UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA AFRO-BRASILEIRA
INSTITUTO DE CIÊNCIAS EXATAS E DA NATUREZA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

DENNIS FREITAS LIMA

EQUAÇÕES DIOFANTINAS E APLICAÇÕES

REDENÇÃO
2021

DENNIS FREITAS LIMA

EQUAÇÕES DIOFANTINAS E APLICAÇÕES

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional da Universidade da Integração Internacional da Lusofonia Afro Brasileira, como parte dos requisitos necessários para a obtenção do título de mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Joserlan Perote da Silva

REDENÇÃO

2021

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Lima, Dennis Freitas.

L696e

Equações Diofantinas e Aplicações / Dennis Freitas Lima. - Redenção, 2022.
106f: il.

Dissertação - Curso de , Mestrado Profissional Em Matemática Em Rede Nacional, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2022.

Orientador: Prof. Dr. Joserlan Perote da Silva.

1. Matemática - Equações Diofantinas. 2. Aplicações. 3. Ensino. I. Título

CE/UF/Dsibiuni CDD 510

DENNIS FREITAS LIMA

EQUAÇÕES DIOFANTINAS E APLICAÇÕES

Dissertação apresentada como requisito para a obtenção do título de Mestre em Matemática, na Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Unilab – Campus Auroras.

Aprovada em: 17 / 12/ 2021.

BANCA EXAMINADORA

Joserlan Perote da Silva

Prof. Dr. Joserlan Perote da Silva (Orientador)
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

João Fco da S. Filho

Prof. Dr. João Francisco da Silva Filho
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Renivaldo Sodré de Sena

Prof. Dr. Renivaldo Sodré de Sena
Instituto Federal do Ceará (IFCE)

Dedico este trabalho às duas mulheres mais importantes da minha vida: minha amada, adorada e estimada mãezinha Maria José, que tudo fez e faz por mim, na tentativa de tornar meu caminho o mais feliz possível; e minha amada, adorada e estimada bebezinha Aila Luz, que é a razão do meu viver, o bem mais precioso que eu tenho em toda minha vida, motivo pelo qual direciono todas minhas forças na tentativa de tornar o caminho dela o mais feliz possível.

AGRADECIMENTOS

Primeiramente a Deus, pois, sem Ele, nós nada seríamos e Dele provém tudo e todos, inclusive, nossos conhecimentos. Sem Vossa permissão, eu nunca conseguiria ter chegado até aqui.

Aos meus pais, por me darem a vida, por me ensinarem, por me criarem, enfim, por sempre estarem ao meu lado em todas as caminhadas, concedendo-me apoio, sustentação, orientação e educação suficientes e adequados em todos os momentos da minha vida.

À minha filha, razão do meu viver e dos meus esforços, direcionamento da minha vida, amor maior, singular e ímpar que possuo. Minha vida é você. E você será sempre minha bebezinha.

Aos meus irmãos, sobrinhos, familiares e amigos, que completam o significado da palavra família e sempre procuram nos entender e ajudar, não somente nas dificuldades, mas em todos os momentos.

Aos meus falecidos avós, principalmente meu avô materno João, meu exemplo de vida, nunca esquecerei nossas conversas e brincadeiras, seus ensinamentos e orientações. Enormes saudades e eternas lembranças.

Ao meu orientador Professor Doutor Joserlan Perote, não só pelas excelentes orientações e sugestões, exercidas pelo seu vasto conhecimento e maturidade matemático, que contribuíram grandiosamente nesta pesquisa, mas pela pessoa que ele é, compreensivo, incentivador, positivo, aconselhador, sempre nos mostrando que somos capazes de conseguir e até mesmo ir além e sempre nos apoiando e parabenizando por cada passo no nosso desenvolvimento.

A todos meus professores, sem exceção, responsáveis não somente pela aquisição e direcionamento do meu conhecimento, mas pelo meu enorme encanto pela matemática, proveniente de suas aulas, ensinamentos, palestras e histórias.

Aos colegas do Profmat, que, apesar da distância, sempre nos mantivemos próximos, sempre nos auxiliamos e hoje somos todos amigos. Sou muito grato pelas horas de estudos coletivos e pelos conhecimentos, reflexões e sugestões compartilhados por todos.

Aos professores participantes da banca examinadora João Francisco da Silva Filho e Renivaldo Sodré de Sena pelo tempo empregado na leitura e avaliação deste trabalho, pelas valiosas colaborações e sugestões sempre no intuito do engradecimento e aprimoramento do mestrando e sua pesquisa.

À Capes, pelo incentivo financeiro dado com a concessão e manutenção da bolsa de estudo, que me auxiliou em todo o processo de desenvolvimento das atividades deste mestrado, principalmente na aquisição de material de estudo e pesquisa e nas despesas das viagens.

“A matemática é o alfabeto com o qual Deus escreveu o universo.” (GALILEU GALILEI)

RESUMO

O presente trabalho é o desenvolvimento de uma pesquisa de revisão bibliográfica sobre as equações diofantinas lineares e quadráticas, as quais possibilitam a resolução de várias situações-problema do cotidiano, além de proporcionar o desenvolvimento do raciocínio lógico e de revisar conceitos matemáticos já ensinados na escola. Este tema se estrutura principalmente em conteúdos pertencentes ao Ensino Fundamental e, portanto, de acesso fácil e completo aos educandos do Ensino Médio, o que justifica seu ensino e o transforma em uma ferramenta contextualizadora e interdisciplinar. Também é mostrado, a aplicação e a importância destas equações nos conjuntos dos números racionais e irracionais, o que possibilita uma melhor compreensão dos números reais comensuráveis, e um novo conceito de máximo divisor comum, denominado máximo divisor comum generalizado, expandindo, com isto, o leque das resoluções de problemas solucionados por estas equações, oferecendo um suporte maior para compreensão dos assuntos associados. A criação, a modelagem e a resolução de diversas situações-problema com aplicação da teoria pesquisada mostra a relevância deste trabalho. Observa-se portanto que é possível e bastante razoável o ensino das equações diofantinas no Ensino Médio, evitando logicamente o rigor matemático e o excesso de formalismos desnecessários neste nível de Ensino, desde que suas aplicações sejam adaptadas ao nível dos educandos, pois elas estabelecem conexões com alguns conteúdos do Ensino Básico, tais como: divisibilidade, máximo divisor comum, mínimo múltiplo comum, equações do primeiro e do segundo graus, função polinomial do primeiro grau, progressão aritmética, geometria plana e analítica, entre outros.

Palavras-chave: Equações Diofantinas. Aplicações. Ensino.

ABSTRACT

The present work is the development of a literature review research on linear and quadratic Diophantine equations, which enable the resolution of various everyday problem-situations, in addition to providing development logical reasoning and reviewing mathematical concepts already taught in school. This theme is structured mainly on contents pertaining to Elementary School and, therefore, of easy and complete access to high school students, which justifies its teaching and transforms it into a contextualizing and interdisciplinary tool. It is also shown, the application and importance of these equations in the sets of rational and irrational numbers, which allows a better understanding of the commensurable real numbers, and a new concept of maximum common divisor, called generalized maximum common divisor, thus expanding the range of problem solving solved by these equations, offering greater support for understanding the associated issues. The creation, modeling and solving of several problem-situations with the application of the researched theory shows the relevance of this work. It is therefore observed that it is possible and quite reasonable to teach Diophantine equations in high school, logically avoiding mathematical rigor and unnecessary formalism at this level of education, provided that their applications are adapted to the level of students, as they establish connections with some contents of Basic Education, such as: divisibility, maximum common divisor, minimum common multiple, first and second degree equations, first degree polynomial function, arithmetic progression, plane and analytical geometry, among others.

Keywords: Diophantine Equations. Applications. Education.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BNCC	Base Nacional Comum Curricular
Capes	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
Enem	Exame Nacional do Ensino Médio
MEC	Ministério da Educação
PCN	Parâmetros Curriculares Nacionais
Profmat	Mestrado Profissional em Matemática em Rede Nacional
Unilab	Universidade da Integração Internacional da Lusofonia Afro-Brasileira

SUMÁRIO

1 INTRODUÇÃO

Neste estudo retratamos alguns conteúdos que nos remetem à Aritmética, como o máximo divisor comum (mdc), destacando uma de suas aplicações, que é um de nossos focos principais, as equações diofantinas lineares, nome este dado como homenagem a Diofanto de Alexandria, matemático grego, considerado o pai da Álgebra.

Apesar de existir vários tipos de equações diofantinas, nos restringimos as equações diofantinas lineares com duas variáveis $aX + bY = c$, com $X, Y \in \mathbb{Z}$, a, b e $c \in \mathbb{Z}$ e a dois tipos de equações diofantinas quadráticas, as equações pitagóricas $x^2 + y^2 = z^2$, com $x, y, z \in \mathbb{N}$ e a equação de Pell $x^2 - ny^2 = 1$, com $x, y \in \mathbb{Z}$ e $n \in \mathbb{N}$ e diferente de um quadrado perfeito.

Realizamos também o estudo sobre equações diofantinas lineares, sendo que, em um primeiro momento, definimos os valores dos coeficientes a e b como pertencentes ao conjunto dos números inteiros e depois ampliamos esses valores de a e b ao conjunto dos números racionais e dos números reais comensuráveis, onde destacamos pares de números irracionais sendo os valores de a e b.

Existem vários modelos e técnicas de resolução para as equações diofantinas. Neste estudo, abordaremos alguns destes. De antemão, algumas ideias que devemos sempre levar em consideração nas resoluções de problemas que envolvem equações diofantinas são: observar as propriedades das constantes inteiras da equação em questão; utilizar desigualdades quando possível, pois estas nos ajudam a reduzir o conjunto solução; pensar em casos particulares, pois estes nos auxiliam na solução geral; e utilizar o mdc e o algoritmo de Euclides para facilitar a resolução.

Sendo assim, formulamos e dividimos nosso trabalho em capítulos, relacionados a seguir com os respectivos conteúdos de forma que se possa contextualizar, propor modelos de resolução e realizar as devidas resoluções em cada situação que vamos apresentar.

No capítulo 2, tratamos de alguns tópicos de Teoria dos Números, como o princípio da indução finita, o princípio da boa ordenação, divisibilidade em números inteiros, máximo divisor comum, onde podemos destacar o algoritmo da divisão de Euclides, que possui inúmeras aplicações práticas e mínimo múltiplo comum (mmc), os quais possuem conceitos preliminares essenciais e necessários para o desenvolvimento das resoluções das equações diofantinas lineares.

No capítulo 3, retratamos um pouco do que se conhece sobre a vida e a obra de Diofanto de Alexandria, com um breve histórico, destacando sua principal obra Aritmética, uma coleção composta de treze livros, seu uso sistemático de símbolos com abreviações para as potências de números e suas relações e também para as operações.

No capítulo 4, abordamos as equações diofantinas propriamente ditas na seguinte sequência: equações diofantinas lineares com duas incógnitas, coeficientes inteiros

e soluções no conjunto dos números inteiros, equações diofantinas lineares com duas incógnitas, coeficientes racionais e soluções no conjunto dos números inteiros, equações diofantinas lineares com duas incógnitas, coeficientes irracionais e soluções no conjunto dos números inteiros; e equações diofantinas quadráticas, com as equações pitagóricas em um primeiro momento e a equação de Pell em um segundo momento. Neste capítulo, podemos observar as condições de solução para cada uma das equações abordadas, bem como os processos para construção das soluções em cada caso e suas aplicações em respectivos exemplos.

Nosso interesse pela Álgebra e Aritmética, foi um dos fatores primordiais para estudarmos as equações diofantinas e suas aplicações. Este trabalho tem como objetivo principal mostrar que as equações diofantinas lineares com duas incógnitas e algumas equações diofantinas quadráticas são conteúdos que podemos abordar, trabalhar e desenvolver durante os três anos do ensino médio, visto que as resoluções de problemas que envolvem estes tipos de equações podem utilizar como base diversos conteúdos que já são tratados durante os ensinos fundamental e médio, tais como, lógica matemática, mdc, mmc, equações e funções polinomiais do primeiro e do segundo graus, progressão aritmética (PA), geometria plana, entre outros.

Para ratificar a motivação do nosso objetivo, temos o fato de que no Exame Nacional do Ensino Médio (Enem) deste corrente ano, uma das questões elencadas no caderno da área de matemática e suas tecnologias foi sobre o assunto equações diofantinas lineares.

Utilizamos a pesquisa bibliográfica como metodologia de investigação do nosso trabalho, visto que a relevância destes conteúdos se apresenta principalmente na modelagem de problemas cotidianos concretos com variáveis discretas indispensável à resolução de equações diofantinas lineares com duas incógnitas e de equações diofantinas quadráticas, o que, mais uma vez, não caracteriza obstáculo aos educandos no ensino médio, pois possibilita e oportuniza novos aprendizados, visto que se exige uma revisão de conteúdos abordados no ensino básico.

2 TEORIA DOS NÚMEROS

Neste capítulo, abordaremos alguns tópicos da teoria dos números, os quais são pré-requisitos a serem utilizados na resolução das equações diofantinas e que servirão como base teórica para o desenvolvimento do estudo das equações diofantinas e para compreensão dos métodos algébricos que fornecem todas as soluções inteiras para estas equações, tomando como norte principalmente as obras de Hefez (2013), (2009) e (2006), Domingues (1991), Alencar Filho (1981), Martinez e et al (2018) e Santos (2007).

2.1 PRINCÍPIO DA INDUÇÃO FINITA

Os números inteiros possuem as operações de adição e de multiplicação bem definidas, com a comutatividade, a associatividade, o elemento neutro, o elemento simétrico e a distributividade multiplicativa com relação à adição se fazendo presentes. Além destas propriedades, o fechamento de $\mathbb{Z}$ e a tricotomia também são observadas nos números inteiros. Mas isto não é suficiente para caracterizar este conjunto numérico. É necessário adicionarmos o Princípio da Boa Ordenação para concluirmos sua caracterização, o qual enunciaremos e demonstraremos no próximo tópico.

Tanto os números racionais não negativos quanto os números reais não negativos possuem quase todas as propriedades dos naturais e dos inteiros, exceto uma propriedade: o Princípio da Indução Finita que vamos enunciá-lo e demonstrá-lo a seguir, pois é um instrumento matemático importantíssimo, demonstrativo da veracidade de sentenças/propriedades para uma sequência de objetos e que, segundo Santos (2007), é uma ferramenta indispensável na demonstração de muitos teoremas.

Teorema 2.1. (Princípio da Indução Finita) *Sejam $A \subset \mathbb{Z}$ e $a \in \mathbb{Z}$ tais que*

- *$a \in A$; e*
- *o conjunto A é fechado com respeito à operação de somar 1 a seus elementos, ou seja, $\forall\ b,\ b \in A \Rightarrow b + 1 \in A$.*

Então, $\{c \in \mathbb{Z}; c \geqslant a\} \subset A$.

Demonstração: Consideremos $A' = \{c \in \mathbb{Z}; c \geqslant a\}$. Agora, suponhamos por absurdo que $A' \not\subset A$. Daí, temos que $A' \setminus A$ não é vazio e todo elemento pertencente a $A' \setminus A$ deve ser maior ou igual a a.

Sendo assim, temos que existe um elemento $d \in A' \setminus A$, com $d > a$, ou seja, $d \in A'$ e $d \notin A$, o que implica em $d - 1 \in A'$ e $d - 1 \in A$.

Agora, temos que, pela hipótese do enunciado, $d \in A$, pois $d = (d-1)+1 \in A$, já que o conjunto A é fechado com respeito à operação de somar 1 a seus elementos, onde chegamos a uma contradição.

Portanto, $A' = \{c \in \mathbb{Z}; c \geqslant a\} \subset A \Rightarrow \{c \in \mathbb{N}; c \geqslant a\} \subset A \subset \mathbb{Z}$. ■

Como variação do Princípio da Indução Finita temos a Segunda Forma do

Princípio da Indução Finita, conhecido também por Princípio da Indução Completa ou Princípio da Indução Forte, que também é muito útil. Utilizamos o Princípio da Indução Forte, quando, ao tentarmos demonstrar alguma sentença ou proposição por indução, na passagem de b para $b+1$, há necessidade de admitirmos que a sentença ou proposição valha não apenas para b, mas valha para todos os números naturais menores do que ou iguais a b.

Seja $P(b)$ uma proposição sobre $A = \{b \in \mathbb{Z}; b \geqslant a,\ a \in \mathbb{Z}\}$. Segue:

$\gg$ se $P(a)$ é verdadeira; e

$\gg$ se para todo c tal que $a \leqslant c$, com $c \in \mathbb{Z}$ vale $P(c) \Rightarrow P(c+1)$;

$\gg$ então para todo $b \in A$, $P(b)$ é verdadeira.

Daí, para provarmos que todo número inteiro b, pertencente ao conjunto A, possui determinada propriedade, podemos utilizar o Princípio da Indução Forte em b, onde devemos:

1) Primeiramente, mostrar que para o valor a, $P(a)$ é verdadeira, que é chamado de base de indução;
2) No segundo momento, supor que para todo c tal que $a \leqslant c$ vale $P(c)$, que é chamado de hipótese de indução;
3) E, por fim, mostrar que para o valor $c+1$, $P(c+1)$ é verdadeira, usando o fato de que para todo c tal que $a \leqslant c$ vale $P(c)$, que é chamado de passo de indução.

De acordo com Martinez e et al (2018, p. 4), ao se verificar a base de indução e o passo de indução conseguimos uma "cadeia de implicações" de modo que $P(b)$ é verdadeira para todo número inteiro $b \geqslant a$.

Do Princípio da Indução Finita, temos o seguinte instrumento utilizado para demonstrar teoremas:

Corolário 2.1. *Seja $a \in \mathbb{Z}$ e $P(b)$ uma sentença/propriedade aberta sobre b. Suponhamos que:*

i) $P(a)$ é verdadeira; e

ii) $\forall b \geqslant a$, com $b \in \mathbb{Z}$, sempre que $P(b)$ for verdadeira, então temos que $P(b+1)$ também é verdadeira.

Então, $P(b)$ é verdadeira $\forall b \geqslant a$.

Demonstração: Seja A um subconjunto de $\mathbb{Z}$ para os quais $P(b)$ é verdadeira, ou seja, $A = \{b \in \mathbb{Z}; P(b)\}$.

Como, pelo Princípio da Indução Finita, temos que por (i), $a \in A$ e, por (ii), $\forall b, b \in A \Rightarrow (b+1) \in A$, então $\{c \in \mathbb{Z}; c \geqslant a\} \subset A$.

Portanto, $P(b)$ é verdadeira $\forall b \geqslant a$. ■

Sendo assim, devemos:

$\ggg$ primeiramente, verificar que a sentença/propriedade vale para o número a_o escolhido (geralmente $a_o = 0$ ou $a_o = 1$, mas há propriedades que começam por $a_o = 2$, $a_o = 3$

ou outro qualquer);

⋙ depois, assumir a hipótese de indução, ou seja, assumir que a sentença/propriedade é verdadeira para algum $a \in \mathbb{N}$; e

⋙ por fim, demonstrar que a sentença/propriedade também vale para $a+1$, sucessor de a.

Se as três condições forem satisfeitas, então a sentença/propriedade vale para qualquer $a \in \mathbb{N}$ tal que $a \geqslant a_o$.

O segredo para a utilização do Príncípio da Indução Finita é, quando chegar no terceiro passo, se utilizar de manipulações algébricas possíveis e cabíveis para encontrar a expressão aceita como verdadeira no passo 2.

Exemplo 2.1. Demonstrar que, para todo inteiro positivo n, a soma dos n primeiros números ímpares resulta em n^2, ou seja,

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Solução: Utilizando o Princípio da Indução Finita, podemos desenvolver os passos que se seguem.

Primeiramente, verificando que o somatório enunciado para o primeiro número ímpar resulta em n^2, isto é, que a propriedade é válida para $n_o = 1$.

$$n = 1 \Rightarrow 1 = 1^2.$$

Agora, supondo a veracidade da sentença descrita no enunciado para algum n, temos que:

$$1 + 3 + 5 + \cdots + (2n-1) = n^2.$$

Por fim, demonstrando que a sentença também é verdadeira se somarmos o próximo número ímpar e observando que, como o último número ímpar representado no somatório foi $(2n-1)$, então o próximo número ímpar será 2 unidades maior, ou seja, $(2n-1+2) = (2n+1)$, obtemos a soma

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1).$$

Como $1 + 3 + 5 + \cdots + (2n-1) = n^2$, suposto acima, então

$$1 + 3 + 5 + \cdots + (2n-1) + (2n+1) = n^2 + (2n+1) = n^2 + 2n + 1.$$

Esta expressão é um trinômio quadrado perfeito. Daí,

$$n^2 + 2n + 1 = (n+1)^2.$$

Logo, a soma dos $(n+1)$ primeiros números ímpares resulta em $(n+1)^2$, como queríamos demonstrar.

Portanto, para todo inteiro positivo n, a soma dos n primeiros números ímpares resulta em n^2. □

Exemplo 2.2. Demonstrar que, para todo inteiro positivo n, a soma das n primeiras potências de 2, começando de 2^0, resulta em $2^n - 1$, ou seja,

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1, \forall n \in \mathbb{Z}_+^*.$$

Solução: Utilizando o Princípio da Indução Finita, podemos desenvolver os passos que se seguem.

