UNIVERSIDADE ESTADUAL DO MARANHÃO - UEMA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO - PPG

PROFMAT
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

ARITMÉTICA MODULAR APLICADA

Marcus Vinicius Viegas Rodrigues

São Luís - MA
2024

ARITMÉTICA MODULAR APLICADA

Marcus Vinicius Viegas Rodrigues

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como parte dos requisitos para obtenção do título de Mestre em Matemática.
Orientador: Prof. Dr. João Coelho Silva Filho.

São Luís - MA
2024

Rodrigues, Marcus Vinicius Viegas.

Aritmética modular aplicada./ Marcus Vinicius Viegas Rodrigues. - São Luís (MA), 2024.

72 p.

Dissertação (Mestrado em Matemática em Rede Nacional - PROFMAT) Universidade Estadual do Maranhão - UEMA, 2024.

Orientador: Prof. Dr. João Coelho Silva Filho.

1. Aritmética Modular. 2. Classes Residuais. 3. Congruência. 4. Equações Diofantinas. I.Título.

CDU 511.8

Elaborado por Luciana de Araújo - CRB 13/445

ARITMÉTICA MODULAR APLICADA

Marcus Vinicius Viegas Rodrigues

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como parte dos requisitos para obtenção do título de Mestre em Matemática.
Orientador: Prof. Dr. João Coelho Silva Filho.

Aprovada em: 04 de Julho de 2024.

Banca Examinadora:

Prof. Dr. João Coelho Silva Filho - Orientador
Universidade Estadual do Maranhão - UEMA

Prof. Dr. Alberto Leandro Correia Costa - Examinador Interno
Universidade Estadual do Maranhão - UEMA

Prof. Dr. Luís Fernando Coelho Amaral - Examinador Externo
Universidade Federal do Maranhão - UFMA

São Luís - MA
2024

Dedico esse trabalho aos meus pais que sempre me incentivaram a estudar e a lutar pelos meus sonhos.

Agradecimentos

"A gratidão é a memória do coração!"

Por isso, quero agradecer primeiramente ao meu bom Deus, que me deu força, sabedoria e paciência para fazer esse trabalho em meio a tantos desafios.

Aos meus pais, Cristina e Assis, que não mediram esforços para facilitar que eu chegasse até aqui, pelo amor, por me ensinarem, por me criarem, enfim, por sempre estarem ao meu lado em todas as caminhadas, concedendo-me apoio, sustentação, orientação e educação suficiente e adequada em todos os momentos da minha vida.

A minha esposa, amiga e companheira Litiele França Gonçalves, pelo apoio, compreensão, paciência e auxílio para eu chegar até aqui.

Ao Professor orientador Dr. João Coelho Silva Filho, pelas excelentes orientações e sugestões exercidas pelo seu vasto conhecimento e maturidade matemática, que contribuíram grandiosamente nesta pesquisa, pela paciência e todo apoio para que este trabalho fosse concluído.

A todos meus colegas de mestrado e professores do PROFMAT. Uma turma maravilhosa, unida e parceira que tive o privilégio de pertencer.

A Secretária Annanda do ProfMat UEMA que sempre esteve à disposição para ajudar.

Também não posso deixar de agradecer aos meus colegas de trabalho e familiares pelo apoio, carinho e torcida durante todo o caminhar do curso.

Enfim, sou grato a todos que contribuíram de forma direta ou indireta para que pudesse chegar a este momento, para a realização deste trabalho e para a conquista desse objetivo.

"A Matemática é a rainha das ciências, e a Aritmética é a rainha da Matemática."

Carl Friedrich Gauss.

RESUMO

Esta dissertação apresenta grandiosas aplicações da Aritmética Modular e mostra a sua importância para o ensino-aprendizagem de matemática. É relatado um Histórico da Aritmética Modular, apresentando os principais nomes da Teoria dos Números e da Congruência Modular, em destaque o Príncipe da Matemática, Gauss. Em seguida, é evidenciado que há possibilidade de inserir objetos de conhecimento da Aritmética Modular nos organizadores curriculares da educação básica, segundo os documentos normativos, autores, pesquisadores e professores. Para enfatizar a importância para o ensino básico, é realizada a fundamentação teórica com os principais tópicos da Teoria dos Números, tais como a Divisibilidade, o Algoritmo da Divisão, o Máximo Divisor Comum, o Algoritmo de Euclides, os Números Primos e as Equações Diofantinas. Além disso, aborda-se a noção de Congruência apresentando diversos exemplos e aplicações no ensino, dando destaque à Aritmética dos Restos, aos Critérios de Divisibilidade, aos Dígitos Verificadores dos CPF, cartões de crédito, ao Calendário e às Congruências Lineares. Por fim, é mostrada as particularidades da Arimética Modular, especificamente as Classes Residuais, em que são constatadas e evidenciadas como principal contribuição desta pesquisa, uma aplicação das Classes Residuais como processo simplificativo na resolução de Equações Diofantinas.

Palavras Chave: Aritmética Modular. Classes Residuais. Congruência. Equações Diofantinas.

ABSTRACT

This dissertation presents great applications of Modular Arithmetic and shows its importance for teaching and learning mathematics. To this end, initially, a brief History of Modular Arithmetic is reported, presenting the main names in Number Theory and Modular Congruence, highlighting the Prince of Mathematics, C. F. Gauss. Next, it is highlighted that there is the possibility of inserting knowledge (content) of Modular Arithmetic in basic education curriculum organizers, according to normative documents, authors, researchers and teachers. Furthermore, emphasizing its importance for basic education, a foundation is made theory with the main topics of Number Theory, such as Divisibility, Division Algorithm, Greatest Common Divisor, Euclid's Algorithm, Numbers Cousins and the Diophantine Equations. Furthermore, the notion of Congruence is addressed by presenting several examples and applications in teaching, highlighting the Arithmetic of Remainders, the Divisibility Criteria, the Check Digits (CPF and credit cards), the Calendar and Linear Congruences. Finally, particularities of the Modular Arimetics, especially the Residual Classes Module m, in which, as the main contribution of this research, applications of the Classes Residuals as a simplifying process in solving Diophantine Equations.

Keywords: Modular Arithmetic. Residual Classes. Congruence. Diophantine Equations.

Sumário

1 INTRODUÇÃO

Nesta pesquisa serão abordadas situações que envolvem a Teoria dos Números, em especial a Aritmética Modular. O termo Aritmética deriva do grego Arithmos, ou seja, significa número. É um ramo da matemática pura que se preocupa com as propriedades dos números inteiros. Sendo assim, ela é reconhecida como a ciência dos números, e compreender essa área é de extrema relevância para o sucesso do processo de ensino e aprendizagem, visto que auxilia na estruturação do raciocínio e contribui para o desenvolvimento de processos transversais, pois muitos problemas que envolvem a Aritmética são facilmente compreendidos até por não-matemáticos.

Atualmente uma das ferramentas mais importantes na Teoria dos Números é a Aritmética Modular, pelo fato de envolver o conceito de Congruência, pois nos permite resolver diversas situações-problemas relacionadas à Divisibilidade, às Congruências Lineares, às Classes Residuais e às Equações Diofantinas Lineares – tópicos que serão enfatizados nesta dissertação. A Aritmética modular tem muita aplicabilidade no cotidiano, no entanto, nos organizadores curriculares do Ensino Básico contém apenas os conceitos e definições básicas de números naturais e suas operações, múltiplos, divisores, números primos, números compostos, regras de divisibilidade, máximo divisor comum, mínimo múltiplo comum e conceitos iniciais de números inteiros e suas operações. Estes tópicos são relacionados à Teoria dos Números, em especial, à Aritmética Modular que é muito mais ampla e os livros didáticos deixam de abordar uma grande parte deles.

Deste modo, diante do exposto, esta pesquisa mostra a importância da Aritmética Modular para o ensino-aprendizagem de matemática. Para tanto, são enfatizados os principais pontos da História da Aritmética Modular, seu enfoque na Educação Básica, e suas aplicações no ensino e no cotidiano, dando ênfaze às Classes Residuais que facilitam a resolução das Equações Diofantinas.

Na primeira seção desta pesquisa são relatados pontos importantes do Histórico da Aritmética Modular, dando ênfaze ao Príncipe da matemática, o alemão Carl Friederich Gauss que inseriu a noção de congruência em sua obra "Disquisitiones Arithmeticae". Em seguida, abordam-se vistas sobre o Ensino de Aritmética Modular na Educação Básica, que embora não possua de forma detalhada os objetos de conhecimentos (conteúdos) dessa área nos organizadores curriculares, exitem documentos normativos, autores, pesquisadores e professores que defendem a inserção da Arimética Modular no Ensino Básico.

Na segunda seção é feita uma fundamentação teórica com os principais tópicos da Teoria Elementar dos Números, tais como a Divisibilidade, ao Algoritmo da Divisão, ao Máximo Divisor Comum, ao Algoritmo de Euclides, aos Números Primos e as Equações Diofantinas. São apresentados ainda, para esses tópicos, exemplos e aplicações.

Na terceira seção aborda-se a noção de Congruência, um dos fundamentais conteúdos da Aritmética Modular, que possui diversos exemplos e aplicações no ensino, como mostrados nesta pesquisa. Ainda nesta parte, é dado destaque à Aritmética dos Restos, aos Críterios de Divisibilidade mnemônicos e não mnemônicos, aos Dígitos Verificadores de CPF e cartões de crédito, ao Calendário e às Congruências Lineares.

Finalizando com maestria, na quarta seção desta dissertação, retratam-se ainda particularidades da Arimética Modular, em especial às Classes Residuais Módulo m. Concluindo, são constatadas e evidênciadas, como principal contribuição desta pesquisa, aplicações das Classes Residuais como um processo simples e ágil na resolução de Equações Diofantinas.

2 O ENSINO DE ARITMÉTICA MODULAR

Nesta parte será enfatizada um pouco do Histórico da Aritmética Modular destacando alguns nomes da construção e do desenvolvimento da matemática, tais como o de Tales de Mileto, Pitágoras de Samos, Diofanto de Alexandria, Pierre de Fermat, Leonhard Euler, Carl Friederich Gauss, entre outros. Consequentemente será abordado o Ensino de Aritmética Modular na visão de alguns documentos norteadores da educação juntamente com a análise de organizadores curriculares da educação básica e posteriormente com visões de alguns autores referente à inserção da Aritmética Modular nos currículos educacionais.

2.1 Histórico da Aritmética Modular

Ao longo da história, a forma de entender e representar os números foi evoluindo de forma eficaz, a fim de tentar solucionar as necessidades da humanidade. Apesar de os números inteiros positivos comporem o sistema matemático mais "simples", o estudo de suas propriedades exerce grande encanto na mente humana desde os primórdios, estingando muitos estudiosos através de seus conceitos e propriedades que vão além de qualquer simplicidade.

Por volta de 2500 a.C., os Sumérios já tinham seu próprio calendário e faziam o uso da base sexagesimal. Notava-se que, no estudo de astronomia, já desenvolviam algum tipo de aritmética.

Os papiros demonstram as formas de escrita e as habilidades dos povos de épocas primitivas, eles são uma das provas matemáticas mais importantes do Antigo Egito, local de origem do Papiro de Rhind ou Papiro de Ahmes datado de 1650 a.C. Esse documento é um dos artigos mais famosos, em que um escriba de nome Ahmes relata a solução de 85 problemas de aritmética, frações, cálculo de áreas, volume e progressões. Assim é possível perceber como a Matemática era praticada neste período da história.

Segundo BARBOSA 2017 (p.23) a primeira abordagem científica da Teoria dos Números é atribuída aos gregos, por volta de 450 a.C. consoante Hefez (2015), acredita-se que Tales de Mileto (624-558 a.C.) tenha introduzido na Grécia o estudo da Matemática que havia aprendido com os egípcios.

O matemático e filósofo grego Pitágoras de Samos (582-497 a.C.) e seus seguidores, chamados de pitagóricos, foram os primeiros a classificar os números em pares, ímpares e primos. Sabe-se que a Teoria dos Números é um ramo da matemática que se preocupa com as propriedades dos números inteiros e que anteriormente já foi chamada de Aritmética Superior, porém esse termo caiu em desuso.

Os gregos antigos abordaram diversos problemas referentes à Teoria dos Números, dentre os quais podemos destacar o cálculo do máximo divisor comum de dois números, a determinação dos números primos menores que um inteiro dado e a demonstração de

que há uma infinidade de números primos.

Pode-se destacar também o matemático e geômetra Euclides de Alexandria (330-275 a.C.) que, consoante solicitação do imperador da parte egípcia da Grécia Antiga: Ptolomeu I, elaborou a obra "Os Elementos", composta por 13 livros. Entre estes, os livros VII, VIII e IX abordam conceitos numéricos a partir de uma linguagem geométrica que faz referência à Teoria dos Números.

Diofanto de Alexandria é outro matemático que também recebe muito destaque. A sua obra "Arithmetica" escrita por volta de 250 d.C., aborda essencialmente soluções de equações indeterminadas com coeficientes inteiros.

GROENWALD, L.O. e F. 2005 afirmam que embora a Matemática tenha sido intensamente estudada por outros autores gregos, e, posteriormente, por árabes, indianos e europeus, a Teoria dos Números, como toda ciência, teve suas perdas pela não divulgação e produção velada no período do apagão científico, cultural e artístico, provocado até o século XVII.

Entre 1621 e 1636, o francês Pierre de Fermat adquiriu uma cópia do texto original em grego da Aritmética de Diofanto, que foi publicada em 1612 por Bachet – divulgou também essa cópia com uma tradução latina, língua utilizada pelos europeus eruditos da época. Fermat teve seu interesse despertado pela Teoria dos Números a partir de anotações das suas ideias que surgiram diante da leitura referente ao texto de Diofanto.

Fermat, que nasceu 1601, não era matemático por profissão e sim magistrado, apesar de lidar muito bem com a matemática. Havia poucos matemáticos na época. Marin Mersenne, frade francês, foi um dos mais famosos encarregados pelas divulgações, por meio de cartas, de novidades e resultados obtidos na matemática para "República de Letras", onde era muito amigo de grandes matemáticos, como Descartes, Pascal e o próprio Fermat.

Foi através das cartas enviadas a Mersenne e a outros matemáticos que grande parte da obra de Fermat ficou conhecida. Após a sua morte em 1665, seu filho Samuel Fermat encarregou-se de coletar e publicar a obra de seu pai, que estava dispersa em cartas e anotações. Ele iniciou desde a publicação da Aritmética de Diofanto, até as anotações feitas por Fermat. Dentre elas a mais famosa anotação é o famoso Último Teorema de Fermat – não existe solução não nula para a equação $x^n + y^n = z^n$, onde $n \geq 3$ e x, y, z são números inteiros. Esse Teorema foi provado em 1995 pelo inglês Andrew Wiles, mais de 300 anos após ser enunciado por Fermat.

O suíço Leonhard Euler (1707-1783), é considerado o sucessor de Fermat. Euler contribuiu para quase todas as áreas da Matemática pura e aplicada com suas obras no período do séc XVIII.

Christian Goldbach (1690-1764) era um professor da Academia das Ciências de Sâo Petesburgo e foi através dele, em uma correspondência, que Euler teve um dos seus primeiros acessos à obra de Fermat. Em 1729, Goldbach indagou Euler, em uma de suas correspondências, da seguinte forma: "[...] você conhece a observação de Fermat de que todos os números da forma $2^{2^n}+1$ são primos? [...]". Euler não demonstrou muito interesse e basicamente um ano depois começou a ler a obra de Fermat. E, em alguns anos depois, provou boa parte dos resultados enunciados por Fermat, inclusive a questão proposta por Goldbach.

Desse modo, Euler proporcionou grande popularização da Teoria dos Números, contudo, o estudo de forma metodológica aperfeiçoou-se com a obra "Disquisitiones Arithmeticae" do alemão Carl Friedrich Gaus (1777-1855), publicada em Leipzig (1801). A obra ficou dividida em sete partes: 1. Congruências em geral; 2. Congruências de primeiro grau; 3. Resto de Potências; 4. Congruências de segundo grau; 5. Formas quadráticas; 6. Aplicações; 7. Divisões do círculo.

Dessa forma, Gauss contribuiu de forma sistemática, com auxílio dos estudos de matemáticos anteriores, para o desenvolver da Aritmética Modular. Segundo BARBOSA 2017 (pg. 25)

> Gauss foi um matemático, astrônomo e físico alemão que contribuiu muito em diversas áreas da ciência, dentre elas a Teoria dos Números, Estatística, Análise Matemática, Astronomia e Óptica. Alguns se referem a ele como "Príncipe da Matemática". Ele considerava a Matemática como rainha das ciências.

Gauss introduziu a noção de congruência, inclusive com a notação usada até hoje. Sendo assim, portanto, fundamental para a Aritmética Modular.

2.2 A Aritmética Modular na Educação Básica

Observa-se que, desde os anos iniciais do ensino fundamental na educação básica, a Aritmética é apresentada de forma concomitante entre o trabalho com números e operações e com o ensino do espaço e das formas, sendo que esses conceitos matemáticos são um dos primeiros assimilados pelas crianças. Conforme MARONESE 2016 (p.21) é necessário evidenciar que mesmo antes de chegar à escola, a criança já possui uma noção de número, a qual foi sendo construída a partir de atitudes naturais de agrupamento e seriação por ela vivenciadas.

Pode-se conceituar a aritmética como o ensino dos números e operações entre eles, mas LINS e GIMENEZ 2000 (p.33) afirmam que é muito mais que isso, a educação aritmética em si também inclui:

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

A Aritmética Modular, a "matemática dos restos", é o ramo da matemática que estuda as propriedades e relações entre números inteiros quando agrupados em classes de congruência. O ensino de Aritmética Modular compõe uma parte fundamental da Teoria dos Números, pois é baseado no conceito de congruência modular, que é uma relação entre dois números inteiros quando a diferença entre eles é divisível por um terceiro número fixo.

Em termos mais simples, dois números são congruentes se, ao serem divididos pelo mesmo número, possuírem o mesmo resto. Por exemplo, em aritmética modular com módulo 5, os números 8 e 13 são congruentes porque ambos deixam o mesmo resto (3) quando divididos por 5.

Diante das pesquisas na literatura específica, evidenciou-se que os conteúdos de Aritmética Modular não estão explicitamente dentre os objetos de conhecimentos propostos pelos documentos normativos da educação brasileira, tais como a Base Nacional Comum Curricular – BNCC (a versão final para a Educação Infantil e o Ensino Fundamental foi homologada no ano de 2017, enquanto a versão para o Ensino Médio foi homologada um ano depois, em 2018) e, de modo mais específico, o Documento Curricular do Território Maranhense – DCTMA (a versão para a Educação Infantil e o Ensino Fundamental foi homologada em 2019 e a versão mais recente para o Ensino Médio foi homologada em 2022). Nesses documentos, a etapa do Ensino Fundamental é dividida em áreas de conhecimento, composta por componentes curriculares que, assim como as áreas, também possuem competências específicas. Já o Ensino médio é estruturado em 5 eixos principais: Formação Geral Básica; Itinerários Formativos; Integração Curricular; Orientação Educacional e Tutoria.

Porém, por mais que não esteja de forma explicita nos currículos, a Aritmética Modular pode ser objeto de estudo na Educação Básica, não com o objetivo de ser apenas mais um conteúdo previsto, mas cada docente tem a possibilidade de atar aos objetos de conhecimento já presente nos organizadores curriculares. A Organização para a Cooperação e Desenvolvimento Econômico - OCDE 2016 (p.47) fortalece esse intuito quando afirma que

> Talvez ainda mais importante que o conteúdo que os alunos levam da escola e o ato de simplesmente "aprender a aprender". Ao longo de suas experiencias escolares, os estudantes adotam estratégias de aprendizado que eles então aplicam ao longo de suas vidas. Estratégias de aprendizado são uma parte integral da aquisição de conhecimento e podem ser definidas como os pensamentos e ações que os alunos usam para completar tarefas de aprendizado.

Observa-se que desenvolver a Aritmética Modular na Educação Básica pode ser um grande motivador para a aprendizagem, em decorrência de sua excelente possibilidade de contextualização, o que permite a construção de diversas e desafiadoras propostas de atividades pedagógicas. Com efeito, contribui para o processo de aprendizagem efetiva, além de promover o letramento matemático e a autonomia dos alunos. Vale destacar ainda que MATTOS, PUGGIAN e LOZANO 2011 (p. 11) complementam que o ensino da Aritmética Modular na Educação Básica auxilia a consolidação do conceito de divisibilidade, proporciona que os alunos conheçam um contexto diferente para a realização das operações aritméticas e, ainda, incentiva um maior desenvolvimento do pensamento aritmético e sua ligação com o algébrico.

