UNIVERSIDADE ESTADUAL DO CEARÁ – UECE

CENTRO DE CIÊNCIAS E TECNOLOGIA – CCT

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL: PROFMAT/SBM

ANTONIEL ABREU DOS ANJOS

Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat

Fortaleza - Ceará

2015

Antoniel Abreu dos Anjos

Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como exigência parcial para a obtenção do título de mestre em Matemática, sob a orientação do Prof. Dr. João Montenegro Miranda.

Fortaleza - Ceará

2015

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Anjos, Antoniel Abreu dos.
Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat [recurso eletrônico] / Antoniel Abreu dos Anjos. - 2015.
1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 81 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2015.
Área de concentração: Mestrado em Matemática.
Orientação: Prof. Dr. João Montenegro de Miranda.

1. Equações Diofantinas. 2. Linear. 3. Descida de Fermat. 4. Álgebra. I. Título.

Antoniel Abreu dos Anjos

Equações Diofantinas: Sequência Didática
e o Método da Descida Infinita de Fermat

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como exigência parcial para a obtenção do título de mestre em Matemática, sob a orientação do Prof. Dr. João Montenegro de Miranda.

Aprovada em: 26/08/2015.

BANCA EXAMINADORA

Prof. Dr. João Montenegro de Miranda

Universidade Estadual do Ceará – UECE

Prof. Dr. José Robério Rogério

Universidade Federal do Ceará – UFC

Prof. Dr. João Marques Pereira

Universidade Estadual do Ceará – UECE

AGRADECIMENTOS

A Deus pela força, coragem e determinação durante o trabalho.

À minha esposa Patrícia pela paciência demonstrada durante as inúmeras vezes que estive em falta com as obrigações de esposo.

Ao meu filho Pedro Emanuel “Zaca”, por chegar a minha vida no momento exato.

À minha família pelo incentivo e dedicação.

Ao meu orientador, Prof. Dr. João Montenegro Miranda, pelo incentivo, sabedoria, paciência e disponibilidade durante a realização deste estudo.

Aos meus colegas de curso, pelo companheirismo e auxilio nos momentos de luta.

“Uma mente que se abre a uma nova ideia, jamais volta ao seu tamanho original.”

(Albert Einstein)

RESUMO

A Álgebra é um dos principais ramos da Matemática atual, e um dos pontos de estudo realizado pela Álgebra são as Equações, dentre essas equações pode-se destacar as Equações Diofantinas. As Equações Diofantinas sejam elas lineares ou não lineares, sempre representaram um importante tópico de estudo no ramo da matemática. Com o embasamento na história da Álgebra Antiga, na história das equações de Diofanto de Alexandria e em alguns conceitos da Teoria dos Números será possível realizar o estudo das soluções das Equações Diofantinas Lineares, nesta abordagem das lineares tem-se como objetivo principal a elaboração de uma sequência didática que possa vir a servir de material de apoio para uma possível abordagem das Equações Diofantinas Lineares na Educação Básica, enquanto na abordagem das não lineares será estudado um método que aborda a existência e a determinação de suas soluções, este método é conhecido como o Método da Descida Infinita de Fermat.

Palavras-chave: Equações Diofantinas; linear; Descida de Fermat; Álgebra.

ABSTRACT

Algebra is one of the main branches of the current Mathematics, and one of the study conducted by points Algebra Equations are among those equations can highlight the Diophantine equations. The Diophantine Equations whether linear or non-linear, have always represented an important topic of study in the branch of mathematics. With the foundation in the history of Algebra Ancient in the history of Alexandria Diophantus equations and some concepts of Number Theory it will be possible to conduct the study of the solutions of equations Diophantine Linear, in this the linear approach has as main objective the development of a didactic sequence that may serve as collateral for a possible approach to Diophantine Linear Equations in Elementary Education while on approach to linear will not be studied a method that addresses the existence and determining their solutions, this method is known as the Infinite Descent Method of Fermat.

Keywords: Diophantine equations; Linear; Fermat's descent; Algebra.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Desde as primeiras civilizações o homem tem contato com os números e a noção de contagem. Segundo BOYER, 1974, o homem pré-histórico também conhecia os números ou a noção de numeração, sobre este fato BOYER, 1974, faz a seguinte observação.

> "... Na Tchecoslováquia foi achado um osso de lobo com profundas incisões,... tais descobertas arqueológicas fornecem provas de que a ideia de número é muito mais antiga do que progressos tecnológicos como o uso de metais ou de veículos com rodas" (BOYER, 1974, p.3).

Foi a partir deste contato com os números que o homem começou a fazer Matemática, as civilizações passaram a usar os números para fazerem contas e medições em geral, posteriormente passaram a relacionar o que ocorria na natureza com os números, e assim a Matemática foi surgindo. Um dos ramos mais antigos da Matemática é a Álgebra, ela é responsável pelo estudo das equações de modo geral, BAUMGART, 1992, p.1 define a Álgebra como sendo a "*ciência das equações*". Durante o decorrer dos tempos vários matemáticos, como Pitágoras, Euclides, Diofanto e Pierre de Fermat, se dedicaram ao estudo da Álgebra, onde cada um desses matemáticos deu grande contribuição ao estudo dessa importante vertente matemática.

Dentre os estudos dos matemáticos citados acima, destaca-se os trabalhos realizados por Diofanto, também conhecido por Diofanto de Alexandria. Considerado o mais importante algebrista grego, Diofanto tem como principal publicação a obra "*Arithmética*", que, segundo DOMINGUES, 1991, p. 118, "*Trata-se de uma coletânea de problemas, na maioria indeterminados, para cuja resolução Diofanto usa sempre métodos algébricos, com o que se distingue substancialmente da matemática grega clássica*". Este trabalho tem como propósito estudar as Equações Diofantinas Lineares e não Lineares, elas recebem este nome em homenagem à Diofanto, pois ele deu grandes contribuições para a solução de tais equações.

No inicio será feito um levantamento histórico sobre a Álgebra Elementar, destacando sua evolução no decorrer dos tempos. A abordagem de alguns tópicos da Teoria dos Números como divisibilidade nos inteiros, divisão euclidiana, máximo divisor comum e algoritmo de Euclides, será feita no segundo capítulo. Já o terceiro

capítulo é dedicado as Equações Diofantinas Lineares, com destaque para as equações com 2 e 3 incógnitas por possuírem uma quantidade significativa de aplicações em forma de situações problemas no dia a dia, ao final do terceiro capítulo serão generalizados os estudos da equações em 2 e 3 incógnitas para equações em n incógnitas.

No quarto capítulo, ocorrerá a abordagem de uma série de aplicações das Equações Diofantinas Lineares em forma de situações problemas, e ao final será apresentado uma sequência didática sobre o tema trabalhado que poderá vir a ser aplicado na educação básica.

A elaboração desta sequência didática se embasa em nossas próprias experiências como docente e discente, uma vez que o tema Equações Diofantinas Lineares jamais apareceu em minha vida escolar enquanto aluno ou enquanto professor, a única ligação existente na questão da linearidade ocorre quando estudamos equações lineares no Ensino Básico, porém a relação entre equações lineares e Equações Diofantinas Lineares, no Ensino Básico, se limita apenas a questão da linearidade. Podemos entender este fato como uma falha de nossos currículos escolares, uma vez que um tema tão importante não tenha seu devido espaço na Educação Básica.

Por fim serão estudadas as Equações Diofantinas não Lineares, inicialmente o foco será dado aos ternos de Pitágoras e algumas de suas propriedades serão aproveitadas para o estudo de outro tópico importante: o método da descida infinita de Fermat.

CAPÍTULO 01

UM PANORAMA DA HISTÓRIA DA ÁLGEBRA ANTIGA

Este capítulo foi escrito na forma de um recorte da história da Álgebra, mais precisamente, abordou-se a Álgebra Elementar, que, segundo BAUMGART, 1992, vai desde 1700 a.C. até 1700 d.C., onde a última data mencionada coincide com o início da Álgebra Moderna. Para um melhor entendimento das fases da Álgebra no decorrer deste trabalho, este capítulo está dividido de acordo com a divisão feita pelos historiadores a respeito das civilizações que foram surgindo no decorrer dos tempos, ou seja, inicia-se com Egito e Mesopotâmia, passando pela Grécia, Índia, Arábia e terminando com a Europa da Idade Média. Em cada etapa aborda-se sobre seus principais acontecimentos e descobertas, e ainda foram feitos comentários sobre seus principais Algebristas.

Deixa-se explícito que essa forma de estudo através das civilizações foi realizada primeiramente por BAUMGART, 1992.

1.1 A Álgebra dos Povos Antigos

A origem da Álgebra não está bem definida, mas acredita-se que ela surgiu simultaneamente no Egito e na Mesopotâmia (Babilônia), ambas com estilo retórico. Embora contemporâneas, a Álgebra babilônica se desenvolveu mais que a Álgebra egípcia. Até mesmo a origem da palavra Álgebra é um fato curioso, pois, na verdade, não existe etimologia nesta palavra, BAUMGART, 1992, explica que:

> "Álgebra é uma variante latina da palavra árabe *al-jabr* (às vezes transliterada *al-jebr*), usada no título do livro, *Hisab al-jabr w'al-muqabalah*, escrito em Bagdá por volta do ano 825 d.C. pelo matemático árabe Mohammed ibn-Musa al-Khowarizmi (Maomé, filho de Moisés, de Khowarizmi)." (BAUMGART, 1992, p. 1).

A história da Álgebra se divide em duas fases, a Álgebra Elementar (antiga) que é responsável pela abordagem das equações e de métodos práticos para resolvê-las, e a Álgebra Abstrata (moderna), que por sua vez foi a grande precursora da Análise.

A fase antiga, que vai desde 1700 a.C. até 1700 d.C., foi marcada pela construção gradativa dos símbolos algébricos e pela solução de equações, para BAUMGART, 1992, o desenvolvimento da notação algébrica se desenvolveu ao longo de três estágios:

- **O Retórico ou Verbal** conhecido também pelo desenvolvimento da álgebra pré-diofantina em que os argumentos da resolução de um problema são escritos em prosa pura, sem abreviações ou símbolos específicos.

- **Sincopado**, aqui se adotavam algumas abreviações para as quantidades e operações que se repetiam mais frequentemente.

- **Simbólico,** nesse estágio as resoluções se expressam numa espécie de taquigrafia matemática formada por símbolos que aparentemente nada têm a ver com os entes que representam.

A Álgebra retórica dos Babilônios e Egípcios

A Álgebra iniciou-se, possivelmente, primeiro na Babilônia e logo após no Egito. Como a Babilônia largou na frente, nada mais lógico que ela tenha obtido resultados mais bem elaborados, enquanto os egípcios resolviam algumas equações lineares através de um método que consistia na aplicação de uma estimativa inicial e de uma correção final, esse método ficou conhecido pelos europeus como o *método da falsa posição*[1], os babilônios já conseguiam resolver de forma bem mais estruturada uma variedade de equações, dentre as quais podemos destacar alguns casos especiais de equações cúbicas e quárticas e principalmente as equações lineares e as equações quadráticas.

A Babilônia e o Egito praticavam uma Álgebra retórica. Um exemplo de problema retórico foi encontrado em escrita cuneiforme escrito em tábuas de argila que data do ano 1700 a.C., tempo do rei Hammurabi. Segundo BAUMGART, 1992, podemos descrever o problema do seguinte modo:

[1] O método da falsa posição consistia na substituição da variável de uma equação qualquer por um valor aleatório inicial, ao final deste processo eram comparados os dois membros da equação, então o valor inicial era corrigido por um valor que equacionasse os dois membros da equação.

I. Comprimento, largura. Multipliquei comprimento por largura, obtendo assim a área: 252. Somei comprimento e largura: 32. Pede-se comprimento e largura.
II. (Dados) 32 soma e 252 produto.
III. (Resposta) 18 comprimento e 14 largura.
IV. Segue-se este método: tome metade de 32 (*16*), multiplique por ela mesma (*16 x 16 = 256*), subtraia 252 do produto (*256 – 252 = 4*), retire a raiz quadrada da diferença anterior ($\sqrt{4}$ = *2*), por fim temos: comprimento igual à 16 + 2 = 18 e largura igual à 16 – 2 = 14.
V. (Prova) Multipliquei 18 x 14 = 252, soma 18 + 14 = 32.

Vale destacar que BAUMGART, 1992, mostra uma generalização de tal problema para quaisquer comprimento (X) e largura (Y).

Essa forma de resolver o problema traz uma breve lembrança do modo que é usado atualmente para construir a formula de Bháskara, mas como os babilônios não conheciam tal fórmula, eles se detinham a este modo menos direto, porém, mais elaborado para resolverem equações quadráticas.

Os egípcios deixaram suas descobertas matemáticas registradas nos mais antigos documentos matemáticos que se conhece na história, os papiros de Rhind e Moscou. Neste documento encontram-se mais de 100 problemas de situações práticas como número de pães, cerveja e o balanceamento para rações de gado e aves. A solução destes problemas envolviam equações lineares com uma ou duas incógnitas e eram resolvidos pelo método da falsa posição como já foi citado acima.

Gregos

A Álgebra grega seguia os métodos da Álgebra babilônica para a resolução de equações, porém, os gregos usavam uma Álgebra “diferente”. Na verdade, os gregos possuíam uma nova visão da Álgebra, eles resolviam problemas algébricos usando a geometria. Euclides, um matemático grego que viveu por volta de 300 a.C., escreveu uma das maiores obras conhecidas. Uma coleção de treze livros

intitulada de *Os Elementos*. Euclides usava a Geometria para provar seus teoremas, como exemplo, podemos a demonstração da identidade $(a + b)^2 = a^2 + 2ab + b^2$. No livro II, proposição 4, dos *Elementos*, Euclides enunciou a identidade da seguinte forma:

"Se uma linha reta é dividida em duas partes quaisquer, o quadrado sobre a linha toda é igual aos quadrados sobre as duas partes, junto com duas vezes o retângulo que as partes contêm."

Para Euclides a identidade enunciada acima possuía a seguinte representação geométrica:

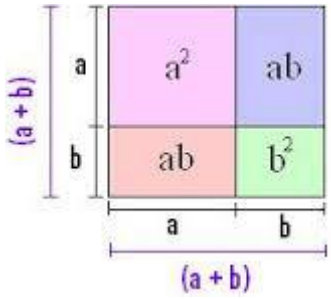

FIGURA 1: $(a + b)^2 = a^2 + 2ab + b^2$. Disponível em: http://www.brasilescola.com/matematica/quadrado-soma.html . (Acessado em 28 de janeiro de 2015.)

Mas, porque uma forma diferente para abordar a mesma Álgebra? A resposta dessa indagação é encontrada bem antes de Euclides, para ser mais preciso, vamos voltar até 540 a.C., época em que viveu Pitágoras um dos pioneiros na matemática grega e fundador da Escola Pitagórica. É nos pitagóricos que se encontra a solução para essa Álgebra diferenciada, pois eles tinham muitos problemas com as frações e os números irracionais, na verdade, Pitágoras não aceitava a ideia dos números irracionais e punia quem ousasse a tocar nesse assunto em sua escola. Quando os pitagóricos descobriram que a diagonal de um quadrado unitário ($\sqrt{2}$) é incomensurável ouve um distúrbio lógico entre eles. Assim, como $\sqrt{2}$ não pode ser representado como uma fração com numerador e denominador ambos inteiros, os matemáticos gregos resolveram expressá-lo de forma geométrica, pois $\sqrt{2}$ pode ser expresso pelo segmento de reta que representa a diagonal de um quadrado unitário.

A Álgebra Grega começou a parar de evoluir com a chegada do império romano. BAUMGART, 2012, descreve esse fato do seguinte modo:

> "A matemática grega deu uma parada brusca. A ocupação romana tinha começado, e não encorajava a erudição matemática, ainda que estimulasse alguns outros ramos da cultura grega. Devido ao estilo pesado da Álgebra geométrica ... esta não poderia sobreviver somente na tradição escrita; necessitava-se de um meio de comunicação vivo, oral." (BAUMGART, 2012, p. 9.)

Árabes e Hindus

A Álgebra Hindu possivelmente sofreu influências das Álgebras Babilônica e Grega. No cenário algébrico hindu destacam-se dois matemáticos Brahmagupta e Bháskara, o primeiro viveu por volta de 628 d.C. na Índia Central e se destacou pelo estilo sincopado[2], segundo BAUMGART, 2012, tem-se a seguinte representação sincopada para a expressão $5xy + \sqrt{35} - 12$, ela seria escrita do seguinte modo:

ya ka 5 bha k(a) 35 ru 12

A tradução para a Álgebra simbólica seria a seguinte:

ya (x), ka (y), 5 (5), bha (produto), k(a)35 (irracional 35), ru (número puro), 12 (12)

Brahmagupta também trabalhou no estudo das soluções gerais de equações do segundo grau, encontrando duas raízes, inclusive uma delas negativa. Ele foi o primeiro matemático a encontrar todas as soluções inteiras possíveis para a equação linear $a.x + b.y = c$ onde a, b e c são inteiros.

Já Bháskara viveu durante o século XII e veio a aperfeiçoar os trabalhos realizados por Brahmagupta, principalmente no campo das equações quadráticas, Bháskara desenvolveu um método usando o complemento de quadrados para encontrar as soluções da equação $ax^2 + bx + c = 0$, com a,b,c reais, esse método é conhecido até os dias de hoje como a *Fórmula de Bháskara*.

