amigos que me ajudaram na questão da formatação deste trabalho.

“A matemática é o alfabeto com o qual, Deus escreveu o universo”.

Galileu Galilei.

RESUMO

A seguinte pesquisa teve como objetivo analisar se os livros didáticos abordados na disciplina Teoria dos Números propõem o uso de aplicações da Aritmética Modular para subsidiar o processo de ensino e aprendizagem. Nossa análise realizou-se no Centro Acadêmico do Agreste da Universidade Federal de Pernambuco, campo para seleção dos livros a serem investigados, os quais foram totalizados em seis, abrangendo os livros que estão presentes na ementa do curso de Matemática-Licenciatura. Para solucionar nosso questionamento utilizamos uma análise qualitativa baseada em Minayo (2007) e a análise de conteúdo defendida por Bardim (2011), as quais se completaram enaltecendo e corroborando com a ideia uma da outra. Evidenciamos a existência de um material passível e interessante para ser abordado no Ensino Superior, com aplicações da Aritmética Modular imersas no nosso cotidiano e que trazem sentido para os algoritmos que são na maioria das vezes não tão claros e objetivos. Exibimos assim uma ponte entre o que está sendo explorado no Ensino Superior para com a Educação Básica em razão de nosso público principal se constituir de futuros professores.

Palavras-chave: Ensino e Aprendizagem. Aritmética Modular. Livro didático.

ABSTRACT

The following study aimed to analyze whether the textbooks covered in Number Theory discipline propose the use of applications of Modular Arithmetic to support the process of teaching and learning. Our analysis took place in the arid zone of the Academic Center of the Federal University of Pernambuco, the field for selecting books to be investigated, which were aggregated into six, including books that are present on the menu of the course of Mathematical Degree. To solve our questioning we use a qualitative analysis based on Minayo (2007) and the content analysis advocated by Bardim (2011), which are completed praising and supporting the idea of each other. We show the existence of a subject material, and interesting to be addressed in higher education, with applications Modular Arithmetic immersed in our daily lives and they bring sense to the algorithms that are most often not as clear and objective. So we display a bridge between what is being explored in higher education towards basic education due to our primary audience be future teachers.

Keywords: Teaching and Learning. Modular arithmetic. Textbook.

Sumário

INTRODUÇÃO	11
Objetivo Geral	14
Objetivos Específicos	14
1.1 Uma breve análise histórica.....	15
1.2 O que é Aritmética Modular?	19
1.3 Definições e propriedades da Aritmética Modular.	20
2. O LIVRO DIDÁTICO NO PROCESSO DE ENSINO E APRENDIZAGEM.....	29
2.1 O livro didático enquanto material didático.	29
2.2 O processo de ensino e aprendizagem: uma visão a partir do livro didático.....	31
3. A ARITMÉTICA MODULAR E SUAS APLICAÇÕES NO COTIDIANO	36
3.1 Exemplos básicos da Aritmética Modular.....	36
3.2 Aplicações mais presentes no nosso dia a dia.....	40
3.2.1 Códigos de barras EAN-13	40
3.2.2 Sistema de identificação ISBN	43
3.2.3 Cadastro de Pessoas Físicas – CPF	45
3.2.4 Criptografia	48
3.3 A Aritmética Modular desde a Educação Básica.	50
4. METODOLOGIA DE PESQUISA	54
4.1 Descrição Metodológica	54
5. APRESENTAÇÃO DAS ANÁLISES E DOS RESULTADOS	58
5.1 Procedimentos adotados para a análise.....	58
5.1.2 Obtenção dos Dados	58
5.2 Análise dos livros	68
CONSIDERAÇÕES FINAIS	70
REFERÊNCIAS.....	72
ANEXOS	75

INTRODUÇÃO

O presente trabalho surgiu em detrimento do processo de ensino e aprendizagem no tocante a disciplina Teoria dos Números do curso de Matemática-Licenciatura do Centro Acadêmico do Agreste da Universidade Federal de Pernambuco. Salientamos que a Teoria dos Números é o ramo da Matemática que estuda as propriedades dos números em geral, sendo a Teoria Elementar dos Números responsável pelas propriedades dos números inteiros. Abordamos como foco principal a Aritmética Modular e o uso de suas aplicações a partir do livro didático.

A Aritmética Modular define uma relação de equivalência entre aqueles números inteiros que divididos por outro número inteiro deixam o mesmo resto. Evidenciamos que o estudo desses restos é o principal tópico da Aritmética Modular, onde os restos equivalentes formam um conjunto o qual denominamos *classe de equivalências*. Dizemos que dois números inteiros são *congruentes* se deixam o mesmo resto quando divididos por um terceiro número inteiro, chamado módulo de congruência. Por exemplo, o número 26 é congruente ao número 12 módulo 7, pois ambos deixam resto 5 ao serem divididos por 7. Representamos a congruência da seguinte forma: $26 \equiv 12(mod\ 7)$.

A motivação para escolha do tema, Aritmética Modular, para o desenvolvimento deste trabalho se deu através da pertinência de aplicações no nosso cotidiano. Muitas dessas aplicações estão no nosso contexto social e cultural, sendo assim um estímulo para o processo de ensino e aprendizagem da Matemática. Ressaltamos ainda que, como estamos tratando o tema em um curso de formação de professores, é importante que os mesmos tenham uma formação que atenda as demandas que o Ensino de Matemática impõe.

A análise do contexto atual revela a importância de se valorizar a Matemática como linguagem necessária aos desafios da contemporaneidade. A Matemática, segundo D'Ambrósio (1986) é comparada com o falar, pois ela é uma linguagem precisa e possibilita ao homem se comunicar. Nesse sentido, podemos apresentar a Aritmética Modular a partir de suas inúmeras aplicações presentes no nosso cotidiano. Como, por exemplo, na prova dos nove, nos critérios de divisibilidade, nos sistemas de identificação CPF¹, ISBN², EAN-13³ e na Criptografia. Sendo os últimos os quais

¹ Cadastro de Pessoas Físicas.

daremos mais enfoque, e é diante destas aplicações da Aritmética Modular que se pretende analisar os livros didáticos sugeridos no curso de Teoria dos Números, principalmente os que estão presentes na ementa.

O livro didático constitui um dos instrumentos que contribui fortemente na prática pedagógica, tendo em vista que o mesmo é um dos materiais mais utilizados pelos docentes para organização e desenvolvimento das atividades em sala de aula e, até mesmo, para aprimorar seu próprio conhecimento sobre o conteúdo. Percebe-se ainda que o livro didático também é de fundamental importância para os discentes, pois se trata de uma fonte valiosa de informação.

O livro didático apresenta funções muito importantes quanto ao seu uso, pois ele é um dos condutores principais na sala de aula e fora dela. É nesse sentido que Gerard e Roegiers (1998) relacionam algumas funções na relação do livro didático com o discente e com o docente. Na relação do livro didático com o discente, os autores destacam: o favorecimento da aquisição de conhecimento socialmente relevante; o desenvolvimento das competências cognitivas, que contribuem para a autonomia dos mesmos; a consolidação, ampliação, aprofundamento e integração dos conhecimentos adquiridos; o auxílio na avaliação da aprendizagem; e a formação social e cultural dos discentes, além de desenvolver a capacidade de convivência e exercício da cidadania. Com relação ao docente e o livro didático, os autores destacam: o auxílio no preparo e planejamento de suas aulas; o favorecimento da aquisição dos conhecimentos; o favorecimento da formação didático pedagógica e o auxílio na avaliação da aprendizagem dos discentes.

A estrutura do livro didático é muito importante tanto para o docente, que o tem como apoio pedagógico, quanto para os discentes, que o utilizam para consulta, principalmente para legitimar o que foi abordado pelo docente. O livro didático assume assim, a função de contribuição e fomentação entre o discurso do docente e o discente, por isso ele deve ser organizado de forma a dialogar tanto com o docente quanto com os discentes, em paralelo com o cotidiano.

Temos o livro didático como um importante material no processo de ensino e aprendizagem, pois é através do mesmo que se pode traçar um paralelo do que está proposto por ele com o que realmente a sociedade vive, fazendo uma interligação direta

² International Standard Book Number-é um sistema internacional que identifica numericamente os livros segundo o título, o autor, o país, a editora, individualizando-os inclusive por edição.

³ European Article Number-é o código exclusivo para o seu produto representado por barras legíveis por scanner.

com os conhecimentos exigidos nos diversos espaços sociais. O cuidado em abordar possíveis aplicações dos conteúdos podem ainda facilitar o entendimento, despertar o interesse e o gosto pelo conteúdo.

Existe um dualismo entre: ensinar de forma puramente abstrata ou contextualizar com aplicações. Os Parâmetros Curriculares Nacionais (PCN) fazem referência ao dualismo do conhecimento matemático:

Duas forças indissociáveis estão sempre a impulsionar o trabalho em Matemática. De um lado, o permanente apelo das aplicações às mais variadas atividades humanas, das mais simples na vida cotidiana, às mais complexas elaborações de outras ciências. De outro lado, a especulação pura, a busca de respostas a questões geradas no próprio edifício da matemática. A dissociabilidade desses dois aspectos fica evidenciada pelos inúmeros exemplos de belas construções abstratas originadas em problemas aplicados e, por outro lado, de surpreendentes aplicações encontradas para as mais puras especulações (BRASIL, 1998, p.2).

No momento que se cria um vínculo entre teoria e prática passa a existir um fundamento para o conhecimento, tornando assim algo complexo e abstrato em concreto, mostrando que o ambiente ao nosso redor pode e deve ser explorado como instrumento matemático. D'Ambrósio (1986) diz que:

O valor da teoria se revela no momento em que ela é transformada em prática. No caso da educação, as teorias se justificam na medida em que seu efeito se faça sentir na condução do dia-a-dia na sala de aula. De outra maneira, a teoria não passará de tal, pois não poderá ser legitimada na prática educativa. (D'AMBROSIO, 1986, p. 43).

Por isso a necessidade de investigar nos livros didáticos as aplicações da Aritmética Modular diante da disciplina Teoria dos Números, que além de envolver um determinado grau de abstração, tem como objeto o estudo dos números inteiros, que estão na base da civilização humana, e também o desenvolvimento de elementos conceituais que servirão de base para outras aprendizagens.

Após todos estes argumentos temos como questionamento: **Os livros didáticos abordados na disciplina Teoria dos Números propõem o uso de aplicações da Aritmética Modular para subsidiar o processo de ensino e aprendizagem?** Para solucionar tal questionamento, pretendemos analisar se os livros didáticos propostos para a disciplina contém aplicações da Aritmética Modular no cotidiano e a interligação que a mesma faz entre a teoria abstrata e a prática utilizada no dia a dia.

O presente trabalho foi dividido em cinco capítulos. No Capítulo 1, está exposto um breve relato histórico sobre o desenvolvimento da Teoria dos Números, descrevendo

o surgimento da Aritmética Modular. Em seguida, focalizamos os conceitos matemáticos envolvidos neste estudo.

O Capítulo 2 aborda o livro didático enquanto material didático, o livro didático de Matemática e uma sistematização de seu desenvolvimento, elencando suas contribuições no processo de ensino e aprendizagem.

No Capítulo 3, descrevemos algumas das inúmeras aplicações da Aritmética Modular que estão inseridas no nosso cotidiano, trazendo para a realidade do indivíduo o conhecimento, até então, visto como algo inteiramente abstrato.

No Capítulo 4, mostramos a escolha do referencial teórico-metodológico, assim como seu processo de desenvolvimento. E no Capítulo 5, será relatado todo o procedimento da análise de dados, assim como as discussões que a mesma traz.

Em meio às justificativas e argumentos abordados, desejamos neste trabalho, atingir os seguintes objetivos:

Objetivo Geral

- Analisar se os livros didáticos abordados na disciplina Teoria dos Números propõem o uso de aplicações da Aritmética Modular para subsidiar o processo de ensino e aprendizagem.

Objetivos Específicos

- Constatar a Aritmética Modular presente no cotidiano;
- Realizar um levantamento dos livros didáticos, adotados na UFPE (Universidade Federal de Pernambuco) - CAA (Centro Acadêmico do Agreste), referentes à disciplina Teoria dos Números;
- Verificar a presença de aplicações da Aritmética Modular a partir do livro didático.

1. CONTEXTO HISTÓRICO DA TEORIA DOS NÚMEROS

A Teoria dos Números remete ao estudo dos números inteiros e suas propriedades. Segundo o matemático Leopold Kronecker, ao se tratar de Matemática, “Deus criou os números naturais e o resto é obra da humanidade”. Contudo, os inteiros positivos representam, sem sombra de dúvida, a primeira criação Matemática humana, sendo os números naturais os quais constituem, em certo sentido, o sistema matemático mais elementar, em que o estudo de suas propriedades desde as mais antigas épocas tem exercido grande fascínio na mente humana, desafiando inúmeras gerações de matemáticos e leigos que apreciam os seus enunciados simples e intrigantes, e cujas demonstrações estão além de qualquer simplicidade.

Apresentamos neste capítulo, um pouco da história da Teoria dos Números, baseados principalmente em Boyer (1974), Coutinho (2009) e Shokranian (2010), e assim, contextualizamos o aparecimento e o desenvolvimento da Aritmética Modular, focando por fim os principais conceitos matemáticos envolvidos em nosso estudo.

1.1 Uma breve análise histórica.

Diante do surgimento de civilizações como egípcios e babilônios, deu-se também o pontapé para o estudo das propriedades dos números inteiros, que vêm sendo desenvolvidas desde tempos remotos até os dias atuais. Observamos que a Matemática trabalhada por essas civilizações limitava-se a um conjunto de conclusões empíricas, as quais foram acumuladas ao longo do tempo (DOMINGUES, 1991). No entanto, ao final do terceiro milênio a.C., tábuas cuneiformes da Mesopotâmia mostravam que a Aritmética já era bastante sofisticada. Essa evolução foi ocorrendo de forma gradativa até que, a partir do século IV a.C., a Matemática passa a ser desenvolvida como de fato a entendemos hoje, isso ocorreu na Grécia antiga, com o trabalho de Euclides, onde a Matemática deixou de se apoiar na observação e experimentação e passou a ser considerada como ciência exata, verdadeira. Conforme Shokranian (2010, p. 10), foi Euclides que “publicou o primeiro trabalho abrangente de conhecimento matemático. Um livro que mudou nossa noção sobre a matemática, e colocou a matemática ao nosso dispor como uma ciência, não mais como um conjunto de dados e problemas isolados”.

Primeiramente, vale ressaltar o que de fato se entende por “LIVRO”, pois a escrita na Grécia antiga era feita a mão e em pergaminho e os livros correspondiam ao

que é chamado atualmente por nós de capítulos. E foi com essa estrutura que o trabalho de Euclides, intitulado *Os Elementos*, foi elaborado. Contrariando o que muitos pensam, o trabalho não trata somente de geometria, ele é dividido em treze livros ou capítulos que cobrem a Matemática elementar até aquela época.

Conforme Shokranian (2010), a criação da Matemática formal, ou seja, uma Matemática baseada na razão e dedução deu-se através da influência do livro de Euclides com ênfase na Teoria dos Números. Ressaltamos os livros VII, VIII e IX, que são dedicados à Teoria dos Números, os quais propõem alguns problemas, como: o cálculo do máximo divisor comum entre dois números, à determinação dos números primos menor que um inteiro dado e a demonstração de que existem infinitos números primos.

Outra contribuição importante ao estudo da Teoria dos Números foi exposta pelo matemático grego Diofanto de Alexandria, frequentemente chamado de pai da Álgebra. Estima-se que o mesmo viveu 84 anos, por uns versos encontrados em seu túmulo, escritos em forma de um enigmático problema. Tem como sua principal obra, e pelo que parece só em parte chegou até nós: *Arithmetica*, a qual é composta originalmente por treze livros, dos quais só conhecemos os seis primeiros. Dedicou-se à resolução exata de equações determinadas e, enfaticamente, de indeterminadas⁴. “Devido à ênfase dada na *Arithmetica* à solução de problemas indeterminados, o assunto, às vezes chamado análise indeterminada, tornou-se conhecido como análise diofantina” (BOYER, 1974. p. 134).

De acordo com Shokranian (2010), a busca por achar as soluções ou provar a existência de solução para uma equação diofantina, tornou-se motivo de ocupação para vários estudiosos, o que possibilitou a criação de diferentes modos de pensamento e estratégias de resolução para esse tipo de problema durante séculos. Assim, outros matemáticos foram influenciados pelo trabalho de Diofanto, e posteriormente, dedicaram-se à Teoria dos Números.