Outros autores defendem também a inserção da Aritmética Modular na educação básica, tais como L. M. SILVA e PONTES 2023 (p.13) ao argumentarem que ela pode auxiliar no desenvolvimento do pensamento matemático e na resolução de problemas. Segundo FERREIRA et al. 2018 (p.49), devido à importância do estudo e aplicabilidade

das congruências modulares que estimulam o desenvolvimento de habilidades essenciais para a formação do aluno, propõe o ensino de Congruências Modulares a partir do 6° ano do Ensino Fundamental.

Conforme a afirmação mencionada anteriormente de Ferreira e diante do Organizador Curricular de Matemática do DCTMA, nota-se que a inserção da Aritmética Modular pode ser feita, não apenas a partir do 6° ano, mas desde o 5° ano do Ensino Fundamental, visto que há possibilidade de fazer a relação dela com alguns objetos de conhecimento de algumas habilidades desse ano e de anos posteriores. Nesse intuito, conforme MARANHÃO 2019 (p.335-350), destacam-se os seguintes códigos de habilidades:

> (EF05MA10) Concluir, por meio de investigações, que a relação de igualdade existente entre dois membros permanece ao adicionar, subtrair, multiplicar ou dividir cada um desses membros por um mesmo número, para construir a noção de equivalência.
> (EF06MA05) Classificar números naturais em primos e compostos[...].
> (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.
> (EF07MA01) Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, [...].
> (EF07MA04). Resolver e elaborar problemas que envolvam operações com números inteiros.
> (EF07MA04MA) Compreender a história do uso de letras ou símbolos na Matemática.

Constata-se que, no Ensino Fundamental do 5° ao 7° ano, há possibilidade da inserção da noção de congruência no componente curricular Matemática. Note que a habilidade número 10 do 5° ano tem como objeto de conhecimento "Propriedades da igualdade e noção de equivalência", desse modo é pertinente abordar a simbologia de congruência $\equiv$ como uma noção de equivalência enfatizando suas propriedades.

Essa noção vai ser aprofundada no 6° ano, visto que a habilidade número 05 e 06 possuem como objetos de conhecimento "Múltiplos e Divisores de um número natural; Números primos e compostos.", percebe-se que os alunos terão um contato mais acentuado com os critérios de divisibilidade, a qual é uma excelente oportunidade para aprofundar a noção de congruência, já que é uma nova maneira de se comparar os números naturais. Por exemplo, dividindo uma turma de 31 alunos em dois grupos, de modo que um grupo A tenha 14 alunos e um grupo B tenha 17, e consequentemente fizermos uma nova divisão dentro de cada grupo formando subgrupos de 3 alunos, notaremos que ambos os grupos terão 2 alunos sobrando. Assim, tem-se que 14 e 17 são congruentes módulo 3, pois quando divididos por 3, o resto é o mesmo.

Consequentemente, de encontro com a habilidade número 01 do 7°ano, cujo objeto de conhecimento é "Múltiplos e divisores de um número natural", a noção de congruência modular pode ser retomada. Nesse mesmo ano, essa noção pode ser aprofundada consoante a habilidade número 04 em que o objeto de conhecimento é "Números inteiros: usos, história, ordenação, associação com pontos da reta numérica e operações", pois ampliaremos a noção para o conjunto dos números inteiros.

SOUZA 2015 (p. 37), defende que a aritmética modular seja introduzida na grade curricular das séries anos do Ensino Fundamental. Nesse sentido, a noção de congruências pode ser aprofundada com inserção também das Equações Diofantinas, pois, segundo MARANHÃO 2019 (p.335-350):

> (EF08MA07) Associar uma equação linear de 1o grau com duas incógnitas a uma reta no plano cartesiano.
> (EF08MA08) Resolver e elaborar problemas [...] representados por sistemas de equações de 1o grau com duas incógnitas e interpretá-los, utilizando, inclusive, o plano cartesiano como recurso.
> (EF08MA02MA) Valorizar a linguagem Matemática para expressar-se com clareza na resolução de problemas.
> (EF09MA06) Compreender as funções como relações de dependência unívoca entre duas variáveis e suas representações numérica[...].

Verifica-se que a habilidade número 07, 08 e 02MA de matemática no 8° ano, cujo objetos de conhecimento são "Associação de uma equação linear do 1° grau a uma reta no plano cartesiano", "Sistemas de equações polinomiais de 1° grau: resolução algébrica e representação no plano cartesiano", permitem ao docente apresentar aos alunos alguns tipos de equações diofantinas, além disso, podendo o mesmo sugerir a aplicação da congruência modular como um novo meio de resolução. Vale salientar que esse ensino corrobora com a terceira competência específica de Matemática para o Ensino Fundamental presente na BNCC, pois estabelece relações entre conceitos e procedimentos de Aritmética e Álgebra (BRASIL 2018). Esse fundamento será aprofundado no ano seguinte, visto que para o 9° ano, obtendo a habilidade número 06 com o objeto de conhecimento "Funções: representações numérica, algébrica e gráfica", que possibilita ao professor propor continuidade ao estudo da congruência modular aplicada às equações diofantinas, relacionando com as representações geométricas.

GOMES et al. 2015 (p.67) propõe o estudo de congruências no Ensino Médio. Nesse mesmo intuito, E. M. OLIVEIRA et al. 2017 (p.05) acredita que esse objeto de estudo quando aplicado nesse nível de ensino pode levar aos educando habilidades que os permitem criar conjecturas, deixando-os confortáveis para fazer abstrações, provocando argumentações de diferentes teores de escrita ou fala. Desse modo, há possibilidades da inserção também da aritmética modular no ensino médio, note que a BNCC aponta cinco competências específicas de matemática:

> COMPETÊNCIA ESPECÍFICA 1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos [...].
> COMPETÊNCIA ESPECÍFICA 2. Articular conhecimentos matemáticos ao propor e/ou participar de ações para investigar desafios do mundo contemporâneo [...].
> COMPETÊNCIA ESPECÍFICA 3. Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos [...].
> COMPETÊNCIA ESPECÍFICA 4. Compreender e utilizar, com flexibilidade e fluidez, diferentes registros de representação matemáticos [...].

> COMPETÊNCIA ESPECÍFICA 5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas[...].(BRASIL, 2019, p. 523).

Cada competência mencionada agrega uma grade habilidades a serem desenvolvidas. A partir de algumas analises e inferências, consoante à BRASIL 2018 (p.525-533) vale destacar os seguintes códigos de habilidades do currículo do ensino médio:

> (EM13MAT301) Resolver e elaborar problemas do cotidiano, [...], que envolvem equações lineares simultâneas [...].
> (EM13MAT302) Construir modelos empregando as funções [...].
> (EM13MAT401) Converter representações algébricas de funções polinomiais de 1º grau em representações geométricas no plano cartesiano, [...].
> (EM13MAT501) Investigar relações entre números expressos em tabelas para representá-los no plano cartesiano [...], reconhecendo quando essa representação é de função polinomial de 1º grau.
> (EM13MAT510) Investigar conjuntos de dados relativos ao comportamento de duas variáveis numéricas [...].

A partir das habilidades em citadas, para o 1° ano do ensino médio o objeto de conhecimento "Conjuntos e Funções; Funções Polinomiais do 1° grau". Verificam-se que os "Conjuntos" podem ser usados para representar classes de equivalência em relação à congruência modular. Por exemplo, se estivermos trabalhando módulo 5, o conjunto $(0, 5, 10, 15, ...)$ representa a classe de equivalência para o $(0\ mod\ 5)$, o conjunto $(1, 6, 11, 16, ...)$ representa a classe de equivalência para $(1\ mod\ 5)$, e assim por diante. Além disso, funções podem ser usadas para representar operações aritméticas que preservam congruência modular. Por exemplo, pode-se definir uma função $f(x)$ que realiza adição modular, com destaque $f(x) = (x + k)\ mod\ n$ para algum inteiro k e módulo n.

Por outro lado, para o 2° ano do ensino médio, tem-se o objeto de conhecimento "Sistemas de Equações Lineares". Verifica-se, em alguns casos, que os sistemas de equações podem ser reformulados como equações diofantinas, que por sua vez, permitem ser resolvidos usando técnicas de congruência modular. Além disso, POMMER et al. 2008 (p. 56):

> que o estudo de equações diofantinas lineares ocorra no Ensino Médio o que disponibilizaria aos alunos uma maneira elegante e sistemática de obter soluções inteiras diferentemente das estratégias abordadas em muitos livros que são por meio de tentativa e erro ou da atribuição de valor a uma variável com a determinação do valor correspondente da outra variável.

Portanto, diante daquilo que foi exposto, pode-se inferir ainda mais que o ensino de Aritmética Modular pode estar sendo alinhado também ao currículo do ensino médio. MATTOS, PUGGIAN e LOZANO 2011 (p.11) al enfatiza que o estudo de assuntos inerentes à teoria dos números favorece o desenvolvimento de ideias fundamentais da matemática, tais como: conjecturas, argumentações e demonstrações, além de ajudar os estudantes no entendimento conceitual da aritmética e da álgebra.

3 TEORIA ELEMENTAR DOS NÚMEROS

A primeira informação confiável sobre o conhecimento Aritmética é encontrada nos monumentos históricos do Antigo Egito e na Babilônia, relativa ao 3°-2° milênio a.C. BOYER e Uta C. 2019.

Segundo BOYER e Uta C. 2019, a Aritmética veio a ocupar-se com uma classe mais vasta de problemas que surgiram naturalmente a partir do estudo dos números inteiros. Consoante às formas que são utilizadas e às situações que são investigadas, essa teoria citada pode ser subdividida em vários campos:

- Teoria Elementar: que utiliza as formas elementares da aritmética para verificação e comprovação das propriedades essenciais do conjunto dos números inteiros e em particular as propriedades dos números primos;
- Teoria analítica dos números: que utiliza a análise real e análise complexa; primordialmente para estudas as propriedades dos números primos;
- Teoria algébrica: que faz uso da álgebra abstrata e estuda os números algébricos;
- Teoria geométrica: que utiliza métodos geométricos, algébricos e analíticos.

Para este trabalho, será dado ênfase ao estudo da Teoria Elementar dos Números, ou seja, a Aritmética modular, visto que é uma área de conhecimentos fundamentais a qualquer cidadão. E para fundamentar melhor os conceitos e definições que serão trabalhados neste capítulo, têm-se como principais fontes as obras de FILHO 1981, HEFEZ 2016a, HEFEZ 2016b, LEITÃO 2019, RIBENBOIM 2012, SANTOS 2012 e VIEIRA 2020.

3.1 Divisibilidade

Definição 3.1.1. *Sejam a e b dois inteiros, com $a \neq 0$. Diz-se que a divide b, e escreve-se $a \mid b$ se, e somente se, existe um inteiro q tal que*

$$b = a \cdot q$$

Nesse caso, diremos também que a é um divisor ou um fator de b ou ainda, que b é um múltiplo de a ou que b é divisível por a. Escreve-se $a \nmid b$ para indicar que a não divide b, mostrando que não existe nenhum número inteiro q tal que $b = a \cdot q$.

Vale destacar que se a é divisor de b, então $(-a)$ também será divisor de b, pois por (3.1) implica que $b = (-a) \cdot (-q)$, com q inteiro. Desse modo, para qualquer inteiro existem dois a dois iguais em valor absoluto e de sinais opostos.

Exemplo 3.1.1. *Note que $-5 \mid 40$, pois $40 = (-5) \cdot (-8)$, e ainda que $5 \nmid 31$, pois não existe um $q \in \mathbb{Z}$ com $31 = (5) \cdot (q)$*

Proposição 3.1.1. *Quaisquer os inteiros a, b, c e d, tem-se:*

1. $a \mid 0$, $1 \mid a$ *e* $a \mid \pm 1$;
2. *Se* $a \mid 1$, *então* $a = \pm 1$;
3. *Se* $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$;
4. *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$;
5. *Se* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$;
6. *Se* $a \mid b$ *com* $b \neq 0$, *então* $|a| \leq |b|$;
7. *Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid (bx + cy)$;

A demonstração dos itens da Proposição anterior é encontrada nas obras dos autores citados no início desta seção. Em seguida, tem-se alguns exemplos.

Exemplo 3.1.2. *Sejam* a, b *e* c *inteiros. Mostre que se* $a \mid b$ *e* $a \mid c$, *então* $a^2 \mid b \cdot c$.

Solução. Como $a \mid b$ e $a \mid c$, tem-se que

$$b = a \cdot q_1, \ com \ q_1 \in \mathbb{Z}. \tag{1}$$

$$c = a \cdot q_2, \ com \ q_2 \in \mathbb{Z}. \tag{2}$$

Com efeito, multiplicando membro a membro das equações (1) e (2), obtém–se:

$$b \cdot c = a \cdot a \cdot (q_1 \cdot q_2) \Longrightarrow b \cdot c = a^2 \cdot (q_1 \cdot q_2).$$

Portanto, $a^2 \mid b \cdot c$.

Exemplo 3.1.3. *Prove que o número* $M = 5^{2024} - 7$ *não é divisível por* 5.

Solução. Suponha, por contradição, que o número M seja divisível por 5. Logo, por definição, existe um número inteiro q de modo que

$$5^{2024} - 7 = 5 \cdot q.$$

Logo,

$$7 = 5^{2024} - 5 \cdot q$$
$$7 = 5 \cdot (5^{2023} - q).$$

Fazendo $5^{2023} - q = q'$, tem-se que

$$7 = 5 \cdot q'.$$

Ou seja, dessa forma, 7 seria divisível por 5, o que é uma contradição. Portanto, o número $M = 5^{2024} - 7$ não é divisível por 5.

Definição 3.1.2. *Sejam* a *e* b *dois inteiros e* $d \neq 0$, *chamamos de Divisor Comum dos inteiros* a *e* b *um inteiro* d *tal que* $d \mid a$ *e* $d \mid b$.

Dizer que d é Divisor Comum de dois inteiros a e b significa que d pertence simultaneamente aos conjuntos $D(a)$ (indica todos os divisores de a) e $D(b)$ (indica todos os divisores de b), onde

$D(a) = \{x \in \mathbb{Z}^*; x \mid a\}$. *Como* $x \mid a \Rightarrow x \mid (-a)$, *logo* $D(a) = D(-a) \Rightarrow a = a{\cdot}1 = (-a){\cdot}(-1)$;

$D(b) = \{x \in \mathbb{Z}^*; x \mid b\}$. *Como* $x \mid b \Rightarrow x \mid (-b)$, *logo* $D(b) = D(-b) \Rightarrow b = b{\cdot}1 = (-b){\cdot}(-1)$.

Assim, $d \in D(a, b)$, ou seja, $D(a, b) = \{x \in \mathbb{Z}^*;\ x \in D(a),\ x \in D(b)\}$, pode-se afirmar ainda que

$$D(a, b) = D(a) \cap D(b).$$

Vale destacar que $1,\ -1,\ a$ e $-a$ são divisores de a e, de modo análogo, $1,\ -1,\ b$ e $-b$ são os divisores de b, esses divisores são chamados de divisores triviais de a e b. Qualquer que seja o inteiro a não nulo, se $x \mid a$ e $x \mid b$ então

$$-a \leq x \leq a \ e\ D(a) \subset [-a,\ a].$$
$$-b \leq x \leq b \ e\ D(b) \subset [-b,\ b].$$

Portanto, qualquer inteiro diferente de zero tem um número finito de divisores.

Dessa forma, como dois inteiros a e b quaisquer admitem sempre -1 e 1 como divisores comuns, pode-se afirmar que o conjunto $D(a, b)$ dos divisores comuns a e b nunca é vazio, ou seja, $D(a, b) \neq \emptyset$. Em particular, se $a = b = 0$, então todo inteiro não nulo é um divisor comum de a e b, isto é, $D(a, b) = \mathbb{Z}^*$.

Exemplo 3.1.4. *Quais os divisores comuns dos inteiros* $a = 20$ *e* $b = -16$.

Solução. Note que

$$D(20) = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 5\ \ \pm 10,\ \pm 20\};$$
$$D(-16) = \{\pm 1,\ \pm 2,\ \pm 4,\ \pm 8\ \ \pm 16\}.$$

Assim,

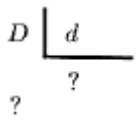
$$D(20, -16) = D(20) \cap D(-16) = \{\pm 1,\ \pm 2,\ \pm 4\}.$$

3.1.1 Algoritmo da Divisão

O Algoritmo da Divisão é um dos principais resultados da Teoria dos Números, também conhecido como Divisão Euclidiana, possui várias aplicabilidades no cotidiano. Esse resultado é atribuído a Euclides, em seu livro VII dos Elementos de Euclides, escrito por volta de 300 a.C.

Esse Algoritmo é estudado desde o Ensino Fundamental e perpassa pelo Médio e Superior, porém MELO e J. L. d. OLIVEIRA 2023 (p.11) ressalta que

Geralmente, quando se fala em divisão entre dois inteiros positivos, digamos D, *dividendo* e d, *divisor*, $D \geq d > 0$, desde os primeiros anos do Ensino Fundamental, costumamos (tanto alunos quanto professores) associá-la ao seguinte dispositivo prático:



e que, devido a tal associação, esse dispositivo passou, erroneamente, a ser chamado de algoritmo da divisão. Essa confusão se dá pelo fato de, ainda no Ensino Fundamental, os alunos não terem absorvido a ideia de divisão entre dois inteiros.

Nesse sentido, se esse Algoritmo não for explicitado da forma correta aos alunos, possivelmente carregarão tais deficiências para toda a vida.

Euclides utiliza o fato de que, mesmo quando um número inteiro $b \neq 0$ não divide o número inteiro a, é possível efetuar a divisão de a por b, com resto. Desse modo, a fim de se compreender o Algoritmo da Divisão, é de grande importância enunciar o Teorema de Eudoxius.

Teorema 3.1.1.1. (Eudoxius) *Considere a e b inteiros com $b \neq 0$. Então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, corresponde a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que,*

$$q \cdot b \leq a < (q+1) \cdot b, \tag{3}$$

para $b > 0$ e

$$q \cdot b \leq a < (q-1) \cdot b, \tag{4}$$

para $b < 0$.

Demonstração. Suponha que $a > 0$ e $b > 0$. Deste modo, existem duas possibilidades:

1. Se $a = q \cdot b$, para algum $q \in \mathbb{Z}$ não há o que provar e o resultado segue;
2. Se $a = q \cdot b$, para todo $q \in \mathbb{Z}$, existe um menor inteiro k que satisfaz a condição: $a < k \cdot b$.

Segue que $(k-1) \cdot b < a$. De fato, se $a < (k-1) \cdot b$ o que é uma contradição, pois uma vez que $a < k \cdot b$ e p é o menor inteiro em que isto ocorre. Portanto, deve-se ter $(k-1) \cdot b < a < k \cdot b$. Tomando $q = k - 1$, obtém-se

$$q \cdot b \leq a < (q+1) \cdot b.$$

Os casos em que $a < 0$ ou $b < 0$ são demonstrados de forma análoga.

Exemplo 3.1.1.1 *Para $a = 20$ e $b = 5$, fazendo $q = 4$, tem-se:*

$$4 \cdot 5 \leq 20 < (4+1) \cdot 5 \Longrightarrow 4 \cdot 5 \leq 20 < 5 \cdot 5.$$

Para $a = -8$ e $b = 3$, tomando $q = -3$, tem-se

$$(-3) \cdot 3 \leq -8 < (-3+1) \cdot 3 \Longrightarrow (-3) \cdot 3 \leq -8 < (-2) \cdot 3.$$

Para $a = 10$ e $b = -4$, tomando $q = -3$, tem-se

$$(-3) \cdot (-4) \leq -10 < (-3-1) \cdot (-4) \Longrightarrow (-3) \cdot (-4) \leq -10 < (-4) \cdot (-4).$$

Utilizando o Teorema de Eudoxius, aprimora-se o entendimento sobre o resultado central desta teoria.

Teorema 3.1.1.2 (Algoritmo da Divisão) *Sejam dois inteiros positivos a e b, com $b \neq 0$ existem e são únicos os inteiros q e r, tais que,*

$$a = q \cdot b + r, \ com \ 0 \leq r < b.$$

Os inteiros q e r são chamados respectivamente de quociente e resto. E $r = 0$ se, e somente se, b é divisor de a, ou seja, $b \mid a$.