[2] O estilo sincopado foi utilizado primeiramente por Diofanto, os hindus apenas se apropriaram dos estudos de Diofanto, falaremos mais sobre este estilo no próximo tópico deste capitulo.

Enquanto os hindus resolviam equações quadráticas, um árabe que viveu por volta do século VIII, que posteriormente viria a ser conhecido como o pai da Álgebra, chamado Al-Khwarizmi, se destacava no estudo da Álgebra principalmente pelos seus dois livros *Al-jabr* e *Liber Algorismi*, nos seis primeiros capítulos do livro Al-jabr Al-Khwarizmi aborda uma Álgebra composta por regras de forma estritamente numérica, trazendo uma lembrança da Álgebra Babilônica, porém após os seis capítulos Al-Khwarizmi passa a abordar uma Álgebra Geométrica, dessa vez relembrando o estilo da Álgebra Grega, logo fica claro as influências babilônicas e gregas na Álgebra de Al-Khwarizmi. Esses trabalhos de Al-Khwarizmi foram traduzidos posteriormente para o latim influenciando grande parte da Álgebra Europeia.

Além dos trabalhos de Al-Khwarizmi, os árabes contribuíram ainda com um engenhoso sistema de numeração decimal, conhecido até os dias de hoje como sistema de numeração Hindu-Arábico, sistema este que foi inicialmente estudado pelos hindus e aprimorado pelos árabes.

Europa, o estilo simbólico

Os avanços desenvolvidos pelos árabes e hindus no campo da Álgebra foram aos poucos chegando à Europa através dos comerciantes que viajavam pelo mundo, foram esses comerciantes os responsáveis pela divulgação do conhecimento, naquela época, em grande parte do mundo. BAUMGART, 2012, faz o seguinte comentário:

> "...ainda mais importante para a Europa, especialmente a Itália, foi o *Liber Abaci* (1202) de Fibonacci (Leonardo de Pisa), onde o autor resolvia equações no estilo retórico e geral de al-Khowarizmi e defendia veementemente o uso dos numerais indu-arábicos, dos quais tomara conhecimento em suas viagens a vários países como mercador e comerciante." (BAUMGART, 2012, p. 11.)

Perto do fim da Idade Média (500 d.C. – 1500 d.C), cidades fortes no comércio foram surgindo, primeiramente na Itália, assim a economia da Europa medieval foi ganhando força, e com o surgimento da imprensa e com os trabalhos dos árabes, hindus e Fibonacci escritos em latim, a Álgebra Simbólica europeia teve

seu nascimento. Com todos esses fatos conspirando a favor da Álgebra, só poderia acarretar em um aprimoramento do seu estilo simbólico, neste cenário destacam-se dois importantes matemáticos algebristas que escreveram trabalhos voltados para o estilo simbólico.

O primeiro é François Viéte (1540 – 1603), nascido na França é considerado por muitos como precursor da Álgebra Simbólica. Foi o primeiro matemático algebrista a demonstrar as vantagens do uso de letras para se referir a quantidades desconhecidas ou incógnitas. Em 1591, publicou a obra *In Artem Analyticam Isagoge* (Introdução a Arte Analítica) neste trabalho Viéte destaca o simbolismo algébrico introduzindo uma convenção extremamente importante para escrita das equações na forma geral, para representar uma quantidade desconhecida usava uma vogal e para representar uma grandeza ou números (coeficiente) usava uma consoante.

O segundo matemático que contribuiu significativamente para o aperfeiçoamento da linguagem algébrica foi René Descartes (1596 – 1650). Descartes, que assim como Viéte também nasceu na França, aperfeiçoou a álgebra de François Viéte, ajudando assim a consolidar a Álgebra Simbólica na Europa. Algumas contribuições de Descartes para a Álgebra Simbólica estão listadas abaixo:

- Criou o símbolo · para a operação de multiplicação;
- Foi o primeiro a introduzir a notação que é usada hoje para os expoentes de uma potencia;
- Determinou que, quando se tratar de equações de um modo geral, as primeiras letras do alfabeto seriam usadas para os coeficientes da incógnita e os termos independentes (se literais) e as últimas letras para representar as incógnitas, por exemplo, $a \cdot x^5 + b \cdot x^3 + c \cdot x^2 + d \cdot x + e$.
- Formulou o método geral para a aplicação da álgebra a problemas geométricos determinados.
- Em sua obra *La Geométrie* apresentou a teoria elementar das equações; regra de sinais; como achar a solução algébrica de equações cúbicas e quárticas;

- E por fim interligou a álgebra com a geometria implantando o plano cartesiano.

Após o aprimoramento da Álgebra simbólica, vários outros matemáticos passaram a se aventurar nos campos algébricos e a partir de então a Álgebra só tem sido melhorada a cada trabalho publicado.

Assim encerra este primeiro tópico deste capítulo, deixando claro que a história da Álgebra não foi totalmente abordada neste tópico, como citado anteriormente, não foi abordada a história da Álgebra abstrata que teve início logo após os avanços obtidos com a notação simbólica.

1.2 Diofanto e suas equações

Diofanto (200 d.C. – 284 d.C.)

FIGURA 2: Diofanto (200 d.C. – 284 d.C.). Disponível em: http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1271/2012_01055_FABIO_PINHEIRO_LUZ.pdf?sequence=1. (Acessado em 16 de fevereiro de 2015.)

Diofanto de Alexandria é tratado como o mais importante algebrista grego, Diofanto viveu por volta do século III da nossa era, ele viveu por certo período na cidade grega conhecida por Alexandria, daí Diofanto de “Alexandria”, nesta cidade centravam-se os principais estudos matemáticos da Grécia antiga, foi em Alexandria que a Álgebra de Diofanto ganhou destaque.

Praticamente nada se sabe sobre a vida de Diofanto, a única informação que temos é em relação a quantos anos ele viveu, isso graças a um enigma gravado na lápide de seu túmulo que Singh, 2002, descreveu da seguinte forma:

> “Deus lhe concedeu graça de ser um menino pela sexta parte de sua vida. Depois, por um doze avos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte e cinco anos depois do casamento Ele concedeu-lhe um filho. Ah! criança tardia e má, depois de viver metade da vida de seu pai o destino frio a levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos, Diofante terminou sua vida”. (SINGH, 2001, p.71)

Pode-se determinar a idade de Diofanto, tendo como referência a citação acima, do seguinte modo:

Seja x o número de anos vividos por Diofanto, assim;

$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$, portanto;

$x = \frac{14x + 7x + 12x + 42x + 756}{84}$; logo;

$84x = 75x + 756$, logo;

$9x = 756$, então;

$x = 84$. Ou seja, Diofanto viveu 84 anos.

Conhecido por usar um estilo matemático diferente para a época, Diofanto foi o primeiro algebrista a abordar o estilo sincopado, em suas obras ele fazia algumas abreviações quando se repetiam com frequência algumas operações matemáticas. Essa sua forma de escrever acabou por influenciar os matemáticos europeus Pierre de Fermat e Renê Descartes a desenvolverem o estilo simbólico.

Diofanto escreveu poucas obras matemáticas, as únicas que se tem conhecimento são: “*Porismas”*, *“Sobre números Poligonais”* e “*Arithmética”*. A primeira obra se perdeu no tempo, mas acredita-se que ela continha alguns artifícios introdutórios para a teoria dos números, uma vez que a palavra *porisma* aparece na obra *Arithmética* em forma de preposições. Da segunda obra sobrou apenas um fragmento, de onde pode-se observar uma representação geométrica dos números, ela contém ainda uma generalização da propriedade dos números triangulares e se encerra com um problema, não resolvido na obra, de saber quando um número é poligonal.

A terceira obra, *Arithmética*, é com certeza a mais importante das três, composta por 13 livros, dos quais apenas 6 sobreviveram ao nosso tempo. Esses livros traziam uma série de problemas numéricos específicos que recaem em equações do primeiro grau ($ax + by = c$) e segundo grau ($a^2 + b^2 = c^2$), ocorrendo casos de surgirem equações com grau acima de dois, por exemplo, $a^4 + b^4 + c^4 = x^4$. Para a resolução destes problemas Diofanto sempre usava métodos algébricos, deste modo, contrastando com a matemática grega clássica.

Segundo DOMINGUES, devido a utilização dos métodos algébricos de Diofanto, denominam-se Equações Diofantinas, todas as equações polinomiais (com qualquer número de incógnitas), com coeficientes inteiros, sempre que se trata de encontrar suas soluções no conjunto dos inteiros. Vale destacar ainda que o famoso matemático francês Pierre de Fermat foi bastante influenciado pela obra *Arithmética* de Diofanto.

Capa do livro *Arithmética*

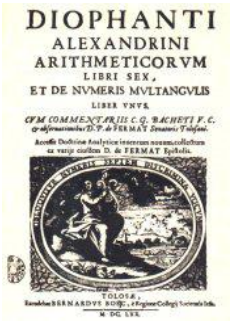
DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

Figura 3: Capa do livro *Arithmética*. Disponível em: http://bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/1380/2012_01182_RILDO_RIBEIRO.pdf?sequence=1. (Acessado em 08 de fevereiro de 2015.)

Abaixo seguem dois problemas pertencentes a obra *Arithmética* de Diofanto, e suas resoluções.

Livro I- problema 17: “Encontrar quatro números cuja soma três a três seja, respectivamente, 22, 24, 27 e 20”.

Solução:

$$\begin{cases} x + y + z = 22 & (i) \\ x + y + w = 24 & (ii) \\ x + z + w = 27 & (iii) \\ y + z + w = 20 & (iv) \end{cases}$$

Por (iii) e (iv), temos, respectivamente, que:

$x = 27 - w - z$ e $y = 20 - w - z$.

Deste modo, substituindo as expressões encontradas em (ii), segue que:

$27 - w - z + 20 - w - z + w = 24$.

Simplificando, segue que:

$23 = 2z + w \qquad (v)$

Substituindo em (i) as expressões encontradas, tem-se:

$27 - w - z + 20 - w - z + z = 22$.

Simplificando novamente obtêm-se:

$25 = z + 2w \qquad (vi)$

De (v) e (vi), segue que:

$$\begin{cases} 2z + w = 23 \\ z + 2w = 25 \end{cases} \Rightarrow \begin{cases} 4z + 2w = 46 \\ z + 2w = 25 \end{cases}$$

Portanto, $3z = 21 \Longrightarrow z = 7$, por (v), $w = 9$

Por (iii) e (iv) segue que $x = 11$ e $y = 4$.

Logo, a solução é 4, 7, 9, 11.

Livro V- problema 30: “Ao embarcar com os companheiros, aos quais pretendia ser agradável, alguém comprou vinho de duas qualidades, um a 8 dracmas[3], outro a 5 dracmas o côngio[4] (oitava parte da ânfora[5]). Pagou por tudo um número de dracmas representado por um quadrado tal que, aumentado de um número prescrito, produz um segundo quadrado cuja raiz dá o número total de côngios. Quantos côngios de 8 dracmas e quantos de 5 dracmas foram comprados?”.

Solução:

Solução exibida por NASCIMENTO, 2014, p. 12.

Considere o número prescrito como sendo 60. Tem-se então o seguinte sistema:

$$\begin{cases} 8x + 5y = z^2 & (i) \\ Z^2 + 60 = (x + y)^2 & (ii) \end{cases}$$

De (i) e (ii) segue que:

$8x + 5y + 60 = (x + y)^2$.

Seja $x + y = a$, neste caso segue que $8x + 5y + 60 = a^2$.

Como Diofanto buscava soluções racionais positivas, da equação acima se podem tirar as seguintes conclusões:

a) $8x + 5y = a^2 - 60 \Rightarrow 8(a - y) + 5y = a^2 - 60 \Rightarrow 8a - 3y = a^2 - 60$ (iii)
donde $8a > a^2 - 60 \Leftrightarrow a \leq 12$.

b) $8x + 5y = a^2 - 60 \Rightarrow 8x + 5(a - x) = a^2 - 60 \Rightarrow 5a + 3x = a^2 - 60$ (iv)
donde $5a < a^2 - 60 \Leftrightarrow 11 \leq a$. Assim, $11 \leq a \leq 12$.

---

[3] Dracmas: era uma unidade monetária grega, a mais antiga do mundo em circulação até ser substituída pelo euro.

[4] Côngio era uma antiga medida romana de capacidade.

[5] Ânfora: antigo vaso com duas asas, utilizado para a conservação e o transporte dos líquidos como vinhos.

Como $a^2 - 60$ é um quadrado, logo pode-se escrevê-lo na forma $(a - b)^2$, assim tem-se, $-60 = -2ab + b^2$, logo, $a = 60 + b^2 / 2b$ e $11 \leq 60 + b^2 / 2b \leq 12$. Conclui-se assim que $19 \leq b \leq 21$.

Diofanto escolheu $b = 20$, o que resulta em $a = 60 + 20^2 / 2.20 \Rightarrow a = 46/4$

Por (iii) segue que $y = 79/12$ e (iv) resulta em $x = 59/12$.

CAPÍTULO 02

TÓPICOS DE TEORIA DOS NÚMEROS

Este capítulo tem por objetivo a análise de alguns tópicos da Teoria dos Números que serão importantes para o estudo futuro das Equações Diofantinas. No decorrer do capítulo faremos algumas demonstrações de teoremas e proposições importantes, a partir deste momento será utilizado o símbolo "■" para representar a conclusão destas demonstrações.

2.1 Divisibilidade nos Inteiros ($\mathbb{Z}$)

Definição 2.1.1: Dados dois números inteiros a e b, com $a \neq 0$, diz-se que a divide b e representa-se por $a \mid b$, se existir um número inteiro c de modo que $a \cdot c = b$. Neste caso pode-se dizer ainda que b é múltiplo de a.

Se a não divide b, então não existe um inteiro c tal que $a \cdot c = b$, neste caso usa-se o símbolo $a \nmid b$.

Proposição 2.1.1: *Sejam a e b inteiros não nulos, e seja c um inteiro qualquer. Então, tem-se que:*

i. $1 \mid c$, $a \mid a$ *e* $a \mid 0$.

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

Demonstração:

(i) decorre das igualdades $c = 1 \cdot c$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

(ii) de $a \mid b$ *e* $b \mid c$, segue que existem p e q inteiros, de modo que $b = a \cdot p$ e $c = b \cdot q$, substituindo o valor de b na segunda expressão obtém-se:

$$c = b \cdot q = a \cdot p \cdot q = a \cdot (p \cdot q)$$

logo, $a \mid c$.

■

Proposição 2.1.2: *Se a, b, c, d, são inteiros com $a \neq 0$ e $b \neq 0$, de modo que $a|b$ e $c|d$, então $a \cdot c \mid b \cdot d$.*

Demonstração: Como $a \mid b$ e $c \mid d$, logo existem p e q inteiros, de modo que $b = a \cdot p$ e $d = c \cdot q$. Então fazendo $b \cdot d$, segue que:

$$b \cdot d = (a \cdot p) \cdot (c \cdot q) = (a \cdot c) \cdot (p \cdot q)$$

Portanto, $a \cdot c \mid b \cdot d$.

■

Observação 2.1.1: Em particular, se $a \mid b$ então $a \cdot c \mid b \cdot c$, para todo c inteiro não nulo.

Proposição 2.1.3: *Sejam a, b e c inteiros, com $a \neq 0$, tais que $a \mid (b + c)$. Então $a \mid b$* se, e somente se, $a \mid c$.

Demonstração: Se $a \mid b$ então existe q também inteiro de modo que $b = a \cdot q$. Como $a \mid (b + c)$, então existe p inteiro tal que $b + c = a \cdot p$, substituindo o valor de b na igualdade $b + c = a \cdot p$ tem-se:

$$a \cdot q + c = a \cdot p, \text{ assim; } c = a \cdot p - a \cdot q = a \cdot (p - q)$$

Ou seja, $a \mid c$.

A demonstração da recíproca é totalmente análoga.

■

Proposição 2.1.4: *Sejam a, b, c, m e n inteiros, com $c \neq 0$, de modo que $c \mid a$ e $c \mid b$ então $c \mid (m \cdot a \pm n \cdot b)$.*

Demonstração: Se $c \mid a$ e $c \mid b$, então existem inteiros k e w tais que:

$$a = k \cdot c \text{ e } b = w \cdot c.$$

Multiplicando a primeira igualdade por m e a segunda por n segue que:

$$m \cdot a = m \cdot k \cdot c \text{ e } n \cdot b = n \cdot w \cdot c.$$

Adicionando-se, membro a membro, resulta em:

$$m \cdot a + n \cdot b = (m \cdot k + n \cdot w) \cdot c, \text{ o que mostra que } c \mid (m \cdot a + n \cdot b).$$

Agora subtraindo, membro a membro, chega-se a:

$m \cdot a - n \cdot b = (m \cdot k - n \cdot w) \cdot c$, o que mostra que $c \mid (m \cdot a - n \cdot b)$.

Logo, $c \mid (m \cdot a \pm n \cdot b)$

■

Proposição 2.1.5: *Sejam a e b inteiros não nulos, se a* | *b e b* | *a, então a* = ± *b.*

Demonstração: Como $a \mid b$ e $b \mid a$, existem p e q inteiros tais que:

$$b = a \cdot p \text{ e } a = b \cdot q.$$

Assim, $a = (a \cdot p) \cdot q$, ou seja, $a = a \cdot (p \cdot q)$, o que implica que $p \cdot q = 1$, ou seja, $p = q = \pm 1$. Portanto, $a = \pm b$.