Mesmo tendo a Matemática como forte fonte de estudo para muitos matemáticos, observou-se que a Teoria dos Números ficou um pouco esquecida até o século XVII. No entanto, Fermat, Euler, Lagrange, Gauss e outros matemáticos deram

⁴ São equações que possuem mais de uma solução.

um novo impulso a Teoria dos Números, tendo em vista que durante a Renascença⁵, muitas obras de autores gregos foram editadas e publicadas na Europa, trazendo esse novo estímulo (COUTINHO, 2009).

Em relação à Teoria dos Números, Fermat destacou-se com relação aos números primos, mais também demonstrou interesse pelos números perfeitos e amigáveis, números figurados, quadrados mágicos e divisibilidade. Mattos (2011) afirma que:

Dentre as contribuições de Fermat, destacam-se sua conjectura sobre números primos; os números da forma $2^{2^n} + 1$, conhecidos como números de Fermat, são sempre primos; o Pequeno Teorema de Fermat, se p é um primo e a um inteiro que não é divisível por p , então p divide $a^{p-1} - 1$; a prova da afirmação de Girard; todo número primo da forma $4n+1$ pode ser escrito de uma e somente uma maneira como soma de dois quadrados; a prova de que nenhum cubo é a soma de dois cubos, isto é, não existem inteiros positivos x, y e z , tais que $x^3 + y^3 = z^3$ e sua anotação mais famosa, o último Teorema de Fermat: Se x, y e z são inteiros e $x^n + y^n = z^n$, onde $n \geq 3$, então $x \cdot y \cdot z = 0$. Outra maneira de se enunciar essa conjectura é dizendo que não existem inteiros x, y, z e n , tal que, $x^n + y^n = z^n$, com $n \geq 3$. (MATTOS, 2011, p.20).

Shokranian (2010) ainda evidencia a importância de Fermat no desenvolvimento da Teoria dos Números, quando afirma que a história da Teoria dos Números pode ser dividida em dois grandes períodos: antes e depois de Fermat. Antes de Fermat, os estudos nesta área ocorriam de forma isolada, com problemas sem conexão. Após Fermat, o número de matemáticos que se propunham a estudar o assunto aumentou consideravelmente e assim, os problemas começaram a ter conexão, pois tinham natureza aritmética. Nessa perspectiva, o desenvolvimento científico ganhou grande impulso na Europa, sistematizando e organizando o estudo da Teoria dos Números através de problemas definidos.

Outro matemático considerável na área foi Euler. Ele começou a demonstrar seu interesse pela Teoria dos Números após algumas trocas de correspondências com Christian Goldbach, matemático russo, nascido em 18 de março de 1690. Foi através de Goldbach que Euler teve acesso à obra de Fermat, quando em uma carta destinada a Euler, em 1729, Goldbach questiona: *Você conhece a observação de Fermat de que todos os números $2^{2^n} + 1$ são primos?*

Em um primeiro instante, Euler não teve nenhuma reação de interesse sobre seu questionamento, mas Goldbach insiste e, por volta de 1730 à obra de Fermat começa a

⁵ É o termo usado para identificar o período da história da Europa entre os séculos XIV e XVII, onde ocorreram transformações nos vários setores da sociedade destacando-se os setores artístico, filosófico e científico.

ser estudada por Euler. “Nos anos seguintes, ele estenderia e provaria grande parte dos resultados enunciados por Fermat” (COUTINHO, 2009, p. 11). Sendo assim, em pouco tempo, ou mais precisamente em 1732, Euler mostrou que a conjectura acima é falsa para n igual a cinco. Dessa maneira, Goldbach além de provocar o interesse de Euler pelas conjecturas de Fermat, oferece outras conjecturas. “Através de seus trabalhos, Euler popularizou a Teoria dos Números como Fermat não o havia conseguido”. (COUTINHO, 2009, p. 11).

Assim, diante da geração de matemáticos modernos, Joseph L. Lagrange ganhará destaque pelo seu interesse em relação à Teoria dos Números. Ele nasceu em 1736 e viveu até 1813, na cidade de Turim, na Itália. “Lagrange é em geral considerado o mais notável matemático do século dezoito, sendo somente Euler um sério rival” (BOYER, 1974, p. 360). Contribuiu de forma ímpar para o desenvolvimento da Teoria dos Números. Um exemplo notório de sua contribuição foi à realização da primeira prova de um resultado conhecido como Teorema de Wilson: *para qualquer primo p , o inteiro $(p - 1)! + 1$ é divisível por p .*

Em 30 de abril de 1777, nasce aquele que é conhecido como “Príncipe dos Matemáticos”, o alemão Carl F. Gauss. Sua habilidade com a Matemática manifestou-se logo na infância e foi notada num certo dia quando o professor mandou que os alunos somassem os números de 1 a 100 e imediatamente Gauss achou a resposta: 5050, aparentemente sem cálculos. Supõe-se que já neste momento, ele tivesse descoberto a fórmula para a soma de uma progressão aritmética. No campo da Teoria dos Números, Gauss entrou numa busca crítica das demonstrações realizadas por seus antecessores na perspectiva de completar o que não tinha sido feito em sua totalidade e identificar algumas lacunas, especialmente, no campo da Aritmética.

Gauss, em 1801 publica “*Disquisitiones Arithmeticae*”, seu trabalho mais conhecido, um livro sobre Teoria dos Números. Essa obra trata da teoria das congruências, da teoria dos restos quadráticos e do estudo das equações binômias e suas ligações com a construção de polígonos regulares. “Essa obra célebre é a principal responsável pelo desenvolvimento da linguagem e notação do ramo da Teoria dos Números conhecido como álgebra das congruências, que fornece um exemplo de classes de equivalência” (BOYER, 1974, p.371).

Ainda nesta obra Gauss apresenta a lei da reciprocidade quadrática, nomeada por ele como a “joia da aritmética”. Em concordância com Shokranian (2010), no momento que Gauss introduz a Aritmética Modular, traz consequências relevantes para Teoria dos

Números, ou seja, aborda o estudo dos números inteiros em dois viés: as equações diofantinas e a divisibilidade. Com isso, grande parte dos problemas e conjecturas passou a ser entendido através da linguagem das congruências, por exemplo, $a^{p-1} \equiv 1 \pmod{m}$ é equivalente ao Pequeno Teorema de Fermat.

Tem-se também como ponto marcante do século XX, a prova do último Teorema de Fermat, que foi apresentada à comunidade Matemática em 1993, como corolário da demonstração de uma conjectura (Conjectura de Shimura-Taniyama). Wiles utilizou ideias de geometria não euclidiana, análise harmônica sobre grupos, álgebra comutativa e de teoria de números algébricos para conseguir resolver essa conjectura. Sendo assim, mais de três séculos depois, consegue-se resposta indiscutível para o Último Teorema de Fermat.

Para Shokranian (2010), atualmente a Teoria dos Números é mais ampla enquanto campo de conhecimento do que foi na Antiguidade, tendo em vista que, a partir do século XX, as aplicações começaram a surgir com domínio na Teoria dos Números, e em paralelo com outros campos da Matemática. Portanto, reforça-se que o estudo da Teoria dos Números vem junto com o surgimento das civilizações e em paralelo com sua evolução, fixando-se assim como uma das áreas mais antigas da Matemática. Porém, enquanto disciplina com um conhecimento sistematizado, é um campo novo e está em pleno crescimento, com contribuições importantes para o desenvolvimento científico.

1.2 O que é Aritmética Modular?

Para chegarmos ao conceito do que é de fato a Aritmética Modular, faz-se a seguinte pergunta: O que é Aritmética? É uma palavra proveniente do grego *arithmetiké* e significa: ciência dos números. Ainda, segundo Peano (1889) e Alfonso (1876) *apud* Sant'Anna (2013), temos um breve discurso o qual responde o mesmo questionamento.

Mestre: "O que é Aritmética?"

Discípulo: "É a arte de contar, ou a ciência dos números, que considera sua natureza e propriedades, possibilitando meios mais simples para expressá-los, compreendê-los, resolvê-los, que é o que chamamos calcular".

(PEANO, Giuseppe, Principia de Arithmetices, 1889 *apud* Sant'Anna, p.9, 2013).

Pergunta: "O que é aritmética?"

Resposta: "A ciência que trata da quantidade discreta".

P.: "Que é quantidade?"

R.: "Tudo o que pode aumentar ou diminuir".

P.: "Sob este ponto de vista, tudo o que existe no universo é quantidade?"

R.: "Sim, senhor. Tudo é quantidade, exceto Deus".

(A. GALLEGO CHAVES, Aritmética para niños, 1876 *apud* Sant'Anna, p.9, 2013).

Em concordância com os autores, afirmamos que a Aritmética é a parte da Matemática que estuda os números, as propriedades e as operações numéricas (soma, subtração, multiplicação e divisão).

A Aritmética Modular é um instrumento de fundamental importância na disciplina Teoria dos Números, trazendo consigo o importante conceito de congruência. Apresentamos as propriedades que seguem da definição de congruência módulo m , como a validade das propriedades reflexiva, simétrica e transitiva que garantem a congruência ser uma relação de equivalência. Sendo assim, esse conteúdo já possibilita explorar as aplicações da Aritmética Modular nos critérios de divisibilidade, nos sistemas de identificação CPF, ISBN, EAN-13, e na criptografia, por exemplo.

1.3 Definições e propriedades da Aritmética Modular.

Antes de enunciar e demonstrar algumas propriedades vale ressaltar que estamos apenas trabalhando com o conjunto dos números inteiros $\mathbb{Z}$ e suas respectivas operações de multiplicação ($\cdot$) e adição ($+$). Os resultados abaixo também podem ser vistos nos livros Elementos de Aritmética⁶ e Introdução à Teoria dos Números⁷.

Iniciamos com o conceito básico de divisibilidade, apresentando em seguida alguns critérios de divisibilidade que são ensinados no Ensino Básico.

Definição 1: Se a e b são inteiros, dizemos que a divide b , denotando por $a|b$, se existir um inteiro c tal que $b = a \cdot c$.

Observação 1: Se a não divide b , escreveremos $a \nmid b$.

Exemplo 1: $-5|10$, pois existe $c = -2$ tal que $10 = (-5) \cdot (-2)$.

Exemplo 2: $7 \nmid 10$, pois não existe $c \in \mathbb{Z}$ tal que $10 = 7 \cdot c$.

Um resultado central da Teoria dos Números é a Divisão Euclidiana a qual enunciamos e demonstramos a seguir, mostrando que a mesma não se constitui como importante apenas na obra de Euclides.

⁶ Hefez, Abramo, 2a edição, SBM, 2005.

⁷ Santos, José Plínio de Oliveira, 3. Ed. Rio de Janeiro: IMPA, 2012.

Teorema 1(Divisão Euclidiana). Sejam a e b dois números naturais com $0 < a < b$.
Existem dois únicos números naturais q e r tais que

$$b = a \cdot q + r, \text{ com } r < a.$$

Demonstração:

Suponhamos que $b > a$ e $\{q \in \mathbb{N}; b - q \cdot a \in \mathbb{N}\}$. Considere a seguinte lista de números:

$$b, b - a, b - 2 \cdot a, b - 3 \cdot a, \dots, b - n \cdot a, \dots \quad (1)$$

Essa lista de números naturais é decrescente, logo finita e, portanto possui um menor elemento. Chamamos de r o menor elemento da lista (1) pelo Princípio da Boa Ordem, no qual todo conjunto não-vazio de inteiros positivos contém um elemento mínimo. Então, existirá um número natural q tal que $r = b - q \cdot a$, sendo o último número natural da lista, ou seja,

$$b, b - a, b - 2 \cdot a, b - 3 \cdot a, \dots, b - n \cdot a, \dots, b - q \cdot a.$$

Como r é um número natural, tem-se $0 \leq r$. Para $r = 0$, o resultado é imediato. Então, basta verificar que $0 < r < a$. Suponha que $r \geq a$. Então existe um número natural c , com $c < r$, tal que $r = c + a$.

Daí,

$$c + a = r = b - q \cdot a$$

$$c = b - q \cdot a - a$$

$$c = b - (q + 1) \cdot a.$$

Dessa forma $c = b - (q + 1) \cdot a$ e c é um elemento da lista (1) menor do que r , o que contradiz a hipótese, pois r é o menor elemento da lista (1), com $r = b - q \cdot a$. Portanto, temos que $b = a \cdot q + r$, com $r < a$, o que prova a existência de q e r .

Mostremos agora a unicidade. Sejam $b = q \cdot a + r$ e $b = q' \cdot a + r'$, com $r < a$ e $r' < a$. Suponha, sem perda de generalidade, que $r \leq r'$. Logo,

$$r \leq r' \Rightarrow 0 \leq r' - r = -q' \cdot a + q \cdot a = (q - q') \cdot a,$$

e

$$0 \leq r \leq r' < a \Rightarrow 0 \leq r' - r < a.$$

Daí,

$$0 \leq (q - q') \cdot a < a \Rightarrow 0 \leq q - q' < 1 \Rightarrow q' - q = 0 \Rightarrow q = q'.$$

Dessa forma, $r = r'$. Portanto, r e q são únicos tais que $b = q \cdot a + r$, com $r < a$.

■

Teorema 2(Algoritmo da Divisão). Sejam a e b números inteiros com $b > 0$, então existem únicos r e q , inteiros, tais que: $a = b \cdot q + r$, com $0 \leq r < b$, onde r é o resto e q é o quociente da divisão.

Demonstração:

O caso de a e b serem números naturais já foi estudado no Teorema 1. Analisaremos agora, o que ocorre com o quociente e o resto na divisão de um número inteiro negativo. Suponha que $a < 0$. Logo, $-a > 0$. Do Teorema 1, tem-se que existem únicos q' e r' tais que $-a = q' \cdot b + r'$, em que $0 \leq r' < b$. Daí,

$$-a = q' \cdot b + r'$$

$$a = -q' \cdot b - r'$$

$$a = -q' \cdot b - b + b - r'$$

$$a = (-q' - 1) \cdot b + b - r', 0 \leq b - r' < b.$$

Dessa forma, $q = (-q' - 1)$ cumpre o papel do quociente, enquanto que $r = b - r'$ representa o resto da divisão de a por b , ficando clara a existência de r e q .

A partir do Teorema 1, onde foi provada a unicidade de q' e de r' , fica garantida a unicidade de q e r .

■

Exemplo 3: Três amigos possuem uma conta em conjunto com saldo devedor de 650 reais. Eles querem dividir o valor igualmente e pagar essa dívida através de um depósito em dinheiro no caixa eletrônico. Sabendo que não é permitido colocar moedas no envelope, qual será o saldo da conta após os três terem depositado o mesmo valor, sendo este valor a menor quantia necessária para quitar a dívida?

Solução:

Fazendo a divisão euclidiana da dívida de 650 reais por 3, tem-se:

$$-650 = (-217) \cdot 3 + 1.$$

Portanto, os três amigos depositarão 217 individualmente e dessa forma sobrará 1 real de saldo positivo na conta.

Definição 2(Paridade de um inteiro). Seja $b = 2$ e $a \in \mathbb{Z}$. Se na divisão de a por b o resto for igual à zero, dizemos que a é um inteiro par. Agora se o resto for 1, dizemos que a é um inteiro ímpar.

Observação 2: É imediato verificar que se a for par tem-se $a = 2 \cdot q$ e se a for ímpar tem-se $a = 2 \cdot q + 1$.

Exemplo 4: Verifique que na divisão de a^2 por 4, com $a \in \mathbb{Z}$, obtemos restos 0 ou 1.

Solução:

Seja $a \in \mathbb{Z}$. Se a for par, então $a = 2 \cdot q$. Daí,

$$a^2 = (2 \cdot q)^2 = 2^2 \cdot q^2 = 4 \cdot q^2 + 0.$$

Logo, a^2 deixa resto zero quando dividido por 4. Se a for ímpar, então

$$a = 2 \cdot q + 1.$$

Daí,

$$a^2 = (2 \cdot q + 1)^2 = 4 \cdot q^2 + 4 \cdot q + 1 = 4 \cdot (q^2 + q) + 1.$$

Logo, a^2 deixa resto 1 quando dividido por 4.

Definição 3: O máximo divisor comum de dois números inteiros a e b (a ou b diferente de zero), denotado por (a, b) , é o maior inteiro que divide a e b .

Com essa definição podemos afirmar algumas propriedades. O máximo divisor comum de dois números é único, pois, se ambos d e d' são máximos divisores comuns de um par de números, a e b , então $d \geq d'$, pois d é o maior divisor comum de a e b , e d' é outro divisor comum. De modo análogo, mostra-se que $d' \geq d$. Neste caso, conclui-se que $d = d'$. Uma propriedade imediata é que não importa a ordem do par de números a e b , ou seja, $mdc(a, b) = mdc(b, a)$.