> Para que o aluno entenda o que significa a divisão entre dois números inteiros, com o segundo inteiro positivo, é de extrema importância que o professor tenha essa compreensão de que esse algoritmo dá significado ao processo ordinário de divisão, sem ter que fazer necessariamente uma associação com o dispositivo citado anteriormente, fazendo com que o aluno confunda a operação de divisão com um mecanismo criado para efetuá-la. Após essa compreensão, como um recurso para facilitar o cálculo da divisão, o dispositivo pode ser usado. Posto isto, e para ampliar os conceitos relativos à divisão de inteiros, o aluno deverá ser apresentado a casos em que a divisão entre dois inteiros quaisquer, com o segundo diferente de zero, também é possível. (MELO e J. L. d. OLIVEIRA 2023, p.12)

Demonstração. Pelo Teorema de Eudoxius, como $b > 0$, existe um inteiro q satisfazendo

$$q \cdot b \leq a < (q+1) \cdot b$$

o que implica $0 \leq a - q \cdot b < b$. Desta forma, se fazer $r = a - q \cdot b$, tem-se garantida a existência de q e r. Mostrando a unicidade, supondo a existência de outro par q_1 e r_1 verificando

$$a = q_1 \cdot b + r_1, \ com \ 0 \leq r_1 < b.$$

Assim $(q \cdot b + r) - (q_1 \cdot b + r_1) = 0$, isto é, $b \cdot (q - q_1) = r_1 - r$, isso implica que $b \mid (r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, $|r_1 - r| < b$ e $b \mid (r_1 - r)$, tem-se $r_1 - r = 0$ e $r = r_1$. Logo, $q_1 \cdot b = q \cdot b$ e $q_1 = q$, uma vez que $b \neq 0$.

Corolário 3.1.1.1 (Algoritmo da Divisão) *Sejam dois inteiros a e b, com $b \neq 0$ existem e são únicos os inteiros q e r, que satisfazem as condições:*

$$a = q \cdot b + r, \ com \ 0 \leq r < |b|.$$

Demonstração. Se $b > 0$, é fácil ver, mas se $b < 0$, então $|b| > 0$, e consequentemente existem e são únicos os inteiros q_1 e r tais que

$$a = q_1 \cdot b + r, \ com \ 0 \leq r < |b|,$$

ou seja, por ser $|b| = -b$, para $b < 0$:

$$a = q_1 \cdot (-b) + r \Rightarrow a = (-q_1) \cdot b + r, \ com \ 0 \leq r < |b|,$$

Portanto, existe e são únicos os inteiros $q = q_1$ e r tais que

$$a = q \cdot b + r, \ com \ 0 \leq r < |b|.$$

Problema 3.1.1.1. *Um turista brasileiro chega a Cuba e troca parte de seu dinheiro na casa de Câmbio, recebendo 175 notas de 50 pesos e 213 notas de 20 pesos. Ele decide trocar este dinheiro pela maior quantidade possível das famosas moedas de 3 pesos cubanos, porque elas têm gravada a imagem do guerrilheiro Che Guevara. Quanto sobrou do dinheiro depois de fazer a troca pelas moedas?*

Solução: Este problema pode ser resolvido encontrando o resto da divisão de

$$n = 175 \cdot 50 + 213 \cdot 20$$

por 3. Porém, destacaremos que não há necessidade de fazer os produtos e a soma envolvidos no número n. Basta substituirmos cada número que aparece em n pelo resto que este deixa na divisão por 3, formando assim um novo número n_1, ou seja,

$$n_1 = 1 \cdot 2 + 0 \cdot 2.$$

$$n_1 = 2.$$

Note que n_1 deixa resto igual a 2 na divisão por 3 e, de fato, verificando em n, tem-se que

$$n = 175 \cdot 50 + 213 \cdot 20 \Longrightarrow n = 13010 = 3 \cdot 4336 + 2.$$

Logo, sobraram 2 pesos depois de fazer a troca.

3.2 Máximo Divisor Comum

Conforme a subsecção **3.1**, especificamente na **Definição 3.1.2**, os divisores de um número a são os números inteiros que dividem a, ou seja, pelos quais a é divisível. Indica-se por $D(a)$ o conjunto dos divisores de a, onde $D(a)$ é finito.

Definição 3.2.1 *Sejam a e b dois inteiros não conjuntamente nulos ($a \neq 0$ ou $b \neq 0$). Chamamos de Máximo Divisor Comum de a e b o inteiro positivo d que satisfaz as seguintes condições:*

1. $d \mid a$ e $d \mid b$;
2. *Se $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$, então $c \leq d$.*

O máximo divisor comum de a e b é indicado por $d = mdc(a,\ b)$, é imediato que $mdc(a,\ b) = mdc(b,\ a)$. Também é imediato os seguintes casos:

1. O $mdc(0,\ 0)$ é indeterminado;
2. O $mdc(a,\ 1) = 1$;
3. Se $a \neq 0$, então o $mdc(a,\ 0) = |a|$;
4. Se $a \neq 0$, então o $mdc(a,\ a) = |a|$;
5. $a \mid b$, então o $mdc(a,\ b) = |a|$;

Ainda mais, é imediato observar que: $mdc(a,\ b) = mdc(-a,\ b) = mdc(a,\ -b) = mdc(-a,\ -b)$.

Proposição 3.2.1 *Se $a,\ b,\ c,\ x_1, e\ y_1 \in \mathbb{Z}$, e $c \mid a$ e $c \mid b$, então $c \mid (ax_1 + by_1)$.*

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

$$a = k_1 \cdot c \tag{5}$$

$$b = k_2 \cdot c, \tag{6}$$

com k inteiro. Multiplicando (5) por x_1 e (6) por y_1, tem-se

$$x_1 \cdot a = x_1 \cdot k_1 c \tag{7}$$

$$y_1 \cdot b = y_1 \cdot k_2 c. \tag{8}$$

Somando membro a membro de (7) e (8), obtem-se que

$$ax_1 + by_1 = (x_1 k_1 + y_1 k_2) \cdot c.$$

O que implica que

$$c \mid (ax_1 + by_1).$$

Teorema 3.2.1 *Seja d o máximo divisor comum entre a e b, então existem inteiros x e y tais que $mdc(a,\ b) = ax\ +\ by$ isto é, o $mdc(a,\ b)$ é uma combinação linear de a e b.*

Demonstração. Considere $\mathbb{L}$ o conjunto de todas as combinações lineares $ma + nb$ onde m e n são inteiros, isto é,

$$\mathbb{L} = \{(ma + nb) \mid (ma + nb) > 0 \ \ e \ \ m,\ n \in \mathbb{Z}.$$

Esse conjunto $\mathbb{L} \neq \varnothing$ pois, existem números negativos, positivos e também o zero. Tomando m_0 e n_0 tais que $c = m_0 a + n_0 n$ seja o menor inteiro positivo pertencente ao conjunto $\mathbb{L}$. Como $d = mdc(a, b)$, pelo Teorema Algoritmo da Divisão de Euclides, existem q e r tais que

$$a = qc + r \quad com \quad 0 \leq r < c.$$

Desse modo,

$$r = a - qc = a - q(m_0 a + n_0 b) = (1 - qm_0)a + (-1n_0)b,$$

isto é, o resto r é uma combinação linear de a e b. Isto mostra que $r \in \mathbb{L}$, pois $(1 - qm_0)$ e $(-qn_0)$ são inteiros, como $0 \leq r < c$ e $c > 0$ é o elemento mínimo de $\mathbb{L}$, então $r = 0$ e $a = qc$, ou seja, $c \mid a$.

De forma análoga se prova que $c \mid b$, logo, c é um divisor comum positivo de a e b. Por outro lado d também é um divisor comum positivo de a e b, então existem inteiros k_1 e k_2 tais que $a = k_1 d$ e $b = k_2 d$ e, desse modo, tem-se que

$$\begin{aligned} c &= m_0 a + n_0 b \\ &= m_0(k_1 d) + n_0(k_2 d) \\ &= d(m_0 k_1 + n_0 k_2), \end{aligned}$$

isto é, $d \mid c$ e $c > 0$, tem-se $d \leq c$, note que se $d < c$ não é possível, ou seja, d é o maior divisor comum positivo de a e b, conclui-se que $d = c$, logo,

$$d = mdc(a, b) = m_0 a + n_0 b.$$

O **Teorema 3.2.1** mostra, a partir de sua demonstração, que o $mdc(a,\ b)$ é o menor inteiro positivo da forma $ax + by$, ou seja, pode ser expresso como uma combinação linear de a e b. Porém, essa combinação linear não é única.

Exemplo 3.2.1. *Dados os inteiros $a = 10$ e $b = 8$, tem-se que :*

$$mdc(10,\ 8) = 2 \Longrightarrow 10x + 8y = 2,$$

tomando $x_0 = 1$ e $y_0 = -1$ tem-se $10 \cdot (1) + 8 \cdot (-1) = 2$. Generalizando, todos os pares de inteiros $(x_0,\ y_0)$ que satisfazem a $10x + 8y = 2$ podem ser obtido por:

$$x = 1 + 4k \quad e \quad y = -1 - 5k,$$

com $k \in \mathbb{Z}$. De fato, $10(1 + 4k) + 8(-1 - 5k) = 2$. Esse conteúdo será mais aprofundado e detalhado na seção de Equações Diofantinas.

3.3 Algoritmo de Euclides

Lema 3.3.1 *Se $a = bq + r$, então $mdc(a,\ b) = mdc(b, r)$.*

Demonstração. Se o $mdc(a,\ b) = d$, então, pela definição de MDC, $d \mid a$ e $d \mid b$, o que implica $d \mid (a - bq)$ ou $d \mid r$, isto é, d é um divisor comum de b e r, pois $d \mid b$ e $d \mid r$.

De forma análoga, se c é um divisor comum qualquer de b e r, ou seja, $c \mid b$ e $c \mid r$, então $c \mid (bq + r)$ ou $c \mid a$, isto é, c é um divisor comum de a e b, daí $c \leq d$, pois $mdc(a,\ b) = d$. Logo, $mdc(b,\ r) = d$.

Sejam a e b dois inteiros tais que $a \neq 0$ ou $b \neq 0$ cujo máximo divisor comum se deseja determinar. Para isso, note que $mdc(a,\ b) = mdc(|a|, |b|)$, suponho que a e b são inteiros positivos distintos, se $a > b$, tais que b não divide a, isto é $b \nmid a$. Daí, aplicando diversas vezes o algoritmo da divisão, teremos as seguintes igualdades:

$$\begin{aligned} a &= bq_1 + r_1,\ com\ 0 < r_1 < b; \\ b &= r_1q_2 + r_2,\ com\ 0 < r_2 < r_1; \\ r_1 &= r_2q_3 + r_3,\ com\ 0 < r_3 < r_2; \\ r_2 &= r_3q_4 + r_4,\ com\ 0 < r_4 < r_3; \\ \vdots &= \vdots \end{aligned}$$

Todos os restos $r_1,\ r_2,\ r_3,\ r_4,\ ...$, são todos inteiros positivos, tais que

$$b > r_1 > r_2 > r_3 > r_4 > ...$$

e existem apenas $b-1$ inteiros positivos menores que b, necessariamente se chega a uma divisão, cujo resto $r_{n+1} = 0$, ou seja:

	q_1	q_2	q_3		q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-1}	r_n
r_1	r_2	r_3	r_4		0	.

O Algoritmo de Euclides também é utilizado para expressar o $mdc(a,\ b)$ na forma de $ax + by$, com x e $y \in \mathbb{Z}$, ou seja, $mdc(a,\ b) = ax + by$. Quando utilizado dessa forma, esse algoritmo é conhecido como Algoritmo de Euclides Estendido.

Exemplo 3.3.1 *Usando o algoritmo de Euclides, encontre os inteiros x e y que satisfazem a seguinte igualdade:*

$$mdc(24,\ 62) = 24x + 62y.$$

Solução: Note que, usando o Algoritmo de Euclides

	2	1	1	2	2
62	24	14	10	4	2
14	10	4	2	0	.

Escrevendo cada divisão da seguinte forma:

$$\begin{aligned} 62 &= 24 \cdot 2 + 14 \\ 24 &= 14 \cdot 1 + 10 \\ 14 &= 10 \cdot 1 + 4 \\ 10 &= 4 \cdot 2 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Desse modo, pelo **Lema 3.3.1**,

$$mdc(62, 24) = mdc(24, 14) = mdc(14, 10) = mdc(10, 4) = 2.$$

Note que $mdc(24, 62) = 2$ e sua expressão como combinação linear de 24 e 62. Assim, isolando das igualdades anteriores os restos $2,\ 4,\ 10,\ e\ 14$, têm-se:

$$14 = 62 - 24 \cdot 2$$

$$10 = 24 - 14 \cdot 1$$
$$4 = 14 - 10 \cdot 1$$
$$2 = 10 - 4 \cdot 2.$$

Substituindo as igualdades, tem-se que:

$$2 = 10 - (14 - 10 \cdot 1) \cdot 2 \Longrightarrow 2 = 10 \cdot (3) + 14 \cdot (-2)$$
$$2 = (24 - 14 \cdot 1) \cdot (3) + 14 \cdot (-2) \Longrightarrow 2 = 24 \cdot (3) + 14 \cdot (-5)$$
$$2 = 24 \cdot (3) + (62 - 24 \cdot 2) \cdot (-5) \Longrightarrow 2 = 24 \cdot (13) + 62 \cdot (-5)$$

Logo,

$$mdc(24, 62) = 2 = 24x + 62y,$$

com $x = 13$ e $y = -5$. Vale destacar que a combinação linear não é única.

Problema 3.3.1 *(Colégio Militar Tiradentes - MA 2020) Maria Clara é dona de uma fábrica de tecidos. A fábrica produz retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas:* 156 *centímetros e* 234 *centímetros. O gerente de produção da fábrica ao ser informado das medidas, deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível.*
Qual o comprimento de cada pedaço de tecido depois de cortadas as peças que sobraram?
a) 90 *cm*
b) 95 *cm*
c) 78 *cm*
d) 85 *cm*
e) 93 *cm*

Solução: Note que, para resolver esse problema, basta encontrar o resultado do Máximo Divisor Comum de 156 e 234. Para tanto, aplicando o Algoritmo de Euclides, tem-se

	1	2
234	156	78
78	0	.

Logo, cada peça de tecido, depois de cortada, deverá ter comprimento igual 78 cm. E, a alternativa *c*) é o gabarito da questão.

3.4 Números Primos

Um dos conceitos mais importantes da matemática é sobre os números primos, visto que desempenham um papel fundamental e estão associados a diversos problemas matemáticos, além das inúmeras aplicações.

Definição 3.4.1 *Um número inteiro positivo p é chamado de primo quando possui somente dois divisores: 1 e o próprio p.*

Definição 3.4.2 *Um número inteiro positivo é chamado de composto quando possui 3 ou mais divisores.*

Exemplo 3.4.1 *12 não é primo, pois, além de 1 e 12, os inteiros positivos 2, 3, 4 e 6 dividem 12.*

Exemplo 3.4.2 *5 é primo, pois os inteiros positivos 2, 3, 4 não dividem 5.*

Quando um inteiro a divide um inteiro b, ou seja, $a \mid b$, equivale a dizer que a divisão de b por a deixa resto zero. Ao contrário, quando um inteiro a não divide um inteiro b, ou seja, $a \nmid b$, equivale a dizer que a divisão de b por a deixa resto diferente de zero.

3.4.1 Teorema Fundamental da Aritmética

Todos os números naturais não primos podem ser formados como produtos de primos e de maneira única, é o que diz o Teorema Fundamental da Aritmética.

Teorema 3.4.1.1. (Teorema Fundamental da Aritmética) *Todo número natural maior que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_i^{k_i},$$

com $0 \leq k_i, \quad i \in \mathbb{N}$.

A demonstração do Teorema encontra-se nos livros de FILHO 1981, HEFEZ 2016a, SANTOS 2012.

Segundo SPINA 2014(p.5)o "Teorema Fundamental da Aritmética é o resultado que nos permite escrever qualquer número como um produto de primos. No ensino Fundamental o utilizamos em muitas ocasiões, simplificar frações, calcular o mmc e mdc entre outras aplicações".

O Teorema Fundamental da Aritmética garate que qualquer número natural composto terá sempre os números primos em sua decomposição. Desse modo, ao utilizar o algoritmo da divisão, pode-se encontrar os fatores primos de um número e representá-lo como um produto de primos.

Exemplo 3.4.1.1. *Escrevendo 30 e 12 como produto de primos, tem-se que:*

$$30 = 2 \cdot 3 \cdot 5$$
$$12 = 2^2 \cdot 3 \ .$$

Problema 3.4.1.1 *(Banco de questões OBMEP 2008 - Adaptada). Advinhe - tenho dois números naturais primos entre si. Se eu somar 50 a cada um deles, encontro números de dois algarismo. Se eu subtrair 32 de cada um deles, também encontro números naturais de 2 algarismos. Quais são os números, sabendo que nenhum deles é primo e que o número par é maior que o ímpar?*

Solução: O problema é solucionado de diversas forma, uma delas é a seguinte:
Note que se somar 50 ou subtrair 32 ainda encontramos números de dois algarismos. Logo, os números procurados serão menores que 50 e maiores que 41. Descartando os números primos desse intervalo, ou seja, 43 e 47, restam $42, 44, 45, 46, 48, 49$. Assim, os números

procurados são 44 *e* 45, 45 *e* 46, 48 *e* 49, mas como o número par é menor que o ímpar, tem-se as possíveis soluções são: 44 *e* 45 ou 48 *e* 49.

3.5 Equações Diofantinas

Chama-se equação Diofantina a qualquer equação polinomial com coeficientes inteiros, independentemente da quantidade de incógnitas. Essa nomenclatura é uma homenagem a Diofanto, matemático grego que residiu na cidade de Alexandria no século III. Muitos o consideram como pai da Álgebra e da Teoria dos números. Ele foi o primeiro a estudar de forma sistemática as soluções inteiras de algumas equações polinomiais em uma abordagem algébrica.

Os matemáticos italianos do século XVI foram os primeiros a apresentar os trabalhos de Diofanto para a Europa. Pouco se sabe sobre a vida pessoal dele. Conta-se que sobre o seu túmulo havia escrito um enigma que continha detalhes para se calcular seu tempo de vida. Contam que o enigma foi gravado por seu amigo, Metrodorus, o qual era descrito da seguinte forma:

> Deus lhe concedeu ser menino pela sexta parte de sua vida, e somando sua duodécima parte a isso, cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança; depois de viver a metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números, ele terminou sua vida. (COHEN e Edward 1948, p.27)

Outra forma de enunciar esse enigma é: "Diofanto passou 1/6 de sua vida como criança, 1/12 como adolescente e mais 1/7 na condição de solteiro. Cinco anos depois de se casar, nasceu seu filho que morreu 4 anos antes de seu pai, e com metade da idade (final) de Diofanto".

Estabelecendo uma equação que resolve tal enigma, tem-se:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 \tag{9}$$

Note que o mmc[2,6,7,12] = 84. Assim, multiplicando (9) ambos os membros por 84, tem-se que:

$$84x = \frac{84x}{6} + \frac{84x}{12} + \frac{84x}{7} + 9 \cdot 84 + \frac{84x}{2} \Longrightarrow 84x = 75x + 9 \cdot 84 \Longrightarrow \mathbf{x = 84}.$$

Assim, considerando a veracidade do enigma e fazendo os devidos cálculos, concluiremos que Diofanto viveu por 84 anos.

Após abordar um breve relato histórico sobre Diofanto de Alexandria, dar-se-á um foco maior para as Equações Diofantinas Lineares. Conforme em FILHO 1981, HEFEZ 2016a e SANTOS 2012.

Definição 3.5.1. *Uma Equação Diofantina Linear é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas do tipo*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b,$$

com $a_1,\ a_2, \ldots,\ a_n$ *inteiros dados, chamados coeficientes,* b *que também é um inteiro dado, é chamado de termo constante e* $x_1,\ x_2, \ldots,\ x_n$ *são as incógnitas.*

Exemplo 3.5.1. *Exemplos de Equações Diofantinas*

1. $18x\ +\ 5y\ =\ 48$;
2. $26x\ +\ 36y\ =\ 20$;
3. $3x\ +\ 5y\ +\ 7z =\ 13$;
4. $2x\ +\ 4y\ + 8z\ =\ 8$;

Dessa forma, não são consideradas equações Diofantinas lineares as do tipo: $x^2 + y^2 = z^2$; $xy + 4y = xy$ e $x - y^3 = -8$. Pois não vão de encontro com a definição 5.1.1. mencionada.

O modo mais simples de equação Diofantina linear observada é o caso de quando uma equação possui duas incógnitas x e y, isto é:

$$ax\ + by\ =\ c,$$

com $a,\ b$ e c são inteiros dados, sendo $a,\ b \neq 0$.

