Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Fernando Henrique Castilheri de Lima

Congruência Modular: Uma Proposta Didática para a Resolução de Equações Diofantinas Lineares

Cuiabá/ MT - 2025

Fernando Henrique Castilheri de Lima

Congruência Modular: Uma Proposta Didática para a Resolução de Equações Diofantinas Lineares

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – **Profmat**, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título de **Mestre em Matemática**.

Área de concentração: Matemática na Educação Básica.
Linha de pesquisa: Formação de Professores de Matemática da Educação Básica

Prof. Dr. Reinaldo de Marchi
Orientador

Cuiabá - MT
2025

Dados Internacionais de Catalogação na Fonte.

L732c Lima, Fernando Henrique Castilheri de.
Congruência Modular: Uma Proposta Didática para a Resolução de Equações Diofantinas Lineares [recurso eletrônico] / Fernando Henrique Castilheri de Lima. -- Dados eletrônicos (1 arquivo : 92 f., il. color., pdf). -- 2025.

Orientador: Reinaldo de Marchi.
Dissertação (mestrado profissional) – Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação Profissional em Matemática, Cuiabá, 2025.
Modo de acesso: World Wide Web: https://ri.ufmt.br.
Inclui bibliografia.

1. Diofanto de Alexandria. 2. Carl Friedrich Gauss. 3. Teoria dos Números. 4. Aritmética Modular. 5. Sequência Didática. I. Marchi, Reinaldo de, *orientador.* II. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DE MATO GROSSO

PRÓ-REITORIA DE ENSINO DE PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

AV. FERNANDO CORRÊA DA COSTA, 2367 - BOA ESPERANÇA - 78.060-900 - CUIABÁ/MT

FONE: (65) 3615-8576 – E-MAIL: PROFMAT.ICET@UFMT.BR

FOLHA DE APROVAÇÃO

TÍTULO**: CONGRUÊNCIA MODULAR: UMA PROPOSTA DIDÁTICA PARA A RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES.**

AUTOR: **MESTRANDO FERNANDO HENRIQUE CASTILHERI DE LIMA**

Dissertação defendida e aprovada em 25 de março de 2025.

COMPOSIÇÃO DA BANCA EXAMINADORA

1. **Prof. Dr. Reinaldo de Marchi** (Presidente Banca/orientador)

Instituição: Universidade Federal de Mato Grosso

2. **Profª. Drª. Anna Lígia Oenning Soares** (Membro Interno)

Instituição: Universidade Federal de Mato Grosso

3. **Prof. Dr. Junior Cesar Alves Soares** (Membro externo)

Instituição: Universidade Estadual de Mato Grosso - campus Barra do Bugres

Cuiabá, 25/03/2025.

Documento assinado eletronicamente por **REINALDO DE MARCHI**, **Docente da Universidade Federal de Mato Grosso**, em 26/03/2025, às 09:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Junior Cesar Alves Soares**, **Usuário Externo**, em 26/03/2025, às 11:54, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **ANNA LIGIA OENNING SOARES**, **Docente da Universidade Federal de Mato Grosso**, em 26/03/2025, às 14:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.ufmt.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **7755338** e o código CRC **CDB1AC7D**.

DEDICATÓRIA

A Deus, fonte inesgotável de força, sabedoria e inspiração, por Sua presença constante, guiando-me em cada etapa desta jornada e abençoando cada passo em direção a este objetivo. À minha esposa, Elisandra, por seu amor, paciência e apoio incondicional, sendo um alicerce fundamental em minha vida e no desenvolvimento deste trabalho. Aos meus pais, por sua dedicação incansável, pelos ensinamentos transmitidos e pelo exemplo de perseverança que sempre me inspiraram a acreditar em meus sonhos e a lutar para concretizá-los. .

Agradecimentos

Agradeço primeiramente a Deus por todas as bênçãos a mim concedidas, pois sei que sem Ele nada seria possível.

Expresso também minha profunda gratidão à minha esposa, Elisandra, cujo companheirismo, paciência e apoio incondicional foram essenciais ao longo desta jornada no mestrado. Sua presença constante em cada desafio, bem como sua crença em meu potencial mesmo nos momentos de incerteza, foram fundamentais para que eu pudesse alcançar esta conquista.

Agradeço aos meus colegas de PROFMAT, principalmente ao Josué, pois dividimos várias angústias e também alegrias durante todo esse período de estudos.

Agradeço ao Coordenador do Mestrado Profmat na UFMT, Prof. Dr. Pedro Manuel Sanchez Aguilar, pela paciência, compreensão e constante disponibilidade, sempre demonstrando extrema cordialidade.

Agradeço a todos os professores do programa, em especial, ao meu orientador, Prof. Dr. Reinaldo de Marchi, que sempre esteve presente quando precisei, um professor amigo que vou levar no meu coração.

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

Carl Friedrich Gauss.

Resumo

O presente trabalho tem como objetivo principal fornecer subsídios teóricos e práticos para estudantes e professores, visando aprimorar a compreensão, a interpretação e a resolução de problemas que podem ser solucionados por meio das equações diofantinas lineares apresentando, para este fim, a congruência modular como uma ferramenta alternativa, valiosa e complementar ao algoritmo de Euclides. Para isso, abordamos tópicos essenciais para a compreensão dos conteúdos envolvidos no itinerário pedagógico, tais como: números inteiros e suas operações, divisibilidade, divisão euclidiana, máximo divisor comum, algoritmo de Euclides e conceitos básicos de aritmética modular.

Paralelamente, buscamos desenvolver jogos pedagógicos como recurso de apoio para professores que desejem implementar o estudo das equações diofantinas na Educação Básica, tendo em vista que a utilização de jogos no ensino de Matemática, quando planejada de maneira intencional, pode criar um ambiente estimulante e desafiador, favorecendo o desenvolvimento do pensamento lógico, a capacidade de cooperação e a construção de conceitos matemáticos. Entendemos que o jogo atua como um facilitador da aprendizagem ao incorporar a dimensão lúdica na resolução de problemas, proporcionando ao aluno um ambiente propício à assimilação de conceitos, ainda que sua formalização tenha ocorrido previamente.

Palavras chave: Diofanto de Alexandria; Carl Friedrich Gauss; Teoria dos Números; Divisão Euclidiana; Aritmética Modular; Sequência Didática.

Abstract

This study aims to provide theoretical and practical support for students and teachers, with the goal of enhancing their understanding, interpretation, and problem-solving skills regarding issues that can be addressed through linear Diophantine equations. It presents modular congruence as an alternative, valuable, and complementary tool to the Euclidean algorithm for this purpose. To achieve this, essential topics will be covered to facilitate comprehension of the relevant concepts within the pedagogical framework, including: integers and their operations, divisibility, Euclidean division, greatest common divisor, the Euclidean algorithm, and fundamental concepts of modular arithmetic.

In parallel, we seek to develop educational games as a supplementary resource for teachers who wish to introduce the study of Diophantine equations in basic education. This initiative is based on the premise that the intentional use of games in mathematics education can create a stimulating and challenging environment, fostering the development of logical thinking, cooperative skills, and the construction of mathematical concepts. We understand that games serve as facilitators of learning by incorporating a playful dimension into problem-solving, providing students with a conducive environment for concept assimilation, even when formalization has occurred beforehand.

Keywords: Diophantus of Alexandria; Carl Friedrich Gauss; Number Theory; Euclidean Division; Modular Arithmetic; Didactic Sequence.

Lista de Figuras

Sumário

Introdução

A Teoria dos Números, um dos ramos mais antigos e fundamentais da Matemática, sempre despertou grande fascínio por suas interseções entre simplicidade e profundidade. Desde os tempos da Antiguidade, com matemáticos como Euclides e Diofanto, até os desenvolvimentos modernos, essa área tem se expandido em complexidade e aplicação.

Neste texto ressaltaremos uma vertente da Teoria dos Números conhecida como Aritimética Modular cujas bases teóricas tiveram início por volta dos anos de 1750 com os trabalhos do matemático suiço Leonhard Euler (1707-1783). No entanto, uma das contribuições mais fecundas, a "Teoria das Congruências", foi introduzida em 1801, por Carl Friedrich Gauss (1777-1855) um dos maiores matemáticos de todos os tempos, no seu livro Disquisitiones Arithmeticae, no qual deu sequência aos estudos de Euler sobre a divisão euclidiana de um número inteiro por um número fixo, ao qual chamou de módulo. Em sua obra, Gauss adotou simbologia e definições que são utilizadas até hoje.

Na Antiguidade, o conceito de divisão com resto era usado intuitivamente. Por exemplo, o calendário lunar e a organização de ciclos astronômicos muitas vezes utilizavam raciocínios similares aos que hoje interpretamos como congruências modulares. Na China antiga, por volta do século III, o Teorema Chinês dos Restos (ou Algoritmo Chinês de Congruências) foi um dos primeiros exemplos de aplicação da aritmética modular. Ele servia para resolver problemas envolvendo divisões múltiplas, facilitando cálculos em diversas áreas, como na astronomia e na agrimensura.

No centro desta evolução encontra-se a congruência modular, uma ferramenta essencial para a compreensão das propriedades dos números inteiros e sua relação com problemas aritméticos. Congruências modulares fornecem uma estrutura matemática poderosa para resolver problemas que envolvem divisibilidade e, em particular, têm um papel crucial na resolução de equações diofantinas lineares, que se baseiam em encontrar soluções inteiras para equações polinomiais.

O ensino da Teoria dos Números e, por consequência, a congruência modular, é interessante do ponto de vista escolar, uma vez que encontramos sua aplicabilidade em temas presentes no cotidiano, como código de barras, sistemas de identificação, criptografia, entre outros.

O ensino de Matemática no Brasil atualmente enfrenta desafios significativos, especialmente no Ensino Médio, que abrange alunos entre 15 e 17 anos. Dados recentes, como os divulgados pela Avaliação Nacional da Educação Básica (ANEB) e pelo Programa Internacional de Avaliação de Estudantes (PISA), revelam um cenário preocupante em termos de desempenho matemático dos alunos brasileiros.

De acordo com o PISA 2022, os alunos brasileiros apresentam desempenho abaixo da média global em Matemática. O Brasil ficou em torno da 70ª posição entre os 79 países avaliados, destacando a necessidade urgente de intervenções na qualidade do ensino. Apenas cerca de 3% dos alunos atingem os níveis mais altos de proficiência, enquanto uma grande parcela permanece nos níveis mais baixos, o que demonstra uma defasagem considerável em relação a países com sistemas educacionais mais avançados.

Além disso, o Índice de Desenvolvimento da Educação Básica (IDEB) de 2021 mostra que o ensino médio não atingiu a meta prevista para Matemática. A média nacional foi de 4,2, enquanto a meta estipulada era de 5,0. Esse dado evidencia uma lacuna na aprendizagem, especialmente entre estudantes de escolas públicas, que enfrentam maior desigualdade de acesso a recursos pedagógicos de qualidade e estreita carga horária da disciplina dentro da Educação Básica, principalmente no Ensino Médio. Isso nos alerta para a necessidade de um ensino mais eficaz onde os alunos compreendam conceitos importantes como os conceitos aritméticos, que são essenciais para a aprendizagem de outros conteúdos, e dessa forma fazer com que o ensino da matemática avance.

Em entrevista concedida a Revista do Professor de Matemática, o professor Elon Lima afirma:

> "O conhecimento matemático é, por natureza, encadeado e cumulativo. Um aluno pode, por exemplo, saber praticamente tudo sobre Proclamação da República Brasileira e ignorar completamente as Capitanias Hereditárias, mas, não será capaz de estudar Trigonometria se não conhecer os fundamentos da Álgebra, nem entenderá essa última se não souber as operações aritméticas, etc. Esse aspecto de dependência acumulada dos assuntos matemáticos leva à uma sequência necessária, que torna difícil pegar o bonde andando" (LIMA, 1995).

No Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT), o estudo das equações diofantinas lineares é contemplado na disciplina de Aritmética (MA14) e, no livro da Coleção PROFMAT (HEFEZ, 2022), assim como em outros livros, a maneira mais usual apresentada para a resolução dessas equações é o algoritmo de Euclides.

Durante o período do Mestrado, em preparação para o Exame Nacional de Qualificação a ser realizado já em março do ano seguinte, tornou-se evidente, ao analisar as

provas dos anos anteriores, que esse conteúdo é frequentemente abordado. Assim, dependendo da equação diofantina apresentada, o processo de expressar o máximo divisor comum (mdc) como uma combinação linear dos coeficientes das incógnitas poderia se tornar extenso e suscetível a erros, devido ao número de etapas envolvidas e à pressão do tempo de prova.

Assim, surgiram as primeiras indagações sobre as maneiras possíveis de resolução das equações diofantinas: existiria uma outra alternativa de resolução? Qual? Seria um caminho factível que poderia simplificar processos em possíveis questões do ENQ (Exame Nacional de Qualificação)?

Além disso, ao consultar professores da educação básica sobre a forma como abordam a resolução dessas equações, a maioria relatou utilizar o algoritmo de Euclides. Assim, na busca por um método alternativo, surgiu a seguinte problemática: Qual seria um outro método prático e eficiente para a resolução de equações diofantinas?

Aprofundando meus estudos, encontrei na congruência modular uma teoria com a qual particularmente me identifiquei muito, tanto para a resolução de equações diofantinas como também para outros conteúdos abordados durante o Mestrado.

A resolução de equações diofantinas lineares da forma $ax+by=c$, com $a, b, c \in \mathbb{Z}$, por meio da congruência modular, pode constituir uma abordagem eficiente e sistemática, especialmente quando comparada à aplicação direta do algoritmo de Euclides para a obtenção da solução geral. A técnica de congruências permite reformular a equação original em um problema de menor complexidade, simplificando sua resolução ao determinar um elemento que satisfaça a relação modular correspondente. Isso elimina a necessidade de sucessivas substituições e retropropagações típicas do método euclidiano.

Diante dessa perspectiva, por que não explorar as equações diofantinas sob a ótica da congruência modular como alternativa ao método de Euclides, tornando essa abordagem o objeto do meu estudo?

Nessa perspectiva, este trabalho poderia ser especialmente útil para professores da Educação Básica que desejassem trabalhar o ensino das equações diofantinas com seus alunos, seja na resolução de problemas ou em outros conteúdos que recaiam neste tipo de equação.

Assim, definiu-se o tema desse trabalho, **Congruência Modular: Uma Proposta Didática para a Resolução de Equações Diofantinas Lineares**.

Reconhecer a pertinência do ensino das congruências modulares na Educação Básica, foi a principal motivação para a escolha do tema que aborda a congruência modular na resolução de equações diofantinas para esta dissertação, pois seus conceitos poderiam contribuir na aprendizagem dos educandos por possuírem diversas aplicações em problemas atuais além de estarem presentes no crescente uso das tecnologias.

Este trabalho tem como objetivo explorar as aplicações da congruência modular na resolução de equações diofantinas lineares, com foco em casos específicos onde essas

ferramentas proporcionam soluções eficientes. A Aritmética Modular, seus conceitos e propriedades contribuem para a dinâmica da vida moderna, onde ela é utilizada, por exemplo, nos diferentes códigos numéricos de identificação, como verificar se o número de Cadastro de Pessoa Física (CPF) está correto, já que todos os algarismos que compõem o número original são utilizados no método de geração do código verificado. Percebe-se claramente o frequente uso de congruência modular, cuja aplicação produz efeitos positivos no cotidiano das pessoas, embora grande parte delas não se dê conta de que a matemática esteja sendo empregada.

A presente dissertação está organizada em uma estrutura composta por introdução, quatro capítulos centrais, considerações finais e referências bibliográficas.

No Capítulo 1, será apresentado um breve histórico sobre a vida e obra de Diofanto de Alexandria, com destaque para sua principal obra, Aritmética, uma coleção de treze livros. Também serão abordadas as contribuições de Carl Friedrich Gauss, enfatizando aspectos fundamentais de sua trajetória, suas descobertas mais relevantes e o impacto que exerceram no pensamento matemático moderno. Além disso, será traçado um panorama histórico da origem e da construção do sistema decimal ao longo do tempo, com destaque para o surgimento dos números inteiros.

No Capítulo 2, serão discutidos o conjunto dos números inteiros, suas operações e propriedades, os números primos e os critérios de divisibilidade para números primos e compostos. Além disso, serão explorados o Mínimo Múltiplo Comum (mmc) e o Maior Divisor Comum (mdc), com a apresentação do algoritmo de Euclides.

No Capítulo 3, são apresentadas as definições das equações diofantinas e da congruência modular, destacando esta última como um recurso prático e relevante na resolução de problemas que envolvem equações diofantinas com duas incógnitas. Além disso, são enunciadas suas propriedades fundamentais e operações associadas. Para ilustrar a aplicação desses conceitos, são resolvidos exemplos utilizando tanto o algoritmo de Euclides quanto a congruência modular.

Por fim, no Capítulo 4, apresenta-se a proposta do produto educacional, que consiste em um plano de aula acompanhado de três jogos matemáticos: "Jogo das Equações Diofantinas com Cartas ou Dados", "Desafio Diofantino" e "Diofantus: O Enigma dos Números". Esses jogos são propostos como ferramentas pedagógicas para o ensino das equações diofantinas, proporcionando uma abordagem interativa e eficaz na assimilação dos conceitos abordados nesta dissertação. Os dois primeiros jogos têm como foco os conceitos fundamentais das equações diofantinas, incluindo a identificação dos coeficientes, a verificação da existência de soluções e a formulação de soluções particulares e gerais. O terceiro jogo, por sua vez, apresenta questões contextualizadas e desafiadoras, alinhadas a avaliações acadêmicas amplamente utilizadas no Brasil, como o Exame Nacional do Ensino Médio (Enem), a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), vestibulares e o Sistema de Avaliação da Educação Básica (Saeb). Dessa forma,

além de favorecer a consolidação do aprendizado sobre equações diofantinas e congruência modular, a proposta busca contribuir para a melhoria do desempenho dos estudantes nessas avaliações.

Capítulo

1

Um Breve Relato Histórico Sobre a Teoria dos Números

Ao longo da história, os números não apenas serviram como instrumentos de contagem, mas também refletiram a evolução do pensamento matemático e das civilizações que os estudaram. Desde os primeiros registros numéricos em culturas antigas até os avanços mais abstratos da matemática moderna, sua interpretação e aplicação transformaram-se profundamente. Neste capítulo, apresentaremos um pouco da história dos números e as contribuições de Diofanto de Alexandria e Carl Friedrich Gauss para a teoria dos números. Nossa abordagem é fundamentada principalmente nas referências como Bombelli [2], Boyer [3], Eves [10], Ifrah [16], Roque [25] e Roque e Pitombeira [26].

1.1 Números ao longo dos anos

Os Parâmetros Curriculares Nacionais (BRASIL, 1998) destacam um aspecto relevante da história da matemática, o qual pode ser integrado ao conteúdo:

> "Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor tem a possibilidade de desenvolver atitudes e valores mais favoráveis do aluno frente ao conhecimento matemático. Além disso, conceitos abordados em conexão com sua história constituem-se em veículos de informação cultural, sociológica e antropológica de grande valor formativo. A História da Matemática é, nesse sentido, um instrumento de resgate da própria identidade cultural" (BRASIL, 1998, p. 42).

Dessa forma, o uso de elementos históricos pode contribuir para uma abordagem

mais humanizada dos conteúdos matemáticos ensinados em sala de aula.

A origem dos números é um tema que permanece envolto em mistério, uma vez que não há registros precisos sobre o período ou o indivíduo responsável pelo desenvolvimento desse conceito fundamental. É plausível, no entanto, hipotetizar que a matemática tenha surgido em resposta às necessidades práticas da vida cotidiana. As primeiras manifestações matemáticas provavelmente surgiram para auxiliar na contagem, no comércio e no controle de recursos essenciais à sobrevivência. Os números podem ter se originado no período Paleolítico, também conhecido como Idade da Pedra Lascada. Durante essa era, os seres humanos se refugiavam em cavernas, nas quais faziam marcas em varas ou desenhos nas paredes, frequentemente utilizados para registrar informações relacionadas à caça e à coleta. Esse tipo de prática remonta a mais de trinta mil anos e está diretamente ligado à organização das atividades humanas primárias, como a gestão de alimentos e o cuidado com os animais.

À medida que as sociedades antigas, como as civilizações egípcia, babilônica e suméria, se estruturavam, as necessidades de contabilidade e registro de propriedades levaram ao desenvolvimento de sistemas numéricos mais sofisticados. Essas civilizações inovaram em sistemas de notação matemática, fundamentais para o gerenciamento de propriedades e trocas comerciais. Embora os números inteiros ainda não fossem plenamente desenvolvidos, as bases para sua compreensão estavam sendo estabelecidas à medida que os povos antigos reconheciam a necessidade de expressar quantidades positivas e negativas em suas interações cotidianas (IFRAH, 1985).