■

Proposição 2.1.6: *Sejam a e b inteiros não nulos, se a* | *b, então* $|a| \leq |b|$.

Demonstração: Como $a \mid b$, então existe um inteiro não nulo p tal que $b = a \cdot p$, logo $|b| = |a| \cdot |p|$, mas $|p| \geq 1$, portanto, $|b| \geq |a|$.

■

Proposição 2.1.7: *Sejam a, b e n números inteiros não negativos, com a + b ≠ 0, então (a + b)* | $(a^{2n+1} + b^{2n+1})$.

Demonstração: A demonstração será feita utilizando o principio de indução finita sobre n. Para $n = 0$, temos que:

$a^{2.0+1} + b^{2.0+1} = a^1 + b^1 = a + b$, logo a proposição é válida para $n = 0$.

Supondo que a proposição seja válida para n, resta mostrar se ela também é válida para $n + 1$. Portanto reescrevendo $a^{2(n+1)+1} + b^{2(n+1)+1}$, tem-se:

$$a^{2(n+1)+1} + b^{2(n+1)+1} = a^2a^{2n+1} - b^2a^{2n+1} + b^2a^{2n+1} + b^2b^{2n+1} = (a^2-b^2)a^{2n+1} + b^2(a^{2n+1}+b^{2n+1})$$

Como $(a + b) \mid (a^2 - b^2)$ e $(a + b) \mid (a^{2n+1} + b^{2n+1})$ por hipótese, segue da Proposição 2.1.4 que $(a + b) \mid (a^{2(n+1)+1} + b^{2(n+1)+1})$.

Portanto $(a + b) \mid (a^{2n+1} + b^{2n+1})$ para todo n inteiro não negativo.

■

Proposição 2.1.8: *Sejam a, b e n números inteiros não negativos, com $a \geq b > 0$, então $(a + b) \mid (a^{2n} - b^{2n})$.*

Demonstração: A demonstração será feita utilizando o principio de indução finita sobre n. Para $n = 0$, segue que:

$a^{2.0} - b^{2.0} = a^0 - b^0 = 0$, como $(a + b) \mid 0$, logo a proposição é válida para $n = 0$.

Supondo que a proposição seja válida para n, resta mostrar se ela também é válida para $n + 1$. Portanto reescrevendo $a^{2(n+1)} - b^{2(n+1)}$, tem-se:

$$a^{2(n+1)} - b^{2(n+1)} = a^2a^{2n} - b^2a^{2n} + b^2a^{2n} - b^2b^{2n} = (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n})$$

Como $(a + b) \mid (a^2 - b^2)$ e $(a + b) \mid (a^{2n} - b^{2n})$ por hipótese, segue da Proposição 2.1.4 que $(a + b) \mid a^{2(n+1)} - b^{2(n+1)}$.

Portanto $(a + b) \mid (a^{2n} - b^{2n})$ para todo n inteiro não negativo.

■

Proposição 2.1.9: *Sejam a, b e n números inteiros não negativos, com $a > b > 0$, então $(a - b) \mid (a^n - b^n)$.*

Demonstração: A demonstração será feita utilizando o principio de indução finita sobre n. Para $n = 0$, segue que:

$a^0 - b^0 = 1 - 1 = 0$, como $(a - b) \mid 0$, logo a proposição é válida para $n = 0$.

Supondo que a proposição seja válida para n, resta mostrar se ela também é válida para $n + 1$. Portanto, reescrevendo $a^{n+1} - b^{n+1}$, tem-se:

$$a^{n+1} - b^{n+1} = aa^n - ba^n + ba^n - bb^n = (a - b)a^n + b(a^n - b^n)$$

Como $(a - b) \mid (a - b)$ e $(a - b) \mid (a^n - b^n)$ por hipótese, segue da Proposição 2.1.4 que $(a - b) \mid a^{n+1} - b^{n+1}$.

Portanto $(a - b) \mid (a^n - b^n)$ para todo n inteiro não negativo.

■

2.2 Divisão Euclidiana

Teorema 2.2.1 *(Divisão Euclidiana) Sejam a e b números naturais com $0 \leq a < b$. Existem dois únicos números naturais q e r tais que $b = a \cdot q + r$, com $0 \leq r < a$.*

Demonstração: Como $b > a$, considere o seguinte conjunto que possui apenas elementos não negativos:

$$A = \{ b - na \,/\, n \in \text{IN e } b - na \geq 0 \}$$

Pelo Princípio da Boa Ordem[6], o conjunto A tem um menor elemento, diga-se $r = b - q \cdot a$. Vamos provar que r satisfaz as condições enunciadas no Teorema, ou seja, $r < a$.

Se $a \mid b$, então $r = 0$ e o teorema estará demonstrado. Se, por outro lado, $a \nmid b$, deve-se mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c > 0$ tal que $r = c + a$. Portanto, sendo $r = c + a = b - q \cdot a$, teríamos $c = b - q \cdot a - a = b - (q + 1) \cdot a$, o que implica $c < r$, o que é uma contradição com o fato de r ser o menor elemento de A. Portanto, $b = a \cdot q + r$ com $r < a$, o que prova a existência de q e r.

Resta provar a unicidade. Tomando dois elementos distintos em A. Note que a diferença entre o maior e o menor desses dois números é um múltiplo de a e, deste modo, essa diferença é no mínimo igual a a. Logo se $r_1 = b - a \cdot q_1$ e $r_2 = b - a \cdot q_2$, com $r_1 < r_2 < a$, teríamos $r_2 - r_1 \geq a$. Isso nos daria, $r_2 \geq r_1 + a \geq a$, absurdo, portanto $r_2 = r_1$.

Como $r_2 = r_1$, segue-se que $b - a \cdot q_1 = b - a \cdot q_2$, o que implica que $a \cdot q_1 = a \cdot q_2$ e, portanto $q_1 = q_2$.

---

[6] O Princípio da Boa Ordem diz que em todo subconjunto C, não vazio, dos naturais; existe $c \in C$, tal que $c \leq x$, para todo $x \in C$.

■

Observação 2.2.1 Os números *q* e *r* são chamados, respectivamente, de *quociente* e *resto* da divisão de *b* por *a*.

Observação 2.2.2 O resto da divisão é zero se, e somente se, $a \mid b$.

Observe que a demonstração do teorema fornece um método para obter o quociente e o resto de uma divisão nos naturais. Como aplicação do teorema 2.2.1 segue o exemplo 2.2.1.

Exemplo 2.2.1. Encontrar o quociente e o resto da divisão de 50 por 9.

Solução: De fato:

$50 - 9 = 41 > 9$
$50 - 2 \cdot 9 = 32 > 9$
$50 - 3 \cdot 9 = 23 > 9$
$50 - 4 \cdot 9 = 14 > 9$
$50 - 5 \cdot 9 = 5 < 9$

O que mostra que $q = 5$ e $r = 5$.

Corolário 2.2.1. *Dados dois números naturais a e b com* $1 < a \leq b$, *existe um número natural n tal que* $na \leq b < (n + 1)a$.

Demonstração: Pelo teorema 2.2.1, existem os números naturais *q* e *r*, com $r < a$, determinados de forma única, tais que $b = a \cdot q + r$, o que implica, $a \cdot q \leq b$.

Por outro lado, $b = a \cdot q + r < a \cdot q + a = a \cdot (q + 1)$. Portanto, $a \cdot q \leq b < a \cdot (q + 1)$. Basta tomar $n = q$ para completar a demonstração do Corolário.

2.3 Máximo Divisor Comum

Dados dois números inteiros *a* e *b*, não simultaneamente nulos, diz-se que um inteiro não nulo *d* é um divisor comum de *a* e *b*, se $d \mid a$ e $d \mid b$.

Por exemplo, os números 1, 2 e 4 são os divisores comuns de 8 e 12

Agora será mostrado o conceito de *máximo divisor comum (mdc)* para dois inteiros não simultaneamente nulos, baseado na definição escrita por Euclides em sua obra *Os Elementos*.

Definição 2.3.1: Sejam *a* e *b* dois inteiros não simultaneamente nulos, diz-se que o inteiro positivo *d* é o *máximo divisor comum (mdc)* de *a* e *b*, e será representado por $d = (a,b)$, se *d* satisfazer as seguintes condições:

(i) *d* é um divisor comum de *a* e de *b*.

(ii) *d* é divisível por todo divisor comum de *a* e de *b*, isto é, se *c* é um divisor comum de *a* e *b* então $c \mid d$.

Observação 2.3.1 O *mdc* de dois inteiros é único e sempre existe.

De fato, se *d* é um mdc de *a* e *b*, e *c* é um divisor comum desses números, então $c \leq d$. Isto mostra que o máximo divisor comum de dois números é o maior dentre todos os divisores comuns desses dois números.

Em particular, se *d* e d_0 são máximos divisores comuns de um mesmo par de números, então $d \leq d_0$ e $d_0 \leq d$, e, consequentemente, $d = d_0$, ou seja, o mdc de dois números é único. Será mostrado mais adiante, segundo o lema de Euclides, que sempre existe o *mdc* de dois naturais.

Esta definição de *mdc* para inteiros a e b vale também para uma quantidade finita de inteiros $a_1; a_2; a_3; \cdots ; a_n$, como por exemplo o *mdc* entre três números

$$mdc(a_1; a_2; a_3) = mdc(mdc(a_1; a_2); a_3) = mdc(a_1; mdc(a_2; a_3))$$

Lema 2.3.1 *(Lema de Euclides). Sejam a, b, n inteiros não nulos, com $a < na < b$. Se existe mdc(a, b − na), então existe mdc(a, b) e mdc(a, b) = mdc(a, b − na).*

Demonstração: Seja $d = (a, b - na)$. Como $d \mid a$ e $d \mid (b - na)$, segue que $d \mid b$, pois $b = b - na + na$. Logo *d* é um divisor comum de *a* e *b*. Supondo que *c* seja um divisor comum de *a* e *b*, logo *c* é um divisor comum de *a* e $b - na$ e, portanto $c \mid d$. Isso prova que $d = (a, b)$.

■

Teorema 2.3.1: *Seja d o máximo divisor comum de a e b. Então existem x_1 e y_1 inteiros, tais que $d = x_1a + y_1b$.*

Demonstração: Seja *A* o conjunto de todas as combinações lineares $xa + yb$, com *x* e *y* inteiros. Obviamente, A contém números negativos, positivos e também o zero. Vamos escolher x_1 e y_1 tais que $c = x_1a + y_1b$ seja o menor inteiro positivo pertencente ao conjunto *A*.

Primeiramente, será provado que $c \mid a$ e $c \mid b$. Supondo que c ł a, logo, pelo Teorema 2.2.1, existem *q* e *r* tais que $a = q \cdot c + r$ com $0 \leq r < c$. Portanto,

$$r = a - q \cdot c = a - q(x_1a + y_1b) = (1 - qx_1)a + (-qy_1)b.$$

Isto mostra que $r \in A$, o que é uma contradição, uma vez que $0 \leq r < c$ e, por hipótese, *c* é o menor elemento positivo de *A*. Logo $c \mid a$ e de forma análoga se prova que $c \mid b$. Daí, $c \mid d$ pois $d = (a, b)$, portanto $c \leq d$.

Como d é o máximo divisor comum de *a* e *b*, então, existem inteiros q_1 e q_2 tais que $a = q_1 \cdot d$ e $b = q_2 \cdot d$ e, portanto,

$$c = x_1 \cdot a + y_1 \cdot b = x_1 \cdot q_1 \cdot d + y_1 \cdot q_2 \cdot d = d \cdot (x_1 \cdot q_1 + y_1 \cdot q_2)$$ o que implica $d \mid c$.

Logo $d \leq c$, e como $c \leq d$, segue que $c = d = x_1a + y_1b$.

■

Pode-se observar facilmente que, dados *a* e *b* inteiros, temos, $(a, b) = (b, a)$, $(0, a) = |a|$, $(1, a) = 1$ e que $(a, a) = |a|$.

Proposição 2.3.1: *Sejam a e b inteiros, com $a \neq 0$, temos que $a \mid b$* se, e somente se, *$(a, b) = |a|$*.

Demonstração: Se $a \mid b$, então $|a|$ é um divisor comum de *a* e *b*, seja *c* um divisor comum de *a* e *b*, como $c \mid a$, logo $c \mid |a|$, portanto $(a, b) = |a|$.

Por outro lado, se $(a, b) = |a|$, logo $|a| \mid b$, mas como $a \mid |a|$, então, $a \mid b$.

■

Observe que dados *a* e *b* inteiros, se existir o (*a, b*) de *a* e *b*, então:

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

Assim, é possível supor sempre *a* e *b* não negativos no cálculo do mdc entre *a* e *b*.

Proposição 2.3.2. *Dados a e b números inteiros e k um inteiro positivo, tem-se que (ka, kb) = k(a, b).*

Demonstração: Seja $d = (a, b)$, pelo teorema 2.3.1 existem *x* e *y* inteiros de modo que $d = xa + yb$. Como $d \mid a$ e $d \mid b$, segue da proposição 2.1.2 que:

$$kd \mid ka \text{ e } kd \mid kb, \text{ com } k \text{ inteiro, portanto } kd \mid (ka, kb)$$

Agora como $(ka, kb) \mid ka$ e $(ka, kb) \mid kb$, segue da proposição 2.1.4 que:

$$(ka, kb) \mid xka + ykb = k(xa + yb) = kd.$$

Logo, como $kd \mid (ka, kb)$, $(ka, kb) \mid kd$ e $(ka, kb) > 0$, segue da proposição 2.1.5 que $(ka, kb) = kd$, ou seja, $(ka, kb) \mid k(a, b)$.

■

Proposição 2.3.3. *Se c > 0 e a e b são divisíveis por c, então:*

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

Demonstração: Como *a* e *b* são divisíveis por c, segue que $\frac{a}{c}$ e $\frac{b}{c}$ são números inteiros. Substituindo *a* por $\frac{a}{c}$ e *b* por $\frac{b}{c}$ e tomando k = *c* na Proposição 2.3.2 chega-se ao resultado desejado.

■

Corolário 2.3.1. *Se (a, b) = d, então:*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

Demonstração: Tomando *c* = *d* na Proposição 2.3.3, segue o resultado.

■

Proposição 2.3.6. *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração: Como $(a, b) = 1$ pelo Teorema 2.3.1, existem inteiros x e y tais que $xa + yb = 1$. Multiplicando os dois membros dessa última equação por c segue que $x(ac) + y(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$, então, pela Proposição 2.1.4, $a \mid x(ac) + y(bc)$, ou seja, $a \mid c$.

■

2.4 Algoritmo da Divisão de Euclides

Essa seção contará com resultados que envolverão o Algoritmo de Euclides, o qual será de grande importância para obter as soluções das Equações Diofantinas Lineares.

Teorema 2.4.1: *(Algoritmo de Euclides) Sejam a e b naturais, com $b \neq 0$. Se o Algoritmo de Euclides for aplicado sucessivamente, então o ultimo resto não nulo r_n, satisfaz a seguinte igualdade $(a, b) = r_n$.*

Demonstração: Dados a; b naturais, pode-se supor que $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda se $a \mid b$, tem-se que $(a, b) = a$.

Supondo, então, que $1 < a < b$ e que $a \nmid b$. Logo, pelo Algoritmo de Euclides, é possível escrever $b = aq_1 + r_1$ com $0 < r_1 < a$. Deste modo existem duas possibilidades:

a) Se $r_1 \mid a$, então, $r_1 = (a, r_1) = (a, b - q_1 \cdot a) = (a, b)$ e termina o algoritmo, ou

b) Se $r_1 \nmid a$, então, pode-se efetuar a divisão de a por r_1, obtendo $a = r_1q_2 + r_2$ com $0 < r_2 < r_1$.

Novamente existem duas possibilidades:

a_1) Se $r_2 \mid r_1$, logo, segue que:

$$r_2 = (r_1, r_2) = (r_1, a - r_1 \cdot q_2) = (r_1, a) = (b - q_1 \cdot a, a) = (b, a) = (a, b).$$

b$_1$) Se $r_2 \nmid r_1$, então efetuando a divisão de r_1 por r_2, obtém-se $r_1 = r_2 \cdot q_3 + r_3$ com $0 < r_3 < r_2$.

Esse processo não pode continuar indefinidamente, pois teríamos uma sequência $a > r_1 > r_2 > r_3 > ...$, que não possui um menor elemento, o que não é possível pelo Princípio da Boa Ordem. Logo, para algum n, temos que $r_n \mid r_{n-1}$ o que implica $(a, b) = r_n$.

■

De um modo mais prático, é possível utilizar o seguinte dispositivo no emprego do algoritmo de Euclides para encontrar o (a, b).