Primeiramente, verificando que o somatório enunciado para o primeiro número inteiro positivo resulta em $2^n - 1$, isto é, que a propriedade é válida para $n_o = 1$.

$$n = 1 \Rightarrow 2^{1-1} = 2^1 - 1 \Rightarrow 2^0 = 2 - 1 \Rightarrow 1 = 1.$$

Agora, supondo a veracidade da sentença descrita no enunciado para algum n, temos que:

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1, \forall n \in \mathbb{N}.$$

Por fim, demonstrando que a sentença também é verdadeira se somarmos a próxima potência de 2 e observando que, como a última potência de 2 representada no somatório foi 2^{n-1}, então a próxima será 2 unidades maior no expoente, ou seja, $2^{n-1+1} = 2^n$, obtemos a soma

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} + 2^n.$$

Como $2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, suposto acima, então

$$2^0 + 2^1 + 2^2 + \cdots + 2^{n-1} + 2^n = 2^n - 1 + 2^n = 2 \cdot 2^n - 1 = 2^{n+1} - 1.$$

Logo, a soma das primeiras $(n + 1)$ potências de 2 resulta em $2^{n+1} - 1$, como queríamos demonstrar.

Portanto, para todo inteiro positivo n, a soma das n primeiras potências de 2 resulta em $2^n - 1$. □

2.2 PRINCÍPIO DA BOA ORDENAÇÃO

De acordo com Hefez (2009), temos as definições a seguir.

Definição 2.1. Um conjunto A, subconjunto de $\mathbb{Z}$, é limitado inferiormente quando existe $a \in \mathbb{Z}$ tal que $a \leqslant b$, $\forall b \in A$.

Definição 2.2. $a \in A$ é um menor elemento de A se $a \leqslant b$, $\forall b \in A$ e, acontecendo isto, o número a será chamado de cota inferior de A.

Convencionalmente, tomamos o conjunto vazio, que apesar de não possuir elemento algum, como um conjunto limitado inferiormente, possuindo qualquer número como uma cota inferior.

Notemos aqui que se o conjunto A possui um menor elemento a, então a é único, pois se a e a' são menores elementos de A, temos que $a \leqslant a'$ e $a' \leqslant a$, que, pela tricotomia, implica $a = a'$.

Exemplo 2.3. Os conjuntos $\mathbb{Z}$ e $-\mathbb{N}$ não limitados inferiormente por não possuírem menor elemento.

Exemplo 2.4. O conjunto $\mathbb{N}$ limitado inferiormente por possuir o número 1 como menor elemento, pois $1 \in \mathbb{N}$ e $1 \leqslant n$ $\forall n \in \mathbb{N}$.

O Princípio da Boa Ordenação diz que se A é um subconjunto não vazio de $\mathbb{Z}$

e limitado inferiormente, então A possui um menor elemento.

Com isto, temos, particularmente, que, como todo e qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente por 1, então todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.

Teorema 2.2. (Princípio da Boa Ordenação) *Se A é um subconjunto não vazio de $\mathbb{N}$ e limitado inferiormente, então A possui um menor elemento.*

Demonstração: Primeiramente seja A' um subconjunto não vazio de $\mathbb{N}$ e suponhamos, por absurdo, que A' não seja um conjunto limitado inferiormente, ou seja, não possua um menor elemento.

Consideremos agora o conjunto B, complementar de A' em relação a $\mathbb{N}$. Desejamos aqui mostrar que

$$B = \mathbb{N}.$$

Sendo assim, consideremos também o conjunto

$$I_b = \{c \in \mathbb{N}; c \leqslant b;\ b \in \mathbb{N}\}$$

e a sentença aberta

$$P(b) : I_b \subset B.$$

Daí, temos que, pelo Princípio da Indução Finita, como $1 \leqslant b$ para todo b, então segue-se que $1 \in B$, pois, caso contrário, 1 seria um menor elemento de A', sendo que A' não possui menor elemento de acordo com a suposição feita no início da demonstração. Logo, $P(1)$ é verdadeira.

Suponhamos agora que $P(b)$ seja verdadeira. Se $b + 1 \in A'$, como nenhum elemento de I_b está em A', teríamos $b+1$ sendo um menor elemento de A', o que, novamente pela suposição feita no início da demonstração, não pode ocorrer.

Com isto, $b + 1 \in B$, e, consequentemente,

$$I_{b+1} = I_b \cup (b + 1) \subset B,$$

provando que $\forall b$, $I_b \subset B$. Logo, temos $\mathbb{N} \subset B$ e $B \subset \mathbb{N}$, o que implica, novamente pela tricotomia, $B = \mathbb{N}$. Se $B = \mathbb{N}$, então A' é vazio e isto é uma contradição.

Portanto, se A é um subconjunto não vazio de $\mathbb{N}$ e limitado inferiormente, então A possui um menor elemento. ■

A seguir o Princípio da Boa Ordenação em $\mathbb{Z}$ para um conjunto limitado inferiormente.

Proposição 2.1. *Se A é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então A possui um menor elemento.*

Demonstração: Seja A' um subconjunto não vazio de $\mathbb{Z}$ e suponhamos que A' não seja um conjunto limitado inferiormente, ou seja, não possua um menor elemento.

Como A' é não vazio, analisemos as seguintes possibilidades:

$1^{\mathbf{a}}$) se A' for um conjunto unitário, seu único elemento é seu menor elemento, onde che-

gamos a uma contradição;

$2^{\mathbf{a}}$) se A' possuir uma quantidade finita de elementos, um destes elementos será menor que todos os demais elementos de S, fazendo dele o menor elemento de S, onde chegamos a uma contradição;

$3^{\mathbf{a}}$) se A' possuir apenas infinitos elementos positivos, então A será um subconjunto de $\mathbb{N}$ e todo subconjunto de $\mathbb{N}$ possui um menor elemento, fazendo deste o menor elemento de A', onde chegamos a uma contradição;

$4^{\mathbf{a}}$) se A' possuir apenas infinitos elementos não negativos, então A' terá o elemento 0 como menor de todos os demais elementos de A', fazendo dele o menor elemento de A', onde chegamos a uma contradição;

$5^{\mathbf{a}}$) se A' possuir infinitos elementos positivos, o zero e uma quantidade finita de elementos negativos, então um destes elementos negativos será menor de todos os demais elementos de A', fazendo dele o menor elemento de A', onde chegamos a uma contradição; e

$6^{\mathbf{a}}$) se A' possuir infinitos elementos positivos, o zero e infinitos elementos negativos, então não existirá um elemento negativo menor que todos os demais elementos de A', e, somente neste caso, podemos perceber que A' não possui um menor elemento.

Sendo assim, como, de acordo com a suposição feita no início da demonstração, A' não possui menor elemento, chegamos a várias contradições, excetuando o último item, em todos os itens acima analisados. Podemos notar aqui que neste último item A' não é limitado inferiormente e nos demais itens A' é limitado inferiormente.

Portanto, se A é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então A possui um menor elemento. ■

Agora, de acordo com Hefez (2009), temos as definições a seguir.

Definição 2.3. Um conjunto A, subconjunto de $\mathbb{Z}$, é limitado superiormente quando existe $a \in \mathbb{Z}$ tal que $a \geqslant b$, $\forall b \in A$.

Definição 2.4. $a \in A$ é um maior elemento de A se $a \geqslant b$, $\forall b \in A$ e, acontecendo isto, o número a será chamado de cota superior de A.

Convencionalmente, tomamos o conjunto vazio, que apesar de não possuir elemento algum, como um conjunto limitado superiormente, possuindo qualquer número como cota superior.

Notemos aqui que se o conjunto S possui um maior elemento a, então a é único, pois se a e a' são maiores elementos de S, temos que $a \geqslant a'$ e $a' \geqslant a$, que, pela tricotomia, implica $a = a'$.

Exemplo 2.5. Os conjuntos $\mathbb{Z}_+$ e $\mathbb{N}$ não limitados superiormente por não possuírem maior elemento.

Exemplo 2.6. O conjunto $-\mathbb{N}$ limitado superiormente por possuir o número -1 como

maior elemento, pois $-1 \in -\mathbb{N}$ e $-1 \geqslant n \ \forall n \in -\mathbb{N}$.

A seguir o Princípio da Boa Ordenação em $\mathbb{Z}$ para um conjunto limitado superiormente.

Proposição 2.2. *Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado superiormente, então S possui um maior elemento.*

Demonstração: Suponhamos que a seja uma cota superior de S. Logo $a \geqslant b$, $\forall b \in S$. Consideremos aqui o conjunto $S' = \{c \in \mathbb{Z}; c = a - b, b \in S\}$.

Como S' é não vazio e $c = a - b \geqslant 0$, $\forall b \in S$, S' é limitado inferiormente. Daí, pelo Teorema 2.2, S' possui um menor elemento $c - d$, com $d \in S$. Sendo assim, se existir $e \in S$, então vai existir $c - e \in S'$ e, logo, $c - e \geqslant c - d$ implicando $d \geqslant e$. Logo, temos que $d = maxS$, ou seja, d é um maior elemento de S.

Portanto, se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado superiormente, então S possui um maior elemento. ■

2.3 DIVISIBILIDADE EM NÚMEROS INTEIROS

A divisão de um número inteiro por outro número inteiro sempre é possível seja através da relação de divisibilidade, seja através da divisão euclidiana, e este fato mune os números inteiros de inúmeras propriedades.

> Na Divisão de um inteiro qualquer a por $b = 2$, os possíveis restos são $r = 0$ e $r = 1$. Se $r = 0$, então o inteiro $a = 2q$ é denominado par; e se $r = 1$, então o inteiro $a = 2q + 1$ é denominado ímpar. Observe que $a^2 = (2q)^2 = 4q^2$ ou $a^2 = (2q + 1)^2 = 4(q^2 + q) + 1$, de modo que na divisão do quadrado a^2 de um inteiro qualquer a por 4 o resto é 0 ou 1. (ALENCAR FILHO, 1981, p. 78).

Como sabemos, o conjunto dos números inteiros é denotado por $\mathbb{Z}$ e representado por $\mathbb{Z} = \{..., -4, -3, -2, -1, 0, 1, 2, 3, 4, ...\}$.

Definição 2.5. Dados dois números inteiros a e b, dizemos que a divide b, quando existir $c \in \mathbb{Z}$ tal que $b = c \cdot a$.

Para tal, escrevemos $a \mid b$, não representando operação alguma em $\mathbb{Z}$, nem tampouco uma fração, sendo apenas uma sentença afirmando a veracidade da existência de c tal que $b = c \cdot a$.

A negação desta sentença deve ser representada por $a \nmid b$, ou seja, esta representação nega a existência de c tal que $b = c \cdot a$.

Exemplo 2.7. Temos que $3 \mid 15$, pois existe um número inteiro $a = 5$ tal que $15 = 5 \cdot 3$.

Exemplo 2.8. Temos que $3 \nmid 7$, pois não existe um número inteiro a tal que $7 = a \cdot 3$.

Definição 2.6. Seja $a \in \mathbb{Z}$, com $a \neq 0$. Se a divide b, dizemos que a é um divisor de b, ou b é divisível por a, ou ainda b é um múltiplo de a. Além disto, se $a \mid b$ e $a > 0$, então

a é um divisor positivo de b; se $a \mid b$ e $a < 0$, então a é um divisor negativo de b; e todo inteiro não nulo é um divisor de si mesmo e de 0.

Proposição 2.3. *Seja $a \in \mathbb{Z}$. Temos que:*
i) $1 \mid a$;
ii) $a \mid a$; *e*
iii) $a \mid 0$.

Demonstração: Em (i), existe um número inteiro $b = a$ tal que $a = b \cdot 1 \Rightarrow a = a \cdot 1$. Em (ii), existe um número inteiro $b = 1$ tal que $a = b \cdot a \Rightarrow a = 1 \cdot a$. E, em (iii), existe um número inteiro $b = 0$ tal que $0 = b \cdot a \Rightarrow 0 = 0 \cdot a$.

Portanto, sendo $a \in \mathbb{Z}$, temos que: $1 \mid a$; $a \mid a$; e $a \mid 0$. ■

Proposição 2.4. *Seja $a \in \mathbb{Z}$. Temos que $0 \mid a$ se, e somente se, $a = 0$.*

Demonstração: Primeiramente, se $0 \mid a$, então existe um número inteiro b tal que $a = b \cdot 0$, e, pela proposição anterior, podemos concluir que $a = 0$, pois $0 = b \cdot 0 \Rightarrow a = 0$.

Por outro lado, se $a = 0$, temos que $0 \mid 0$, pois existe infinitos números c tais que $0 = c \cdot 0$.

Portanto, sendo $a \in \mathbb{Z}$, temos que $0 \mid a \Leftrightarrow a = 0$. ■

Observemos aqui que, por definição e pelas proposições acima, $0 \mid 0$ não é uma indefinição e que todo número inteiro divide 0, ou seja, o número 0 possui infinitos divisores.

Proposição 2.5. *Sejam $a, b \in \mathbb{Z}$. Temos que $a \mid b$ se, e somente se, $\mid a \mid$ divide $\mid b \mid$.*

Demonstração: Como $\mid a \mid = \pm a$ divide $\mid b \mid = \pm b$, então
- quando $\mid a \mid = a$ e $\mid b \mid = b$, existe um número inteiro c tal que $b = c \cdot a$;
- quando $\mid a \mid = -a$ e $\mid b \mid = b$, existe um número inteiro c tal que $b = (-c) \cdot (-a)$;
- quando $\mid a \mid = a$ e $\mid b \mid = -b$, existe um número inteiro c tal que $-b = (-c) \cdot a$; e
- quando $\mid a \mid = -a$ e $\mid b \mid = -b$, existe um número inteiro c tal que $-b = (-c) \cdot (-a)$.

Portanto, sendo $a, b \in \mathbb{Z}$, temos que $a \mid b$ se, e somente se, $\mid a \mid$ divide $\mid b \mid$. ■

Observemos aqui que, por definição e pelas proposições acima, fica definido que todo e qualquer número inteiro a é divisível por ± 1 e por $\pm a$.

Proposição 2.6. *Sejam $a, b \in \mathbb{Z}$. Temos que se $a \mid b$ e $b \mid c$ então $a \mid c$.*

Demonstração: Se $a \mid b$ e $b \mid c$, então existem $d, e \in \mathbb{Z}$ tais que $b = d \cdot a$ e $c = e \cdot b$.

Agora, substituindo b da primeira na segunda equação, temos que:

$$c = e \cdot b \Leftrightarrow c = e \cdot d \cdot a \Leftrightarrow c = (d \cdot e) \cdot a \Leftrightarrow c = f \cdot a,$$

ou seja, existe um número inteiro $f = d \cdot e$ tal que $c = f \cdot a$. Logo, $a \mid c$.

Portanto, sendo $a, b \in \mathbb{Z}$, temos que se $a \mid b$ e $b \mid c$ então $a \mid c$. ■

Exemplo 2.9. Como $3 \mid 6$ e $6 \mid 12$, então $3 \mid 12$.

Proposição 2.7. *Sejam $a, b, c, d \in \mathbb{Z}$. Temos que se $a \mid b$ e $c \mid d$ então $ac \mid bd$.*

Demonstração: Se $a \mid b$ e $c \mid d$, então existem $e, f \in \mathbb{Z}$ tais que $b = e \cdot a$ e $d = f \cdot c$. Daí, temos que

$$b \cdot d = e \cdot a \ \cdot \ f \cdot c \Rightarrow \ b \cdot d = (e \cdot f) \cdot a \cdot c.$$

Logo $a \cdot c \mid b \cdot d$.

Portanto, sendo $a, b, c, d \in \mathbb{Z}$, temos que se $a \mid b$ e $c \mid d$ então $ac \mid bd$. ■

Proposição 2.8. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid (b \pm c)$. Então temos que $a \mid b \Leftrightarrow a \mid c$.*

Demonstração: Primeiramente, suponhamos que $a \mid (b + c)$, então existe $d \in \mathbb{Z}$ tal que $b + c = d \cdot a$. Se $a \mid b$, então temos que existe $e \in \mathbb{Z}$ tal que $b = e \cdot a$. Substituindo a segunda equação na primeira, obtemos

$$b + c = d \cdot a \Rightarrow e \cdot a + c = d \cdot a \Rightarrow c = (d - e) \cdot a.$$

Logo $a \mid c$.

Suponhamos agora que $a \mid (b - c)$, então existe $f \in \mathbb{Z}$ tal que $b - c = f \cdot a$. Se $a \mid b$, então temos que existe $g \in \mathbb{Z}$ tal que $b = g \cdot a$. Substituindo a segunda equação na primeira, obtemos

$$b - c = f \cdot a \Rightarrow g \cdot a - c = f \cdot a \Rightarrow c = (g - f) \cdot a.$$

Logo $a \mid c$.

Por outro lado, suponhamos novamente que $a \mid (b + c)$, então existe $h \in \mathbb{Z}$ tal que $b + c = h \cdot a$. Se $a \mid c$, então temos que existe $i \in \mathbb{Z}$ tal que $c = i \cdot a$. Substituindo a segunda equação na primeira, obtemos

$$b + c = h \cdot a \Rightarrow b + i \cdot a = h \cdot a \Rightarrow b = (h - i) \cdot a.$$

Logo $a \mid b$.

Suponhamos agora que $a \mid (b - c)$, então existe $j \in \mathbb{Z}$ tal que $b - c = j \cdot a$. Se $a \mid c$, então temos que existe $k \in \mathbb{Z}$ tal que $c = k \cdot a$. Substituindo a segunda equação na primeira, obtemos

$$b - c = j \cdot a \Rightarrow b - k \cdot a = j \cdot a \Rightarrow b = (j + k) \cdot a.$$

Logo $a \mid b$.

Portanto, sendo $a, b, c \in \mathbb{Z}$ tais que $a \mid (b \pm c)$, então temos que $a \mid b \Leftrightarrow a \mid c$. ■

Proposição 2.9. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$. Então temos que, para todo $d, e \in \mathbb{Z}$, $a \mid (d \cdot b + e \cdot c)$.*

Demonstração: Como $a \mid b$ e $a \mid c$, então temos que existe $f, g \in \mathbb{Z}$ tais que $b = f \cdot a$ e $c = g \cdot a$.

Daí, temos que

$$d \cdot b + e \cdot c = d \cdot (f \cdot a) + e \cdot (g \cdot a) \Rightarrow$$
$$d \cdot b + e \cdot c = (d \cdot f) \cdot a + (e \cdot g) \cdot a \Rightarrow$$
$$d \cdot b + e \cdot c = (d \cdot f + e \cdot g) \cdot a.$$

Logo $a \mid (d \cdot b + e \cdot c)$.

Portanto, sendo $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$, então temos que, para todo

$d, e \in \mathbb{Z}$, $a \mid (d \cdot b + e \cdot c)$. ■

Definição 2.7. Combinação linear é um somatório de múltiplos de um conjunto de objetos, ou seja, é uma expressão algébrica formada a partir de um conjunto de objetos, onde efetuamos a multiplicação de cada objeto por uma respectiva constante.

Toda combinação linear tem a seguinte forma:

$$a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 + ...,$$

com a_i sendo as constantes, x_i, sendo os objetos e $i \in \mathbb{N} \cup \{0\}$.

Exemplo 2.10. Temos que $2a + 3b$ e $-3a + 5b$ são combinações lineares de a e b, pois são expressões da forma $c \cdot a + d \cdot b$, onde c e d são constantes e a e b são os objetos.

Observemos aqui que a Proposição 2.9 nos afirma que sendo $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $a \mid c$, então a divide qualquer combinação linear de b e c, ou seja, a divide qualquer adição de múltiplos de b e de c.

Teorema 2.3. (Algoritmo da Divisão Euclidiana) *Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem dois números inteiros únicos q e r que satisfazem a equação*

$$a = b \cdot q + r, \ \textit{com } 0 \leqslant r <\mid b \mid .$$

Demonstração: Primeiramente, para provarmos a existência de q e r, consideremos aqui o conjunto $A = \{c \in \mathbb{Z}; c = a - b \cdot d; d \in \mathbb{Z}\} \cap \{\mathbb{N} \cup \{0\}\}$.

Agora, pela construção do conjunto A, existe $e \in \mathbb{Z}$ tal que

$$e \cdot (-b) > -a \ \Rightarrow \ a - b \cdot e > 0,$$

demonstrando, com isto, que $A \neq \emptyset$.

Como A é limitado inferiormente por 0 ou por algum número natural, então, pelo Princípio da Boa Ordenação, temos que A possui um menor elemento r, que iremos supor $r = a - b \cdot q$. Como $r \in A$, então $r \geqslant 0$. Supondo agora, por absurdo, que $r \geqslant \mid b \mid$, temos que existe $f \in \mathbb{N} \cup \{0\}$ tal que

$$r = \mid b \mid + f \ \Rightarrow \ 0 \leqslant f < r,$$

onde chegamos a uma contradição, pois r é o menor elemento de A e

$$r = a - b \cdot q \Rightarrow \mid b \mid + f = a - b \cdot q \Rightarrow f = a - b \cdot q - \mid b \mid \Rightarrow f = a - b \cdot (q \pm 1) \in A,$$

com $f < r$.

Portanto, dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem dois números inteiros q e r que satisfazem a equação $a = b \cdot q + r$, com $0 \leqslant r <\mid b \mid$.

Agora, para provarmos a unicidade de q e r, suponhamos que existam inteiros q_1, q_2, r_1, r_2, com $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, $q_1 \neq q_2$, $r_1 \neq r_2$, $0 \leqslant r_1 <\mid b \mid$ e $0 \leqslant r_2 <\mid b \mid$.