Foi na China, há mais de dois mil anos, que os matemáticos começaram a desenvolver conceitos de números negativos e suas regras operatórias. Inicialmente, esses números eram utilizados para representar débitos e dívidas. Posteriormente, essa prática foi assimilada pela matemática hindu, que incorporou e sistematizou as regras de sinais, contribuindo de forma fundamental para a consolidação do conceito de números negativos na matemática mundial.

Acredita-se que os primeiros estudos sobre Teoria dos Números tenham sido iniciados pelos egípcios e babilônios. No entanto, foi com Pitágoras (580-500 a.C., aproximadamente) e os membros de sua escola, conhecidos como pitagóricos, que essa área começou a se desenvolver de forma mais estruturada. Eles estabeleceram diversas conexões entre os números e conceitos do cotidiano, com o objetivo de fundamentar e expandir os argumentos filosóficos da época.

A Aritmética, ao longo da história, foi moldada pelas contribuições de diversos teóricos matemáticos, tendo como principal marco inicial a obra "Os Elementos", de Euclides (aproximadamente 300 a.C.) que lançou as bases para o estudo sistemático dos números.

> "Frequentemente, se pensa, erradamente, que Os elementos de Euclides só tratam de geometria. (...) três livros (VII, VIII e IX) são dedicados à teoria

> dos números. A palavra "número" para os gregos sempre se referia ao que chamamos números naturais – os inteiros positivos." (BOYER, 1996, p. 78).

1.2 Diofanto de Alexandria

Durante o período conhecido como "Segunda Idade Alexandrina"ou "Idade da Prata", que abrange aproximadamente os anos 250 a 350 d.C., emergiu o matemático Diofanto de Alexandria, vide Figura 1.1. Amplamente reconhecido como o "Pai da Álgebra", conforme Boyer, Diofanto exerceu uma profunda influência sobre matemáticos europeus que mais tarde se dedicariam ao desenvolvimento da Teoria dos Números.

> "Se pensarmos primariamente em termos de notação, Diofanto tem boas razões para pretender o título de pai da álgebra, mas em termos de motivação e conceitos a pretensão é menos justificada." (BOYER, 1996, p. 123).

Considerado um dos maiores algebristas da antiguidade grega, pouco se sabe com precisão sobre a nacionalidade de Diofanto ou o período exato em que viveu. Embora existam algumas evidências indiretas que sugerem que Diofanto possa ter sido contemporâneo de Herão, a maioria dos historiadores o situa no século III d.C., apontando Alexandria como o centro de sua atividade intelectual. Diofanto (Diophantus) tem o seu nome ligado à cidade que foi o maior centro de atividade matemática na Grécia antiga: Alexandria. Nenhuma outra cidade foi o centro de atividade matemática por tanto tempo. Através de manuscritos que citam o seu nome ou sua obra é que se pode deduzir em que época ele existiu. Diofanto é autor de três importantes obras: Aritmética, sua obra mais significativa, da qual sobreviveram seis dos treze livros originais; Sobre Números Poligonais, do qual restou apenas um fragmento; e Porismas, que se perdeu. A obra Aritmética foi amplamente estudada e comentada ao longo dos séculos, e a primeira iniciativa documentada para traduzir o texto original grego ocorreu em 1463, quando o matemático *Regiomontanus*, ao descobrir um exemplar da obra em Pádua, solicitou sua tradução.

A *Aritmética* é uma obra que apresenta uma abordagem analítica da teoria algébrica dos números racionais, consolidando Diofanto como um dos maiores gênios em seu campo. O primeiro livro da obra dedica-se ao estudo das equações determinadas em uma incógnita, enquanto os demais abordam as equações indeterminadas de segundo grau e, em alguns casos, de grau superior, com duas ou três incógnitas. Diofanto restringia-se a admitir soluções dentro dos números racionais positivos e, em sua maioria, buscava uma única solução para cada problema.

Os problemas algébricos indeterminados, nos quais se busca apenas soluções racionais, passaram a ser conhecidos como problemas diofantinos. No entanto, o uso contemporâneo dessa terminologia frequentemente impõe a restrição de que as soluções sejam inteiras.

Figura 1.1: Diofanto de Alexandria.

Uma outra tradução, com muitos comentários e méritos, foi feita em 1575 por Xilander (nome grego adotado pelo professor da Universidade de Heidelberg, Wilhelm Holzmann). Essa mesma tradução, foi usada pelo francês Bachet de Méziriac, em 1621, que publicou a primeira edição do texto em grego juntamente com uma tradução latina acompanhada de notas. Uma segunda edição apareceu em 1670, impressa de maneira negligente, mas apesar disso, é historicamente importante por conter as famosas notas marginais de Fermat que tanto estimularam as pesquisas em Teoria dos Números. Mais tarde apareceram traduções para o francês, alemão e inglês.

De acordo com Roque (2012), a contribuição mais notória de Diofanto consiste na introdução de uma forma de representação para o valor desconhecido em um problema, denominado por ele como arithmos, termo que deu origem à palavra "aritmética".

A Aritmética de Diofanto distingue-se consideravelmente das obras matemáticas anteriores, apresentando-se como um tratado de notável sofisticação e engenhosidade. Embora, à primeira vista, possa ser comparada aos grandes clássicos da Idade Alexandrina, ela se afasta profundamente das abordagens convencionais e da matemática grega tradicional. Diferente dos métodos algébricos empregados anteriormente, a obra de Diofanto inaugura uma nova vertente, utilizando técnicas que guardam semelhanças com a álgebra babilônica em diversos aspectos. No entanto, enquanto os matemáticos babilônicos focavam na obtenção de soluções aproximadas para equações de até terceiro grau, o trabalho de Diofanto é amplamente dedicado à resolução exata de equações, tanto determinadas quanto indeterminadas.

Um enigma que estava junto dos seus restos mortais, denotava que Diofanto viveu até os 84 anos. Segundo dizem, esse enigma teria sido gravado por seu amigo, Metrodorus, cujo resultado revela a idade de Diofanto. O enigma dizia o seguinte:

"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 ". (BOYER, 1996)

Outra forma de enunciar este 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-lhe um filho que morreu 4 anos antes de seu pai, com metade da idade (final) de seu pai".

A equação que resolve tal enigma será:

$$\frac{X}{6} + \frac{X}{12} + \frac{X}{7} + 5 + \frac{X}{2} + 4 = X$$

Considerando-se a veracidade de tal enigma, concluímos que Diofanto viveu por 84 anos, mas não deve ser tomado como um problema típico dos que interessavam ao matemático, pois este deu pouca atenção às equações do primeiro grau.

Diofanto é famoso por suas investigações em equações que agora conhecemos como "Equações Diofantinas", que são equações polinomiais com soluções inteiras ou racionais. Ele introduziu uma abordagem algébrica que estava muito à frente de seu tempo, desenvolvendo métodos para resolver certos tipos de equações indeterminadas, ou seja, aquelas que possuem múltiplas soluções. Sua obra foi pioneira ao tentar resolver equações usando raciocínio simbólico, embora ele tenha feito isso com uma notação muito mais rudimentar em comparação com a álgebra moderna. Diofanto também é creditado por ter introduzido o conceito de uma potência negativa e o uso de símbolos para representar termos desconhecidos e suas potências, o que foi um passo importante na formalização da álgebra. Assim, o legado de Diofanto está profundamente ligado ao progresso da matemática, particularmente na teoria dos números e na resolução de problemas envolvendo números inteiros e sua obra continua a ser uma fonte de inspiração e desafio para matemáticos ao longo dos séculos.

Sendo assim, não se pode atribuir o desenvolvimento da matemática apenas ao conhecimento de filósofos e matemáticos gregos como Euclides, Arquimedes, Ptolomeu e Diofanto. Há registros tão relevantes e pouco disseminados dessa ciência exata feitos por outras civilizações. No entanto, pela importância histórica, queremos, nesta pesquisa, destacar o trabalho do grego Diofanto, devido à sua relevante contribuição para o estudo de equações com duas incógnitas, tanto que um tipo especial dessas equações carrega hoje o nome de diofantinas.

1.3 Números Inteiros

O avanço no entendimento dos números inteiros ocorreu de forma gradual, com destaque para a obra do matemático italiano Rafael Bombelli (1526-1572). Em sua obra L'Algebra, publicada em 1572, Bombelli formulou as primeiras regras operatórias claras para os números inteiros, desmistificando o uso dos sinais positivo e negativo. Ele apresentou, de maneira prática, como operar com esses números, estabelecendo conceitos fundamentais para o desenvolvimento da álgebra. Através de exemplos como:

> "Mais por mais dá mais; menos por menos dá mais;
>
> mais por menos dá menos; menos por mais dá menos;
>
> mais 8 por mais 8, dá 64; menos 5 por menos 6, dá mais 30;
>
> menos 4 por mais 5, dá menos 20; mais 5 por menos 4, dá menos 20." (HEFEZ, 2022).

Bombelli (1572) não apenas formalizou as regras operatórias, mas também deu estrutura ao entendimento do conceito de número, o que possibilitou o desenvolvimento subsequente da matemática moderna.

Outro avanço significativo na história dos números foi o desenvolvimento do sistema de numeração posicional, originado na Índia por volta do século VII. Esse sistema, difundido para outras regiões do mundo pelos árabes, foi crucial para a evolução dos números inteiros, pois permitiu a representação mais eficiente de grandes quantidades. A introdução do zero, um conceito já utilizado pelos gregos antigos para denotar a ausência de quantidade, foi essencial para a estruturação do sistema de numeração posicional. Na Índia, porém, o zero adquiriu um status de número, sendo integrado ao sistema numérico e expandindo as possibilidades de cálculo e representação numérica.

> "Sabemos que alguns matemáticos indianos, bem como Fibonacci, já propunham interpretar um número negativo como uma perda, no lugar de um ganho. No século XV, Nícolas Chuquet já representava o número negativo -a como 0 - a, o que mostra que o sinal - ainda não era um atributo do número, mas sim a indicação de uma operação." (ROQUE E CARVALHO, 2012)

Dentre os sistemas numéricos antigos, um dos mais notáveis é o sistema sexagesimal, adotado pelos babilônios. Mesmo nos dias de hoje, ele continua sendo utilizado para a representação de medidas de tempo e ângulos, por meio de minutos e segundos.

O sistema decimal que utilizamos, baseado na base 10, de acordo com Abramo Hefez, deriva de uma adaptação do sistema sexagesimal dos babilônios. Esse sistema teve sua origem na China e na Índia, expandindo-se posteriormente pelo Oriente Médio, onde foi amplamente adotado pelos árabes.

1.4 Carl Friedrich Gauss

O desenvolvimento da Aritmética atingiu um ponto culminante no século XVII, com os trabalhos inovadores de Pierre de Fermat (1601-1665), cujas contribuições foram cruciais para o avanço dessa disciplina. Nos séculos XVIII e XIX, outros matemáticos notáveis, como Leonhard Euler (1707-1783) e Carl Friedrich Gauss (1777-1855), vide Figura 1.2, também desempenharam papéis significativos na evolução da Aritmética. É importante destacar que, a partir do século XIX, em decorrência das investigações de Gauss, a Aritmética transforma-se em Teoria dos Números. Essa transição não apenas consolidou a Aritmética como uma disciplina central da matemática, mas também abriu novos caminhos para a pesquisa e a aplicação de conceitos numéricos.

Gauss nasceu em Brunswick, na Alemanha, em 1777. Seu pai, um trabalhador braçal, possuía uma visão rígida e desfavorável em relação à educação. Sua mãe, embora pouco instruída, sempre o incentivou nos estudos e manteve, ao longo de sua vida, um imenso orgulho pelas conquistas do filho. Foi uma das mais notáveis crianças-prodígio, do tipo que surge raramente. Conta-se que, aos três anos de idade, corrigiu um erro aritmético em um rascunho feito por seu pai.

A obra mais influente e sem precedentes de Gauss é a *Disquisitiones Arithmeticae*, um trabalho de importância fundamental para a teoria dos números moderna. Nesse estudo, Gauss apresenta descobertas notáveis sobre a construção de polígonos regulares, além de introduzir uma notação simples para congruência.

Figura 1.2: Carl Friedrich Gauss

"Os grandes músicos podem ser divididos em intérpretes ou compositores brilhantes e poucos são ambas as coisas. Analogamente, os grandes matemáticos

> podem ser divididos em operadores formais ou criadores de teorias brilhantes, e poucos são ambas coisas. Euler foi antes de tudo um grande operador formal, Lagrange foi um grande teórico e Gauss, com grande cintilância, foi ambas as coisas. Assim, Euler seria um Heifetz, Lagrange um Beethoven e Gauss um Johann Sebastian Bach". (EVES, 2004).

Gauss foi o primeiro a apresentar uma demonstração rigorosa do Teorema Fundamental da Álgebra, que já havia sido enunciado por outros matemáticos, mas sem uma prova completa.

> "Gauss teve o poder de mudar os rumos da matemática a partir dos seus trabalhos revolucionários, apresentados com extremo rigor e grande concisão e elegância. Por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um príncipe da rainha das ciências." (HEFEZ, 2016).

A história dos números inteiros está intrinsecamente ligada ao avanço das civilizações humanas e à resolução de problemas práticos, desde a contagem de recursos no período Paleolítico até a navegação avançada durante a Era dos Descobrimentos. A evolução do conceito de números inteiros, de sua forma primitiva até sua formalização na matemática moderna, reflete as necessidades sociais, comerciais e científicas de cada período histórico. A interação entre matemática e navegação, especialmente no uso de coordenadas geográficas e trigonometria esférica, destaca o papel central dos números inteiros na história do conhecimento humano e em suas aplicações práticas.

Capítulo

2

Aritmética dos Números Inteiros

Neste capítulo, exploraremos os principais aspectos do conjunto dos números inteiros, incluindo suas operações, propriedades e critérios de divisibilidade. Além disso, abordaremos o estudo dos números primos, bem como o cálculo do Mínimo Múltiplo Comum (mmc) e do Máximo Divisor Comum (mdc), destacando suas aplicações práticas. Tais conceitos são baseados em Bezerra [1], Domingues [7] e [8], Filho [11], Hefez [13] e Jurkiewicz [17].

2.1 O Conjunto dos Números Inteiros

O conjunto dos números inteiros, usualmente denotado pela letra $\mathbb{Z}$, é um dos conjuntos numéricos fundamentais da matemática com características particulares. Ele é composto pelos inteiros negativos, o zero e os inteiros positivos, ou seja,

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

A notação $\mathbb{Z}$ tem origem na palavra alemã *Zahlen*, que significa números. Esse conjunto se estende infinitamente em ambas as direções, abrangendo tanto os inteiros negativos quanto os positivos. Assim, ele é um exemplo clássico de um conjunto infinito.

Os inteiros surgem em diversas áreas, como na contagem de objetos, na representação de dívidas ou perdas, e nas medições de quantidades discretas. Além disso, o conjunto dos inteiros é fechado para as operações de adição e multiplicação, o que significa que, ao realizar essas operações entre dois inteiros quaisquer, o resultado será sempre um número pertencente a $\mathbb{Z}$.

O conjunto $\mathbb{Z}$, juntamente com essas duas operações, possui algumas propriedades, apresentadas aqui como axiomas, ou seja, assumiremos tais propriedades como verdadeiras, não sendo necessário demonstrá-las.

2.2 Adição de Números Inteiros

A adição dos números inteiros é uma operação fundamental no conjunto dos inteiros $\mathbb{Z}$, preservando sua integridade, pois a soma de quaisquer dois inteiros $a, b \in \mathbb{Z}$ resulta sempre em outro inteiro, ou seja, $a + b \in \mathbb{Z}$. Isso garante que o conjunto dos inteiros é fechado em relação à adição.

A operação de adição obedece a diversas propriedades fundamentais que são essenciais para o entendimento de operações mais complexas na matemática.

2.2.1 Axiomas da Adição de Números Inteiros

1. **A adição é comutativa**: A soma de dois números inteiros independe da ordem dos termos. Em outras palavras, alterar a ordem dos números que estão sendo somados não muda o resultado. Dessa forma, para $a, b \in \mathbb{Z}$, temos que

$$a + b = b + a.$$

Por exemplo,

$$4 + (-5) = -5 + 4 = -1.$$

2. **A adição é associativa**: Ao somar três ou mais números inteiros, a forma como os números são agrupados (colocados entre parênteses) não altera o resultado da soma. Mais precisamente, dados os números inteiros a, b e c, a propriedade

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

Veja esse exemplo numérico:

$$(5 + 3) + (-4) = 5 + (3 + (-4)) = 4.$$

3. **Existência e unicidade do elemento neutro da adição**: O número zero, denotado por 0, é o elemento neutro para a adição, pois somá-lo a qualquer número inteiro não altera o valor desse número, ou seja,

$$a + 0 = a,$$

qualquer que seja o inteiro a. Por exemplo:

$$6 + 0 = 6.$$

4. **Existência e unicidade do oposto (inverso aditivo)**: Todo número inteiro possui um oposto, que é o número que, quando somado a ele, resulta no elemento neutro

0. O oposto de um número a é $-a$. Assim,

$$a + (-a) = (-a) + a = 0.$$

Como exemplo, temos que o elemento oposto de 7 é -7 e vale:

$$7 + (-7) = 0$$

É importante observar que o elemento oposto de -7 é 7, o que implica em $-(-7) = 7$. Em geral, vale que $-(-a) = a$ para todo $a \in \mathbb{Z}$.

Exemplos adicionais:

Exemplo 2.1. Considere a adição de dois números inteiros, $7 + (-3)$. Aqui, somar -3 a 7 significa mover 3 unidades para a esquerda na reta numérica, resultando em $7 - 3 = 4$.

Exemplo 2.2. Se somarmos dois números negativos, como $(-3) + (-6)$, o resultado será a soma dos valores absolutos com o sinal negativo, ou seja, $-(3 + 6) = -9$.

Esses axiomas ilustram como a adição de números inteiros é estruturada de forma consistente, oferecendo uma base sólida para o estudo de outras operações e conceitos em álgebra e teoria dos números.

2.3 Multiplicação de Números Inteiros

Dados $a, b \in \mathbb{Z}$, denotamos o produto (ou multiplicação) por $a \cdot b \in \mathbb{Z}$. Além dessa notação, também são comumente utilizadas $a \cdot b$ e ab. A multiplicação de números inteiros é uma operação fundamental que também é fechada em $\mathbb{Z}$, ou seja, o produto de quaisquer dois números inteiros é sempre um número inteiro. Além disso, a multiplicação compartilha diversas propriedades com a adição, embora apresente algumas características específicas.

2.3.1 Axiomas da Multiplicação de Números Inteiros

1. **A multiplicação é comutativa**: A ordem dos fatores não altera o produto. Em outras palavras, multiplicar dois números inteiros em qualquer ordem resulta no mesmo valor, ou seja,

$$a \cdot b = b \cdot a,$$

para quaisquer inteiros a e b. Por exemplo:

$$4 \cdot (-5) = (-5) \cdot 4 = -20.$$

2. **A multiplicação é associativa**: O agrupamento dos fatores em uma multiplicação com três ou mais números inteiros não altera o produto. Assim, dados $a, b, c \in \mathbb{Z}$, temos que

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Veja o exemplo:

$$(5 \cdot 3) \cdot (-4) = 5 \cdot (3 \cdot (-4)) = -60.$$

3. **Existência e unicidade do elemento unidade**: O número 1 é o elemento neutro da multiplicação. Qualquer número inteiro multiplicado por 1 resulta no próprio número, isto é,

$$a = a,$$

para todo número inteiro a. Por exemplo:

$$9 \cdot 1 = 9.$$

4. **Elemento Nulo (Propriedade do Zero)**: Qualquer número inteiro multiplicado por 0 resulta em 0. Em símbolos

$$a \cdot 0 = 0$$

para todo número inteiro a. Veja esse exemplo:

$$3 \cdot 0 = 0.$$

5. **Propriedade Distributiva**: A multiplicação de um número inteiro em relação à adição ou subtração de inteiros distribui-se sobre os termos. Dessa forma, para $a, b, c \in \mathbb{Z}$, temos que

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{e} \quad a \cdot (b - c) = a \cdot b - a \cdot c.$$

Exemplo:

$$3 \cdot (3 + 4) = 3 \cdot 3 + 3 \cdot 4 = 9 + 12 = 21.$$

2.3.2 Sinais na Multiplicação

Quando multiplicamos dois números inteiros com o mesmo sinal, o resultado é positivo.

$$(-6) \cdot (-4) = 24 \quad \text{e} \quad 6 \cdot 4 = 24.$$

Quando multiplicamos dois números inteiros com sinais diferentes, o resultado é negativo.

$$(-5) \cdot 4 = -20 \quad \text{e} \quad 5 \cdot (-4) = -20.$$

Exemplo 2.3. Multiplicando dois números positivos, temos:

$$7 \cdot 5 = 35.$$

O produto de dois números inteiros positivos é sempre positivo.