Geralmente, para dividir b por a, com $b = aq + r$ utiliza-se o seguinte esquema:

	q
b	a
r	

Se o processo for continuado, tem-se agora a divisão: $a = rq_1 + r_1$, que colocando novamente no esquema, chega-se à:

	q	q_1
b	a	R
r	r_1	

Continuando o processo até quando possível, pode-se encontrar o (a, b), aplicando o dispositivo prático:

	q	q_1	q_2	...	q_{n-1}	q_n	q_{n+1}
b	a	r	r_1	...	r_{n-2}	r_{n-1}	$r_n = (a,b)$
r	r_1	r_2	r_3	...	r_n	0	

Exemplo 2.4.1: Calcular o *mdc* entre 121 e 14.

	8	1	1	1	4
121	14	9	5	4	1 = (121, 14)
9	5	4	1	0	

O algoritmo de Euclides acima fornece que:

$1 = 5 – 4 \cdot 1$

$4 = 9 – 5 \cdot 1$

$5 = 14 – 9 \cdot 1$

$9 = 121 – 14 \cdot 8$

De onde, segue que o (121, 14) = 1. Utilizando as equações anteriores, tem-se que:

$1 = 5 – 4 \cdot 1$

$1 = 5 – (9 – 5 \cdot 1) \cdot 1$

$1 = 2 \cdot 5 – 9$

$1 = 2 \cdot (14 – 9 \cdot 1) – 9$

$1 = 2 \cdot 14 – 3 \cdot 9$

$1 = 2 \cdot 14 – 3 \cdot (121 – 14 \cdot 8)$

$1 = 26 \cdot 14 – 3 \cdot 121$

Logo, é possível escrever que:

$1 = (121; 14) = 121 \cdot (–3) + 14 \cdot (26)$.

CAPÍTULO 3

EQUAÇÕES DIOFANTINAS LINEARES

Neste capítulo serão abordadas as Equações Diofantinas Lineares e seus métodos de resoluções. Serão estudadas as Equações Diofantinas Lineares de duas ou três incógnitas, finalizando com as de n incógnitas.

3.1 Equações Diofantinas Lineares em duas incógnitas

Denomina-se por Equação Diofantina Linear em duas incógnitas, equações do tipo $ax + by = c$, onde a, b e c são números inteiros, não simultaneamente nulos. Também são inteiros os números x e y, que representam incógnitas. Neste caso x e y são chamados de soluções da equação.

Equações desse tipo nem sempre possuem soluções no conjunto dos inteiros, como exemplo, observe a equação $2x + 4y = 7$. Essa equação não possui solução nos inteiros uma vez que, $2x + 4y = 2(x + 2y)$ resulta em um número par, o que é um absurdo, uma vez que 7 é impar.

A equação $2x + 4y = 7$, quando analisada analiticamente num plano, representa uma reta. Mostrar que a equação não possui soluções inteiras significa dizer que esta reta não possui pontos de coordenadas (x, y), com x e y inteiros.

A seguir, serão estudadas as condições para que a equação $ax + by = c$ possua soluções inteiras e como determina-las.

Teorema 3.1.1: *A Equação Diofantina $ax + by = c$, com $a \neq 0$ ou $b \neq 0$, terá solução inteira se, e somente se, $d = (a, b)$ divide c.*

Demonstração: Admita que a equação $ax + by = c$ possua solução inteira, (x_0, y_0), ou seja, $ax_0 + by_0 = c$. Por outro lado, $d|ax_0$ e $d|by_0$, pois $d|a$ e $d|b$. Logo, tem-se que $d|ax_0 + by_0 = c$, isto é, $d|c$.

Reciprocamente suponha que $d = (a, b)$ divide c, será mostrado agora que a Equação Diofantina tem solução nos conjuntos dos números inteiros. Como $d|c$, então existe um inteiro t tal que $c = td$, e como $d = mdc(a, b)$, pelo teorema 2.3.1 existem inteiros m e n tais que $am + bn = d$.

Deste modo, segue que $t(am + bn) = td$, onde $atm + btn = c$. Como tm e tn são inteiros, basta tomar $tm = x$ e $tn = y$, assim o par (tm, tn) é uma solução da equação $ax + by = c$.

■

Se a Equação Diofantina $ax + by = c$ tem solução, então ela é equivalente à equação $a_1x + b_1y = c_1$, onde:

$$a_1 = a/(a, b),\ b_1 = b/(a, b) \text{ e } c_1 = c/(a, b)$$

Note que, pelo Corolário 2.3.1, $(a_1, b_1) = 1$ e, portanto, é possível restringir-se apenas as equações do tipo $ax + by = c$, com $(a, b) = 1$, que sempre possuem soluções.

Proposição 3.1.1. *Seja x_0, y_0 uma solução particular da equação $ax + by = c$, onde $(a, b) = 1$. Então todas as soluções inteiras x, y da equação são da seguinte forma:*

$$x = x_0 - tb,\ y = y_0 + ta, \text{ onde } t \text{ é inteiro}$$

Demonstração: Seja x, y uma solução qualquer da equação $ax + by = c$, logo;

$$ax_0 + by_0 = ax + by = c$$

Portanto, $a(x_0 - x) = b(y - y_0)$ *(i)*

Como $(a, b) = 1$, segue que $b| x_0 - x$, logo;

$$x_0 - x = tb, \text{ ou seja, } x = x_0 - tb, \text{ com } t \text{ inteiro}$$

Substituindo $x_0 - x$ por tb em *(i)*, obtém-se:

$$y - y_0 = ta, \text{ ou seja, } y = y_0 + ta$$

Por outro lado, x, y como no enunciado, é solução, pois;

$$ax + by = a(x_0 - tb) + b(y_0 + ta) = ax_0 + by_0 = c$$

■

Exemplo 3.1.1. *Exprimir* 100 *como soma de dois inteiros positivos de modo que o primeiro seja divisível por* 7 *e o segundo seja divisível por* 11*.*

Solução: Sejam $7x$ e $11y$ esses dois números. Assim, tem-se $7x + 11y = 100$. Como $1 = (7, 11) | 100$ então a equação tem solução.

Usando o Algoritmo de Euclides, será encontrada uma solução particular para a equação $7x + 11y = 100$.

	1	1	1	3
11	7	4	3	1
4	3	1	0	

Observando o algoritmo segue que,

$1 = 4 - 1 \cdot 3$

$3 = 7 - 1 \cdot 4$

$4 = 11 - 1 \cdot 7$

Segue que:

$1 = 4 - 1 \cdot 3$

$1 = 4 - 1 \cdot (7 - 1 \cdot 4)$

$1 = 2 \cdot 4 - 7$

$1 = 2 \cdot (11 - 1 \cdot 7) - 7$

$1 = 7 \cdot (-3) + 11 \cdot (2)$

Multiplicando por 100, tem-se:

$$100 = 7 \cdot (-300) + 11 \cdot (200)$$

Logo, a equação terá como solução particular $x_0 = -300$ e $y_0 = 200$. A solução geral é, então, dada por $(x, y) = (-300 - 11t, 200 + 7t)$.

Como $x > 0$ e $y > 0$, segue que:

$-300 - 11t > 0$, ou seja, $t < -27{,}27$

$200 + 7t > 0$, ou seja, $-28{,}57 < t$.

Logo, $t = -28$, deste modo, tem-se $(x, y) = (-300 - 11\cdot(-28), 200 + 7\cdot(-28)) = (8, 4)$. Assim, os números procurados são $7x = 56$ e $11y = 44$.

Exemplo 3.1.2. *Determinar o menor inteiro positivo que dividido por* 8 *e por* 15 *deixa os restos* 6 *e* 13*, respectivamente.*

Solução: Seja n o número inteiro positivo. Pelo algoritmo da divisão, existem x e y positivos tais que $n = 8x + 6$ e $n = 15y + 13$.

Assim, $8x + 6 = 15y + 13 \rightarrow 8x - 15y = 7$. Como $1 = (8, 15)|7$ a equação tem solução.

Usando o Algoritmo de Euclides, será encontrada uma solução particular para a equação $8x - 15y = 7$.

	1	1	7
15	8	7	1
7	1	0	

Observando o algoritmo segue que:

$1 = 8 - 1 \cdot 7$
$7 = 15 - 1 \cdot 8$.

Segue que:

$1 = 8 - 1 \cdot 7$
$1 = 8 - 1 \cdot (15 - 1 \cdot 8)$
$1 = 8\cdot(2) - 15\cdot(1)$.

Multiplicando por 7, tem-se;

$$7 = 8\cdot(14) - 15\cdot(7).$$

Logo, a equação tem como solução particular $x_0 = 14$ e $y_0 = 7$. A solução geral é, então, dada por $(x, y) = (14 + 15t, 7 + 8t)$.

Como $x > 0$ e $y > 0$, segue que:

$14 - 15t > 0$, ou seja, $t < 14/15$

$7 - 8t > 0$, ou seja, $t < 7/8$.

Como $7/8 < 14/15$, logo $t < 7/8$.

O menor valor de n será obtido ao tomar o menor valor de x e y que satisfaça a equação $8x - 15y = 7$ e, isso acontece quando $t = 0$. Deste modo $(x, y) = (14, 7)$ e, portanto, $n = 118$.

3.2 Equações Diofantinas Lineares em três incógnitas

Denomina-se Equação Diofantina Linear em três incógnitas, equações do tipo $a_1x + a_2y + a_3z = b$, onde a_1, a_2, a_3 e b são números inteiros, não simultaneamente nulos, também são inteiros os números x, y e z, que são chamados soluções da equação.

Teorema 3.2.1: *A equação $a_1x + a_2y + a_3z = b$ admite solução se, e somente se, $d = mdc(a, b, c)$ divide b.*

Demonstração: É claro que se a equação possuir solução então $d|b$, pois a demonstração segue o mesmo raciocínio utilizado na demonstração do teorema 3.1.1.

Reciprocamente como $d|b$ considere $d_1 = (a_1, a_2)$ e observe que $d = (d_1, a_3)$. Nesse caso, pelo teorema 2.3.1 existem os inteiros u, v, k e w, tais que $d_1 = a_1u + a_2v$ e $d = d_1k + a_3w$, isto é:

$$d = (a_1u + a_2v)k + a_3w \rightarrow d = a_1uk + a_2vk + a_3w.$$

Tomando $uk = x_0$, $vk = y_0$ e $w = z_0$, tem-se $d = a_1x_0 + a_2y_0 + a_3z_0$. Daí, como $d|b$, existe um número inteiro q, tal que $b = dq$.

Veja que:

$$d = a_1x_0 + a_2y_0 + a_3z_0 \rightarrow b = dq = a_1qx_0 + a_2qy_0 + a_3qz_0.$$

Logo, (qx_0, qy_0, qz_0) é uma solução particular de $a_1x + a_2y + a_3z = b$.

■

Exemplo 3.2.1. *Encontre uma solução particular da equação 30x + 27y + 15z = 6.*

Solução: É preciso inicialmente calcular o *mdc*(30, 27), assim pelo Algoritmo de Euclides segue que;

	1	9
30	27	3
3	0	

Observando o algoritmo segue que:

$0 = 27 - 3 \cdot 9$

$3 = 30 - 27 \cdot 1$

Assim, o *mdc*(30, 27) = 3. Aplicando novamente o Algoritmo de Euclides para calcular o mdc(3, 15) tem-se:

	1	9
30	27	3
3	0	

Observando o algoritmo segue que:

$0 = 15 - 3 \cdot 5$

$3 = 30 - 27 \cdot 1$

Segue que:

$0 = 15 - 3 \cdot 5$

$0 = 15 - (30 - 27 \cdot 1) \cdot 5$

$0 = 15 – 30\cdot5 + 27\cdot5$,

Adicionando 3 a ambos os membros da igualdade, segue que:

$3 = 15 – 30\cdot5 + 27\cdot5 + 3$
$3 = 15 – 30\cdot5 + 27\cdot4 + 27 + 3$
$3 = 30\cdot(-4) + 27\cdot(4) + 15\cdot(1)$

Multiplicando por 2, tem-se;

$$6 = 30\cdot(-8) + 27\cdot(8) + 15\cdot(2)$$

Logo, a equação possui como solução particular $x_0 = -8$, $y_0 = 8$ e $z_0 = 2$.

Para encontrar a solução geral de uma Equação Diofantina Linear de três variáveis, deve-se utilizar os seguintes passos:

- Por meio de uma substituição, deve-se reduzir a equação original a uma equação com duas variáveis e em seguida resolver essa nova equação.
- A partir dessa solução, é necessário retornar a substituição feita inicialmente e resolver mais uma equação com duas variáveis. Obtendo ao final deste processo a solução geral.

Considere a equação $a_1x + a_2y + a_3z = b$, com a_1, a_2 e a_3 não simultaneamente nulos. Se a equação possui solução então $d = mdc(a_1; a_2; a_3) \mid b$. Reduzindo essa equação para duas variáveis, considerando $a_1x + a_2y = p$, tem-se;

$$p + a_3z = b$$

Essa equação possui solução, pois $mdc(1; a_3) = 1$ e $1 \mid b$, logo pela preposição 3.1.1, a equação tem como solução geral,

$$p = p_0 – a_3t_1 \text{ e } z = z_0 + t_1, \text{ onde } t_1 \text{ é inteiro}$$

A partir dessa solução geral encontrada, será escolhido um valor conveniente para t_1, que satisfaça a seguinte condição:

$$d_1 = mdc(a_1; a_2) \mid (p_0 – a_3t_1)$$

De acordo com essa condição será encontrada a solução geral da equação $a_1x + a_2y = p = p_0 + a_3t_1$, e posteriormente, encontrada a solução geral da equação $a_1x + a_2y + a_3z = b$.

Como $d_1 \mid (p_0 - a_3t_1)$, logo a equação $a_1x + a_2y = p_0 - a_3t_1$ tem solução, então ela é equivalente à equação $a_4x + a_5y = b_1$, onde:

$$a_4 = a_1/d_1,\ a_5 = a_2/d_1 \text{ e } b_1 = (p_0 - a_3t_1)/d_1 \text{ e ainda } (a_4, a_5) = 1$$

Portanto a solução da equação $a_1x + a_2y = p_0 - a_3t_1$ é:

$$x = x_0 - a_5t_2,\ y = y_0 + a_4t_2, \text{ onde } t_2 \text{ é inteiro}$$

Desta forma a solução geral da equação $a_1x + a_2y + a_3z = b$ é:

$$x = x_0 - a_5t_2,\ y = y_0 + a_4t_2 \text{ e } z = z_0 + t_1.$$

Essa solução é gerada a partir de um valor apropriado, atribuído ao parâmetro t_1 no processo de descoberta dessa solução. Desta forma, é possível afirmar que a cada t_1 apropriado será gerado um novo conjunto solução.

Exemplo 3.2.2. *Encontre a solução geral da equação $30x + 27y + 15z = 6$.*

Solução: Inicialmente será encontrada a solução geral da equação $p + 15z = 6$, onde $30x + 27y = p$. É fácil ver que $p_0 = -9$ e $z_0 = 1$ é uma solução particular da equação $p + 15z = 6$,

Logo a solução geral da mesma equação é:

$$p = -9 - 15t_1 \text{ e } z = 1 + t_1, \text{ com } t_1 \text{ inteiro}$$

Agora é preciso encontrar a solução geral da equação $30x + 27y = p = -9 - 15t_1$, pelo exemplo 3.2.1 segue que $3 = (30, 27)$, e como $3 \mid -9 - 15t_1$, logo a equação possui solução.

Ainda pelo exemplo 3.2.1 tem-se que:

$3 = 30\cdot(1) + 27\cdot(-1)$

Multiplicando por $(–9 – 15t_1)/3$ segue que:

$3\cdot (–9 – 15t_1)/3 = 30\cdot (–9 – 15t_1)/3 + 27\cdot (9 + 15t_1)/3$

$30\cdot (–3 – 5t_1) + 27\cdot (3 + 5t_1) = –9 – 15t_1 = p$

Logo uma solução particular é $x_0 = –3 – 5t_1$ e $y_0 = 3 + 5t_1$.

Portanto a solução geral da equação $30x + 27y = p = –9 – 15t_1$ é:

$x = –3 – 5t_1 – 27t_2$ e $y = 3 + 5t_1 + 30t_2$, com t_2 inteiro

Desta forma a solução geral da equação $30x + 27y + 15z = 6$ é:

$x = –3 – 5t_1 – 27t_2$, $y = 3 + 5t_1 + 30t_2$ e $z = 1 + t_1$, com t_1, t_2 inteiros.

Vale lembrar que no exemplo 3.2.1 foi encontrada a solução particular $x_0 = -8$, $y_0 = 8$ e $z_0 = 2$, para a equação $30x + 27y + 15z = 6$, neste caso particular pode-se observar que $z = 1 + t_1$, logo, $2 = 1 + t_1$, ou seja, $t_1 = 1$.

Aplicando $t_1 = 1$ e usando a solução particular do exemplo 3.2.1 nas equações $x = –3 – 5t_1 – 27t_2$, $y = 3 + 5t_1 + 30t_2$, encontra-se $t_2 = 0$, mostrando que o valor de t_2 varia de acordo com o valor de t_1 quando se procura uma solução particular.

3.3 Equações Diofantinas Lineares em n incógnitas

A abordagem das Equações Diofantinas Lineares de n incógnitas seguirá o raciocínio usado por CAMPOS, 2013, p. 37.

Considere agora a equação $a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + a_nx_n = b$, onde cada a_i, com i = 1; 2; 3; ⋯ ; n, sejam inteiros não nulos simultaneamente. A mesma argumentação usada para provar o Teorema 3.1.1 garante que essa equação admite soluções se, $d = mdc(a_1; a_2; a_3; \cdots ; a_n)$ divide b.