Desta forma, temos que

$$-\mid b \mid < -r_2 \leqslant r_1 - r_2 \leqslant r_1 <\mid b \mid .$$

Isto implica $r_1 - r_2 <\mid b \mid$.

Agora, de $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$, temos que

$$b \cdot q_1 - b \cdot q_2 = r_2 - r_1 \Rightarrow \mid b \mid \cdot \mid q_1 - q_2 \mid = \mid r_1 - r_2 \mid <\mid b \mid .$$

Notemos aqui que esta afirmação somente é possível e verdadeira se tivermos as igualdades $q_1 = q_2$ e $r_1 = r_2$.

Portanto, dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem dois números inteiros únicos q e r que satisfazem a equação $a = b \cdot q + r$, com $0 \leqslant r <\mid b \mid$. ■

Na equação $a = q \cdot b + r$, com $0 \leqslant r < b$, os inteiros, q e r são chamados respectivamente de quociente e resto da divisão de a por b, valendo lembrar aqui que b somente é divisor de a se $r = 0$. Neste caso, temos que $a = b \cdot q$ e o quociente q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$ ou a/b.

Exemplo 2.11. Sabendo-se que na divisão de 322 por $b > 0$, o quociente é 12 e o resto é r, como determinar os possíveis valores de b e r?

Solução: Sabemos que $a = bq + r; 0 \leqslant r < b$. Assim, substituindo os valores dados no enunciado, obtemos:

$$322 = 12b + r; 0 \leqslant r < b \Rightarrow r = 322 - 12b.$$

Logo,

$$0 \leqslant r < b \Rightarrow 0 \leqslant 322 - 12b < b.$$

Resolvendo esta desigualdade simultânea temos:

1°) $0 \leqslant 322 - 12b \Rightarrow 12b \leqslant 322 \Rightarrow b \leqslant 26,8333...$; e

2°) $322 - 12b < b \Rightarrow 322 < 13b \Rightarrow b > 24,76$.

Logo, como $b \in \mathbb{N}$ e $r \in \mathbb{N} \cup \{0\}$, então os possíveis valores para b e r são:

1) quando $b = 26 \Rightarrow r = 322 - 12 \cdot b \Rightarrow r = 322 - 12 \cdot 26 \Rightarrow r = 322 - 312 \Rightarrow r = 10$; ou

2) quando $b = 25 \Rightarrow r = 322 - 12 \cdot b \Rightarrow r = 322 - 12 \cdot 25 \Rightarrow r = 322 - 300 \Rightarrow r = 22$.

Portanto, quando $b = 26 \Rightarrow r = 10$ e $b = 25 \Rightarrow r = 22$. □

A equação $322 = 12b + r$ vista acima é um exemplo de equação diofantina linear com duas variáveis, do tipo $ax + by = c$ que será abordada mais adiante neste trabalho, onde serão tratrados também outros modelos de resolução para tal.

Corolário 2.2. *Dados $a, b \in \mathbb{Z}$, com $b > 0$, existe um número inteiro único q tal que*

$$qb \leqslant a < (q + 1)b.$$

Demonstração: Pela Divisão Euclidiana, temos que existem $q, r \in \mathbb{Z}$, com $0 \leqslant r < b$, univocamente determinados, tais que $a = b \cdot q + r \Rightarrow r = a - b \cdot q$. Daí, temos que

$$0 \leqslant r < b \text{ e } r = a - b \cdot q \Rightarrow 0 \leqslant a - b \cdot q < b.$$

Somando-se $b \cdot q$ aos três membros da desigualdade, obtemos

$$0 + b \cdot q \leqslant a - b \cdot q + b \cdot q < b + b \cdot q \Rightarrow b \cdot q \leqslant a < b \cdot (1 + q).$$

Portanto, dados $a, b \in \mathbb{Z}$, com $b > 0$, existe um número inteiro único q tal que $qb \leqslant a < (q + 1)b$. ■

Exemplo 2.12. Dados $a = 45$ e $b = 4$. Verifique se a é um múltiplo de b ou não. Caso não seja, determine também os múltiplos consecutivos de 4 entre os quais a se situa.

Solução: Como não existe algum inteiro q da forma $45 = 4 \cdot q$, então podemos concluir que 45 não é múltiplo de 4, ou seja, a não é um múltiplo de b.

Assim, como sabemos que $44 = 4 \cdot (11)$, $a = 45 = 4 \cdot (11) + 1$ e $48 = 4 \cdot (12)$, então temos $4 \cdot (11) < 4 \cdot (11) + 1 = 45 = a < 4 \cdot (12)$.

Portanto, $a = 45$ não é múltiplo de 4 e os múltiplos consecutivos de 4 entre os quais $a = 45$ se situa são $44 = 4 \cdot 11$ e $48 = 4 \cdot 12$. □

2.4 MÁXIMO DIVISOR COMUM

Falaremos agora sobre o máximo divisor comum (*mdc*) de dois números inteiros. Na educação, é impressionante como o assunto *mdc*, que apresenta várias aplicações importantes no ambiente matemático da Teoria dos Números, é pouco visto, trabalhado e desenvolvido no Ensino Fundamental e no Ensino Médio.

De acordo com o Ministério da Educação (BRASIL, 1998b), os Parâmetros Curriculares Nacionais (PCN) do 6° ao 9° ano do Ensino Fundamental, mostram que, nos ciclos finais do Ensino Fundamental, alguns aspectos relacionados ao estudo dos números naturais são abordados e desenvolvidos de forma a comprometer a aprendizagem dos educandos, tais como a ausência de certas situações-problema e o excesso de cálculos para a obtenção do *mdc* sem que se perceba a compreensão de conceitos e relações que possibilitem a ampliação do entendimento sobre os números.

> No Ensino Fundamental – Anos Finais, os estudos de Álgebra retomam, aprofundam e ampliam o que foi trabalhado no Ensino Fundamental – Anos Iniciais. Nessa fase, os alunos devem compreender os diferentes significados das variáveis numéricas em uma expressão, estabelecer uma generalização de uma propriedade, investigar a regularidade de uma sequência numérica, indicar um valor desconhecido em uma sentença algébrica e estabelecer a variação entre duas grandezas. É necessário, portanto, que os alunos estabeleçam conexões entre variável e função e entre incógnita e equação. As técnicas de resolução de equações e inequações, inclusive no plano cartesiano, devem ser desenvolvidas como uma maneira de representar e resolver determinados tipos de problema, e não como objetos de estudo em si mesmos. (BRASIL, 2018a, p. 270-271).

O MEC, através do PCN acima citado, conclui que para consolidar a aprendizagem é imprescindível o desenvolvimento, ao longo dos ciclos finais do Ensino Fundamental, de um trabalho sistemático sobre os números naturais de forma que se possa analisar as diferentes ordens de grandeza e posição e possa interpretar as variadas formas de representação.

De acordo com BNCC (BRASIL, 2018a, p. 527), "os estudantes têm também a oportunidade de desenvolver o pensamento algébrico, tendo em vista as demandas para identificar a relação de dependência entre duas grandezas em contextos significativos e comunicá-la, utilizando diferentes escritas algébricas, além de resolver situações-problema por meio de equações e inequações."

Posto isto inicialmente, lembremos aqui que obtemos os números divisores quando ao dividirmos um número por este divisor chegamos a um quociente igual a um número inteiro e a um resto igual a zero, ou seja, um número é chamado de divisor quando a divisão de um número por ele tem como resultado um número inteiro e zero como resto. Observemos também que quando obtemos como resto de uma divisão o valor zero chamamos esta divisão de exata.

Definição 2.8. Dados os números $a, b \in \mathbb{Z}$, dizemos que b é divisor de a, quando $b \mid a$.

Exemplo 2.13. O número 16 possui divisão exata por ± 1, ± 2, ± 4, ± 8 e ± 16. Com isto, temos que ± 1, ± 2, ± 4, ± 8 e ± 16 são divisores de 16.

Exemplo 2.14. O número 36 possui divisão exata por ± 1, ± 2, ± 3, ± 4, ± 6, ± 9, ± 12, ± 18 e ± 36. Com isto, temos que ± 1, ± 2, ± 3, ± 4, ± 6, ± 9, ± 12, ± 18 e ± 36 são divisores de 36.

Definição 2.9. Dados os números $a, b, c \in \mathbb{Z}$, dizemos que c é divisor comum de a e b, quando $c \mid a$ e $c \mid b$ simultaneamente.

Exemplo 2.15. Os divisores de 16 são ± 1, ± 2, ± 4, ± 8 e ± 16 e os divisores de 36 são ± 1, ± 2, ± 3, ± 4, ± 6, ± 9, ± 12, ± 18 e ± 36. Temos que ± 1, ± 2 e ± 4 são divisores comuns de 16 e 36.

De acordo com Milies e Coelho (2001), temos a definição a seguir.

Definição 2.10. Dados os números $a, b \in \mathbb{Z}$ não nulos, chamamos de $mdc(a, b)$ o maior de seus divisores comuns, ou seja,

$$mdc(a, b) = max\ D(a, b),$$

com $D(a, b)$ sendo o conjunto dos divisores comuns de a e de b.

O máximo divisor comum pode ser denotado por $(a, b) = d$ ou $mdc(a, b) = d$ ou ainda $MDC(a, b) = d$. Utilizaremos como forma de representação a sigla minúscula seguida de dois números entre parênteses $mdc(a, b) = d$, com $a, b, d \in \mathbb{Z}$ e $a \neq 0$ ou $b \neq 0$), significando que o valor depois da igualdade d é o máximo divisor comum dos dois números entre parênteses a e b.

O mdc é uma ferramenta matemática utilizada para facilitar a resolução de problemas e equações e está associada aos divisores comuns de dois ou mais números, sendo o maior número que pode dividir vários números ao mesmo tempo.

Com isto, o $mdc(a, b)$ corresponde ao maior número que divide a e b, ou seja, o maior divisor cuja divisão tanto por a quanto por b é exata.

Exemplo 2.16. Os divisores comuns de 16 e 36 são ± 1, ± 2 e ± 4. Temos que

$$mdc(16, 36) = 4.$$

O $mdc(16, 36)$ corresponde ao maior número inteiro que divide 16 e 36 ao mesmo tempo, ou seja, o maior divisor cuja divisão tanto de 16 e de 36 por ele é exata, ou

ainda, o maior número que seja divisor de 16 e de 36 simultaneamente. Portanto, ao olharmos para os divisores comuns de 16 e por 36 listados acima, temos que o $mdc(16, 36) = 4$.

Segundo Hefez (2013), (2009) e (2006, p.86), podemos afirmar que um número $d \geqslant 0$ é $mdc(a, b)$, com $a, b, d \in \mathbb{Z}$ se d é um divisor comum de a e b e se d é divisível por todos os divisores comuns de a e b.

De acordo com Martinez e et al (2018, p.18), quando $a = b = 0$, então convencionamos que $mdc(a, b) = mdc(0, 0) = 0$ e quando $mdc(a, b) = 1$, então chamamos a e b de coprimos (primos entre si ou relativamente primos).

Para Domingues (1991, p.44), quando $mdc(a, b) = mdc(0, 0) = 0$, temos que "o mdc não é o maior dos divisores comuns, pois $1 \mid 0$, $2 \mid 0$, $3 \mid 0$, $\cdots$, não existindo um maior divisor comum para 0 e 0".

Como propriedades do $mdc(a, b)$, temos as seguintes afirmações (decorrentes das definições e das proposições da seção anterior e desta seção):

i) $mdc(a, 0) =\mid a \mid$;

ii) $mdc(a, 1) = 1$;

iii) $mdc(a, b) = mdc(b, a)$;

iv) $mdc(a, a) =\mid a \mid$;

v) se a divide b, então $mdc(a, b) =\mid a \mid$;

vi) $mdc(-a, -b) = mdc(-a, b) = mdc(a, -b) = mdc(a, b)$;

vii) $mdc(a, b) = mdc(a - b, b)$;

viii) $mdc(a, b) = 1 \Rightarrow mdc(a, b^2) = 1$, $mdc(a^2, b) = 1$ e $mdc(a^2, b^2) = 1$.

Exemplo 2.17. De acordo com a propriedade (v), o $mdc(-3, 0) = \mid -3 \mid = 3$ e o $mdc(-6, 12) =\mid -6 \mid= 6$.

A propriedade (vi) do máximo divisor comum desta lista acima nos permite supor sem perda de generalidade que $a \geq b \geq 0$.

Na propriedade (vii), devemos ter o conjunto $D(a, b)$ (divisores comuns de a e b) igual ao conjunto $D(a - b, b)$ (divisores comuns de $a - b$ e b), para que a igualdade $mdc(a, b) = mdc(a - b, b)$ seja verdadeira e, com isto, observamos que estando um destes conjuntos bem definido, o outro também estará.

Sendo assim, para $b = 0$ ambos conjuntos estão bem definidos com $a \neq 0$, fazendo os dois conjuntos iguais; e para $b \neq 0$ ambos conjuntos também estão bem definidos. Pois vejamos que se $d \in D(a, b)$, então $d \mid a$ e $d \mid \pm b$. Assim,

$$d \mid a = a - b + b = (a - b) + b \Rightarrow d \mid (a - b).$$

Por outro lado e reciprocamente, se $d \in D(a - b, b)$, então $d \mid (a - b)$ e $d \mid b$. Logo,

$$d \mid (a - b) + b = a - b + b \Rightarrow d \mid a,$$

ou seja, $d \in D(a, b)$.

Na propriedade $(viii)$, temos que como $mdc(a, b) = 1$, ou seja, $a \nmid b$ e $b \nmid a$,

então:

$\rightsquigarrow$ $mdc(a, b^2) = mdc(a, b \cdot b) = mdc(a, b) = 1$;

$\rightsquigarrow$ $mdc(a^2, b) = mdc(a \cdot a, b) = mdc(a, b) = 1$; e

$\rightsquigarrow$ $mdc(a^2, b^2) = mdc(a \cdot a, b \cdot b) = mdc(a, b) = 1$.

Para se determinar os divisores de um número inteiro qualquer temos uma lista de critérios de divisibilidade que nos auxiliam e que, de acordo com Santos (2007, p.20), são basicamente aplicações da Proposição 2.9.

Uma outra forma de se determinar o *mdc* é através da decomposição dos números em fatores primos.

Exemplo 2.18. O número 16 pode ser escrito na forma por $16 = 2 \cdot 2 \cdot 2 \cdot 2$ e o número 36 pode ser escrito na forma $36 = 2 \cdot 2 \cdot 3 \cdot 3$. Daí, observamos os fatores comuns nas decomposições realizadas e o *mdc* é o valor da multiplicação destes números comuns. E, novamente, temos que, neste caso, existe um único fator comum nas duas decomposições realizadas é o número 2, porém este se repete simultaneamente duas vezes. Logo, o $mdc(16, 36) = 2 \cdot 2 = 4$. Portanto, o $mdc(16, 36) = 4$.

Podemos também verificar e utilizar o fator (divisor) comum com seu respectivo menor expoente para determinar o *mdc* de dois números inteiros. Observemos, no exemplo acima, que $16 = 2^4$ e $36 = 2^2 \cdot 3^2$. Então, o $mdc(16, 36) = 2^2 = 4$.

Exemplo 2.19. O número 20 pode ser escrito na forma por $20 = 2 \cdot 2 \cdot 5 = 2^2 \cdot 5$ e o número 50 pode ser escrito na forma $50 = 2 \cdot 5 \cdot 5 = 2 \cdot 5^2$. Daí, observamos os fatores comuns nas decomposições realizadas e temos que, neste caso, os fatores comuns nas duas decomposições realizadas são os números 2 e 5. Portanto, como o *mdc* é o valor da multiplicação destes fatores comuns com seus respectivos menores expoentes, o $mdc(20, 50) = 2 \cdot 5 = 10$.

Em seu livro Os Elementos, Livro VII, Proposição 2, Euclides demonstra a existência do $mdc(a, b)$, com $a, b \in \mathbb{N}$, sendo que ele se utiliza do resultado do lema abaixo enunciado e demonstrado.

Lema 2.1. *Sejam $a, b, c \in \mathbb{Z}$. Se existe $mdc(a, b - c \cdot a)$, então também existe $mdc(a, b)$, com $mdc(a, b) = mdc(a, b - c \cdot a)$.*

Demonstração: Seja $d = mdc(a, b - c \cdot a)$. Como $d \mid a$ e $d \mid (b - c \cdot a)$, então, pela Proposição 2.8, temos que $d \mid b$, fazendo de d um divisor comum de a e b.

Supondo e também um divisor comum de a e b, logo e também é um divisor comum de a e $b - c \cdot a$ e, ainda, $e \mid d$, demonstrando que $d = mdc(a, b)$. Com isto, temos que $d = mdc(a, b - c \cdot a)$ e $d = mdc(a, b)$.

Portanto, sendo $a, b, c \in \mathbb{Z}$, se existe $mdc(a, b - c \cdot a)$, então também existe $mdc(a, b)$, com $mdc(a, b) = mdc(a, b - c \cdot a)$. ■

Exemplo 2.20. Dados $a \in \mathbb{Z}$, com $a \neq 1$ e $m \in \mathbb{N}$, prove que

$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc(a-1, m).$$

Solução: Primeiramente para $m = 1$, temos que

$$1 = 1 \Rightarrow$$
$$mdc\,(1, a-1) = mdc(a-1, 1) \Rightarrow$$
$$mdc\left(\frac{a-1}{a-1}, a-1\right) = mdc(a-1, 1) \Rightarrow$$
$$mdc\left(\frac{a^1-1}{a-1}, a-1\right) = mdc(a-1, 1) \Rightarrow$$
$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc(a-1, m).$$

Agora, suponhamos que $m \geqslant 2$. Deste modo, temos que

$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc\left(a^{m-1} + a^{m-2} + ... + a + 1, a-1\right) \Rightarrow$$
$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc\left((a^{m-1}-1) + (a^{m-2}-1) + ... + (a-1) + m, a-1\right).$$

De acordo com Hefez (2013, p. 49), temos que

$$a-1 \mid \left[(a^{m-1}-1) + (a^{m-2}-1) + ... + (a-1)\right].$$

Como $(a^{m-1}-1) + (a^{m-2}-1) + ... + (a-1) = b \cdot (a-1)$ para algum $b \in \mathbb{N}$, então, pelo Lema 2.1, temos que

$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc\,(b \cdot (a-1) + m, a-1)$$
$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc\,(a-1, b \cdot (a-1) + m)$$
$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc\,(a-1, m).$$

Portanto, dados $a \in \mathbb{Z}$, com $a \neq 1$ e $m \in \mathbb{N}$, temos que

$$mdc\left(\frac{a^m-1}{a-1}, a-1\right) = mdc(a-1, m). \qquad \square$$

Proposição 2.10. (Algoritmo de Euclides) *Dados $a, b \in \mathbb{N}$, então o $mdc(a, b)$ sempre existe.*

Demonstração: Dados $a, b \in \mathbb{N}$, suponhamos, sem perda de generalidade, que $b \leqslant a$. Analisando quatro casos, temos que:

1°) Se $b = 1$, então $mdc(a, b) = mdc(a, 1) = 1$, o que determina a existência do $mdc(a, b)$;

2°) Se $b = a$, então $mdc(a, b) = mdc(a, a) =\mid a \mid$, o que determina a existência do $mdc(a, b)$;

3°) Se $b \mid a$, então $mdc(a, b) =\mid b \mid$, o que determina a existência do $mdc(a, b)$; e

4°) Se $b \nmid a$ e $1 < b < a$, então, pelo algoritmo da divisão euclidiana,

$$a = b \cdot q_1 + r_1, \text{ com } 0 < r_1 < b.$$

Daí, temos duas possibilidades:

1) $r_1 \mid b$, de onde, pelo Lema 2.1,

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 \cdot b) = mdc(b, a) = mdc(a, b),$$

o que determina a existência do mdc(a,b); e

2) $r_1 \nmid b$, de onde, novamente pelo algoritmo da divisão euclidiana, temos que

$$b = q_2 \cdot r_1 + r_2, \text{ com } 0 < r_2 < r_1.$$

Outra vez, temos duas possibilidades:

2.1) $r_2 \mid r_1$, de onde, pelo Lema 2.1,

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

o que também determina a existência do mdc(a,b); e

2.2) $r_2 \nmid r_1$, de onde, novamente pelo algoritmo da divisão euclidiana,

$$r_1 = q_3 \cdot r_2 + r_3, \text{ com } 0 < r_3 < r_2.$$

Na continuação sucessiva deste processo, como $b > r_1 > r_2 > ...$, chegaremos em um momento no qual, pelo Princípio da Boa Ordenação, não será mais possível a continuação, pois esta é uma sequência de números naturais que sempre possui um menor elemento.

Deste modo, em algum momento da sequência tratada no parágrafo anterior, vai existir para algum $c \in \mathbb{N}$ um $r_c \mid r_{c-1}$, implicando na existência de um $mdc(a, b) = r_c$.

Portanto, dados $a, b \in \mathbb{N}$, então o $mdc(a, b)$ sempre existe. ■

Podemos sintetizar o Algoritmo de Euclides nos diagramas que se seguem:

$\leftrightsquigarrow$ distribuição dos valores $a = q_1 \cdot b + r_1$;

	q_1
a	b
r_1	

$\leftrightsquigarrow$ distribuição dos valores $b = q_2 \cdot r_1 + r_2$;

	q_1	q_2
a	b	r_1
r_1	r_2	

$\leftrightsquigarrow$ distribuição dos valores até onde for possível;

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

Exemplo 2.21. Calcular o mdc(350, 155).