Exemplo 2.4. Multiplicando números com sinais diferentes, temos:

$$(-8) \cdot 2 = -16.$$

Nesse caso, o resultado é negativo porque os sinais dos números são opostos.

Exemplo 2.5. O produto de dois números negativos, como:

$$(-9) \cdot (-4) = 36,$$

resulta em um número positivo, uma vez que o produto de dois números com o mesmo sinal é sempre positivo.

2.3.3 Regra dos Sinais

Sejam a e b inteiros. Então vale:

1. $-(-a) = a$
2. $(-a) \cdot b = -(ab) = a \cdot (-b)$
3. $(-a) \cdot (-b) = ab$

Demonstração: Notamos inicialmente que podemos interpretar o axioma **Existência do Oposto:** para cada inteiro a existe um único elemento que chamaremos oposto de a e indicaremos por $-a$, tal que:

$$a + (-a) = 0.$$

da seguinte forma: o oposto de um elemento a é o único inteiro que verifica a equação $a + x = 0$. Para provar o item 1, basta observar que a verifica a equação

$$(-a) + x = 0.$$

Consequentemente, a é o oposto de $-a$ (que é o elemento indicado por $-(-a)$).
Para provar a primeira igualdade do item 2, basta observar que $(-a)b$ é a solução de

$ab + x = 0$, já que:

$$ab + (-a)b = [(-a) + a]b = 0 \cdot b = 0.$$

Analogamente, verifica-se que:

$$ab + a(-b) = 0.$$

Para o item 3, podemos observar diretamente que, aplicando o item 2, temos:

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(ab)).$$

Assim, usando também o item 1 no último termo, segue que:

$$(-a) \cdot (-b) = ab.$$

2.4 Divisão de Números Inteiros

Como a divisão de um número inteiro por outro nem sempre resulta em um número inteiro, utiliza-se a relação de divisibilidade para expressar quando essa divisão é exata.

Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. 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. Observe que a notação $a \mid b$ (a divide b) não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c inteiro tal que $b = ca$. A negação dessa sentença é representada por $a \nmid b$ (a não divide b), significando que não existe nenhum número c tal que $b = ca$.

Quando $b = a \cdot c$, definimos a operação de divisão $b \div a = c$. Como exemplo, considere $3 \mid 12$, pois $12 = 3 \cdot 4$. Pela definição de divisão, isso implica que $12 \div 3 = 4$.

2.4.1 Propriedades da Divisão de Números Inteiros

1. **Não Fechada:** A divisão não é uma operação fechada no conjunto dos números inteiros. Isso significa que, ao dividir dois inteiros, o resultado nem sempre será um número inteiro.

$$8 \div 3 = \frac{8}{3} \quad \text{(que não é um número inteiro).}$$

2. **Não Comutativa:** A divisão não é comutativa, ou seja, a ordem dos fatores altera o resultado.

$$10 \div 2 = 5, \quad \text{mas} \quad 2 \div 10 = \frac{1}{5}.$$

3. **Não Associativa:** A divisão, assim como a subtração, não é uma operação

associativa, pois a mudança na ordem do agrupamento dos termos pode alterar o resultado.

$$(32 \div 4) \div 2 = 8 \div 2 = 4, \quad \text{mas} \quad 32 \div (4 \div 2) = 32 \div 2 = 16.$$

4. **Elemento Neutro (Identidade da Divisão):** O número 1 é o elemento neutro para a divisão. Dividir qualquer número por 1 resulta no próprio número.

$$17 \div 1 = 17.$$

5. **Elemento Nulo (Propriedade do Zero):** Dividir 0 por qualquer número diferente de zero resulta em 0, pois $0 = a \cdot 0$ para todo $a \in \mathbb{Z}$.

$$0 \div 8 = 0.$$

No entanto, não é possível dividir por zero. A divisão por zero é indefinida e não tem significado dentro da aritmética.

$$9 \div 0 \quad \text{é indefinido.}$$

De fato, se fosse possível escrever $9 \div 0 = n$, com $n \in \mathbb{Z}$, então pela definição de divisão, segue que $9 = 0 \cdot n = 0$, o que é falso.

2.4.2 Sinais na Divisão

Quando dividimos dois números inteiros com o mesmo sinal, o resultado é positivo. Por exemplo,

$$(-16) \div (-4) = 4 \quad \text{e} \quad 16 \div 4 = 4.$$

Quando dividimos dois números inteiros com sinais diferentes, o resultado é negativo. Por exemplo,

$$(-16) \div 4 = -4 \quad \text{e} \quad 16 \div (-4) = -4.$$

Exemplo 2.6. $10 \div 2 = 5$. Aqui, o resultado é um número inteiro porque 2 divide 10 exatamente 5 vezes.

Exemplo 2.7. $7 \div 2 = \frac{7}{2} = 3,5$. Neste caso, o resultado não é um número inteiro, evidenciando que a divisão de dois inteiros pode resultar em um número fracionário.

Exemplo 2.8. $(-8) \div (-2) = 4$. A divisão de dois números inteiros negativos resulta em um número positivo.

Exemplo 2.9. $15 \div (-3) = -5$. A divisão de um número positivo por um número negativo resulta em um número negativo.

2.5 Critérios de Divisibilidade

A aritmética modular, também conhecida como aritmética dos restos, fundamenta-se na divisão de um número inteiro por outro, estabelecendo uma relação de divisibilidade entre eles.

Para começar o estudo sobre divisibilidade, é fundamental compreender o conceito de divisor. Lembrando que o inteiro a é divisor do inteiro b e denotamos $a \mid b$, quando existe um inteiro c tal que $c \cdot a = b$. Em notação formal:

$$a \mid b \iff (\exists\, c \in \mathbb{Z} \mid c \cdot a = b).$$

Quando a é divisor de b, dizemos que "b é divisível por a" ou que "b é múltiplo de a".

Propriedades da Divisibilidade: Vamos estabelecer algumas propriedades da divisibilidade. A demonstração pode ser consultada em Hefez [11] e [12].

Proposição 2.1. *Sejam a, b e $c \in \mathbb{Z}$. Temos que:*

I. $1 \mid a$, $a \mid a$ *e* $a \mid 0$;

II. Se $a \mid 1$, *então* $a = \pm 1$;

III. Se $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$;

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

V. Se $a \mid b$, *com* $b \neq 0$, *então* $|a| \leq |b|$;

VI. $0 \mid a \iff a = 0$;

VII. a *divide* b *se, e somente se,* $|a|$ *divide* $|b|$;

VIII. Se $a \mid b$ *e* $b \mid c$, *então* $a \mid c$;

IX. Se $a \mid b$ *e* $a \mid c$, *então* $a \mid (bx + cy)$, *para todo* $x, y \in \mathbb{Z}$;

X. Se $a \mid (b \pm c)$, *então* $a \mid b \iff a \mid c$.

Algumas regras nos permitem determinar se um número $n \in \mathbb{Z}$ é divisível ou não por outro, e evidentemente, a um custo bem menor que efetuar a divisão. Dessa forma, as congruências associadas à escrita de todo número $n = a_r \ldots a_2 a_1 a_0$ em sua forma decimal

$$n = a_r 10^r + \cdots + a_2 10^2 + a_1 10^1 + a_0$$

é uma ferramenta muito útil na determinação dos critérios de divisibilidade. Descreveremos a seguir algumas dessas regras.

Divisibilidade por 2 e por 5

Considerando a escrita decimal de n, podemos colocar 10 em evidência a partir do algarismo das dezenas e escrever:

$$n = \left(a_r 10^{r-1} + \cdots + a_2 10^1 + a_1\right) 10 + a_0,$$

onde a_0 é o algarismo das unidades. Observando que, no segundo membro, o primeiro valor é divisível por 2, 5 e 10. Portanto, para um n qualquer, sua divisão por 5 ou por 2 só dependerá do seu algarismo das unidades e, dessa forma, temos dois casos a considerar:

Divisibilidade por 5: Se a_0 for 0 ou 5, n é divisível por 5, logo: todo número que termina em 0 ou 5 é divisível por 5.

Exemplo 2.10. Os números 935, 140, 85 e 70 são todos divisíveis por 5, pois terminam em 0 ou 5. Já os números 357, 121, 92 e 551, por exemplo, não são divisíveis por 5, pois não terminam em 0 ou 5.

Divisibilidade por 2: Se a_0 for 0, 2, 4, 6 ou 8, n é divisível por 2, logo: todo número que termina em 0, 2, 4, 6 ou 8 é divisível por 2.

Exemplo 2.11. O número 438 é divisível por 2, pois termina em 8, que é um número par.

Divisibilidade por 3

Um número inteiro é divisível por 3 se a soma dos seus dígitos for divisível por 3. Isso ocorre porque qualquer potência de 10 quando dividido por 3 deixa resto 1. O critério pode ser aplicado a qualquer número, independentemente do seu tamanho. Se a soma dos dígitos resultar em um número que seja múltiplo de 3, então o número original também será divisível por 3. Deixamos a demonstração desse fato no Exemplo 3.11.

Exemplo 2.12. Considere o número 573. A soma dos dígitos é $5 + 7 + 3 = 15$. Como 15 é divisível por 3, o número 573 também é divisível por 3.

Exemplo 2.13. Para o número 821, a soma dos dígitos é $8 + 2 + 1 = 11$. Como 11 não é divisível por 3, o número 821 não é divisível por 3.

Divisibilidade por 9

O critério de divisibilidade por 9 é análogo ao critério de divisibilidade por 3, devido ao fato que toda potência de 10 quando dividida por 9 também deixa resto 1. No caso da divisibilidade por 9, a soma dos dígitos deve ser divisível por 9.

Exemplo 2.14. Considere o número 486. A soma dos dígitos é $4+8+6=18$. Como 18 é divisível por 9, o número 486 é divisível por 9.

Exemplo 2.15. Para o número 731, a soma dos dígitos é $7+3+1=11$. Como 11 não é divisível por 9, o número 731 não é divisível por 9.

Divisibilidade por 4

Um número inteiro é divisível por 4 se os dois últimos dígitos desse número formarem um número que seja divisível por 4. Essa regra se deve ao fato de que o número 100 (a base dos números de três dígitos ou mais) é divisível por 4, portanto, apenas os dois últimos dígitos influenciam a divisibilidade por 4. Em outras palavras, não é necessário verificar o número completo, basta observar os dois últimos dígitos. Para a demonstração, veja o Exemplo 3.12.

Exemplo 2.16. Considere o número 1324. Os dois últimos dígitos são 24, e como 24 é divisível por 4, o número 1324 também é divisível por 4.

Exemplo 2.17. Para o número 751, os dois últimos dígitos são 51. Como 51 não é divisível por 4, o número 751 também não é divisível por 4.

Esse critério é especialmente útil para números grandes, permitindo uma verificação rápida da divisibilidade por 4 com base em uma pequena parte do número.

Divisibilidade por 8

O critério de divisibilidade por 8 é semelhante ao critério de divisibilidade por 4, mas, ao invés de observar os dois últimos dígitos, analisamos os três últimos dígitos do número. Um número é divisível por 8 se os seus três últimos dígitos formarem um número que seja divisível por 8. Isso ocorre porque o número 1000 (a base dos números de quatro dígitos ou mais) é divisível por 8. Para a demonstração, veja o Exemplo 3.13.

Exemplo 2.18. Considere o número 54816. Os três últimos dígitos são 816. Como $816 \div 8 = 102$, que é um número inteiro, o número 54816 é divisível por 8.

Exemplo 2.19. Para o número 7329, os três últimos dígitos são 329. Como $329 \div 8$ não resulta em um número inteiro, o número 7329 não é divisível por 8.

Este critério permite uma verificação rápida da divisibilidade por 8, especialmente em números compostos por mais algarismos. O foco nos três últimos dígitos simplifica o processo, tornando-o eficiente e direto.

Divisibilidade por 6

Um número é divisível por 6 se ele for divisível tanto por 2 quanto por 3. Ou seja, um número deve ser par (critério de divisibilidade por 2) e a soma de seus dígitos deve ser divisível por 3 (critério de divisibilidade por 3). Esta regra é derivada do fato de que 6 é o produto dos números 2 e 3, de modo que um número divisível por 6 deve satisfazer simultaneamente os critérios desses dois divisores.

- **Divisível por 2:** O número é par, ou seja, termina em 0, 2, 4, 6 ou 8.
- **Divisível por 3:** A soma dos dígitos do número é divisível por 3.

Exemplo 2.20. Considere o número 354. Para verificar sua divisibilidade por 6, aplicamos o critério que exige que o número seja divisível simultaneamente por 2 e por 3. Primeiramente, o número 354 é divisível por 2, pois seu último dígito, 4, é par. Em seguida, para testar a divisibilidade por 3, somamos seus dígitos: $3 + 5 + 4 = 12$. Como 12 é divisível por 3 ($12 \div 3 = 4$), concluímos que 354 é também divisível por 3. Assim, como 354 é divisível por 2 e por 3, podemos afirmar que ele é divisível por 6.

Exemplo 2.21. Considere o número 245. Para verificar sua divisibilidade por 6, começamos aplicando o critério de divisibilidade por 2, que estabelece que um número é divisível por 2 se, e somente se, seu último dígito for par. No caso do número 245, o último dígito é 5, que é ímpar. Portanto, 245 não é divisível por 2. Como a divisibilidade por 2 é uma condição necessária para que um número seja divisível por 6, concluímos que 245 não pode ser divisível por 6, independentemente de examinarmos a divisibilidade por 3. A falta de divisibilidade por 2 é suficiente para afirmar que 245 não atende ao critério de divisibilidade por 6.

Divisibilidade por 7

O critério de divisibilidade por 7 pode ser aplicado de várias maneiras. Um método comum envolve a manipulação dos dígitos do número para verificar sua divisibilidade por 7. Um dos métodos mais práticos consiste em dobrar o último dígito do número, subtraí-lo do número formado pelos demais dígitos, e verificar se o resultado é divisível por 7. Esse processo pode ser repetido até que se obtenha um número fácil de verificar.

Exemplo 2.22. Considere o número 161. O último dígito é 1. Dobramos 1 para obter 2 e subtraímos de 16 (os demais dígitos), resultando em $16 - 2 = 14$. Como 14 é divisível por 7, o número 161 também é divisível por 7.

Exemplo 2.23. Para o número 672, o último dígito é 2. Dobramos 2 para obter 4 e subtraímos de 67 (os demais dígitos), resultando em $67 - 4 = 63$. Como 63 é divisível por 7, o número 672 também é divisível por 7.

Este método pode ser repetido até que se chegue a um número pequeno, facilitando a verificação da divisibilidade por 7. Embora um pouco mais trabalhoso, esse critério pode ser usado para números de qualquer tamanho.

Divisibilidade por 7: Um novo método?

Em novembro de 2019, o jovem Chika Ofili, um estudante nigeriano residente no Reino Unido, recebeu reconhecimento por propor um novo critério de divisibilidade pelo número 7. Com apenas 12 anos de idade, Ofili desenvolveu essa técnica sob a orientação da professora Mary Ellis, chefe do departamento de Matemática da Westminder Under School, no contexto de um trabalho escolar.

A relevância de sua contribuição foi amplamente reconhecida, e ele foi agraciado com o prêmio TruLittle Hero Awards, concedido pela organização Cause4Children Limited. Esse prêmio tem como objetivo homenagear e incentivar realizações excepcionais de crianças e jovens com menos de 17 anos no Reino Unido.

O método sugerido por Ofili estabelece um critério alternativo para verificar a divisibilidade por 7 e pode ser descrito da seguinte maneira: dado um número inteiro qualquer, considera-se seu último dígito, que deve ser multiplicado por 5. O valor obtido é então somado ao número formado pelos demais algarismos do número original. Se o resultado for divisível por 7, então o número inicial também o será.

Para ilustrar essa técnica, consideremos o número $n = 532$. O último algarismo é 2, e os demais formam o número 53. Aplicando a regra, temos:

$$53 + 2 \cdot 5 = 53 + 10 = 63,$$

que é divisível por 7. Logo, 532 também é divisível por 7.

Caso o número obtido após a aplicação do método não permita identificar imediatamente sua divisibilidade por 7, o procedimento pode ser repetido até alcançar um valor que seja reconhecidamente divisível por esse número. Por exemplo, para $n = 987$, aplica-se a regra:

$$98 + (7 \cdot 5) = 98 + 35 = 133.$$

Se a divisibilidade de 133 não for evidente, o processo pode ser repetido:

$$13 + 3 \cdot 5 = 13 + 15 = 28.$$

Como 28 é divisível por 7, conclui-se que 987 também é.

Por que essa "nova" regra funciona?

Proposição 2.2. *O inteiro $n = 10k + a_0$, com $k, a_0 \in \mathbb{Z}$, é divisível por 7 se, e somente se, o inteiro $k + 5a_0$ for divisível por 7.*

Prova: Se $n = 10k + a_0$ for divisível por 7, então:

$$10k + a_0 = 7q, \quad q \in \mathbb{Z}.$$

Daí,

$$\begin{aligned} k + 5a_0 &= k + 5(7q - 10k) \\ &= k + 35q - 50k \\ &= -49k + 35q \\ &= 7(5q - 7k). \end{aligned}$$

Como $r = (5q - 7k) \in \mathbb{Z}$, segue que $k + 5a_0$ é divisível por 7. Reciprocamente, se $k + 5a_0$ for divisível por 7, então:

$$k + 5a_0 = 7q, \quad q \in \mathbb{Z}.$$

Daí,

$$\begin{aligned} 10k + a_0 &= 10(7q - 5a_0) + a_0 \\ &= 70q - 50a_0 + a_0 \\ &= 7(10q - 7a_0). \end{aligned}$$

Como $s = (10q - 7a_0) \in \mathbb{Z}$, concluímos que $10k + a_0$ é divisível por 7.

O caso de Chika Ofili chamou atenção porque ele conseguiu redescobrir de maneira independente e intuitiva, sem o conhecimento de publicações acadêmicas, um critério de divisibilidade por 7. No entanto, é importante destacar que já existem diversos artigos sobre critérios de divisibilidade, incluindo publicações da RPM (Revista do Professor de Matemática). Em particular, a edição nº 12 dessa revista já mencionava esse mesmo critério de divisibilidade por 7.

O artigo da RPM nº 12, intitulado **"Outros critérios de divisibilidade"**, de autoria de Mário Gustavo Pinto Guedes, já abordava o critério de divisibilidade por 7, o que antecede a "descoberta" de Chika Ofili.

2.6 Números Primos

Um conjunto fundamental na Teoria dos Números é o dos números primos. Um número primo pode ser definido como um número natural maior que 1 que possui exatamente dois divisores positivos: 1 e ele mesmo.

Definição 2.1. *Um inteiro $p > 1$ é chamado número primo se não possui um divisor d satisfazendo $1 < d < p$. Se um inteiro $a > 1$ não é primo, ele é chamado de número*

composto.

O seguinte teorema é o alicerce dos fundamentos dos números inteiros, conhecido como Teorema Fundamental da Aritmética.

Teorema 2.1. *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração: Com efeito, se n é primo, nada há que demonstrar, e se n é composto, então, n possui um divisor primo p_1 em sua decomposição e é do tipo:

$$n = p_1 n_1, \quad \text{com } 1 < n_1 < n \tag{2.1}$$

Se n_1 é primo, então a igualdade (2.1) representa n como produto de fatores primos, e se, ao invés, n_1 é composto, então n_1 possui um divisor primo p_2, isto é, $n_1 = p_2 n_2$, e temos:

$$n = p_1 p_2 n_3, \quad \text{com } 1 < n_2 < n_1 \tag{2.2}$$

Se n_2 é primo, então a igualdade (2.2) representa n como produto de fatores primos, e se, ao invés, n_2 é composto, então n_2 possui um divisor primo p_3, isto é, $n_2 = p_3 n_3$, e temos:

$$n = p_1 p_2 p_3 n_3, \quad \text{com } 1 < n_3 < n_2$$

E assim por diante. Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > n_3 \cdots > 1,$$

e como só existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k que é um primo p_k ($n_k = p_k$) e por conseguinte teremos:

$$n = p_1 p_2 p_3 \dots p_k,$$

igualdade que representa o inteiro positivo $n > 1$ como produto de fatores primos.

No Livro IX dos *Elementos*, Euclides apresenta o seguinte resultado:

Teorema 2.2. *Existem infinitos números primos.*

Demonstração: Suponha que exista apenas um número finito de números primos $p_1, p_2, \dots, p_r$. Considere o número natural

$$n = p_1 p_2 p_3 \dots p_r + 1.$$

Temos pelo Teorema 2.1 que o número n possui um fator primo p que deve ser um dos $p_1, p_2, \dots, p_r$ e consequentemente, divide o produto $p_1 p_2 \dots p_r$. Mas, pelo item IX da

Proposição 2.1, isto implica que p divide 1, o que é um absurdo. Portanto, existem infinitos primos.