Se $d_1 = mdc(a_1; a_2)$, então existem k_1 e k_2 inteiros para os quais $a_1k_1 + a_2k_2 = d_1$. E como $d_2 = mdc(d_1; a_3)$, então existem k_3, k_4 inteiros de maneira que $d_2 = d_1k_3 +$

a_3k_4. Procedendo de forma análoga n – 1 vezes, chega-se em $d = mdc(d_{n-1}; a_n)$, então, $a_1(x'_1q) + a_2(x'_2q) + a_3(x'_3q) + \cdots + a_{n-1}(x'_{n-1}q) + a_n(x'_nq) = dq = b$ para algum q inteiro, o que mostra que uma das soluções particulares da equação inicial é a seguinte:

$$(x'_1q; x'_2q; x'_3q; \cdots ; x'_{n-1}q; x'_nq)$$

Para encontrar a solução geral da equação $a_1x_1 + a_2x_2 + a_3x_3 + \cdots + a_{n-1}x_{n-1} + a_nx_n = b$, é necessário reduzir a equação original a uma Equação Diofantina Linear de duas incógnitas. Para isso, deve-se fazer uma substituição de n – 1 incógnitas por outra incógnita qualquer, diferente das já existentes. Feito isso, basta encontrar a solução geral desta nova equação gerada.

Aplicando esse processo repetidas vezes, serão encontrados todos os valores de x_i com i = 1; 2; 3; ⋯ ; n, assim como desenvolvido para encontrar a solução geral das Equações Diofantinas Lineares de duas e três incógnitas.

Vale ressaltar ainda que sempre é possível obter equações equivalentes as geradas quando se aplica uma incógnita qualquer, de modo que nessas novas equações tenham-se $d_i = 1$, com i = 1; 2; 3; ⋯ ; n – 1.

Então, a solução geral de uma Equação Diofantina Linear de n variáveis, se apresenta da seguinte forma:

$x_1 = x'_1 – a_2t_{n-1}$, $x_2 = x'_2 + a_1t_{n-1}$, $x_3 = x'_3 + t_{n-2}$, ⋯ , $x_n = x'_n + t_1$, com t_i inteiro e i = 1; 2; 3; ⋯ ; n – 1

A seguir será mostrado um problema simples para exemplificar o método citado acima.

Exemplo 3.3.1. *Encontre a solução geral da equação a + 2b + 3c + 4d + 5e = 6.*

Solução: Como $d = mdc(1, 2, 3, 4, 5) = 1$ divide 6, logo a equação possui solução. Fazendo a substituição $a + 2b + 3c + 4d = p$, tem-se a seguinte equação $p + 5e = 6$, que possui solução pois $mdc(1,5) = 1$ e divide 6.

É fácil ver que $p_0 = 1$ e $e_0 = 1$, é uma solução particular da equação $p + 5e = 6$, logo sua solução geral é:

$$p = 1 - t_1,\ e = 1 + t_1, \text{ com } t_1 \text{ inteiro}$$

Deste modo, segue que, $a + 2b + 3c + 4d = p = 1 - t_1$, que possui solução pois $mdc(1, 2, 3, 4) = 1$. Agora fazendo $a + 2b + 3c = p'$, tem-se $p' + 4d = 1 - t_1$ que possui solução, pois $mdc(1,4) = 1$.

É fácil ver que:

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

$1\cdot(1 - t_1) = 1\cdot(-3)\cdot(1 - t_1) + 4\cdot(1)\cdot(1 - t_1)$

$1 - t_1 = 1\cdot(-3 + 3t_1) + 4\cdot(1 - t_1)$

Logo $p'_0 = -3 + 3t_1$, $d_0 = 1 - t_1$ é uma solução particular da equação $p' + 4d = 1 - t_1$.

Portanto a solução geral da equação $p' + 4d = 1 - t_1$ é:

$$p' = -3 + 3t_1 - 4t_2,\ d = 1 - t_1 + t_2 \text{ com } t_1,\ t_2 \text{ inteiros.}$$

Assim, segue que, $a + 2b + 3c = p' = -3 + 3t_1 - 4t_2$, que possui solução pois $mdc(1, 2, 3) = 1$. Então fazendo $a + 2b = p''$, implica em $p'' + 3c = -3 + 3t_1 - 4t_2$ que possui solução, pois $mdc(1,3) = 1$.

É fácil ver que:

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

$1\cdot(-3 + 3t_1 - 4t_2) = 1\cdot(-2)\cdot(-3 + 3t_1 - 4t_2) + 3\cdot(1)\cdot(-3 + 3t_1 - 4t_2)$

$-3 + 3t_1 - 4t_2 = 1\cdot(6 - 6t_1 + 8t_2) + 3\cdot(-3 + 3t_1 - 4t_2)$

Logo $p''_0 = 6 - 6t_1 + 8t_2$, $c_0 = -3 + 3t_1 - 4t_2$ é uma solução particular da equação $p'' + 3c = -3 + 3t_1 - 4t_2$.

Portanto, a solução geral da equação $p'' + 3c = -3 + 3t_1 - 4t_2$ é:

$$p'' = 6 - 6t_1 + 8t_2 - 3t_3,\ c = -3 + 3t_1 - 4t_2 + t_3, \text{ com } t_1, t_2, t_3 \text{ inteiros.}$$

Por fim, tem-se $a + 2b = p'' = 6 - 6t_1 + 8t_2 - 3t_3$, que possui solução, pois $mdc(1, 2) = 1$.

É fácil ver que:

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

$$1\cdot(6 - 6t_1 + 8t_2 - 3t_3) = 1\cdot(-1)\cdot(6 - 6t_1 + 8t_2 - 3t_3) + 2\cdot(1)\cdot(6 - 6t_1 + 8t_2 - 3t_3)$$

$$6 - 6t_1 + 8t_2 - 3t_3 = 1\cdot(-6 + 6t_1 - 8t_2 + 3t_3) + 2\cdot(6 - 6t_1 + 8t_2 - 3t_3)$$

Logo $a_0 = -6 + 6t_1 - 8t_2 + 3t_3$, $b_0 = 6 - 6t_1 + 8t_2 - 3t_3$ é uma solução particular da equação $a + 2b = 6 - 6t_1 + 8t_2 - 3t_3$

Portanto a solução geral da equação $a + 2b = 6 - 6t_1 + 8t_2 - 3t_3$ é:

$$a = -6 + 6t_1 - 8t_2 + 3t_3 - 2t_4,\ b = 6 - 6t_1 + 8t_2 - 3t_3 + t_4, \text{ com } t_1, t_2, t_3, t_4 \text{ inteiros.}$$

Então a solução geral da equação $a + 2b + 3c + 4d + 5e = 6$ é:

$$a = -6 + 6t_1 - 8t_2 + 3t_3 - 2t_4,\ b = 6 - 6t_1 + 8t_2 - 3t_3 + t_4,\ c = -3 + 3t_1 - 4t_2 - t_3,\ d = 1 - t_1 + t_2,\ e = 1 + t_1, \text{ com } t_1, t_2, t_3, t_4 \text{ inteiros.}$$

Vale observar trivialmente que se $t_1 = t_2 = t_3 = t_4 = 0$ tem-se a seguinte solução particular:

$$a = -6,\ b = 6,\ c = -3,\ d = 1,\ e = 1$$

Deste modo, aplicando os valores encontrados na equação $a + 2b + 3c + 4d + 5e = 6$ obtém-se:

$$-6 + 2\cdot(6) + 3\cdot(-3) + 4\cdot(1) + 5\cdot(1) = -6 + 12 - 9 + 4 + 5 = 6$$

CAPÍTULO 4

PROBLEMAS ENVOLVENDO EQUAÇÕES DIOFANTINAS LINEARES

Neste capítulo deste trabalho, que está dividido em dois tópicos, serão abordados primeiramente os problemas que envolvem as Equações Diofantinas Lineares e por fim será apresentada uma breve sequência didática para o ensino básico sobre o tema estudado. Vale ressaltar que grande parte desses problemas com as Equações Diofantinas ocorre em forma de situações problemas do cotidiano.

4.1 Aplicações Práticas Envolvendo Equações Diofantinas Lineares

Apresentam-se alguns problemas práticos que podem ocorrer no dia a dia na forma das Equações Diofantinas Lineares com duas variáveis ou três variáveis.

Problema 4.1.1. *(Proposto por Euller) Um grupo de homens e mulheres gastaram numa taberna 1000 patacas. Cada homem pagou 19 patacas e cada mulher 13. Quantos eram os homens e quantas eram as mulheres?*

Solução: O problema proposto por Euller fornece a seguinte equação $19x + 13y = 1000$, onde x e y representam respectivamente o número de homens e mulheres pedidos por Euller.

Como $(19, 13) = 1$, logo a equação $19x + 13y = 1000$ possui solução. Usando o algoritmo de Euclides tem-se:

	1	2	6
19	13	6	1
6	1	0	

Observando o algoritmo é possível escrever:

$1 = 13 - 2 \cdot 6$

$6 = 19 - 1 \cdot 13.$

Segue que:

$1 = 13 - 2 \cdot 6$

$1 = 13 - 2 \cdot (19 - 1 \cdot 13)$

$1 = 19 \cdot (-2) + 13 \cdot (3)$.

Multiplicando por 1000, tem-se;

$$1000 = 19 \cdot (-2000) + 13 \cdot (3000).$$

Logo, a equação tem como solução particular $x_0 = -2000$ e $y_0 = 3000$. A solução geral é, então, dada por $(x, y) = (-2000 - 13t, 3000 + 19t)$. Com t inteiro.

Como $x > 0$ e $y > 0$, segue que:

$-2000 - 13t > 0$, ou seja, $t < -153{,}84$

$3000 + 19t > 0$, ou seja, $t > -157{,}89$.

Como $7/8 < 14/15$, logo $t < 7/8$.

Logo os possíveis valores para t são: -154, -155, -156, -157. Organizando esses valores em uma tabela obtém-se a seguinte situação:

t	-154	-155	-156	-157
x	2	15	28	41
y	74	55	36	17

Portanto, encontra-se os seguintes números de homens e de mulheres:

(a) 2 homens e 74 mulheres.

(b) 15 homens e 55 mulheres.

(c) 28 homens e 36 mulheres.

(d) 41 homens e 17 mulheres.

Problema 4.1.2. *Se um macaco sobe uma escada de dois em dois degraus, sobra um degrau; se ele sobe de três em três degraus, sobram dois degraus. Quantos degraus a escada possui, sabendo que o número de degraus é múltiplo de sete e está compreendido entre 40 e 100?*

Solução: Do enunciado é possivel encontrar duas equações, $2x + 1 = n$ e $3y + 2 = n$, onde n é o número de degraus da escada e cada uma das equações descreve uma situação diferente descrita no enunciado.

Unindo as duas equações, tem-se:

$$2x + 1 = n = 3y + 2, \text{ ou seja, } 2x - 3y = 1$$

Como $(2, 3) = 1$, logo a equação $2x - 3y = 1$ possui solução. É fácil ver que $x_0 = 2$ e $y_0 = 1$ é uma solução particular da equação. A solução geral é, então, dada por $(x, y) = (2 + 3t, 1 + 2t)$. Com t inteiro.

Como $2x + 1 = n$, substituindo $x = 2 + 3t$, obtém-se; $5 + 6t = n$.

Mas como $40 \leq n \leq 100$, logo, segue que:

$40 \leq 5 + 6t \leq 100$
$35 \leq 6t \leq 95$
$5{,}8 \leq t \leq 15{,}8$

Logo os possíveis valores para t são: 6, 7, 8, 9, 10, 11, 12, 13, 14, 15. Organizando esses valores em uma tabela obtém-se a seguinte situação:

t	6	7	8	9	10	11	12	13	14	15
n	41	47	53	59	65	71	77	83	89	95

Portanto, para que n seja múltiplo de 7, deve-se ter $t = 12$, concluindo então que $n = 77$ degraus.

Problema 4.1.3. *Uma papelaria fez uma promoção de cadernos pequenos e cadernos grandes. Cada caderno pequeno custa R$ 4,00 e cada caderno grande custa R$ 6,00. Com R$ 40,00, quais as possíveis quantidades de cadernos pequenos e grandes que posso comprar, sabendo que vou comprar no mínimo 2 cadernos pequenos e 3 cadernos grandes?*

Solução: Sejam x e y respectivamente as quantidades de cadernos pequenos e grandes que é possível comprar. Logo, do enunciado obtem-se a equação $4x + 6y = 40$, que é equivalente a equação $2x + 3y = 20$.

Como $(2, 3) = 1$, logo a equação $2x + 3y = 20$ possui solução. É fácil ver que $2\cdot(-1) + 3\cdot(1) = 1$, portanto $2\cdot(-20) + 3\cdot(20) = 20$.

Logo, a equação possui como solução particular $x_0 = -20$ e $y_0 = 20$. A solução geral é, então, dada por $(x, y) = (-20 - 3t, 20 + 2t)$. Com t inteiro.

Das condições do enunciado segue que:

$x \geq 2 \rightarrow -20 - 3t \geq 2 \rightarrow t \leq -7{,}33$

$y \geq 3 \rightarrow 20 + 2t \geq 3 \rightarrow t \geq -8{,}5$

Logo, deve-se ter $t = -8$, assim $x = 4$ e $y = 4$, ou seja, nas condições do enunciado só é possível comprar 4 cadernos pequenos e 4 cadernos grandes.

Problema 4.1.4. (UFC – CE 2004) *Um poliedro convexo só tem faces triangulares e quadrangulares. Se ele tem 20 arestas e 10 vértices; encontre o número de faces triangulares desse poliedro.*

a) 12 b) 11 c) 10 d) 9 e) 8

Solução: Sejam x e y o número de faces triangulares e quadrangulares, respectivamente. Como cada face triangular tem 3 lados, cada face quadrangular tem 4 lados e o número de arestas de um poliedro é igual a metade da soma dos lados de todos os polígonos que formam esse poliedro, pode-se escrever a seguinte equação $3x + 4y = 40$.

Como $(3, 4) = 1$, logo a equação $3x + 4y = 40$ possui solução. É fácil ver que $3\cdot(-1) + 4\cdot(1) = 1$, portanto $3\cdot(-40) + 4\cdot(40) = 40$

Logo, a equação possui como solução particular $x_0 = -40$ e $y_0 = 40$. A solução geral é, então, dada por $(x, y) = (-40 - 4t, 40 + 3t)$. Com t inteiro.

Como os valores de x e y devem ser inteiros positivos, segue que:

$x > 0 \rightarrow -40 - 4t > 0 \rightarrow t < -10$

$y > 0 \rightarrow 40 + 3t > 3 \rightarrow t > -13$,

Logo os possíveis valores para t são: -11, -12, -13, Organizando esses valores em uma tabela obtém-se a seguinte situação:

t	-11	-12	-13
x	4	8	12
y	7	4	1

Logo, existem três soluções distintas, porém a relação de Euller para poliedros convexos nos diz que V + F = A + 2, ou seja, 10 + F = 20 + 2, portanto o poliedro pedido deverá ter 12 faces.

Assim é necessário que, $x + y = 12 \rightarrow -40 - 4t + 40 + 3t = 12 \rightarrow t = -12$, logo a única solução do problema é obtida quando $t = -12$, portanto o poliedro tem 8 faces triangulares e 4 faces quadrangulares.

Problema 4.1.5. (OBMEP – 2012 – NÍVEL 3) *Para fazer várias blusas iguais, uma costureira gastou R$ 2,99 para comprar botões de 4 centavos e laços de 7 centavos. Ela usou todos os botões e laços que comprou. Quantas blusas ela fez?*

a) 2 b) 5 c) 10 d) 13 e) 23

Solução: Sejam x e y, *respectivamente,* as quantidades de botões e laços comprados. Assim, pode-se deduzir a seguinte equação $0{,}04x + 0{,}07y = 2{,}99$, que é equivalente a equação $4x + 7y = 299$.

Como $(4, 7) = 1$, logo a equação $4x + 7y = 299$ possui solução. É fácil ver que $4\cdot(2) + 7\cdot(-1) = 1$, portanto $4\cdot(598) + 4\cdot(-299) = 299$

Logo, a equação possui como solução particular $x_0 = 598$ e $y_0 = -299$. A solução geral é, então, dada por $(x, y) = (598 - 7t, -299 + 4t)$. Com t inteiro.

Como ela usou todos os botões e laços que comprou, então pode-se supor sem perda de generalidade que o número de botões é múltiplo do número de laços. Ou seja, x = $k \cdot y$, com k inteiro.

Portanto, tem-se que $1 \leq y \leq x$. Logo, pode-se observar as seguintes desigualdades.

$1 \leq -299 + 4t \rightarrow t \geq 300/4 \rightarrow t \geq 75$

$-299 + 4t \leq 598 - 7t \rightarrow 11t \leq 897 \rightarrow t \leq 81{,}5$

Assim, os possíveis valores para t são: 75, 76, 77, 78, 79, 80, 81, Organizando esses valores em uma tabela encontra-se a seguinte situação:

t	75	76	77	78	79	80	81
x	73	66	59	52	45	38	31
y	1	5	9	13	17	21	25

De todas as soluções possíveis existem duas delas que satisfazem a condição x = $k \cdot y$, que ocorrem quando t = 75 e t = 78, analisando os itens do enunciado, é possível concluir que o item correto é o item d. Portanto a solução do problema é 13 laços.