Podemos usar o Algoritmo da Divisão (Teorema 2) para encontramos o máximo divisor entre dois números, o que foge da resolução comum, que seria o método de decomposição em números primos.

Exemplo 5: Qual é máximo divisor comum de 1126 e 522?

Solução: Utilizando a divisão euclidiana para dividir 1126 por 522, em seguida dividindo 522 por 82, que é o resto da divisão anterior e assim, sucessivamente, até obtermos resto zero. Teremos que todo divisor comum de dois números, também será divisor do resto da divisão desses números, ou seja, $mdc(1126, 522)$ é igual ao $mdc(522, r)$ sendo r o resto da divisão de 1126 por 522. Então,

$$1126 = 2 \cdot 522 + 82$$

$$522 = 6 \cdot 82 + 30$$

$$82 = 2 \cdot 30 + 22$$

$$30 = 1 \cdot 22 + 8$$

$$22 = 2 \cdot 8 + 6$$

$$8 = 1 \cdot 6 + 2$$

$$6 = 3 \cdot 2 + 0$$

Observe que da última equação temos $\text{mdc}(6,2) = 2$, e portanto: $\text{mdc}(1126,522)$ é igual ao $\text{mdc}(522,82)$, e também $\text{mdc}(82,30)$ é igual ao $\text{mdc}(30,22)$ e continuando $\text{mdc}(22,8)$ é igual ao $\text{mdc}(8,6)$, que é igual ao $\text{mdc}(6,2) = 2$, isto é, $\text{mdc}(1126,522) = 2$.

A depender dos números dados, essa resolução a partir da divisão euclidiana fica mais prática que a resolução por decomposição em fatores primos. Vejamos outro exemplo.

Exemplo 6: Usando o algoritmo da decomposição em fatores primos, determine o $\text{mdc}(100,120)$.

Solução: Fazendo as decomposições dos números 100 e 120 respectivamente:

$$\begin{array}{r|l} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

$$\begin{array}{r|l} 120 & 2 \\ 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

Como $100 = 2^2 \cdot 5^2$ e $120 = 2^3 \cdot 3 \cdot 5$, o $\text{mdc}(100,120)$ será o produto dos fatores primos comuns com o menor dos expoentes de cada fator primo comum, ou seja,

$$\text{mdc}(100,120) = 2^2 \cdot 5 = 4 \cdot 5 = 20.$$

Este exemplo mostra a vantagem de um método em relação ao outro método. Observe o mesmo exemplo cuja solução é obtida através da divisão euclidiana:

$$120 = 1 \cdot 100 + 20$$

$$100 = 5 \cdot 20 + 0$$

Portanto, o $\text{mdc}(100,120) = 20$. Note que, com a resolução de apenas dois algoritmos, obteve-se o resultado desejado, diferentemente da decomposição por fatores primos.

Conseguimos também estabelecer certas similaridades. Quando dados dois números inteiros distintos, obtivermos o mesmo resto na divisão deles por um inteiro qualquer. Isto é, dados 14 e 50 inteiros quaisquer, deixam resto 2 quando divididos por 6. Se somarmos ou subtrairmos de ambos o mesmo valor, ainda obteremos o mesmo resto quando divididos por 6. Vejamos:

$$14 + 10 = 24$$

e

$$50 + 10 = 60.$$

Notemos que 24 e 60 deixam resto zero na divisão por 6.

Tem-se a congruência como um dos principais tópicos dessa pesquisa juntamente com a Aritmética dos restos, com o objetivo de enaltecer a divisão euclidiana nos números naturais e inteiros e mostrar o conceito do próprio resto, o que será de fundamental importância para o desenvolvimento das aplicações contidas no Capítulo 3.

Definição 4: Se a e b são inteiros dizemos que a é congruente a b módulo m ($m > 0$) quando $m|(a - b)$. Denotamos por $a \equiv b(mod\ m)$. Se $m \nmid (a - b)$, dizemos que a é incongruente a b módulo m . Denotamos por $a \not\equiv b(mod\ m)$.

Exemplo 7: $133 \equiv 97(mod\ 4)$, pois $133 = 4 \cdot 33 + 1$ e $97 = 4 \cdot 24 + 1$ ambos têm resto 1 na divisão por 4, e ainda $4|133 - 97$.

De maneira análoga, $17 \not\equiv 11(mod\ 5)$, pois $17 = 5 \cdot 3 + 2$ e $11 = 5 \cdot 2 + 1$ ambos têm restos diferentes na divisão por 5, e ainda $5 \nmid 17 - 11$.

Proposição 1: a e b são inteiros e $a \equiv b(mod\ m)$ se, e somente se, existe um inteiro k tal que

$$a = b + k \cdot m.$$

Demonstração: Se $a \equiv b(mod\ m)$, então $m|a - b$. Assim, existe $k \in \mathbb{Z}$ tal que

$$k \cdot m = a - b,$$

ou seja,

$$a = b + k \cdot m.$$

Reciprocamente, se existe $k \in \mathbb{Z}$ tal que

$$a = b + k \cdot m,$$

então,

$$a - b = k \cdot m,$$

ou seja, $m|a - b$, e portanto, $a \equiv b(\text{mod } m)$.

■

Proposição 2 (Relações de equivalência). Seja $m \in \mathbb{Z}$, com $m > 0$. Para quaisquer $a, b, c \in \mathbb{Z}$, vale:

- (i) $a \equiv a(\text{mod } m)$;
- (ii) $a \equiv b(\text{mod } m) \Rightarrow b \equiv a(\text{mod } m)$;
- (iii) $a \equiv b(\text{mod } m)$ e $b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m)$.

Demonstração: As três propriedades acima são conhecidas respectivamente como, reflexiva, simétrica e transitiva. Iremos demonstrar cada uma.

(i) Seja $a \in \mathbb{Z}$. Observe que

$$a - a = 0 = m \cdot 0.$$

Logo, existe $k \in \mathbb{Z}$, a saber, $k = 0$ tal que,

$$a - a = m \cdot k.$$

Portanto,

$$a \equiv a(\text{mod } m).$$

(ii) Considere $a, b \in \mathbb{Z}$. Existe $k' \in \mathbb{Z}$ de forma que $a - b = m \cdot k'$. Observe que

$$b - a = -(a - b) = -m \cdot k' = m(-k').$$

Tomando $k = -k' \in \mathbb{Z}$, segue que

$$b - a = m \cdot k.$$

Portanto,

$$b \equiv a(\text{mod } m).$$

(iii) Sejam $a, b \in \mathbb{Z}$ tais que

$$a \equiv b(\text{mod } m) \text{ e } b \equiv c(\text{mod } m),$$

ou seja, existem $k', k'' \in \mathbb{Z}$ de forma que

$$a - b = m \cdot k' \text{ e } b - c = m \cdot k''.$$

Note que

$$a - c = a - b + b - c = (a - b) + (b - c) = m \cdot k' + m \cdot k'' = m \cdot (k' + k'').$$

Fazendo $k = k' + k'' \in \mathbb{Z}$, obtemos

$$a - c = m \cdot k.$$

Portanto,

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

■

Proposição 3: Sejam a, b, c, d e $m \in \mathbb{Z}$, com $m > 1$. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:

- (i) $a \pm c \equiv b \pm d \pmod{m}$;
- (ii) $a \cdot c \equiv b \cdot d \pmod{m}$.

Demonstração: Os itens acima serão provados respectivamente:

- (i) Pelas hipóteses, temos que

$$m|a - b \text{ e } m|c - d \Rightarrow m|(a \pm c) - (b \pm d).$$

Daí,

$$a \pm c \equiv b \pm d \pmod{m}.$$

- (ii) Pelas hipóteses, existem k e $k' \in \mathbb{Z}$

$$a \cdot c = b \cdot c + k \cdot m \cdot c \quad (1)$$

e

$$b \cdot c = b \cdot d + b \cdot k' \cdot m.$$

Substituindo $b \cdot c$ na equação (1), tem-se

$$a \cdot c = b \cdot d + b \cdot k' \cdot m + k \cdot m \cdot c = b \cdot d + m(b \cdot k' + k \cdot c).$$

Daí,

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

ou seja,

$$a \cdot c \equiv b \cdot d \pmod{m}.$$

■

Exemplo 8: $16 \equiv 37 \pmod{7}$, pois 16 e 37 deixam restos 2 na divisão por 7. Temos ainda que $32 \equiv 60 \pmod{7}$, pois 32 e 60 deixam restos 4 na divisão por 7. Assim, $16 + 32 \equiv 37 + 60 \pmod{7}$, ou seja, $48 \equiv 97 \pmod{7}$, pois 48 e 97 deixam restos 6 na divisão por 7. Podemos observar também que, $16 \cdot 32 \equiv 37 \cdot 60 \pmod{7}$, isto é, $512 \equiv 2220 \pmod{7}$, pois 512 e 2220 deixam restos 1 na divisão por 7.

Salientamos que não consta neste trabalho todos os Teoremas, Propriedades e Proposições da disciplina de Teoria dos Números, tendo em vista que os mais importantes para prosseguir com o desenvolvimento da pesquisa e os quais serão usados na resolução das aplicações que abordamos no capítulo 3 foram devidamente enunciados e demonstrados neste capítulo.

2. O LIVRO DIDÁTICO NO PROCESSO DE ENSINO E APRENDIZAGEM

Abordamos o livro didático em um contexto sobre materiais didáticos, pois o mesmo se caracteriza como um dos recursos mais utilizados pelos professores no processo de ensino e aprendizagem. Evidenciamos sua importância e influência com relação à instituição escolar desde o Ensino Infantil até o Ensino Superior. Para reafirmar a sua importância, analisamos como se constitui esse material didático, assim como também abordamos o conceito do livro didático no Brasil e sua influência no âmbito do ensino enquanto instrumento de aprendizagem.

2.1 O livro didático enquanto material didático.

O livro didático é considerado por vários autores como um material didático, dependendo de que forma e com qual finalidade ele estará sendo usado. Diante deste aspecto, algumas inquietações surgem, ou seja, o que é um material? Qual o conceito de didático? E ainda, o que é um material ser didático?

Ao ser analisada a palavra material, encontra-se diferentes conceitos nas diversas áreas de conhecimento. No entanto, aquela que apresenta elementos em sua totalidade para este estudo é descrita por Ferreira (2001, p. 451) que define *material*, sendo o “conjunto dos objetos que formam uma obra, construção [...]”. Sendo assim, material é a reunião de objetos para desencadear algum fim. E didático? De acordo com o Dicionário Aurélio, *didático* é algo “que é próprio ou relativo ao ensino, à instrução; que tem por fim instruir”. Desta forma, ser didático é ter como finalidade a instrução, ou seja, facilitar o processo de ensino e aprendizagem. Então, a unção dos dois conceitos nos mostra o conceito de material didático que, segundo Bandeira (2011, p. 14), “[...] pode ser definido amplamente como produtos pedagógicos utilizados na educação e, especificamente, como material instrucional que se elabora com finalidade didática”.

Considera-se didático o material que reúna meios e recursos que facilitem e auxiliem o ensino e a aprendizagem, ou seja, utilizado no âmbito educativo para facilitar a aquisição de conceitos, habilidades e atitudes. Podendo ser considerados como suporte os recursos impressos, audiovisual, visual ou auditivo, por exemplo. A garantia da presença desses materiais didáticos no contexto escolar é estabelecida conforme a Lei de Diretrizes e Bases da Educação Nacional (LDB), nº. 9394/96, art. 4º, inciso VIII. E é atribuída ao estado, que deve garantir “atendimento ao educando, em todas as etapas da

educação básica, por meio de programas suplementares de material didático-escolar [...]” (BRASIL, 1996, p. 03).

Os materiais didáticos se caracterizam por subsidiar os professores em seu trabalho docente, sendo reconhecidos como instrumentos importantes no processo da ação educacional. Com isso, pode-se destacar uma diversidade de materiais didáticos presentes nas diversas áreas de ensino. Em relação ao ensino da Matemática, podemos usar inúmeros objetos como materiais concretos, que vão desde recursos tecnológicos até os materiais palpáveis. Porém, diante dessa diversidade de materiais didáticos, o que se destaca é o livro didático, que atende todos os níveis educacionais e é utilizado constantemente nas salas de aula.

A utilização de livros didáticos em aulas de Matemática é uma prática comum entre professores da área. No entanto, para utilizar este artifício de ensino devem-se considerar alguns parâmetros, evitando-se a utilização como único recurso pedagógico e/ou a utilização de livros inadequados ao contexto escolar em que se atua. Segundo Freitas (2007, p. 89), a partir do Ensino Fundamental até o superior, “o livro torna-se um poderoso instrumento na mediação dos conhecimentos necessários à construção do sujeito”. O mesmo traz como artefatos incorporados ao trabalho escolar, condições em que o ensino e a aprendizagem se realizem e, neste sentido, eles têm uma grande importância e podem cumprir funções específicas, dependendo de suas características e das formas pelas quais eles participam da produção das aulas. Consequentemente, no contexto escolar, esse material didático torna-se instrumento necessário ao profissional da educação, influenciando em aspectos fundamentais para uma aprendizagem significativa. Essa influência é destacada por Freitas (2007, p. 89) quando faz a ressalva da contribuição desse material para a educação.

O livro didático é um dos mais fortes e influentes recursos encontrados nas escolas brasileiras. Cabe a ele um papel bastante relevante: o de apresentar às crianças o mundo da escrita e sua forma peculiar de construir conhecimentos que são socialmente reconhecidos, legitimados, valorizados. E é essa legitimação social que faz com que seja o livro, ainda que em realidades culturais materialmente desenvolvidas, a âncora das práticas pedagógicas. (FREITAS, 2007, p. 89).

Ainda em concordância com os Parâmetros Curriculares Nacionais (PCN), temos que:

Ao se pensar em percursos de aprendizagem, não se pode deixar de mencionar a importância do livro didático, mesmo porque, em muitas das nossas escolas, ele é o material didático mais utilizado pelo professor. Ele pode ser uma excelente ferramenta no processo de

ensino e aprendizagem e não pode ser desconsiderado pelo professor. Sabemos que, em muitos contextos, é o livro didático que define o que será estudado e, mais que isso, como será estudado, ou seja, define os conteúdos e a metodologia de ensino adotados pelos docentes. (BRASIL, 2012, p.51)

Por isso, é fundamental que o docente saiba analisar e usar o livro didático de forma adequada, pois é através dele que o mesmo pode dinamizar as aulas exercendo com maior afinco o papel de docente e contribuindo no processo de aprendizagem a partir do ensino. No entanto, para utilizar esse artifício de ensino (ênfase na Matemática), devem-se considerar alguns parâmetros, evitando-se a escolha de livros nos quais não tenham exemplificações claras, contexto histórico e não proponha o uso de aplicações relacionando à teoria, muitas vezes abstrata, com as aplicações práticas do cotidiano.

2.2 O processo de ensino e aprendizagem: uma visão a partir do livro didático.

O processo de ensino e aprendizagem tem como complementação e orientação o livro didático que se constitui como um material de apoio ao profissional de educação. De acordo com o Guia de Livros Didáticos de Matemática (PNLD⁸ Matemática 2014, p.12), “no processo de ensino e aprendizagem, o livro didático é um interlocutor que dialoga com o professor e com o aluno. Nesse diálogo, o livro é portador de uma perspectiva sobre o saber a ser estudado e sobre o modo mais eficaz de aprendê-lo”. Ainda em concordância com o Guia de Livros Didáticos de Matemática (PNLD Matemática 2013, p.12), este afirma que o ensino de Matemática “[...] não se reduz a transmissão de informação sobre o saber acumulado neste campo”.

O envolvimento do docente na escolha dos recursos didáticos, os quais irão levar para trabalhar com os discentes, em especial o livro didático, deve ser bastante criterioso. Faz-se necessário discutir critérios os quais instrumentalizem o processo dessa escolha e fomentem de fato a discussão sobre os caminhos que se deseja trilhar na educação, e assim poder escolher um material que estimule a atuação do docente e desperte o querer aprender do discente. Libâneo (1990) *apud* Vasconcelos e Souto (2003), ainda ressalta que:

Ao selecionar os conteúdos da série em que irá trabalhar, o professor precisa analisar os textos, verificar como são abordados os assuntos, para enriquecê-los com sua própria contribuição e a dos alunos, comparando o que se afirmar com fatos, problemas, realidades de

⁸ Programa Nacional do Livro Didático.

vivência real dos alunos [...]. Ao recorrer ao livro didático para escolher os conteúdos, elaborar o plano de ensino e de aulas, é necessário ao professor o domínio seguro da matéria e bastante sensibilidade crítica. (Libâneo (1990) *apud* Vasconcelos e Souto p.101, 2003).