2.7 Mínimo Múltiplo Comum

Um número inteiro é múltiplo de outro quando é divisível por esse outro número inteiro. O conjunto dos múltiplos de um inteiro qualquer é obtido multiplicando-se esse número por todos os elementos do conjunto dos números inteiros.

Exemplo 2.24. Denotando por $M(a)$ o conjunto dos múltiplos de a, temos os seguintes exemplos:
$M(3) = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, \ldots\}$ são os múltiplos de 3,
$M(6) = \{\ldots, -36, -30, -24, -18, -12, -6, 0, 6, 12, 18, 24, 30, 36, \ldots\}$ os múltiplos de 6,
$M(-6) = \{\ldots, -36, -30, -24, -18, -12, -6, 0, 6, 12, 18, 24, 30, 36, \ldots\}$ os múltiplos de -6 e
$M(9) = \{\ldots, -54, -45, -36, -27, -18, -9, 0, 9, 18, 27, 36, 45, 54, \ldots\}$ os múltiplos de 9.

Observação 1: Podemos verificar que o elemento 0 (zero) é múltiplo de todo número inteiro, já que é divisível por todos eles.

Observação 2: Números opostos, como 7 e -7, possuem os mesmos múltiplos. Sejam a e b dois números inteiros, chama-se mínimo múltiplo comum de a e b, representado por $\text{mmc}(a, b)$, o menor número natural, diferente de zero, que é múltiplo comum de a e b.

Exemplo 2.25. Como $M(2) = \{\ldots, -12, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, 12, \ldots\}$ e $M(-5) = \{\ldots, -30, -25, -20, -15, -10, -5, 0, 5, 10, 15, 20, 25, 30, \ldots\}$, temos que a interseção desses múltiplos é

$$M(2) \cap M(-5) = \{\ldots, -30, -20, -10, 0, 10, 20, 30, \ldots\} = M(10)$$

então teremos $\text{mmc}(2, -5) = 10$. Agora vamos determinar o mmc entre 3 e 6. Naturalmente, todo múltiplo de 6 também é múltiplo de 3, visto que $6n = 3 \cdot 2n$, o que implica que $M(6) \subset M(3)$. Daí,

$$M(3) \cap M(6) = M(6).$$

Portanto $\text{mmc}(3, 6) = 6$.

Na Educação Básica, os alunos aprendem a calcular o mmc entre números naturais através da fatoração simultânea, processo em que se decompõem simultaneamente os dois ou mais números em fatores primos, e depois multiplica-se esses fatores, obtendo o mínimo múltiplo comum entre eles, o que torna bem mais simples o processo.

Exemplo 2.26. Calcule o $\text{mmc}(12, 30)$:

$$\begin{array}{r|l} 12,\ 30 & 2 \\ 6,\ 15 & 2 \\ 3,\ 15 & 3 \\ 1,\ 5 & 5 \\ \hline 1,\ 1 & 2 \cdot 2 \cdot 3 \cdot 5 = \mathbf{60} \end{array}$$

Assim, temos que o mmc(12,30) = 60.

Exemplo 2.27. Calcule o mmc$(15, 25, 40)$:

$$\begin{array}{r|l} 15,\ 25,\ 40 & 2 \\ 15,\ 25,\ 20 & 2 \\ 15,\ 25,\ 10 & 2 \\ 15,\ 25,\ 5 & 2 \\ 15,\ 25,\ 5 & 3 \\ 5,\ 25,\ 5 & 5 \\ 1,\ 5,\ 1 & 5 \\ \hline 1,\ 1,\ 1 & 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = \mathbf{600} \end{array}$$

Assim, temos que o mmc$(15, 25, 40) = 600$.

2.7.1 Máximo Divisor Comum

O Máximo Divisor Comum (mdc), também conhecido como Maior Divisor Comum, é o maior número inteiro que divide dois ou mais números sem deixar resto. O Máximo Divisor Comum é uma ferramenta fundamental na aritmética e na teoria dos números, sendo amplamente utilizado em operações como simplificação de frações, resolução de equações e análise de propriedades de divisibilidade. O conceito de (mdc) é particularmente útil em situações em que se deseja encontrar a maior quantidade possível que pode ser compartilhada por dois ou mais conjuntos de objetos, sem deixar excesso.

Para encontrar o (mdc) entre dois ou mais números, há diferentes métodos, sendo o método das divisões sucessivas (ou algoritmo de Euclides) e a decomposição em fatores primos os mais comuns.

2.7.2 Método das Divisões Sucessivas

Embora nem sempre seja possível efetuar a divisão exata entre números inteiros, a divisão euclidiana garante que qualquer número inteiro pode ser dividido por outro de modo a obter um quociente inteiro e um resto menor que o divisor. Conforme lemos:

> "Quando não existir uma relação de divisibilidade entre dois números inteiros, veremos que, ainda assim, será possível efetuar uma 'divisão com resto

pequeno', chamada de divisão euclidiana." (HEFEZ, 2016, p. 40).

A divisão euclidiana é um conceito fundamental da teoria dos números e formaliza a ideia de dividir um número inteiro por outro, garantindo um quociente e um resto bem definidos.

Dado dois inteiros a e b, com $b \neq 0$, a **divisão euclidiana** estabelece que existem únicos inteiros q (quociente) e r (resto) tais que:

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

Aqui, r representa o "resto pequeno"mencionado na citação, ou seja, um valor sempre menor que o módulo do divisor $|b|$. Quando $r = 0$, dizemos que b divide a exatamente ($b \mid a$), caso contrário, a divisão não é exata. Por exemplo, ao dividir 17 por 5, obtemos:

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

onde $q = 3$ e $r = 2$, confirmando que $0 \leq 2 < 5$.

ALGORITMO DE EUCLIDES: Esse método é um dos mais eficientes para encontrar o (mdc) entre dois números. Ele é baseado na ideia de que o (mdc) entre dois números a e b (onde $a > b$) é o mesmo que o (mdc) entre b e o resto da divisão de a por b. O processo é repetido até que o resto seja zero, e o divisor nessa etapa será o (mdc).

Exemplo 2.28. Vamos encontrar o (mdc) entre 48 e 18 usando o método das divisões sucessivas.

$\text{mdc}(48, 18) = \text{mdc}(48 - (2 \cdot 18), 18) = \text{mdc}(18, 12) = \text{mdc}(18 - (1 \cdot 12), 12) = \text{mdc}(12, 6) = \text{mdc}(0, 6) = 6$

Passo 1: Primeiro, dividimos 48 por 18. O objetivo é encontrar o quociente e o resto da divisão:

$$48 = 18 \cdot 2 + 12.$$

Como o resto é 12 e não zero, aplicamos o algoritmo novamente, agora considerando os números 18 e 12.

Passo 2: Agora, dividimos 18 por 12:

$$18 = 12 \cdot 1 + 6.$$

Como o resto é 6 e não zero, aplicamos o algoritmo novamente, agora considerando os números 12 e 6.

Passo 3: Agora, dividimos 12 por 6:

$$12 = 6 \cdot 2 + 0.$$

Neste momento, o resto é zero, o que significa que o algoritmo termina. O último divisor não nulo encontrado é 6.

Conclusão: O máximo divisor comum entre 48 e 18 é:

$$\text{mdc}(48, 18) = 6.$$

2.7.3 Decomposição em Fatores Primos

Outro método eficaz para encontrar o (mdc) é decompor os números em seus fatores primos. O (mdc) é obtido tomando os fatores primos comuns com os menores expoentes.

Exemplo 2.29. Vamos encontrar o (mdc) entre 60 e 45 usando a decomposição em fatores primos.

Decompondo 60:

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

Decompondo 45:

$$45 = 3^2 \cdot 5.$$

Os fatores comuns são 3 e 5, e devemos pegar o menor expoente de cada fator. Portanto, o (mdc) é:

$$3^1 \cdot 5^1 = 15.$$

Assim, o $\text{mdc}(60, 45) = 15$.

2.7.4 Aplicações do Máximo Divisor Comum

O (mdc) tem várias aplicações práticas. Ele é essencial, por exemplo, na simplificação de frações. Para simplificar uma fração, basta dividir o numerador e o denominador pelo (mdc) entre eles. O (mdc) também é usado em problemas de divisão de quantidades em partes iguais, onde se deseja encontrar o maior grupo possível que possa ser formado sem deixar sobras.

Exemplo 2.30. Suponha que você tenha 120 maçãs e 90 laranjas e deseja dividi-las em grupos de tamanhos iguais, sem sobras. O maior número de grupos possíveis será dado pelo MDC entre 120 e 90.

Decompondo 120:

$$120 = 2^3 \cdot 3 \cdot 5.$$

Decompondo 90:

$$90 = 2 \cdot 3^2 \cdot 5.$$

Os fatores comuns são 2, 3 e 5, e o menor expoente de cada um é 1. Portanto, o (mdc) é:

$$2^1 \cdot 3^1 \cdot 5^1 = 30.$$

Logo, as frutas podem ser divididas em grupos de 30 unidades.

Em resumo, o (mdc) é uma operação essencial para a análise de divisibilidade e simplificação de frações, e seus métodos de cálculo são eficazes tanto em operações manuais quanto em algoritmos computacionais.

Capítulo

3

Equações Diofantinas Lineares

Este capítulo se dedica à apresentação do caso mais simples de equações diofantinas lineares, aquelas com duas incógnitas, dada sua relação com problemas envolvendo equações lineares. Essas questões são abordadas no contexto dos sistemas de equações lineares no Ensino Médio, em conformidade com as habilidades previstas na **Base Nacional Comum Curricular (BNCC)** para essa etapa da Educação Básica, especificamente: **(EM13MAT301), (EM13MAT401) e (EM13MAT501)**. Tais conceitos e atividades aqui propostas são baseados em Dmitri [6], Dutenhefner [9], Hefez [14] e Santos [27].

As equações diofantinas, que levam o nome do matemático grego Diofanto de Alexandria, têm suas raízes na Antiguidade, quando problemas envolvendo inteiros foram formulados e estudados. Diofanto, no século III, explorou soluções inteiras para equações polinomiais, especialmente em sua obra *Arithmetica*, onde apresentou métodos para encontrar essas soluções em problemas que, em muitos casos, envolviam a busca por números inteiros que satisfizessem certas condições.

O propósito deste capítulo é mostrar uma importante aplicação da aritmética dos restos, as equações diofantinas lineares. Em diversas provas de conhecimentos básicos, como a Olimpíada Brasileira de Matemática das Escolas Públicas e Privadas (OBMEP), podem ser encontrados problemas cujas soluções recaem sobre as equações diofantinas lineares. O que vamos enunciar na sequência são resultados importantes para o estudo desse tipo de equação.

3.1 Resolvendo Equações Diofantinas via Algoritmo de Euclides

Chama-se equação diofantina a toda equação polinomial com coeficientes inteiros, independente da quantidade de incógnitas. Focaremos nosso estudo no caso mais

simples de equações diofantinas, as com duas incógnitas. Uma equação diofantina de duas variáveis é dita linear se ela é da forma:

$$ax + by = c$$

onde a, b e $c \in \mathbb{Z}$ com a e b não nulos.

Ao nos depararmos com equações desse tipo, certamente alguns pontos precisam ser muito bem esclarecidos:

- Quais são as condições para que a equação possua solução?
- Quantas são as soluções?
- Como calcular as soluções, caso existam?

Daremos a seguir respostas a essas perguntas no caso das equações em questão.

Considere as equações diofantinas abaixo:

a) $4x + 7y = 3$

b) $2x + 6y = 11$

Observe que na equação do item (a) temos que $a = 4$, $b = 7$ e $c = 3$. O $\text{mdc}(4, 7) = 1$, ou seja, $\text{mdc}(4, 7) \mid 3$ e que $x_0 = -1$ e $y_0 = 1$ representa uma solução particular para $4x + 7y = 3$. Porém esta solução não é única, já que $x_0 = 6$ e $y_0 = -3$ também constitui outra solução para a mesma equação.

Agora observando a equação do item (b), verificamos que $a = 2$, $b = 6$ e $c = 11$. Como o $\text{mdc}(2, 6) = 2$, temos que o $\text{mdc}(2, 6) \nmid 11$ e assim concluímos que a equação não possui soluções inteiras. Podemos notar que não existem x e $y \in \mathbb{Z}$, tais que $2x + 6y = 11$, uma vez que $2x + 6y$ resulta em um número par e, portanto, nunca igual a 11.

Proposição 3.1. *Uma equação diofantina $ax + by = c$, em que $a \neq 0$ e $b \neq 0$, admite solução se, e somente se, $d = mdc(a, b)$ divide c*

Demonstração: ($\Rightarrow$) Vamos mostrar que dada uma solução da equação diofantina, então, $d \mid c$. Considere x_0, y_0 soluções da equação. Assim,

$$ax_0 + by_0 = c.$$

Seja $d = \text{mdc}(a, b)$, então $d \mid a$ e $d \mid b$, logo, a e b podem ser reescritos como $a = k_1 d$ e $b = k_2 d$, com $k_1, k_2 \in \mathbb{Z}$. Substituindo os valores de a e b na equação acima, temos que:

$$c = ax_0 + by_0 = k_1 dx_0 + k_2 dy_0 = d(k_1 x_0 + k_2 y_0) = dq.$$

Portanto, $d \mid c$.

($\Leftarrow$) Considere $d = \text{mdc}(a, b)$. Pela relação de Bèzout, existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.

Por hipótese temos que $d \mid c$, isto é, existe $t \in \mathbb{Z}$ tal que $c = dt$. Segue então que:

$$c = dt = (ax_0 + by_0)t = a(x_0t) + b(y_0t),$$

com x_0t, y_0t solução da equação $ax + by = c$.

Proposição 3.2. *Seja (x_0, y_0) uma solução particular da equação diofantina $ax + by = c$, com $a \neq 0$ e $b \neq 0$. Então essa equação admite infinitas soluções e o conjunto dessas soluções é:*

$$S = \left\{ \left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t \right) \mid t \in \mathbb{Z} \right\},$$

sendo $d = mdc(a, b)$.

Demonstração: Consideremos (x', y') uma solução da equação $ax + by = c$. Então, $ax' + by' = c = ax_0 + by_0$, onde podemos reescrever da seguinte forma:

$$a(x' - x_0) = b(y_0 - y'). \tag{I}$$

Seja $d = \text{mdc}(a, b)$. Logo, $a = dr$ e $b = ds$, com $r, s \in \mathbb{Z}$ e $\text{mdc}(r, s) = 1$. Então,

$$r(x' - x_0) = s(y_0 - y'). \tag{II}$$

Pela equação (II), temos que $r \mid s(y_0 - y')$. Como $\text{mdc}(r, s) = 1$, necessariamente $r \mid (y_0 - y')$, ou seja, existe $t \in \mathbb{Z}$ tal que $y_0 - y' = rt$. Assim,

$$y' = y_0 - rt = y_0 - \frac{a}{d}t. \tag{III}$$

Então, para encontrarmos a forma das soluções x_0, basta substituirmos o valor de y' na equação (I). Temos que

$$a(x' - x_0) = b\left(y_0 - \left(y_0 - \frac{a}{d}t \right) \right).$$

Isso implica na seguinte equação:

$$a(x' - x_0) = \frac{ba}{d}t.$$

Segue que

$$a(x' - x_0) = \frac{ba}{d}t \implies x' - x_0 = \frac{b}{d}t.$$

Logo,

$$x' = x_0 + \frac{b}{d}t.$$

Por outro lado, o par $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ é solução da equação dada, para todo $t \in \mathbb{Z}$. De fato, substituindo esses valores na equação, temos

$$ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c.$$

Vejamos alguns exemplos de equações diofantinas e suas resoluções utilizando o meio mais usual que é o algoritmo de Euclides.

Exemplo 3.1. Determinar todas as soluções inteiras da equação diofantina linear

$$2x + 3y = 25 \tag{3.1}$$

Solução: Inicialmente, vamos determinar o mdc$(2, 3)$ pelo algoritmo de Euclides:

	1	2
3	2	1
1	0	

Tabela 3.1: Diagrama: mdc(3,2)=1

Logo, encontramos que mdc$(2, 3) = 1$. Segue que:

$$1 = 3 - 2 \cdot 1$$

Como mdc$(2, 3) = 1$, a equação tem solução, pois mdc$(2, 3) \mid 25$. Agora, expressando 1 como uma combinação linear, temos:

$$1 = 3 - 2 \cdot 1 \quad \text{ou} \quad 1 = 3 \cdot 1 - 2 \cdot 1 \quad \text{ou} \quad 1 = 3 \cdot 1 + 2 \cdot (-1)$$

Multiplicando essa igualdade por 25, obtemos:

$$2 \cdot (-25) + 3 \cdot 25 = 25$$

Dessa forma, obtemos o par de inteiros $x_0 = -25$ e $y_0 = 25$, que é uma solução particular da equação dada. Assim, a solução geral é dada por:

$$\begin{cases} x = -25 + 3t \\ y = 25 - 2t \end{cases} \quad \text{com} \quad t \in \mathbb{Z}.$$

Exemplo 3.2. Determinar todas as soluções inteiras da equação diofantina linear:

$$7x + 9y = 5$$

Solução: Inicialmente vamos determinar o mdc$(7, 9)$ pelo algoritmo de Euclides:

	1	3	2
9	7	2	1
2	1	0	

Logo, encontramos o mdc$(7, 9) = 1$. Daí, segue que:

$$1 = 7 - 2 \cdot 3$$

$$2 = 9 - 7 \cdot 1$$

Como o mdc$(7, 9) = 1$, a equação tem solução, pois mdc$(7, 9)|5$. Agora, expressando 1 como uma combinação linear, temos:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ 1 &= 7 - (9 - 7) \cdot 3 \\ 1 &= 7 \cdot 4 + 9 \cdot (-3) \end{aligned}$$

Dessa forma, temos que:

$$7 \cdot (4) + 9 \cdot (-3) = 1$$

Multiplicando essa igualdade por 5, temos:

$$7 \cdot (20) + 9 \cdot (-15) = 5$$

Com isso, obtemos o par de inteiros $x_0 = 20$ e $y_0 = -15$ que é uma solução particular da equação dada. Assim, temos que a solução geral é dada por:

$$\begin{cases} x = 20 + 9t \\ y = -15 - 7t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Exemplo 3.3. Um lava-rápido oferece dois tipos de lavagem de veículo: **lavagem simples**, ao preço de $R\$20,00$, e **lavagem completa**, ao preço de $R\$35,00$. Para cobrir as despesas com produtos e funcionários e não ter prejuízos, o lava-rápido deve ter uma receita diária de, pelo menos, $R\$300,00$. Para não ter prejuízos, o menor número de lavagens diárias que o lava-rápido deve efetuar é:

a) 6 b) 8 c) 9 d) 15 e) 20

Solução: Considerando x como a quantidade de lavagens simples e y como a quantidade de lavagens completas, temos a seguinte equação diofantina linear:

$$20x + 35y = 300, \quad \text{com } x, y \in \mathbb{N} \cup \{0\}.$$

Vamos determinar o $\text{mdc}(35, 20)$ pelo algoritmo de Euclides:

	1	1	3
35	20	15	5
15	5	0	

Logo, encontramos que o $\text{mdc}(35, 20) = 5$. Daí, segue que:

$$35 = 1 \cdot 20 + 15 \implies 35 - 20 = 15,$$

$$20 = 1 \cdot 15 + 5 \implies 20 - 15 = 5.$$

Como $5 \mid 300$, a equação tem solução. Agora, expressando 5 como uma combinação linear, temos:

$$\begin{aligned} 5 &= 20 - 15 \\ 5 &= 20 - (35 - 20) \\ 5 &= 20 + 20 - 35 \\ 5 &= 2 \cdot 20 - 35 \\ 5 &= 20 \cdot 2 + 35 \cdot (-1) \end{aligned}$$

Daí segue que

$$20 \cdot 2 + 35 \cdot (-1) = 5$$

Multiplicando essa igualdade por 60, temos:

$$20 \cdot 120 + 35 \cdot (-60) = 300.$$

Assim, obtemos o par de inteiros $(x_0, y_0) = (120, -60)$, que é uma solução particular da

equação dada. Portanto, temos que a solução geral é dada por:

$$\begin{cases} x = 120 + \dfrac{35}{5} \cdot t \\ y = -60 - \dfrac{20}{5} \cdot t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

$$\begin{cases} x = 120 + 7t \\ y = -60 - 4t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Como o problema apresentado sugere que encontremos as soluções inteiras não negativas, temos que:

$$120 + 7t \geq 0 \quad \text{(I)} \quad \text{e} \quad -60 - 4t \geq 0 \quad \text{(II)}.$$

Resolvendo as inequações acima, obtemos: Para (I):

$$120 + 7t \geq 0 \implies 7t \geq -120 \implies t \geq \frac{-120}{7} \implies t \geq -17,142857\ldots$$

Para (II):

$$-60 - 4t \geq 0 \implies -4t \geq 60 \implies t \leq \frac{-60}{4} \implies t \leq -15.$$

Logo, concluímos que os valores de t que satisfazem as condições do problema pertencem ao seguinte intervalo:

$$-17 \leq t \leq -15, \quad \text{com } t \in \mathbb{Z}.$$

Agora, analisando cada valor de t: Para $t = -17$:

$$x = 120 + 7 \cdot (-17) = 1,$$

$$y = -60 - 4 \cdot (-17) = 8.$$

Assim, obtemos o par $(x, y) = (1, 8)$. Para $t = -16$:

$$x = 120 + 7 \cdot (-16) = 8,$$

$$y = -60 - 4 \cdot (-16) = 4.$$

Assim, obtemos o par $(x, y) = (8, 4)$. Para $t = -15$:

$$x = 120 + 7 \cdot (-15) = 15,$$

$$y = -60 - 4 \cdot (-15) = 0.$$

Assim, obtemos o par $(x, y) = (15, 0)$. Portanto, os pares de inteiros $(1, 8)$, $(8, 4)$, e $(15, 0)$ representam as soluções inteiras não negativas da Equação Diofantina associada

ao problema em questão. Como o problema pede apenas o menor número de lavagens para que o lava-jato não tenha prejuízo, a solução é o par ordenado $(1, 8)$, totalizando 1 lavagem simples e 8 lavagens completas por dia. Assim, concluímos que a alternativa correta é a **c**.