Definição 3.5.2. *Equação Diofantina linear com duas variáveis é uma equação polinomial indeterminada na qual suas variáveis só podem assumir valores inteiros, sendo formada por uma igualdade entre a soma de dois monômios de grau um e um monômio de grau zero.*

A solução inteira da equação $ax\ + by\ =\ c$ é todo par de inteiros x_0 e y_0, tais que

$$ax_0\ + by_0\ =\ c.$$

Vale destacar que se suscita importante fazer os seguintes questionamentos:

- a) Em quais condições a equação $ax\ + by\ =\ c$ admite solução?
- b) Caso admita, quantas existem e como determiná-las?

Tais questionamentos serão solucionados no decorrer deste tópico. Note que resolver $ax\ + by\ =\ c$ em valores reais equivale geometricamente a traçar uma reta no plano, algo simples de se fazer. Desse modo, neste trabalho, dar-se-á destaque às soluções inteiras. Veja o exemplo resolvido de uma equação Diofantina linear abaixo.

Exemplo 3.5.2. *Resolvendo a equação Diofantina linear com duas incógnitas:*

$$7x\ +\ 5y\ =\ 33.$$

Tem-se que

$$7 \cdot 4 \ + \ 5 \cdot 1 \ = \ 33$$
$$7 \cdot 9 \ + \ 5 \cdot (-6) \ = \ 33$$
$$7 \cdot (-1) \ + \ 5 \cdot 8 \ = \ 33$$
$$7 \cdot 14 \ + \ 5 \cdot (-13) \ = \ 33$$
$$7 \cdot (-6) \ + \ 5 \cdot 15 \ = \ 33.$$

Logo, os pares de inteiros: $(4, 1)$*;* $(9, -6)$*;* $(-1, 8)$*;* $(14, -13)$ *e* $(-6, 15)$ *são considerados soluções da equação* $7x \ + \ 5y \ = \ 33$*. Porém esses pares destacados não são as únicas soluções.*

Contudo, há equações Diofantinas lineares com duas incógnitas que não admitem soluções, como por exemplo

$$6x \ + \ 2y \ = \ 5,$$

onde $2y$ é um número par da forma $2a$ e $6x$ é outro número par da forma $2b$, além disso, 5 é um número ímpar da forma $2c + 1$. Isso nos mostra que

$$2b \ + \ 2a \ \neq \ 2c \ + \ 1$$
$$2(b \ + \ a) \ \neq \ 2c \ + \ 1,$$

com efeito, $d = (a + b)$, tem-se

$$2d \ \neq \ 2c \ + \ 1.$$

Assim, confirma-se que a equação $6x \ + \ 2y \ = \ 5$ não tem solução, visto que 5 é ímpar e $6x \ + \ 2y$ resulta sempre em um número par, para quaisquer valores de x e y. E os dois membros da equação não podem ser iguais. Portanto, não existe solução em $\mathbb{Z}$ para a equação $6x \ + \ 2y \ = \ 5$.

Posteriormente, notar-se-á que a existência de soluções de uma equação Diofantina está diretamente ligada ao máximo divisor comum dos coeficientes da equação, tal conteúdo abordado e trabalhado desde o ensino fundamental. Para responder ao questionamento a), feito anteriormente, observaremos a seguir:

Teorema 3.5.1 *A Equação Diofantina Linear* $ax + by = c$ *tem solução se, e somente se,* d *divide* c*, sendo* $d = mdc(a, \ b)$*.*

Demonstração. ($\Longrightarrow$) Suponha que x_0 e y_0 seja uma solução para a Equação Diofantina Linear $ax \ + \ by \ = \ c$, assim:

$$ax_0 \ + \ by_0 \ = \ c.$$

Como o $mdc(a, \ b) = d$, existem inteiros r e s tais que $a = dr$ e $b = ds$, e tem-se:

$$c \ = \ ax_0 \ + \ by_0 \ = \ drx_0 \ + \ dsy_0 \ = \ d \cdot (rx_0 \ + \ sy_0).$$

Assim, $rx_0 \ + \ sy_0$ é inteiro, logo d divide c, ou seja, $d \mid c$.

($\Longleftarrow$) Suponha que d divide c, ou seja, $d \mid c$. Assim existe t inteiro, tal que

$$c \ = \ d \cdot t. \tag{10}$$

Como o $mdc(a, b) = d$, tem-se que existem inteiros x_0 e y_0 tais que

$$d \;=\; ax_0 \;+\; by_0. \tag{11}$$

Multiplicando ambos os lados de (11) por t tem-se:

$$d \cdot t \;=\; (ax_0 \;+\; by_0) \cdot t \;\Longrightarrow\; c \;=\; a(tx_0) \;+\; b(ty_0).$$

De (10), $t = \dfrac{c}{d}$, isto é, o par de inteiros:

$$x \;=\; tx_0 \;=\; \left(\frac{c}{d}\right) \cdot x_0 \;\; e \;\; y \;=\; ty_0 \;=\; \left(\frac{c}{d}\right) \cdot y_0$$

é uma solução para a equação $ax + by = c$.

Corolário 3.5.1. *Se d divide c , sendo $d = mdc(a,\ b)$ e se o par de inteiros x_0 e y_0 é uma solução particular da equação diofantina linear $ax \;+\; by \;=\; c$, então todas as outras soluções dessa equação são dadas pela fórmula:*

$$x \;=\; x_0 \;+\; \left(\frac{b}{d}\right) \cdot t \qquad e \qquad y \;=\; y_0 \;-\; \left(\frac{a}{d}\right) \cdot t,$$

com $t \in \mathbb{Z}$.

Demonstração. Suponha que x_0 e y_0 inteiros seja uma solução particular para a equação Diofantina linear $ax \;+\; by \;=\; c$, e seja x_1 e y_1 outra solução qualquer da mesma equação. Então

$$\begin{aligned} x_0 + by_0 = \quad c \quad &= ax_1 + by_1 \\ &\Downarrow \\ a(x_1 - x_0) \;&=\; b(y_0 - y_1). \end{aligned} \tag{12}$$

Como o $mdc(a,\ b) = d$, e existem inteiros r e s tais que $a = dr$ e $b = ds$, com r e s primos entre si, substituindo em (12), tem-se:

$$(dr)\,(x_1 - x_0) = (ds)\,(y_0 - y_1) \Longrightarrow r \cdot (x_1 - x_0) = s \cdot (y_0 - y_1)$$

Assim, $r \mid s(y_0 - y_1)$, e sabendo que o $mdc(r,\ s) = 1$ implica que $r \mid (y_0 - y_1)$. Portanto, para qualquer inteiro t, tem-se:

$$y_0 - y_1 = rt \quad e \quad x_1 - x_0 = st.$$

Como $a = dr \Rightarrow r = \dfrac{a}{d}$ e $b = ds \Rightarrow s = \dfrac{b}{d}$, tem-se a solução:

$$x_1 \;=\; x_0 \;+\; \left(\frac{b}{d}\right) \cdot t \qquad e \qquad y_1 \;=\; y_0 \;-\; \left(\frac{a}{d}\right) \cdot t,$$

Note que os resultados de x_1 e y_1 satisfazem qualquer equação da forma $ax+by = c$, para qualquer inteiro t. Veja que:

$$ax_1 \;+ by_1 \;=$$

$$a\left[x_0 + \left(\frac{b}{d}\right)\cdot t\right] + b\left[y_0 + \left(\frac{a}{d}\right)\cdot t\right] =$$
$$(ax_0 + by_0) + \left(\frac{ab}{d} - \frac{ab}{d}\right)\cdot t =$$
$$c + 0\cdot t = \ c.$$

Portanto, se $mdc(a,\ b) = d$ e $d \mid c$, então para qualquer equação Diofantina da forma $ax + by = c$ existirá uma infinidade de soluções, uma para cada valor do inteiro arbitrário t.

Para encontrar uma solução particular, pode-se fazer por tentativa, ou recorrer ao Algoritmo de Euclides. Por afim, após identificar a particular, a solução geral é obtida usando o Teorema (3.5.2).

Exemplo 3.5.3 *Resolva a equação* $24x + 14y = 18$.

Solução: A equação tem solução, pois $mdc(24, 14) \mid 18$.

Com efeito, $24x + 14y = 18 \Longrightarrow 12x + 7y = 9$

Buscando uma solução particular $(x_0,\ y_0)$ pelo Algoritmo de Euclides para $12x + 7y = 9$, tem-se que:

$$12 = 7\cdot 1 + 5$$
$$7 = 5\cdot 1 + 2$$
$$5 = 2\cdot 2 + 1.$$

Substituindo as equações acima uma nas outras, obtém-se

$$1 = 12\cdot 3 - 7\cdot 5$$

Multiplicando ambos os membros da equação acima por 9, tem-se

$$9 = 12\cdot 27 + 7\cdot(-45).$$

Portanto, $x_0 = 27$ e $y_0 = -45$ é solução particular da equação $12x + 7y = 9$ e, consequentemente, as soluções são

$$\begin{cases} x = 27 + 7\cdot t \\ y = -45 - 12\cdot t \end{cases} \qquad t \in \mathbb{Z}.$$

Exemplo 3.5.4 *Resolva a equação* $17x - 28y = 37$.

Solução: Perceba que a equação tem solução, pois $mdc(17, -28) \mid 37$.

Buscando uma solução particular $(x_0,\ y_0)$ pelo Algoritmo de Euclides para $17x - 28y = 37$, tem-se que:

$$\begin{aligned} 28 = 17\cdot 1 + 11 \quad &\Longrightarrow \quad 11 = 28 - 17\cdot 1 \\ 17 = 11\cdot 1 + 6 \quad &\Longrightarrow \quad 6 = 17 - 11\cdot 1 \\ 11 = 6\cdot 1 + 5 \quad &\Longrightarrow \quad 5 = 11 - 6\cdot 1 \\ 6 = 5\cdot 1 + 1 \quad &\Longrightarrow \quad 1 = 6 - 5\cdot 1. \end{aligned}$$

Substituindo as equações acima uma nas outras, obtem-se

$$1 = 17 \cdot (5) - 28 \cdot (3)$$

Multiplicando ambos os membros da equação acima por 37, tem-se

$$37 = 17 \cdot (185) - 28 \cdot (111).$$

Portanto, $x_0 = 185$ e $y_0 = 111$ é solução particular da equação $17x + 28y = 37$ e, consequentemente, as soluções são

$$\begin{cases} x = 27 + 7 \cdot t \\ y = -45 - 12 \cdot t \end{cases} \qquad t \in \mathbb{Z}.$$

Problema 3.5.1 *Dispondo de R$100,00, quais são as quantias que se podem gastar comprando selos de R$5,00 e de R$7,00?*

Solução: A situação se resume em resolver a equação $5x + 7y = 100$, de modo que (x, y) pertencem aos inteiros, tal que $x > 0$ e $y > 0$.

Note que, $mdc(5, 7) = 1$ e $1 \mid 100$, logo a equação $5x + 7y = 100$ tem solução inteira. Do Algoritmo de Euclides, obtem-se

$$7 = 5 \cdot 1 + 2$$

$$5 = 2 \cdot 2 + 1.$$

Fazendo das igualdades acima: $1 = 5 - 2 \cdot 2$ e $2 = 7 - 5 \cdot 1$, em seguida substituindo, tem-se

$$1 = 5 + (7 + 5(-1))(-2)$$

$$1 = 5 + 7(-2) + 5(2)$$

$$1 = 5(3) + 7(-2).$$

Multiplicando ambos os lados do resultado acima por 100, tem-se que

$$100 = 5(300) + 7(-200).$$

Assim, a solução geral da equação é

$$x = 300 + 7t, \qquad y = -200 - 5t; \qquad sendo \;\; t \in \mathbb{Z}.$$

Entretanto, essa não é a solução final do problema, visto que $x \geq 0$ e $y \geq 0$. Portanto, basta fazer

$$300 + 7t > 0 \quad e \quad -200 - 5t > 0.$$

Das inequações implica

$$-42 < t < -40.$$

Portanto, quando

$$t = -40 \Longrightarrow x = 20 \quad e \quad y = 0$$

$$t = -41 \Longrightarrow x = 13 \quad e \quad y = 5$$

$$t = -42 \Longrightarrow x = 6 \quad e \quad y = 10.$$

Logo, as soluções são

- 13 selos de 5 reais e 5 selos de 7 reais;
- 6 selos de 5 reais e 10 selos de 7 reais.

Problema 3.5.2. *Dispondo de R$110,00, quais são as quantias que se podem gastar comprando selos de R$7,00 e de R$9,00?*

Solução: A situação se resume em resolver a equação $7x + 9y = 110$, de modo que (x, y) pertencem aos inteiros, tal que $x > 0$ e $y > 0$.

Note que, $mdc(7, 9) = 1$ e $1 \mid 110$, logo a equação $7x + 9y = 110$ tem solução inteira. Do Algoritmo de Euclides, obtém-se

$$9 = 7 \cdot 1 + 2$$
$$7 = 3 \cdot 2 + 1.$$

Fazendo das igualdades acima: $1 = 7 - 3 \cdot 2$ e $2 = 9 - 7 \cdot 1$, em seguida substituindo uma na outra, tem-se

$$1 = 7(1) + (9 + 7(-1))(-3)$$
$$1 = 7(1) + 7(3) + 9(-3)$$
$$1 = 7(4) + 9(-3).$$

Multiplicando ambos os lados do resultado acima por 110, tem-se

$$110 = 7(440) + 9(-330).$$

Assim, a solução geral da equação é

$$x = 440 + 9t, \qquad y = -330 - 7t; \qquad sendo \;\; t \in \mathbb{Z}.$$

Entretanto, essa não é a solução final do problema, visto que $x \geq 0$ e $y \geq 0$. Portanto, basta fazer

$$440 + 9t \geq 0 \quad \text{e} \quad -330 - 7t \geq 0.$$

Das inequações implica que t está

$$-48 \leq t \leq -48 \quad ou\ seja \quad t = -48$$

Portanto, quando

$$t = -48 \Longrightarrow \quad x = 8 \quad e \quad y = 6.$$

Logo, a solução é 8 selos de 7 reais e 6 selos de 9 reais.

4 CONGRUÊNCIA

É perceptível que no cotidiano há diversos fenômenos relacionados a ideia de períodos ou ciclos: situações que ocorrem sempre em um mesmo dia, uma vez na semana, têm ciclos de 7 dias; a rotação da Terra em torno do seu próprio eixo tem ciclo de 24 horas e a sua translação em torno do sol tem ciclo de 365 dias e 6 horas; os relógios de ponteiros têm um clico de 12 horas. Diante das situações, conhecendo o período de um dado fenômeno cíclico, nota-se que é possível prever exatamente suas repetições. Essa noção relaciona-se à Teoria das Congruências - uma parte da Aritmética que é fascinante.

A noção de congruência e a sua notação, utilizada até os dias atuais, foi introduzida por Carl Friedrich Gauss, o Príncipe da Matemática, com apenas 24 anos de idade, por meio da obra *Disquisitiones Arithmeticae* (Investigações Aritméticas) em 1801.

Desse modo, as proposições, teoremas, definições, etc. apresentadas neste capítulo podem ser encontrados FILHO 1981, HEFEZ 2016a, LEITÃO 2019, SANTOS 2012, A. d. A. SILVA 2000 e VIEIRA 2020.

4.1 Aritmética Dos Restos

A Teoria das Congruências ou Aritmética dos Restos, ocupa um espaço de destaque na Teoria dos Números. Conforme FRANCO 2016,

> A congruência e a aritmética modular têm muitas aplicações. Dentre elas, a justificativa para os critérios de divisibilidade, exemplificação de conceitos que envolvem as propriedades das operações, construção de códigos e no estudo de modelagem para fenômenos periódicos que envolvem diferentes campos do conhecimento.

Assim, nota-se que as propriedades da Aritmética dos Restos são fortes ferramentas para se estudar divisibilidade sobre $\mathbb{Z}$ com mais profundidade. Desse modo, tem-se que

Definição 4.1.1. *Seja $\boldsymbol{m}$ um número natural. Diz-se que dois números inteiros a e b são congruentes módulo $\boldsymbol{m}$ se os restos de sua divisão euclidiana por $\boldsymbol{m}$ são iguais. Quando os inteiros a e b são congruentes módulo $\boldsymbol{m}$, escreve-se*

$$a \equiv b \ mod \ \mathbf{m}.$$

Exemplo 4.1.1. $8 \equiv 5 \ mod \ \boldsymbol{3}$*, pois os restos da divisão de 8 e de 5 por 3 são iguais a 2.*

Caso o resto das divisões de dois inteiros a e b por $\mathbf{m}$ não forem iguais, diz-se que a e b são incongruentes, ou seja, não são congruentes, módulo $\mathbf{m}$. Nesse caso, escreveremos $a \not\equiv b \ mod \ \mathbf{m}$.

Cabe ressaltar que, como o resto da divisão de um qualquer número inteiro por 1 é sempre nulo, ou seja, $a \equiv b \ mod \ \mathbf{1}$, quaisquer que sejam $a, \ b \in \mathbb{Z}$, fica trivial para aritmética dos restos. Consequentemente, é utilizado $\mathbf{m} > 1$.

A partir da Definição 4.1.1, para verificar se dois números são congruentes módulo $\mathbf{m}$, não é necessário efetuar a divisão euclidiana de ambos por $\mathbf{m}$ para depois comparar seus restos. Basta aplicar o seguinte resultado:

Proposição 4.1.1. *Suponha que $a, \ b, \ \boldsymbol{m} \in \mathbb{Z}$, com $\boldsymbol{m} > 1$. Tem-se que $a \equiv b \ mod \ \boldsymbol{m}$ se, e somente se, $\boldsymbol{m} \mid (b - a)$.*

Demonstração. Sejam $a = \mathbf{m}q_1 + r_1$, com $0 \leq r_1 < \mathbf{m}$ e $b = \mathbf{m}q_2 + r_2$, com $0 \leq r_2 < \mathbf{m}$, as divisões euclidianas de a e b por $\mathbf{m}$, respectivamente. Logo

$$b - a = \begin{cases} \mathbf{m}(q_2 - q_1) \ + \ (r_2 - r_1), & se \quad r_2 \geq r_1 \\ \mathbf{m}(q_2 - q_1) \ + \ (r_1 - r_2), & se \quad r_1 \geq r_2 \end{cases}$$

onde $r_2 - r_1 < \mathbf{m}$ ou $r_1 - r_2 < \mathbf{m}$, ou seja, $|r_1 - r_2| < \mathbf{m}$. Portanto, $a \equiv b \ mod \ \mathbf{m}$, se, e somente se, $r_1 = r_2$ o que é equivalente a dizer que $\mathbf{m} \mid (b - a)$.

Proposição 4.1.2. *Se $a, \ b \in \mathbb{Z}$, então $a \equiv b \ mod \ \boldsymbol{m}$ se, e somente se, existir um inteiro k tal que $a = b + k\boldsymbol{m}$.*

Demonstração. ($\Longrightarrow$) Se $a \equiv b \ mod \ \mathbf{m}$, então $\mathbf{m} \mid (b - a)$. Isso implica na existência de um k inteiro tal que $a - b = k\mathbf{m}$, assim $a = b + k\mathbf{m}$.
($\Longleftarrow$) Se $a = b + k\mathbf{m}$, então $a - b = k\mathbf{m}$, sendo k inteiro, isto é $\mathbf{m} \mid (b - a)$. Logo, $a \equiv b \ mod \ \mathbf{m}$.

Proposição 4.1.3. *Sejam $a, \ b, \ c$ e $\boldsymbol{m} \in \mathbb{Z}$, com $\boldsymbol{m} > 1$, os seguintes itens são verdadeiros:*

1. *$a \equiv a \ mod \ \boldsymbol{m}$;*
2. *$a \equiv b \ mod \ \boldsymbol{m}$ então $b \equiv a \ mod \ \boldsymbol{m}$;*
3. *$a \equiv b \ mod \ \boldsymbol{m}$ e $b \equiv c \ mod \ \boldsymbol{m}$, então $a \equiv c \ mod \ \boldsymbol{m}$*

Demonstração.

(1) Note que $\mathbf{m} \mid (a - a)$, visto que $\mathbf{m} \mid 0$. Isso implica que $a \equiv a \ mod \ \mathbf{m}$.

(2) Se $a \equiv b \ mod \ \mathbf{m}$, então $\mathbf{m} \mid (b - a)$, ou seja, $a = b + k\mathbf{m}$, sendo k inteiro. Assim, $b = a - k\mathbf{m}$, o que implica em $b - a = -k\mathbf{m}$, isto é, $b - a = (-k)\mathbf{m}$, com $b \equiv a \ mod \ \mathbf{m}$. *Proposição* 4.1.2.