Com base nessas ideias, é perceptível que os docentes devem fazer uma análise com tópicos pertinentes a escolha do livro didático e assim estimular o debate neste sentido. Portanto, os docentes devem ter critérios próprios para selecionar o material mais adequado, considerando suas necessidades e principalmente a dos discentes, visando possibilidades de contextualização e quaisquer recursos adicionais que favoreçam o diálogo educativo entre discente, docente e o livro didático.

Freitas (2007, p. 13) argumenta que o processo de ensino e aprendizagem é formado por um desencadeamento de “[...] elementos que vão desde a postura do docente até os meios empregados para promover o ensino e garantir a aprendizagem”. Observa-se que o docente deve portar-se de uma postura crítica e sensível no desenvolvimento deste processo, principalmente no campo que está sendo abordada a pesquisa, pois, como se trabalha com futuros professores, e esses por sua vez irão se apropriar de métodos e didáticas adquiridos para fazer a intermediação do conhecimento com seus futuros alunos, então devem estar portando argumentos críticos e com veracidade.

Vale ressaltar que para o livro didático atingir o nível de importância dentro da educação, especificamente no Brasil, foram anos de decretos, análises e procedimentos diversos, visando sempre sua melhoria dentro do espaço educacional. Tanto do ponto de vista da abordagem de conteúdos quanto da metodologia de ensino e aprendizagem adotada, a cada ano fica mais criterioso a escolha desses exemplares para ocuparem o ambiente escolar, sempre procurando livros que deem subsídio para o trabalho pedagógico.

Propomos um recorte cronológico com alguns dos principais momentos na trajetória histórica do livro didático no Brasil. A pesquisa de Gomes (2014), feita para obtenção do título de mestre, analisa a influência do livro didático de Matemática no processo de ensino e aprendizagem. Vejamos alguns dados que constam no quadro abaixo.

Quadro 1- Percurso histórico do livro didático no Brasil.

Ano/Período histórico	Descrição
1930-1945 (Estado Novo)	-Políticas públicas mais consistentes sobre materiais didáticos, em detrimento as primeiras atividades desenvolvidas pelo Estado Novo, com relação a recursos educacionais; -Oficialização e regulamentação da primeira política de legislação e controle de produção dos livros didáticos. E Instituição da Comissão Nacional do Livro Didático (CNLD). Tudo por meio do Decreto n. 1.006, de 30/12/1938.
1964-1984 (Regime Militar)	-Novos acordos educacionais; -Acordos entre o Ministério da Educação (MEC) e a Agência Norte-Americana para o Desenvolvimento Internacional (USAID), capacitar de forma técnica por meio do livro didático; -Severo controle no sistema educacional e nos materiais didáticos, a fim de atender a demanda do novo contexto escolar que estava para surgir.
1985	-Após fim do período Militar, cria-se um novo programa responsável pela compra e distribuição dos livros didáticos o PNLD (Programa Nacional do Livro Didático), por meio do Decreto nº 91.542. Este permanece até os dias atuais.
1990	-Discussão mais sistemática pelo Ministério da Educação (MEC), sobre a qualidade do livro didático; -Novos projetos pedagógicos divulgados por meio dos Guias do livro didático e dos Parâmetros Curriculares Nacionais (PCN).
1996	-Inicia-se o processo de avaliação pedagógica dos livros inscritos para o PNLD 1997.
2010	-Decreto 7084, de 27 de janeiro de 2010. Regula a participação das escolas e procedimentos de escolha do livro didático no PNLD.

Fonte: Gomes, Daiane, 2014.

A partir desse explanado histórico, se configura a devida importância que o livro didático tem na educação brasileira, e é nessa perspectiva que os docentes têm que perceber sua relevância na influência da aprendizagem. Por isso, destacamos que a ação desenvolvida pelo profissional docente nesse processo é valiosa e construtiva, desde o

momento da escolha do material didático a ser trabalhado até as propostas educativas por ele apresentadas no intuito de intermediar a aprendizagem a partir de seu ensino.

O livro didático está ligado a um conjunto de valores ideológicos e culturais, os quais estão imersos na sociedade, e isso mostra o poder desse instrumento pedagógico e o quão importante ele se configura no processo de construção do conhecimento. Dessa forma, cabe aos docentes à responsabilidade da escolha do livro até a forma mais adequada de usar esse recurso. Conforme salienta Romanatto (1987),

...o livro didático ainda tem uma presença marcante em sala de aula e, muitas vezes, como substituto do professor quando deveria ser mais um dos elementos de apoio ao trabalho docente. ...os conteúdos e métodos utilizados pelo professor em sala de aula estariam na dependência dos conteúdos e métodos propostos pelo livro didático adotado. Muitos fatores têm contribuído para que o livro didático tenha esse papel de protagonista na sala de aula. ... um livro que promete tudo pronto, tudo detalhado, bastando mandar o aluno abrir a página e fazer exercícios, é uma atração irresistível. O livro didático não é um mero instrumento como qualquer outro em sala de aula e também não está desaparecendo diante dos modernos meios de comunicação. O que se questiona é a sua qualidade. Claro que existem as exceções (ROMANATTO, 1987, p.85).

Ao escolher o livro didático, o docente, entre outros critérios, deve considerar a proposta pedagógica, os modos de contextualização e apresentação dos conteúdos, nível de complexidade e relações estabelecidas com o cotidiano dos estudantes. Todo esse cuidado se deve ao que destaca Biehl e Bayer (2009, p. 02): “[...] o livro didático é um dos mais importantes componentes do cotidiano escolar em todos os níveis de ensino”, tendo em vista ser ele um recurso de fácil acesso, tanto para o docente quanto para os discentes. E por ser um recurso que exprime acessibilidade, deve estar de acordo com a realidade e interligado com uma proposta de contemplação estimulada pelo docente. Como diz Biehl e Bayer:

Um bom projeto educacional exige um professor atuante, com uma prática que se apropria da realidade como instrumento pedagógico e que utiliza os materiais didáticos disponíveis, incluindo o livro didático, de forma apropriada e devidamente contextualizada com o processo de ensino- aprendizagem. Só podemos dizer que um livro é completo se ele está bem inserido neste contexto. (BIEHL E BAYER, 2009, p. 11).

Compreende-se que o livro didático de Matemática como recurso auxiliar na apresentação dos conteúdos pode contribuir no ensino do docente e, principalmente, na aprendizagem do discente, associando as atividades propostas em sala com situações nas quais o mesmo possa perceber a aplicação destas em suas atividades diárias. O livro

precisa assumir a função de texto de referência. Por isso a importância de fazer a ligação com os conteúdos abordados em sala de aula com aspectos do cotidiano.

É pertinente termos sempre a consciência que “[...] o livro didático pode mostrar-se como instrumento eficiente, mas cabe ao professor o papel de mediador insubstituível dentro do processo de ensino e aprendizagem.” (BIEHL e BAYER, 2009, p. 07). Portanto, a forma pedagógica com que o docente irá trabalhar com o livro didático vai estabelecer se as possíveis funções do mesmo no processo de ensino e aprendizagem vão ser eficazes ou não.

3. A ARITMÉTICA MODULAR E SUAS APLICAÇÕES NO COTIDIANO

Nosso cotidiano está repleto de aplicações simples, porém úteis, da Aritmética Modular. Sabendo disso, pontuamos aqui algumas importantes e interessantes utilidades.

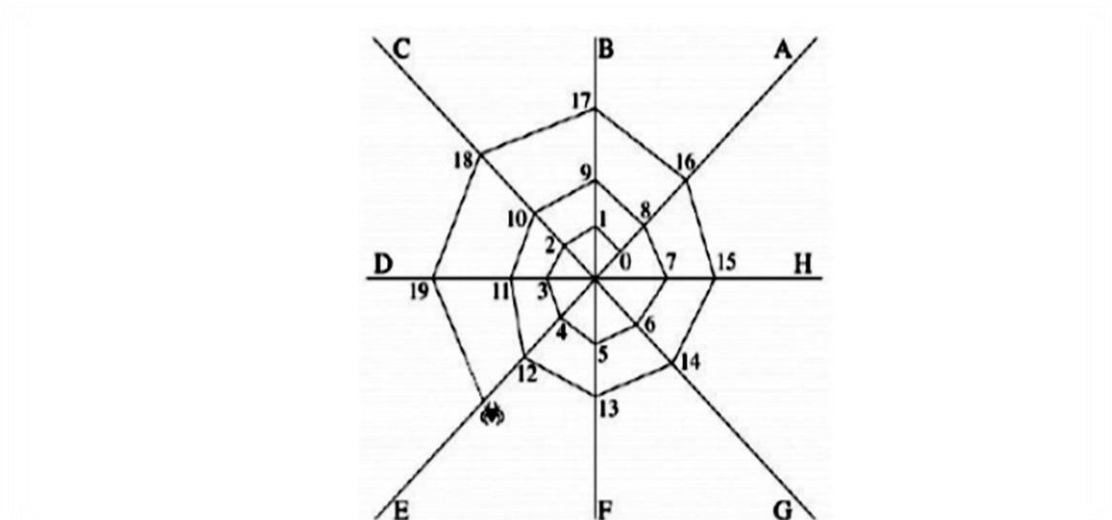
3.1 Exemplos básicos da Aritmética Modular.

A partir das definições e propriedades básicas expostas no Capítulo 1, temos ferramentas suficientes para resolver algumas atividades relacionadas à congruência. Vamos aqui desenvolver três exemplos que, segundo Sá (2007, p. 1-4) poderiam ser colocados a alunos ainda não familiarizados com o tema, como introdução ao assunto.

Visamos o aluno que ainda não teve o contato direto com as propriedades da congruência, assim não usufruindo delas para solucionar o problema, mais sim, a partir da estratégia usada para resolução do problema, se aproximar das propriedades da congruência. O primeiro exemplo foi retirado do banco de questões do site da OBMEP⁹.

Exemplo 1: A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?

Figura 1-Teia de aranha



Fonte: bancoobmep2010

⁹ Olimpíada Brasileira de Matemática das Escolas Públicas.

Solução: Observando a Teia de aranha, pode-se construir uma tabela relacionando cada fio aos respectivos números que estão contidos nele. Assim,

Quadro 2-Enumeração da Teia

FIOS	A	B	C	D	E	F	G	H
	0	1	2	3	4	5	6	7
	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23
	24	25	26	27	28	29	30	31
	...	...	...	...	...	...	...	...

Fonte: O autor, 2015.

Tem-se duas formas para a resolução do exemplo. O primeiro caminho seria continuar construindo a quadro até que aparecesse o número 118. Dessa forma, encontraríamos o fio que a aranha estaria. Porém, essa resolução não seria tão prática se por acaso o exemplo pedisse para indicarmos o fio correspondente ao número 1010.

O segundo caminho é a resolução por Aritmética Modular. Observemos que a cada oito números percorridos na teia, voltamos ao fio inicial, isto é, os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentem de oito em oito.

Notemos também que a partir dos múltiplos de oito, pode-se representar todos os fios. Sendo assim, o fio A corresponde aos números que são múltiplos de 8, ou seja, números que divididos por 8 deixam resto zero ($8 \cdot n + 0, \text{com } n \in \mathbb{N}$). O fio B corresponde aos números que são múltiplos de 8, mais 1, ou seja, números que divididos por 8 deixam resto 1 ($8 \cdot n + 1, \text{com } n \in \mathbb{N}$). Essa lógica se mantém até o fio H, no qual representa os números que divididos por oito deixam resto 7, ou seja, ($8 \cdot n + 7, \text{com } n \in \mathbb{N}$). Portanto, para sabermos em qual fio se encontra o número 118, basta analisarmos o resto na sua divisão por oito, que é 6, ou seja, pertence à família dos números que estão no fio G, pois todos os números que estão no fio G deixam resto 6 ao serem divididos por 8. E a essa particularidade dá-se o nome de congruência, isto é, todos os números do mesmo fio, são congruentes entre si, no módulo 8.

Exemplo 2: Aritmética do relógio (Que constitui de fato a definição de congruência). Analisemos um caso de congruência, módulo 12 (nos relógios analógicos).

Figura 2-Relógios Analógicos



Fonte: <http://www.bodet.pt>

Aplicação: Neste exemplo, vamos estabelecer as congruências no módulo 12, podendo perceber e entender a relação entre as horas em um relógio analógico.

Notemos que 13 horas e 1 hora, ambos divididos por 12, deixam resto 1, ou seja, são congruentes no módulo 12. E representamos assim,

$$1 \equiv 13(mod\ 12).$$

Observemos também que 19 horas é congruente a 7 horas, módulo 12. Pois, tanto 19, como 7, divididos por 12, deixam resto 7. Logo,

$$7 \equiv 19(mod\ 12).$$

E assim sucessivamente para todas as horas,

$$1 \equiv 13 \equiv 25 \equiv \dots (mod\ 12).$$

$$\vdots$$

$$7 \equiv 19 \equiv 31 \equiv \dots (mod\ 12).$$

$$\vdots$$

$$12 \equiv 24 \equiv 36 \equiv \dots (mod\ 12).$$

Como o módulo é doze, então todos os números naturais estarão na classe de equivalência dos restos na divisão por 12. Temos assim um caso clássico de congruência.

Exemplo 3: Em dezembro de 2014, não recordei bem a data, mas já estava planejando qual seria o dia da apresentação do meu Trabalho de conclusão de curso (TCC) em 2015. No entanto, só sabia o dia da semana referente ao 1º janeiro do referido ano, que iria ser numa quinta-feira. Pretendo apresentar o TCC em 7 de julho de 2015, porém não sei o dia que cairá essa data. Como faço para saber sem analisar o calendário?

Solução: Primeiramente iremos fazer a referência do dia com a data da primeira semana do ano, sendo isso possível, pois sabemos o dia referente ao 1º de janeiro de 2015. Portanto,

Quadro 3- Dia da semana/ data do mês.

Dia da semana	Data do mês
Quinta-feira	1
Sexta-feira	2
Sábado	3
Domingo	4
Segunda-feira	5
Terça-feira	6
Quarta-feira	7

Fonte: O autor, 2015.

Temos então aqui um caso de congruência, módulo 7, por se tratar dos sete dias da semana. Agora precisamos saber quantos dias existem de 1 de janeiro até 7 de julho de 2015. Vejamos:

Quadro 4- Meses do ano/ quantidade de dias.

Meses do ano	Quantidade de dias
Janeiro	31
Fevereiro	28(2015 não é bissexto)
Março	31
Abril	30
Maio	31
Junho	30
Julho	07
TOTAL	188

Fonte: O autor, 2015.

Agora, basta dividirmos 188 por 7 e o respectivo resto representará o dia da semana ao qual procuramos. Então,

$$\begin{array}{r} 188 \div 7 \\ 6 \quad 26 \end{array}$$

Logo, o 188 é congruente a 6 módulo 7, e como o dia 6 de janeiro de 2015 foi numa terça-feira, o 188º dia desse mesmo ano também o será e, também todas as demais terças-feiras deste ano serão ocupadas por números congruentes a 6 módulo 7.

A partir desses exemplos elencados por Sá (2007), é notório o quanto no nosso cotidiano existem fenômenos periódicos, e diante desse fato podem-se apresentar estas aplicações na disciplina Teoria dos Números, proporcionando a interação do futuro professor com exemplificações reais, onde se faz presente à noção de congruência módulo m .

3.2 Aplicações mais presentes no nosso dia a dia.

No nosso dia a dia, lidamos constantemente com números de identificação, os quais não conseguimos detectar tão facilmente se houver alguma troca entre seus algarismos. Diferentemente das letras, por exemplo, um erro de ortografia em determinada palavra é facilmente percebido. Diante da nossa dificuldade em perceber um erro entre os algarismos de um número de um código de identificação qualquer, foram criados os chamados dígitos de controle ou verificação, os quais são baseados normalmente na noção de congruência.

Apresentamos a seguir exemplos encontrados no nosso cotidiano de alguns casos de dígitos de controle usados como identificadores.

3.2.1 Códigos de barras EAN-13

O código de barras é um valioso instrumento nas atividades que desempenhamos na nossa vida, pois desde as compras no supermercado até os protocolos bancários estamos trabalhando com essa representação gráfica. Essa ferramenta permite o acesso mais rápido a diversas informações, diminuição de erros, atendimentos mais eficazes, gerenciamento remoto, entre outros.

Fica evidente a motivação para trabalhar os códigos de barras em sala de aula tratando-se de aplicações da Aritmética Modular, uma vez que é um elemento presente no mundo todo e que serve para fazer identificações em diversas áreas como: indústria, comércio, bancos, bibliotecas, hospitais, correios, transportes, controles de acesso.

O EAN-13 é um dos códigos de barras mais utilizados no mundo todo, o qual é constituído por 13 algarismos, sendo que o último é o dígito de controle (ou de verificação). A congruência estabelecida para encontrar o dígito de verificação é módulo 10 e a base que compõem a multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita.