Exemplo 3.4. De quantos modos podemos comprar selos de cinco e de três reais, de modo a gastar cinquenta reais?

Solução: Considerando x como a quantidade de selos de cinco reais e y como a quantidade de selos de três reais, temos a seguinte Equação Diofantina Linear:

$$5x + 3y = 50, \quad \text{com } x, y \in \mathbb{N} \cup \{0\}.$$

Vamos determinar o $\text{mdc}(3, 5)$ pelo algoritmo de Euclides:

	1	1	2
5	3	2	1
2	1	0	

Logo, encontramos que $\text{mdc}(3, 5) = 1$. Daí, segue que:

$$5 = 1 \cdot 3 + 2 \quad \Longrightarrow \quad 5 - 3 = 2$$

$$3 = 1 \cdot 2 + 1 \quad \Longrightarrow \quad 3 - 2 = 1$$

Como $1 \mid 50$, temos que a equação possui solução. Agora, expressando 1 como uma combinação linear, temos:

$$\begin{aligned} 1 &= 3 - 2 \\ 1 &= 3 - (5 - 3) \\ 1 &= 3 \cdot 2 - 5 \\ 1 &= 5 \cdot (-1) + 3 \cdot 2 \end{aligned}$$

Logo, temos que:

$$5 \cdot (-1) + 3 \cdot 2 = 1$$

Multiplicando a igualdade por 50, temos:

$$5 \cdot (-50) + 3 \cdot 100 = 50$$

Concluímos então que $(x_0, y_0) = (-50, 100)$ representa uma solução particular da equação

dada. A solução geral da equação diofantina em questão é:

$$\begin{cases} x = -50 + 3t \\ y = 100 - 5t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Como estamos à procura de soluções não negativas apenas, temos a seguinte condição:

$$x \geq 0 \quad \Longrightarrow \quad -50 + 3t \geq 0$$

$$y \geq 0 \quad \Longrightarrow \quad 100 - 5t \geq 0$$

Assim, o problema admite as seguintes soluções:

$$(10, 0); \quad (7, 5); \quad (4, 10); \quad (1, 15),$$

totalizando 4 modos diferentes.

Exemplo 3.5. Um cachecol custa 19 reais, mas o caso é que o comprador, que comprou apenas um cachecol, só tem notas de 2 reais, e o caixa só tem notas de 5 reais. Nessas condições, será possível pagar a importância da compra, e de que modo? (Suponha que a quantidade máxima de notas de cada tipo seja 40).

Solução: Seja x a quantidade de notas de 2 reais e y a quantidade de notas de 5 reais. Assim, podemos traduzir o problema pela Equação Diofantina:

$$2x - 5y = 19.$$

Inicialmente, vamos determinar o $\text{mdc}(2, 5)$ pelo algoritmo de Euclides:

	2	2
5	2	1
1	0	

Logo, encontramos que o $\text{mdc}(2, 5) = 1$. Daí, segue que:

$$1 = 5 - 2 \cdot 2$$

Como o $\text{mdc}(2, 5) = 1$, a equação possui solução, pois o $\text{mdc}(2, 5) \mid 19$. Agora, expressando 1 como uma combinação linear, temos:

$$1 = 5 - 2 \cdot 2$$
$$1 = 2 \cdot 3 - 5 \cdot 1$$

Multiplicando essa igualdade por 19, temos:

$$2 \cdot 57 - 5 \cdot 19 = 19$$

Concluímos então que $(x_0, y_0) = (57, 19)$ representa uma solução particular da equação dada. A solução geral da equação diofantina em questão é:

$$\begin{cases} x = 57 - 5t \\ y = 19 - 2t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Como estamos à procura de soluções inteiras não negativas, temos a seguinte condição:

$$x \geq 0 \quad \Longrightarrow \quad 57 - 5t \geq 0$$

$$y \geq 0 \quad \Longrightarrow \quad 19 - 2t \geq 0$$

Assim, o problema admite as seguintes soluções:

$$(37, 11); \quad (32, 9); \quad (27, 7); \quad (22, 5); \quad (17, 3); \quad (12, 1)$$

Portanto, de acordo com as condições do problema, é possível pagar a compra de 6 modos, que são eles: 37 notas de 2 reais e 11 notas de 5 reais; 32 notas de 2 reais e 9 notas de 5 reais; 27 notas de 2 reais e 7 notas de 5 reais; 22 notas de 2 reais e 5 notas de 5 reais; 17 notas de 2 reais e 3 notas de 5 reais; 12 notas de 2 reais e 1 nota de 5 reais.

Exemplo 3.6. Resolva a equação $24x + 14y = 18$.

Solução: Primeiramente, devemos verificar se essa equação tem solução. Como o mdc $(24, 14) = 2 \mid 18$, temos que a equação diofantina admite solução em $\mathbb{Z}$. Dividindo ambos os membros da equação por 2, obtemos a seguinte equação equivalente:

$$12x + 7y = 9.$$

Vamos calcular $\text{mdc}(12, 7)$ utilizando o algoritmo de Euclides:

	1	1	2	2
12	7	5	2	1
5	2	1	0	

Logo, encontramos que o $\text{mdc}(7, 12) = 1$. Daí, segue que:

$$12 = 1 \cdot 7 + 5 \implies 12 - 7 = 5$$

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

$$5 = 2 \cdot 2 + 1 \implies 5 - 4 = 1$$

Como o mdc$(7, 12) \mid 9$, temos que a equação possui solução.
Agora, expressando 1 como uma combinação linear, temos:

$$\begin{aligned}
1 &= 5 - 4 \\
1 &= 5 - 2 \cdot (2) \\
1 &= 5 - 2 \cdot (7 - 5) \\
1 &= 5 - 2 \cdot (7) + 2 \cdot (5) \\
1 &= 5 \cdot (3) - 2 \cdot (7) \\
1 &= (12 - 7) \cdot 3 - 2 \cdot (7) \\
1 &= 3 \cdot (12) - 3 \cdot (7) - 2 \cdot (7) \\
1 &= 12 \cdot (3) + 7 \cdot (-5)
\end{aligned}$$

Logo, temos que:

$$12 \cdot (3) + 7 \cdot (-5) = 1$$

Multiplicando essa igualdade por 9, temos:

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

Concluímos então que $(x_0, y_0) = (27, -45)$ representa uma solução particular da equação dada.
A solução geral da equação diofantina em questão é:

$$\begin{cases} x = 27 + 7t \\ y = -45 - 12t \end{cases}, \quad \text{com } t \in \mathbb{Z}.$$

Exemplo 3.7. Para poder ir ao passeio da escola, Reginaldo guardou sua mesada para comprar seu lanche. Depois de pesquisar qual lanche levaria e quanto pagaria no total, Reginaldo optou pelos seguintes lanches:

- Hambúrguer: R$ 4,00 (unidade)
- Sanduíches: R$ 6,00 (unidade)

Sabendo que Reginaldo dispunha de R$ 50,00, e que haveria divisão de lanches entre os colegas, de quantas maneiras ele pode comprar os lanches?

Solução: Considere x como a quantidade de hambúrgueres e y como a quantidade de

sanduíches. Podemos traduzir o problema por meio da seguinte equação diofantina:

$$4x + 6y = 50$$

Dividindo a equação, em ambos os membros, por 2, temos:

$$2x + 3y = 25$$

Como 2 e 3 são primos entre si, temos que o $\text{mdc}(2,3) = 1$. Como $\text{mdc}(2,3) \mid 25$, concluímos que a equação possui solução.
Agora, expressando 1 como uma combinação linear, temos:

$$1 = 3 - 2$$
$$1 = 3 \cdot (1) + 2 \cdot (-1)$$

Logo, temos que:

$$2 \cdot (-1) + 3 \cdot (1) = 1$$

Multiplicando essa igualdade por 25, temos:

$$2 \cdot (-25) + 3 \cdot (25) = 25$$

Concluímos, então, que $(x_0, y_0) = (-25, 25)$ representa uma solução particular da equação dada. A solução geral da equação diofantina em questão é:

$$\begin{cases} x = -25 + 3t \\ y = 25 - 2t \end{cases}, \quad \text{com } t \in \mathbb{Z}.$$

Como estamos à procura de soluções inteiras positivas, temos as seguintes condições:

$$x \geq 0 \implies -25 + 3t \geq 0$$

$$y \geq 0 \implies 25 - 2t \geq 0$$

Logo, concluímos que:

$$9 \leq t \leq 12$$

Encontramos, assim, quatro soluções para a equação, ou seja:

$$(2,7),\ (5,5),\ (8,3),\ (11,1)$$

são soluções da equação diofantina apresentada no exemplo.

3.2 Resolvendo Equações Diofantinas via Congruência Modular

As equações diofantinas integram um campo clássico da teoria dos números, cujo principal objetivo é a determinação de soluções inteiras ou racionais para equações polinomiais. Dentre as diversas abordagens para resolver tais equações, destacam-se o algoritmo de Euclides e a congruência modular, ambas ferramentas fundamentais na matemática discreta. O algoritmo de Euclides, um dos métodos mais antigos e eficientes para encontrar o máximo divisor comum (mdc) entre dois números inteiros, desempenha um papel crucial na solução de equações diofantinas lineares, pois permite a reescrita das equações na forma de combinação linear dos coeficientes. Por outro lado, apresentaremos nessa seção, que a congruência modular fornece um arcabouço alternativo, que permite reduzir a complexidade das equações por meio da análise dos resíduos em aritmética modular.

3.2.1 Aritmética Modular

Formalmente, dizemos que os inteiros a e b são congruentes módulo n, com $n > 1$, e escrevemos em símbolos $a \equiv b \mod n$, quando a e b deixam o mesmo resto ao serem divididos por n. Por exemplo, 16 e 22 são congruentes módulo 3, pois $16 = 3 \cdot 5 + 1$ e $22 = 3 \cdot 7 + 1$, ou seja, 16 e 22 deixam resto 1 quando divididos por 3. Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \mod 1$, quaisquer que sejam a e $b \in \mathbb{Z}$. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, consideremos $n > 1$.

Essa relação possui diversas propriedades fundamentais, como a reflexividade, simetria e transitividade, além de ser compatível com as operações aritméticas, permitindo a realização de operações como adição, subtração e multiplicação de congruências. A congruência modular é essencial em várias áreas da matemática, incluindo a teoria dos números, criptografia e algoritmos, e se baseia em resultados importantes, como o Teorema da Reciprocidade Quadrática e o Teorema Chinês do Resto, que ampliam as aplicações e a compreensão dessa fascinante estrutura algébrica. Por meio da análise de suas propriedades e aplicações, a congruência modular consolida-se como um fundamento essencial da matemática contemporânea, oferecendo ferramentas indispensáveis para a resolução de problemas complexos e o desenvolvimento de teorias inovadoras.

Proposição 3.3. *Dados $a, b, n \in \mathbb{Z}$ com $n > 1$, temos por definição que:*

$$a \equiv b \bmod n \iff n \mid (b - a).$$

Demonstração: Provemos inicialmente que $a \equiv b \bmod n \implies n \mid (b - a)$. Partindo de $a \equiv b \bmod n$, sabemos que a e b têm o mesmo resto r quando divididos por n. Isto

significa que existem $q_1, q_2 \in \mathbb{Z}$ tais que:

$$a = q_1 n + r \quad \text{e} \quad b = q_2 n + r$$

Assim:

$$r = a - q_1 n,$$

e como $b = q_2 n + r$, obtemos:

$$b = q_2 n + (a - q_1 n) \implies b - a = n(q_2 - q_1).$$

Portanto:

$$n \mid (b - a).$$

Agora provaremos que $n \mid (b - a) \implies a \equiv b \bmod n$. Como $n \mid (b - a)$, temos:

$$b - a = qn \quad \text{onde } q \in \mathbb{Z}.$$

Seja r o resto da divisão de a por n, então existe $q_1 \in \mathbb{Z}$ tal que:

$$a = q_1 n + r, \quad \text{onde } 0 \leq r < n.$$

Substituindo na igualdade $b = a + qn$, obtemos:

$$b = q_1 n + r + qn \implies b = (q_1 + q)n + r.$$

Como $0 \leq r < n$, vemos que $q_1 + q \in \mathbb{Z}$ e r satisfazem a condição de quociente e resto na divisão de b por n. E como quociente e resto são únicos neste processo, resulta que r também é o resto na divisão de b por n.

Portanto a e b têm o mesmo resto r na divisão por n, como desejávamos provar.

3.2.2 Propriedades da Congruência Modular

Proposição 3.4. *Dados inteiros a, b, c e n, sendo $n > 1$, temos:*

i) ***(Reflexividade)*** $a \equiv a \ mod\ n$,

ii) ***(Simetria)*** $a \equiv b \ mod\ n \implies b \equiv a \ mod\ n$,

iii) ***(Transitividade)*** $a \equiv b \ mod\ n$ *e* $b \equiv c \ mod\ n \implies a \equiv c \ mod\ n$.

Demonstração:

i) Como $n \mid 0$, então $n \mid (a - a)$, o que implica $a \equiv a \bmod n$.

ii) Se $n \mid (b-a)$, então $n \mid (a-b)$, pois $a - b = -(b-a)$.

iii) Se $n \mid (b-a)$ e $n \mid (c-b)$, então $n \mid (c-a)$, pois $c - a = (c-b) + (b-a)$.

Exemplo 3.8. Vamos apresentar alguns exemplos relacionados com a proposição anterior:

a) A propriedade reflexiva pode ser ilustrada pelo exemplo:

$$7 \equiv 7 \bmod 4,$$

tendo em vista que $4 \mid 7 - 7 = 0$.

b) Apresentamos agora um exemplo relacionado à simetria:

$$13 \equiv 5 \bmod 8 \implies 5 \equiv 13 \bmod 8$$

Temos que 13 deixa resto 5 quando dividido por 8.

c) Para a transitividade, considere o exemplo:

$$17 \equiv 5 \bmod 6, \quad 5 \equiv 11 \bmod 6 \implies 17 \equiv 11 \bmod 6.$$

Temos que 17 e 11 deixam resto 5 quando divididos por 6.

Proposição 3.5. *Se a, b, c, e n são inteiros, com $n > 1$, tais que $a \equiv b \ mod\ n$, então:*

i) $(a + c) \equiv (b + c) \ mod\ n$;

ii) $(a - c) \equiv (b - c) \ mod\ n$;

iii) $ac \equiv bc \ mod\ n$.

Demonstração:

(i) Por hipótese temos que $n \mid (a-b)$. Logo, existe um $q \in \mathbb{Z}$ tal que $(a-b) = (a+c) - (b+c) = n \cdot q$. Logo $(a+c) \equiv (b+c) \bmod n$.

(ii) Por hipótese temos que $n \mid (a-b)$. Logo, existe um $q \in \mathbb{Z}$ tal que $(a-b) = (a-c) - (b-c) = n \cdot q$. Portanto $(a-c) \equiv (b-c) \bmod n$.

(iii) Por hipótese temos que $n \mid (a-b)$, logo, existe um $q \in \mathbb{Z}$, tal que $a - b = n \cdot q$. Multiplicando por c a última equação em ambos os membros iremos obter $(ca - cb) = ncq$ o que implica que $n \mid (ac - cb)$ e, portanto $ac \equiv bc \bmod n$.

Proposição 3.6. *Sejam a, b, c, d, m, $n \in \mathbb{Z}$, com $m, n > 1$. Então, temos:*

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

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

iii) *Se* $a \equiv b \bmod m$ *e* $c \equiv d \bmod m$, *então* $(a - c) \equiv (b - d) \bmod m$.

iv) *Se* $a \equiv b \bmod n$ *e* $a \equiv b \bmod m$, *com* $\text{mdc}(n, m) = 1$, *então* $a \equiv b \bmod (n \cdot m)$.

Observação: Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \bmod m$, então temos que $a^n \equiv b^n \bmod m$.

Exemplo 3.9. A seguinte propriedade: Se $a \equiv b \bmod n$ e $c \equiv d \bmod n$, então:

$$a + c \equiv b + d \bmod n$$

$$a - c \equiv b - d \bmod n,$$

pode ser exemplificada no seguinte caso:

$$8 \equiv 3 \bmod 5, \quad 7 \equiv 2 \bmod 5 \implies (8 + 7) \equiv (3 + 2) \bmod 5$$

Temos que (8+7)=15 e (3+2)=5 deixam resto 0 quando dividido por 5.

Exemplo 3.10. A propriedade de multiplicação: Se $a \equiv b \bmod n$, então para qualquer inteiro c, temos:

$$ac \equiv bc \bmod n,$$

é ilustrada no seguinte exemplo:

$$9 \equiv 4 \bmod 5 \implies 9 \cdot 3 \equiv 4 \cdot 3 \bmod 5.$$

Temos que $(9 \cdot 3) = 27$ e $(4 \cdot 3) = 12$ deixam resto 2 quando dividido por 5.

Exemplo 3.11. Usando congruências, vamos provar o seguinte critério de divisibilidade por 3: Um número $a = a_0a_1a_2 \cdots a_n$ é divisível por 3 se e somente se $a_0 + a_1 + a_2 + \cdots + a_n$ é divisível por 3.

De fato, podemos representar o número a na forma decimal:

$$a = a_0 + 10a_1 + 10^2a_2 + \cdots + 10^na_n$$

onde $a_0, a_1, \ldots, a_{n-1}$ são os algarismos de a. Sabemos que:

$$10 \equiv 1 \bmod 3$$

Portanto,

$$10^k \equiv 1 \bmod 3 \quad \text{para todo } k \geq 0$$

Substituindo na expressão de a, temos:

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_n \bmod 3$$

Logo, $a \equiv 0 \pmod 3$ se, e somente se,

$$a_0 + a_1 + a_2 + \cdots + a_n \equiv 0 \bmod 3$$

Concluímos, então, que um número é divisível por 3 se, e somente se, a soma dos seus algarismos também é divisível por 3.

Como $10 \equiv 1 \bmod 9$, segue que $10^k \equiv 1 \bmod 9$ para todo inteiro $k \geq 0$. Dessa forma, com uma pequena alteração na demonstração do exemplo anterior, podemos concluir que

$$a \equiv a_0 + a_1 + a_2 + \cdots + a_n \bmod 9,$$

e consequentemente, a é divisível por 9 se, e somente se $a_0 + a_1 + a_2 \cdots + a_n$ é divisível por 9.