Problema 4.1.6. *Um restaurante está fazendo a seguinte promoção: 5 sucos, 10 fatias pizza e 6 salgados custam juntos R$ 48,00. Quanto custa cada um dos produtos consumidos?*

Solução: Sejam x, y e z, respectivamente, os preços unitários do suco, fatia de pizza e salgado.

De acordo com o enunciado tem-se a seguinte equação $5x + 10y + 6z = 48$, que possui solução, pois (5, 10, 6) = 1. Fazendo $5x + 10y = p$, obtém-se uma nova equação $p + 6z = 48$, que possui solução, pois (1, 6) = 1.

É fácil ver que $1 \cdot (-5) + 6 \cdot (1) = 1$, portanto $1 \cdot (-240) + 6 \cdot (48) = 48$. Logo, a equação possui como solução particular $p_0 = -240$ e $z_0 = 48$. A solução geral é, então, dada por $(p, z) = (-240 - 6k, 48 + k)$ com k inteiro.

Como os preços unitários do suco, fatia de pizza e salgado são positivos, segue que:

$p > 0 \rightarrow -240 - 6k > 0 \rightarrow k < -40$

$z > 0 \rightarrow 48 + k > 0 \rightarrow k > -48$

Logo, os possíveis valores para k são: −41, −42, −43, −44, −45, −46, −47, Organizando esses valores em uma tabela encontra-se a seguinte situação:

k	−41	−42	−43	−44	−45	−46	−47
p	6	12	18	24	30	36	42
z	7	6	5	4	3	2	1

Analisando a equação $5x + 10y = p$, segue que para essa equação ter solução, (5, 10) = 5 deve dividir p. Isso ocorre apenas quando $p = 30$. Logo, se obtém a seguinte equação $5x + 10y = 30$, que é equivalente a equação $x + 2y = 6$.

É fácil ver que $1 \cdot (6) + 2 \cdot (0) = 6$, logo, a equação possui como solução particular $x_0 = 6$ e $y_0 = 0$. A solução geral é, então, dada por $(x, y) = (6 - 2t, t)$. Com t inteiro. Como x e y devem ser positivos, segue que:

$x > 0 \rightarrow 6 - 2t > 0 \rightarrow t < 3$

$y > 0 \rightarrow t > 0$

Logo os possíveis valores para t são: 1 e 2. Organizando esses valores em uma tabela encontra-se a seguinte situação:

t	1	2
x	4	2
y	1	2

Substituindo os valores de $t = \{1, 2\}$ nas equações $x = 6 - 2t$ e $y = t$ e o valor de $k = -45$ na equação $z = 48 + k$, se chega aos seguinte valores para os preços dos produtos.

Preço do suco (x): R$ 2,00 Preço do suco (x): R$ 4,00

Preço da fatia de pizza (y): R$ 2,00 Preço da fatia de pizza (y): R$ 1,00

Preço do salgado (z): R$ 3,00 Preço do salgado (z): R$ 3,00

Problema 4.1.6. Combinando moedas de 1, 10, e 25 centavos, como se pode pagar uma dívida de 59 centavos?

Solução: Sejam x, y e z, respectivamente, os números de moedas de 1, 10, 25 centavos usadas para pagar a dívida.

De acordo com o enunciado tem-se a seguinte equação $x + 10y + 25z = 59$, que possui solução, pois $(1, 10, 25) = 1$. Fazendo $x + 10y = p$, se obtém uma nova equação $p + 25z = 59$, que possui solução, pois $(1, 25) = 1$.

É fácil ver que $1\cdot(9) + 25\cdot(2) = 59$. Logo, tem-se como solução particular da equação $p + 25z = 59$, os valores $p_0 = 9$ e $z_0 = 2$. A solução geral é, então, dada por $(p, z) = (9 – 25k, 2 + k)$ com k inteiro.

Como os números de moedas devem não negativos, segue que:

$p \geq 0 \rightarrow 9 – 25k \geq 0 \rightarrow k \leq 9/25$

$z \geq 0 \rightarrow 2 + k \geq 0 \rightarrow k \geq –2$

Logo os possíveis valores para k são: -2, -1, 0. Organizando esses valores em uma tabela encontra-se a seguinte situação:

k	-2	-1	0
p	59	34	9
z	0	1	2

Analisando a equação $x + 10y = p$, é possível concluir que para essa equação ter solução, $(1, 10) = 1$ deve dividir p. Isso ocorre para qualquer valor de p encontrado na equação $p + 25z = 59$. Logo se obtém as seguintes equações: $x + 10y = 59$, $x + 10y = 34$, $x + 10y = 9$.

Analisando a equação $x + 10y = 59$, que ocorre quando $k = -2$

É fácil ver que $1\cdot(9) + 10\cdot(5) = 59$, logo, a equação possui como solução particular $x_0 = 9$ e $y_0 = 5$. A solução geral é, então, dada por $(x, y) = (9 - 10t_1, 5 + t_1)$ com t_1 inteiro. Como x e y devem ser não negativos, segue que:

$x \geq 0 \rightarrow 9 - 10t_1 \geq 0 \rightarrow t_1 \leq 9/10$

$y \geq 0 \rightarrow 5 + t_1 \geq 0 \rightarrow t_1 \geq -5$

Logo, os possíveis valores para t_1 são: -5, -4, -3, -2, -1, e 0. Organizando esses valores em uma tabela encontra-se a seguinte situação:

t_1	-5	-4	-3	-2	-1	0
x	59	49	39	29	19	9
y	0	1	2	3	4	5

Assim se pode concluir que se $k = -2$, temos pela equação $p + 25z = 59$ que $z = 0$ e tem-se ainda pela tabela anterior os possíveis valores de x e y. Deste modo obtém-se as primeiras soluções para a equação $x + 10y + 25z = 59$, são elas:

$x = 59$, $y = 0$ e $z = 0$
$x = 49$, $y = 1$ e $z = 0$
$x = 39$, $y = 2$ e $z = 0$
$x = 29$, $y = 3$ e $z = 0$
$x = 19$, $y = 4$ e $z = 0$
$x = 9$, $y = 5$ e $z = 0$

Analisando a equação $x + 10y = 34$, que ocorre quando $k = -1$

É fácil ver que $1\cdot(4) + 10\cdot(3) = 34$, logo, a equação possui como solução particular $x_0 = 4$ e $y_0 = 3$. A solução geral é, então, dada por $(x, y) = (4 - 10t_2, 3 + t_2)$ com t_2 inteiro. Como x e y devem ser não negativos, segue que:

$x \geq 0 \rightarrow 4 - 10t_2 \geq 0 \rightarrow t_2 \leq 4/10$

$y \geq 0 \rightarrow 3 + t_2 \geq 0 \rightarrow t_2 \geq -3$

Logo, os possíveis valores para t_2 são: −3, −2, −1, e 0. Organizando esses valores em uma tabela encontramos a seguinte situação:

t_2	−3	−2	−1	0
X	34	24	14	4
Y	0	1	2	3

Assim é possível concluir que se $k = -1$, segue pela equação $p + 25z = 59$ que $z = 1$ e temos ainda pela tabela anterior os possíveis valores de x e y. Deste modo se obtém outras soluções para a equação $x + 10y + 25z = 59$, são elas:

$x = 34$, $y = 0$ e $z = 1$
$x = 24$, $y = 1$ e $z = 1$
$x = 14$, $y = 2$ e $z = 1$
$x = 4$, $y = 3$ e $z = 1$

Analisando a equação $x + 10y = 9$, que ocorre quando $k = 0$

É fácil ver que $1\cdot(9) + 10\cdot(0) = 9$, logo, a equação tem como solução particular $x_0 = 9$ e $y_0 = 0$. A solução geral é, então, dada por $(x, y) = (9 - 10t_3, t_3)$ com t_3 inteiro. Como x e y devem ser não negativos, segue que:

$x \geq 0 \rightarrow 9 - 10t_3 \geq 0 \rightarrow t_3 \leq 9/10$

$y \geq 0 \rightarrow t_3 \geq 0$

Logo, o único valor possível para t_3 é 0. De onde se conclui que os possíveis valores de x e y são, respectivamente, 9 e 0.

Assim se conclui que se $k = 0$, segue pela equação $p + 25z = 59$ que $z = 2$ e se obtém ainda a última solução para a equação $x + 10y + 25z = 59$, é ela:

$x = 9$, $y = 0$ e $z = 2$

Portanto, existem 11 formas distintas de se pagar a dívida de 59 centavos com moedas de 1, 10 e 25 centavos.

Assim se encerra as situações problemas que envolvem Equações Diofantinas Lineares, deixando exposto que as equações abordadas aqui representam apenas uma gota d'água quando comparadas a imensidão do mar que são os diferentes tipos de Equações Diofantinas Lineares.

4.2 Sequência didática: Equações Diofantinas Lineares no ensino básico

Quando aluno do Ensino Básico nunca tive contato com as Equações Diofantinas, e, atualmente, como professor da rede estadual do Ceará nunca lecionei tal tema em minhas aulas do Ensino médio, pois este tema não faz parte da grade curricular de meus alunos. Estudei este conteúdo de forma indireta através das funções lineares durante o primeiro ano do Ensino Médio, porém, enquanto aluno do Ensino Básico, jamais tinha observado que funções lineares poderiam ter outro ponto de vista.

Diante de tal situação, decidi escrever este tópico que pode vir a servir de material de apoio para futuras abordagens das Equações Diofantinas Lineares por professores do Ensino Básico.

Atividade 4.2.1. *1º encontro – 4 aulas de 50 minutos*

No primeiro encontro deve ser realizada uma revisão de conceitos da teoria dos números, mais precisamente, a abordagem deve ocorrer sobre divisibilidade nos inteiros, divisão euclidiana, mdc e algoritmo de Euclides. É indicado a utilização do 2º capítulo deste trabalho como referencial teórico.

São propostos ainda os seguintes exercícios para avaliar os alunos e para finalizar os conceitos estudados.

Exercício 4.2.1.1. (Divisibilidade nos Inteiros) *Encontrar os divisores dos números 18, 36 e 24.*

Solução:

D(18) = 1; 2; 3; 6; 9; 18.

D(36) = 1; 2; 3; 4; 6; 9; 12; 18; 36.

D(24) = 1; 2; 3; 4; 6; 8; 12; 24.

Exercício 4.2.1.2. (Divisão Euclidiana) *Encontrar o quociente e o resto da divisão de 80 por 14.*

Solução: Considere as diferenças sucessivas:

$80 - 14 = 66 > 14$,
$80 - 2 \cdot 14 = 52 > 14$,
$80 - 3 \cdot 14 = 38 > 14$,
$80 - 4 \cdot 14 = 24 > 14$,
$80 - 5 \cdot 14 = 10 < 14$,

Que nos dá $q = 5$ e $r = 10$.

Exercício 4.2.1.3. (Divisão Euclidiana) *Encontrar os possíveis restos na divisão de um natural qualquer por três.*

Solução: Considere as seguintes desigualdades:

$1 = 3 \cdot 0 + 1$ $\quad$ $7 = 3 \cdot 2 + 1$

$2 = 3 \cdot 0 + 2$ $\quad$ $8 = 3 \cdot 2 + 2$

$3 = 3 \cdot 1 + 0$ $\quad$ $9 = 3 \cdot 3 + 0$

$4 = 3 \cdot 1 + 1$ $\quad$ $10 = 3 \cdot 3 + 1$

$5 = 3 \cdot 1 + 2$ $\quad$ $11 = 3 \cdot 3 + 2$

$6 = 3 \cdot 2 + 0$ $\quad$ $12 = 3 \cdot 4 + 0$

Logo, se concluir que os possíveis restos são: 0, 1 e 2.

Exercício 4.2.1.4. (mdc) *Encontrar o máximo divisor comum de 32 e 56.*

Solução: Nesse exemplo o professor dever lembrar que um dos caminhos para encontrar o mdc de dois ou mais números é encontrar todos os divisores de cada um dos números, e através de uma observação, encontrar qual é o maior deles. Nesse caso, tem-se:

D(32) = 1; 2; 4; 8; 16; 32 e
D(56) = 1; 2; 4; 7; 8; 19; 28; 56:

Onde se obtém que os divisores comuns são: 1, 2, 4 e 8, e o maior deles é o 8. Portanto, (32, 56) = 8.

Exercício 4.2.1.5. (algoritmo de Euclides) *Encontrar o máximo divisor comum de 32 e 56 usando o algoritmo de Euclides.*

Solução: Nesse exemplo o professor deve usar a ferramenta do algoritmo de Euclides para mostrar sua aplicabilidade no cálculo do mdc de dois inteiros. De modo que os alunos percebam sua eficiência diante do modo utilizado no exercício anterior.

Primeiro se deve efetuar a divisão de 56 por 32, em que se encontra quociente 1 e resto 24, conforme a tabela abaixo:

	1	
56	32	24
24		

Em seguida é preciso continuar com a divisão de 32 por 24, em que se obtém quociente 1 e resto 8, conforme a tabela abaixo:

	1	1	
56	32	24	8
24	8		

Como ainda não foi encontrado resto 0, é preciso continuar esse processo, agora dividindo 24 por 8, o qual se encontra quociente 3 e resto 0.

	1	1	3	
56	32	24	8	0

24	8	0		

Como o último resto diferente de 0 é o 8, então (32, 56) = 8.

Exercício 4.2.1.6. (mdc e algoritmo de Euclides) *Seu José possui 126 maçãs e 72 laranjas. Ele quer vende-las juntas em uma só embalagem com a mesma quantidade de maçãs e laranjas em cada embalagem. Qual será o maior número possível de maçãs e laranjas que seu José poderá colocar em cada embalagem?*

Solução: Para se encontrar o maior número possível de maçãs e laranjas por embalagem, primeiramente se deve encontrar o mdc de 126 e 72. Usando o algoritmo de Euclides tem-se:

	1	1	3	
126	72	54	18	0
54	18	0		

Como o último resto diferente de 0 é o 18, então (126, 72) = 18. Portanto seu José poderá colocar no máximo 18 maçãs e 18 laranjas por embalagem.

No final da resolução do problema o professor deve chamar atenção para os divisores de 18, pois estes representam as quantidades de maçãs e laranjas que podem colocadas na embalagem de modo a se ter o mesmo número de maçãs e laranjas.

Atividade 4.2.2. *2º encontro – 4 aulas de 50 minutos*

O segundo encontro deve ser iniciado com o conceito de Equação Diofantina Linear, usando como ponto de partida uma equação que possui solução única de modo a motivar os alunos para o tema, em seguida serão abordadas as equações com infinitas soluções, neste momento se deve instigar os alunos a utilizarem o método de tentativa e erro, por fim será mostrado quando uma Equação Diofantina Linear possui solução e como encontrar todas as suas soluções.

Os seguintes exercícios podem ser usados no decorrer das aulas, alguns podem ser usados no final das aulas de modo a avaliar os alunos e para finalizar os conceitos estudados.

Neste segundo encontro pode-se usar o 3º capítulo deste trabalho como referencial teórico.

Exercício 4.2.2.1. (solução única) *Pedro foi a uma loja de roupas e acessórios, ao chegar ele ficou interessado por um modelo de camisa que custa R$ 18,00 e por um modelo de boné que custa R$ 5,00. Pedro decidiu que gastaria todos os R$ 33,00 que havia levado para gastar em compras comprando camisas e bonés de seu gosto. Quantas camisas e bonés Pedro pode comprar de modo a gastar todo o seu dinheiro?*

Solução: 1 camisa e 3 bonés, única solução.

Nesse exemplo o professor deve pedir aos alunos que tentem encontrar a solução para o problema, após alguém encontrar a solução ele deve perguntar se existem soluções diferentes para ajudar os alunos a utilizarem o método da tentativa e erro. O professor deve ainda observar que a equação estudada é a seguinte $18x + 5y = 33$, onde x e y representam, respectivamente, o número de camisas e bonés que Pedro pode comprar.

Exercício 4.2.2.2. (tentativa e erro) Maria deu R$ 20,00 para seus dois filhos comprarem doces que custam R$ 2,00 e R$ 3,00. Quais as possíveis combinações de doces que eles podem comprar gastando todo o dinheiro?

Solução: As possíveis soluções são:

10 doces de R$ 2,00 e 0 doces de R$ 3,00;

7 doces de R$ 2,00 e 2 doces de R$ 3,00;

4 doces de R$ 2,00 e 4 doces de R$ 3,00;

1 doces de R$ 2,00 e 6 doces de R$ 3,00;

O professor deve esperar os alunos encontrarem as possíveis soluções do problema, caso necessário ele pode avisar aos alunos que eles estão lidando com a equação $2x + 3y = 20$, onde x e y representam, respectivamente, o número de doces que custam R$ 2,00 e R$ 3,00 que as crianças podem comprar.