Seja $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}$ a sequência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$ e somar os produtos obtidos. Vamos representar por S a soma obtida. O dígito que está faltando representamos por a_{13} o qual deve ser somado com S gerando assim um múltiplo de 10, ou seja, $10|S + a_{13}$. Temos assim a seguinte congruência:

$$S + a_{13} \equiv 0(\text{mod } 10). \quad (1)$$

Ao dividirmos S por 10 basta subtrairmos o seu resto r para que o número obtido também seja múltiplo de 10. Logo,

Ao dividirmos S por 10 basta subtrairmos o seu resto r para que o número obtido também seja múltiplo de 10. Logo,

$$S - r \equiv 0(\text{mod } 10), \text{ sendo } r \text{ o resto.} \quad (2)$$

Por transitividade de (1) e (2), obtemos:

$$S + a_{13} \equiv S - r(\text{mod } 10)$$

Daí,

$$a_{13} \equiv -r(\text{mod } 10),$$

ou seja,

$$a_{13} + r \equiv 0(\text{mod } 10).$$

Portanto,

$$a_{13} + r = 10 \cdot q, \text{ com } q \in \mathbb{Z}.$$

Tomando $q = 1$, tem-se

$$a_{13} + r = 10,$$

isto é,

$$a_{13} = 10 - r.$$

Desta maneira, conclui-se que o dígito de controle de qualquer código de barras é facilmente encontrado sabendo-se o resto da soma obtida através dos 12 primeiros algarismos multiplicados pela base disposta acima.

Exemplo 4:

Figura 3- Código de Barras.



Fonte: [HTTPS:\\precisodocodigodebarras.com. br.](https://precisodocodigodebarras.com.br)

Notamos primeiramente, que além de usar a Aritmética Modular para encontrarmos o 13º dígito do código de barras, aguçamos nosso conhecimento diante das várias informações que os códigos nos trazem. No código acima, o dígito verificador já está apresentado, logo analisamos sua veracidade.

1º Passo: Multiplicar os 12 primeiros algarismos pela base dada.

$$a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a_6 \ a_7 \ a_8 \ a_9 \ a_{10} \ a_{11} \ a_{12}$$

×

$$1 \ 3 \ 1 \ 3 \ 1 \ 3 \ 1 \ 3 \ 1 \ 3 \ 1 \ 3$$

2º Passo: Somar os respectivos produtos.

$$S = a_1 \cdot 1 + a_2 \cdot 3 + a_3 \cdot 1 + a_4 \cdot 3 + a_5 \cdot 1 + a_6 \cdot 3 + a_7 \cdot 1 + a_8 \cdot 3 + a_9 \cdot 1 + a_{10} \cdot 3 + a_{11} \cdot 1 + a_{12} \cdot 3.$$

3º Passo: Fazer a divisão da soma obtida por 10.

$$S = 10 \cdot q + r, \text{ sendo } q \text{ o quociente e } r \text{ o resto.}$$

4º Passo: Subtrair o resto obtido na divisão anterior de 10.

$$a_{13} = 10 - r.$$

Agora com todos os passos descritos, resta apenas resolver os algoritmos. Então,

$$S = 4 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 1 \cdot 3 + 6 \cdot 1 + 6 \cdot 3 + 8 \cdot 1 + 3 \cdot 3 + 2 \cdot 1 + 6 \cdot 3 + 6 \cdot 1 + 8 \cdot 3.$$

Logo,

$$S = 4 + 24 + 9 + 3 + 6 + 18 + 8 + 9 + 2 + 18 + 6 + 24.$$

Ou seja,

$$S = 131.$$

Portanto,

$$131 = 10 \cdot 13 + 1,$$

o que implica

$$a_{13} = 10 - 1,$$

isto é,

$$a_{13} = 9.$$

Como queríamos demonstrar, o dígito verificador (13º dígito) do código de barras é 9, provando toda a Aritmética Modular envolvida neste algoritmo. E ainda, reforçamos que essa relação vale para qualquer código de barras.

3.2.2 Sistema de identificação ISBN

O sistema International Standard Book Number, mais comumente conhecido por ISBN, tem como principal finalidade a identificação numérica de livros. É um sistema reconhecido e utilizado mundialmente, o que possibilita independente do idioma, o reconhecimento de qual país o livro foi destinado.

Hoje se têm no mercado dois tipos de ISBN: o ISBN-10, para os livros lançados entre 1969 e 2006, possuindo dez dígitos, e o ISBN-13, usado após 1 de janeiro de 2007, possuindo três dígitos a mais que o ISBN-10. Mostramos então, como é feito o cálculo do dígito de verificação do ISBN-10, tendo em vista que para o ISBN-13, os resultados são os mesmos que foram apresentados anteriormente para os códigos de barras, EAN-13.

Analizamos como se fomenta o cálculo do dígito de controle e\ou verificação do ISBN-10:

Seja $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ a sequência formada pelos 9 primeiros dígitos do ISBN-10. Devemos multiplicá-los, nessa ordem, pela base $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$ e somar os produtos obtidos. O dígito que está faltando representamos por a_{10} . O mesmo deve ser o menor valor possível, tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S , o número $S + a_{10}$ deve ser múltiplo de 11, ou seja, $11|S + a_{10}$. Temos a seguinte congruência:

$$S + a_{10} \equiv 0(mod\ 11).$$

Exemplo 5:

Figura 4-ISBN-10



Fonte: Livro, Anjos e Demônios.

Na contracapa do livro Anjos e Demônios, de Dan Brown, temos o seguinte código do ISBN-10: 85-7542-146-8. Vejamos agora o cálculo do dígito de controle:

1º Passo: Multiplicar os 9 primeiros algarismos pela base dada.

$$a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9$$

×

$$10\ 9\ 8\ 7\ 6\ 5\ 4\ 3\ 2$$

2º Passo: Somar os respectivos produtos.

$$S = a_1 \cdot 10 + a_2 \cdot 9 + a_3 \cdot 8 + a_4 \cdot 7 + a_5 \cdot 6 + a_6 \cdot 5 + a_7 \cdot 4 + a_8 \cdot 3 + a_9 \cdot 2.$$

3º Passo: Fazer a divisão da soma obtida por 11.

$$S = 11 \cdot q + r, \text{ sendo } q \text{ o quociente e } r \text{ o resto.}$$

4º Passo: Subtrair o resto obtido na divisão anterior de 11.

$$a_{10} = 11 - r.$$

Agora com todos os passos descritos, resta apenas resolver os algoritmos. Então,

$$S = 8 \cdot 10 + 5 \cdot 9 + 7 \cdot 8 + 5 \cdot 7 + 4 \cdot 6 + 2 \cdot 5 + 1 \cdot 4 + 4 \cdot 3 + 6 \cdot 2.$$

Logo,

$$S = 80 + 45 + 56 + 35 + 24 + 10 + 4 + 12 + 12.$$

Ou seja,

$$S = 278.$$

Portanto,

$$278 = 11 \cdot 25 + 3,$$

o que implica

$$a_{10} = 11 - 3,$$

isto é,

$$a_{10} = 8.$$

O dígito de controle é 8, como queríamos certificar.

Observação 4: No ISBN-10, se o dígito de controle for igual a 10 (no caso do resto da divisão por 11 ser igual a 1), é usada a representação do 10 em algarismos romanos, ou seja, usa-se um **X**.

3.2.3 Cadastro de Pessoas Físicas – CPF

O Cadastro de Pessoas Físicas (CPF) é um documento de identificação do cidadão, cuja numeração possui 11 dígitos, sendo dividido em dois blocos: o primeiro composto por nove algarismos e o segundo por dois algarismos que são nomeados de

dígitos de controle ou verificação. Eles têm a função de identificar e individualizar cada indivíduo evitando fraudes.

Para determinarmos esses dois dígitos de controle foi usado novamente a noção de congruência, mostrando assim, mais uma aplicação da Aritmética Modular. Nesse caso, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Seja $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9$ a sequência formada pelos 9 primeiros dígitos do CPF, devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. O dígito que está faltando, representamos por a_{10} , o qual deve ser subtraído da soma obtida, gerando um múltiplo de 11, isto é, se a soma obtida é S , o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $11 | S - a_{10}$.

Assim, tem-se a seguinte congruência:

$$S - a_{10} \equiv 0 \pmod{11}.$$

E notório que o dígito de controle será o próprio resto da divisão por 11 da soma obtida.

Exemplo 6:

Figura 5-CPF



Fonte: <http://www.globalnetmanaus.com.br>

Vejamos como obter o primeiro dígito de controle do CPF acima ilustrado:

1º Passo: Multiplicar os 9 primeiros algarismos pela base dada.

$$a_1 \ a_2 \ a_3 \ a_4 \ a_5 \ a_6 \ a_7 \ a_8 \ a_9$$

×

$$1 \ 2 \ 3 \ 4 \ 5 \ 6 \ 7 \ 8 \ 9$$

2º Passo: Somar os respectivos produtos.

$$S = a_1 \cdot 1 + a_2 \cdot 2 + a_3 \cdot 3 + a_4 \cdot 4 + a_5 \cdot 5 + a_6 \cdot 6 + a_7 \cdot 7 + a_8 \cdot 8 + a_9 \cdot 9.$$

3º Passo: Fazer a divisão da soma obtida por 11.

$$S = 11 \cdot q + r, \text{ sendo } q \text{ o quociente e } r \text{ o resto.}$$

4º Passo: Identificar o resto da divisão por 11.

$$a_{10} = r.$$

Agora com todos os passos descritos, resta apenas resolver os algoritmos. Então,

$$S = 4 \cdot 1 + 9 \cdot 2 + 3 \cdot 3 + 4 \cdot 4 + 9 \cdot 5 + 3 \cdot 6 + 4 \cdot 7 + 9 \cdot 8 + 3 \cdot 9.$$

Logo,

$$S = 4 + 18 + 9 + 16 + 45 + 18 + 28 + 72 + 27.$$

Ou seja,

$$S = 237.$$

Portanto,

$$237 = 11 \cdot 21 + 6,$$

o que implica,

$$a_{10} = 6.$$

Dessa forma, o primeiro dígito de controle é 6 como queríamos mostrar. Para determinarmos o segundo dígito de controle, usamos a mesma ideia, sendo que agora acrescentamos o 10º dígito e a base de multiplicação incluirá o zero, $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Portanto,

$$S = 4 \cdot 0 + 9 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 9 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + 9 \cdot 7 + 3 \cdot 8 + 6 \cdot 9.$$

Logo,

$$S = 0 + 9 + 6 + 12 + 36 + 15 + 24 + 63 + 24 + 54.$$

Ou seja,

$$S = 243.$$

Portanto,

$$243 = 11 \cdot 22 + 1,$$

o que implica,

$$a_{10} = 1.$$

Assim, o segundo dígito de controle é o 1. Portanto, o nosso CPF tem a seguinte numeração: 493.493.493 – 61.

Observação 5: Caso o resto da divisão por 11 fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, seria usado neste caso o dígito zero.

3.2.4 Criptografia

A criptografia tem como principal propósito o envio de mensagens a um destinatário sem que terceiros consigam interpretá-las. O nível de complexidade para a produção de mensagens criptografadas, vai desde os códigos binários de um computador até as transações bancárias, isso incluindo as aplicações da Aritmética Modular, as quais possuem um caráter motivador e didático interessante.

A noção básica de criptografia não foge muito a realidade dos jovens, pois eles estão a todo tempo criando códigos para se comunicarem sem que outras pessoas que não pertençam a seus grupos consigam decodificar essas mensagens, garantindo assim o sigilo pretendido. Normalmente, usam símbolos e desenhos como códigos para corresponder às letras desejadas.

Dentre as várias formas de abordar a criptografia no ambiente escolar podemos fazer o uso das funções invertíveis (afim, exponencial, logarítmica), como também o uso de matrizes. Associando a cada letra do alfabeto um número, dá-se uma mensagem criptografada, ou seja, apenas com a sequência numérica e o receptor usando um dos métodos matemáticos irá decodificar e descobrir a mensagem.

Exemplo 7: Primeiramente associamos a cada letra do alfabeto um número correspondente, conforme a tabela abaixo:

Tabela 2- Correspondência numérica de cada letra.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Fonte: O autor, 2015.

Em seguida determina-se qual o tipo de função que irá trabalhar para cifrar a palavra. O receptor receberá apenas uma sequência numérica que terá sido obtida pela imagem da função. Ao receber a mensagem, o receptor deverá calcular a imagem da função inversa f^{-1} .

Para ilustrar nosso exemplo, escolhemos a seguinte função afim $f(x) = 7 \cdot x - 2$. E codificamos a frase “MELHOR TURMA CAA”, obtendo:

- ✓ $M = 13$, logo $f(13) = 7 \cdot 13 - 2 = 89$.
- ✓ $E = 5$, logo $f(5) = 7 \cdot 5 - 2 = 33$.
- ✓ $L = 12$, logo $f(12) = 7 \cdot 12 - 2 = 82$.
- ✓ $H = 8$, logo $f(8) = 7 \cdot 8 - 2 = 54$.
- ✓ $O = 15$, logo $f(15) = 7 \cdot 15 - 2 = 103$.
- ✓ $R = 18$, logo $f(18) = 7 \cdot 18 - 2 = 124$.
- ✓ $T = 20$, logo $f(20) = 7 \cdot 20 - 2 = 138$.
- ✓ $U = 21$, logo $f(21) = 7 \cdot 21 - 2 = 145$.
- ✓ $A = 1$, logo $f(1) = 7 \cdot 1 - 2 = 5$.
- ✓ $C = 3$, logo $f(3) = 7 \cdot 3 - 2 = 19$.

Agora com todas as letras devidamente codificadas temos a seguinte mensagem 89 33 82 54 103 124 138 145 124 89 5 19 5 5. Para decodificá-la o receptor deverá obter a chave que neste caso é a função inversa, ou seja, $f^{-1}(x) = \frac{x+2}{7}$. No entanto, basta apenas encontramos a imagem dessa função usando a mensagem dada, isto é:

- ✓ $f^{-1}(89) = \frac{89+2}{7} = \frac{91}{7} = 13 = M$.
- ✓ $f^{-1}(33) = \frac{33+2}{7} = \frac{35}{7} = 5 = E$.
- ✓ $f^{-1}(82) = \frac{82+2}{7} = \frac{84}{7} = 12 = L$.
- ✓ $f^{-1}(54) = \frac{54+2}{7} = \frac{56}{7} = 8 = H$.

E assim sucessivamente até decodificar toda a mensagem e obter a frase desconhecida. Logo, evidenciamos mais uma ferramenta para aplicação da Aritmética Modular e com um enfoque que pode ser trabalhado desde a Educação Básica.

3.3 A Aritmética Modular desde a Educação Básica.

Todas as aplicações vistas até aqui podem facilmente ser abordadas desde a Educação Básica, tendo suas devidas alterações. Salientamos que a nossa pesquisa visa o processo de ensino e aprendizagem do discente, ou melhor, do futuro professor, e é de fundamental importância saber como a Aritmética Modular vem sendo abordada na Educação Básica. A partir de duas dissertações recentes de Sant'Anna (2013) e Santos (2013), os quais evidenciam o uso da Aritmética Modular cada vez mais presente nos concursos de acesso ao nível médio das Escolas Militares e na OBMEP, explanamos suas aplicações.

Questões envolvendo divisibilidade e contagens periódicas estão cada vez mais presentes em objetos de seleção como os citados acima. Porém, os alunos da Educação Básica não estão tendo o devido preparo. Segundo Sant'Anna (2013),

Os concursos de acesso ao nível médio das Escolas Militares abordam questões ligadas à divisibilidade com frequência. Algumas delas são facilmente resolvidas através da maneira tradicionalmente ensinada, porém outras se tornam bastante trabalhosas. Assim a Teoria das Congruências mostra-se útil como ferramenta facilitadora da aprendizagem da divisibilidade, pois apresenta soluções comparativamente sucintas, ou seja, menos cansativas e trabalhosas. (SANT'ANNA, 2013, p.31).

Na mesma linha de pensamento de Sant'Anna (2013), Santos (2013) afirma que:

[...] Dessa forma, evidencia-se a falta de preparo dos alunos, também deve-se observar que isso se deve a falta de preparação dos docentes. Sem uma preparação diferenciada, os alunos geralmente não tem um desempenho satisfatório em olimpíadas matemáticas. A maioria das questões olímpicas envolvem um raciocínio mais elaborado e que exige um trabalho prévio de treinamento. Pensando nessa problemática a própria equipe da OBMEP, elabora materiais de apoio, como o banco de questões, e promove treinamentos. (SANTOS, 2013, p.37).