	2	3	1	7
350	155	40	35	$5 = mdc(350, 155)$
40	35	5	0	

Podemos observar na resolução acima que:

- $5 = 40 - 1 \cdot 35$;
- $35 = 155 - 3 \cdot 40$; e
- $40 = 350 - 2 \cdot 155$.

Isto nos fornece que

$$5 = 40 - 1 \cdot 35 \Rightarrow$$
$$5 = 40 - 1 \cdot (155 - 3 \cdot 40) \Rightarrow$$
$$5 = 4 \cdot 40 - 1 \cdot 155 \Rightarrow$$
$$5 = 4 \cdot (350 - 2 \cdot 155) - 1 \cdot 155 \Rightarrow$$
$$5 = (4 \cdot 350) + (-9 \cdot 155),$$

ou seja, podemos escrever $5 = mdc(350, 155)$ como múltiplo de 350 mais um múltiplo de 155, ou seja, como uma combinação linear de 350 e de 155, o que será de grande valia nas resoluções das equações diofantinas, pois a generalização deste fato nos permite escrever o $mdc(x, y)$, com $x, y \in \mathbb{Z}$, na forma $ax + by$, com $a, b \in \mathbb{Z}$, ou seja, na forma de uma combinação linear de a e de b.

Sendo assim, consideremos aqui $a, b \in \mathbb{Z}$ e definamos o conjunto

$$I(a, b) = \{e \cdot a + f \cdot b; e, f \in \mathbb{Z}\}.$$

Com isto, se a e b não forem nulos simultaneamente, então temos que

$$I(a, b) \cap \mathbb{N} \neq \emptyset,$$

pois, por exemplo, $a^2 + b^2 \in I(a, b) \cap \mathbb{N}$, visto que $a^2 + b^2 = a \cdot a + b \cdot b$.

Consideremos também um outro conjunto

$$d\mathbb{Z} = \{g \cdot d; g \in \mathbb{Z}\}.$$

Teorema 2.4. *Sejam a e $b \in \mathbb{Z}$ não ambos nulos. Se $d = min I(a, b) \cap \mathbb{N}$, então temos que d é o $mdc(a, b)$ e $I(a, b) = d\mathbb{Z}$.*

Demonstração: Consideremos $c \in \mathbb{Z}$ e suponhamos que $c \mid a$ e $c \mid b$. Com isto, pela Proposição 2.9, temos que c divide qualquer combinação linear de a e b, ou seja, $c \mid e \cdot a + f \cdot b$ com $e, f \in \mathbb{Z}$ e, consequentemente, c divide todo e qualquer elemento pertencente a $I(a, b)$, inclusive $c \mid d$.

Consideremos também um certo $h \in I(a, b)$ e suponhamos, por absurdo, que $d \nmid h$. Então, pelo algoritmo da divisão euclidiana, temos que

$$h = dq + r, \text{ com } 0 \leqslant r < d.$$

Como $d, h \in I(a, b)$, então d é da forma $i \cdot a + j \cdot b$ e h é da forma $k \cdot a + l \cdot b$ para determinados $i, j, k, l \in \mathbb{Z}$. Então, temos que

$$h = dq + r \Rightarrow r = h - dq \Rightarrow$$

$$r = k \cdot a + l \cdot b - (i \cdot a + j \cdot b)q \Rightarrow$$
$$r = k \cdot a + l \cdot b - i \cdot a \cdot q - j \cdot b \cdot q \Rightarrow$$
$$r = (k - i \cdot q) \cdot a + (l - j \cdot q) \cdot b,$$

com $r \in I(a,b) \cap \mathbb{N}$, onde chegamos em um absurdo, pois $d = minI(a,b) \cap \mathbb{N}$ e $r < d$.

Daí, como $d = minI(a,b) \cap \mathbb{N}$, então $d \mid a$ e $d \mid b$.

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

Agora, novamente pela Proposição 2.9, como todos os elementos de $I(a,b)$ são divisíveis por d, então temos que $I(a,b) \subset d\mathbb{Z}$. E, por outro lado, temos que todo $g \cdot d \in d\mathbb{Z}$ é da forma

$$gd = g \cdot (i \cdot a + j \cdot b) = g \cdot i \cdot a + g \cdot j \cdot b = (g \cdot i) \cdot a + (g \cdot j) \cdot b,$$

ou seja, $gd \in I(a,b)$.

Logo, $d\mathbb{Z} \subset I(a,b)$ e, como $I(a,b) \subset d\mathbb{Z}$ e $d\mathbb{Z} \subset I(a,b)$, então podemos concluir que $I(a,b) = d\mathbb{Z}$.

Portanto, sendo a e $b \in \mathbb{Z}$ não ambos nulos, se $d = minI(a,b) \cap \mathbb{N}$, então temos que d é o $mdc(a,b)$ e $I(a,b) = d\mathbb{Z}$. ■

Observemos aqui que o Teorema acima demonstrado nos fornece uma outra prova, diferente da feita no Algoritmo de Euclides, das existências do $mdc(a,b)$ e de $c, d \in \mathbb{Z}$ tais que $mdc(a,b) = c \cdot a + d \cdot b$ e é conhecido por Teorema de Bachet-Bézout. Portanto, se $e \in \mathbb{Z}$ é tal que $e \mid a$ e $e \mid b$, então $e \mid mdc(a,b)$, que é uma condição de existência de solução das equações diofantinas lineares a ser vista e utilizada mais adiante.

Corolário 2.3. *Sejam a e $b \in \mathbb{Z}$ não ambos nulos e $c \in \mathbb{N}$. Temos que*

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

Demonstração: Observemos que $I(c \cdot a, c \cdot b) = c \cdot I(a,b)$, pois

$$I(c \cdot a, c \cdot b) = \{c \cdot e \cdot a + c \cdot f \cdot b; e, f \in \mathbb{Z}\} \Rightarrow$$
$$I(c \cdot a, c \cdot b) = \{c \cdot (e \cdot a + f \cdot b)\} \Rightarrow$$
$$I(c \cdot a, c \cdot b) = c \cdot \{(e \cdot a + f \cdot b)\} \Rightarrow$$
$$I(c \cdot a, c \cdot b) = c \cdot I(a,b).$$

Então, daí e do Teorema 2.4, podemos concluir que

$$mdc(c \cdot a, c \cdot b) = min(c \cdot I(a,b) \cap \mathbb{N}) = c \cdot min(I(a,b) \cap \mathbb{N}) = c \cdot d = c \cdot mdc(a,b).$$

Portanto, sendo a e b dois números inteiros não ambos nulos e $c \in \mathbb{N}$, temos que $mdc(c \cdot a, c \cdot b) = c \cdot mdc(a,b)$. ■

Corolário 2.4. *Sejam a e $b \in \mathbb{Z}$ não ambos nulos. Temos que*

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

Demonstração: Pelo Corolário 2.3, temos que

$$mdc(a,b)\cdot mdc\left(\frac{a}{mdc(a,b)},\frac{b}{mdc(a,b)}\right)=$$

$$=mdc\left(mdc(a,b)\cdot\frac{a}{mdc(a,b)},mdc(a,b)\cdot\frac{b}{mdc(a,b)}\right)=mdc(a,b).$$

Logo, temos $mdc(a,b)\cdot mdc\left(\frac{a}{mdc(a,b)},\frac{b}{mdc(a,b)}\right)=mdc(a,b)\Rightarrow mdc(a,b)\cdot 1=mdc(a,b)$, ou seja, $mdc\left(\frac{a}{mdc(a,b)},\frac{b}{mdc(a,b)}\right)=1$.

Portanto, sendo a e b dois números inteiros não ambos nulos, temos que $mdc\left(\frac{a}{mdc(a,b)},\frac{b}{mdc(a,b)}\right)=1$. ■

Observemos aqui que o Corolário 2.4 afirma que $\frac{a}{mdc(a,b)}$ e $\frac{b}{mdc(a,b)}$ são coprimos, pois, por ele, $mdc\left(\frac{a}{mdc(a,b)},\frac{b}{mdc(a,b)}\right)=1$.

2.5 MÍNIMO MÚLTIPLO COMUM

Falaremos um pouco agora sobre o mínimo múltiplo comum (mmc) de dois números inteiros. Na educação, já é um assunto mais trabalhado e desenvolvido no Ensino Fundamental e no Ensino Médio.

Como vamos necessitar quando tratarmos das equações diofantinas lineares com coeficientes racionais e irracionais, façamos as seguintes definições:

Definição 2.11. Dizemos que $a\in\mathbb{Z}$ é múltiplo de $b\in\mathbb{Z}$ quando $a=bc$ para algum $c\in\mathbb{Z}$.

Definição 2.12. Dizemos que $a\in\mathbb{Z}$ é múltiplo comum de $b,c\in\mathbb{Z}$ quando $a=bd$ para algum $d\in\mathbb{Z}$ e $a=ce$ para algum $e\in\mathbb{Z}$, ou seja, se a é múltiplo de b e c ao mesmo tempo.

Definição 2.13. Dizemos que $c\in\mathbb{Z}$ é o mínimo múltiplo comum de $a,b\in\mathbb{Z}$ e escreveremos $mmc(a,b)$ quando

- $c>0$;
- c é múltiplo comum de a,b; e
- c é o menor múltiplo comum de a,b, tal que se c' também é um múltiplo comum de a,b, então $c\leqslant c'$.

Exemplo 2.22. O $mmc(3,5)=15$, pois 15 é o menor múltiplo comum de 3 e 5.

Exemplo 2.23. O $mmc(3,6)=6$, pois 6 é o menor múltiplo comum de 3 e 6.

Exemplo 2.24. O $mmc(12,20)=60$, pois 60 é o menor múltiplo comum de 12 e 20.

Proposição 2.11. *Dados $a,b\in\mathbb{Z}$, temos que $mmc(a,b)$ existe e*

$$\frac{|\,a\cdot b\,|}{mdc(a,b)}=mmc(a,b).$$

Demonstração: Podemos observar que quando temos $a = 0$ ou $b = 0$, a igualdade $\frac{|\ a \cdot b\ |}{mdc(a,b)} = mmc(a,b)$ é satisfeita. Podemos observar ainda que a igualdade será satisfeita para a e b se, e somente se, esta for satisfeita para $\pm a$ e $\pm b$. Daí, podemos supor, sem perda de generalidade, que $a, b \in \mathbb{N}$.

Fazendo $c = \frac{ab}{mdc(a,b)}$, temos que

$$c = \frac{ab}{mdc(a,b)} \Rightarrow c = a \cdot \frac{b}{mdc(a,b)} = b \cdot \frac{a}{mdc(a,b)},$$

ou seja, temos que $a \mid c$, pois $c = a \cdot \frac{b}{mdc(a,b)} \Rightarrow \frac{c}{a} = \frac{b}{mdc(a,b)} \in \mathbb{N}$ e $b \mid c$, pois $c = b \cdot \frac{a}{mdc(a,b)} \Rightarrow \frac{c}{b} = \frac{a}{mdc(a,b)} \in \mathbb{N}$. Logo, c é múltiplo comum de a e b.

Agora, consideremos d um múltiplo comum de a e b. Daí, temos que $d = a \cdot e$ e $d = b \cdot f$, de onde obtemos

$$d = a \cdot e = b \cdot f \Rightarrow e \cdot \frac{a}{mdc(a,b)} = f \cdot \frac{b}{mdc(a,b)}.$$

Como pelo Corolário 2.4 temos que $\frac{a}{mdc(a,b)}$ e $\frac{b}{mdc(a,b)}$ são coprimos, então $\frac{a}{mdc(a,b)}$ divide f e $\frac{b}{mdc(a,b)}$ divide e e, consequentemente, $c = b \cdot \frac{a}{mdc(a,b)}$ divide $b \cdot f$ e $c = a \cdot \frac{b}{mdc(a,b)}$ divide $a \cdot e$. Logo $c \mid d$, ou seja, $c = mmc(a,b)$.

Portanto, dados a, b pertencentes ao conjuntos dos números inteiros, temos que $mmc(a,b)$ existe e $\frac{|\ a \cdot b\ |}{mdc(a,b)} = mmc(a,b)$. ■

Observemos aqui que se a e b são coprimos, então temos que $mdc(a,b) = 1$ e $\frac{|\ a \cdot b\ |}{mdc(a,b)} = mmc(a,b) \Rightarrow mmc(a,b) = |\ a \cdot b\ |$.

Exemplo 2.25. Sejam $a, b \in \mathbb{N}$. Mostrar que, na sequência numérica $a, 2a, 3a, ..., a \cdot b$, existem exatamente $mdc(a,b)$ números divisíveis por b.

Solução: Primeiramente, temos que observar o fato de que os números da sequência divisíveis por b também são divisíveis por a. Logo obtemos os números:

$$mmc(a,b), 2 \cdot mmc(a,b), 3 \cdot mmc(a,b), ..., a \cdot b$$

Como, pela Proposição 2.11, temos que

$$\frac{|\ a \cdot b\ |}{mdc(a,b)} = mmc(a,b) \Rightarrow a \cdot b = mdc(a,b) \cdot mmc(a,b),$$

então a sequência acima pode ser escrita na forma

$$mmc(a,b), 2 \cdot mmc(a,b), 3 \cdot mmc(a,b), ..., mdc(a,b) \cdot mmc(a,b).$$

Portanto, sendo $a, b \in \mathbb{N}$, temos que, na sequência numérica $a, 2a, 3a, ..., a \cdot b$, existem exatamente $mdc(a,b)$ números divisíveis por b. □

3 DIOFANTO DE ALEXANDRIA

Neste capítulo abordaremos um pouco da história de Diofanto, matemático grego que deixou grandes contribuições para a Matemática, especialmente no campo da Álgebra, tomando como suporte teórico principalmente as obras de Boyer e Merzbach (2012) e Boyer (2008), Domingues (1991), Eves (2011), Freitas (2015), Roque (2012) e Roque e Pitombeira (2012), Souza (2017).

Em homenagem a Diofanto de Alexandria, matemático helenístico do século III, foram denominadas algumns tipos de equações com seu nome, as chamadas equações diofantinas. Tendo ainda seu nome relacionado à Análise Diofantina, ou seja, o estudo matemático de situações e problemas propostos por Diofanto.

A obra "Os Elementos", de Euclides de Alexandria, foi um marco na Matemática da Grécia e, depois deles, houve um período de estagnação entre o século II a.C. e o século II d.C.

De acordo com Roque e Pitombeira (2012, p.107), "o início do século II a.E.C. foi marcado por um declínio na atenção dos matemáticos aos problemas geométricos avançados, o que não representou uma decadência do campo matemático, mas um deslocamento de interesse em direção a outras áreas".

Figura 1 – Diofanto de Alexandria

Fonte: Freitas (2015, p.17).

Diophanti Alexandrini, o Diofanto de Alexandria, aparece neste cenário, sem precisão de datas, nascido entre 201 e 214 e falecido entre 284 e 298. A maioria dos historiadores apontam que ele viveu no século III d.C., sendo considerado o maior algebrista grego, mesmo tendo poucos registros sobre sua vida e suas obras. Ele desempenhou papel semelhante à Euclides na Geometria e à Ptolomeu na Astronomia.

Foi encontrado um problema que fornece detalhes de sua vida na obra chamada de "Antologia Grega" (uma coleção de problemas algébricos do século V ou IV) e também escrito em sua tumba, segundo Roque (2012), os quais enunciam respectivamente o seguinte:

> Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem; Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança tardia; depois de chegar à medida de metade da vida de seu pai, o destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida. (BOYER, 2008, p. 121).

"Aqui jaz Diofanto. Maravilhosa habilidade. Pela arte da álgebra a lápide nos diz sua idade: Deus deu um sexto da vida como infante, um duodécimo mais como jovem, de barba abundante; e ainda uma sétima parte antes do casamento; em cinco anos nasce-lhe o rebento. Lastima! O filho do mestre e sábio do mundo se vai. Morreu quando atingiu metade da idade final do pai. Quatro anos a mais de estudos consolam-no do pesar; Para então, deixando a terra, também ele alívio encontrar."

Se os enunciados forem verdadeiros, estas informações nos levam a constatar que Diofanto viveu por 84 anos, pois representando-as com uma equação algébrica no intuito de descobrir sua idade, com x representando-a, temos que:

$$\begin{aligned} x &= \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 \\ x - \frac{x}{6} - \frac{x}{12} - \frac{x}{7} - \frac{x}{2} &= 5 + 4 \\ \frac{84x}{84} - \frac{14x}{84} - \frac{7x}{84} - \frac{12x}{84} + \frac{42x}{84} &= 9 \\ \frac{9x}{84} &= 9 \\ 9x &= 9 \cdot 84 \\ x &= 84 \text{ anos.} \end{aligned}$$

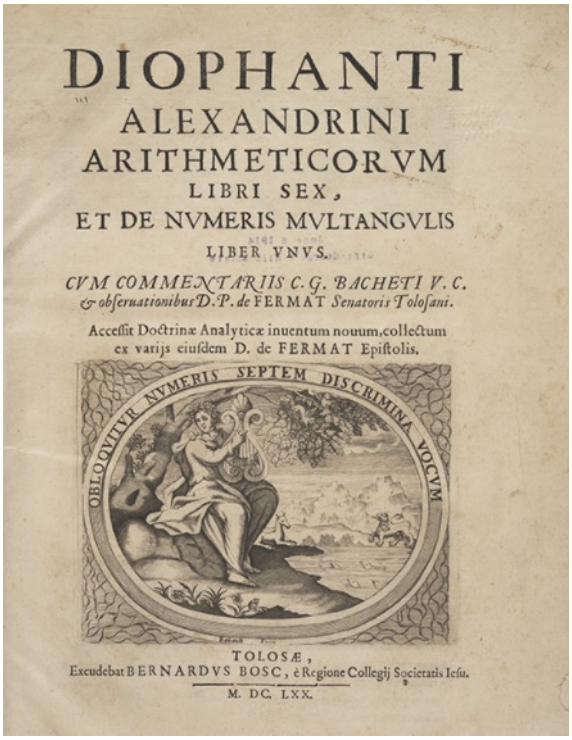
> Diofanto escreveu três tratados: Aritmética, Sobre Números Poligonais, do qual restaram fragmentos, e Porismas, que foi perdido. Seu tratado Aritmético (no grego, significa "ciência dos números") é uma obra-prima, pioneira no tratamento do difícil assunto a que hoje chamamos de Teoria dos Números, sem deixar qualquer dúvida de que seu autor era um gênio do mais alto nível. (FREITAS, 2015, p. 16).

A obra de Diofanto, mesmo contemplando várias subáreas da Matemática, com toda certeza proporcionou um enorme avanço na álgebra, tendo sido fonte de inspiração para diversos outros matemáticos a investirem e investigarem no campo da Teoria dos Números.

Sua obra mais conhecida é Aritmética, uma coleção composta de treze livros, como relatado pelo próprio autor no prefácio. Apenas seis destes livros foram conhecidos na língua original; depois, outros quatro livros, que alguns pesquisadores e historiadores julgam ser parte desta obra, foram encontrados, só que estavam traduzidos em árabe. Aritmética foi encontrada por Johann Müller, um matemático e astrônomo alemão, em 1464, em Veneza, e traduzido primeiramente por outro alemão, filólogo clássico, hebraísta,

matemático e astrônomo, Wilhelm Holzmann (1532-1576).

Figura 2 – Capa do Livro VI - Arithmetica



Fonte: Frank (2018).

Aritmética é uma coletânea com diversos problemas sob forma de exemplos numéricos específicos, com a finalidade de determinar uma generalidade para cada tipo de problema, sendo suas demonstrações apenas ilustrações, em casos particulares concretos. Nela se vê uma abordagem analítica da teoria dos números, envolvendo equações do 1º e 2º graus. Contém também a resolução de uma equação cúbica e problemas algébricos indeterminados. Diofanto procurava soluções racionais positivas, não se preocupando com a quantidade de soluções possíveis.

Boyer e Merzbach (2012, p.133 - 134) observaram um alto grau de habilidade matemática, assemelhando-se aos trabalhos "algébricos" dos babilônios, não existindo nada parecido na matemática grega construída até esta época. Devemos destacar também que Diofanto não utilizava as "ferramentas" geométricas desenvolvidas até então para a resolução das equações.

Sobre os seis livros que conservaram-se em grego podemos relatar que:

- o primeiro livro traz problemas que envolvem equações de 1° e de 2° graus;
- o segundo livro, em uma cópia, nas margens do problema de número 8, estavam descritas as infinitas soluções da equação pitagórica $x^2 + y^2 = z^2$. Pierre de Fermat (1601 - 1665), matemático e cientista francês, havia escrito as seguintes palavras traduzidas para nosso idioma: "*Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração*

verdadeiramente maravilhosa disto, que todavia esta margem não é sufucientemente grande para cabê-la." Tal afirmação é conhecida como o *Último Teorema de Fermat*, demonstrada por Andrew Wiles, um matemático inglês, somente em 1995;

- o terceiro livro contém, pela primeira vez, uma recorrência à geometria para se obter a solução do seu problema 19;
- o quarto livro trata, na maioria de seus problemas, de números cúbicos;
- o quinto livro trabalha com problemas de 2° grau e 3° graus; e
- o sexto livro faz tratativa a resolução de triângulos retângulos de lados racionais.