Exercício 4.2.2.3. (tentativa e erro) *Júlia é uma menina muito gulosa, todos os meses ela utiliza R$ 90,00 para comprar bolos ou salgados. Se cada bolo que ela compra custa R$ 6,00 e cada salgado custa R$ 10,00, quais as possibilidades que ela tem de compra?*

Solução: As possíveis soluções são:

15 bolos de R$ 6,00 e 0 salgados de R$ 10,00;

10 bolos de R$ 6,00 e 3 salgados de R$ 10,00;

5 bolos de R$ 6,00 e 6 salgados de R$ 10,00;

0 bolos de R$ 6,00 e 9 salgados de R$ 10,00;

Assim como no exercício anterior o professor deve esperar os alunos encontrarem as possíveis soluções do problema, neste caso ele deve avisar aos alunos que eles estão lidando com a equação $6x + 10y = 90$, onde x e y representam, respectivamente, o número de bolos e salgados.

Exercício 4.2.2.4. (sem solução) De acordo com exercício anterior s*e depois de alguns meses, Júlia passou a utilizar R$ 55,00 para comprar bolos ou salgados, quais as possíveis possibilidades de compra, se os bolos passaram a custar R$ 2,00 e os salgados R$ 4,00?*

Solução: Como citado no enunciado esse problema não possui solução inteira, pois o mdc(2, 4) = 2 e 2 não divide 55, o professor também pode comentar sobre a diferença de paridade entre os membros da igualdade na equação. Pressupõe-se que os alunos ainda não tenham tido contato com tal situação, portanto o professor deve pedir para que seus alunos procurem a solução de tal problema e só após algum aluno perceber a situação do problema ou eles desistirem é que o professor deve interferir utilizando os conceitos adequados.

É após este exercício que o professor deve introduzir a discussão sobre quando uma Equação Diofantina Linear possui ou não solução inteira, e caso possua, como determinar tais soluções.

Exercício 4.2.2.5. *Verificar se as equações abaixo apresentam ou não soluções inteiras.*

a) $3x + 5y = 1$

Solução: A equação possui solução pois $(3, 5) = 1$, e $1 \mid 1$

b) $5a - 10b = 150$

Solução: A equação possui solução pois $(5, 10) = 5$, e $5 \mid 150$

c) $4x + 18y = 9$

Solução: A equação não possui solução, pois $(4, 18) = 2$, e $2 \nmid 9$

Exercício 4.2.2.6. (todas as soluções) *Encontrar todas as soluções inteiras das equações dos exercícios 4.2.2.1, 4.2.2.2, 4.2.2.3.*

Solução: (4.2.2.1) Neste exercício tem-se a equação $18x + 5y = 33$, como $(18, 5) = 1$ e $1|33$, logo a equação possui solução. Usando o algoritmo de Euclides segue que:

	3	1	1	2
18	5	3	2	1
3	2	1	0	

Observando o algoritmo segue que,

$1 = 3 - 1 \cdot 2$

$2 = 5 - 1 \cdot 3$

$3 = 18 - 3 \cdot 5$

Segue que:

$1 = 3 - 1 \cdot 2$

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

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

$1 = 2 \cdot (18 - 3 \cdot 5) - 1 \cdot 5$

$1 = 18 \cdot (2) + 5 \cdot (-7)$

Multiplicando por 33, se obtém:

$$33 = 18 \cdot (66) + 5 \cdot (-231)$$

Logo, a equação possui como solução particular $x_0 = 66$ e $y_0 = -231$. A solução geral é, então, dada por $(x, y) = (66 - 5t, -231 + 18t)$.

No caso do problema 4.2.2.1 é necessário buscar valores positivos para x e y, logo, tem-se que:

$x > 0 \rightarrow 66 - 5t > 0 \rightarrow t < 66/5$

$y > 0 \rightarrow -231 + 18t > 0 \rightarrow t > 231/18$

Analisando as desigualdades se conclui que ocorre solução única, pois, $t = 13$, logo $x = 1$ e $y = 3$.

(4.2.2.2) Neste exercício se obtém a equação $2x + 3y = 20$, como $(2, 3) = 1$ e $1|20$, logo a equação possui solução.

É fácil ver que $1 = 2\cdot(-1) + 3\cdot(1)$, multiplicando a igualdade por 20 tem-se: $20 = 2\cdot(-20) + 3\cdot(20)$

Logo, a equação possui como solução particular $x_0 = -20$ e $y_0 = 20$. A solução geral é, então, dada por $(x, y) = (-20 - 3t, 20 + 2t)$.

No caso do problema 4.2.2.2 é indicado buscar valores não negativos para x e y, logo, segue que:

$x \geq 0 \rightarrow -20 - 3t \geq 0 \rightarrow t \leq -20/3$

$y \geq 0 \rightarrow 20 + 2t \geq 0 \rightarrow t \geq -10$

Analisando as desigualdades se conclui que os possíveis valores de t são: -7, -8, -9, -10. Organizando esses valores em uma tabela se obtém a seguinte situação:

t	-7	-8	-9	-10
x	1	4	7	10
y	6	4	2	0

(4.2.2.3) Neste exercício tem-se a equação $6x + 10y = 90$ que é equivalente a equação $3x + 5y = 45$, como $(3, 5) = 1$ e $1|45$, logo a equação possui solução.

É fácil ver que $1 = 3\cdot(2) + 5\cdot(-1)$, multiplicando a igualdade por 45 segue que: $45 = 3(90) + 5\cdot(-45)$

Logo, a equação possui como solução particular $x_0 = 90$ e $y_0 = -45$. A solução geral é, então, dada por $(x, y) = (90 - 5t, -45 + 3t)$.

No caso do problema 4.2.2.3 também é indicado buscar valores não negativos para x e y, logo, tem-se que:

$x \geq 0 \rightarrow 90 - 5t \geq 0 \rightarrow t \leq 18$
$y \geq 0 \rightarrow -45 + 3t \geq 0 \rightarrow t \geq 15$

Analisando as desigualdades segue que os possíveis valores de t são: 15, 16, 17, 18. Organizando esses valores em uma tabela encontramos a seguinte situação:

t	15	16	17	18
x	15	10	5	0
y	0	3	6	9

Assim se encerra o objetivo principal deste trabalho, uma sequência didática sobre Equações Diofantinas Lineares no ensino básico, caso o leitor procure outras sequências são indicadas as seguintes referências: VANSAN, 2014; RIBEIRO, 2014 E SILVA, 2013.

CAPÍTULO 5

EQUAÇÕES DIOFANTINAS NÃO LINEARES

Saindo da linearidade, neste quinto capítulo serão estudadas algumas Equações Diofantinas não Lineares. Diofanto também se aprofundou no estudo das Equações Diofantinas não Lineares. Como exemplo dessas equações se pode citar a equação $x^n + y^n = z^n$, essa equação não possui soluções não nulas. O matemático francês Pierre de Fermat fez a afirmação que essa equação só possuía solução trivial, essa afirmação ficou conhecida até os dias de hoje como o "*último teorema de Fermat*".

Um fato curioso a respeito de Fermat e seu último teorema, ocorreu quando o matemático afirmou que a equação $x^n + y^n = z^n$ não possuía solução não trivial para n natural com $n > 2$, a curiosidade se dá pelo fato de Fermat não demonstrar tal teorema pois, segundo o próprio Fermat, na folha onde ele fazia tais anotações não possuía espaço disponível para que ele pudesse escrever tal demonstração. Essa demonstração só foi conhecida no dia 23 de junho de 1993, mais de trezentos anos depois de Fermat fazer sua famosa citação, pelo matemático inglês Andrew Wiles, Wiles usou de argumentos muitos complexos para demonstrar um dos problemas mais famosos da matemática na atualidade.

5.1 Ternos Pitagóricos

Pitágoras foi um matemático grego que viveu por volta do século V antes de cristo, hoje muitos o conhecem devido ao seu famoso teorema que é intitulado por "Teorema de Pitágoras", este teorema diz que o quadrado sobre a hipotenusa de um triângulo retângulo é igual a soma dos quadrados sobre os catetos desse mesmo triângulo, após Pitágoras demonstrar esse teorema várias outras demonstrações surgiram.

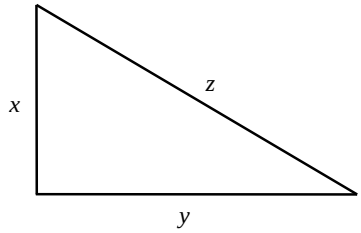

FIGURA 4: Triângulo de Pitágoras. Fonte: Autor.

É possível representar o teorema de Pitágoras pela seguinte equação:

$$x^2 + y^2 = z^2 \qquad \text{(I)}$$

Se um terno de inteiros (x, y, z) satisfaz a equação I, esse terno recebe o nome de terno pitagórico. É fácil perceber que $x = y = z = 0$ é solução de I, também é trivial o caso em que $x = 0$ ou $y = 0$ ou $z = 0$.

Proposição 5.1.1: *(x, y, z) é um terno pitagórico se, e somente se, (kx, ky, kz), com k inteiro não nulo, também o for.*

Demonstração: Se *(x, y, z)* é um terno pitagórico, então $x^2 + y^2 = z^2$, assim multiplicando a igualdade por k^2, segue;

$$k^2(x^2 + y^2) = k^2z^2, \text{ ou seja, } (kx)^2 + (ky)^2 = (kz)^2,$$

o que prova que *(kx, ky, kz)* também é um terno pitagórico.

Reciprocamente se *(kx, ky, kz)* é um terno pitagórico, então $k^2x^2 + k^2y^2 = k^2z^2$, logo multiplicando a igualdade por $1/ k^2$, tem-se;

$$\frac{k^2x^2 + k^2y^2}{k^2} = \frac{k^2z^2}{k^2}, \text{ ou seja, } x^2 + y^2 = z^2,$$

Provando assim que *(x, y, z)* também é um terno pitagórico.

■

Deste modo ao analisar uma solução da equação $x^2 + y^2 = z^2$, é indicado a restrição apenas ao terno pitagórico *(x, y, z)* onde as coordenadas do terno não possuem nenhum fator em comum maior que 1, ou seja, quando x, y e z são primos entre si. Neste caso, se diz que o terno pitagórico é primitivo.

Teorema 5.1.1: *As soluções (x, y, z) primitivas da equação $x^2 + y^2 = z^2$ com x, y, z inteiros não nulos, são dadas por:*

$$(x, y, z) = (2uv, (u^2 – v^2), (u^2 + v^2)) \text{ ou } (x, y, z) = ((u^2 – v^2), 2uv, (u^2 + v^2))$$

Onde u e v são inteiros não nulos, com u > v, mdc(u, v) = 1 e u e v de paridades distintas.

Demonstração: Antes de iniciar a demonstração do teorema serão feitas algumas observações.

Seja *(x, y, z)* um terno pitagórico primitivo, pode-se afirmar que $mdc(x, y) = mdc(x, z) = mdc(y, z) = 1$.

De fato, se p é um primo divisor comum de x e y, então p divide $x \cdot x + y \cdot y = z^2$, ou seja, p divide z^2 e, como p é primo, p divide z. Absurdo, pois *(x, y, z)* é solução primitiva de $x^2 + y^2 = z^2$. Portando $mdc(x, y) = 1$. Do mesmo modo se prova que $mdc(x, z) = mdc(y, z) = 1$.

Como consequência da prova acima, conclui-se que x e y não podem ser ambos pares, nem ambos ímpares. Vejamos:

Como $(x, y) = 1$, segue que x e y não podem ser ambos pares. Agora, se x e y são ambos ímpares, segue que $x = 2a + 1$ e $y = 2b + 1$, com a e b inteiros, então $x^2 + y^2 = (2a + 1)^2 + (2b + 1)^2 = 2 + 4(a + a^2 + b + b^2)$, ou seja, $x^2 + y^2 = z^2$ deixa resto 2 quando dividido por 4. Absurdo, pois z^2 é um quadrado, e todo quadrado deixa resto 0 ou resto 1 quando divisível por 4.

Assim se conclui que se *(x, y, z)* é um terno pitagórico primitivo, exatamente um dos inteiros x ou y é par e z é ímpar. Ao analisar o primeiro caso será assumido, sem perda de generalidade, que x é par (o caso y par é análogo).

Agora, a demonstração do teorema. Iniciaremos escrevendo a equação $x^2 + y^2 = z^2$ da seguinte forma:

$$x^2 = z^2 – y^2 = (z – y) \cdot (z + y) \qquad \text{(I)}$$

Como *x* é par, segue que *z – y* e *z + y* são inteiros pares, assim ambos os membros da igualdade podem ser divididos por 4, e deste modo obtém-se:

$$\left(\frac{1}{2}x\right)^2 = \frac{1}{4}(z+y)\cdot(z-\mathrm{y})$$

Fazendo $m = \frac{1}{2}(z+y)$ e $n = \frac{1}{2}(z-\mathrm{y})$, segue que;

$$\left(\frac{1}{2}x\right)^2 = m\cdot n \quad \text{(II)}$$

Segue de (II) que *m* e *n* são primos entre si, de fato, se *p* é um divisor comum de *m* e *n*, *p* divide *m* + *n* = *z* e *p* divide *m* – *n* = *y*, o que é um absurdo, pois, *mdc*(*y*, *z*) = 1.

Pode-se concluir ainda de (II) e do teorema fundamental da aritmética[7] que *m* e *n* são quadrados perfeitos, uma vez que *mdc*(*m*, *n*) = 1 e *m*·*n* é um quadrado perfeito.

Portanto, existem inteiros positivos *u* e *v*, de modo que $m = u^2$ e $n = v^2$ com *mdc*(*u*, *v*) = 1.

Então $u^2 = m = \frac{1}{2}(z+y)$ e $v^2 = n = \frac{1}{2}(z-\mathrm{y})$ e $u^2\cdot v^2 = \left(\frac{1}{2}x\right)^2$. Assim segue que:

$$x = 2uv,\ y = u^2 - v^2 \text{ e } z = u^2 + v^2$$

Vale ressaltar que *u* e *v,* têm paridades distintas, pois *y* e *z* são ambos ímpares. Se no decorrer da demonstração ao invés de *x* par e *y* ímpar, ocorresse *y* par e x ímpar, ao final da demonstração seria obtida a outra solução do enunciado do teorema.

■

A tabela seguinte mostra parcialmente uma representação dos ternos pitagóricos primitivos com *u* e *v* positivos.

[7] O teorema fundamental da aritmética diz que todo número natural *a* > 1 existem números primos p_1, p_2, ... , p_r, com r > 0, de maneira que $a = p_1 \cdot p_2 \cdot \ldots \cdot p_r$. Além disso se $a = q_1 \cdot q_2 \cdot \ldots \cdot q_s$ com s > 0, onde os q_i são igualmente primos, então r = s e cada q_i é igual a cada p_j.

v \ *u*	2	3	4	5	6	7
1	(4, 3, 5)		(8, 15, 17)		(12, 35, 37)	
2		(12, 5, 13)		(20, 21, 29)		(28, 45, 53)
3			(24, 7, 25)			
4				(40, 9, 41)		(56, 33, 65)
5					(60, 11, 61)	
6						(84, 13, 85)

5.2 Descida Infinita de Fermat

Como visto no tópico anterior, a equação pitagórica $x^2 + y^2 = z^2$ possui uma infinidade de soluções. Porém, existem equações que não possuem solução além da trivial. Veja a proposição a seguir.

Proposição 5.2.1. *A equação $x^2 + y^2 + z^2 = 2xyz$ não tem soluções inteiras não nulas.*

Demonstração: Observando que como o segundo membro da equação é par, logo, é necessário que no primeiro membro da equação, exatamente um dos termos é par ou todos os três termos são pares.

Porém, pode-se supor sem perda de generalidade x par e y, z ímpares, logo se têm que $x^2 + y^2 + z^2$ deixa resto 2 quando dividido por quatro, mas $2xyz$ deixa resto 0 quando dividido por 4, absurdo. Portanto, se conclui que todos os termos do primeiro membro são pares.

Logo, se (x, y, z) satisfaz a equação dada, existem inteiros x_1, y_1 e z_1 tais que $x = 2x_1$, $y = 2y_1$ e $z = 2z_1$, deste modo tem-se que;

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1$$

Usando o mesmo argumento, segue que existem inteiros x_2, y_2 e z_2 tais que $x_1 = 2x_2$, $y_1 = 2y_2$ e $z_1 = 2z_2$, deste modo tem-se que;

$$x_2^2 + y_2^2 + z_2^2 = 8x_2y_2z_2$$

Este argumento pode ser repetido indefinidamente e, assim, se chega a;

$$x = 2x_1 = 2^2x_2 = 2^3x_3 = \cdots = 2^nx_n = \cdots$$

$$y = 2y_1 = 2^2y_2 = 2^3y_3 = \cdots = 2^ny_n = \cdots$$

$$z = 2z_1 = 2^2z_2 = 2^3z_3 = \cdots = 2^nz_n = \cdots$$

Logo, x, y e z são divisíveis por 2^n, para todo inteiro n. Ora, mas isso só é possível se $x = y = z = 0$.

■

Alguns casos não podem ser resolvidos com argumentos simples como o caso anterior. Para ajudar nesses casos, o matemático francês Pierre de Fermat desenvolveu um método que ficou conhecido como *Descida Infinita de Fermat*, esse método será explicado segundo MUNIZ NETO, 2000.

Esquematicamente, consiste na seguinte ideia:

i. Supor que uma dada equação possui uma solução em inteiros não nulos.
ii. Concluir daí que ela possui uma solução em inteiros positivos que seja, em algum sentido, mínima.
iii. Deduzir a existência de uma solução positiva menor que a mínima, chegando a uma contradição.