Por isso, durante a abordagem da disciplina Teoria dos Números, o futuro professor deverá adquirir um conhecimento além das demonstrações para poder fazer a relação da teoria com a prática no momento que se deparar numa sala de aula da

Educação Básica, podendo assim, proporcionar um amadurecimento mais efetivo da Aritmética Modular nesse nível de ensino. Vejamos então algumas dessas questões:

Questão 1: (Colégio Militar de Fortaleza – 2011) Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:

- a) 1 b) 2 c) 3 d) 4 e) 5

Solução: Temos duas formas para resolução dessa questão, a forma tradicional e por Aritmética Modular. Sendo assim, mostramos as duas formas:

✓ Tradicional:

$$\begin{cases} a = 7 \cdot q + 6 \\ b = 7 \cdot q' + 5 \end{cases}$$

Somando membro a membro, tem-se

$$a + b = 7 \cdot q + 7 \cdot q' + 6 + 5 = 7 \cdot (q + q') + 11 = 7 \cdot (q + q') + 7 + 4,$$

Ou seja,

$$a + b = 7 \cdot (q + q' + 1) + 4.$$

Assim, $a + b$ deixa resto 4.

✓ Aritmética Modular:

$$\begin{cases} a \equiv 6(mod\ 7) \\ b \equiv 5(mod\ 7) \end{cases}$$

Somando membro a membro, tem-se

$$a + b \equiv 6 + 5(mod\ 7) = 11(mod\ 7)$$

Pelo fato de $a + b$ ser congruente a 11 no $(mod\ 7)$, basta apenas saber o resto de 11 dividido por 7, que é 4.

Questão 2: (Colégio Naval – 2003) O resto da divisão de $5^{131} + 7^{131} + 9^{131} + 15^{131}$ por 12 é igual a:

- a) 0 b) 2 c) 7 d) 9 e) 11

Solução: Nesse tipo de questão, é notório que não há uma maneira tradicional de resolução, ou seja, será necessária a utilização das propriedades operatórias da Aritmética Modular. Porém, observamos que se trata de uma prova para nível médio.

Modo de resolução:

$$\begin{cases} 5 \equiv -7 \pmod{12} \\ 9 \equiv -3 \pmod{12} \\ 15 \equiv 3 \pmod{12} \end{cases}$$

Substituindo as equivalências na equação temos,

$$5^{131} + 7^{131} + 9^{131} + 15^{131} \equiv (-7)^{131} + 7^{131} + (-3)^{131} + 3^{131} \pmod{12}$$

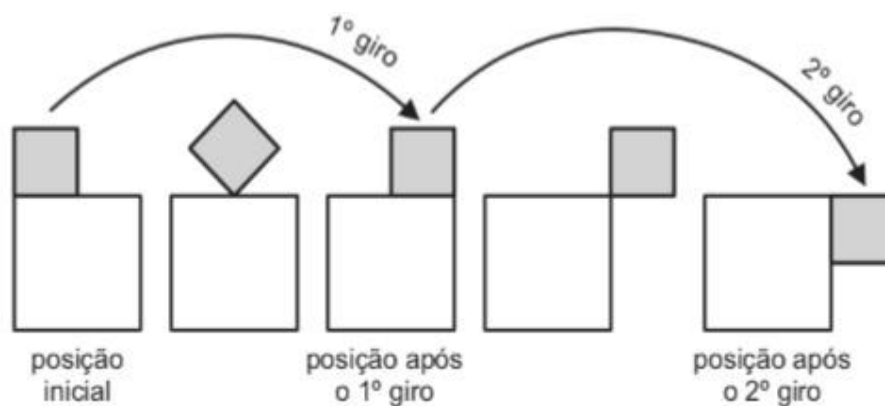
Notamos que os termos se anulam, ou seja,

$$5^{131} + 7^{131} + 9^{131} + 15^{131} \equiv 0 \pmod{12}.$$

Portanto, a expressão deixa resto zero ao ser dividida por 12.

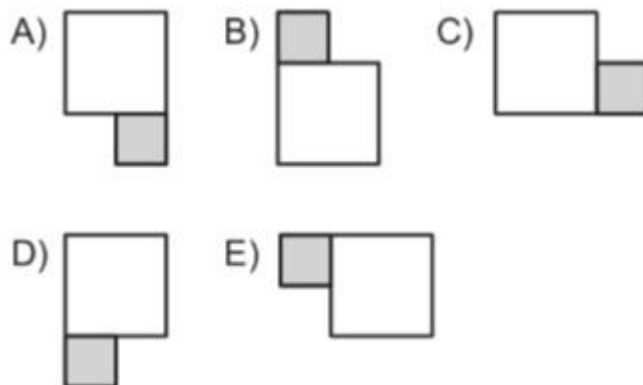
Questão 3: [OBMEP (2012), 1a Fase, Nível 1] Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.

Figura 6-Posição dos quadrados após os giros.



Fonte: bancoobmep2012.

Qual das figuras a seguir representa a posição dos dois quadrados após o 2012º giro?



Solução: Observamos que após oito giros sucessivos o quadrado menor retorna à sua posição inicial. Então, usamos a divisão euclidiana 2012 por 8, ou seja, $2012 = 8 \cdot 251 + 4$. Portanto, após o 2012º giro o quadrado menor terá dado 251 voltas completas no quadrado maior e mais quatro giros, parando na posição que corresponde à alternativa A.

Diante destas questões, percebe-se a utilidade da Aritmética Modular como ferramenta para a Educação Básica, pois a mesma já vem sendo cobrada de forma implícita como nestas questões que acabamos de ver, tendo em vista que se o aluno não conhece essa ferramenta fica quase inviável a resolução das mesmas.

4. METODOLOGIA DE PESQUISA

Neste capítulo descrevemos os métodos adotados para a realização da pesquisa, no intuito de estabelecer uma melhor percepção de como a mesma se compôs. Abordamos como referencial teórico-metodológico a pesquisa qualitativa e a análise de conteúdo como instrumento para coleta de dados.

4.1 Descrição Metodológica

Na perspectiva de obter dados que correspondessem à problemática apresentada, a pesquisa constitui um caráter qualitativo, em que o pesquisador procura aprofundar-se na compreensão dos fenômenos que estuda. De acordo com Minayo (2007, p. 174), a pesquisa qualitativa se caracteriza como uma “pesquisa de cunho compreensivo”, onde o ambiente estudado é o que se faz mais importante nessa perspectiva proporcionando ao pesquisador maior autonomia no processo de análise dos dados.

A pesquisa aborda também a análise de conteúdo em livros didáticos do Ensino Superior, no intuito de identificar aspectos relevantes acerca de aplicações da temática. A análise de conteúdo teve seu berço nos Estados Unidos, onde foi aplicada como um instrumento de análise das comunicações há mais de meio século. Adotamos como referencial teórico-metodológico a abordagem de Laurence Bardin, no que envolve a análise de conteúdo. Segundo Bardin (2011):

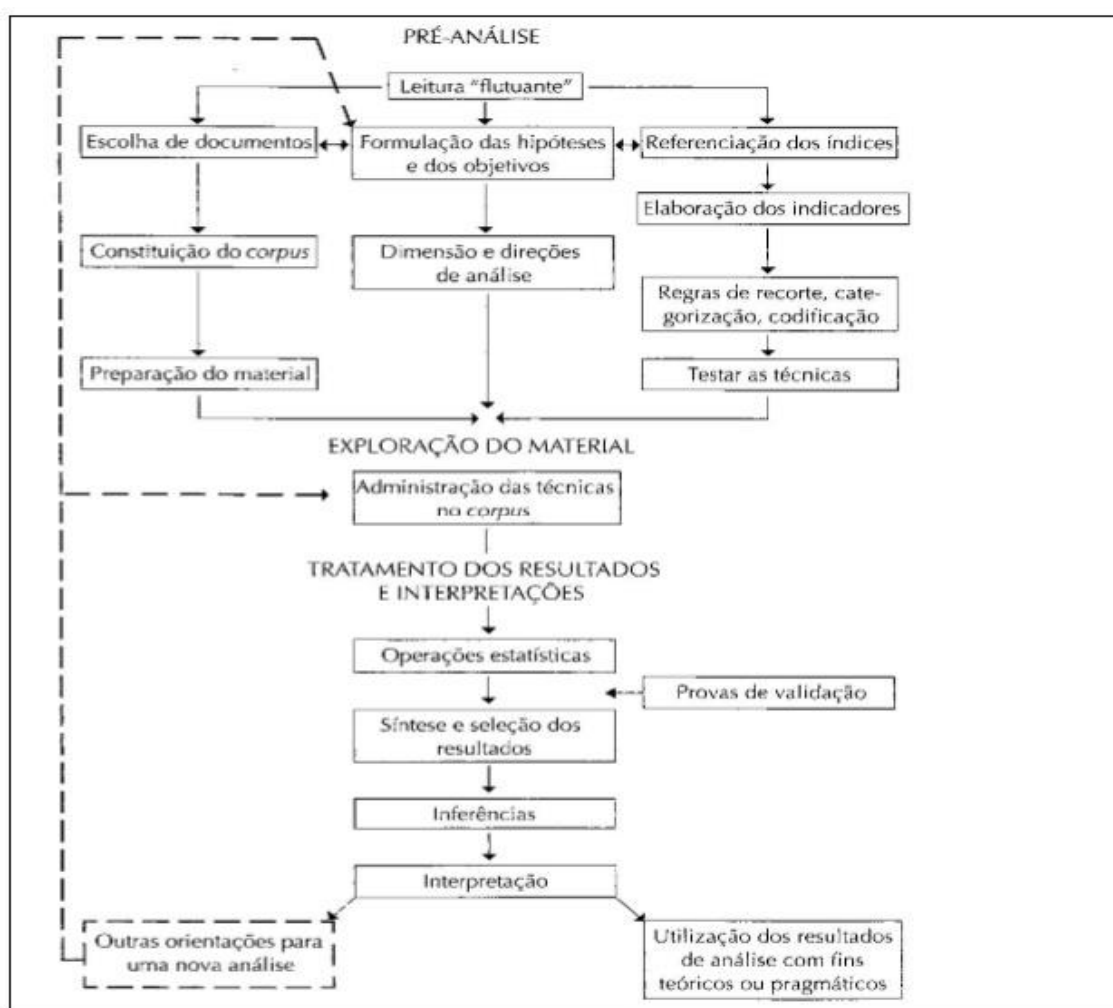
Descrever a história da “análise de conteúdo” é essencialmente referenciar as diligências que nos Estados Unidos marcaram o desenvolvimento de um instrumento de análise de comunicações; é seguir passo a passo o crescimento quantitativo e a diversificação qualitativa dos estudos empíricos apoiados na utilização de uma das técnicas classificadas sob a designação genérica de análise de conteúdo; é observar a posteriori os aperfeiçoamentos materiais e as aplicações abusivas de uma prática que funciona há mais de meio século. Mas também é pôr em questão as suas condições de aparecimento e de extensão em diversos setores das ciências humanas, e tentar clarificar as relações que a análise de conteúdo mantém ou não com disciplinas vizinhas pelo seu objeto ou pelos seus métodos (Bardin, 2011, p.19).

Ainda segundo Bardin (2011), a análise de conteúdo permite a concepção de conhecimentos abordados através de variáveis inferidas por indicadores, sejam eles quantitativos ou qualitativos, a partir de procedimentos sistemáticos e objetivos. Define também o tratamento da informação a partir de três polos cronológicos, ou seja,

- Pré-análise, na qual se escolhem os documentos, se formulam hipóteses e objetivos para a pesquisa e se elaboram indicadores que fundamentem a interpretação final;
- Exploração do material, na qual se aplicam as técnicas específicas segundo os objetivos e;
- Tratamento dos resultados, a inferência e a interpretação.

Cada fase segue regras bastante específicas, podendo ser utilizado tanto em pesquisas quantitativas quanto em pesquisas qualitativas. A figura a seguir traz um resumo esquemático das fases da análise de conteúdo.

Figura 7-Resumo esquemático do desenvolvimento de uma análise de conteúdo.



Fonte: (Bardin, 2011, p. 132).

A partir do processo esquemático de Bardin para a análise de conteúdo, iremos pontuar os livros didáticos a serem analisados através de categorização, onde a própria autora salienta que:

A categorização é uma operação de classificação de elementos constituintes de um conjunto por diferenciação e, em seguida, por reagrupamento segundo o gênero (analogia), com os critérios previamente definidos. As categorias são rubricas ou classes, as quais reúnem um grupo de elementos (unidades de registro) sob um título genérico, agrupamento esse efetuado em razão das características comuns destes elementos. (Bardin, 2011, p. 147).

Nessa perspectiva, foram escolhidos para a análise especialmente os livros apresentados na ementa atual (vide anexo) da disciplina Teoria dos Números do curso de Matemática-Licenciatura do CAA. Os livros estão descritos abaixo:

- DU SAUTOY, Marcus. A música dos números primos: a história de um problema não resolvido na matemática. Rio de Janeiro: J. Zahar, 2007;
- LANDAU, Edmund. Teoria elementar dos números. São Paulo: Ciência Moderna, 2002;
- MAIO, Waldemar de. Álgebra: estruturas algébricas básicas e fundamentos da teoria dos números. Rio de Janeiro: LTC, 2007.

Além dessas três referências abordadas na ementa do curso, os docentes que lecionam a disciplina Teoria dos Números também exploram outras três referências, as quais nos convêm analisar. São:

- HEFEZ, Abramo. Elementos de Aritmética. 2ª edição, SBM, 2005;
- SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números. 3ª edição. Rio de Janeiro: IMPA, 2012;
- SHOKRANIAN, Salahoddin. Teoria dos Números. . 2ª edição, Brasília: Universidade de Brasília, 1999.

Baseados no referencial teórico-metodológico de Bardin em paralelo com os PCN criaram-se unidades de análise e se definiram as categorias a elas associadas, conforme segue:

Quadro 5-Categorizações.

Unidades de análise	Categorias
Conteúdos	Divisibilidade
	Congruência
Processo de ensino e aprendizagem	O livro incentiva o uso de conhecimentos extraescolares.
	O livro estimula competências matemáticas mais elaboradas, além da repetição e da memorização.
	O livro estabelece relação com o contexto histórico.
Aspectos pedagógicos	O livro introduz os conteúdos por explanação teórica com sistematização, seguida de exemplos e atividades de aplicação.
	O conhecimento matemático está abordando outras áreas da própria Matemática.
	O conhecimento matemático está interligado com outras áreas do conhecimento.
	O conhecimento matemático está contextualizado com práticas sociais e o cotidiano.

Fonte: O autor, 2015.

Observemos que foram criadas três unidades de análise, subdivididas com suas respectivas categorias. Totalizando assim, nove categorias, as quais analisemos minuciosamente a partir dos livros citados acima. Detalhamos com total seriedade os dados obtidos, salientando que os livros selecionados para análise não são analisados em sua totalidade, isto é, delimitamos para a análise apenas os capítulos que fazem referência a Aritmética Modular e o estudo de suas propriedades.

5. APRESENTAÇÃO DAS ANÁLISES E DOS RESULTADOS

Objetivamos neste capítulo apresentar, interpretar, discutir e analisar os dados coletados por meio da análise de conteúdo explorada nos livros didáticos de Teoria dos Números a partir de uma abordagem qualitativa.

5.1 Procedimentos adotados para a análise

Iniciamos nossa abordagem referente à obtenção dos dados apoiados na descrição de Laurence Bardin. Em um primeiro momento, selecionamos os livros a serem estudado, o que segundo Bardin (2011) já constitui uma parte da pré-análise, a qual se completou no momento da formulação de hipóteses. E para sintetizar esses indicadores, classificamos os livros seguindo uma unidade de análise e a partir de cada unidade fundamentamos as categorias as quais nos mostra o desfecho da pesquisa enquanto inferência e interpretação dos dados.

5.1.2 Obtenção dos Dados

Antes de começarmos nossa obtenção de dados dispomos abaixo um quadro com os respectivos termos usados na nossa análise, uma vez que os mesmos podem dar um sentido dubio dependendo da interpretação do leitor. Dessa forma, esclarecemos o que os termos expressos demonstram dentro desta pesquisa.

Quadro 6- Sentido dos termos usados

Termos usados na análise de dados	
Pontos particulares	De forma pontual, ou seja, dentro de um exemplo em determinada passagem na resolução de um algoritmo.
Competências Matemáticas elaboradas	São regras de demonstração, juntamente com a linguagem matemática formal.
Enormes	Quantidade muito grande exposta dentro do espaço analisado.
Notório	Está presente em todo o capítulo.