(3) Se $a \equiv b \ mod \ \mathbf{m}$, então $a - b = \mathbf{m}k_1$, com k_1 inteiro, assim

$$a = b + \mathbf{m}k_1 \tag{13}$$

e se $b \equiv c \ mod \ \mathbf{m}$, então $b - c = \mathbf{m}k_2$, com k_2 inteiro, e

$$b = c + \mathbf{m}k_2. \tag{14}$$

somando (13) e (14) membro a membro, tem-se:

$$a + b = b + c + (k_1 + k_2)\mathbf{m}.$$

O que implica em $a = c + (k_1 + k_2)\mathbf{m}$, sendo $k_1 + k_2$ inteiro. Portanto, tem-se que $a \equiv c \; mod \; \mathbf{m}$.

Diante dessa última Proposição definida no conjunto dos inteiros, percebe-se que a relação de congruência é também uma relação de equivalência, pois são validas as Propriedades: Reflexiva, Simétrica e Transitiva.

Teorema 4.1.1. *Se a, b, c e $\boldsymbol{m}$ são inteiros, com $\boldsymbol{m} > 0$, tem-se que $a \equiv b \; mod \; \boldsymbol{m}$, então :*

1. $a + c \equiv b + c \; mod \; \mathbf{m}$;
2. $a - c \equiv b - c \; mod \; \mathbf{m}$;
3. $a \cdot c \equiv b \cdot c \; mod \; \mathbf{m}$.

Demonstração.

(1) Como $a \equiv b \; mod \; \mathbf{m}$, tem-se que $a - b = \mathbf{m}k$, com k inteiro. E pode-se escrever $a - b = (a + c) - (b + c)$, assim $(a + c) - (b + c) + \mathbf{m}k$. Desse modo $(a + c) = (b + c) + \mathbf{m}k$, logo $a + c \equiv b + c \; mod \; \mathbf{m}$.

(2) Como $a - b = (a - c) - (b - c)$ e por hipótese $(a - b) = \mathbf{m}k$, tem-se que $(a - c) - (b - c) = \mathbf{m}k$, daí $a - c \equiv b - c \; mod \; \mathbf{m}$.

(3) Como $a - b = \mathbf{m}k$, tem-se $ac - bc = \mathbf{m}kc$, logo $a \cdot c \equiv b \cdot c \; mod \; \mathbf{m}$.

Teorema 4.1.2. *Se a, b, c, d e $\boldsymbol{m}$ são inteiros, tais que $a \equiv b \; mod \; \boldsymbol{m}$ e $c \equiv d \; mod \; \boldsymbol{m}$, então:*

1. $a + c \equiv b + d \; mod \; \mathbf{m}$;
2. $a - c \equiv b - d \; mod \; \mathbf{m}$;
3. $a \cdot c \equiv b \cdot d \; mod \; \mathbf{m}$.

Demonstração.

(1) Se $a \equiv b \; mod \; \mathbf{m}$ e $c \equiv d \; mod \; \mathbf{m}$, então então $a - b = \mathbf{m}k_1$ e $c - d = \mathbf{m}k_2$. Somando ambos os membros tem-se que

$$(a - b) + (c - d) = \mathbf{m}(k_1 + k_2),$$

o que implica em

$$(a + c) + (-b - d) = \mathbf{m}(k_1 + k_2),$$

assim,

$$(a + c) - (b + d) = \mathbf{m}(k_1 + k_2).$$

Isso implica em

$$a + c \equiv b + d \; mod \; \mathbf{m}.$$

(2) Como hipótese $a-b=\mathbf{m}k_1$ e $c-d=\mathbf{m}k_2$, subtraindo ambos os membros, tem-se que

$$(a-b)-(c-d)=\mathbf{m}(k_1-k_2).$$

Isso implica em

$$(a-c)-(b-d)=\mathbf{m}(k_1-k_2).$$

logo

$$a\ -\ c\ \equiv\ b\ -\ d\ mod\ \mathbf{m}.$$

(3) Com a mesma hipótese que $a-b=\mathbf{m}k_1$ e $c-d=\mathbf{m}k_2$, multiplicando ambos os membros por c na primeira igualdade e ambos os membros por b na segunda igualdade, tem-se:

$$ac-bc=\mathbf{m}k_1c \tag{15}$$

e

$$bc-bd=\mathbf{m}k_2b, \tag{16}$$

somando (15) e (16), obtém-se que:

$$ac-bc+bc-bd=\mathbf{m}(k_1c-k_2b),$$

assim,

$$ac-bd=\mathbf{m}(k_1c-k_2b).$$

Portanto,

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

Teorema 4.1.3. *Sejam $a,\ b,\ c$ e $\boldsymbol{m}$ são inteiros, com $\boldsymbol{m}>1$, se $ac\ \equiv\ bc\ mod\ \boldsymbol{m}$, então $a\ \equiv\ b\ mod\ \left(\frac{\boldsymbol{m}}{d}\right)$, onde $d=mdc(c,\ \boldsymbol{m})$.*

Demonstração. De $ac\ \equiv\ bc\ mod\ \mathbf{m}$, tem-se que $ac-bc=\mathbf{m}k$, com k inteiro, o que implica em $c(a-b)=\mathbf{m}k$. Dividindo ambos os membros por d, tem-se:

$$\left(\frac{c}{d}\right)(a-b)=\mathbf{m}\left(\frac{k}{d}\right)\Longrightarrow\left(\frac{c}{d}\right)(a-b)=k\left(\frac{\mathbf{m}}{d}\right).$$

Logo, $\left(\frac{\mathbf{m}}{d}\right)$ divide $\left(\frac{c}{d}\right)(a-b)$. Como $mdc\left(\frac{\mathbf{m}}{d}\ ,\ \frac{c}{d}\right)=1$, tem-se $\left(\frac{\mathbf{m}}{d}\right)$ divide $(a-b)$.

Portanto, $a\ \equiv\ b\ mod\ \left(\frac{\mathbf{m}}{d}\right)$, tem-se $d=mdc(c,\ \mathbf{m})$.

Corolário 4.1.1. *Para todos $n\in\mathbb{N}$, com $a,\ b\in\mathbb{Z}$, se $a\ \equiv\ b\ mod\ \boldsymbol{m}$, então tem-se que*

$$a^n\ \equiv\ b^n\ mod\ \mathbf{m}.$$

Demonstração. A demonstração segue diretamente da identidade:

$$a^n-b^n=(a-b).(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}),$$

como $\mathbf{m}\mid(a-b)$, o que implica em $a-b=\mathbf{m}q$, com q inteiro, $\mathbf{m}\mid(a^n-b^n)$, logo $a^n\ \equiv\ b^n\ mod\ \mathbf{m}$.

Exemplo 4.1.2. *Determine o resto da divisão de* 3^{9999} *por* 5.

Solução: Note que resolver a potência 3^{9999} e depois dividir por 5 é um caminho longo e extremamente difícil. Essa situação fica mais fácil de ser resolvida quando utilizamos congruência, veja:

$$3^2 = 9 \equiv -1 \ mod\ 5.$$

A partir disso, pode-se afirmar que

$$(3^2)^2 \equiv (-1)^2 \ mod\ 5$$
$$3^4 \equiv 1 \ mod\ 5.$$

Elevando ambos os membros da última congruência acima por 2499, tem-se

$$(3^4)^{2499} \equiv 1^{2499} \ mod\ 5$$
$$3^{9996} \equiv 1 \ mod\ 5.$$

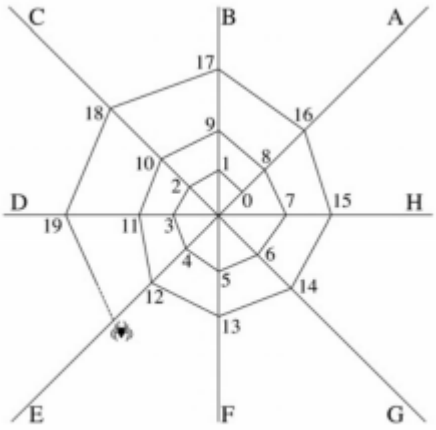
Multiplicando ambos os membros da última congruência acima por 3^3, obtém-se

$$3^{9996} \cdot 3^3 \equiv 1 \cdot 3^3 \equiv 27 \ mod\ 5$$
$$3^{9999} \equiv 2 \ mod\ 5.$$

Logo, o resto da divisão de 3^{9999} por 5 é igual a 2.

Problema 4.1.1. *(OBMEP, 2010) 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 1.*

Figura 1: Teia de aranha



Fonte: Banco de questões OBMEP

A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?
(a) B
(b) D
(c) E
(d) G
(e) H

Solução: Perceba que há mais de uma forma de resolver esse problema. Entretanto, a solução é utilizando congruência. Diante do problema, veja que o número de fios é igual a 8. Portanto, tem-se

$$118 \equiv 6 \ mod \ 8$$

o que significa que dividindo 118 por 8, obtém-se o resto 6. Logo, o número 118 estará no mesmo fio que os números que deixam resto 6 na divisão por 8, portanto, no fio G.

Problema 4.1.2. *(OBMEP, 2019) No Planeta Pemob as semanas têm 5 dias: Aba, Eba, Iba, Oba e Uba, nessa ordem. Os anos são divididos em 6 meses com 27 dias cada um. Se o primeiro dia de um certo ano foi Eba, qual foi o último dia desse ano?*
(a) Aba
(b) Eba
(c) Iba
(d) Oba
(e) Uba

Solução: Perceba que, assim como o problema anterior, há mais de uma forma de resolver essa questão. Entretanto, a solução é utilizando congruência. Note que no planeta Pemob, cada ano tem $6 \cdot 27 = 162$ dias, e cada semana tem 5 dias. Quando efetuamos a divisão de 162 por 2, obtém-se o resto 2. Assim,

$$162 \equiv 2 \ mod \ 5.$$

Visto que o primeiro dia deste ano foi Eba tem-se que o quinto dia é Aba. Assim, se $x \equiv 0 \ mod \ 5$, sabe-se que x é o dia Aba, consequentemente, Eba, é congruente a 1 mod 5; e Iba é congruente a 2 mod 5. Como, $162 \equiv 2 \ mod \ 5$, então o último dia do ano é Iba.

4.2 Critérios de Divisibilidade

A congruência modular é utilizada também para estabelecer critérios de divisibilidade. Os critérios de divisibilidade podem ser considerados como regras que permitem verificar se um número inteiro é divisor de um outro número inteiro, baseando-se em propriedades da sua representação decimal.

Um numéro inteiro $N = n_r n_{r-1} n_{r-2} \cdots n_2 n_1 n_0$ pode ser escrito na base decimal como:

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

em que os números $n_i \in \{0, \cdots, 9\}$ são chamados de dígitos de N. Esse resultado é em decorrência do algoritmo de Euclides.

Desse modo, serão utilizados os conceitos e propriedades das congruências para definir alguns critérios de divisibilidade.

4.2.1 Divisibilidade por 2

Utilizando a noção de congruência, note que

$$10 \equiv 0 \ mod \ 2,$$

segue-se do item 3 do **Teorema 4.1.1.** que

$$10^i \cdot n_i \equiv 0 \ mod \ 2,$$

para algum $i \geq 1$. Portanto,

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

$$N = 10 \cdot (n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^1 + n_1 \cdot 10^0) + n_0$$

$$N = 10 \cdot (n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^1 + n_1 \cdot 10^0) + n_0 \equiv \ 0 \ mod \ 2,$$

assim,

$$N \equiv \ n_0 \ mod \ 2,$$

logo N é divisível por 2 se, e somente se, n_0 é divisível por 2, ou seja, se n_0 for par.

Exemplo 4.2.1.1. *Verifique se o número* 3794 *é divisível por* 2.

Solução: Note que

$$3794 = 3 \cdot 10^3 + 7 \cdot 10^2 + 9 \cdot 10^1 + 4 \equiv 0 + 0 + 0 + 4 \equiv 4 \ mod \ 2,$$

como $4 \equiv 0 \ mod \ 2$, por transitividade $3794 \equiv 0 \ mod \ 2$. O que implica que o número 3794 é divisível por 2.

Exemplo 4.2.1.2. *Aplicações do critério de divisibilidade por 2:*

1. *O resto da divisão do número* 234.567.891 *por* 2 *é* 1.
2. *O resto de* 2024 *por* 2 *é* 0.

4.2.2 Divisibilidade por 3

Utilizando a noção de congruência, note que

$$10 \equiv 1 \ mod \ 3,$$

segue-se do item 3 do **Teorema 4.1.1.**, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \ mod \ 3$, da mesma forma, $10^3 \equiv 10 \cdot 10 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \ mod \ 3$, o que implica em

$$10^i \equiv 1 \ mod \ 3$$

para $i \geq 1$.

Isso mostra que se,

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

então, $N \equiv (n_r + n_{r-1} + n_{r-2} + \cdots n_2 + n_1 + n_0)\ mod\ 3$. Um número inteiro N é divisível por 3 quando a soma de seus algarismos é divisível por 3

Exemplo 4.2.2.1. *Verifique se o número* 456789 *é divisível por* 3*:*

Solução: Note que

$$456789 = 4 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 9 \equiv 4 + 5 + 6 + 7 + 8 + 9 = 39\ mod\ 3,$$

como $39 \equiv 0\ mod\ 3$, por transitividade $456789 \equiv 0\ mod\ 3$. O implica que o número 456789 é divisível por 3.

4.2.3 Divisibilidade por 4

Utilizando a noção de congruência, note que

$$10 \equiv 2\ mod\ 4,$$

segue-se do item 3 do **Teorema 4.1.1.**, $10^2 \equiv 2^2 \equiv 0 \cdot 1\ mod\ 4$, da mesma forma, $10^3 \equiv 2^3 \equiv 1 \cdot 0 \cdot 1\ mod\ 4$, o que implica em

$$10^i \equiv 0\ mod\ 4$$

para $i \geq 2$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

então

$$N \equiv 0 + 0 + 0 + \cdots + 10^1 \cdot n_1 + n_0\ mod\ 4.$$

Logo, N é divisível por 4 se, e somente se, $10^1 \cdot n_1 + n_0$, ou seja, $n_1 n_0$ é divisível por 4. Um número inteiro N é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4, ou seja, $N \equiv (2n_1 + n_0)\ mod\ 4$.

Exemplo 4.2.3.1. *Verifique se o número* 456784 *é divisível por* 4*:*

Solução: Note que

$$456784 = 4 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 4 \equiv 0 + 0 + 0 + 0 + 10 \cdot 8 + 4 = 84\ mod\ 4,$$

como $84 \equiv 0\ mod\ 4$, por transitividade $456784 \equiv 0\ mod\ 4$. O implica que o número 456784 é divisível por 4.

4.2.4 Divisibilidade por 5

Utilizando a noção de congruência, note que

$$10 \equiv 0\ mod\ 5,$$

segue-se do item 3 do **Teorema 4.1.1**, o que implica em

$$10^i \equiv 0 \ mod \ 5$$

para $i \geq 1$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

então

$$N \equiv 0 + 0 + 0 + \cdots + n_0 \ mod \ 5.$$

Logo, N é divisível por 5 se, e somente se, n_0 é divisível por 5, ou seja, se n_0 for 0 ou 5.

Exemplo 4.2.4.1 *Verifique se o número* 3670 *é divisível por* 5*:*

Solução: Note que

$$3670 = 3 \cdot 10^3 + 6 \cdot 10^2 + 6 \cdot 10^1 + 0 \equiv 0 + 0 + 0 + 0 \equiv 0 \ mod \ 5,$$

como $0 \equiv 0 \ mod \ 5$, por transitividade $3670 \equiv 0 \ mod \ 5$. O que implica que o número 3670 é divisível por 5.

4.2.5 Divisibilidade por 6

Utilizando a noção de congruência, note que

$$10 \equiv 4 \ mod \ 6,$$

segue-se do item 3 do **Teorema 4.1.1.**, $10^2 \equiv 4^2 \equiv 4 \ mod \ 6$, da mesma forma, $10^3 \equiv 4^3 \equiv 4 \ mod \ 6$, o que implica em

$$10^i \equiv 4^i \equiv 4 \ mod \ 6$$

para $i \geq 1$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0$$

então

$$N \equiv 4 \cdot (n_r + \cdots + n_2 + n_1) + n_0 \ mod \ 6.$$

Portanto, $6 \mid N$ se, e somente se, $4 \cdot (n_r + \cdots + n_2 + n_1) + n_0 \equiv 0 \ mod \ 6$. Ou seja, pode-se dizer que um número inteiro N é divisível por 6 quando a soma do algarismo da unidade com o quádruplo de cada um dos outros algarismos é divisível por 6.

Ainda mais, um número inteiro N é divisível por 6 quando é divisível por 2 e 3 simultaneamente. Uma justificativa desse critério vem do Teorema Fundamental da Aritmética, pois a partir dele obtém-se a decomposição em fatores primos do 6, que $6 = 2 \cdot 3$.

Exemplo 4.2.5.1 *Verifique se o número* 489324 *é divisível por* 6*:*

Solução: Note que

$489324 = 4\cdot 10^5+8\cdot 10^4+9\cdot 10^3+3\cdot 10^2+2\cdot 10^1+4 \equiv 4\cdot(4+8+9+3+2)+4 = 108\ mod\ 6,$

como $108 \equiv 0\ mod\ 6$, por transitividade $489324 \equiv 0\ mod\ 6$. O que implica que o número 489324 é divisível por 6.

4.2.6 Divisibilidade por 7

Note que

$$N = n_r \cdot 10^{r-1} + n_{r-1} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^1 + n_1 \equiv 2 \cdot n_0\ mod\ 7.$$

Com efeito,

$$n_r n_{r-1} \cdots n_1 n_0 = 10(n_r n_{r-1} \cdots n_1) + n_0.$$

Suponha que

$$n_r n_{r-1} \cdots n_1 - 2n_0 = 7k,$$

para algum $k \in \mathbb{N}$. Então

$$n_r n_{r-1} \cdots n_1 = 7k + 2n_0.$$

Como

$$n_r n_{r-1} \cdots n_1 n_0 = 10(n_r n_{r-1} \cdots n_1) + n_0 \quad e \quad n_r n_{r-1} \cdots n_1 = 7k + 2n_0$$

isso implica que

$n_r n_{r-1} \cdots n_1 n_0 = 10(n_r n_{r-1} \cdots n_1) + n_0 = 10(7k+2n_0) + n_0 = 70k + 21n_0 = 7(10k+3n_0),$

que é divisível por 7.

Por outro lado, suponha que N seja divisível por 7, logo $N = n_r n_{r-1} \cdots n_1 n_0 = 7k_1$, com $k_1 \in \mathbb{Z}$. Se $n_r n_{r-1} \cdots n_1 - 2n_0 = t$, com $t \in \mathbb{Z}$, então $n_r n_{r-1} \cdots n_1 = t + 2n_0$. Assim,

$$n_r n_{r-1} \cdots n_1 n_0 = 10(n_r n_{r-1} \cdots n_1) + n_0 = 10(t + 2n_0) + n_0 = 10t + 21n_0.$$

Como $n_r n_{r-1} \cdots n_1 n_0$ é divisível por 7, tem-se que $10t + 21n_0$ também divisível por 7. Mas isso só é válido se $t = 7k_2$, com $k_2 \in \mathbb{Z}$

Portanto, $n_r n_{r-1} \cdots n_1 - 2n_0$ é divisível por 7. Ou seja, um número $N = n_r n_{r-1} n_{r-2} \cdots n_2 n_1 n_0$ é divisível por 7 se, e somente se, o número que não contém o último algarismo de N, isto é $(n_r \cdots n_2 n_1)$, subtraído do dobro do último algarismo n_0 de N for divisível por 7. Se o número obtido for grande, repita o processo até que seja possível verificar a divisão por 7.

Exemplo 4.2.6.1 *Verifique se o número* 336 *é divisível por* 7*:*

Solução: Note que

$$336 \equiv 33 - 2 \cdot 6 = 21\ mod\ 7,$$

como $21 \equiv 0\ mod\ 7$, por transitividade $336 \equiv 0\ mod\ 7$. O que implica que o número 336 é divisível por 7.

4.2.7 Divisibilidade por 8

Utilizando a noção de congruência, note que

$$10 \equiv 2 \ mod \ 8,$$

segue-se do item 3 do **Teorema 4.1.1**, $10^3 \equiv 2^3 \equiv 0 \ mod \ 8$, o que implica em

$$10^i \equiv 0 \ mod \ 8$$

para $i \geq 3$.