Roque e Pitombeira (2012, p.133) relatam que esta obra é a parte do desenvolvimento da álgebra conhecido como estágio intermediário ou álgebra sincopada, caracterizado por abreviações para quantidades e operações que se repetem constantemente.

Surge então, com Diofanto, um modo matemático de pensar mais próximo do que se chama atualmente de "álgebra", ao introduzir uma forma de representação dos valores desconhecidos em um problema, chamando-o de aritmos (arithmos), provindo da palavra "aritmética" (arithmetike), onde algumas abreviaturas designam quantidades e operações, iniciando a chamada "álgebra sincopada".

Três períodos são distinguidos no desenvolvimento da álgebra. São eles:

1°) álgebra retórica, onde se explica tudo através de palavras;
2°) álgebra sincopada, onde se usam algumas abreviaturas; e
3°) álgebra simbólica, onde se usam diversos símbolos.

Nos seis livros citados da obra Aritmética, Diofanto utilizou as seguintes abreviações para as potências de números e para relações e operações, como sua forma de sincopação:

i) ς (que é a última letra da palavra arithmos, para designar a quantidade desconhecida);
ii) ΔY (que é a primeira letra de dynamis, para designar o quadrado da quantidade desconhecida);
iii) KY (que é a primeira letra de kybos, para designar o cubo)
iv) $\Delta Y \Delta$ (que é o quadrado-quadrado para designar a quarta potência);
v) ΔKY (que é o quadrado-cubo, para designar a quinta potência); e
vi) $KY\ K$(que é o cubo-cubo, para designar a sexta potência).

> [...]nas obras preservadas de Diofanto há um uso sistemático de abreviações para potências de números e para relações e operações, sendo que, um número desconhecido é representado por um símbolo parecido com a letra grega ζ; o quadrado disto parece como Δ^{γ}, o cubo com κ^{γ}, a quarta potência, dita quadrado-quadrado, como $\Delta^{\gamma}\Delta$; a quinta potência ou quadrado-cubo, como $\Delta\kappa^{\gamma}$; a sexta potência ou cubo-cubo como $\kappa^{\gamma}\kappa$ e a igualdade como ι. O símbolo Λ era utilizado para representar o sinal de menos, sendo que, todos os termos negativos de uma expressão eram reunidos e antes deles era escrito o símbolo de menos. Já para indicar a adição de termos não utilizou nenhum símbolo específico, pois a mesma era feita por justaposição e os termos independentes eram indi-

> cados pelo símbolo μ seguido de seu coeficiente numérico. E por fim, os coeficientes sempre eram representados após o símbolo que representava a incógnita,[...]. (SOUZA, 2017, p. 29).

Segundo Roque e Pitombeira (2012, p.132): "o fato de haver símbolos para as potências superiores ao cubo já indica a separação entre a aritmética de Diofanto e a geometria, uma vez que, na geometria da época, uma potência maior que três para um número não correspondia a nenhuma grandeza".

Ainda para Roque e Pitombeira (2012, p.133), as inovações realizadas nas resoluções feitas por Diofanto são: a não recorrência a alguma construção geométrica para resolução dos problemas e operar com quantidades conhecidas e desconhecidas do mesmo modo, ou seja, estas quantidades possuindo o mesmo estatuto na resolução.

Sendo assim, devemos supor que todas as quantidades sejam conhecidas, pois, somente assim, é possível introduzirmos um símbolo para uma quantidade desconhecida (no caso de Diofanto, a letra ς), o que caracteriza um novo pensamento algébrico. Para Diofanto, o arithmos é uma "quantidade indeterminada de unidades", enquanto os números são uma quantidade determinada de unidades e ambos são sujeitos ao mesmo tipo de tratamento no problema estudado.

Assim, podemos agrupar os "diferentes" tipos numéricos por espécies, ou seja, os monômios, e por expressões, ou seja, as operações entre espécies.

Como exemplo de um problema da obra Aritmética, mostramos a seguir, do Livro II, o problema 8 já citado anteriormente: "Decompor o quadrado 16 em dois quadrados".

A resolução proposta por Diofanto é a seguinte: "*Se quisermos decompor* 16 *em dois quadrados e supusermos que o primeiro é* 1 *aritmo, o outro terá* 16 *unidades menos um quadrado de aritmo e, portanto,* 16 *unidades menos um quadrado de aritmo é um quadrado. Formemos um quadrado de um conjunto qualquer de aritmos diminuído de tantas unidades como tem a raiz de* 16 *unidades, ou seja, o quadrado de* 2 *aritmos menos* 4 *unidades. Este quadrado terá* 4 *unidades de aritmo e* 16 *unidades menos* 16 *aritmos, que igualaremos a* 16 *unidades menos um quadrado de aritmo e somando a um e outro lado os termos negativos e restando os semelhantes, resulta que* 5 *quadrados de aritmo equivalem a* 16 *aritmos e, portanto,* 1 *aritmo vale* $\frac{16}{5}$*; logo, um dos números é* $\frac{256}{25}$ *e o outro é* $\frac{144}{25}$*, cuja soma é* $\frac{400}{25}$*, ou seja,* 16 *unidades, e cada um deles é um quadrado*". Assim:

$$16 = x^2 + y^2$$
$$x = \varsigma \text{ e } y^2 = (16 - \Delta Y) = (2\varsigma - 4)^2$$
$$(2\varsigma - 4)^2 = 16 - \Delta Y$$
$$4\Delta Y - 16\varsigma + 16 = 16 - \Delta Y$$
$$4\Delta Y - 16\varsigma + \Delta Y + 16\varsigma = -\Delta Y + \Delta Y + 16\varsigma$$
$$5\Delta Y = 16\varsigma$$

$$5\varsigma = 16$$

$$1\varsigma = \frac{16}{5} \Rightarrow\ x = \frac{16}{5} \Rightarrow\ x^2 = \frac{256}{25}$$

$$16 - \Delta Y = 16 - \left(\frac{16}{5}\right)^2 = \frac{400}{25} - \frac{256}{25} = \frac{144}{25} \Rightarrow y^2 = \frac{144}{25} \Rightarrow y = \frac{12}{5}$$

$$16 = x^2 + y^2 \Rightarrow \frac{400}{25} = \frac{256}{25} + \frac{144}{25} \Rightarrow \left(\frac{20}{5}\right)^2 = \left(\frac{16}{5}\right)^2 + \left(\frac{12}{5}\right)^2.$$

Como um exemplo de resolução de um problema nos três períodos da Álgebra, da obra Aritmética, mostramos a seguir, do Livro I, o problema 27, onde é solicitado encontrar dois números cuja soma e o produto sejam números dados.

1) Resolução na álgebra retórica: consideremos que a soma é 20 e o produto, 96. Supomos que a diferença entre os dois números seja 2 aritmos, dividimos 20 por dois obtendo 10. A partir deste resultado, consideramos 10 subtraído de 1 aritmo e 10 acrescentado de 1 arithmo, obtendo 20, ou seja, a soma desejada. Para que o produto seja 96, multiplicamos estas mesmas quantidades, obtendo 100, subtraído do quadrado do arithmo (um dynamo). Chegamos a conclusão de que o dynamo deve ser 4, logo, o valor do aritmo é 2. Então, os valores procurados são, portanto, $10 - 2$ e $10 + 2$, ou seja, 8 e 12;
2) Resolução na álgebra sincopada: sendo os dois números iguais, cada um deles seria 10. Supomos que a diferença entre eles seja 2ς, ou seja, os dois números procurados são obtidos retirando ς de um deles e adicionando ς ao outro. Então, temos que $(10 - \varsigma) + (10 + \varsigma) = 20$ e $(10 - \varsigma) \cdot (10 + \varsigma) = 96$. Observamos, então, que $100 - \Delta Y = 96$, e concluímos que $\varsigma = 2$. Logo, os números procurados $10 - \varsigma$ e $10 + \varsigma$ são, respectivamente, 8 e 12;
3) Resolução na álgebra simbólica: temos $x + y = 20$ e $x \cdot y = 96$. Se os dois fossem números iguais, então $x = 10$ e $y = 10$. Suponhamos que seja $2x$ a diferença entre eles, então existe z tal que $x = 10 - z$ e $y = 10 + z$. Substituímos na equação $x \cdot y = 96$ para obtermos: $(10 - z) \cdot (10 + z) = 96$; logo, $100 - z^2 = 96$. Então, $z = 2$. Logo, os números procurados $x = 10 - z$ e $y = 10 + z$ são, respectivamente, 8 e 12.

De acordo com Boyer (2008), este pensamento de Diofanto, baseado na invenção e no uso de símbolos, utilizados para simplificar tanto a escrita quanto os cálculos matemáticos, introduziu um novo modo matemático de pensar.

Segundo Pommer e Pommer (2012, p. 32), a obra de Diofanto é um novo ramo matemático, com metodologia própria, estranha ao modo de pensar dos gregos antigos, na qual muitos problemas são abordados com motivação geométrica, contudo suas resoluções não fazem uso da Geometria, ou seja, não utilizam o recurso das figuras e, sim, as manipulações algébricas.

Ainda por Pommer e Pommer (2012, p. 33), a obra de Diofanto de Alexandria

é quase toda dedicada à resolução exata de equações, tanto determinadas como indeterminadas e é pioneira em determinar soluções para um problema particular com as quais se acumulam regras de manipulação de equações, de diversos graus de dificuldade, dependendo logicamente dos artifícios utilizados em cada situação.

Este desenvolvimento algébrico, evidenciado na associação aos símbolos, permitiu que as soluções dos problemas se tornassem mais sintéticas, fornecendo contribuições significativas na Teoria dos Números, campo da matemática onde as equações diofantinas lineares se fazem presentes.

> Devido a essa sua utilização de métodos algébricos, hoje recebem o nome de equações diofantinas todas as equações polinomiais (com qualquer número de incógnitas), com coeficientes inteiros, sempre que se trata de procurar suas possíveis soluções entre os inteiros. (DOMINGUES, 1991, p. 119).

4 EQUAÇÕES DIOFANTINAS

Neste capítulo, abordaremos as equações diofantinas propriamente ditas, apresentando e caracterizando as lineares, as equações pitagóricas e a equação de Pell. Definiremos também as equações diofantinas lineares no conjuntos dos números inteiros ($\mathbb{Z}$), no conjunto dos números racionais ($\mathbb{Q}$) e no conjunto dos números irracionais ($\mathbb{I}$), tomando como norte principalmente as obras de Hefez (2013), (2009) e (2006), Domingues (1991), Eves (2011), Alencar Filho (1981), Martinez e et al (2018), Ripoll J., Ripoll C. e Sant'Ana (2006), Rocque e Pitombeira (1991), Savóis e Freitas (2015).

São exemplos de equações diofantinas:

- Equação Diofantina Linear: $aX + bY = c$, com X e Y sendo as variáveis da equação e a, b e c sendo constantes dadas;
- Equação Diofantina Exponencial: $aX^n + bY^n = cZ^n$, com X, Y e Z sendo as variáveis da equação e a, b, c e n sendo constantes dadas;
- Equação Diofantina Infinita: $N = A^2 + 2B^2 + 3C^2 + 4D^2 + \cdots$, com $N \in \mathbb{Z}$ sendo a variável da equação e $A, B, C, D, ...$ sendo constantes dadas, que é a expressão da sentença: "De quantas formas distintas pode se escrever um certo $N \in \mathbb{Z}$ como o seguinte somatório: um determinado quadrado adicionado do dobro de um determinado quadrado adicionado do triplo de um determinado quadrado adicionado do quádruplo de um determinado quadrado e assim sucessivamente?".

Existem determinadas equações diofantinas que são estudadas individualmente por ser um vasto leque de equações, como:

- ▷ $X^n + Y^n = Z^n$, com X, Y e Z sendo as variáveis da equação e $n \in \mathbb{N}$ sendo uma constante dada, onde para $n = 2$, temos os ternos pitagóricos (X, Y, Z) como infinitas soluções; e para valores maiores de $n > 2$, temos o Último Teorema de Fermat-Willies;
- ▷ $X^2 - nY^2 = \pm 1$, com X e Y sendo as variáveis da equação e n sendo uma constante dada, conhecida por equação de Pell, em homenagem ao matemático inglês John Pell e estudada por Brahmagupta, matemático e astrônomo indiano, no século VII e também por Fermat no século XVII;
- ▷ $\frac{4}{n} = \frac{1}{X} + \frac{1}{Y} + \frac{1}{Z}$, com X, Y e Z sendo as variáveis da equação e n sendo uma constante dada, conhecida por Conjectura de Erdõs-Straus a qual afirma que para todo positivo $n \geqslant 2$, existe uma solução (X, Y, Z), com $X, Y, Z \in \mathbb{Z}_+^*$, tendo sua forma polinomial similar a equação polinomial $4XYZ = nXY + nXZ + nYZ = n(XY + XZ + YZ)$; entre tantas outras.

Problemas Diofantinos restringem-se a determinar soluções em $\mathbb{Z}$ que devem servir para a equação gerada em cada situação. Utilizando uma linguagem mais técnica, as equações diofantinas definem uma curva algébrica, ou uma superfície algébrica ou um objeto mais genérico e solicitam que sejam determinadas as coordenadas que tornam

possível este objeto.

4.1 EQUAÇÕES DIOFANTINAS LINEARES COM DUAS VARIÁVEIS

Definição 4.1. Equações diofantinas lineares são equações polinomiais com duas ou mais variáveis formada pelo somatório de monômios de grau um e um monômio de grau zero, que possuem apenas soluções no conjunto dos números inteiros, ou seja, são equações da forma

$$a_0x_0 + a_1x_1 + a_2x_2 + ... + a_nx_n = c,$$

com $a_0, a_1, a_2, ..., a_n \in \mathbb{Z}$, onde se procura determinar somente as soluções pertencentes ao conjunto dos números inteiros.

Sendo assim, podemos afirmar que uma equação diofantina linear escreve c como uma combinação linear inteira de todos os a_i, com $0 \leqslant i \leqslant n$. Nesta parte do trabalho, abordaremos particularmente as equações diofantinas lineares com duas variáveis.

Vários problemas de aritmética têm suas respectivas resoluções, determinadas no conjunto dos números inteiros ($\mathbb{Z}$), em equações da forma

$$aX + bY = c$$

com $a, b, c \in \mathbb{Z}$, sendo estas denominadas equações diofantinas lineares com duas variáveis.

Definição 4.2. Equação diofantina linear com duas variáveis é uma equação polinomial indeterminada na qual suas variáveis só podem assumir valores inteiros, sendo formada por uma igualdade entre a soma de dois monômios de grau um e um monômio de grau zero.

Como mencionado acima, aqui, retringiremo-nos as equações diofantinas lineares da forma $aX + bY = c$, com $a, b, c \in \mathbb{Z}$. Neste tipo de equação, devemos sempre observar as propriedades das constantes inteiras, utilizar desigualdades quando possível, pensar em casos particulares e utilizar o mdc e o algoritmo de Euclides para facilitar a resolução de cada questão. Todos estes detalhes vamos ter a oportunidade de utilizar nos exemplos que iremos solucionar no decorrer deste capítulo.

Exemplo 4.1. Determinar todas as soluções inteiras da equação $2x + 3y = 5$.

Solução: Observemos que a equação $2x + 3y = 5$ é uma equação diofantina linear com as variáveis x e y, onde seus respectivos coeficientes são $a = 2$ e $b = 3$ e ainda temos $c = 5$.

Notemos aqui que como $c = 5$ é ímpar e $2x$ é par, então devemos ter $3y$ sendo ímpar. Daí, $3y = 2y_0 + 1$ e, consequentemente, $2x + 3y = 5 \Rightarrow 2x + 2y_0 + 1 = 5 \Rightarrow 2x = 5 - (2y_0 + 1) \Rightarrow x = \dfrac{4 - 2y_0}{2} \Rightarrow x = 2 - y_0$.

Portanto, todas as soluções inteiras da equação $2x + 3y = 5$ são da forma $(x, y) = (2 - y_0, y_0)$. □

Para Rocque e Pitombeira (1991), uma equação diofantina aparece costumeira

e naturalmente em determinados problemas que envolvem agrupamentos e, quando estudamos um problema matemático, é muito conveniente que exista um "método" ou um "processo" que nos forneça a existência ou não de soluções e que, caso exista solução, forneça-nos todas elas.

Nem sempre existe solução para uma equação diofantina, como podemos observar no exemplo

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

onde $6x$ é um número par da forma $2a$ e $2y$ é outro número par da forma $2b$ e 5 é um número ímpar da forma $2c + 1$. Com isto, temos que

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

com $d = (a + b)$.

Sendo assim, no lado esquerdo da igualdade $6x + 2y = 5$, temos a soma dos monômios $6x$ e $2y$ que sempre resultará em um valor par, pois quaisquer números multiplicados por 6 ou por 2 resultarão em um valor par e a soma deles continuará sendo par. E, no lado direito da igualdade, aparece um valor ímpar. Logo, os dois membros da equação não podem ser iguais. Portanto, não existe solução alguma em $\mathbb{Z}$ para a equação $6x + 2y = 5$.

A existência de soluções de uma equação diofantina linear está intrinsecamente ligada ao máximo divisor comum dos coeficientes da equação, conteúdo este apresentado e trabalhado durante as séries do ensino fundamental.

Rocque e Pitombeira (1991) afirmam que "existe de fato um critério que nos permite decidir se a equação $aX + bY = c$ tem ou não soluções inteiras, e ele é uma aplicação genuína e não-trivial da noção de máximo divisor comum". Então, vejamos as proposições a seguir.

Proposição 4.1. *Sejam $a, b, c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em $\mathbb{Z}$ se, e somente se, $mdc(a, b) \mid c$.*

Demonstração: Temos que

$$I(a, b) = \{a \cdot d + b \cdot e;\ d, e \in \mathbb{Z}\} = mdc(a, b)\mathbb{Z}.$$

Já temos que $c \in \mathbb{Z}$. Como c é uma combinação linear de a e b, é lógico e necessário que, para equação $aX + bY = c$ possuir solução, devemos ter $c \in I(a, b)$, que equivale a $c \in mdc(a, b)\mathbb{Z}$, que também equivale a $mdc(a, b) \mid c$.

Por outro lado, se temos $mdc(a, b) \mid c$, isto equivale a $c \in mdc(a, b)\mathbb{Z}$, que equivale a $c \in I(a, b)$.

Portanto, a equação $aX + bY = c$ admite solução em $\mathbb{Z}$ se, e somente se, $mdc(a, b) \mid c$. ■

A equação $aX + bY = c$, com $a \neq 0$ ou $b \neq 0$ e $mdc(a, b) \mid c$ é equivalente à

equação

$$a_1X + b_1Y = c_1,$$

onde

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

Sendo $mdc(a_1, b_1) = 1$, então, de acordo com os Corolários 2.3 e 2.4, podemos nos restringir às equações $aX + bY = c$, com $mdc(a,b) = 1$, que possuem sempre soluções e estas podem ser determinadas a partir de uma solução particular qualquer.

Proposição 4.2. *Seja (x_0, y_0) uma solução particular qualquer da equação $aX + bY = c$, com $mdc(a,b) = 1$. Então, as demais soluções (x, y) em $\mathbb{Z}$ da equação são da forma:*

$$x = x_0 + zb,\ y = y_0 - za,\ \textit{com } z \in \mathbb{Z}.$$

Demonstração: Tomemos (x_1, y_1) uma outra solução da equação $aX + bY = c$.

Daí, e utilizando a solução dada no enunciado, temos que

$$ax_0 + by_0 = ax_1 + by_1 \Rightarrow$$
$$ax_1 - ax_0 = by_0 - by_1 \Rightarrow$$
$$a \cdot (x_1 - x_0) = b \cdot (y_0 - y_1).$$

Como, também pelo enunciado, $mdc(a,b) = 1$, então temos que $a \mid (y_0 - y_1)$ e $b \mid (x_1 - x_0)$, já que $a \nmid b$ e $b \nmid a$. Daí, podemos obter

$$x_1 - x_0 = zb \Rightarrow x_1 = x_0 + zb, \text{ com } z \in \mathbb{Z}.$$

Substituindo $x_1 - x_0 = zb$ em $a \cdot (x_1 - x_0) = b \cdot (y_0 - y_1)$, temos que

$$a \cdot (x_1 - x_0) = b \cdot (y_0 - y_1) \Rightarrow$$
$$a \cdot zb = b \cdot (y_0 - y_1) \Rightarrow$$
$$y_0 - y_1 = za \Rightarrow$$
$$y_1 = y_0 - za.$$

Por outro lado, como (x_1, y_1) é solução da equação $aX + bY = c$, então, tomando $X = x_1$ e $Y = y_1$, pelo enunciado na proposição, temos que

$aX + bY = ax_1 + by_1 = a \cdot (x_0 + zb) + b \cdot (y_0 - za) = ax_0 + abz + by_0 - abz = ax_0 + by_0 = c.$

Portanto, sendo (x_0, y_0) uma solução particular da equação $aX + bY = c$, com $mdc(a,b) = 1$, então, temos que as demais soluções (x, y) em $\mathbb{Z}$ da equação são da forma: $x = x_0 + zb,\ y = y_0 - za$, com $z \in \mathbb{Z}$. ■

Vale ressaltar que, na proposição acima:

- se trocarmos o sinal de z, ou seja, trocarmos z por $-z$, as soluções x, y em $\mathbb{Z}$ da equação $aX + bY = c$, com $mdc(a,b) = 1$, passam a ser escritas na forma $x = x_0 - zb$, $y = y_0 + za$, com $z \in \mathbb{Z}$; e
- estas duas formas de escritas gerais das soluções x, y em $\mathbb{Z}$ da equação $aX + bY = c$, com $mdc(a,b) = 1$, geram infinitas soluções $\in \mathbb{Z}$.