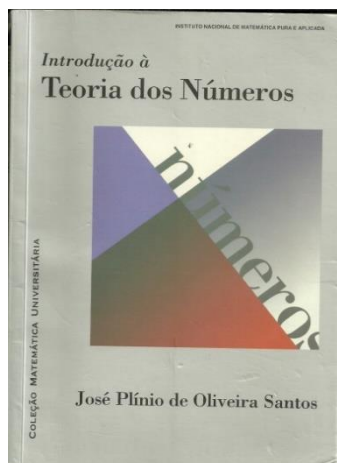
Alguns	Quantidade pequena, exposta dentro do espaço analisado.
Grande abordagem	É exposto com grande frequência dentro do capítulo.
Visivelmente	Ligação direta entre determinados termos.

Fonte: O autor, 2015.

Optamos por começar nossa análise através das referências que não estão presentes na ementa do curso, no entanto, já foram ou estão sendo utilizadas pelos docentes do CAA.

Livro 1:

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3ª edição. Rio de Janeiro: IMPA, 2012.



Conteúdos

- **Divisibilidade:** A divisibilidade é abordada a partir do conjunto dos números inteiros, explorando em seguida assuntos como Indução, Algoritmo da divisão, MDC e MMC, como também os critérios de divisibilidade, presentes também nos problemas resolvidos e propostos.
- **Congruência:** O livro traz um capítulo abordando apenas congruência e suas propriedades a partir do conjunto dos números inteiros. No início do capítulo, o autor faz referência ao surgimento da congruência e o seu percurso, abordando a relação de equivalência entre os números e suas classes de resíduos módulos m e enfatizando a grande abordagem sobre os números primos, os quais possuem consideráveis propriedades, como também faz forte referência à divisibilidade.

Em relação aos problemas resolvidos e propostos o livro nos remete a usar a definição em grande parte deles.

Processo de ensino e aprendizagem

- **O livro incentiva o uso de conhecimentos extraescolares:** Em nenhum momento o livro propõe o uso de conhecimentos extraescolares.
- **O livro estimula competências matemáticas mais elaboradas, além da repetição e da memorização:** Diante das demonstrações dos exemplos, teoremas, entre outros, o uso de competências Matemáticas elaboradas é notório. Utiliza-se de uma linguagem mais aplicada ao campo científico da Matemática. Traz enormes listas de exercícios, os quais são resolvidos em sua maioria através do mesmo procedimento, reforçando assim o uso da repetição e juntamente com ela a memorização.
- **O livro estabelece relação com o contexto histórico:** O livro possui uma grande defasagem em relação ao contexto histórico. Não podemos descrever esse fato como uma totalidade, pois foi possível identificar um tópico ou outro que fizesse referência ao contexto histórico.

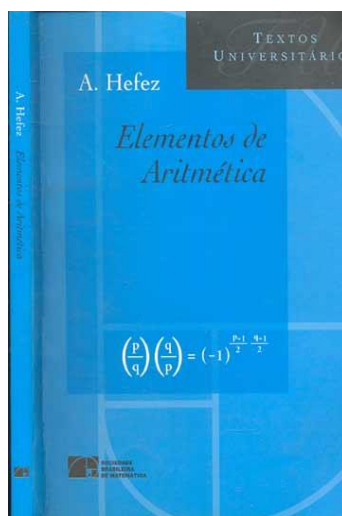
Aspectos pedagógicos

- **O livro introduz os conteúdos por explanação teórica com sistematização, seguida de exemplos e atividades de aplicação:** O livro expõe primeiramente a explanação teórica com sistematização, seguida de exemplos. Em relação às atividades de aplicação, elas não se encontram durante o decorrer do capítulo, tendo em vista que no final de cada capítulo encontra-se uma seção de problemas resolvidos e outra seção de problemas propostos, no entanto, em nenhuma das seções têm-se atividades com o uso de aplicações.
- **O conhecimento matemático está abordando outras áreas da própria Matemática:** O livro diante dos vários conceitos abordados sobre a Teoria dos Números, com referência a Aritmética Modular, faz o uso de outras áreas da Matemática para se chegar ao objetivo pretendido, além de fazer inferências a inúmeros contextos expostos dentro do próprio ambiente matemático.

- **O conhecimento matemático está interligado com outras áreas do conhecimento:** O livro não faz interligação alguma do conteúdo abordado com outras áreas do conhecimento.
- **O conhecimento matemático está contextualizado com práticas sociais e o cotidiano:** O livro não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano, nem tão pouco em relação a outros aspectos.

Livro 2:

HEFEZ, Abramo. **Elementos de Aritmética**. 2ª edição, SBM, 2005.



Conteúdos

- **Divisibilidade:** A divisibilidade é abordada a partir do conjunto dos números naturais. São explorados assuntos como Indução, Divisão Euclidiana, MDC e MMC, como também os Critérios de divisibilidade, presentes também nos problemas resolvidos e propostos.
- **Congruência:** O livro traz um capítulo abordando apenas congruência e suas propriedades a partir do conjunto dos números naturais. No início do capítulo o autor faz referência ao surgimento da congruência e o seu percurso, como também a define ser uma aritmética com os restos da divisão euclidiana por um numero fixado. Ainda, aborda a relação de equivalência entre os números e suas classes de resíduos módulo m , enfatizando também a grande abordagem sobre os números primos, os quais possuem consideráveis propriedades. Em relação aos problemas o livro traz uma lista a qual precisamos usar a definição e logo em seguida traz uma seção de aplicações dialogando tanto com o capítulo de congruência como também com o de divisibilidade.

Processo de ensino e aprendizagem

- **O livro incentiva o uso de conhecimentos extraescolares:** Ao final de cada capítulo o livro traz uma seção de exercícios, os quais o autor chama de “Problemas”. Dentre esses problemas temos alguns em que o discente deverá ter um conhecimento extraescolar para compreender a proposta do problema e assim poder resolvê-lo. Esse fato de relacionar o conteúdo com conhecimentos extraescolares possibilita ao discente uma visão mais ampla do seu campo de estudo enquanto aspectos sociais e culturais do qual o mesmo faz parte.
- **O livro estimula competências matemáticas mais elaboradas, além da repetição e da memorização:** Diante das demonstrações dos exemplos, teoremas, entre outros, o uso de competências Matemáticas elaboradas é notório. Utiliza-se de uma linguagem mais aplicada ao campo científico da Matemática, no entanto, nos problemas propostos que não são muitos, e não se aborda com afinco o uso da repetição. Temos problemas que pedem o simples resolva e demonstre, como também problemas contextualizados e aplicados em contextos próprios de vivência dos discentes, quebrando assim a prática da repetição e da memorização.
- **O livro estabelece relação com o contexto histórico:** O livro aborda dentro dos capítulos o uma reflexão histórica sobre aquele determinado assunto. Como por exemplo, como ocorreu o surgimento, a época, quem expôs aquele argumento, entre outros.

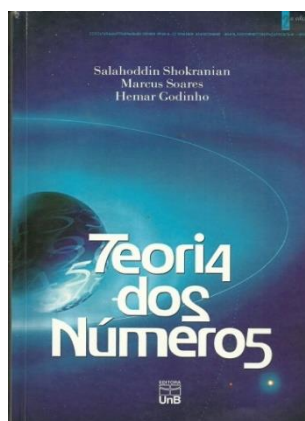
Aspectos pedagógicos

- **O livro introduz os conteúdos por explanação teórica com sistematização, seguida de exemplos e atividades de aplicação:** O livro expõe primeiramente a explanação teórica com sistematização, seguida de alguns exemplos. Os exemplos não são de difícil entendimento, porém são poucos. Em relação às atividades de aplicação, elas aparecem durante o capítulo dialogando diretamente com o conteúdo e/ou aparecem fundamentadas como um único capítulo, no entanto, fazem referência aos conteúdos expostos anteriormente. Temos ainda atividades com o uso de aplicações dentro dos problemas propostos.

- **O conhecimento matemático está abordando outras áreas da própria Matemática:** O livro diante dos vários conceitos abordados sobre a Teoria dos Números, com referência a Aritmética Modular, faz o uso de outras áreas da Matemática para se chegar ao objetivo pretendido. Além de fazer inferências a inúmeros contextos expostos dentro do próprio ambiente matemático, assim as áreas da Matemática dialogam visivelmente dentro do campo de conhecimento da própria Matemática.
- **O conhecimento matemático está interligado com outras áreas do conhecimento:** O livro faz interligação dos conteúdos abordados com outras áreas do conhecimento, como por exemplo, contextos históricos os quais retratam época e os principais envolvidos e ainda, o processo metodológico através de jogos.
- **O conhecimento matemático está contextualizado com práticas sociais e o cotidiano:** O livro traz alguns tipos de contextualização referente as práticas sociais e o cotidiano. Essa contextualização é perceptível através dos jogos, como também das explicações sobre determinados povos, assim como instrumentos, ou seja, materiais didáticos usados no dia a dia e relevantes dentro da sociedade.

Livro 3:

SHOKRANIAN, Salahoddin. **Teoria dos Números**. 2ª edição, Brasília: Universidade de Brasília, 1999.



Conteúdos

- **Divisibilidade:** A divisibilidade é abordada a partir do conjunto dos números inteiros. Ainda no início do capítulo intitulado Divisibilidade e Números Primos, o autor faz a ressalva de que irá estabelecer belos resultados sobre os números

inteiros, dentre eles o estudo de máximo divisor comum entre inteiros não nulos. São explorados assuntos como Indução, Divisão Euclidiana, MDC e MMC, como também os critérios de divisibilidade. Além de estarem presentes também nos problemas resolvidos e propostos.

- **Congruência:** O livro não traz um capítulo abordando apenas congruência e suas propriedades. Ele introduz os teoremas e propriedades referentes à congruência dentro dos demais capítulos e dessa forma evidencia-se uma falta de interação entre os determinados conceitos. Pois se passa despercebido argumentos bastante relevantes dentro da discussão congruência.

Processo de ensino e aprendizagem

- **O livro incentiva o uso de conhecimentos extraescolares:** Em nenhum momento o livro propõe o uso de conhecimentos extraescolares.
- **O livro estimula competências matemáticas mais elaboradas, além da repetição e da memorização:** Diante das demonstrações dos exemplos, Teoremas, entre outros, o uso de competências Matemáticas elaboradas é notório. Utiliza-se de uma linguagem mais aplicada ao campo científico da Matemática. Traz listas de exercícios adequadas ao tamanho do capítulo, os quais são resolvidos em sua maioria através de procedimentos diversos que foram abordados no decorrer do capítulo. Podendo estimular a memorização mais sem o uso de repetição.
- **O livro estabelece relação com o contexto histórico:** O livro não faz relação alguma com o contexto histórico.

Aspectos pedagógicos

- **O livro introduz os conteúdos por explicação teórica com sistematização, seguida de exemplos e atividades de aplicação:** O livro expõe primeiramente a explicação teórica com sistematização, seguida de exemplos e exercícios. Os exemplos não são de difícil entendimento e os exercícios também tem uma linguagem simples e objetiva. Em relação às atividades de aplicação, elas não se encontram durante o decorrer do capítulo, tendo em vista que no final de cada capítulo encontra-se uma seção de exercícios, porém, também não tem nenhum que faça referência a aplicações. Vale ressaltar ainda que o autor cita em

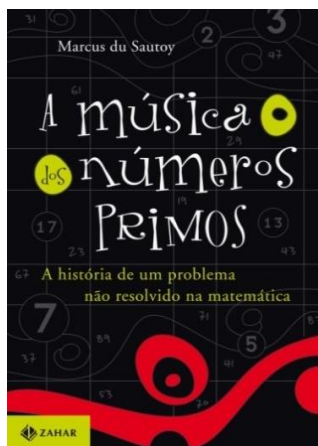
algumas passagens do livro que o uso de aplicações é importante e que estão se multiplicando rapidamente nos vários campos da matemática, tanto pura quanto aplicada. No entanto, não mostra nenhuma atividade a partir de aplicação.

- **O conhecimento matemático está abordando outras áreas da própria Matemática:** O livro diante dos vários conceitos abordados sobre a Teoria dos Números, com referência a Aritmética Modular faz o uso de outras áreas da Matemática para se chegar ao objetivo pretendido. Além de fazer inferências a inúmeros contextos expostos dentro do próprio ambiente matemático.
- **O conhecimento matemático está interligado com outras áreas do conhecimento:** O livro não faz interligação alguma do conteúdo abordado com outras áreas do conhecimento.
- **O conhecimento matemático está contextualizado com práticas sociais e o cotidiano:** O livro não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano, nem tão pouco em relação a outros aspectos.

Agora iniciemos a análise dos livros sugeridos na ementa do curso, na ordem que estão dispostos na ementa.

Livro 4:

DU SAUTOY, Marcus. **A música dos números primos: a história de um problema não resolvido na matemática.** Rio de Janeiro: J. Zahar, 2007.



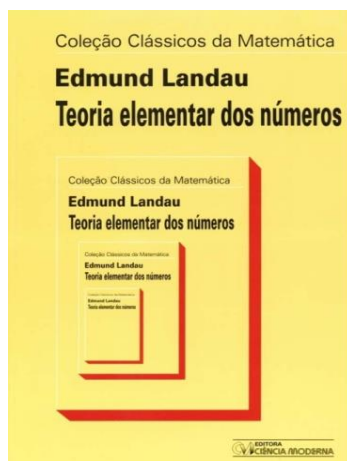
Diante da análise deste livro compreendemos que ele está inserido na ementa da disciplina Teoria dos Números de forma a contribuir com o processo histórico da mesma. O livro faz uma reconstituição das tentativas feitas por diversos matemáticos tendo como objetivo demonstrar a validade da Conjectura de Riemann. Assim, a reunião

desses confrontos constitui todo o cenário da história da matemática e dos matemáticos até o século atual. Além de ter esse caráter histórico e persuasivo sobre a construção matemática, também tem várias passagens lúdicas as quais desperta no leitor o instinto de pesquisar, conhecer e se apropriar desses determinados fatos históricos.

Em relação às unidades de análise estabelecidas para a observação dos livros, juntamente com suas categorizações, não foi possível analisar este livro a partir delas. Tendo em vista que o livro se trata de uma rica e abrangente narrativa, e que mesmo trazendo argumentos que possibilitam o enquadramento em alguma das categorias elencadas, os dados iriam ficar dispersos dentro da análise geral.

Livro 5:

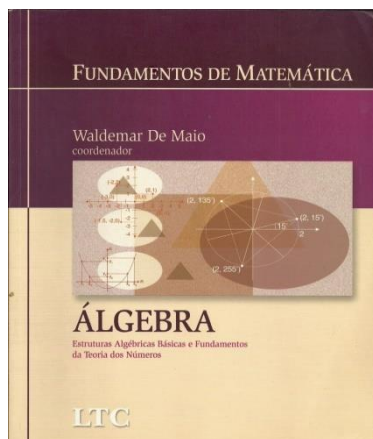
LANDAU, Edmund. **Teoria elementar dos números**. São Paulo: Ciência Moderna, 2002.



Este livro não foi analisado, pois não tivemos acesso a essa referência. Mesmo o livro sendo um dos sugeridos na ementa da disciplina Teoria dos Números, ele não se faz presente no acervo da biblioteca do Centro Acadêmico do Agreste da Universidade Federal de Pernambuco, no qual esta sendo realizada a pesquisa. De forma lamentável essa obra não é palpável aos discentes.

Livro 6:

MAIO, Waldemar de. **Álgebra: estruturas algébricas básicas e fundamentos da teoria dos números**. Rio de Janeiro: LTC, 2007.



Conteúdos

- **Divisibilidade:** A divisibilidade é abordada a partir do conjunto dos números inteiros. O livro tem como um tópico “conjunto quociente” o qual explora os assuntos de divisibilidade, além de apresentar problemas resolvidos e propostos.
- **Congruência:** O livro não traz um capítulo abordando apenas congruência e suas propriedades. Ele introduz os teoremas e propriedades referentes à congruência dentro dos demais capítulos e dessa forma evidencia-se uma falta de interação entre determinados conceitos. Se passa despercebido argumentos bastante relevantes dentro da discussão congruência.

Processo de ensino e aprendizagem

- **O livro incentiva o uso de conhecimentos extraescolares:** Em pontos particulares o livro propõe que você tenha a noção de tempo em relação há horas, dias e anos, como também a noção de casa em relação aos seus repartimentos e a mobília, isso ocorre enquanto exemplificação.
- **O livro estimula competências matemáticas mais elaboradas, além da repetição e da memorização:** O livro não estimula o uso de demonstração diante das atividades propostas. Não é visível o uso de competências matemáticas mais elaboradas, pois o livro utiliza de uma linguagem simples. Traz nos exercícios, a exigência de procedimentos os quais são resolvidos de formas diferentes não estimulando a repetição.
- **O livro estabelece relação com o contexto histórico:** O livro em nenhum momento faz referência a contexto histórico.