Exemplo 3.12. Vamos agora provar que um número $a = a_n a_{n-1} \cdots a_2 a_1 a_0$ é divisível por 4 se e somente se o número formado pelos seus dois últimos algarismos, $a_1 a_0$, é divisível por 4. Escrevendo a na forma decimal, temos:

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

Queremos mostrar que:

$$4 \mid a \iff 4 \mid (10a_1 + a_0).$$

Como $10 \equiv 2 \bmod 4$, podemos reescrever cada potência de 10 em módulo 4. Note que para $k \geq 2$, temos:

$$10^k \equiv 0 \bmod 4,$$

o que significa que todos os termos de grau maior que 1 na expansão de a desaparecem em módulo 4. Logo, a expressão torna-se:

$$a \equiv a_1 10^1 + a_0 \equiv a_1 \cdot 2 + a_0 \bmod 4.$$

Portanto, a divisibilidade de a por 4 depende apenas dos dois últimos algarismos, $a_1 a_0$, o que prova que:

$$4 \mid a \iff 4 \mid (10a_1 + a_0) \iff 4 \mid a_1 a_0.$$

Exemplo 3.13. Vamos agora provar que um número $a = a_n a_{n-1} \cdots a_2 a_1 a_0$ é divisível por 8 se e somente se o número formado pelos seus três últimos algarismos, $a_2 a_1 a_0$, é

divisível por 8. Escrevendo a na forma decimal, temos:

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

Queremos mostrar que:

$$8 \mid a \iff 8 \mid (100a_2 + 10a_1 + a_0).$$

Como $10 \equiv 2 \pmod 8$, podemos reescrever cada potência de 10 em módulo 8. Note que para $k \geq 3$, temos:

$$10^k \equiv 0 \pmod 8,$$

o que significa que todos os termos de grau maior que 2 na expansão de a desaparecem em módulo 8. Logo, a expressão torna-se:

$$a \equiv a_2 10^2 + a_1 10^1 + a_0 \equiv a_2 \cdot 4 + a_1 \cdot 2 + a_0 \pmod 8.$$

Portanto, a divisibilidade de a por 8 depende apenas dos três últimos algarismos, $a_2 a_1 a_0$, o que prova que:

$$8 \mid a \iff 8 \mid (100a_2 + 10a_1 + a_0).$$

3.2.3 Congruências e Equações Diofantinas

A congruência modular é uma ferramenta extremamente útil para a resolução de equações diofantinas no campo dos números inteiros. O objetivo agora é demonstrar na prática, por meio da resolução de problemas, que a congruência modular pode constituir uma importante alternativa a utilização do algoritmo de Euclides no processo de resolução de equações diofantinas lineares com duas incógnitas..

Resolveremos agora os exemplos 1 e 4 considerados na Seção 3.1, utilizando os conceitos da congruência modular e suas propriedades.

Exemplo 3.14. Determinar todas as soluções inteiras da equação diofantina linear:

$$2x + 3y = 25 \tag{I}$$

Como $\text{mdc}(2, 3) = 1$, a equação tem solução, pois $\text{mdc}(2, 3) \mid 25$. Primeiramente decidimos resolver a equação utilizando $\mod 2$, pois 2 é um dos coeficientes da equação diofantina apresentada. Assim temos:

$$2x + 3y \equiv 25 \mod 2$$

Dividindo por 2 os coeficientes 2, 3 e 25 e anotando seus restos, obtemos:

$$0x + 1y \equiv 1 \mod 2 \implies y \equiv 1 \mod 2$$

Assim, podemos escrever que:

$$y = 1 + 2t, \text{ com } t \in \mathbb{Z}. \tag{II}$$

Dessa forma, substituindo (II) em (I) e fazendo as devidas simplificações, obtemos:

$$\begin{aligned} 2x + 3(1 + 2t) &= 25 \\ 2x + 3 + 6t &= 25 \\ 2x &= 22 - 6t \\ x &= 11 - 3t. \end{aligned} \tag{III}$$

Logo, por (II) e (III), temos que $(x_0, y_0) = (11, 1)$ representa uma solução particular da equação diofantina apresentada. Note que temos outras maneiras de resolver essa mesma equação, isto é, existem outros valores para x e y que também satisfazem a equação, o que chamamos de solução geral.

Portanto, concluímos que a solução geral da equação diofantina é:

$$\begin{cases} x = 11 - 3t \\ y = 1 + 2t \end{cases}, \quad \text{com } t \in \mathbb{Z}.$$

Poderíamos ter resolvido, por exemplo, a equação diofantina em questão de outra maneira, adotando agora mod 3, pois 3 também é um dos coeficientes da equação apresentada. Assim obtemos:

$$2x + 3y \equiv 25 \bmod 3$$

Conservando o coeficiente 2, temos que os coeficentes 3 e 25 deixam resto 0 e 1 respectivamente quando divididos por 3. Substituindo na congruência, obtemos:

$$2x + 0y \equiv 1 \bmod 3 \implies 2x \equiv 1 \bmod 3$$

Nesta etapa, precisamos encontrar um valor para x de modo que, quando multiplicado por 2 deixa resto 1 na divisão por 3. Logo, concluímos que um possível valor é 2, pois $2 \cdot 2 = 4$ e 4 deixa resto 1 na divisão por 3. Assim temos que:

$$x \equiv 2 \bmod 3$$

Assim, podemos escrever que:

$$x = 2 + 3s \quad \text{(IV)}, \quad \text{com } s \in \mathbb{Z}.$$

Substituindo (IV) em (I), obtemos:

$$\begin{aligned} 4 + 6s + 3y &= 25 \\ 3y &= 21 - 6s \\ y &= 7 - 2s, \quad s \in \mathbb{Z}. \end{aligned} \tag{V}$$

Assim, por (IV) e (V), temos que $(x_0, y_0) = (2, 7)$ representa também uma solução particular da equação diofantina. Portanto, concluímos que a solução abaixo também representa uma solução geral da equação diofantina em questão:

$$\begin{cases} x = 2 + 3s \\ y = 7 - 2s \end{cases}, \quad \text{com } s \in \mathbb{Z}.$$

Ao fazer s percorrer todos os inteiros, obtemos um conjunto solução único, embora ele possa ser expresso por diferentes parametrizações.

Exemplo 3.15. De quantos modos podemos comprar selos de cinco e de três reais, de modo a gastar cinquenta reais?

Solução: Considerando x como a quantidade de selos de cinco reais e y como a quantidade de selos de três reais, temos a seguinte equação diofantina linear:

$$5x + 3y = 50, \quad \text{com } x, y \in \mathbb{N} \cup \{0\}. \tag{I}$$

Como $\text{mdc}(5, 3) = 1$, a equação tem solução, pois $\text{mdc}(5, 3) \mid 50$. Primeiramente decidimos resolver a equação utilizando mod 5, pois 5 é um dos coeficientes da equação diofantina apresentada. Assim temos:

$$5x + 3y \equiv 50 \bmod 5$$

Conservando o coeficiente 3, temos que os coeficientes 5 e 50 deixam resto 0 quando divididos por 5. Logo obtemos:

$$0x + 3y \equiv 0 \bmod 5 \implies 3y \equiv 0 \bmod 5$$

Nesta etapa, precisamos encontrar um valor para y, de modo que $3 \cdot y$ deixa resto 0 quando dividido por 5. Um possível valor é $y = 0$, logo:

$$y \equiv 0 \bmod 5$$

Assim, podemos escrever que:

$$y = 0 + 5t, \quad \text{com } t \in \mathbb{N} \cup \{0\}. \tag{II}$$

Substituindo (II) em (I), obtemos:

$$5x + 3 \cdot (5t) = 50 \implies 5x + 15t = 50$$

Isolando $5x$ e simplificando a equação, segue que

$$5x = 50 - 15t \implies x = 10 - 3t, \quad \text{com } t \in \mathbb{N} \cup \{0\}.$$

A solução geral da equação diofantina em questão é:

$$\begin{cases} x = 10 - 3t \\ y = 5t \end{cases}, \quad \text{com } t \in \mathbb{Z}.$$

Como estamos à procura de soluções inteiras não negativas apenas, temos a seguinte condição:

$$x \geq 0 \implies 10 - 3t \geq 0$$

$$y \geq 0 \implies 5t \geq 0$$

Assim, o problema admite os seguintes valores para t:

$$0 \leq t \leq 3.$$

Logo, concluímos que os valores que satisfazem o problema apresentado são: $(10, 0)$; $(7, 5)$; $(4, 10)$; $(1, 15)$, totalizando 4 modos diferentes.

Capítulo

4

Um Percurso Didático para Equações Diofantinas

O estudo de equações do primeiro grau com duas incógnitas é fundamental para o desenvolvimento do raciocínio lógico e da capacidade de resolução de problemas, habilidades essenciais tanto no ambiente escolar quanto em situações do cotidiano. Essas equações permitem ao aluno compreender como diferentes variáveis se relacionam e interagem, proporcionando uma visão mais ampla dos conceitos matemáticos e suas aplicações práticas. As atividades aqui propostas apresentam diversas metodologias de resoluções, provocando os educandos à investigação e à pesquisa por meio de situações-problemas contextualizadas, tornando-os instigadores e curiosos, levando-os a desenvolver, além de seu raciocínio lógico, suas interpretações e análises de problemas antes vistos apenas numericamente, estimulando assim o seu prazer em estudar matemática.

Tal estudo vem ao encontro com as competências e habilidades que a BNCC (Base Nacional Comum Curricular) da área de Matemática e suas Tecnologias propõe, que é de proporcionar ao educando, diante de situações problemas que envolvam o tema apresentado nesta dissertação, conhecimento ou pré-requisitos necessários para que sejam capazes de, logo no início, identificar os conceitos e procedimentos matemáticos que possam ser utilizados na chamada formulação matemática do problema. Depois disso, eles devem aplicar esses conceitos, executar procedimentos e, ao final, compatibilizar os resultados com o problema original, comunicando a solução aos colegas por meio de argumentação consistente. Dentre as habilidades elencadas pela BNCC para o Ensino Médio, visando o desenvolvimento da Competência Específica 3: Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos – Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente, destacamos a

habilidade que será enfatizada por este trabalho:

- **(EM13MAT301)** Resolver e elaborar problemas do cotidiano, da Matemática e de outras áreas do conhecimento, que envolvem equações lineares simultâneas, usando técnicas algébricas e gráficas, incluindo ou não tecnologias digitais.

OBJETIVO GERAL:

- Introduzir o estudo de equações diofantinas no Ensino Médio e apresentar a congruência modular como uma ferramenta alternativa e prática para sua resolução.

OBJETIVOS ESPECÍFICOS:

- Compreender que as equações diofantinas formam uma classe específica de equações polinomiais, cujas soluções estão exclusivamente relacionadas a números inteiros.
- Aplicar os conceitos de equações diofantinas e congruência modular na resolução de equações com duas incógnitas, visando desenvolver a habilidade de buscar soluções inteiras para problemas que envolvem relações entre quantidades discretas, incentivando os educandos a explorar métodos algébricos e aritméticos, compreendendo a natureza das soluções inteiras e como encontrá-las, quando elas existirem.

PÚBLICO ALVO: As atividades foram pensadas para serem aplicadas a alunos que estão cursando o 1° Ano do Ensino Médio, por já possuírem uma bagagem de conhecimentos ou pré-requisitos necessários para a compreensão do conteúdo que será desenvolvido.

RECOMENDAÇÕES METODOLÓGICAS: A proposta das atividades foi pensada para serem aplicadas em seis encontros com duração de 1 hora e 40 minutos cada.

MATERIAL NECESSÁRIO: Celular, chromebook ou computador com acesso à internet, caderno, caneta, lápis, calculadora.

PRÉ-REQUISITOS: Os pré-requisitos necessários para a realização das atividades são:

1. Equações e Sistemas Polinomiais do 1° grau;
2. Cálculo do Máximo Divisor Comum – (mdc);
3. Operações com Números Inteiros (Adição, Subtração, Multiplicação e Divisão);
4. Congruência Modular e suas Propriedades.

Apresentamos, a seguir, as atividades propostas. As referências foram baseadas em Brasil [4], Grando [12], Hefez [14], Iezzi [15], OBMEP [22].

4.1 Itinerário Pedagógico

Espera-se que a sequência de atividades aqui delineada contribua para a formação dos estudantes, estimulando não apenas a resolução algorítmica, mas também a reflexão crítica acerca das propriedades e aplicações das equações diofantinas e da congruência modular.

Segundo Zabala, sequência didática é definida como "Um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos." (ZABALA, 1998).

Atividade 1

Num primeiro momento com os discentes, aconselhamos uma breve revisão de conteúdos considerados pré-requisitos para o aprendizado de equações diofantinas, como problemas que envolvam o máximo divisor comum, equações de primeiro grau e sistemas de equações de primeiro grau com duas variáveis. Para tanto, trazemos alguns exemplos de exercícios a serem trabalhados e desenvolvidos com os alunos.

Problema 1: Kárita presenteará as mulheres da sua família com brincos e colares. Ela possui 18 brincos e 24 colares. Ela deseja empacotar os kits com brinco e colar utilizando-se do menor número de pacotes possível e de modo que a quantidade de colares e a quantidade de brincos de um kit para o outro seja a mesma e o mínimo possível. A quantidade de kits que a Kárita conseguirá montar é de:

a) 6 kits b) 4 kits c) 3 kits d) 2 kits e) 1 kit

Solução: Aplicando-se o algoritmo de Euclides, utilizando as propriedades listadas nos capítulos anteriores, temos que o mdc(18,24) é:

	1	3
24	18	6
6	0	

Portanto, encontramos que o máximo divisor comum entre $(24, 18) = 6$. Como o máximo divisor comum entre 18 e 24 é 6, temos que $18 : 6 = 3$ e $24 : 6 = 4$. Logo serão feitos 6 kits, cada um contendo 3 brincos e 4 colares. Assim, a alternativa correta é a).

Problema 2: Enzo e Laís colheram 162 laranjas e querem reparti-las de modo que Laís fique com 10 a mais que Enzo. Quantas laranjas deve receber cada um?

Solução: Vamos resolver este problema utilizando uma equação linear. Seja x o número

de laranjas que Enzo vai receber. Assim, Laís receberá $x + 10$, pois ela deve ficar com 10 laranjas a mais que Enzo. A soma das laranjas de Enzo e Laís deve ser igual a 162. Podemos então montar a seguinte equação:

$$x + (x + 10) = 162$$

Simplificando:

$$2x + 10 = 162$$

Subtraindo 10 de ambos os lados:

$$2x = 152$$

Agora, dividimos ambos os lados por 2:

$$x = \frac{152}{2} = 76$$

Portanto, Enzo vai receber 76 laranjas. Como Laís recebe 10 laranjas a mais, ela ficará com $76 + 10 = 86$ laranjas.

Problema 3: Dona Luana e seu Ênio, pais de Miguel, promoveram uma festinha dos amigos de classe do filho. Cada menino levou mais dois meninos convidados, e cada menina, mais uma menina convidada. Ao todo, compareceram os 25 alunos da classe e mais 35 convidados. Quantos meninos e quantas meninas compõem a classe do Miguel?

Solução: O presente exercício trata de um sistema de equações de primeiro grau. Para resolvê-lo, os alunos devem identificar os dados no enunciado, montar as equações e, em seguida, resolvê-las.

Problema com duas incógnitas: Neste problema, temos x como o número de meninos da classe e y como o número de meninas. Sabemos que a classe tem 25 alunos, logo temos a equação:

$$x + y = 25$$

Além disso, ao todo, foram 35 convidados. Cada menino levou 2 amigos, logo, o total de convidados meninos é $2x$. Cada menina levou uma amiga, o total de meninas convidadas é y. A soma dos convidados é dada pela equação:

$$2x + y = 35$$

Com essas duas equações, temos o seguinte sistema:

$$\begin{cases} x + y = 25 \\ 2x + y = 35 \end{cases}$$

Para resolver o sistema pelo método de substituição, isolamos y na primeira equação:

$$x + y = 25 \quad \Longrightarrow \quad y = 25 - x$$

Substituímos essa expressão de y na segunda equação:

$$2x + (25 - x) = 35 \quad \Longrightarrow \quad 2x + 25 - x = 35 \quad \Longrightarrow \quad x = 10$$

Agora, substituímos $x = 10$ na expressão de $y = 25 - x$:

$$y = 25 - 10 \quad \Longrightarrow \quad y = 15$$

Portanto, a classe tem 10 meninos e 15 meninas.

Atividade 2

Num segundo momento, trazemos para aula a apresentação da definição formal de equações diofantinas.

Problema 1: Considere a seguinte equação $21x + 48y = 6$.

Temos uma equação diofantina do tipo $ax + by = c$, onde $a = 21$, $b = 48$ e $c = 6$, sendo x, y as incógnitas a serem encontradas, como as soluções da equação. Uma equação diofantina terá solução se, e somente se, mdc(a, b) dividir c.

Vamos verificar se a equação dada tem solução utilizando o algoritmo de Euclides para determinarmos mdc$(21, 48)$. Então:

	2	3	2
48	21	6	3
6	3	0	

Logo, encontramos que o mdc$(48, 21) = 3$. Daí, segue que:

$$48 = 21 \cdot 2 + 6 \quad \Longrightarrow \quad 48 - 42 = 6$$

$$21 = 6 \cdot 3 + 3 \quad \Longrightarrow \quad 21 - 18 = 3$$

Como o mdc$(21, 48) \mid 6$, temos que a equação possui solução. Agora, expressando 3 como uma combinação linear, temos:

$$3 = 21 - 18$$

$$3 = 21 - 3 \cdot 6$$

$$3 = 21 - 3 \cdot (48 - 42)$$

$$3 = 21 - 3 \cdot 48 + 3 \cdot 42$$

$$3 = 21 - 3 \cdot 48 + 126$$

$$3 = 147 - 3 \cdot 48$$

$$3 = 21 \cdot 7 - 3 \cdot 48$$

$$3 = 21 \cdot 7 + 48 \cdot (-3)$$

Logo, temos que:

$$21 \cdot 7 + 48 \cdot (-3) = 3.$$

Multiplicando essa igualdade por 2, temos:

$$21 \cdot 14 + 48 \cdot (-6) = 6.$$

Concluímos, então, que $(x_0, y_0) = (14, -6)$ representa uma solução particular da equação dada. A solução geral da equação diofantina em questão é:

$$\begin{cases} x = 14 + 16t \\ y = -6 - 7t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Atividade 3

Neste terceiro momento, vamos introduzir a grande ideia de Gauss de desenvolver uma aritmética dos restos da divisão por um certo número fixado.

Definição 4.1. *Seja dado um número inteiro maior do que 1. Dizemos que dois números inteiros a e b são congruentes módulo n se a e b possuírem o mesmo resto quando divididos por n. Neste caso, simbolizaremos esta situação da seguinte maneira:*

$$a \equiv b \bmod n.$$

Quando a e b não são congruentes módulo n, escreve-se:

$$a \not\equiv b \bmod n.$$

Exemplo 4.1. Vejamos alguns exemplos de congruência:

a) $15 \equiv 8 \bmod 7$, pois os restos das divisões de 15 e 8 por 7 são os mesmos (iguais a 1).

b) $27 \equiv 32 \bmod 5$, pois os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2).

c) $35 \equiv 27 \bmod 4$, pois os restos das divisões de 35 e 27 por 4 são os mesmos (iguais a 3).

d) $29 \not\equiv 31 \bmod 3$, pois o resto da divisão de 29 por 3 é 2, enquanto o resto da divisão de 31 por 3 é 1.

Para mostrar que $a \equiv b \bmod n$, não é necessário efetuar a divisão de a e b por n, como mostrado nos exemplos anteriores, bastando verificar se n divide $(b - a)$.

Atividade 4

Num quarto e último momento, traremos mais um exercício cuja solução envolve o emprego das equações diofantinas, apresentando dois métodos diferentes. Enquanto na **solução 1** utilizaremos a ideia de plano cartesiano, ou seja, os alunos deverão encontrar valores para x e y, que serão pares ordenados que satisfaçam a equação e marcá-los no plano cartesiano. Ressaltamos que, na reta obtida, muitas vezes nem todos os pontos solucionam a situação-problema apresentada, dependendo das particularidades enunciadas no corpo da questão. Na **solução 2**, traremos uma solução por meio da congruência modular, como veremos a seguir.

Problema 1: Em um evento de matemática da escola, há 77 participantes. Para realizar uma dinâmica, a comissão organizadora do evento deseja separar os participantes em grupos de 7 e 14 pessoas. Quantos grupos de 7 pessoas e quantos grupos de 14 pessoas podem ser formados? Liste os casos possíveis.

Solução 1: Pelos dados apresentados no problema, consideremos x para representar a quantidade de grupos contendo 7 participantes e y a quantidade de grupos contendo 14 participantes. Concluímos que a situação pode ser representada pela seguinte equação diofantina com duas variáveis:

$$7x + 14y = 77$$

Essa equação pode ser representada no plano cartesiano através dos pares ordenados contidos na reta:

$$14y = 77 - 7x$$

Dividindo a equação por 7, obtemos:

$$2y = 11 - x$$

ou equivalentemente:

$$y = \frac{11 - x}{2}$$

com $1 \leq x \leq 11$, pois queremos encontrar soluções inteiras e não negativas para a equação.