Um método que sempre nos permite determinar uma solução particular para uma equação do tipo $aX + bY = c$, com $mdc(a,b) = 1$ é utilizarmos o Algoritmo de

Euclides, pois, de acordo com ele, podemos sempre determinar números inteiros d, e tais que $a \cdot d + b \cdot e = mdc(a, b) = 1$, bastando multiplicarmos ambos os membros de $a \cdot d + b \cdot e = 1$ por c, para obtermos $a \cdot c \cdot d + b \cdot c \cdot e = c$. Daí,

$$x_0 = c \cdot d \text{ e } y_0 = c \cdot e$$

é uma solução particular desejada para a equação.

O Algoritmo de Euclides também nos é apresentado durante as séries do ensino fundamental, porém ele não nos é apresentado como Algoritmo de Euclides, e é trabalhado de outras formas e não em conjunto com o *mdc*.

> Quando os coeficientes de x e de y numa equação diofantina linear não são ambos positivos, sua resolução pode ser feita mais facilmente observando que: se (x_0, y_0) é solução de $ax + by = c$, então $(-x_0, y_0)$, $(x_0, -y_0)$ e $(-x_0, -y_0)$ são soluções respectivamente de $-ax + by = c$, $ax - by = c$ e $-ax - by = c$. (DOMINGUES, 1991, p. 121).

Exemplo 4.2. Determine uma solução particular qualquer e as expressões que determinam todas as soluções para a equação $3x + 5y = 300$, com $x, y \in \mathbb{Z}$

Solução: Podemos afirmar que a equação $3x + 5y = 300$, com $x, y \in \mathbb{Z}$, possui solução, pois temos que $mdc(3, 5) = 1$.

Para determinarmos uma solução particular (x_0, y_0), utilizamos o algoritmo de Euclides por onde temos que:

i) $3 = 1 \cdot 5 - 2 \Rightarrow 2 = 1 \cdot 5 - 1 \cdot 3$;

ii) $5 = 2 \cdot 2 + 1 \Rightarrow 1 = 1 \cdot 5 - 2 \cdot 2$; e

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

Agora, multiplicando ambos membros da última igualdade acima por 300, obtemos

$$2 \cdot 3 \cdot 300 - 1 \cdot 5 \cdot 300 = 1 \cdot 300 \Rightarrow 3 \cdot 600 + 5 \cdot (-300) = 300,$$

de onde podemos afirmar que:

1) $x_0 = 2 \cdot 300 = 600$ e $y_0 = -1 \cdot 300 = -300$ é uma solução particular da equação $3x + 5y = 300$; e,
2) consequentemente, $x = 600 + 5z$ e $y = -300 - 3z$, com $z \in \mathbb{Z}$, são expressões que geram todas as soluções da equação $3x + 5y = 300$.

Portanto, $x_0 = 600$ e $y_0 = -500$ é uma solução particular da equação diofantina linear $3x + 5y = 300$ e $x = 600 + 5z$ e $y = -300 - 3z$, com $z \in \mathbb{Z}$, são as expressões que geram todas as soluções desta equação. □

Exemplo 4.3. No intuito de melhorar as vacinas contra a covid-19, um laboratório, para examinar amostras de sangue, dispõe de 2 máquinas distintas que, quando acionadas de cada vez: uma examina 15 amostras e outra examina 25 amostras. Qual é a quantidade de vezes que estas máquinas deverão ser acionadas para examinar um total de 1 mil e 500 amostras?

Solução: Podemos solucionar o problema resolvendo a equação $15x + 25y = 1500$, com $x, y \in \mathbb{Z}^+$, onde x representaria a quantidade de vezes que a primeira máquina seria acionada e y representaria a quantidade de vezes que a segunda máquina seria acionada.

Sendo assim, podemos perceber que a equação $15x + 25y = 1500$ é equivalente a equação $3x + 5y = 300$, solucionada no exercício anterior, porém nem todas as soluções desta segunda equação servem para a primeira, visto que não existe uma quantidade negativa de vezes de acionar máquinas.

Com isto, podemos afirmar que as soluções devem ser pares x, y de números inteiros não negativos, variando desde a primeira máquina sem ser acionada e a segunda máquina sendo acionada 60 vezes até o caso em que a primeira máquina é acionada 100 vezes e a segunda máquina não é acionada.

Daí, temos que $0 \leqslant x \leqslant 100$ e $0 \leqslant y \leqslant 60$, mas também nem todos estes valores inteiros servem para a solução.

Deste modo, tomemos (x_0, y_0) como uma solução particular, onde x_0 é o menor valor possível para x, que no caso é $x_0 = 0$, e obtemos $y_0 = 60$, maior valor de y, ao resolvermos a equação

$$15x + 25y = 1500 \Rightarrow 15x_0 + 25y_0 = 1500 \Rightarrow$$

$$15 \cdot 0 + 25y_0 = 1500 \Rightarrow 25y_0 = 1500 \Rightarrow y_0 = \frac{1500}{25} \Rightarrow y_0 = 60.$$

Daí, as demais soluções da equação são da forma $x = x_0 + 5z, y = y_0 - 3z \Rightarrow x = 0 + 5z = 5z, y = 60 - 3z$, com $z \in \mathbb{N} \cup \{0\}$, $0 \leqslant z \leqslant 20$, $0 \leqslant x \leqslant 100$ e $0 \leqslant y \leqslant 60$, ou seja, o conjunto solução S será formado por vinte e um pares (x, y) relacionados a seguir:

$$S = \{(0, 60), (5, 57), (10, 54), (15, 51), (20, 48), (25, 45), (30, 42), (35, 39), (40, 36), (45, 33),$$
$$(50, 30), (55, 27), (60, 24), (65, 21), (70, 18), (75, 15), (80, 12), (85, 9), (90, 6), (95, 3), (100, 0)\}.$$

Observemos aqui que o maior valor de z pode ser determinado efetuando uma das divisões:

- $100 \div 5 = 20$, onde 100 é o valor máximo de x, 5 é o valor de b e 20 é o valor máximo de z; ou
- $60 \div 3 = 20$, onde 60 é o valor máximo de y, 3 é o valor de a e 20 é o valor máximo de z,

o que gera os vinte e um possíveis pares (x, y) para determinar o conjunto solução S, pois $z \in \mathbb{N} \cup \{0\}$ e $0 \leqslant z \leqslant 20$, ou seja, z pode assumir qualquer valor inteiro de 0 a 20.

Portanto, a quantidade de vezes que as duas máquinas deverão ser acionadas para examinar um total de 1500 amostras é um dos pares (x, y), onde x é a quantidade de vezes que a primeira máquina deve ser acionada e y é a quantidade de vezes que a segunda máquina deve ser acionada, tomado junto ao conjunto solução S acima relacionado, possuindo um total de vinte e uma possibilidades. □

Observemos também, no exemplo acima, como mostramos no final da seção

do Máximo Divisor Comum, que os valores de x são múltiplos de 5 variando de 0 a 100, em ordem crescente, enquanto os valores de y são múltiplos de 3 variando de 0 a 60 em ordem decrescente, ou seja, como

$$mdc(15, 25) = 5 \Rightarrow mdc(5 \cdot 3, 5 \cdot 5) = 5 \Rightarrow 5 \cdot mdc(3, 5) = 5 \Rightarrow mdc(3, 5) = 1,$$

então podemos escrever $5 = mdc(15, 25)$ como múltiplo de 3 somado com um múltiplo de 5, isto é, $5 = 3 \cdot 5 + 5 \cdot (-2)$.

Exemplo 4.4. Em decorrência da pandemia, uma empresa resolveu ajudar seus funcionários com um auxílio alimentação em tíquetes na quantia de $R\$550,00$. Sabendo que a empresa disponibiliza tíquetes de $R\$50,00$ e $R\$150,00$, de quantas formas distintas a empresa pode entregar o auxílio de $R\$550,00$ aos seus funcionários?

Solução: Podemos solucionar o problema resolvendo a equação $50x + 150y = 550$, com $x, y \in \mathbb{Z}^+$, onde x representaria a quantidade de tíquetes de $R\$50,00$ e y representaria a quantidade de tíquetes de $R\$150,00$.

Sendo assim, podemos perceber que a equação $50x + 150y = 550$ é equivalente a equação $x + 3y = 11$, porém nem todas as soluções desta segunda equação servem para a primeira, visto que não existe uma quantidade negativa de tíquetes.

Observemos que

i) se a quantidade de tíquetes de $R\$50,00$ for 0 (zero), não temos como obter $R\$550,00$ somente com tíquetes de $R\$150,00$, mas se a quantidade de tíquetes de $R\$150,00$ for 0 (zero), conseguimos obter $R\$550,00$ somente com tíquetes de $R\$50,00$, no caso com 11 tíquetes. Então, tomemos esta solução como uma solução particular x_0, y_0, com $x_0 = 11$ e $y_0 = 0$;

ii) se a quantidade de tíquetes de $R\$50,00$ for 12, totaliza o valor de $R\$600,00$, o que nos mostra no máximo esta quantidade sendo 11; e

iii) se a quantidade de tíquetes de $R\$150,00$ for 4, totaliza o valor de $R\$600,00$, o que nos mostra no máximo esta quantidade sendo 3.

Daí, as demais soluções da equação são da forma $x = x_0 - 3z, y = y_0 + z \Rightarrow x = 11 - 3z, y = 0 + z = z$, com $z \in \mathbb{N} \cup \{0\}$, $0 \leqslant z \leqslant 3$, $0 \leqslant x \leqslant 11$ e $0 \leqslant y \leqslant 3$, ou seja, o conjunto solução S será formado por quatro pares (x, y) relacionados a seguir:

$$S = \{(11, 0), (8, 1), (5, 2), (2, 3)\}.$$

Neste caso, podemos perceber que o maior valor de z é 3, pois, como o maior valor de y é 3, temos

$$y = y_0 + z \Rightarrow 3 = 0 + z \Rightarrow z = 3,$$

o que gera os quatro possíveis pares (x, y) os quais determinam o conjunto solução S, pois $z \in \mathbb{N} \cup \{0\}$ e $0 \leqslant z \leqslant 3$, ou seja, z pode assumir qualquer valor inteiro de 0 a 3.

Portanto, a empresa pode entregar o auxílio de $R\$550,00$ aos seus funcionários de quatro formas distintas. □

Observemos também, no exemplo acima, como mostramos no final da seção do Máximo Divisor Comum, que os valores de x são múltiplos de 3 adicionados de um múltiplo de 1 e variando de 2 a 11, em ordem decrescente (por exemplo, $11 = 3{\cdot}4{+}1{\cdot}(-1)$; $8 = 3 \cdot 3 + 1 \cdot (-1)$; $5 = 3 \cdot 2 + 1 \cdot (-1)$; $2 = 3 \cdot 1 + 1 \cdot (-1)$), enquanto os valores de y são múltiplos de 1 variando de 0 a 3 em ordem crescente, ou seja, como

$$mdc(50, 150) = 50 \Rightarrow mdc(1 \cdot 50, 3 \cdot 50) = 50 \Rightarrow 50 \cdot mdc(1, 3) = 50 \Rightarrow mdc(1, 3) = 1,$$

então podemos escrever $50 = mdc(50, 150)$ como um múltiplo de 1 somado a um múltiplo de 3 adicionado de um múltiplo de 1 ou simplesmente como um múltiplo de 1 somado a um múltiplo de 3, isto é, $50 = 1 \cdot 1 + 3 \cdot 16 + 1 \cdot 1 = 1 \cdot 2 + 3 \cdot 16$.

Exemplo 4.5. Considere que os ingressos de um cinema custam $R\$9,00$ para estudantes e $R\$15,00$ para o público geral, e que, em certo dia, durante determinado período, a arrecadação nas bilheterias desse cinema foi de $R\$6000,00$. Determine quais o maior e o menor números de ingressos que foram vendidos neste dia, sabendo que um mínimo de 100 ingressos de cada tipo foram vendidos.

Solução: Podemos solucionar o problema resolvendo a equação $9x + 15y = 6000$, com $x, y \in \mathbb{Z}^+$, onde x representaria a quantidade de ingressos para estudantes e y representaria a quantidade de ingressos para o público geral.

Sendo assim, podemos perceber que a equação $9x+15y = 6000$ é equivalente a equação $3x+5y = 2000$, porém nem todas as soluções desta segunda equação servem para a primeira, visto que não existe uma quantidade negativa de ingressos, além de existir aqui um número mínimo de ingressos de cada tipo.

Com isto, podemos afirmar que as soluções devem ser pares x, y de números inteiros não negativos, variando desde a quantidade de 100 ingressos para estudantes e a quantidade de 340 ingressos para o público geral até o caso em que a a quantidade de 100 ingressos para o público geral e a quantidade de 500 ingressos para estudantes.

Estes valores podem ser obtidos da seguinte forma, como devem ser utilizadas um mínimo de 100 ingressos de cada tipo, então, na equação $3x+5y = 2000$ substituímos

1°) o valor de x por 100 e calcula-se o valor para y, como 100 é a quantidade mínima de x, então o valor y a ser determinado será máximo;

2°) o valor de y por 100 e calcula-se o valor para x, como 100 é a quantidade mínima de y, então o valor x a ser determinado será máximo.

Daí, temos que $100 \leqslant x \leqslant 500$ e $100 \leqslant y \leqslant 340$, mas também nem todos os valores naturais servem para a solução.

Deste modo, tomemos (x_0, y_0) como uma solução particular, onde x_0 é o menor valor possível para x, que no caso é $x_0 = 100$, e y_0 é o maior valor de y, que no caso é $y_0 = 340$, ao resolvermos a equação

$$9x + 15y = 6000 \Rightarrow 3x_0 + 5y_0 = 2000 \Rightarrow$$

$$3.100 + 5y_0 = 2000 \Rightarrow 5y_0 = 1700 \Rightarrow y_0 = \frac{1700}{5} \Rightarrow y_0 = 340.$$

Daí, as demais soluções da equação são da forma $x = x_0 + 5z, y = y_0 - 3z \Rightarrow$ $x = 100+5z, y = 340-3z$, com $z \in \mathbb{N}\cup\{0\}$, $0 \leqslant z \leqslant 80$, $100 \leqslant x \leqslant 500$ e $100 \leqslant y \leqslant 340$, ou seja, o conjunto solução S será formado por oitenta e um pares (x, y) da seguinte forma:

$$S = \{(100, 340), (105, 337), (110, 334), ..., (490, 106), (495, 103), (500, 100)\},$$

onde todos os valores de x são múltiplos de 5, isto é $x = 100 + 5z = 5 \cdot (20 + z)$ e todos os valores de y são um múltiplo de 5 somado a um múltiplo de 3 (por exemplos, $340 = 5 \cdot 71 + 3 \cdot (-5)$; $100 = 5 \cdot 23 + 3 \cdot (-5)$).

Observemos aqui que o maior valor de z pode ser determinado efetuando uma das equações:

- $x = x_0 + 5z$, onde 500 é o valor máximo de x, 100 é o valor de x_0 e 80 é o valor máximo de z ou seja, $500 = 100 + 5z \Rightarrow 5z = 400 \Rightarrow z = 80$; ou
- $y = y_0 - 3z$, onde 100 é o valor mínimo de y, 340 é o valor de y_0 e 80 é o valor máximo de z ou seja, $100 = 340 - 3z \Rightarrow 3z = 240 \Rightarrow z = 80$,

o que gera oitenta e um possíveis pares (x, y) os quais determinam o conjunto solução S, pois $z \in \mathbb{N} \cup \{0\}$ e $0 \leqslant z \leqslant 80$, ou seja, z pode assumir qualquer valor inteiro de 0 a 80.

Como a questão solicita o cálculo do maior e do menor números de ingressos que foram vendidos no dia, com uma venda mínima de 100 ingressos de cada tipo, podemos fazê-lo apenas com as quantidades máxima e mínima de cada tipo de ingressos já determinadas, ou seja, x máximo + y mínimo e y máximo + x mínimo, que nos dá os valores de $100+340 = 440$ e $500+100 = 600$, sendo 440 a quantidade mínima de ingressos vendidos e 600 a quantidade máxima de ingressos vendidos no dia.

Portanto, 440 é a quantidade mínima de ingressos vendidos e 600 é a quantidade máxima de ingressos vendidos no dia, obtidos a partir da soma $x + y$ tomados dos pares (x, y), junto ao conjunto solução S acima descrito, possuindo um total de oitenta e uma possibilidades. □

Observemos que para restringirmos os valores de z, também podemos utilizar o seguinte procedimento, como o número mínimo de cada garrafa deve ser 100 unidades, façamos então:

i) $100 + 5z \geqslant 100 \Rightarrow 5z \geqslant 0 \Rightarrow z \geqslant 0$;

ii) $340 - 3z \geqslant 100 \Rightarrow -3z \geqslant -240 \Rightarrow z \leqslant 80$,

ou seja, $0 \leqslant z \leqslant 80$.

Observemos também que ao analisarmos os valores de z, temos que

⋈ quanto menor for o valor de z, menor será o número de ingressos para estudantes e maior será o o número de ingressos para o público geral, ou seja, quando $z = 0$, ao substituirmos este valor na solução geral temos $x = 100 + 5 \cdot 0 \Rightarrow x = 100$ e $y = 340 - 3 \cdot 0 \Rightarrow y = 340$, totalizando 440 ingressos; e

⋈ quanto maior o valor de z, maior será o número de ingressos para estudantes e menor

será o o número de ingressos para o público geral, ou seja, quando $z = 80$, ao substituirmos este valor na solução geral temos $x = 100 + 5 \cdot 80 \Rightarrow x = 100 + 400 \Rightarrow x = 500$ e $y = 340 - 3 \cdot 80 \Rightarrow y = 340 - 240 \Rightarrow y = 100$, totalizando 600 ingressos.

E, por fim, observemos ainda, como mostramos no final da seção do Máximo Divisor Comum, que

$$mdc(9, 15) = 3 \Rightarrow mdc(3 \cdot 3, 3 \cdot 5) = 3 \Rightarrow 3 \cdot mdc(3, 5) = 3 \Rightarrow mdc(3, 5) = 1,$$

ou seja, então podemos escrever $3 = mdc(9, 15)$ como múltiplo de 3 somado a um múltiplo de 5, isto é, $3 = 3 \cdot 6 + 5 \cdot (-3)$.

Exemplo 4.6. A moeda de um determinado país é o dynamund e suas cédulas são apenas de 4 dynamumds e de 7 dynamumds. A partir de quantos dynamunds é possível pagar qualquer quantia sem receber troco?

Antes de solucionarmos esta situação-problema, com o intuito de facilitar a realização dos cálculos, devemos apresentar as definições, as proposições, o teorema e os corolários que se seguem.

Como vimos nos exemplos acima, às vezes se faz necessário solucionarmos equações diofantinas lineares $aX + bY = c$, onde $a, b, c \in \mathbb{N}$ no conjunto $\mathbb{N} \cup \{0\}$.

Proposição 4.3. *Sejam $a, b \in \mathbb{N}$, com $mdc(a, b) = 1$. Temos que todo e qualquer número inteiro c pode ser unicamente escrito na forma*

$$c = d \cdot a + e \cdot b,$$

com $d, e \in \mathbb{Z}$ e $0 \leqslant d \leqslant b$.

Demonstração: Já sabemos que existem $f, g \in \mathbb{Z}$ tais que $f \cdot a + g \cdot b = mdc(a, b) = 1$. Agora, ao multiplicarmos ambos membros de $f \cdot a + g \cdot b = 1$ por c, obtemos $c \cdot f \cdot a + c \cdot g \cdot b = c$. Temos também, pelo algoritmo da divisão euclidiana, que existem $q, r \in \mathbb{Z}$, com $0 \leqslant r \leqslant b$, tais que $c \cdot f = q \cdot b + r$. Substituindo isto em $c \cdot f \cdot a + c \cdot g \cdot b = c$, obtemos

$$\begin{gathered} c \cdot f \cdot a + c \cdot g \cdot b = c \Rightarrow \\ (q \cdot b + r) \cdot a + c \cdot g \cdot b = c \Rightarrow \\ q \cdot b \cdot a + r \cdot a + c \cdot g \cdot b = c \Rightarrow \\ r \cdot a + (q \cdot a + c \cdot g) \cdot b = c. \end{gathered}$$

Fazendo, $d = r$ e $e = q \cdot a + c \cdot g$, temos que

$$\begin{gathered} r \cdot a + (q \cdot a + c \cdot g) \cdot b = c \Rightarrow \\ c = d \cdot a + e \cdot b, \end{gathered}$$

com $0 \leqslant d \leqslant b$ e $d, e \in \mathbb{Z}$.

O que prova a existência de $c = d \cdot a + e \cdot b$, com $d, e \in \mathbb{Z}$ e $0 \leqslant d \leqslant b$.

Agora, suponhamos que existam $h, i \in \mathbb{Z}$, tais que $d \cdot a + e \cdot b = h \cdot a + i \cdot b$, com $0 \leqslant d, h \leqslant b$.

Daí, temos que

$$d \cdot a + e \cdot b = h \cdot a + i \cdot b \Rightarrow$$

$$d \cdot a - h \cdot a = i \cdot b - e \cdot b \Rightarrow$$
$$(d - h) \cdot a = (i - e) \cdot b,$$

com $\mid d - h \mid < b$.