Aspectos pedagógicos

- **O livro introduz os conteúdos por explicação teórica com sistematização, seguida de exemplos e atividades de aplicação:** O livro expõe a explicação teórica com sistematização, seguida de exemplos. Em relação às atividades de aplicação, é perceptível em pontos particulares do livro, trazendo no prefácio um discurso voltado para a importância do uso de aplicações no desenvolvimento do processo de ensino e aprendizagem.
- **O conhecimento matemático está abordando outras áreas da própria Matemática:** O livro diante dos vários conceitos abordados sobre a Teoria dos Números, com referência a Aritmética Modular, faz o uso de outras áreas da Matemática para se chegar ao objetivo pretendido. Além de fazer inferências a inúmeros contextos expostos dentro do próprio ambiente matemático, enfatizando a Geometria Plana.
- **O conhecimento matemático está interligado com outras áreas do conhecimento:** O livro não faz interligação alguma do conteúdo abordado com outras áreas do conhecimento.
- **O conhecimento matemático está contextualizado com práticas sociais e o cotidiano:** O livro não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano nem tão pouco em relação a outros aspectos.

5.2 Análise dos livros

O objetivo principal da nossa análise foi diagnosticar a presença de aplicações da Aritmética Modular nos livros usados no processo de ensino e aprendizagem da disciplina Teoria dos Números. Diante deste argumento e corroborando com o que foi analisado pode-se afirmar que o Livro1 não faz uso de conhecimentos extraescolares, não expõe nenhuma atividade com uso de aplicações e não faz interligação alguma do conteúdo abordado com outras áreas do conhecimento. De forma geral o livro não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano nem tão pouco em relação a outros aspectos.

No Livro 2, o autor traz alguns problemas nos quais o discente deverá ter um conhecimento extraescolar para compreender a proposta do problema e assim poder resolvê-lo. As atividades de aplicação aparecem durante o capítulo dialogando diretamente com o conteúdo e/ou aparecem fundamentadas como um único capítulo, no

entanto, fazem referência aos conteúdos expostos anteriormente. Temos ainda atividades com o uso de aplicações dentro dos problemas propostos, além de fazer interligação dos conteúdos abordados com outras áreas do conhecimento, através de jogos, que constituem materiais didáticos relevantes.

No Livro 3, o uso de conhecimentos extraescolares não é abordado. Em relação às atividades de aplicação, elas não se encontram durante o decorrer do capítulo, ressaltando ainda que o autor cita em algumas passagens do livro que o uso de aplicações é importante e que estão se multiplicando rapidamente nos vários campos da matemática, tanto pura quanto aplicada. No entanto, o livro não mostra nenhuma atividade a partir de aplicação e não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano nem tão pouco em relação a outros aspectos.

O Livro 4, por se tratar de uma rica e abrangente narrativa histórica da Teoria dos Números é um livro que apresenta aplicações e contextualizações que estão inseridos no nosso cotidiano, porém não aborda conceitos e conteúdos exigidos dentro da disciplina. Ressaltando que pode ele ser usado como um complemento, mas não como único livro. Já o Livro 5, não podemos afirmar nada sobre o mesmo, pois infelizmente não tivemos acesso a ele.

O Livro 6, apresenta em pontos particulares o uso de conhecimentos extraescolares, como também de aplicações. O livro traz no prefácio um discurso voltado para a importância do uso de aplicações no desenvolvimento do processo de ensino e aprendizagem. De forma geral o livro não traz nenhum tipo de contextualização, nem referente a práticas sociais e o cotidiano nem tão pouco em relação a outros aspectos.

A partir das colocações acima podemos afirmar que o livro que se enquadra no perfil do nosso objetivo é o Livro 2 em comparação com os demais. O livro em questão traz uma linguagem acessível ao discente como também possui uma maior concentração de aplicações e/ou propostas das mesmas, salientando que este livro não se encontra na ementa da disciplina. Temos também o Livro 6 que faz o uso das aplicações em pontos bem particulares. Já o Livro 4 serve apenas como complemento dentro da disciplina, por se tratar de uma narrativa. E, os Livros 1 e 3 não abordam o uso de aplicações em nenhum momento, mostrando-nos uma defasagem nesse aspecto.

CONSIDERAÇÕES FINAIS

Esta pesquisa objetivou investigar como os livros didáticos da disciplina Teoria dos Números estão abordando as aplicações da Aritmética Modular, tendo em vista as inúmeras formas de aplicabilidade que a mesma apresenta no nosso cotidiano, e com a finalidade de se ter um melhor aproveitamento no processo de ensino e aprendizagem. O intuito é fazer uma conexão entre a Matemática teórica, ensinada na sala de aula, e a Matemática aplicada, estudando o desenvolvimento de diversas aplicações presentes na sociedade na qual estamos inseridos.

Ao analisar de forma geral, os livros aqui estudados necessitam de uma abordagem mais significativa em relação ao uso de aplicações para mediar melhor o processo de ensino e aprendizagem, tendo em vista que é uma disciplina apresentada para futuros professores, estes precisarão de argumentos convincentes para responder perguntas do tipo: Para que serve? De que forma serve esses conteúdos dentro do espaço social, cultural? Por isso, o futuro professor deve se apropriar desses subsídios enquanto se encontra dentro do universo de estudo, a graduação.

Os teoremas e proposições, entre outros argumentos da Aritmética Modular apresentados nesta pesquisa, são de fundamental importância na formação do futuro professor de Matemática, pois o mesmo tem como desafio na Educação Básica de fazer a imersão desse conteúdo que ultimamente vem sendo cobrado sem que os professores tenham a apropriação devida.

Construiu-se uma discussão com a análise desses livros que mostra a necessidade do uso de aplicações inseridas nos mesmos, possibilitando ao aluno uma segunda forma de visualizar o que aparentemente se mostra tão abstrato e sem conexão com a realidade. Ainda é coerente afirmar que as aplicações desenvolvem o raciocínio lógico e se torna uma ferramenta para o melhor entendimento do conteúdo, como também estimula o aluno que estará futuramente na posição de professor.

A partir do que foi analisado, podemos reforçar que o livro didático se apresenta como recurso importante na atuação do professor, como também para o estudo dos alunos. Por isso, no momento da escolha do livro a ser utilizado, o professor já deve analisar as funções que o mesmo pode exercer no processo de ensino e aprendizagem, não bastando só esse aspecto, pois o modo como o professor irá usar o livro fará toda uma diferença.

Além disso, atingimos o objetivo de articular sobre a importância da existência de um material passível e interessante para ser abordado no Ensino Superior, desmistificando a ideia de que o livro no Ensino Superior deve apenas conter o conteúdo de forma abstrata sem mostrar sua real importância para o aluno que será futuramente o professor.

Corroboramos ainda que este trabalho poderá ser usado por professores, tanto do Ensino Superior quanto do Ensino Médio, como um instrumento para o desenvolvimento de aulas de Aritmética. Portanto, a linguagem abordada durante todo o trabalho foi de forma sucinta e objetiva, e as aplicações expostas da Aritmética Modular tiveram como intuito, além de ser um estímulo para o processo de ensino e aprendizagem, deixar os alunos curiosos e interessados em aprender mais sobre os assuntos das aulas de Matemática.

Contudo, aponta-se a necessidade de outros estudos que complementem a problemática estudada, tanto quanto ao uso do livro didático no processo de ensino e aprendizagem da Matemática, como também o uso de aplicações interessantes da Matemática que poderão ser também aproveitadas na Educação Básica.

REFERÊNCIAS

- ALLEVATO, N. S. G.; TERTO, L. L. **Funções quadráticas nos livros didáticos: um estudo sob a ótica da resolução de problemas**. In: CURI, E.; ALLEVATO, N. S. G. (Org.). Pesquisas e práticas em educação: matemática, física e tecnologias computacionais. São Paulo: Terracota, 2009. p. 33-50.
- BANDEIRA, Denise. **Material didático: conceito, classificação geral e aspectos da elaboração**, 2011. Disponível em< <http://www.Videolivreria.com.br> >acesso em 19 de setembro, 2014.
- BARDIN, L. (2011). **Análise de conteúdo** (Tradução de Luís Antero Reto e Augusto Pinheiro). São Paulo: Edições 70.
- BIEHL E BAYER, Juliana Vocaboglo; Arno. **A escolha do livro didático de matemática**. X Encontro Gaúcho Matemática, 2009.
- BOYER, B. C. **História da matemática**. Tradução: Elza F. Gomide. São Paulo: Edgard Blucher, 1974.
- BRASIL. Ministério da Educação e do Desporto. **Parâmetros Curriculares Nacionais: matemática, terceiro e quarto ciclos do ensino fundamental**. Brasília: MEC/SEF, 1996-1998.
- COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2009.
- D'AMBROSIO, Ubiratan. **Da realidade à ação: reflexões sobre educação e matemática**. São Paulo: Sammus; Campinas: Ed. Universidade Estadual de Campinas, 1986.
- DOMINGUES, H. H. **Fundamentos de aritmética**. São Paulo: Atual, 1991.
- DU SAUTOY, Marcus. **A música dos números primos: a história de um problema não resolvido na matemática**. Rio de Janeiro: J. Zahar, 2007.
- FERREIRA, Aurélio Buarque de Holanda. **Mini Aurélio – Dicionário**. 4º Ed., Nova Fronteira, 2001.
- FREITAS, Olga. **Equipamentos e materiais didáticos**. Brasília: Universidade de Brasília, 2007. Disponível em:< <http://portal.mec.gov.br> >. Acesso em: 01 fev. 2015.
- GERARD, F. M.; ROEGIERS, X. **Conceber e avaliar manuais escolares**. Porto: Ed. Porto, 1998.
- GOMES, Daiane. **O livro didático no processo de ensino e aprendizagem da matemática: Considerações de professores de escolas públicas de Ji-Paraná**. 2014. 49f. Monografia (Licenciatura em Matemática) – Departamento de Matemática e Estatística, Universidade Federal de Rondônia, Ji-Paraná.

Guia de livros didáticos - **PNLD 2013: Matemática: Ensino fundamental anos iniciais**. Brasília- DF: Ministério da Educação, Secretária de Educação Básica, 2012.

Guia de livros didáticos - **PNLD 2014: Matemática: Ensino fundamental anos finais**. Brasília- DF: Ministério da Educação, Secretária de Educação Básica, 2013.

Guia de livros didáticos - **PNLD 2015: Matemática: Ensino Médio**. Brasília- DF: Ministério da Educação, Secretária de Educação Básica, 2014.

HEFEZ, Abramo. **Elementos da Aritmética**, 2a edição, SBM, 2005.

LAJOLO, M. **Livro didático: um (quase) manual do usuário**. In: Em aberto, ano 16, n. 69, Brasília, 1996.

LANDAU, Edmund. **Teoria elementar dos números**. São Paulo: Ciência Moderna, 2002;

MAIO, Waldemar de. **Álgebra: estruturas algébricas básicas e fundamentos da teoria dos números**. Rio de Janeiro: LTC, 2007.

MATTOS, Sérgio Ricardo Pereira de. **Aritmética modular na formação continuada de professores: Desenvolvendo o pensamento aritmético e algébrico** / Sérgio Ricardo Pereira de Mattos. – 2011.

MINAYO, Maria C. de Souza. **O Desafio do Conhecimento: pesquisa qualitativa em saúde**. 10 Ed., São Paulo, Hucitec, 2007.

OGLIARI, Lucas Nunes. **A matemática no cotidiano e na sociedade: perspectiva do aluno de ensino médio** / Lucas Nunes Ogliari. $\frac{3}{4}$ Porto Alegre, 2008.145 f.: il.

OLIVEIRA, E. M. Q. **O uso do livro didático de matemática por professores do ensino fundamental**. 2007. 152f. Dissertação (Mestrado em Educação) - Universidade Federal de Pernambuco, Recife, 2007.

OLIVEIRA, J. B. A. et al. **A política do livro didático**. São Paulo: Sammus, 1984.

ROMANATTO, Mauro, Carlos. **A noção de número natural em livros didáticos de matemática: comparações entre textos tradicionais e modernos**. Dissertação (mestrado) – Universidade Federal de São Paulo, São Carlos – SP, 1987.
www.sbempaulista.org.br.

SÁ, I. P. **A Magia da Matemática: Atividades Investigativas, Curiosidades e Histórias da Matemática**. Rio de Janeiro: Ciência Moderna, 2007.

SANTALÓ, L. A. **Matemática para não matemáticos**. In: PARRA, C.; SAIZ, I. (Org.). Didática da Matemática. Porto Alegre: Artmed, 2008.p. 11.

SANT'ANNA, Iury Kersnowsky de. **A Aritmética Modular como ferramenta para as séries finais do Ensino Fundamental**. Dissertação apresentada ao Curso de Mestrado Profissional em Matemática (PROFMAT), ministrado pelo Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2013.

SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**, 3a edição, IMPA, 2012.

SANTOS, Paulo Sergio de Almeida. **Congruência e Equações Diofantinas Lineares: Uma Proposta para o Ensino Básico**. 2013, 111f.

SHOKRANIAN, Salahoddin. **Teoria dos Números**. 2ª edição, Brasília: Universidade de Brasília, 1999.

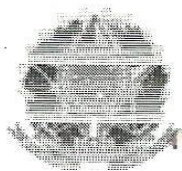
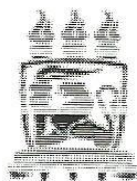
SHOKRANIAN, S. **Uma breve história da Teoria dos Números no século vinte**. Rio de Janeiro: Moderna, 2010.

VASCONCELOS, S. D.; SOUTO, E. **O livro didático no ensino fundamental - proposta de critérios para análise de conteúdo**. Ciência & Educação, v.9, n.1, 2003.

ANEXOS

Ementa

Teoria dos Números



UNIVERSIDADE FEDERAL DE PERNAMBUCO
PRÓ-REITORIA PARA ASSUNTOS ACADÊMICOS
DIRETORIA DE DESENVOLVIMENTO DO ENSINO

PROGRAMA DE COMPONENTE CURRICULAR

TIPO DE COMPONENTE (Marque um X na opção)

☒ Disciplina

☐ Prática de Ensino

☐ Atividade complementar

☐ Módulo

☐ Monografia

☐ Trabalho de Graduação

STATUS DO COMPONENTE (Marque um X na opção)

☒ Obrigatório

☐ Eletivo

☐ Optativo

DADOS DO COMPONENTE

Código	Nome	Carga Horária		Nº créditos	CH Global	Período
MATM0044	Teoria dos Números	Teórica 60	Prática 0	4	60	6º

Pré-requisitos	-	Co-requisitos	-	Requisitos C.H.	-
----------------	---	---------------	---	-----------------	---

EMENTA

Números naturais: princípio de indução matemática. Números inteiros, divisibilidade. Representação dos números naturais. Algoritmo de Euclides. MDC. Equações Diofantinas. Números Primos. Congruência.

OBJETIVOS DO COMPONENTE

Apresentar de maneira concisa os fundamentos aritméticos envolvendo o anel dos inteiros, necessários para solidificar as bases do aluno enquanto professor da educação básica, bem como introduzi-lo à conceitos algébricos importantes para sua vida acadêmica e profissional.

METODOLOGIA

Aulas expositivas interativas, com momentos de discussão e aulas de resolução de problemas.

AVALIAÇÃO

Provas escritas, listas de exercícios, trabalhos, seminários ou outros, conforme legislação vigente da UFPE, a critério do professor.

CONTEÚDO PROGRAMÁTICO

- Números inteiros;
- Princípio de Indução;
- Divisibilidade;
- O algoritmo da divisão;
- Máximo divisor Comum;
- O algoritmo de Euclides;
- Números Primos;
- Mínimo múltiplo comum;
- Critérios de divisibilidade;
- Representação dos números inteiros;
- Congruência;
- Congruência linear;
- Equações Diofantinas;
- Teorema de Wilson;
- Pequeno Teorema de Fermat;
- Teorema de Euler;
- O Teorema Chinês do Resto;
- Princípio da Casa dos Pombos;
- Demonstração combinatória do pequeno Teorema de Fermat e do Teorema de Wilson;
- Outros tópicos.

BIBLIOGRAFIA BÁSICA

- DU SAUTOY, Marcus. A música dos números primos: a história de um problema não resolvido na matemática. Rio de Janeiro: J. Zahar, 2007.
- LANDAU, Edmund. **Teoria elementar dos números**. São Paulo: Ciência Moderna, 2002.
- MAIO, Waldemar de. Álgebra: estruturas algébricas básicas e fundamentos da teoria dos números. Rio de Janeiro: LTC, 2007.