Isso mostra que se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

então

$$N \equiv 0 + 0 + 0 + \cdots + 0 + n_2 n_1 n_0 \ mod \ 8.$$

Logo, N é divisível por 8 se, e somente se, $10^2 \cdot n_2 + 10^1 \cdot n_1 + n_0$, ou seja, $n_2 n_1 n_0$ é divisível por 8. Assim, um número inteiro N é divisível por 8 se, e somente se, quando termina em 000 ou quando os três algarismos da direita for divisível por 8.

Exemplo 4.2.7.1 *Verifique se o número* 456784 *é divisível por* 8*:*

Solução: Note que

$$456784 = 4 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 4 \equiv 0 + 0 + 0 + 10^2 \cdot 7 + 10 \cdot 8 + 4 = 784 \ mod \ 8,$$

como $784 \equiv 0 \ mod \ 8$, por transitividade $456784 \equiv 0 \ mod \ 8$. O que implica que o número 456784 é divisível por 8.

4.2.8 Divisibilidade por 9

Utilizando a noção de congruência, note que

$$10 \equiv 1 \ mod \ 9,$$

segue-se do item 3 do **Teorema 4.1.1**, $10^2 \equiv 10 \cdot 10 \equiv 1 \cdot 1 \ mod \ 9$, da mesma forma, $10^3 \equiv 10 \cdot 10 \cdot 10 \equiv 1 \cdot 1 \cdot 1 \ mod \ 9$, o que implica em

$$10^i \equiv 1 \ mod \ 9$$

para $i \geq 1$.

Isso mostra que, se

$$N = n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + n_{r-2} \cdot 10^{r-2} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0,$$

então

$$N \equiv (n_r + n_{r-1} + n_{r-2} + \cdots n_2 + n_1 + n_0) \ mod \ 9.$$

Logo, um número inteiro N é divisível por 9 quando a soma de seus algarismos é divisível por 9.

Exemplo 4.2.8.1 *Verifique se o número* 456789 *é divisível por* 9*:*

Solução: Note que

$456789 = 4 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10^1 + 9 \equiv 4 + 5 + 6 + 7 + 8 + 9 = 39 \ mod\ 9,$

como $39 \not\equiv 0 \ mod\ 9$, por transitividade $456789 \not\equiv 0 \ mod\ 9$. O que implica que o número 456789 não é divisível por 9.

4.2.9 Divisibilidade por 11

Utilizando a noção de congruência, note que

$$10 \equiv (-1) \ mod\ 11$$
$$10^2 \equiv (-1) \cdot (-1) \equiv 1 \ mod\ 11$$
$$10^3 \equiv (-1) \cdot (-1) \cdot (-1) \equiv (-1) \ mod\ 11,$$

assim, $10^{2i} \equiv 1 \ mod\ 11$ e $10^{2i+1} \equiv (-1) \ mod\ 11$, com $i = 0, 1, 2, \cdots, r$. Portanto, dado um número $N = n_r n_{r-1} \cdots n_0$, n base 10, tem-se que:

$$n_0 \equiv n_0 \ mod\ 11$$
$$n_1 \cdot 10 \equiv -n_1 \ mod\ 11$$
$$n_2 \cdot 10^2 \equiv n_2 \ mod\ 11$$
$$n_3 \cdot 10^3 \equiv -n_3 \ mod\ 11$$
$$n_4 \cdot 10^4 \equiv n_4 \ mod\ 11$$
$$\vdots$$
$$n_r \cdot 10^r \equiv (-1)^r n_r \ mod\ 11.$$

Somando membro a membro as congruências acima, tem-se:

$n_r \cdot 10^r + n_{r-1} \cdot 10^{r-1} + \cdots + n_1 \cdot 10^1 + n_0 \cdot 10^0 \equiv n_0 - n_1 + n_2 - n_3 + \cdots + (-1)^r \cdot n_r \ mod\ 11,$

assim

$$N \equiv n_0 - n_1 + n_2 - n_3 + \cdots + (-1)^r \cdot n_r \ mod\ 11.$$

Portanto, N é divisível por 11 se, e somente se, $n_0 - n_1 + n_2 - n_3 + \cdots + (-1)^r \cdot n_r$ é divisível por 11. Ou seja, um número inteiro N é divisível por 11 se, e somente se, quando a diferença não negativa entre a soma dos algarismo de ordem ímpar (I) e a soma dos algarismo de ordem par (P) for um número divisível por 11.

Exemplo 4.2.9.1. *Verifique se o número* 856589 *é divisível por* 11*:*

Solução: Note que

$$856589 = 8 \cdot 10^5 + 5 \cdot 10^4 + 6 \cdot 8 - 5 + 6 - 5 + 8 - 9 = 3 \ mod\ 11,$$

como $3 \not\equiv 0 \ mod\ 11$, por transitividade $856589 \not\equiv 0 \ mod\ 11$. O que implica que o número 856589 não é divisível por 11.

Observação 4.1.1 *Os críterios de divisibilidade a seguir são na forma não mnemônica.*

4.2.10 Divisibilidade por 13

Dado um $a = (n_r \cdots n_1 n_0)$, considere $k = n_r \cdots n_2 n_1$. Sendo 13 um primo na forma aditiva $k + 4n_0$ ou na forma subtrativa $k - 9n_0$ é divisível por p, se $k + n_0$ é múltiplo de p.

Exemplo 4.2.10.1 *Verifique se o número* 52819 *é divisível por* 13*:*

Solução: Utilizando $k + 4n_0$, tem-se que

$$5281 \quad e \quad 4 \cdot 9 = 36,$$

somando $5281 + 36 = 5317$, analogamente, tem-se que

$$531 \quad e \quad 4 \cdot 7 = 28,$$

somando $531 + 28 = 559$, do mesmo modo, tem-se que

$$55 \quad e \quad 4 \cdot 9 = 36,$$

somando $55 + 36 = 91$, de forma análoga, tem-se que

$$9 \quad e \quad 4 \cdot 1 = 4,$$

somando $9 + 4 = 13$, como 91 é múltiplo de 13, conclui-se que 52819 é divisível por 13.

4.2.11 Divisibilidade por 17

Dado um $a = (n_r \cdots n_1 n_0)$, considere $k = n_r \cdots n_2 n_1$. Sendo 17 um primo na forma aditiva $k + 12n_0$ ou na forma subtrativa $k - 5n_0$ é divisível por p, se $k + n_0$ é múltiplo de p.

Exemplo 4.2.11.1 *Verifique se o número* 23715 *é divisível por* 17*:*

Solução: Utilizando $k + 12n_0$, tem-se que

$$2371 \quad e \quad 12 \cdot 5 = 60,$$

somando $2371 + 60 = 2431$, analogamente, tem-se que

$$243 \quad e \quad 12 \cdot 1 = 12,$$

somando $243 + 12 = 255$, do mesmo modo, tem-se que

$$25 \quad e \quad 12 \cdot 5 = 60,$$

somando $25 + 60 = 85$, de forma análoga, tem-se que

$$8 \quad e \quad 12 \cdot 5 = 60,$$

somando $8 + 60 = 68$, como 68 é múltiplo de 17, conclui-se que 23715 é divisível por 17.

4.2.12 Divisibilidade por 19

Dado um $a = (n_r \cdots n_1 n_0)$, considere $k = n_r \cdots n_2 n_1$. Sendo 19 um primo na forma aditiva $k + 2n_0$ ou na forma subtrativa $k - 17n_0$ é divisível por p, se $k + n_0$ é múltiplo de p.

Exemplo 4.2.12.1 *Verifique se o número* 420945 *é divisível por* 19*:*

Solução: Utilizando $k + 2n_0$, tem-se que

$$42094 \quad e \quad 2 \cdot 5 = 10,$$

somando $42094 + 10 = 42104$, analogamente, tem-se que

$$4210 \quad e \quad 2 \cdot 4 = 8,$$

somando $4210 + 8 = 4218$, do mesmo modo, tem-se que

$$421 \quad e \quad 2 \cdot 8 = 16,$$

somando $421 + 16 = 437$, de forma análoga, tem-se que

$$43 \quad e \quad 2 \cdot 7 = 14,$$

somando $43 + 14 = 57$, do mesmo modo, tem-se que

$$5 \quad e \quad 2 \cdot 7 = 14,$$

somando $5 + 14 = 19$, como 57 é múltiplo de 19, conclui-se que 420945 é divisível por 19.

4.3 Dígito Verificador

O mundo da informação é vasto e complexo, e garantir a precisão dos dados é crucial para diversos setores. A aritmética modular colabora garantindo o dígito verificador no intuito de combater erros e garantir a confiabilidade em sistemas como códigos de barras, documentos de identidade, códigos ISBN, números de contas bancárias, cartões e outros.

4.3.1 CPF

O Cadastro de Pessoa Física (CPF) é um conjunto de números que serve para identificação de uma pessoa. O cadrasto possui 11 dígitos, dos quais o nono dígito identifica o estado brasileito de emissão da pessoa conforme a Tabela I, já os dois ultimos dígitos são os verificadores.

Tabela I - Dígito Identificador

Estado Emissor	**Dígito**
DF, GO, MS, MT e TO	1
AC, AM, AP, PA, RO e RR	2
CE, MA e PI	3
AL, PB, PE e RN	4
BA e SE	5
MG	6
ES e RJ	7
SP	8
PR e SC	9
RS	0

Os dois últimos números são dígitos verificadores (ou de controle), sendo essa mais uma aplicação de congruência, que utiliza congruência módulo 11, operando com os nove primeiros algarismos:

$$c = [\ a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ ]$$

e esses algarismos ficam sendo multiplicados, conforme a ordem dada no documento, pela primeira matriz de pesos pré-estabelecida em CPF's por:

$$p = [\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ].$$

Assim, é feito o produto matricial entre c e p^t, dando uma soma (S) e a congruência usada é:

$$S - a_{10} \equiv 0\ mod\ 11,$$

$$a_{10} \equiv S\ mod\ 11 \qquad ou \qquad S \equiv a_{10}\ mod\ 11.$$

Para encontrar o segundo dígito verificador o mesmo processo é realizado, todavia acrescentando a_{10} em c e a matriz p passa a ser:

$$p = [\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ].$$

Em outras palavras, o decimo dígito, ou primeiro verificador é calculado assim: multiplica-se o primeiro número por 1, o segundo por 2, o terceiro por 3, até o nono que deve ser multiplicado por 9. Soma-se os resultados obtidos e calcula-se o resto da divisão por 11, tal resto será o primeiro dígito de controle, exceto se tal resto for 10, situação em que o dígito será 0. Para o segundo dígito de controle multiplica-se o segundo número por 1, o terceiro por 2, o quarto por 3 até o décimo número que deve ser multiplicado por 9, soma-se os resultados obtidos e divide-se por 11, o segundo dígito de controle é o resto dessa divisão. Como antes, se tal resto for 10, o dígito verificador será 0.

Exemplo 4.3.1.1 *Encontre os dígitos verificadores do CPF fictício dado por*: **515.253.545-**$a_{10}a_{11}$.

Solução: Para encontrar o primeiro dígito, faz-se o produto das matrizes:

$$c_1 = [\ 5\ 1\ 5\ 2\ 5\ 3\ 5\ 4\ 5\ ] \text{ e } p_1 = [\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ],$$

assim, obtém-se a soma (S) em cada caso:

$$S_1 = 5 \cdot 1 + 1 \cdot 2 + 5 \cdot 3 + 2 \cdot 4 + 5 \cdot 5 + 3 \cdot 6 + 5 \cdot 7 + 4 \cdot 8 + 5 \cdot 9$$

$$S_1 = 5 + 2 + 15 + 8 + 25 + 18 + 35 + 32 + 45$$

$$S_1 = 5 + 2 + 15 + 8 + 25 + 18 + 35 + 32 + 45$$

$$S_1 = 185.$$

Logo,

$$S_1 - a_{10} \equiv 0 \ mod \ 11$$

$$185 - a_{10} \equiv 0 \ mod \ 11.$$

Portanto, a_{10} é igual a 9.

Agora, para calcular o último dígito, toma-se

$c_2 = [\ 5\ 1\ 5\ 2\ 5\ 3\ 5\ 4\ 5\ 9\ ]$ e $p_1 = [0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ ]$.

Assim, encontra-se a outra soma:

$$S_2 = 5 \cdot 0 + 1 \cdot 1 + 5 \cdot 2 + 2 \cdot 3 + 5 \cdot 4 + 3 \cdot 5 + 5 \cdot 6 + 4 \cdot 7 + 5 \cdot 8 + 9 \cdot 9$$

$$S_2 = 0 + 1 + 10 + 6 + 20 + 15 + 30 + 28 + 40 + 81$$

$$S_2 = 231.$$

Mas, como

$$S_2 - a_{11} \equiv 0 \ mod \ 11,$$

tem-se que

$$231 - a_{11} \equiv 0 \ mod \ 11.$$

Logo, $a_{11} = 0$, e o CPF será **515.253.545-90**.

4.3.2 Cartões de crédito

A ideia de o cartão de crédito surgiu com Frank MacNamara, porém funcionava como um cartão de compra. Essa ideia chegou no Brasil por volta de 1956 por "Diners". Alguns anos depois, em 1968, foi lançando o primeiro cartão de crédito de banco o "Credicard".

Os cartões de crédito predominantes no mundo possuem de 14 a 19 dígitos. No Brasil, possuem 16 dígitos, sendo que os primeiros quatro dígitos definem o banco emissor, e do quinto ao décimo quinto dígito determinam os dados do cliente, enquanto o último dígito será o dígito verificador, o qual é obtido dos anteriores por meio de congruência módulo 10.

Para encontrar o dígito verificador, consideraremos um cartão de crédito que possuem uma sequência numérica de 16 dígitos e que é expressado matematicamente por:

$$a_1a_2a_3a_4 \cdot a_5a_6a_7a_8 \cdot a_9a_{10}a_{11}a_{12} \cdot a_{13}a_{14}a_{15}a_{16}.$$

Para determinar o DV a_{16} deve-se primeiro tomar os dígitos com índice ímpares e calcular o x_i, sendo que

$$x_i = \begin{cases} 2a_i & se \quad 2a_i \leq 9 \\ 2a_i - 9 & se \quad 2a_i > 9, \end{cases}$$

com $a_i \in \mathbb{Z}$, $0 \leq a_i \leq 9$ e $i \in \{1, 2, 3, ..., 16\}$. Agora, calcula-se a soma S pelo somatório desses x_i com o somatório dos a_i de índice par, dado por:

$$S = \sum_{i=1}^{8} x_{2i-1} + \sum_{i=1}^{8} a_{2i},$$

e o dígito verificador a_{16} advem da seguinte congruência:

$$a_{16} \equiv -S \ mod \ 10.$$

Exemplo 4.3.2.1 *Suponha que o número* $7435.1013.1117.525a_{16}$ *seja de um cartão de crédito. Determine o dígito verificador desse cartão.*

Solução: Encontrando os x_i:

$$x_1 = 2a_1 = 2 \cdot 7 = 14 > 9 \Longrightarrow x_1 = 2a_1 - 9 \Longrightarrow x_1 = 5$$
$$x_3 = 2a_3 = 2 \cdot 3 = 6 \leq 9 \Longrightarrow x_3 = 6$$
$$x_5 = 2a_5 = 2 \cdot 1 = 2 \leq 9 \Longrightarrow x_5 = 2$$
$$x_7 = 2a_7 = 2 \cdot 1 = 2 \leq 9 \Longrightarrow x_7 = 2$$
$$x_9 = 2a_9 = 2 \cdot 1 = 2 \leq 9 \Longrightarrow x_9 = 2$$
$$x_{11} = 2a_{11} = 2 \cdot 1 = 2 \leq 9 \Longrightarrow x_{11} = 2$$
$$x_{13} = 2a_{13} = 2 \cdot 5 = 10 > 9 \Longrightarrow x_{13} = 2a_{13} - 9 \Longrightarrow x_{13} = 1$$
$$x_{15} = 2a_{15} = 2 \cdot 5 = 10 > 9 \Longrightarrow x_{15} = 2a_{15} - 9 \Longrightarrow x_{15} = 1.$$

Aplicando o algoritmo, tem-se

$$S = \sum_{i=1}^{8} x_{2i-1} + \sum_{i=1}^{8} a_{2i},$$

$$S = (5+6+2+2+2+2+1+1) + (4+5+0+3+1+7+2)$$

$$S = 33.$$

Logo, usando a congruência

$$a_{16} \equiv -S \ mod\ 10$$

$$a_{16} \equiv -33 \ mod\ 10$$

$$a_{16} \equiv -3 \ mod\ 10$$

$$a_{16} \equiv 7 \ mod\ 10.$$

Portanto, o dígito verificador $a_{16} = 7$, o que implica que o número do cartão de crédito será 7435.1013.1117.525**7**.

4.4 Calendário

O registro do passar do tempo foi objeto de preopucação do homem há centenas de anos. Atualmente, utilizam-se considerações astronômicas para propor definições ao passar do dia e ano, por exemplo. Contudo, as noções de semana e mês variam da cultura de cada povo.

Nessa perspectiva de contar o passar do tempo, desenvolveu-se o calendário, que é um sistema de contagem e agrupamento de dias, que visa atender principalmente às necessidades civis e religiosas de uma cultura, organizadas com o propósito de medir e registrar eventos ao longo de "grandes períodos". Existem aproximadamente 40 calendários em uso no mundo, os quais podem ser classificados em:

- **Solares:** baseados no movimento da terra em torno do sol e considerando que os meses não têm conexão com o movimento da lua. Um exemplo é o Calendário Gregoriano.
- **Lunares:** fundamentados no movimento da lua, considerando que o ano não tem conexão com o movimento da Terra em torno do sol. Um exemplo é o Calendário Islâmico.
- **Lunisolares:** os anos estão relacionados com o movimento da terra em torno do sol e os meses com o movimento da lua em torno da terra. Um exemplo é o Calendário Hebreu.

No Brasil e no Ocidente é utilizado o Calendário Gregoriano, derivado do Solar. Os meses desse calendário são constituídos por 30 ou 31 dias, exceto fevereiro que possui 29 dias nos anos bissextos e 28 nos demais. Observa-se que há 97 anos de 366 dias (anos bissextos) em cada período de 400 anos. Isso advém da seguinte regra:

- Todo ano divisível por 4 é um ano bissexto.

- Entretanto, todo ano divisível por 100 não é um ano bissexto.
- Entretanto, todo ano divisível por 400 é um ano bissexto sempre.

Logo, por exemplo, 1700, 1800, 1900, 2100 e 2200 não são anos bissextos. Porém, 1600, 2000 e 2400 são anos bissextos.

Quando se trata de calendário, nota-se que há um grande enredo matemático por trás. O calendário possui alguns elementos arbitrários onde podemos usar algoritmos com operações básicas de matemática para relacionar uma data estabelecida ao dia da semana em que ela se deu (OLIVEIRA, 2015 apud. FRANCO 2016FRANCO, 2016 p.71). Utilizando congruência modulo m no calendário, referente ao mês de julho de 2024 conforme a Figura 3, observa-se que

Figura 3 - Calendário

Fonte: https://br.pinterest.com/pin/633318766377340108/. Acesso em 03/02/2024.

analisando a disposição dos dias nessse mês, considerando $\mathbf{m} = 7$, teremos

$$Domingo: \quad n \equiv 0 \ mod \ \mathbf{7};$$

$$Segunda: \quad n \equiv 1 \ mod \ \mathbf{7};$$

$$Terca: \quad n \equiv 2 \ mod \ \mathbf{7};$$

$$Quarta: \quad n \equiv 3 \ mod \ \mathbf{7};$$

$$Quinta: \quad n \equiv 4 \ mod \ \mathbf{7};$$

$$Sexta: \quad n \equiv 5 \ mod \ \mathbf{7};$$

$$Sabado: \quad n \equiv 6 \ mod \ \mathbf{7}.$$

Para determinar, por exemplo, qual dia da semana seria 30 de julho de 2024, bastaria apenas saber a que classe de congruência que esse dia pertenceria em módulo 7. Dessa forma, dividindo 30 por 7. resulta em um quociente 4 e resto 2. Assim, $30 \equiv 2 \ mod \ 7$, ou seja, sabe-se que segunda-feira é a data inicial do mês, dia 1, a classe de restos 2 pertence nesse sentindo às terças-feiras. Portanto, dia 30 de julho de 2024 é terça-feira (mostrado na Figura 3).