Assim, atribuindo valores a x, encontramos o valor de y, formando nossos pares ordenados. Observamos, porém, que x deve ser um número ímpar, não negativo, e menor

ou igual a 11, para que a equação tenha as soluções desejadas. Portanto:

$$\begin{aligned}
&\text{Quando } x = 1 \quad \Longrightarrow \quad y = \frac{11-1}{2} \quad \Longrightarrow \quad y = 5 \quad \Longrightarrow \quad A = (1,5),\\
&\text{Quando } x = 3 \quad \Longrightarrow \quad y = \frac{11-3}{2} \quad \Longrightarrow \quad y = 4 \quad \Longrightarrow \quad B = (3,4),\\
&\text{Quando } x = 5 \quad \Longrightarrow \quad y = \frac{11-5}{2} \quad \Longrightarrow \quad y = 3 \quad \Longrightarrow \quad C = (5,3),\\
&\text{Quando } x = 7 \quad \Longrightarrow \quad y = \frac{11-7}{2} \quad \Longrightarrow \quad y = 2 \quad \Longrightarrow \quad D = (7,2),\\
&\text{Quando } x = 9 \quad \Longrightarrow \quad y = \frac{11-9}{2} \quad \Longrightarrow \quad y = 1 \quad \Longrightarrow \quad E = (9,1),\\
&\text{Quando } x = 11 \quad \Longrightarrow \quad y = \frac{11-11}{2} \quad \Longrightarrow \quad y = 0 \quad \Longrightarrow \quad F = (11,0).
\end{aligned}$$

Portanto, encontramos 6 pares ordenados que satisfazem a equação: $A = (1,5)$, $B = (3,4)$, $C = (5,3)$, $D = (7,2)$, $E = (9,1)$ e $F = (11,0)$.

Resta-nos, agora, colocá-los no plano cartesiano e, assim, encontrar a reta que contém o conjunto discreto formado pelos pares ordenados que representam geometricamente a solução da equação diofantina apresentada.

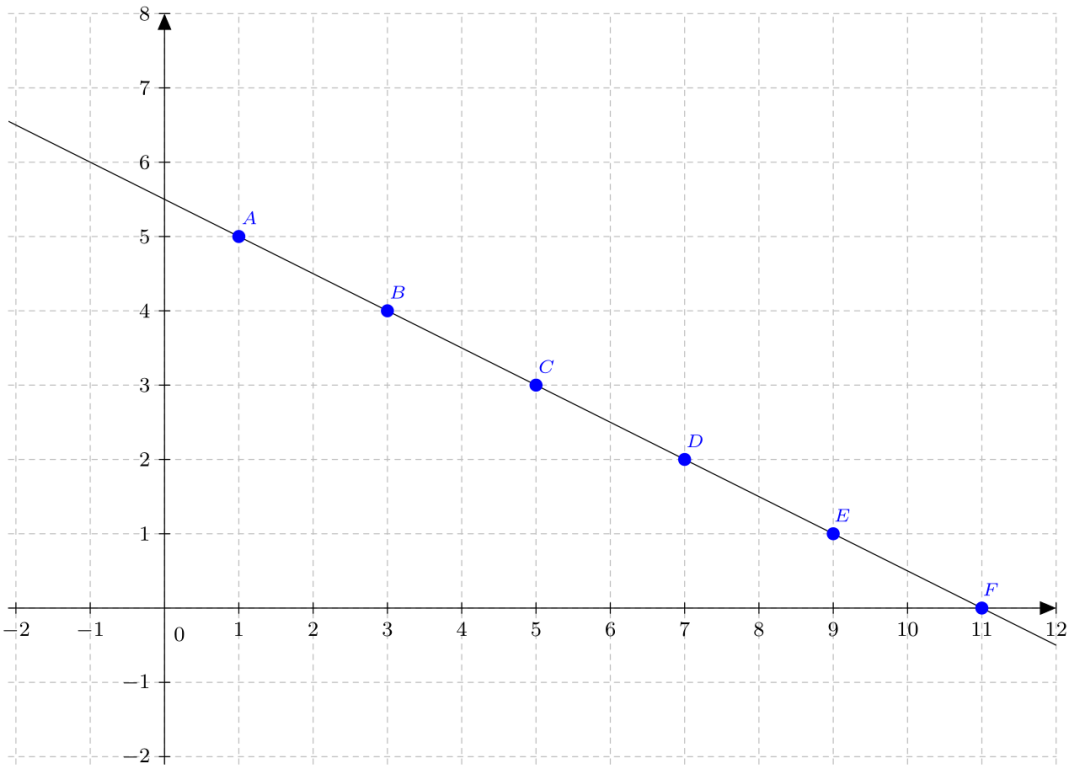


Figura 4.1: Soluções Inteiras e não Negativas da Equação Linear 7x + 14y =77

Solução 2: Agora, resolveremos o **Problema 1** utilizando a **congruência modular**. Consideramos a equação linear:

$$7x + 14y = 77$$

Dividindo ambos os lados por 7, obtemos:

$$x + 2y = 11 \tag{I}$$

Aplicando o conceito de congruência modular, temos:

$$x + 2y \equiv 11 \pmod 2 \quad \Longrightarrow \quad x \equiv 1 \pmod 2 \quad \Longrightarrow \quad x = 1 + 2t \tag{II}$$

onde $t \in \mathbb{Z}$. Substituindo a expressão de x dada por (II) na equação (I), obtemos:

$$(1 + 2t) + 2y = 11 \quad \Longrightarrow \quad 2y = 10 - 2t \quad \Longrightarrow \quad y = 5 - t \tag{III}$$

com $t \in \mathbb{Z}$. A partir das soluções encontradas nas equações (II) e (III), concluímos que a solução particular da equação dada é:

$$(x_0, y_0) = (1, 5).$$

Portanto, a solução geral da equação diofantina é dada por:

$$\begin{cases} x = 1 + 2t \\ y = 5 - t \end{cases} \quad \text{com } t \in \mathbb{Z}.$$

Como estamos à procura de soluções inteiras não negativas, temos as seguintes condições:

$$x \geq 0 \quad \Longrightarrow \quad 1 + 2t \geq 0 \quad \Longrightarrow \quad t \geq -\frac{1}{2}$$

$$y \geq 0 \quad \Longrightarrow \quad 5 - t \geq 0 \quad \Longrightarrow \quad t \leq 5$$

Logo, como t é um número inteiro, concluímos que:

$$0 \leq t \leq 5.$$

Encontramos, assim, seis soluções para a mesma equação, ou seja:

$$(1, 5);\ (3, 4);\ (5, 3);\ (7, 2);\ (9, 1);\ (11, 0).$$

Ao todo, obtemos 6 pares ordenados que satisfazem a situação-problema apresentada.

4.2 Jogos Matemáticos

No Ensino Médio, o uso de jogos nas aulas de Matemática é pouco frequente. Isso ocorre, principalmente, devido à ênfase em conteúdos que vão de encontro à preparação para os exames de ingresso no ensino superior, o que dificulta a inclusão de atividades lúdicas no processo pedagógico. Além disso, a necessidade de cumprir todo o extenso conteúdo programático previsto e, atualmente, com a reduzida carga horária da disciplina, faz com que os professores recorram, na maioria das vezes, aos mesmos métodos tradicionais de ensino, como o uso do livro didático, do quadro branco, a resolução de listas de exercícios padronizados e a apresentação de seminários.

> "O jogo propicia um ambiente favorável ao interesse da criança, não apenas pelos objetos que o constituem, mas também pelo desafio das regras impostas por uma situação imaginária que, por sua vez, pode ser considerada como um meio para o desenvolvimento do pensamento abstrato".(GRANDO, 2004)

É essencial envolver os estudantes em atividades que favoreçam a transição da imaginação para a abstração. Esse processo deve ocorrer por meio da formulação de hipóteses, da experimentação de conjecturas, da reflexão, da análise e da síntese, permitindo que elas desenvolvam estratégias variadas para a resolução de problemas em contextos lúdicos.

4.2.1 Jogo das "Equações Diofantinas Lineares com Cartas ou Dados"

Objetivo

Resolver equações diofantinas lineares geradas a partir de cartas ou dados, promovendo o aprendizado de forma lúdica e interativa.

Material Necessário

- Um baralho comum (52 cartas, sem os curingas) ou 3 dados comuns (opcional, para variação do jogo).
- Papel e lápis para cada jogador ou equipe.

Definições e Valores das Cartas

- **Ás:** valor 1.
- **Cartas numéricas (2 a 10):** valor igual ao número na carta.

- **Valete, Dama e Rei:** valores 11, 12 e 13, respectivamente.
- Os naipes são ignorados para fins de cálculo.

Regras do Jogo

1. Distribuir as Cartas

   Cada jogador ou equipe começa com 5 cartas ou 3 dados.

2. Gerar a Equação

   - Dois valores são retirados (de cartas ou dados) e se tornam os coeficientes a e b da equação diofantina linear:

   $$ax + by = c$$

   - O valor de c pode ser gerado de duas formas:
     - Se utilizar o baralho, sorteando e somando duas outras cartas.
     - Se utilizar os dados, lançando um dado (ou somando o valor de três dados).

3. Resolver a Equação Os jogadores ou equipes devem encontrar uma solução inteira para os valores de x e y. Dependendo do nível do jogo, pode-se restringir as soluções a números inteiros positivos ou permitir qualquer inteiro.

4. Pontuação

   - O jogador ou equipe que primeiro apresentar corretamente uma solução particular ou demonstrar de forma válida a inexistência de soluções inteiras para a equação receberá 10 pontos.
   - **Bônus:** 5 pontos extras se identificar corretamente a solução geral da equação, que tem a forma:

   $$x = x_0 + kb, \quad y = y_0 - ka, \quad \text{com } k \in \mathbb{Z}.$$

Variações do Jogo

- **Nível Fácil:** Use valores pequenos para a e b (≤ 6).
- **Nível Difícil:** Inclua valores maiores de a, b e c para aumentar a complexidade.
- **Com Dados:** Substitua o baralho por dois ou três dados para gerar a, b e c.
- **Desafios Extras:** Restrinja as soluções a números positivos ou imponha condições adicionais (ex.: $x > y$, ou $x, y \geq 0$).

Exemplo de Rodada

1. **Cartas retiradas:** 7 e 3. Esses valores definem os coeficientes $a = 7$ e $b = 3$.
2. **Valor de c :** Sortear duas outras cartas, por exemplo 4 e 8, que somadas determinam: $c = 4 + 8 = 12$.
3. **Equação gerada:**
$$7x + 3y = 12$$
4. **Solução:** Os jogadores devem encontrar os valores de x e y que satisfazem a equação. Uma solução possível é $x = 3$, $y = -3$.
5. **Solução Geral:**
$$x = 3 + 3k, \quad y = -3 - 7k, \quad \text{com } k \in \mathbb{Z}.$$

Contribuições do Jogo no Processo de Ensino Aprendizagem

- Desenvolve o raciocínio lógico e habilidades matemáticas.
- Introduz conceitos de forma lúdica e prática.
- Incentiva o trabalho em equipe e a competição saudável.

4.2.2 Jogo: "Desafio Diofantino"

Os jogadores competem para encontrar o número de soluções de uma equação diofantina linear gerada aleatoriamente com base no lançamento de dados e sorteio de cartas. Quem encontrar a solução mais rápido ou acumular mais pontos vence.

Materiais Necessários

- Dois dados comuns de seis lados (D6) para gerar os coeficientes.
- Um baralho com cartas numeradas de 1 a 10 (ou cartas do baralho tradicional, ignorando os naipes).
- Papel e lápis para cada jogador.
- 15 fichas ou marcadores para cada jogador.

Configuração do Jogo:

Cada jogador recebe 15 fichas para contabilizar os pontos.

Dinâmica do Jogo:

1. O professor regente é escolhido como o "Mestre Diofantino".
2. O Mestre lança os dois dados para gerar os coeficientes a e b.
3. O Mestre sorteia uma carta do baralho para definir o valor de c.
4. A equação montada é da forma:

$$ax + by = c$$

   onde a e b são os números obtidos nos dados, e c é o número da carta.

5. Os jogadores têm 1 minuto para encontrar pelo menos uma solução inteira para (x, y) ou demonstrar de forma válida a inexistência de soluções inteiras para a equação.
6. Cada solução encontrada deve ser validada pelo Mestre.

Pontuação

- O primeiro jogador a encontrar uma solução correta recebe 2 fichas.
- Outros jogadores que apresentarem soluções corretas dentro do tempo recebem 1 ficha.
- Se ninguém encontrar a solução, o Mestre Diofantino ganha 1 ficha.

Fim do Jogo

O jogo termina quando um jogador acumular 15 fichas, ou após 20 rodadas. O jogador com mais fichas ao final vence.

Exemplo de Rodada

- O Mestre lança os dados e obtém $a = 3$ e $b = 4$.
- Uma carta é sorteada, digamos $c = 10$.
- A equação formada é:

$$3x + 4y = 10$$

- Os jogadores tentam resolver a equação.
  - Um jogador encontra $(x = 2, y = 1)$, valida com o Mestre e ganha 2 fichas.
  - Outro jogador apresenta $(x = -2, y = 4)$ e também é validado, ganhando 1 ficha.

4.2.3 Jogo: "Diofantus: O Enigma dos Números"

O jogo é composto por:

- Um tabuleiro que possui um percurso com 40 casas, conforme a Figura 4.2;
- 20 cartas com questões ou situações-problema a serem resolvidas, conforme a Figura 4.3;
- Um dado cúbico, numerado de 1 a 6;
- Sete peças de cores diferentes, para identificação de cada uma das equipes.

Observações:

- Será reservado, na mesa do jogo, um espaço ao lado do tabuleiro para posicionar as 20 cartas-questões, garantindo o desenvolvimento da atividade.
- Com relação às casas do tabuleiro, existem quatro tipos, conforme a Figura 4.5.

Regras e Desenvolvimento do Jogo

1. Os estudantes devem ser divididos em equipes compostas por aproximadamente 6 componentes.
2. No dia da aplicação do jogo, os membros de cada equipe se apresentarão utilizando camisetas na cor sorteada no dia anterior, compondo assim as equipes: azul, preta, amarela, verde, vermelha, entre outras, variando de acordo com o número de alunos da turma. Será disponibilizada uma peça de acordo com a cor da equipe para ser utilizada no tabuleiro.
3. A sala de aula será organizada conforme o mapa Figura 4.4 no dia da aplicação do jogo: "Diofantus: O Enigma dos Números". Cada equipe deverá eleger um membro que será o "Capitão", responsável por realizar os comandos do jogo (lançar o dado, mover a peça da equipe no tabuleiro, retirar e ler em voz alta a carta-questão quando a peça de sua equipe ocupar a "Casa do Diofanto").

4. Para o início do jogo, o estudante "Capitão" escolhido de cada equipe retira uma bola da urna contendo todas as cores das equipes participantes, definindo assim a ordem do jogo. Posicionada a primeira equipe, as demais devem se organizar no sentido horário, respeitando a sequência do sorteio.

5. As 20 cartas-questões devem ser embaralhadas pelo docente e colocadas em monte no espaço da mesa do jogo, junto ao tabuleiro, com as questões voltadas para baixo. As cartas-resposta ficam sob a posse do professor/mediador.

6. As equipes jogam o dado, de acordo com a ordem estabelecida, e percorrem as casas correspondentes ao número obtido, observando os seguintes critérios:

   (a) Caso a peça seja movida para uma casa branca, a próxima equipe joga o dado e a partida continua.

   (b) Caso a peça seja movida para a "Casa do Diofanto", o jogador representante da equipe retira a carta superior do monte e deve lê-la em voz alta para todas as equipes (de maneira clara, por duas vezes) e devolvê-la ao final do monte. Após o sinal de "valendo" do mediador, todas as equipes deverão encontrar uma solução dentro do tempo máximo de 6 minutos. Finalizado o tempo, que será administrado pelo professor, o aluno "Capitão" entregará a folha-resposta para o professor/mediador, que julgará como certo ou errado.

      - Se a solução estiver correta, a peça da equipe permanece na "Casa do Diofanto" e a próxima equipe continua a partida.
      - Caso contrário, a peça deve voltar para a última casa em que estava antes do lançamento do dado, e a próxima equipe (no sentido horário) tem a oportunidade de apresentar sua solução. Na situação em que nenhuma das demais equipes apresente uma possível solução, uma nova carta-questão será retirada pelo professor/mediador e enunciada às equipes para resolução dentro do prazo de mais 6 minutos. Finalizado tempo, e respeitando a ordem de sorteio inicial, a primeira equipe tem a oportunidade de resposta novamente, passando "a vez" para a próxima equipe em caso de resposta errada, e assim sucessivamente.
        A cada resposta correta relativa às questões das "Casas do Diofanto", a equipe somará 10 pontos.

   (c) Caso a peça seja movida para uma casa de avanço, a equipe move sua peça imediatamente de acordo com o valor apresentado. Caso a peça caia na "Casa do Diofanto", segue-se o procedimento descrito na regra 6 (b).

      - Se uma equipe precisar responder à mesma questão mais de uma vez, deverá apresentar uma solução distinta da já exposta anteriormente. O

registro e controle das soluções mencionadas ficarão sob a supervisão do professor/mediador.

- O método de resolução das questões apresentadas no jogo será definido pelos alunos, que poderão utilizar todos os recursos abordados nesta dissertação.
- As questões que eventualmente não forem resolvidas pelas equipes serão discutidas e solucionadas pelo professor no quadro, com a participação dos educandos, visando esclarecer dúvidas e dificuldades relacionadas aos conceitos abordados em sala de aula durante a aplicação do projeto.

(d) Será considerada vencedora a equipe que, após alcançar a casa 'Fim', obtiver a maior pontuação. A premiação será realizada com a entrega de medalhas, conforme descrito a seguir:

- 1ª colocação: medalha de ouro;
- 2ª colocação: medalha de prata;
- 3ª colocação: medalha de bronze.

7. Toda a turma será premiada pelo empenho e participação na atividade com um lanche especial, elaborado pela equipe de nutrição da unidade escolar.

Organização e Representação Visual do Jogo Pedagógico

Figura 4.2: Tabuleiro do Jogo/Imagem: Wellington Gonzales Engenharia

Escreva a solução geral em Z da seguinte equação diofantina:

$3x + 7y = 33$.

CARTA 1

De quantas maneiras podemos trocar uma nota de R$ 20,00 por moedas de R$0,10 e R$0,25?

CARTA 2

De quantos modos diferentes podemos gastar R$50,00 comprando borrachas de R$3,00 ou canetas de R$5,00?

CARTA 3

Resolva a equação $4x + 6y = 10$, enunciando uma solução particular e a solução geral.

CARTA 4

(Colégio Naval) Um funcionário usa uma empilhadeira para transportar bobinas de 70kg ou de 45kg, sendo uma de cada vez. Quantas viagens com carga deverá fazer, no mínimo, para transportar exatamente uma tonelada dessa carga?

CARTA 5

(Colégio Naval) Seja A o conjunto formado pelos pares (x,y), onde x e y são inteiros positivos tais que $2x + 3y = 2018$. Sendo assim, é correto afirmar que a quantidade de elementos do conjunto A é:

a)256 b)336 c)512 d)640 e)720

CARTA 6

Um teatro cobra R$1,80 pelo ingresso de um adulto e R$0,75 por criança. Em uma determinada noite foram arrecadados R$90,00. Admitindo que o número de adultos foi maior que o de crianças, quantas pessoas compareceram?

CARTA 7

Havia 63 pencas de banana iguais junto a 7 bananas. Elas foram divididas igualmente entre 23 viajantes. Qual é o número de bananas em cada penca?

CARTA 8

Como dividir um total de 109 balas em saquinhos, com 3 e 7 balas em cada um, de modo que não sobre nenhum?

CARTA 9

Em um pátio do DETRAN, sabe-se que há 400 pneus retirados de carros e motos que foram apreendidos no mês de setembro. Quantos veículos de cada categoria foram apreendidos sabendo que a diferença entre os dois números é a menor possível?

CARTA 10

Um parque de diversão cobra R$ 1,00 a entrada de crianças e R$3,00 a de adultos. Para que a arrecadação de um dia seja R$200,00, qual o maior número de pessoas, entre adultos e crianças, que poderiam frequentar o parque neste dia? Quantas crianças e quantos adultos?

CARTA 11

De quantas maneiras podemos comprar selos de cinco reais e de sete reais, de modo a gastar cem reais?

CARTA 12

Uma empresa paga para cada funcionário R$ 600,00 em tíquetes de alimentação, com valores de R$60,00 e R$120,00 cada tíquete. De quantas formas pode ser organizado o carnê de tíquetes de um funcionário?

CARTA 13

Um cinema disponibiliza, às quintas-feiras, ingressos com valores de R$10,00 pela manhã e R$12,00 pela tarde. De quantas maneiras podem ser vendidos os ingressos para que se tenha um saldo de R$200,00 ao final do dia?