Como, pelo enuciado da proposição, $mdc(a, b) = 1$, então devemos ter que

i) $b \mid d - h$, que só pode acontecer se $d = h$; e

ii) $a \mid i - e$, que só pode acontecer se $i = e$.

O que prova a unicidade de $c = d \cdot a + e \cdot b$, com $d, e \in \mathbb{Z}$ e $0 \leqslant d \leqslant b$.

Portanto, sendo $a, b \in \mathbb{N}$, com $mdc(a, b) = 1$, temos que todo e qualquer número inteiro c pode ser unicamente escrito na forma $c = d \cdot a + e \cdot b$, com $d, e \in \mathbb{Z}$ e $0 \leqslant d \leqslant b$. ■

Definição 4.3. Sejam $a, b \in \mathbb{N}$. Temos que

$$S(a, b) = \{d \cdot a + e \cdot b; d, e \in \mathbb{N} \cup \{0\}\},$$

é o conjunto semigrupo gerado por a e b.

Definição 4.4. Sejam $a, b \in \mathbb{N}$. Temos que

$$L(a, b) = \mathbb{N}/S(a, b),$$

é o conjunto de lacunas de $S(a, b)$.

A equação $aX + bY = c$, com $mdc(a, b) = 1$ tem solução no conjunto $\mathbb{N} \cup \{0\}$ se, e somente se, $c \in S(a, b)$. Sendo assim, caracterizemos os elementos de $S(a, b)$.

Proposição 4.4. *Temos que $c \in S(a, b)$, se, e somente se, existem $f, g \in \mathbb{N} \cup \{0\}$, com $f < b$, determinados univocamente por c, tais que $c = f \cdot a + g \cdot b$.*

Demonstração: Se temos $c = f \cdot a + g \cdot b$, com $f, g \in \mathbb{N} \cup \{0\}$, então temos que $c \in S(a, b)$.

Por outro lado, se temos $c \in S(a, b)$, então temos que c é da forma $c = h \cdot a + i \cdot b$, com $h, i \in \mathbb{N} \cup \{0\}$.

Temos, pelo algoritmo da divisão euclidiana, que $h = q \cdot b + r$, com $0 \leqslant r \leqslant b$ e substituindo este resultado em $c = h \cdot a + i \cdot b$, obtemos,

$$c = h \cdot a + i \cdot b \Rightarrow$$
$$c = (q \cdot b + r) \cdot a + i \cdot b \Rightarrow$$
$$c = q \cdot b \cdot a + r \cdot a + i \cdot b \Rightarrow$$
$$c = r \cdot a + (q \cdot a + i) \cdot b.$$

Fazendo, $r = f$ e $g = q \cdot a + i$, temos que

$$c = r \cdot a + (q \cdot a + i) \cdot b = c \Rightarrow$$
$$c = f \cdot a + g \cdot b,$$

com $f, g \in \mathbb{N} \cup \{0\}$, $0 \leqslant f \leqslant b$ e $g = q \cdot a + i$.

A unicidade decorre da Proposição 4.3.

Portanto, temos que $c \in S(a, b)$, se, e somente se, existem $f, g \in \mathbb{N} \cup \{0\}$, com $f < b$, determinados univocamente por c, tais que $c = f \cdot a + g \cdot b$. ■

Corolário 4.1. *Temos que $L(a, b) = \{d \cdot a - e \cdot b; d, e \in \mathbb{N}; d < b\}$.*

Demonstração: Pela Proposição 4.4, se c é da forma $c = f \cdot a + g \cdot b$, com $f, g \in \mathbb{N} \cup \{0\}$, então temos que $c \in S(a, b)$.

Então, se c for da forma $c = h \cdot a - i \cdot b$, com $h, i \in \mathbb{N}$, temos que $c \in L(a, b)$, pois vejamos que, pelo algoritmo da divisão euclidiana, que $h = q \cdot b + r$, com $0 \leqslant r \leqslant b$ e substituindo este resultado em $c = h \cdot a - i \cdot b$, obtemos,

$$c = h \cdot a - i \cdot b \Rightarrow$$
$$c = (q \cdot b + r) \cdot a - i \cdot b = c \Rightarrow$$
$$c = q \cdot b \cdot a + r \cdot a - i \cdot b = c \Rightarrow$$
$$c = r \cdot a - (i - q \cdot a) \cdot b.$$

Fazendo, $r = f$ e $g = i - q \cdot a$, temos que

$$c = r \cdot a - (i - q \cdot a) \cdot b = c \Rightarrow$$
$$c = f \cdot a - g \cdot b,$$

com $f, g \in \mathbb{N}$, $0 \leqslant f \leqslant b$ e $g = i - q \cdot a$. F A unicidade decorre da Proposição 4.3.

Logo, temos que $c \in L(a, b)$, se, e somente se, existem $d, e \in \mathbb{N}$, com $d < b$, determinados univocamente por c, tais que $c = d \cdot a - e \cdot b$ e, por definição, se $c \in L(a, b)$, então $c \notin S(a, b)$.

Portanto, temos que $L(a, b) = \{d \cdot a - e \cdot b; d, e \in \mathbb{N}; d < b\}$. ■

Teorema 4.1. *Temos que a equação $aX + bY = c$, com $mdc(a, b) = 1$, tem solução em $\mathbb{N} \cup \{0\}$ se, e somente se, $c \notin L(a, b) = \{d \cdot a - e \cdot b; d, e \in \mathbb{N}; d < b\}$.*

Demonstração: Por definição, sabemos que se $c \in S(a, b)$, então $c \notin L(a, b)$ ou se $c \in L(a, b)$, então $c \notin S(a, b)$.

Portanto, pelo Corolário 4.1, temos que dada uma equação diofantina linear $aX + bY = c$, com $mdc(a, b) = 1$, esta possui solução em $\mathbb{N} \cup \{0\}$ se, e somente se, $c \notin L(a, b) = \{d \cdot a - e \cdot b; d, e \in \mathbb{N}; d < b\}$. ■

Corolário 4.2. *Sejam $a, b \in \mathbb{N}$, com $mdc(a, b) = 1$. Temos que $(a-1) \cdot (b-1)$ é o menor número inteiro tal que $c \in S(a, b)$ para todo e qualquer $c \geqslant (a - 1) \cdot (b - 1)$.*

Demonstração: Observemos que o conjunto $L(a, b)$ é um conjunto finito com seu maior elemento da forma $maxL(a, b) = (b - 1) \cdot a - b$.

Daí, podemos concluir que, pelo Teorema 4.1 como a equação $aX + bY = c$, com $mdc(a, b) = 1$, somente possui solução em $\mathbb{N} \cup \{0\}$ se $c \notin L(a, b)$, então

$$c > maxL(a, b) = (b - 1) \cdot a - b \Rightarrow$$
$$c \geqslant (b - 1) \cdot a - b + 1 \Rightarrow$$
$$c \geqslant (b - 1) \cdot a - (b - 1) \Rightarrow$$
$$c \geqslant (a - 1) \cdot (b - 1).$$

Logo, a equação $aX + bY = c$, com $mdc(a, b) = 1$, não possui solução em $\mathbb{N} \cup \{0\}$ se $c = (a - 1) \cdot (b - 1) - 1$.

Portanto, sendo $a, b \in \mathbb{N}$, com $mdc(a, b) = 1$, temos que $(a - 1) \cdot (b - 1)$ é o menor número inteiro tal que $c \in S(a, b)$ para todo e qualquer $c \geqslant (a - 1) \cdot (b - 1)$. ■

Observemos aqui o número natural $c = (a-1)\cdot(b-1)$, chamado de condutor de $S(a,b)$, mostra-nos que o maior elemento do conjunto de lacunas de $S(a,b)$ é a lacuna $c-1 = (a-1)\cdot(b-1) = (b-1)\cdot a - b$.

Agora, podemos solucionar o Exemplo 4.6: A moeda de um determinado país é o dynamund e suas cédulas são apenas de 4 *dynamunds* e de 7 *dynamunds*. A partir de quantos *dynamunds* é possível pagar qualquer quantia sem receber troco?

Solução: Podemos solucionar o problema resolvendo a equação $4x + 7y = c$, com as variáveis $x, y \in \mathbb{N} \cup \{0\}$, onde x representaria a quantidade de cédulas de 4 *dynamunds* e y representaria a quantidade de cédulas de 7 *dynamunds*.

Temos que, pelo Corolário 4.2

- $a = 4$;
- $b = 7$;
- $mdc(4,7) = 1$;
- $c = (a-1)\cdot(b-1) = (4-1)\cdot(7-1) = 3\cdot 6 = 18$;
- $c - 1 = 18 - 1 = 17$.

Com isto, podemos afirmar que a partir de 18 *dynamunds* não existem mais lacunas no conjunto solução da equação $4x + 7y = c$ e que a maior lacuna é o valor de 17 *dynamunds*.

Portanto, a partir de 18 *dynamunds* é possível pagar qualquer quantia sem receber troco neste país. □

Observemos aqui que se tivéssemos que determinar as lacunas deveríamos fazer os seguintes cálculos:

1°) considerar o conjunto $L(4,7) = \{d\cdot 4 - e\cdot 7; d, e \in \mathbb{N}; d < 7; e < 4\}$;
2°) $d \in \{1,2,3,4,5,6\}$;
3°) $e \in \{1,2,3\}$;
4°) $d = 1$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 1\cdot 4 - 1\cdot 7 = 4 - 7 = -3$, que não serve como solução, pois é um valor negativo;
5°) $d = 2$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 2\cdot 4 - 1\cdot 7 = 8 - 7 = 1$;
6°) $d = 3$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 3\cdot 4 - 1\cdot 7 = 12 - 7 = 5$;
7°) $d = 4$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 4\cdot 4 - 1\cdot 7 = 16 - 7 = 9$;
8°) $d = 5$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 5\cdot 4 - 1\cdot 7 = 20 - 7 = 13$;
9°) $d = 6$ e $e = 1 \Rightarrow d\cdot 4 - e\cdot 7 = 6\cdot 4 - 1\cdot 7 = 24 - 7 = 17$;
10°) $d = 1$ e $e = 2 \Rightarrow d\cdot 4 - e\cdot 7 = 1\cdot 4 - 2\cdot 7 = 4 - 14 = -10$, que não serve como solução, pois é um valor negativo;
11°) $d = 2$ e $e = 2 \Rightarrow d\cdot 4 - e\cdot 7 = 2\cdot 4 - 2\cdot 7 = 8 - 14 = -6$, que não serve como solução, pois é um valor negativo;
12°) $d = 3$ e $e = 2 \Rightarrow d\cdot 4 - e\cdot 7 = 3\cdot 4 - 2\cdot 7 = 12 - 14 = -2$, que não serve como solução, pois é um valor negativo;

13°) $d = 4$ e $e = 2 \Rightarrow d \cdot 4 - e \cdot 7 = 4 \cdot 4 - 2 \cdot 7 = 16 - 14 = 2$;

14°) $d = 5$ e $e = 2 \Rightarrow d \cdot 4 - e \cdot 7 = 5 \cdot 4 - 2 \cdot 7 = 20 - 14 = 6$;

15°) $d = 6$ e $e = 2 \Rightarrow d \cdot 4 - e \cdot 7 = 6 \cdot 4 - 2 \cdot 7 = 24 - 14 = 10$;

16°) $d = 1$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 1 \cdot 4 - 3 \cdot 7 = 4 - 21 = -17$, que não serve como solução, pois é um valor negativo;

17°) $d = 2$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 2 \cdot 4 - 3 \cdot 7 = 8 - 21 = -13$, que não serve como solução, pois é um valor negativo;

18°) $d = 3$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 3 \cdot 4 - 3 \cdot 7 = 12 - 21 = -9$, que não serve como solução, pois é um valor negativo;

19°) $d = 4$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 4 \cdot 4 - 3 \cdot 7 = 16 - 21 = -5$, que não serve como solução, pois é um valor negativo;

20°) $d = 5$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 5 \cdot 4 - 3 \cdot 7 = 20 - 21 = -1$, que não serve como solução, pois é um valor negativo; e

21°) $d = 6$ e $e = 3 \Rightarrow d \cdot 4 - e \cdot 7 = 6 \cdot 4 - 3 \cdot 7 = 24 - 21 = 3$.

Portanto, temos que $L(4, 7) = \{1, 2, 3, 5, 6, 9, 10, 13, 17\}$.

Com isto, c não pode assumir nenhum destes valores para que a equação diofantina linear $4x + 7y = c$ possua solução em $\mathbb{N} \cup \{0\}$.

Quando estudamos equações diofantinas lineares com duas variáveis, podemos associá-las a uma função polinomial do 1° grau, por esta poder ser escrita na forma $ax + by = c$, com $a, b, c \in \mathbb{R}$. Porém, os conjuntos numéricos em que cada tipo de equação é definida são distintos. Observemos aqui que função polinomial do 1° grau é outro conteúdo apresentado no ensino fundamental e trabalhado e desenvolvido tanto no ensino fundamental e quanto no ensino médio.

Sendo assim, podemos afirmar que toda equação diofantina linear com duas variáveis pode ser associada a uma função polinomial do 1° grau fazendo-se a restrição das variáveis x e y pertencerem ao conjunto $\mathbb{Z}$, ou seja, as soluções inteiras de uma função polinomial do 1° grau são soluções de uma equação diofantina linear com duas variáveis associada a ela, ou ainda, permitindo-se que as variáveis x e y de uma equação diofantina pertençam ao conjunto $\mathbb{R}$ obtemos uma função polinomial do 1° grau.

Um outro detalhe deve ser considerado aqui. Não podemos tomar valores pertencentes ao conjunto $\mathbb{I}$ para os coeficientes a e b de uma função diofantina, salvo se os valores forem números comensuráveis, como veremos mais adiante, pois, assim, não existirá uma função polinomial do 1° grau associada a esta equação diofantina. Logo, podemos afirmar que a solução de uma equação diofantina linear com duas variáveis é formada pelo conjunto de pares cartesianos (x, y) da função polinomial do 1° grau que possua os mesmos coeficientes $a, b \in \mathbb{Z}$ da equação $ax + by = c$, com $x, y \in \mathbb{Z}$.

Exemplo 4.7. Determinar a solução geral para equação diofantina $3x + 2y = 7$, associar esta a uma função polinomial do 1° grau $f : \mathbb{R} \to \mathbb{R}$ e mostrar que exitem pares cartesianos que satisfazem à função polinomial do 1° grau, mas que não pertencem ao conjunto solução

da equação diofantina.

Solução: Inicialmente, temos que $mdc(3,2) = 1$ e $1 \mid 7$, ou seja, a equação diofantina $3x + 2y = 7$ possui infinitas soluções em $\mathbb{Z}$. Pelo Algoritmo de Euclides, temos que $1 = 3 \cdot (1) + 2 \cdot (-1)$ e que multiplicando ambos membros desta igualdade por 7, obtemos $7 = 3 \cdot (7) + 2 \cdot (-7)$, e, daí, a solução geral da equação é $x = 7 + 2z$ e $y = -7 - 3z$, com $z \in \mathbb{Z}$, onde para

i) $z = -3$, temos que $x = 7 + 2z = 7 + 2 \cdot (-3) = 1$ e $y = -7 - 3z = -7 - 3 \cdot (-3) = 2$, $(1, 2)$ é solução para equação diofantina $3x + 2y = 7$;

ii) $z = -2$, temos que $x = 7 + 2z = 7 + 2 \cdot (-2) = 3$ e $y = -7 - 3z = -7 - 3 \cdot (-2) = -1$, $(3, -1)$ é solução para equação diofantina $3x + 2y = 7$;

iii) $z = -1$, temos que $x = 7 + 2z = 7 + 2 \cdot (-1) = 5$ e $y = -7 - 3z = -7 - 3 \cdot (-1) = -4$, $(5, -4)$ é solução para equação diofantina $3x + 2y = 7$;

iv) $z = 0$, temos que $x = 7 + 2z = 7 + 2 \cdot 0 = 7$ e $y = -7 - 3z = -7 - 3 \cdot 0 = -7$, $(7, -7)$ é solução para equação diofantina $3x + 2y = 7$;

v) $z = 1$, temos que $x = 7 + 2z = 7 + 2 \cdot 1 = 9$ e $y = -7 - 3z = -7 - 3 \cdot 1 = -10$, $(9, -10)$ é solução para equação diofantina $3x + 2y = 7$; e

vi) $z = 2$, temos que $x = 7 + 2z = 7 + 2 \cdot 2 = 11$ e $y = -7 - 3z = -7 - 3 \cdot 2 = -13$, $(11, -13)$ é solução para equação diofantina $3x + 2y = 7$.

Observemos aqui, que os valores de x para solução variam de 2 em 2 unidades e os valores de y para solução variam de 3 em 3 unidades.

Agora, construiremos uma tabela com alguns pares cartesianos (x, y), atribuindo valores a x e determinando os valores de y, que são solução da equação polinomial do 1° grau:

$$3x + 2y = 7 \Rightarrow 2y = 7 - 3x \Rightarrow y = \frac{7 - 3x}{2} \Rightarrow f(x) = \frac{7 - 3x}{2}.$$

Sendo assim, para

I) $x = -3$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot (-3)}{2} = \dfrac{16}{2} = 8$, $(-3, 8)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$;

II) $x = -2$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot (-2)}{2} = \dfrac{13}{2} = 6,5$, $(-2; 6,5)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$;

III) $x = -1$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot (-1)}{2} = \dfrac{10}{2} = 5$, $(-1, 5)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$;

IV) $x = 0$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot 0}{2} = \dfrac{7}{2} = 3,5$, $(0; 3,5)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$;

V) $x = 1$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot 1}{2} = \dfrac{4}{2} = 2$, $(1, 2)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$;

VII) $x = 2$, temos que $y = \dfrac{7 - 3x}{2} = \dfrac{7 - 3 \cdot 2}{2} = \dfrac{1}{2} = 0,5$, $(2; 0,5)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$; e

$VII)$ $x = 3$, temos que $y = \dfrac{7-3x}{2} = \dfrac{7-3\cdot 3}{2} = \dfrac{-2}{2} = -1$, $(3,-1)$ é par cartesiano da função polinomial do 1° grau $3x + 2y = 7$.

x	-3	-2	-1	0	1	2	3
y	8	$6,5$	5	$3,5$	2	$0,5$	-1
(x,y)	$(-3;8)$	$(-2;6,5)$	$(-1,5)$	$(0;3,5)$	$(1,2)$	$(2;0,5)$	$(3,-1)$

Analisando a função polinomial do 1° grau, podemos observar que alguns pares cartesianos (x, y) têm coordenadas inteiras as quais também são soluções da equação diofantina que possui mesmos coeficientes $a = 3$ e $b = 2$ e mesmo valor constante $c = 7$ da função polinomial do 1° grau.

Portanto, temos que a solução geral para equação diofantina $3x + 2y = 7$ é $x = 7 + 2z$ e $y = -7 - 3z$, com $z \in \mathbb{Z}$, que está associada a função polinomial do 1° grau $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = \dfrac{7-3x}{2}$ e, de acordo com os cálculos efetuados acima, existem pares cartesianos da função f que não pertencem ao conjunto solução da equação diofantina apresentada. □

Vale aqui salientar que quando determinamos uma solução particular (x_0, y_0) da equação diofantina, a partir desta solução, conseguimos encontrar todos os demais pares (x_e, y_e), com $e \in \mathbb{N}$ que também são solução da equação, pois como a solução geral é representada por $x = x_0 + \dfrac{b}{d} \cdot z$ e $y = y_0 - \dfrac{a}{d} \cdot z$, com $z \in \mathbb{Z}$ e $d = mdc(a, b)$, então basta aumentarmos ou diminuirmos $\dfrac{b}{d}$ no valor de x_0 e, respectivamente, diminuirmos ou aumentarmos $\dfrac{a}{d}$ no valor de y_0 e repetirmos este processo em cada par (x_e, y_e) encontrado, o que podemos observar na tabela construída acima.

Exemplo 4.8. Usando os conhecimentos de geometria analítica, analisar as equações diofantinas lineares $5x - 4y = c$, com $c \in \mathbb{Z}$ e mostrar que conhecendo uma solução particular em cada função polinomial do 1° grau a ela associada, podemos determinar todas as soluções das equações diofantinas $5x - 4y = c$.

Solução: Primeiramente, como o $mdc(5, -4) = 1$ e 1 divide qualquer número, então temos que c pode assumir qualquer valor inteiro que as equações diofantinas lineares $5x - 4y = c$ possuirão infinitas soluções.