Exemplo *O ano de* 2005 *começou em um sábado. Qual o dia da semana termina esse ano?*

Solução: De modo inicial deve-se observar que o rescpectivo ano possui 365 dias, organizados de 7 em 7 dias formam 52 ciclos semanais completos e sobra um dia. Sendo que cada dia inicia no sábado e termina na sexta-feira, porém deve-se acrescentar 1 dia ao próximo ciclo. Dessa forma, o último dia também será em um sábado. Pois,

$$365 \equiv\ x\ mod\ 7,$$

e

$$365 \equiv\ 1\ mod\ 7.$$

Observação: Generalizando, exceto os anos bissextos, todos os anos iniciam e terminam no mesmo dia da semana.

4.5 Congruências Lineares

Definição 4.5.1 *Sejam a e b inteiros quaisquer e* $\boldsymbol{m}$ *um inteiro positivo, define–se congruência linear toda equação da forma:*

$$ax\ \equiv\ b\ mod\ \mathbf{m}. \tag{17}$$

Para todo inteiro x_0 que satisfaz a equação (17) tal que

$$ax_0\ \equiv\ b\ mod\ \mathbf{m},$$

diz–se que x_0 é uma solução para a congruência linear.

Note que o inteiro x_0 é uma solução particular da congruência linear

$$ax\ \equiv\ b\ mod\ \mathbf{m},$$

então para todo x tal que $x\ \equiv\ x_0\ mod\ \mathbf{m}$ podemos construir uma infinidade de outras soluções, todas mutuamente congruentes módulo $\mathbf{m}$.

Proposição 4.5.1 *Dados a, b e* $\boldsymbol{m} \in \mathbb{Z}$*, com* $\boldsymbol{m}$*>0, a congruência*

$$ax\ \equiv\ b\ mod\ \mathbf{m}$$

possui solução se, e somente se, $mdc(a,\ \boldsymbol{m}) \mid b$.

Demonstração. ($\Longrightarrow$) Suponha que a congruência linear adimita solução e seja o inteiro x_0 sua soluçao, logo

$$ax_0\ \equiv\ b\ mod\ \mathbf{m} \quad \Longrightarrow \quad ax_0 - b = \mathbf{m}y_0 \quad \Longrightarrow \quad ax_0 - \mathbf{m}y_0 = b.$$

Daí, existe um $mdc(a,\ \mathbf{m})$ tal que $mdc(a,\ \mathbf{m}) \mid a$ e $mdc(a,\ \mathbf{m}) \mid \mathbf{m}$>. Desse modo, segue que $mdc(a,\ \mathbf{m}) \mid (ax_0 - \mathbf{m}y_0)$ e logo $mdc(a,\ \mathbf{m}) \mid b$.
($\Longleftarrow$) Se $mdc(a,\ \mathbf{m}) \mid b$ então $mdc(a,\ \mathbf{m}) \mid (ax_0 - \mathbf{m}y_0)$ o que implica em

$$ax_0 - \mathbf{m}y_0 = mdc(a,\ \mathbf{m}). \tag{18}$$

Multiplicando ambos os membros a expressão (18) por k, tem-se:

$$ax_0 \cdot k - \mathbf{m}y_0 \cdot k = [mdc(a,\ \mathbf{m})] \cdot k.$$

Fazendo $[mdc(a,\ \mathbf{m})] \cdot k = b$, tem-se

$$a(x_0 \cdot k) - \mathbf{m}(y_0 \cdot k) = b \quad \Longrightarrow \quad a(x_0 \cdot k) - b = \mathbf{m}(y_0 \cdot k) \quad \Longrightarrow \quad a(x_0 \cdot k) \ \equiv \ b \ mod \ \mathbf{m}$$

Logo, o inteiro $(k \cdot x_0)$ é uma solução da congruência linear: $ax \ \equiv \ b \ mod \ \mathbf{m}$

Teorema 4.5.1 *Sejam a, b e* $\boldsymbol{m} \in \mathbb{Z}$*, com* $\boldsymbol{m}$*>1 e* $mdc(a,\ \boldsymbol{m}) \mid b$*.. Se* x_0 *é solução da congruência* $ax \ \equiv \ b \ mod \ \boldsymbol{m}$*, então*

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \cdots ,\ \ x_0 + (d-1)\frac{m}{d},$$

onde $d \ = \ mdc(a,\ \boldsymbol{m})$*, formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo* $\boldsymbol{m}$*.*

Demonstração. Toda solução x da congruência $ax \ \equiv \ b \ mod \ \mathbf{m}$ é congruente , módulo $\mathbf{m}$, a $x_0 + i \cdot \frac{\mathbf{m}}{d}$ para algum $0 \leq i < d$ e

$$ax \ \equiv \ ax_0 \ mod \ \mathbf{m}$$

e, pelo **Teorema 4.1.3.** $[ac \ \equiv \ bc \ mod \ \mathbf{m} \iff a \ \equiv \ b \ mod \ \left(\frac{\mathbf{m}}{d}\right);\ d = mdc(c,\ \mathbf{m})]$ tem-se que

$$x \ \equiv \ x_0 \ mod \ \frac{\mathbf{m}}{d}.$$

Logo, $x - x_0 = \dfrac{km}{d} \Rightarrow \ k = \dfrac{d(x - x_0)}{m}$, sendo $k \in \mathbb{Z}$. Pela divisão euclidiana, existe $0 \leq i < d$ tal que $k = qd + i$ e, assim

$$\frac{d(x - x_0)}{m} = qd + i \quad \Longrightarrow \quad x - x_0 = qm + i \cdot \frac{m}{d} \quad \Longrightarrow \quad x - \left(x_0 - i \cdot \frac{m}{d}\right) = qm.$$

Portanto,

$$x = x_0 + qm + i\frac{m}{d} \equiv x_0 + i \cdot \frac{m}{d} \ mod \ m.$$

Reciprocamente, os números $\left(x_0 + i \cdot \dfrac{m}{d}\right)$, com $0 \leq i < d$, são soluções da congruência, pois

$$a \cdot \left(x_0 + i \cdot \frac{m}{d}\right) = ax_0 + i \cdot \frac{a}{d}m \equiv ax_0 \equiv b \ mod \ m.$$

Finalmente, esses números são dois a dois incongruentes módulo m, pois se, para $0 \leq i < d$,

$$x_0 + i \cdot \frac{m}{d} \equiv x_0 + j \cdot \frac{m}{d} \ mod \ m,$$

então

$$i \cdot \frac{m}{d} \equiv j \cdot \frac{m}{d} \ mod \ m.$$

Como, $0 \leq i,\ j < d$, então $0 \leq i \cdot \dfrac{m}{d},\ j \cdot \dfrac{m}{d} < m$, e como m divide $\left|i \cdot \dfrac{m}{d} - j \cdot \dfrac{m}{d}\right|$, segue-se que $i \cdot \dfrac{m}{d} = j \cdot \dfrac{m}{d}$ e, portanto, $i = j$.

Corolário 4.5.1. *Se $d = mdc(a,\ \mathbf{m})$, e d divide b, então a congruência linear $ax \equiv b\ mod\ \mathbf{m}$ possui d soluções mutualmente incongruentes módulo $\mathbf{m}$.*

Demonstração: Suponha que x_0 seja solução para congruência linear, então as soluções x são da forma $x = x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t$, com t sendo um inteiro qualquer. Se

$$x_1 = x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t_1 \quad e \quad x_2 = x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t_2$$

são as soluções, e se $x_1 \equiv x_2\ mod\ \mathbf{m}$, então

$$x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t_1 \equiv x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t_2\ mod\ \mathbf{m}$$

$$t_1 \equiv t_2\ mod \left(\frac{\mathbf{m}}{mdc\left(\mathbf{m}, \frac{\mathbf{m}}{d}\right)}\right)$$

$$t_1 \equiv t_2\ mod\ d$$

visto que o $mdc\left(\mathbf{m}, \frac{\mathbf{m}}{d}\right) = \frac{\mathbf{m}}{d}$ e $0 \leq t_1 < t_2 \leq d-1$. Isso mostra que $d \mid (t_2 - t_1)$, o que é impossível, isto é, $0 < t_2 - t_1 < d$.

Portanto, para todo inteiro $x_0 + \left(\frac{\mathbf{m}}{d}\right) \cdot t$ é congruente módulo $\mathbf{m}$ para algum d. Logo, duas soluções x_1 e x_2 são mutuamente incongruente módulo $\mathbf{m}$ se, e somente se, t_1 e t_2 são incongruente módulo d e existem d soluções mutuamente incongruentes.

Definição 4.5.2. *Seja x um inteiro. O inverso de x é um inteiro y tal que*

$$x \cdot y \equiv 1\ mod\ \mathbf{m}.$$

Corolário 4.5.2. *A congruência $yx \equiv 1\ mod\ \mathbf{m}$, com $mdc(y,\ m) = 1$, admite uma única solução módulo $\mathbf{m}$. Essa solução será chamada de inverso multiplicativo módulo $\mathbf{m}$.*

Demonstração: Como $mdc(y, m) = 1$, tem-se que $y \cdot x \equiv 1\ mod\ \mathbf{m}$, isto é

$$y \cdot x_0 \equiv 1\ mod\ \mathbf{m},$$

de modo que o inteiro y tem um único inverso módulo $\mathbf{m}$: $x = x_0$.

Exemplo 4.5.1 *Resolva a congruência linear $3x \equiv 5\ mod\ 7$.*

Solução: Note que $mdc(3, 7) = 1$ e 1 divide 5, e a congruência linear $3x \equiv 5\ mod\ 7$ tem exatamente uma solução mutuamente incongruente módulo 7.

Assim, para encontrar o inverso multiplicativo de 3 módulo 7, basta multiplicar a congruência linear $3x \equiv 5\ mod\ 7$ em ambos os lados por 5, isto é:

$$5 \cdot 3x \equiv 5 \cdot 5\ mod\ 7 \quad \Longrightarrow \quad 15x \equiv 25\ mod\ 7$$

o que implica em $x \equiv 4\ mod\ 7$.

Logo, as soluções de $3x \equiv 5\ mod\ 7$ são da forma $x = 4 + 7 \cdot k$, sendo k um inteiro qualquer.

Exemplo 4.5.2. *Resolva a congruência linear $3x \equiv 6\ mod\ 15$.*

Solução: O $mdc(3, 15) = 3$ e 3 divide 6, daí a congruência tem exatamente 3 soluções mutuamente incongruentes módulo 15. Dessa forma, $x_0 = 2$ é uma solução para a congruência linear $3x \equiv 6 \ mod \ 15$, consequentemente as três soluções são dadas:

$$x = 2 + \left(\frac{15}{3}\right) \cdot k = 2 + 5k,$$

onde $k = 0,\ 1,\ 2$.

Logo, isso implica que $x = 2,\ 7,\ 12$.

Problema 4.5.1. *Pode o dobro de um número natural deixar resto igual a* 9 *quando dividido por* 26*? E quando dividido por* 25*?*

Solução: 1) Respondendo à primeira indagação, e transforma o problema na seguinte congruência linear

$$2x \equiv 9 \ mod \ 26.$$

O $mdc(2, 26) = 2$, mas 2 não divide 9, logo a congruência linear $2x \equiv 9 \ mod \ 26$ não tem solução, ou seja, é impossível o dobro de um número natural x deixar resto 9 quando dividido por 26

2) Respondendo à segunda indagação, de modo análogo, é transformado a situação na seguinte congruência linear

$$2x \equiv 9 \ mod \ 25$$

e o $mdc(2, 25) = 1$, e 1 divide 9, logo a congruência linear tem solução, ou seja, é possível o dobro de um número natural x deixar resto 9 quando dividido por 25. Resolvendo essa congruência linear, para encontrar o inverso multiplicativo de 2 módulo 25, basta multiplicar por 13, isto é:

$$13 \cdot 2x \equiv 13 \cdot 9 \ mod \ 25 \quad \Longrightarrow \quad 26x \equiv 117 \ mod \ 25 \quad \Longrightarrow \quad x \equiv 17 \ mod \ 25.$$

Logo, para que o dobro de um número natural x deixe resto 9 quando dividido por 25, esse número deve ser da forma $x = 17 + 25k$, com $k \in \mathbb{N}$.

5 CLASSES RESIDUAIS E APLICAÇÕES

Nesta parte serão apresentados os conceitos, as definições e propriedades necessárias para mostrar uma contribuição deste trabalho para os docentes de matemática, que são as aplicações das Classes Residuais às Equações Diofantinas. As definições e resultados apresentados poderão ser encontrados em FILHO 1981, HEFEZ 2016b, LEITÃO 2019, SANTOS 2012 e A. d. A. SILVA 2000.

5.1 Classe Residual

Definição 5.1.1 (Sistema completo de resíduos). *Conjunto de todos os restos possíveis da divisão euclidiana de um inteiro a por m, com* $m > 1$*, cujos m elementos:* $\{0,\ 1,\ 2,\ \cdots,\ m-1\}$*, em uma ordem qualquer, são dois a dois incongruentes módulo m, será denominado por Sistema Completo de Resíduos Módulo m.*

Desse modo, passando a designar resto r como sendo um *resíduo módulo m.* E assim, diante da congruência podemos substituir qualquer um dos elementos do sistema completo de resíduos por um de seus representantes, além disto, qualquer conjunto de m elementos da forma $\{r_1,\ r_2,\ r_3,\ \cdots,\ r_m\}$ também será um sistema completo de resíduos, desde que satisfaça:

- $r_i \not\equiv r_j\ mod\ m$ para $i \neq j$;
- Para todo inteiro a, existe um r_i, tal que, $a \equiv r_i\ mod\ m$.

Será introduzido agora a noção de classe residual módulo m. Dado um inteiro $m > 1$ e considerando a classe de restos r módulo m, que será representado por $\overline{r}$, repartiremos o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando divididos por m. Isso nos dá a seguinte partição de $\mathbb{Z}$:

$$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ mod\ m\}$$

$$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ mod\ m\}$$

$$\overline{2} = \{x \in \mathbb{Z};\ x \equiv 2\ mod\ m\}$$

$$\vdots$$

$$\overline{m-1} = \{x \in \mathbb{Z};\ x \equiv m-1\ mod\ m\}.$$

Note que não é interessante haver continuação apos $\overline{m-1}$, visto que se tem: $\overline{m} = \overline{0}$, $\overline{m+1} = \overline{1}$, $\cdots$ e assim sucessivamente. Assim, tem-se que:

Definição 5.1.2 *O conjunto* $\overline{r} = \{x \in \mathbb{Z};\ x \equiv r\ mod\ m\}$ *é chamado de Classe Residual Módulo* m *do elemento* r *de* $\mathbb{Z}$. *O conjunto de todas as classes residuais módulo* m *será representado por* $\mathbb{Z}_m$. *Portanto*

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

Exemplo 5.1.1 *Se* $m = 2$, *então* $\mathbb{Z}_2 = \{\overline{0},\ \overline{1},\}$, *com*

$$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ mod\ 2\}$$

o que implica que $x = 2k$, *com* $k \in \mathbb{Z}$, *ou seja,* $\overline{0} = \{x \in \mathbb{Z};\ x\ é\ par\}$. *De modo semelhante,*

$$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ mod\ 2\}$$

isso implica que $\overline{1} = \{x \in \mathbb{Z};\ x\ é\ ímpar\}$. *Logo,*

$$\overline{r} = \begin{cases} \overline{0}, & se,\ e\ somente\ se, \quad r\ é\ par; \\ \overline{1}, & se,\ e\ somente\ se, \quad r\ é\ ímpar. \end{cases}$$

Exemplo 5.1.2 *Se* $m = 3$, *então* $\mathbb{Z}_3 = \{\overline{0},\ \overline{1},\ \overline{2}\}$, *com*

$$\overline{0} = \{x \in \mathbb{Z};\ x \equiv 0\ mod\ 3\} = \{3k;\ k \in \mathbb{Z}\}$$

$$\overline{1} = \{x \in \mathbb{Z};\ x \equiv 1\ mod\ 3\} = \{3k+1;\ k \in \mathbb{Z}\}$$

$$\overline{2} = \{x \in \mathbb{Z};\ x \equiv 2\ mod\ 3\} = \{3k+2;\ k \in \mathbb{Z}\}$$

Portanto,

$$\overline{r} = \begin{cases} \overline{0} & , \ se\ \ r\ \ é\ \ múltiplo\ \ de\ \ 3; \\ \overline{1} & , \ se\ \ r\ \ tem\ \ resto\ \ 1\ \ quando\ \ dividido\ por\ 3; \\ \overline{2} & , \ se\ \ r\ \ tem\ \ resto\ \ 2\ \ quando\ \ dividido\ por\ 3. \end{cases}$$

As classes residuais possuem as seguintes propriedades:

Proposição 5.1.1 *Sejam* $\overline{a}$ *e* $\overline{b}$ *as classes residuais módulo* $\boldsymbol{m}$ *de dois inteiros quaisquer* a *e* b.

1. $\overline{a} = \overline{b}$ *se, e somente se,* $a \equiv b\ mod\ \boldsymbol{m}$;
2. *Se* $\overline{a}$ *e* $\overline{b}$ *não são disjuntas* $(\overline{a} \cap \overline{b} \neq \varnothing)$, *então coincidem:* $\overline{a} = \overline{b}$;
3. *Se* $\overline{a}$ *e* $\overline{b}$ *são distintas* $(\overline{a} \neq \overline{b})$, *então são disjuntas:* $\overline{a} \cap \overline{b} = \varnothing$.

Demonstração.
(1) ($\Longrightarrow$) Suponha que $a \equiv b\ mod\ \mathbf{m}$ e seja x um elemento qualquer de $\overline{a}$, ou seja, $x \in \overline{a}$. Então:

$$x \equiv a\ mod\ \mathbf{m} \quad e \quad a \equiv b\ mod\ \mathbf{m} \quad \Longrightarrow \quad x \equiv b\ mod\ \mathbf{m}$$

e isso significa que $x \in \overline{b}$. Logo,

$$\overline{a} \subset \overline{b}. \tag{19}$$

Seja, agora y um elemento qualquer de $\overline{b}$, ou seja, $y \in \overline{b}$. Então,

$$y \equiv b \; mod \; \mathbf{m} \quad e \quad a \equiv b \; mod \; \mathbf{m} \quad \Longrightarrow \quad y \equiv a \; mod \; \mathbf{m}$$

e isso significa que $y \in \overline{a}$. Logo,

$$\overline{b} \subset \overline{a}. \tag{20}$$

Das inclusões (19) e (20), resulta que, de fato, $\overline{a} = \overline{b}$.
($\Longleftarrow$) Reciprocamente, suponha que $\overline{a} = \overline{b}$. Então existe um elemento d, tal que $d \in \overline{a}$, o que implica também em $d \in \overline{b}$. Portanto, $a \equiv b \; mod \; \mathbf{m}$.

(2) Com efeito, se $\overline{a}$ e $\overline{b}$ não são disjuntas, então existe pelo menos um inteiro c tal que $c \in \overline{a}$ e $c \in \overline{b}$. E segue que

$$c \equiv a \; mod \; \mathbf{m} \quad e \quad c \equiv b \; mod \; \mathbf{m} \quad \Longrightarrow \quad a \equiv b \; mod \; \mathbf{m}$$

Logo, pelo item (1), conclui-se que $\overline{a} = \overline{b}$.

(3) Com efeito, suponha que, se $\overline{a}$ e $\overline{b}$ não são disjuntas, então existe um inteiro c tal que $c \in \overline{a}$ e $c \in \overline{b}$. E segue que

$$c \equiv a \; mod \; \mathbf{m} \quad e \quad c \equiv b \; mod \; \mathbf{m} \quad \Longrightarrow \quad a \equiv b \; mod \; \mathbf{m}$$

Logo, pelo item (1), conclui-se que $\overline{a} = \overline{b}$, o que é impossível, visto que, por hipótese, $\overline{a} \neq \overline{b}$.

Desse modo, a partir da propriedade (3) implica que a reunião de todas as classes residuais módulo $\mathbf{m}$ é igual a $\mathbb{Z}$. Pode-se perceber que, pelo **Exemplo 5.1.1.** quando $\mathbf{m} = 2$, há duas classes residuais para $\mathbb{Z}_2 = \{\overline{0},\ \overline{1}\}$, ambas disjuntas e cuja reunião é o próprio $\mathbb{Z}$.

Ademais, segue que o conjunto dos inteiros $\{0,\ 1,\ 2,\ 3, \cdots,\ m-1\}$ é um sistema completo de resíduos se, e somente se $\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \cdots \overline{m-1}\}$ são as m classes residuais módulo $\mathbf{m}$, que atuam tal com "$ficheiro$" com $\mathbf{m}$ "$gavetas$" nas quais é organizado cada um dos elementos de $\mathbb{Z}$, que por sua vez, fica particionado em $\mathbf{m}$ subconjuntos formados por inteiros mutualmente congruentes módulo $\mathbf{m}$.