CARTA 14

Marcos é fã de música e reserva, por mês, R$120,00 para comprar CD's e DVD's. Em média, um CD custa R$10,00 e um DVD R$15,00. Quais as possibilidades de aquisição dos itens, gastando exatamente R$120,00?

CARTA 15

Um fazendeiro deseja comprar filhotes de pato e de galinha, gastando um total de R$1770,00. Um filhote de pato custa R$31,00 e um de galinha custa R$21,00. Quantos de cada um dos dois tipos o fazendeiro poderá comprar?

CARTA 16

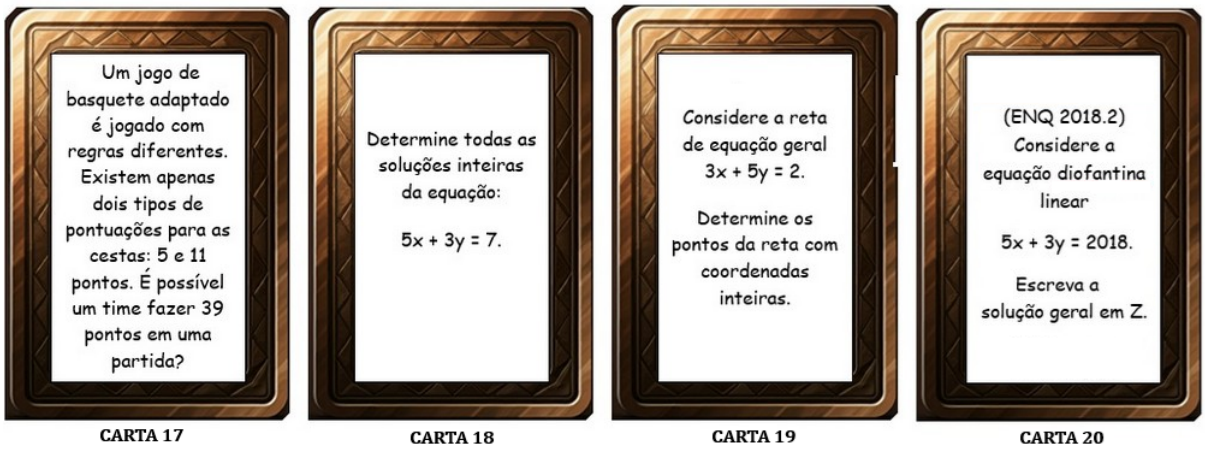


Figura 4.3: Cartas-Questões/Imagem: Próprio Autor

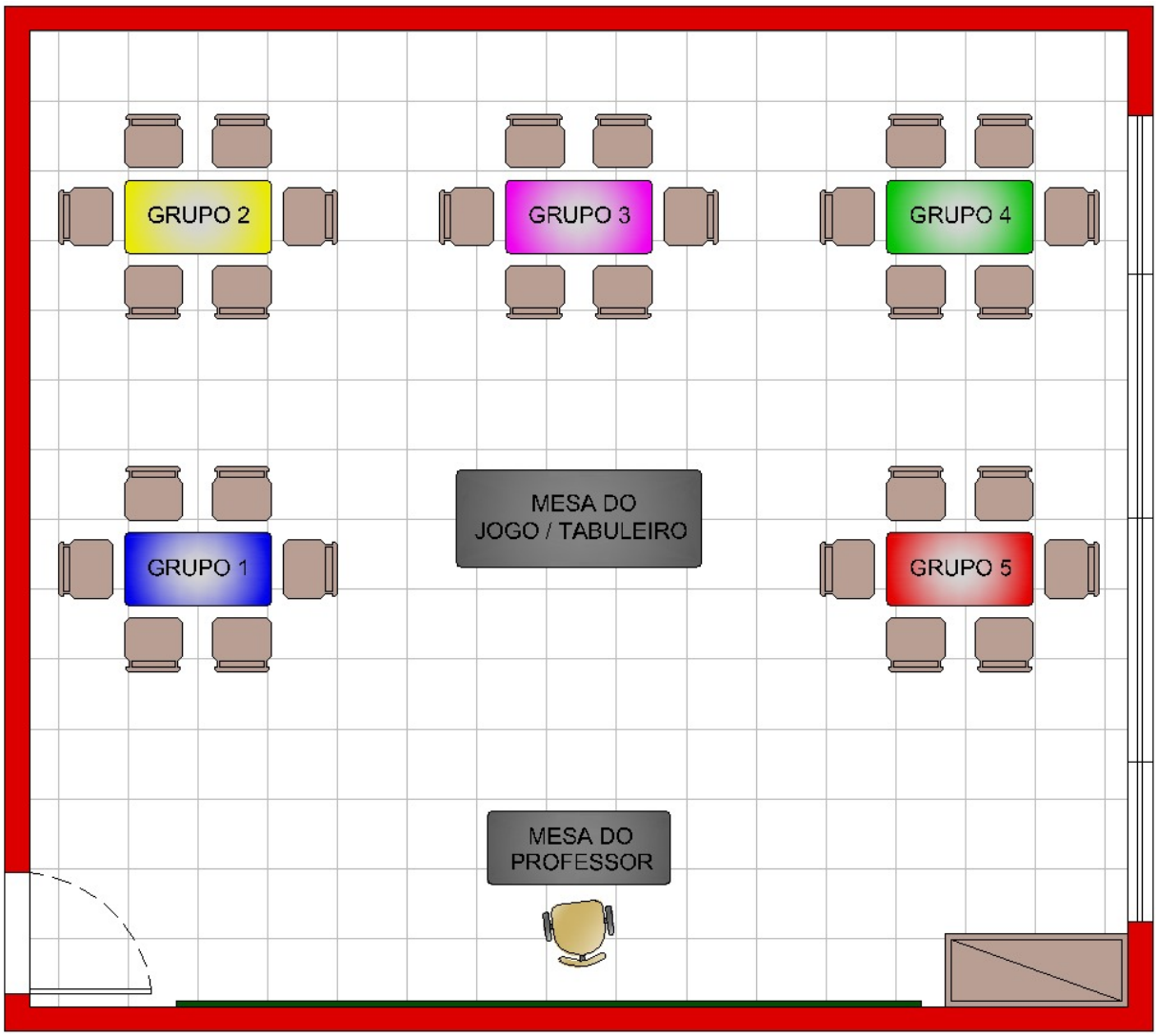


Figura 4.4: Mapa da Sala de Aula/Imagem: Wellington Gonzales Engenharia

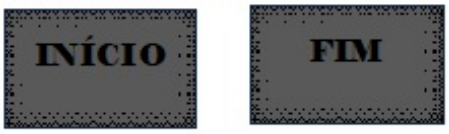
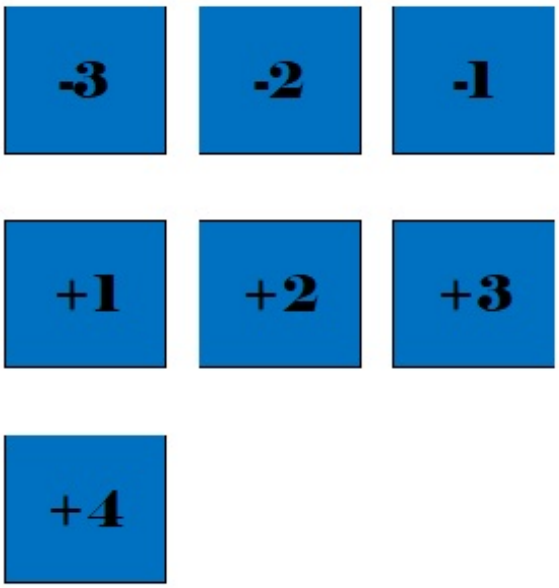
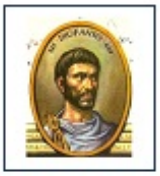
CATEGORIA DA CASA	IMAGEM
Casas de Início e Fim	
Casas Brancas	
Casas de Avanço ou Recuo	
Casas das Cartas	

Figura 4.5: Categoria das Casas

Respostas Esperadas para as Cartas-Questões

Carta 1: Uma solução particular seria:

$$(x_0, y_0) = (4, 3)$$

Logo podemos escrever a seguinte solução geral:

$$\begin{cases} x = 4 + 7t \\ y = 3 - 3t \\ t \in \mathbb{Z} \end{cases}$$

Para representar outras soluções particulares e assim novas soluções gerais, basta variar o valor de t.

Carta 2: Existem 41 maneiras.

Carta 3: Existem 4 modos.

Carta 4: Uma solução particular seria:

$$(x_0, y_0) = (1, 1)$$

Logo podemos escrever a seguinte solução geral:

$$\begin{cases} x = 1 - 3t \\ y = 1 + 2t \\ t \in \mathbb{Z} \end{cases}$$

Para representar outras soluções particulares e assim novas soluções gerais, basta variar o valor de t.

Carta 5: O menor número de viagens são 15, sendo 13 viagens com bobinas de 70 kg e 2 viagens com bobinas de 45 kg.

Carta 6: Alternativa correta é a b) 336.

Carta 7: O enunciado da questão é satisfeito em 3 casos: (45,12) ; (50,0) ; (40,24), respectivamente 57, 50 ou 64 pessoas.

Carta 8: O número de bananas em cada penca pode ser expresso por 28. Nesse caso, cada viajante receberia 77 bananas. Outra solução possível seria 51 bananas em cada penca (nesse caso, cada viajante receberia 140 bananas). Variando o valor do parâmetro na solução geral encontrada, outras soluções poderão ser apresentadas.

Carta 9: Considerando x pacotes contendo 3 balas e y pacotes contendo 7 balas, temos os seguintes pares de solução (x, y): (34,1) ; (27,4) ; (20,7) ; (13,10) ; (6,13), totalizando 5 modos.

Carta 10: Seriam 67 carros e 66 motos no pátio do Detran.

Carta 11: O maior número de pessoas que poderiam frequentar o parque é 200, sendo 200 crianças e 0 adultos.

Carta 12: Existem 3 maneiras. Considerando x selos de cinco reais e y selos de sete reais (x, y), temos as seguintes soluções: (20,0) ; (13,5) ; (6,10).

Carta 13: Existem 6 maneiras. Considerando x tíquetes no valor de sessenta reais e y tíquetes no valor de cento e vinte reais (x, y), temos as seguintes soluções: (0,5) ; (2,4) ; (4,3) ; (6,2) ; (8,1) ; (10,0).

Carta 14: Existem 4 maneiras. Considerando x ingressos no valor de 10 reais e y ingressos no valor de 12 reais (x, y), temos as seguintes soluções: (20,0) ; (14,5) ; (8,10) ; (2,15).

Carta 15: Existem 5 maneiras. Considerando x CD e y DVD e escrevendo (x, y), temos as seguintes soluções: (12,0) ; (9,2) ; (6,4) ; (3,6) ; (0,8).

Carta 16: Existem 3 maneiras. Considerando x o números de patos e y o número de galinhas (x, y), temos as seguintes soluções: (9,71) ; (30,40) ; (51,9).

Carta 17: Não é possível fazer 39 pontos na partida sugerida em questão.

Carta 18: Uma solução particular seria:

$$(x_0, y_0) = (2, -1)$$

Logo podemos escrever a seguinte solução geral:

$$\begin{cases} x = 2 + 3t \\ y = -1 - 5t \\ t \in \mathbb{Z} \end{cases}$$

Para representar outras soluções particulares e assim novas soluções gerais, basta variar o valor de t.

Carta 19: Uma solução particular seria:

$$(x_0, y_0) = (-1, 1)$$

Logo podemos escrever a seguinte solução geral:

$$\begin{cases} x = -1 - 5t \\ y = 1 + 3t \\ t \in \mathbb{Z} \end{cases}$$

Para representar outras soluções particulares e assim novas soluções gerais, basta variar o valor de t.

Carta 20: Uma solução particular seria:

$$(x_0, y_0) = (1, 671)$$

Logo podemos escrever a seguinte solução geral:

$$\begin{cases} x = 1 + 3t \\ y = 671 - 5t \\ t \in \mathbb{Z} \end{cases}$$

Para representar outras soluções particulares e assim novas soluções gerais, basta variar o valor de t.

4.2.4 Resultados Esperados

Trabalhar equações diofantinas na Educação Básica representa uma oportunidade valiosa para estimular o raciocínio lógico e introduzir conceitos fundamentais da teoria dos números, incentivando os alunos a explorarem soluções inteiras para problemas matemáticos. Além disso, a resolução de equações diofantinas simples desenvolve o pensamento crítico e a persistência dos estudantes, que precisam aplicar estratégias criativas e dedutivas para encontrar soluções possíveis, promovendo um entendimento mais profundo da Matemática e sua aplicabilidade.

Com o desenvolvimento das atividades propostas, espera-se que os alunos sejam capazes de aplicar o raciocínio lógico na interpretação e resolução de situações-problema, integrando seus conhecimentos matemáticos para alcançar soluções precisas. Além disso, almeja-se que reconheçam a presença das equações diofantinas em conteúdos previamente estudados, consolidando sua compreensão desses conceitos. O objetivo principal é que os alunos desenvolvam habilidades fundamentais, como identificar, formular, analisar e solucionar problemas envolvendo equações diofantinas, ampliando e aprofundando os aprendizados adquiridos ao longo de sua formação.

Com os conceitos de congruência modular aqui apresentados, presume-se que os educandos utilizem esta ferramenta prática e eficiente na resolução de equações diofantinas, principalmente na resolução das questões propostas no jogo *Diofantus: O Enigma dos*

Números. Ao explorar este conteúdo, espera-se facilitar o desenvolvimento do pensamento abstrato e de habilidades na resolução de problemas, uma vez que diversas situações-problema presentes no dia a dia dos alunos do Ensino Médio podem ser resolvidas utilizando a congruência modular, que nada mais é do que trabalhar com os restos obtidos através da divisão de números inteiros.

Considerações Finais

O estudo das equações diofantinas é um tema amplo e desafiador, que pode atuar como mobilizador de estratégias aritméticas e algébricas no Ensino Médio. Originadas nos trabalhos de Diofanto, um algebrista grego, essas equações são geralmente resolvidas no conjunto dos números inteiros e possuem forte ligação com a teoria dos números.

Através deste trabalho, justifica-se a importância de abordar as equações diofantinas lineares na Educação Básica, especialmente com os alunos do Ensino Médio, demonstrando como o conhecimento desse conteúdo pode ampliar as possibilidades de estratégias para a resolução de equações do tipo $ax + by = c$. Utilizando recursos matemáticos que promovam uma argumentação fundamentada, espera-se que os estudantes evitem limitar-se ao método por tentativa e erro, prática comumente adotada.

Procura-se também apresentar, na maioria dos casos, o conceito de equações diofantinas por meio da abordagem de situações-problema relacionadas ao cotidiano, uma metodologia que tem se mostrado um recurso didático eficaz no processo de ensino e aprendizagem dos alunos.

Outro ponto relevante é a ênfase dada à congruência modular, uma ferramenta importante da teoria dos números, como uma abordagem prática e eficiente no processo de busca por soluções inteiras possíveis para uma equação diofantina.

Ao aplicar-se na resolução de uma equação diofantina, a congruência modular permite simplificar o problema, reduzindo-o em relação a um módulo específico, o que facilita a análise de possíveis soluções inteiras. Esse método possibilita verificar a viabilidade de uma solução antes mesmo de resolver a equação completamente, além de eliminar valores inviáveis para soluções inteiras em certos módulos.

Ao propor a introdução desse conteúdo no Ensino Médio, considerou-se a necessidade de evitar uma formalização excessiva, a fim de não transformar esse ambiente em uma extensão do Ensino Superior, o que se distanciaria dos objetivos previamente estabelecidos. No entanto, a viabilidade dessa abordagem se justifica, uma vez que seus requisitos se fundamentam em conceitos presumivelmente assimilados no Ensino Fundamental e, portanto, acessíveis aos estudantes.

Assim, por meio da análise, da leitura e do estudo da abordagem desta dissertação,

propõe-se uma nova perspectiva sobre a importância do conteúdo de equações diofantinas, bem como de seus métodos de resolução, proporcionando tanto uma explanação concisa quanto a elaboração de um plano de ação que pode constituir uma ferramenta didática para professores da Educação Básica.

Referências Bibliográficas

[1] BEZERRA, Maria de Nazaré Carvalho. *Teoria dos Números: um curso introdutório.* Belém: AEDI/UFPA, 2018.

[2] BOMBELLI, Rafael. *L'Algebra parte maggiore dell'aritmetica divisa in tre libri di Rafael Bombelli da Bologna.* Nella stamparia di Giovanni Rossi: Bologna, 1572.

[3] BOYER, C. B. *História da Matemática.* 2ª edição. São Paulo, 1996.

[4] BRASIL. Ministério da educação e cultura. Base Nacional Curricular Comum: Educação é a Base. Brasília: MEC, 2017. Disponível em: http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf. Acesso em: 19 jun. 2024.

[5] BRASIL, Ministério da Educação e do Desporto. Secretaria de Educação Fundamental. Parâmetros Curriculares Nacionais. Introdução. Brasília: MEC/SEF, 1998.

[6] DMITRI, Fomin; GENKIN, Sergey; ITENBERG, Ilia. *Círculos Matemáticos: A Experiência Russa.* Rio de Janeiro: IMPA, 2012.

[7] DOMINGUES, H. H. *Fundamentos de Aritmética.* Atual Editora Ltda, São Paulo, 1991.

[8] DOMINGUES, H. H. *Fundamentos de Aritmética 2.ed. rev.* Ed. da UFSC, Florianópolis, 2017.

[9] DUTENHEFNER, Francisco; CADAR, Luciana. *Encontros de Aritmética. PIC. SBM.*, Rio de Janeiro, 2015.

[10] EVES, Howard, *Introdução à história da matemática*, Howard Eves; tradução: Hygino H. Domingues. Editora da Unicamp: Campinas, 2004.

[11] FILHO, Alencar E. *Teoria Elementar dos Números.* São Paulo: Nobel, 1981.

[12] GRANDO, Regina Célia. *O jogo e a matemática no contexto da sala de aula.* São Paulo: Paulus, 2004.

[13] HEFEZ, Abramo. *Aritmética. 2ª ed.* Rio de Janeiro: SBM, 2016.

[14] HEFEZ, Abramo. *Aritmética. 3ª ed.* Rio de Janeiro: SBM, 2022.

[15] IEZZI, Gelson; DOLCE, Osvaldo; MACHADO, Antonio. *Matemática e realidade:* 7° *Ano.* 6ª ed. São Paulo: Atual, 2009.

[16] IFRAH, G. *Os números, a história de uma grande invenção.* 11ª ed. São Paulo: Globo, 1985.

[17] JURKIEWICZ, Samuel. *Divisibilidade e Números Inteiros, Apostila do PIC. OBMEP.* Rio de Janeiro: IMPA, 2017.

[18] LA ROQUE, Gilda; PITOMBEIRA, João Bosco. *Uma Equação Diofantina e Suas Resoluções.* Revista do Professor de Matemática, São Paulo: 1991.

[19] LIMA, Elon L. *Meu Professor de Matemática e outras histórias.* Rio de Janeiro: IMPA, 1991.

[20] LIMA, Elon L. *Sobre o ensino da Matemática. Revista do Professor de Matemática. Sociedade Brasileira de Matemática.* Rio de Janeiro: SBM, 1995.

[21] LIMA, Elon L. *A Matemática do Ensino Médio – Volume 2.* 6ª edição, Rio de Janeiro: IMPA, 2006.

[22] OBMEP, *Olimpíadas Brasileiras de Matemática das Escolas Públicas (OBMEP). Banco de Questões 2015.* Disponível em: https://drive.google.com/file/d/1H_gDFg98q5xJTLS6MEUfuzq6-nTC3odU/view. Acesso em: 15 de novembro de 2024.

[23] OCDE, Pisa 2022 Results (Volume II) *Where All Students Can Succeed, PISA, OECD Publishing, Paris, 2019.* Disponível em: https://www.oecd.org/pisa/publications/PISA2018_CN_BRA.pdf. Acesso em: 20 de dezembro de 2024.

[24] REVISTA DO PROFESSOR DE MATEMÁTICA. Rio de Janeiro: n°101, 2020.

[25] ROQUE, Tatiana. *História da Matemática: uma Visão Crítica, Desfazendo Mitos e Lendas.* Zahar, São Paulo, 2012.

[26] ROQUE, Tatiana; PITOMBEIRA, João Bosco. *Tópicos de História da Matemática.* Rio de Janeiro: SBM, 2012.

[27] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números.* 3ª ed. Rio de Janeiro: IMPA, 2010.

[28] ZABALA, Antoni. *A prática educativa: como ensinar; tradução: Ernani F. da F. Rosa.* Porto Alegre: Penso, 2014. Editado como livro impresso em 1998.