Proposição 5.2.2. *A equação $3x^2 + y^2 = 2z^2$ não possui soluções inteiras não nulas.*

Demonstração: Supondo que a equação possua uma solução inteira positiva não nula, por exemplo, pode-se supor que o terno *(a, b, c)* seja uma solução, de modo que essa solução seja mínima, ou seja, dentre todas as soluções *(x, y, z)*, com x, y e z inteiros positivos temos que *(x, y, z) = (a, b, c)*, no qual $z = c$ é o menor possível.

Usando a condição acima, é necessário trabalhar em cima da equação $3a^2 + b^2 = 2c^2$. Segue que b é múltiplo de 3. De fato, se b não fosse múltiplo de 3 , seguiria

de $3a^2 + b^2 = 2c^2$ que c também não seria múltiplo de 3. Segue ainda que b^2 deixaria resto 1 quando dividido por 3.

Analisando agora os restos de cada termo da equação quando dividido por 3, observa-se que $3a^2 + b^2$ deixaria resto 1 enquanto $2c^2$ deixaria resto 2. Logo a igualdade $3a^2 + b^2 = 2c^2$ não poderia ocorrer. Portanto b é múltiplo de 3, e consequentemente c também é múltiplo de 3.

Fazendo $b = 3b_1$ e $c = 3c_1$, com b_1 e c_1 inteiros não nulos, e substituindo na equação $3a^2 + b^2 = 2c^2$, segue que;

$$3a^2 + 9b_1^2 = 18c_1^2 \rightarrow a^2 + 3b_1^2 = 6c_1^2$$

Assim concluímos que a também é múltiplo de 3, fazendo $a = 3a_1$, teremos;

$$9a_1^2 + 3b_1^2 = 6c_1^2 \rightarrow 3a_1^2 + b_1^2 = 2c_1^2$$

Logo, (a_1, b_1, c_1) é outra solução da equação $3x^2 + y^2 = 2z^2$, com $c_1 < c$, mas isso é uma contradição contra a minimalidade da solução (a, b, c). Portanto, a equação $3x^2 + y^2 = 2z^2$ não possui soluções não nulas.

■

O método das descidas de Fermat será aproveitado, para se fazer a demonstração de uma parte do último teorema de Fermat, será mostrado que a equação $x^n + y^n = z^n$, onde n é um múltiplo de 4, não possui soluções não inteiras.

Proposição 5.2.3. *A equação $x^n + y^n = z^n$, onde n é um múltiplo de 4, não possui soluções inteiras não nulas.*

Demonstração: Para a demonstração de tal proposição, serão usados alguns conceitos desenvolvidos no tópico anterior.

Seja $n = 4k$, onde k é um número natural. Assim a equação $x^n + y^n = z^n$, equivale a seguinte equação $(x^k)^4 + (y^k)^4 = (z^{2k})^2$, ou seja, (x^k, y^k, z^{2k}) será uma solução da equação $a^4 + b^4 = c^2$. Deste modo, basta mostrar que essa última equação não admite soluções não nulas.

Supondo, por absurdo, que existam inteiros positivos *a*, *b*, *c* tais que $a^4 + b^4 = c^2$. Pode-se também supor, pelo método da descida infinita de Fermat, que *a*, *b* e *c* é solução primitiva, ou seja, foram escolhidos de tal modo que não há outra solução positiva *a',b',c'* com *c'* < *c*. Deste modo, *a* e *b* são primos entre si, e pelo teorema 5.1.1 tem-se a existência de inteiros positivos primos entre si *u* e *v* tais que $a^2 = u^2 - v^2,\ b^2 = 2uv,\ c = u^2 + v^2$. Como $a^2 + v^2 = u^2$, segue novamente do teorema 5.1.1 a existência de inteiros positivos primos entre si *p* e *q* tais que

$$a = p^2 - q^2,\ v = 2pq,\ u = p^2 + q^2.$$ Mas aí $b^2 = 2uv = 4pq(p^2 + q^2)$

Como *p* e *q* são primos entre si, segue que ambos são também primos com $p^2 + q^2$. Portanto, sendo $4pq(p^2 + q^2)$ um quadrado deve-se ter *p*, *q* e $p^2 + q^2$ quadrados, digamos $p = \alpha^2, q = \beta^2, p^2 + q^2 = \gamma^2$, com α, β, γ positivos. Por fim, segue que $\alpha^4 + \beta^4 = \gamma^2$, com $c = u^2 + v^2 > u = p^2 + q^2 = \gamma^2 \geq \gamma$, contrariando a minimalidade de *c*. Logo, não há soluções inteiras não nulas de $x^n + y^n = z^n$ quando *n* for múltiplo de 4.

■

5.3 Equação de PELL

Para a elaboração deste tópico serão utilizadas as referências MUNIZ NETO, 2000, e MIRANDA, 2007.

Se *d* é um inteiro positivo que não é um quadrado perfeito, sabe-se que $\sqrt{d}$ é um número irracional. A equação $x^2 - dy^2 = m$, onde *m* representa um inteiro qualquer, é conhecida como a *Equação de Pell*. Ao analisar as soluções da equação, é fácil perceber que, no caso *m = 0*, a Equação de Pell não tem solução além da trivial (*x = y = 0*), pois, caso contrário, se teria $\sqrt{d} = {}^{x}/_{y}$, o que iria contradizer a irracionalidade de $\sqrt{d}$.

A seguir será feita uma abordagem sobre a determinação das soluções da Equação de Pell para casos com $m \neq 0$.

Proposição 5.3.1. *Dado um número irracional α, existem infinitos racionais* $\frac{p}{q}$*, com p e q inteiros não nulos primos entre si, tais que* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$.

Demonstração: Dado um inteiro positivo *N* qualquer, considere os *N*+1 elementos do intervalo [0, 1) da forma $j_1\alpha - [j\alpha]$, com $0 \leq j \leq N$, onde $[x]$ representa o *maior inteiro que não supera x*. Como [0,1) = $\bigcup_{k=0}^{N-1}\left[\frac{k}{N}, \frac{k+1}{N}\right[$, pelo *Princípio das Gavetas de Dirichlet*[8], existem dois desses elementos, diga-se $j'\alpha - [j'\alpha]$ e $j''\alpha - [j''\alpha]$ pertencentes a um mesmo intervalo $\left[\frac{k}{N}, \frac{k+1}{N}\right[$. Supondo, sem perda de generalidade, que $j' < j''$ e chamando $q = j' - j''$ e $p = [j'\alpha] - [j''\alpha]$, segue que:

$$0 < |q\alpha - p| < \frac{1}{N}, \text{ logo; } \left|\alpha - \frac{p}{q}\right| < \frac{1}{qN} \leq \frac{1}{q^2}$$

É possível supor que *p* e *q* são primos entre si. De fato, se $p = p'c$ e $q = q'c$, para algum inteiro $c>1$, então $\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{q^2} < \frac{1}{q'^2}$.

Para garantir a existência de infinitos tais pares, suponha que foram encontrados *p* e *q* primos entre si e tais que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. Escolhendo agora um natural qualquer *n* tal que $\frac{1}{n} < \left|\alpha - \frac{p}{q}\right|$. Usando o mesmo raciocínio acima, chegamos a um par de inteiros primos entre si *p*', *q*', com $\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{nq'}$ e $q' \leq n$.

Portanto, $\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{nq'} < \left|\alpha - \frac{p}{q}\right|$ e $\left|\alpha - \frac{p'}{q'}\right| < \frac{1}{nq'} \leq \frac{1}{q'^2}$, com $(p', q') \neq (p, q)$

■

Proposição 5.3.2. *Se d é um inteiro positivo que não é um quadrado perfeito, existe um inteiro m tal que a equação* $x^2 - dy^2 = m$ *admite infinitas soluções inteiras.*

Demonstração: Como $\sqrt{d}$ é irracional, segue pela Proposição 1, que existem infinitos pares (*x, y*) de inteiros primos entre si tais que $\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}$. Deste modo, se *x* e *y* são inteiros satisfazendo essa desigualdade, segue que;

[8] Também conhecido por princípio da casa dos pombos, o princípio de Dirichlet pode ser enunciado do seguinte modo: Se tivermos n + 1 pombos para serem colocados em n casas, então pelo menos uma casa deverá conter, pelo menos, dois pombos.

$$|x^2 - dy^2| = \left|x - \sqrt{d}y\right|\left|x + \sqrt{d}y\right| < \frac{1}{y}\left(\left|x - \sqrt{d}y\right| + 2\sqrt{d}y\right) < \frac{1}{y}\left(\frac{1}{y} + 2\sqrt{d}y\right) < 2\sqrt{d} + 1$$

Logo existe algum inteiro não nulo *m* entre $-\left(2\sqrt{d} + 1\right)$ e $2\sqrt{d}$ + 1 que se repete um número infinito de vezes entre os valores de $x^2 - dy^2$, com (*x*, *y*) satisfazendo a condição $\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}$. Mas isto é o mesmo que dizer que a equação $x^2 - dy^2 = m$ admite infinitas soluções.

■

Proposição 5.3.3. *A equação $x^2 – dy^2 = 1$, onde d é um inteiro positivo que não é um quadrado perfeito, admite soluções.*

Demonstração: Conforme a Proposição 5.3.2, pode-se tomar um inteiro não nulo *m* de modo que a equação $x^2 – dy^2 = m$ admite infinitas soluções inteiras. Podemos escolher duas dessas soluções (x_1, y_1) e (x_2, y_2) de modo que $|x_1| \neq |x_2|$, mas $x_1 \equiv x_2$ (mod*m*) e $y \equiv y_2$ (mod*m*). Logo;

$$\left(x_1 + y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right) = (x_1x_2 - dy_1y_2) + \left(x_2y_1 - x_1y_2\sqrt{d}\right) \qquad (i)$$

Porém, $x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv 0$(mod*m*) e $x_2y_1 \equiv x_1y_2$ (mod*m*) e, daí, existem inteiros *u* e *v* tais que $x_1x_2 - dy_1y_2 = mu$ e $x_2y_1 - x_1y_2\sqrt{d} = mv$. Segue, então, de (i) que;

$$\left(x_1 + y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right) = m\left(u + v\sqrt{d}\right), \text{ logo;}$$

$$\left(x_1 - y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right) = m\left(u - v\sqrt{d}\right)$$

Multiplicando, membro a membro, as duas igualdades acima, obtém-se;

$$m^2 = (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = m^2(u^2 - dv^2), \text{ ou seja; } u^2 - dv^2 = 1$$

Assim, a demonstração estará concluída ao mostrar que *u* e *v* não são nulos. De fato, se *u = 0*, teríamos *–dv²* = 1, o que é um absurdo, pois *d* é inteiro positivo. Se *v = 0*, teríamos *u* = 1 ou -1, porém de (i), segue que;

$\left(x_1 + y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right) = \pm m$, logo; $\left(x_1 + y_1\sqrt{d}\right) = \pm\left(x_2 + y_2\sqrt{d}\right)$ e $|x_1| = |x_2|$

O que contraria nossa hipótese sobre as soluções (x_1, y_1) e (x_2, y_2).

■

Proposição 5.3.4. *Se d é um inteiro positivo que não é um quadrado perfeito então existe uma solução (x_0, y_0) da equação $x^2 - dy^2 = 1$, onde x_0 e y_0 são inteiros positivos, de modo que todas as demais soluções (x_n, y_n) dessa equação satisfazem a condição $x_n + y_n\sqrt{d} = \left(x_0 + y_0\sqrt{d}\right)^n$ para algum inteiro n.*

Demonstração: Mais uma vez, teremos uma aplicação do *método da descida infinita de Fermat*. Consideremos a solução (x_0, y_0) da equação dada, com coordenadas inteiras positivas, de modo que, dentre todas as soluções da equação, o valor $\left(x_0 + y_0\sqrt{d}\right)^n$ seja o menor possível.

Vamos identificar cada solução (x, y) da equação com o número $x + y\sqrt{d}$. Pela igualdade $x^2 - dy^2 = \left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right)$ é fácil ver que o produto de duas soluções da equação também é uma solução, no sentido da identificação acima. Vamos mostrar que todas as soluções da equação dada são da forma $\left(x_0 + y_0\sqrt{d}\right)^n$, para algum inteiro n. Suponha que (u, v) seja uma solução da equação em e que $u + v\sqrt{d}$ não seja uma potência com expoente inteiro de $x_0 + y_0\sqrt{d}$. Assim, para algum n, temos;

$$\left(x_0 + y_0\sqrt{d}\right)^n < u + v\sqrt{d} < \left(x_0 + y_0\sqrt{d}\right)^{n+1}$$

Multiplicando cada membro da expressão acima pela solução $\left(x_0 - y_0\sqrt{d}\right)^n$, obtemos;

$$1 < (u + v\sqrt{d})\left(x_0 - y_0\sqrt{d}\right)^n < x_0 + y_0\sqrt{d}$$

O que é um absurdo, pois como o produto de soluções também é solução, logo $(u + v\sqrt{d})\left(x_0 - y_0\sqrt{d}\right)^n$ é uma solução, o que contraria a minimalidade da solução $x_0 + y_0\sqrt{d}$.

Portanto todas as soluções da equação $x^2 - dy^2 = 1$ satisfazem a condição $x_n + y_n\sqrt{d} = \left(x_0 + y_0\sqrt{d}\right)^n$.

■

Conclusão

No decorrer deste trabalho, principalmente nos capítulos 3 e 4, foi possível observar que o tema abordado possui grande importância na educação básica, uma vez que as Equações Diofantinas Lineares possuem uma infinidade de situações problemas que podem ser aplicados na educação básica.

Destaca-se também a importância do primeiro capítulo que aborda o contexto histórico em que a Álgebra Elementar foi desenvolvida, primeiro por esta abordagem nos trazer um rumo norteador para uma compreensão do desenvolvimento da Álgebra, e segundo por este capítulo servir como introdução à Álgebra para futuros leitores que não tenham muito contato com esta parte da matemática.

No que diz respeito à parte educacional, conclui-se que a Sequência didática, abordada no quarto capitulo, tem um forte impacto na questão do ensino das Equações Diofantinas Lineares, pois, como já foi mencionado anteriormente, essas equações e seus métodos de resolução não são abordados com grande ênfase na educação básica, logo se um discente dispõe de tal material, ele poderia rever a questão do ensino das Equações Diofantinas Lineares na educação básica. Não foram investigados os motivos da não abordagem direta das Equações Diofantinas Lineares, pois este não consistia em um dos objetivos deste trabalho.

Por fim, tem-se como ultimo resultado a abordagem no quinto capítulo, do tópico Descida Infinita de Fermat. Este tema veio a aprimorar a parte matemática pura do presente trabalho, já que o método de Fermat é uma importante ferramenta no estudo das soluções de Equações Diofantinas não Lineares.

Espera-se contribuir de forma positiva para um aprimoramento do estudo das Equações Diofantinas e ajudar aos professores interessados a repassar seus conhecimentos sobre essas equações a seus alunos, seja na educação básica ou na educação superior.

Referências Bibliográficas.

BAUMGART, John K. **História da Álgebra** / John K. Baumgart; trad. Hygino H. Domingues. – São Paulo: Atual. 108f. 1992. – (Tópicos de historia da matemática para uso em sala de aula: v, 4)

BOYER, Carl B. **História da matemática**. São Paulo: Editora E. Blucher, 1974.

CAMPOS, Gisele Duardo Maciano. **Equações Diofantinas Lineares**. 2013. 71 f. Dissertação (mestrado) – Universidade Federal de Mato Grosso.

DOMINGUES, Hygino Hugueros. **Fundamentos de Aritmética**. São Paulo: Editora Atual, 1991.

HEFEZ, Abramo. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

MIRANDA, Michelle Crescêncio de. – **Heurísticas e *Equações Diofantinas* –** FAMAT em Revista – nº 9 – 2007. p. 181 à 187. Disponível em: http://www.portal.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/Famat_revista_09_artigo_.10.pdf.

MUNIZ NETO, A. C. – **Equações Diofantinas – EUREKA!** – Sociedade Brasileira de Matemática – nº 7 – 2000.

NASCIMENTO, Natália Medeiros do. **Equações diofantinas e o método das secantes e tangentes de Fermat**. 2014. 45 f. Dissertação (mestrado) – Universidade Federal do Ceará.

RIBEIRO, Rildo. **Equações Diofantinas: uma abordagem para o Ensino Médio**. 2014. 43 f. Dissertação (mestrado) – Universidade de Brasília.

SILVA, Adriano Valeriano Da. **Uso das Equações Diofantinas Lineares no ensino fundamental**. 2013. 74 f. Dissertação (mestrado) – Universidade Federal de Alagoas.

SILVA, Edna Lúcia Da. **Metodologia da pesquisa e elaboração de dissertação**/Edna Lúcia da Silva, Estera Muszkat Menezes. – 3. ed. rev. atual. – Florianópolis: Laboratório de Ensino a Distância da UFSC, 2001. 121p.

SINGH, Simon. **O último teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos** / Simon Singh; tradução de Jorge Luiz Calife. – 9ª ed. Rio de Janeiro: Record, 313f. 2002.

VANSAN, Alexandre Hungaro. **Equações Diofantinas: Um Projeto para a Sala de Aula e o Uso do Geogebra**. 2014. 67 f. Dissertação (mestrado) – Universidade Estadual de Maringá.