Como já mostrado, uma característica importante das classes residuais é que transformam a congruência $a \equiv b \; mod \; \mathbf{m}$ na igualdade $\overline{a} = \overline{b}$. Outra característica é que em $\mathbb{Z}_m$ valem as operações:

Adição: $\overline{a} + \overline{b} = \overline{a + b}$.

Multiplicação: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$.

Essas operações gozam das seguintes propriedades.

Propriedades da Adição. Para todos $\overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_m$, tem-se

A_1) **Associatividade:** $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;

A_2) **Comutatividade:** $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;

A_3) **Existência de Zero:** $\overline{a} + \overline{0} = \overline{a}$ para todo $\overline{a} \in \mathbb{Z}_m$;

A_4) **Existência de simétrico:** $\overline{a} + \overline{-a} = \overline{0}$.

Propriedades da Multiplicação. Para todos $\overline{a},\ \overline{b},\ \overline{c} \in \mathbb{Z}_m$, tem-se

M_1) **Associatividade:** $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;

M_2) **Comutatividade:** $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;

M_3) **Existência de unidade:** $\overline{a} \cdot \overline{1} = \overline{a}$;

AM) **Distributividade:** $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$.

Exemplo 5.1.3. *As tabelas de adição e multiplicação em* $\mathbb{Z}_2 = \{\ \overline{0},\ \overline{1}\ \}$ *são*

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Exemplo 5.1.4 *As tabelas de adição e multiplicação em* $\mathbb{Z}_3 = \{\ \overline{0},\ \overline{1},\ \overline{2}\ \}$ *são*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Exemplo 5.1.5 *As tabelas de adição e multiplicação em* $\mathbb{Z}_4 = \{\ \overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\ \}$ *são*

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Um elemento $\overline{a} \in \mathbb{Z}_m$ será dito *inversível*, quando existir $\overline{b} \in \mathbb{Z}_m$ tal que $\overline{a} \cdot \overline{b} = 1$. Nesse caso, diremos que $\overline{b}$ é o inverso de $\overline{a}$.

Proposição 5.1.2. *Um elemento* $\overline{a}$ *é inversível se, e somente se, o* $mdc(a,\ m) = 1$.

Demonstração.
($\Longrightarrow$) Se $\overline{a}$ é inversível, então existe $\overline{b} \in \mathbb{Z}_m$ tal que

$$\overline{1} = \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Logo $a \cdot b \equiv 1\ mod\ \mathbf{m}$, isto é, existe um inteiro t tal que $a \cdot b + t \cdot \mathbf{m} = \mathbf{1}$ e consequentemente, $mdc(a,\ m) = 1$.
($\Longleftarrow$) Reciprocamente, se $mdc(a,\ m) = 1$, existem inteiros b e t tais que $a \cdot b + \mathbf{m} \cdot t = 1$ e, consequentemente,

$$\overline{1} = \overline{a \cdot b + \mathbf{m} \cdot t} = \overline{a \cdot b} + \overline{\mathbf{m} \cdot t} = \overline{a} \cdot \overline{b} + \overline{0} = \overline{a} \cdot \overline{b}.$$

Portanto, $\overline{a}$ é inversível.

Exemplo 5.1.7. *Encontre o elemento inversível de* $\overline{5}$ *em* $\mathbb{Z}_6$.

Solução:
Note que, dado $\mathbb{Z}_6 = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$ pela tabela de multiplicação,

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Como $\overline{5} \cdot \overline{5} = \overline{1}$, $\overline{5}$ é inversível em $\mathbb{Z}_6$ com inverso o próprio $\overline{5}$.

5.1.1 Aplicações às Equações Diofantinas

O objetivo é transformar uma equação diofantina em equações de classes residuais, para tanto, inicialmente é necessário converter para congruências lineares, pois uma característica importante das classes residuais é que transformam a congruência $a \equiv b \ mod \ m$ na igualdade $\overline{a} = \overline{b}$ em $\mathbb{Z}_m$.

Assim, dados $a,\ b$, e n inteiros, a equação diofantina $ax + by = n$, pelo **Teorema 3.5.1**, admite solução se, e somente se, $d \mid n$, sendo $d = mdc(a, b)$.

Pelo **Corolário 3.5.1**, seja o par de inteiros $x_0,\ y_0$ uma solução particular da equação $ax + by = n$. Então o par $x,\ y$ é solução geral da equação se, e somente se,

$$x \ = \ x_0 \ + \ \left(\frac{b}{d}\right) \cdot t \qquad e \qquad y \ = \ y_0 \ - \ \left(\frac{a}{d}\right) \cdot t,$$

com $t \in \mathbb{Z}$.

Com efeito, pela **Proposição 4.5.1**, tem-se que

$$x \equiv x_0 \ mod \left(\frac{b}{d}\right).$$

Considerando a equação

$$ax + by = n$$

e escolhendo adequadamente um p primo e divisor de b, pela **Proposição 4.5.1**, tem-se que

$$ax \equiv n \ mod \ p.$$

Infere-se da **Proposição 5.1.1** que existe um x_0 inteiro, tal que $ax_0 \equiv n \ mod \ p$. Isso equivale a dizer que a congruência linear apresentada é equivalente a uma equação de classe residuais. Assim, $\overline{ax_0}$ é igual a classe $\overline{n}$ em $\mathbb{Z}_p$ ou seja,

$$ax_0 \equiv n \ mod \ p \quad \Longleftrightarrow \quad \overline{ax_0} = \overline{n} \quad \Longrightarrow \quad \overline{a} \cdot \overline{x_0} = \overline{n} \quad em \ \ \mathbb{Z}_p. \tag{21}$$

Pode-se dizer ainda que (21), por definição, equivale a

$$\overline{a} \cdot x = \overline{n} \tag{22}$$

tem solução em $\mathbb{Z}_p$.

Logo, resolver a congruência linear $ax_0 \equiv n \ mod \ p$, se reduz a resolver em $\mathbb{Z}_p$ a equação:

$$\overline{a} \cdot \overline{x} = \overline{n}.$$

Assim, tomando $\overline{a}^{-1}$ como classe inversa de $\overline{a}$ em $\mathbb{Z}_p$, implica que

$$\overline{x} = \overline{n} \cdot \overline{a}^{-1} \tag{23}$$

como já visto, (23) pode ser reduzido a

$$x \equiv a^{-1} \cdot n \ mod \ p.$$

Portanto, $x_0 = a^{-1} \cdot n$ adequado será uma solução particular da equação Diofantina. Substituindo x_0 em $ax + by = n$ encontra-se y_0.

Dessa forma, pelo **Corolário 3.5.1**, conclui-se finalmente que uma equação Diofantina

$$ax + by = n,$$

com $d = mdc(a, \ b)$, tem como soluções x e y em $\mathbb{Z}$.

Observação 5.1.1 *De modo análogo, pode-se também escolher adequadamente um p primo e divisor de a.*

Nesta seção são utilizadas Classes Residuais para resolver equações Diofantinas.

Exemplo 5.1.1 *Resolva a equação Diofantina* $8x + 13y = 135$.

Solução. A equação Diofantina tem solução, visto que $mdc(8, 13) \mid 135$. Tomando adequadamente $p = 13$, tem-se:

$$(8x + 13y) \equiv 135 \ mod \ 13$$

$$8x \equiv 5 \ mod \ 13.$$

Resolver a congruência linear acima, se reduz a resolver em $\mathbb{Z}_{13}$ a equação:

$$\overline{8} \cdot \overline{x} = \overline{5}. \tag{24}$$

Multiplicando a equação (24) por $\overline{5}$, tem-se

$$\overline{5} \cdot \overline{8} \cdot \overline{x} \equiv \overline{5} \cdot \overline{5} \ mod \ 13$$

e

$$x \equiv 12 \ mod \ 13.$$

Portanto,

$$x = 12 + 13t, \ t \in \mathbb{Z}.$$

Considerando $x_0 = 12$ uma solução particular e substituindo em $8x+13y = 135$, encontra-se $y_0 = 3$ e

$$y = 3 - 8t.$$

Assim, a solução geral é

$$\begin{cases} x = 12 + 13t \\ y = 3 - 8t \end{cases} \quad t \in \mathbb{Z}.$$

Exemplo 5.1.2 *Resolva a equação Diofantina* $17x - 28y = 37$.

Solução. A equação Diofantina tem solução, visto que $mdc(17, -28) \mid 37$. Tomando adequadamente $p = 17$, tem-se:

$$(17x - 28y) \equiv 37 \ mod \ 17$$
$$-11y \equiv 3 mod \ 17$$
$$6y \equiv 3 mod \ 17.$$

Resolver a congruência linear acima, se reduz a resolver em $\mathbb{Z}_{17}$ a equação:

$$\overline{6} \cdot y = \overline{3}. \tag{25}$$

Multiplicando a equação (25) por $\overline{3}$, tem-se

$$y \equiv 9 \ mod \ 17.$$

Portanto,

$$y = 9 - 17t, \ t \in \mathbb{Z}.$$

Considerando $y_0 = 9$ uma solução particular e substituindo em $17x - 28y = 37$, encontra-se $x_0 = 17$. Assim, a solução geral é

$$\begin{cases} x = 17 - 28t \\ y = 9 - 17t \end{cases} \quad t \in \mathbb{Z}.$$

Observação 5.1.2 *O exemplo anterior foi resolvido na seção das equações Diofantinas (exemplo 3.5.4), contudo, utilizando classes residuais, a resolução fica mais ágil e simples.*

Exemplo 5.1.3 *Resolva a equação Diofantina* $45x - 14y = 11$.

*Solução.*A equação Diofantina tem solução, visto que $mdc(45, -14) \mid 11$. Tomando adequadamente $p = 7$, tem-se:

$$(45x - 14y) \equiv 11 \ mod \ 7$$
$$3x \equiv 4 \ mod \ 7. \tag{26}$$

Multiplicando a equação (26) por $\overline{5}$, tem-se

$$5 \cdot 3 \cdot x \equiv 4 \cdot 5 \ mod \ 7,$$

e

$$x \equiv 6 \ mod \ 7 \quad \Longrightarrow \quad x \equiv -1 \ mod \ 7.$$

Assim, $x = -1 + 7k$, com $k \in \mathbb{Z}$. Assumindo $k = 0$, tem $x_0 = -1$ como uma solução particular, substituindo na equação $45x - 14y = 11$, encontra-se $y_0 = -4$. Assim, a solução geral é

$$\begin{cases} x = -1 - 14t \\ y = -4 - 45t \end{cases} \quad t \in \mathbb{Z}.$$

Exemplo 5.1.4. *Resolva a equação Diofantina* $25x - 28y = 37$.

*Solução.*A equação Diofantina tem solução, visto que $mdc(25, -28) \mid 37$. Tomando adequadamente $p = 7$, tem-se que

$$(25x - 28y) \equiv 37 \ mod \ 7$$
$$4x \equiv 2 \ mod \ 7. \tag{27}$$

Para a equação (27), $\overline{2}$ é o inverso de $\overline{4}$ em Z_7. Multiplicando a equação por $\overline{2}$, tem-se que

$$x \equiv 4 \ mod \ 7 \quad \Longrightarrow \quad x \equiv -3 \ mod \ 7.$$

Assim, $x = -3 + 7k$, com $k \in \mathbb{Z}$. Assumindo $k = 0$, tem $x_0 = -3$ como uma solução particular, substituindo na equação $25x - 28y = 37$, encontra-se $y_0 = -4$, e

$$y = -4 - 25t.$$

Assim, a solução geral é

$$\begin{cases} x = -3 - 28t \\ y = -4 - 25t \end{cases} \Longrightarrow \begin{cases} x = 25 - 28t \\ y = 21 - 25t \end{cases} \quad t \in \mathbb{Z}.$$

Problema 5.1.1 *Em uma loja dois produtos custam R$ 71,00 e 83,00, respectivamente. Que quantidade inteiras de ambos podem ser compradas com R$ 1.670,00?*

Solução. A equação Diofantina que modela o problema é $71x + 83y = 1670$ e tem solução, visto que $mdc(71, 83) \mid 1670$. Tomando adequadamente $p = 71$, tem-se que

$$(71x + 83y) \equiv 1670 \ mod \ 71$$
$$83y \equiv 1670 \ mod \ 71$$
$$12y \equiv 37 \ mod \ 71. \tag{28}$$

Para a equação (28), $\overline{6}$ é classe inversa de $\overline{12}$. Multiplicando a equação por $\overline{6}$, tem-se

$$6 \cdot 12 \cdot y \equiv 6 \cdot 37 \ mod \ 71$$

Isso é

$$y \equiv 222 \ mod \ 71$$
$$y \equiv 9 \ mod \ 71.$$

Considerando $y = 9$ uma solução particular e substituindo em $71x+83y = 1670$, encontra-se $x = 13$.

$$x = 13 + 83t.$$

Assim, a solução geral é $x = 13$ e $y = 9$, ou seja, podem-se comprar 13 produtos que custam R$ 71,00 e 9 que custam R$ 83,00.

Problema 5.1.2 *Dispondo de R$ 110,00 quais as quantias que se podem gastar comprando selos que custam R$ 7,00 e R$ 9,00?*

Solução: A equação que modela o problema é $7x + 9y = 110$ e possui solução. Assim, escolhendo $p = 7$, tem-se que

$$(7x + 9y) \equiv 110 \ mod \ 7$$

$$2y \equiv 5 \ mod \ 7. \tag{29}$$

Multiplicando (29) por 4, tem-se que

$$4 \cdot 2y \equiv 5 \cdot 4 \ mod \ 7$$

$$y \equiv 6 \ mod \ 7.$$

Assumindo $y = 6$ e substituindo na equação $7x + 9y = 110$, obtém-se $x = 8$.

Portanto, a solução para o problema são 8 selos de 7 reais e 6 selos de 9 reais.

Observação 5.1.3 *Note que o problema anterior foi resolvido na seção das equações Diofantinas (Problema 3.5.2), contudo, utilizando classes residuais, a resolução fica mais simples e ágil.*

Problema 5.1.3 *Determine os múltiplos positivos de* 11 *e* 9 *cuja soma é igual a 270.*

Solução: A equação que modela o problema é $11x + 9y = 270$ e possui solução. Assim, escolhendo $p = 11$, tem-se que

$$(11x + 9y) \equiv 270 \ mod \ 11.$$

$$9y \equiv 6 \ mod \ 11. \tag{30}$$

Multiplicando (30) por 5, tem-se

$$5 \cdot 9y \equiv 5 \cdot 6 \ mod \ 11$$

$$y \equiv 8 \ mod \ 11.$$

Assumindo $y_0 = 8$ e substituindo na equação $11x + 9y = 270$, obtém-se $x_0 = 18$.

Portanto, a solução para o problema é

$$\begin{cases} x = 18 + 9t \\ y = 8 - 11t \end{cases} \quad t = -1 \ \ e \ \ t = 0.$$

6 CONSIDERAÇÕES FINAIS

Compreende-se que a importância da Aritmética Modular no ensino é extraordinária e totalmente relevante. Por mais que não esteja presente nos currículos do ensino básico, os docentes de matemática podem inserir, consoante a documentos educacionais e pesquisadores docentes de matemática, esse objeto de conhecimento em suas aulas, desde que atrelados aos conteúdos de Teoria dos Números contidos nas grades curriculares. Isso se dá pelo fato da Aritmética Modular trazer um rol de aplicações de fácil compreensão pelos alunos da educação básica, tais como à divisibilidade, ao calendário, ao relógio, ao CPF, aos cartões de crédito, entre outros.

Por outro lado, no ensino superior, a Aritmética Modular, além de proporcionar de forma geral uma alta visão sobre o comportamento das operações nos inteiros, essencialmente na divisão, possui ricas aplicações de modo muito amplo tais como aos Critérios de Divisibilidade, à Criptografia, às Equações Diofantinas e assim por diante. Pode-se destacar ainda, que as Classes Residuais (conteúdo de Aritmética Modular) são ferramentas poderosas, como mostrado suas aplicações neste trabalho, quando se trata de resolução das equações diofantinas lineares, pois é um método simples e facilitador para os discentes e docentes de matemática.

Portanto, conclui-se que a Aritmética Modular tem aplicações em diversas áreas do conhecimento, como por exemplo, desde a Criptografia até a Teoria dos Números. Ela oferece uma nova perspectiva sobre a natureza dos números, tornando a matemática mais interessante e divertida. Desafia os alunos a pensar de forma crítica e criativa, estimula o raciocínio lógico e a abstração matemática, buscando soluções para problemas que não se encaixam nas regras matemáticas tradicionais. E é notório que esta dissertação é sucinta e possui uma exposição teórica e prática facilitadora que encoraja o leitor a fazer bom uso do resultado apresentado.

REFERÊNCIAS

BARBOSA, Janayna M. R. (2017). "Congruências modulares e aplicações no Ensino Básico". Tese de dout. Universidade de São Paulo.

BOYER, Carl B e MERZBACH Uta C. (2019). *História da matemática*. Editora Blucher.

BRASIL (2018). *Base Nacional Comum Curricular*. MEC.

COHEN, Morris Raphael e DRABKIN Israel Edward (1948). *A source book in Greek science*.

FERREIRA, Rosiane Barros et al. (2018). "Congruência modular no ensino básico." Em.

FILHO, Edgard de Alencar (1981). *Teoria elementar dos números*. Nobel.

FRANCO, Tânia Regina Rodrigues (2016). "Divisibilidade e congruências: aplicações no ensino fundamental II". Em.

GOMES, Ataniel Rogério Gonçalves et al. (2015). "Uma abordagem do ensino de congruência na educação básica". Em.

GROENWALD, C. L. O., SAUER L.O. e FRANKE R. F. (2005). "A história da matemática como recurso didático para o ensino da teoria dos números e a aprendizagem da matemática no ensino básico". Em: *Paradígma* 26.2, pp. 35–55.

HEFEZ, Abramo (2016a). *Aritmética*. SBM.

— (2016b). *Elementos de Aritmética*. SBM.

LEITÃO, Filliphe de Almeida (2019). "Aritmética modular e suas aplicações: uma experiência de atuação no Ensino Básico". Em.

LINS, R. C. e Joaquim GIMENEZ (2000). *Perspectivas Em Aritmética E Álgebra P/O Séc. Xxi*. Papirus Editora.

MARANHÃO (2019). *Documento Curricular do Território Maranhense: para a Educação Infantil e o Ensino Fundamental*. FGV Editora.

MARONESE, Diego A. (2016). "Tópicos de aritmética modular na educação básica: uma proposta de atividades". Em.

MATTOS, Sergio R. P., Cleonice PUGGIAN e Abel G. LOZANO (2011). "Aritmética Modular E Suas Possibilidades Na Formação Continuada De Professores De Matemática (CO)". Em: *XIII CONFERÊNCIA INTERAMERICANA DE EDUCAÇÃO MATEMÁTICA*.

MELO, Carlos Ian Bezerra de e João Luzeilton de OLIVEIRA (2023). "O algoritmo da divisão na formação inicial do professor de matemática". Em: *Educação Matemática Pesquisa* 25.3, pp. 344–372.

OCDE (2016). *Ten Questions for Mathematics Teachers... and How PISA Can Help Answer Them. PISA*. ERIC.

OLIVEIRA, Elizabeth Magalhães et al. (2017). "UMA PROPOSTA DE ENSINO DE ARITMÉTICA MODULAR PARA EDUCAÇÃO BÁSICA". Em: *VII CONGRESSO INTERNACIONAL DE ENSINO DE MATEMÁTICA-2017*.

POMMER, Wagner Marcelo et al. (2008). "Equações diofantinas lineares: um desafio motivador para alunos do ensino médio". Em.

RIBENBOIM, Paulo (2012). *Números primos: velhos mistérios e novos recordes*. IMPA.

SANTOS, José Plínio de Oliveira (2012). *Introdução à Teoria dos Números*. IMPA.

SILVA, Antônio de Andrade (2000). "Números, Relações e Criptografia". Em: *Departamento de Matemática-UFPB, Paraíba*.

SILVA, Luciano M. e Edel Alexandre Silva PONTES (2023). "Aritmética Modular como proposta de ensino de Matemática: uma experiência prática em uma Escola Pública

de ensino fundamental". Em: *Revista Diálogos em Educação Matemática* 2.1, e202304–e202304.

SOUZA, Leticia Vasconcellos de (2015). "Congruência modular nas séries finais do ensino fundamental". Em.

SPINA, André Vinícius (2014). "Números primos e criptografia". Tese de dout. [sn].

VIEIRA, Vandenberg Lopes (2020). *Um curso básico em teoria dos números*. Editora Livraria da Física.