Agora, tomemos alguns valores pontuais $c = 3$, $c = 7$ e $c = 15$ de modo que possamos analisar individualmente cada equação diofantina linear mas facilmente. Fazendo

► $c = 3$, temos que $5x - 4y = 3$. Se $x = 3 \Rightarrow 5x - 4y = 3 \Rightarrow 5 \cdot 3 - 4y = 3 \Rightarrow -4y = 3 - 15 \Rightarrow -4y = -12 \Rightarrow y = 3 \Rightarrow$, de onde $(x_0, y_0) = (3, 3)$ é uma solução particular para equação diofantina $5x - 4y = 3$. E se $x = -1 \Rightarrow 5x - 4y = 3 \Rightarrow 5 \cdot (-1) - 4y = 3 \Rightarrow -4y = 3 + 5 \Rightarrow -4y = 8 \Rightarrow y = -2 \Rightarrow$, de onde $(-1, -2)$ é uma solução particular para equação diofantina $5x - 4y = 3$. E se $x = -5 \Rightarrow$

$5x - 4y = 3 \Rightarrow 5 \cdot (-5) - 4y = 3 \Rightarrow -4y = 3 + 25 \Rightarrow -4y = 28 \Rightarrow y = -7 \Rightarrow$, de onde $(-5, -7)$ é uma solução particular para equação diofantina $5x - 4y = 3$;

- $c = 7$, temos que $5x - 4y = 7$. Se $x = 3 \Rightarrow 5x - 4y = 7 \Rightarrow 5 \cdot 3 - 4y = 7 \Rightarrow -4y = 7 - 15 \Rightarrow -4y = -8 \Rightarrow y = 2 \Rightarrow$, de onde $(x_0, y_0) = (3, 2)$ é uma solução particular para equação diofantina $5x - 4y = 7$. E se $x = -1 \Rightarrow 5x - 4y = 7 \Rightarrow 5 \cdot (-1) - 4y = 7 \Rightarrow -4y = 7 + 5 \Rightarrow -4y = 12 \Rightarrow y = -3 \Rightarrow$, de onde $(-1, -3)$ é uma solução particular para equação diofantina $5x - 4y = 7$. E se $x = -5 \Rightarrow 5x - 4y = 7 \Rightarrow 5 \cdot (-5) - 4y = 7 \Rightarrow -4y = 7 + 25 \Rightarrow -4y = 32 \Rightarrow y = -8 \Rightarrow$, de onde $(-5, -8)$ é uma solução particular para equação diofantina $5x - 4y = 7$; e
- $c = 15$, temos que $5x - 4y = 15$. Se $x = 3 \Rightarrow 5x - 4y = 15 \Rightarrow 5 \cdot 3 - 4y = 15 \Rightarrow -4y = 15 - 15 \Rightarrow -4y = 0 \Rightarrow y = 0 \Rightarrow$, de onde $(x_0, y_0) = (3, 0)$ é uma solução particular para equação diofantina $5x - 4y = 15$. E se $x = -1 \Rightarrow 5x - 4y = 15 \Rightarrow 5 \cdot (-1) - 4y = 15 \Rightarrow -4y = 15 + 5 \Rightarrow -4y = 20 \Rightarrow y = -5 \Rightarrow$, de onde $(-1, -5)$ é uma solução particular para equação diofantina $5x - 4y = 15$. E se $x = -5 \Rightarrow 5x - 4y = 15 \Rightarrow 5 \cdot (-5) - 4y = 15 \Rightarrow -4y = 15 + 25 \Rightarrow -4y = 40 \Rightarrow y = -10 \Rightarrow$, de onde $(-5, -10)$ é uma solução particular para equação diofantina $5x - 4y = 15$.

Observemos aqui que, pelos cálculos efetuados e pelo comentário realizado acima deste exemplo, estamos acrescentando $\dfrac{b}{mdc(5, -4)} = -4$ em x_0 e diminuindo $\dfrac{a}{mdc(5, -4)} = 5$ em y_0 respectivamente, pois temos que $mdc(5, -4) = 1$, e ao repetirmos este processo em cada solução particular determinada, obtemos todos os pares cartesianos que pertencem ao conjunto solução das equações diofantinas lineares correspondentes.

Sendo assim, como o valor de x aumenta de 4 em 4 e o valor de y aumenta de 5 em 5 e, pela geometria analítica, sabemos que o vetor $\overrightarrow{v} = (5, -4)$ é ortogonal a todas as retas $5x - 4y = c$, ou seja, as retas das funções polinomiais do 1° grau associadas, $5x - 4y = 3$, $5x - 4y = 7$ e $5x - 4y = 15$, são paralelas, então, pelo Teorema de Pitágoras, obtemos

$$d^2 = 4^2 + 5^2 \Rightarrow d^2 = 16 + 25 \Rightarrow d^2 = 41 \Rightarrow d = \sqrt{41},$$

onde d é a distância entre os pares cartesianos soluções respectivas em cada uma das equações $5x - 4y = 3$, $5x - 4y = 7$ e $5x - 4y = 15$.

Logo, temos que esta distância entre os pares cartesianos que são soluções em cada uma das equações diofantinas lineares $5x - 4y = c$ é constante e igual a $\sqrt{41}$ e podemos aplicar este procedimento utilizado para qualquer valor de $c \in \mathbb{Z}$, pois $mdc(5, -4) = 1$.

Portanto, conhecendo uma solução particular, que também seja solução da equação diofantina associada, em cada função polinomial do 1° grau associada às equações diofantinas $5x - 4y = c$, então, podemos determinar todas as soluções destas equações. □

Também podemos associar as equações diofantinas lineares com duas variáveis às progressões aritméticas (P.A.) de primeira ordem, que é uma sequência numérica na

qual a diferença entre um termo e seu termo antecessor é sempre constante, para qualquer termo da sequência em questão. Observemos aqui que P.A. do 1° grau é um conteúdo apresentado, trabalhado e desenvolvido no ensino médio.

Temos que, em uma P.A., o termo geral é dado por $a_n = a_1 + (n-1) \cdot r$, com a_n sendo o termo geral, a_1 sendo o primeiro termo, $n \in \mathbb{N}$ sendo a posição do termo a ser determinado e r sendo a razão definida por $r = a_2 - a_1 = a_3 - a_2 = ... = a_n - a_{n-1}$.

Daí, temos que $a_n = a_1 + (n-1) \cdot r \Rightarrow a_n = a_1 - r + r \cdot n \Rightarrow$ e fazendo $x = n$ e $y = a_n$, obtemos $y = a_1 - r + r \cdot x \Rightarrow -r \cdot x + y = a_1 - r$ que possui a forma de uma equação diofantina linear com duas variáveis, ou seja, $ax + by = c$, com $a = -r$, $b = 1$ e $c = a_1 - r$ e como $mdc(-r, 1) = 1$ e $1 \mid (a_1 - r)$, então a equação possui infinitas soluções.

Como $n \in \mathbb{N}$ e $-r \cdot x + y = a_1 - r$ está associada a $ax + by = c$, então temos que a solução geral é dada por $x = x_0 + bz \Rightarrow x = 1 + z$ e $y = y_0 - a \cdot z \Rightarrow y = a_1 + r \cdot z$, com $z \in \mathbb{N}$, pois sempre $a = -r$, $b = 1$, $x_0 = 1$ e $y_0 = a_1$.

Com isto, podemos afirmar que toda equação diofantina linear com duas variáveis da forma $ax + y = c$, com $x \in \mathbb{N}$ e $y \in \mathbb{Z}$ está associada a uma progressão aritmética.

Porém, se tomarmos uma P.A. que possui qualquer termo sendo um número decimal, então, já que em uma equação diofantina linear $y \in \mathbb{Z}$ e $y = a_n$, teremos que esta P.A. não está associada a alguma equação diofantina linear com duas variáveis. Em outras palavras, se pelo menos um dos valores de $y = a_n$ de uma P.A. de primeira ordem pertencerem ao conjunto $\mathbb{Q}$, não existe associação alguma desta P.A. com uma equação diofantina linear, pois as soluções das equações diofantinas lineares pertencem ao conjunto dos números inteiros.

Exemplo 4.9. Determinar a equação diofantina linear associada a P.A. $(5, 8, 11, 14, ...)$ e sua solução geral.

Solução: Pelo enunciado, temos que, na P.A., $a_1 = 5$, $r = 3$ que determinam o termo geral $a_n = a_1 + (n-1) \cdot r \Rightarrow a_n = 5 + (n-1) \cdot 3 \Rightarrow a_n = 5 + 3n - 3 \Rightarrow a_n = 2 + 3n$. Fazendo $x = n$ e $y = a_n$, obtemos $y = 2 + 3x \Rightarrow -3x + y = 2$.

Daí, temos que a solução geral da equação é dada por $x = x_0 + z \Rightarrow x = 1 + z$ e $y = y_0 + r \cdot z \Rightarrow y = 5 + 3z$, com $z \in \mathbb{N}$, pois $x_0 = 1$, $y_0 = a_1 = 5$ e $r = 3$.

Portanto, a equação diofantina $-3x+y = 2$ está associada a P.A. $(5, 8, 11, 14, ...)$ e sua solução geral é $x = 1 + z$ e $y = 5 + 3z$, com $z \in \mathbb{N}$. □

Exemplo 4.10. Sabendo que uma P.A. é determinada pelo termo geral $a_n = 4 + 5n$, determinar a equação diofantina linear associada e sua solução geral.

Solução: Pelo enunciado, temos que, na P.A., $a_n = 4 + 5n$, onde o número multiplicando n é a razão da P.A., ou seja, $r = 5$ e daí, calculando a_1, temos que para $n = 1$

$$a_n = 4 + 5n \Rightarrow a_1 = 4 + 5 \cdot 1 \Rightarrow a_1 = 9.$$

Fazendo $x = n$ e $y = a_n$, obtemos $y = 4 + 5x \Rightarrow -5x + y = 4$.

Daí, temos que a solução geral da equação é dada por $x = x_0 + z \Rightarrow x = 1 + z$ e $y = y_0 + r \cdot z \Rightarrow y = 9 + 5z$, com $z \in \mathbb{N}$, pois $x_0 = 1$, $y_0 = a_1 = 9$ e $r = 5$.

Portanto, a equação diofantina $-5x + y = 4$ está associada a P.A. determinada pelo termo geral $a_n = 4 + 5n$ e sua solução geral é $x = 1 + z$ e $y = 9 + 5z$, com $z \in \mathbb{N}$. □

Exemplo 4.11. Determinar a P.A. e seu termo geral associados a equação diofantina linear $2x + y = 5$.

Solução: Para associar a equação diofantina linear $2x + y = 5$ a uma P.A., esta equação deve respeitar a fórmula $-r \cdot x + y = a_1 - r$. Daí, temos que $r = -a = -2$ e $c = a_1 - r = 5 \Rightarrow a_1 + 2 = 5 \Rightarrow a_1 = 3$.

Agora, fazendo $x = n$ e $y = a_n$, temos que o termo geral da P.A. será:

$$2x + y = 5 \Rightarrow 2n + a_n = 5 \Rightarrow a_n = 5 - 2n,$$

de onde obtemos

- para n = 2, $a_n = 5 - 2n \Rightarrow a_2 = 5 - 2 \cdot 2 \Rightarrow a_2 = 1$;
- para n = 3, $a_n = 5 - 2n \Rightarrow a_3 = 5 - 2 \cdot 3 \Rightarrow a_3 = -1$;
- para n = 4, $a_n = 5 - 2n \Rightarrow a_2 = 5 - 2 \cdot 4 \Rightarrow a_2 = -3$; e assim por diante.

Logo a P.A. associada a equação diofantina linear $2x + y = 5$ é $(3, 1, -1, -3, ...)$.

Portanto, a equação diofantina $2x + y = 5$ está associada a P.A. $(3, 1, -1, -3, ...)$, que é determinada pelo termo geral $a_n = 5 - 2n$. □

Exemplo 4.12 (Enem 2021)**.** Um lava-rápido oferece dois tipos de lavagem de veículos: lavagem simples, ao preço de $R\$20,00$ e lavagem completa, ao preço de $R\$35,00$. Para cobrir as despesas com produtos e funcionários e não ter prejuízos, o lava-rápido deve ter uma receita diária de, pelo menos, $R\$300,00$.

Para não ter prejuízos, o menor número de lavagens diárias que o lava-rápido deve efetuar é

a) 6.

b) 8.

c) 9.

d) 15.

e) 20.

Solução: Podemos solucionar o problema resolvendo a equação $20x + 35y \geqslant 300$, com $x, y \in \mathbb{N} \cup \{0\}$, onde x representaria a quantidade de lavagens simples e y representaria a quantidade de lavagens completas.

Sendo assim, podemos perceber que a equação $20x + 35y \geqslant 300$ é equivalente a equação $4x + 7y \geqslant 60$, porém nem todas as soluções desta segunda equação servem para a primeira, visto que não existe uma quantidade negativa de lavagens.

Observemos que

i) se a quantidade de lavagens simples for 0 (zero), então obtemos $4x + 7y \geqslant 60 \Rightarrow 4 \cdot 0 + 7y \geqslant 60 \Rightarrow y \geqslant \frac{60}{7} \Rightarrow y \geqslant 8,571428571428...$, ou seja, 9 lavagens completas, totalizando uma receita diária de $9 \cdot R\$35,00 = R\$315,00$;

ii) se a quantidade de lavagens simples for 1 (uma), então obtemos $4x + 7y \geqslant 60 \Rightarrow 4 \cdot 1 + 7y \geqslant 60 \Rightarrow y \geqslant \frac{56}{7} \Rightarrow y \geqslant 8$, ou seja, 8 lavagens completas, totalizando uma receita diária de $1 \cdot R\$20,00 + 8 \cdot R\$35,00 = R\$20,00 + R\$280,00 = R\$300,00$;

iii) se a quantidade de lavagens simples for 2 (duas), então obtemos $4x + 7y \geqslant 60 \Rightarrow 4 \cdot 2 + 7y \geqslant 60 \Rightarrow y \geqslant \frac{52}{7} \Rightarrow y \geqslant 7,428571428571...$, ou seja, 8 lavagens completas, totalizando uma receita diária de $2 \cdot R\$20,00 + 8 \cdot R\$35,00 = R\$40,00 + R\$280,00 = R\$320,00$; e

iv) se a quantidade de lavagens simples for 3 (duas), então obtemos $4x + 7y \geqslant 60 \Rightarrow 4 \cdot 3 + 7y \geqslant 60 \Rightarrow y \geqslant \frac{48}{7} \Rightarrow y \geqslant 6,857142857142...$, ou seja, 7 lavagens completas, totalizando uma receita diária de $3 \cdot R\$20,00 + 7 \cdot R\$35,00 = R\$60,00 + R\$245,00 = R\$305,00$.

Sendo assim, para o lava-rápido possuir uma receita diária igual ou superior a $R\$300,00$, o número mínimo de lavagens é 9, isto podendo acontecer de duas formas: sendo nenhuma lavagem simples e 9 lavagens completas ou sendo 1 lavagem simples e 8 lavagens completas.

Observemos que com 2 lavagens simples seriam necessárias ainda 8 lavagens completas, totalizando 10 lavagens, mas não pode ser a resposta da questão, pois é solicitado o menor número de lavagens.

Vejamos também que se forem realizadas 2 lavagens simples e 7 lavagens completas, não obtemos a receita diária desejada, pois $2 \cdot R\$20,00 + 7 \cdot R\$35,00 = R\$40,00 + R\$245,00 = R\$285,00$, o mesmo acontecendo se forem realizadas 3 lavagens simples e 6 lavagens completas, obtemos a receita diária de $3 \cdot R\$20,00 + 6 \cdot R\$35,00 = R\$60,00 + R\$210,00 = R\$270,00$.

Portanto, para não ter prejuízos, o menor número de lavagens diárias que o lava-rápido deve efetuar é 9, ou seja, alternativa correta letra c. □

4.2 EQUAÇÕES DIOFANTINAS LINEARES COM COEFICIENTES RACIONAIS

O conjunto $\mathbb{Q}$, conhecido como conjunto dos números racionais é um conjunto numérico formado por elementos que podem ser representados na forma de uma fração $\frac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$, ou seja, números inteiros, números decimais finitos ou números decimais infinitos e periódicos.

Cotidianamente, deparamo-nos com situações que envolvem os números racionais, tais como situações nas quais temos que utilizar dinheiro, seguir uma receita, fatiar uma pizza, cortar uma laranja ou dividir uma barra de chocolate, ou seja, tais situações exigem noções de cálculos com décimos, centésimos, percentuais, enfim, com frações. Po-

demos também fazer uma relação entre frações, números decimais e porcentagens, pois estes conceitos se equivalem.

Vale observarmos aqui, que todos estes conteúdos mencionados acima são apresentados no ensino fundamental e trabalhados e desenvolvidos tanto no ensino fundamental quanto no ensino médio.

Exemplo 4.13. Escrever a fração $\frac{6}{8}$ na forma de outra fração, na forma de um número decimal e na forma de porcentagem.

Solução: Primeiro, na forma de outra fração, $\frac{6}{8} = \frac{3}{4}$, pois $8 \cdot 3 = 6 \cdot 4$, ou ainda, simplificando o numerador e o denominador de $\frac{6}{8}$ por 2, obtemos $\frac{6}{8} = \frac{6 \div 2}{8 \div 2} = \frac{3}{4}$.

Agora, na forma de um número decimal, temos que $\frac{6}{8} = \frac{3}{4}$, e multiplicando o numerador e o denominador de $\frac{3}{4}$ por 25, obtemos $\frac{3}{4} = \frac{3 \cdot 25}{4 \cdot 25} = \frac{75}{100}$ e, efetuando a divisão, obtemos que $\frac{6}{8} = \frac{3}{4} = 0,75$.

Por fim, na forma de porcentagem, temos que $\frac{6}{8} = \frac{3}{4} = \frac{75}{100}$ e substituindo o denominador 100 pelo símbolo %, obtemos $\frac{6}{8} = \frac{3}{4} = \frac{75}{100} = 75\%$

Portanto, temos que $\frac{6}{8} = \frac{3}{4} = 0,75 = \frac{75}{100} = 75\%$. □

Como sabemos, uma equação diofantina linear $ax + by = c$ possui seus coeficientes $a, b \in \mathbb{Z}$. Porém, de acordo com Savóis e Freitas D. (2015, p. 48), com alguns pequenos ajustes, ou seja, com a generalização de alguns conceitos definidos somente para o conjunto $\mathbb{Z}$ até então, podemos ampliar conceitos, como *mdc* e os próprios coeficientes da equação diofantina linear, ao conjunto $\mathbb{Q}$ e aos números reais comensuráveis.

> Este conceito de *mdc* generalizado será utilizado mais adiante para possibilitar a resolução de equações do tipo diofantinas com coeficientes racionais e deste modo estender o emprego dos métodos de resolução destas equações para problemas que até o momento são solucionados através de outros artifícios matemáticos. (SAVÓIS; FREITAS D. , 2015, p. 52).

Exemplo 4.14. Determinar o $mdc(0,9; 1,5)$.

Solução: Ampliando os Corolários 2.3 e 2.4 ao conjunto $\mathbb{Q}_+^*$, temos que

$$mdc(0,9; 1,5) = mdc\left(\frac{9}{10}; \frac{15}{10}\right) = \frac{1}{10} \cdot mdc(9, 15) = \frac{1}{10} \cdot 3 = 0,3.$$

Portanto, o $mdc(0,9; 1,5) = 0,3$. □

Podemos também enunciar e demonstrar aqui, o Máximo Divisor Comum Generalizado mostrado por Ripoll J., Ripoll C. e Sant'Ana (2006), que, coincidentimente, nos leva ao resultado dos Corolários 2.3 e 2.4, quando os ampliamos ao conjunto $\mathbb{Q}_+^*$.

Definição 4.5. Dizemos que dois segmentos da reta são comensuráveis quando podemos obter ambos por meio de uma quantidade inteira de emendas não sobrepostas de um determinado segmento de reta.

> Os gregos da Antiguidade acreditaram, por muito tempo, que dois quaisquer segmentos de reta eram sempre comensuráveis. Entre 450 e 400 a.C., contudo, provou-se que o segmento diagonal de um quadrado não era comensurável com o seu lado. Isto gerou uma forte crise na Matemática grega, chamada Crise dos Incomensuráveis, que só foi resolvida depois de muitos anos de discussão, discussão esta que levou à formulação precisa do problema da comensurabilidade em termos de medida de segmentos de retas e que se encerrou com a criação dos números reais absolutos. (RIPOLL J. ; RIPOLL C. ; SANT'ANA , 2006, p. 3).

Definição 4.6. Dizemos que dois números $a, b \in \mathbb{R}$ são comensuráveis quando existem números $c, d \in \mathbb{Z}$ não nulos, tais que $ac = bd$.

Observemos aqui que:

- dois números racionais são sempre comensuráveis;
- dois números irracionais podem ser ou não ser comensuráveis, por exemplos, $\sqrt{2}$ e $2 \cdot \sqrt{2}$ são comensuráveis e $\sqrt{2}$ e $\sqrt{3}$ não são comensuráveis; e
- dois números reais podem ser ou não ser comensuráveis, por exemplos, dois números racionais são sempre comensuráveis, ou $\sqrt{3}$ e $2 \cdot \sqrt{3}$ são comensuráveis, ou um número racional e um número irracional não são comensuráveis, ou $\sqrt{3}$ e $\sqrt{5}$ não são comensuráveis.

Mostremos o porquê de $\sqrt{2}$ e $\sqrt{3}$ não serem comensuráveis. Para que $\sqrt{2}$ e $\sqrt{3}$ sejam comensuráveis, devem existir $a, b \in \mathbb{N}$ tais que $a \cdot \sqrt{2} = b \cdot \sqrt{3}$ e, ao elevarmos ao quadrado os dois lados desta igualdade, obtemos $a \cdot \sqrt{2} = b \cdot \sqrt{3} \Rightarrow 2 \cdot a^2 = 3 \cdot b^2$, onde chegamos a um absurdo, visto que a quantidade de vezes que o fator 2 pode aparecer do lado esquerdo da igualdade é ímpar e do lado direito da igualdade é par.

Com isto, podemos afirmar que para determinarmos a comensurabilidade entre duas grandezas, temos apenas que verificar a racionalidade de suas razões, ou seja, se as razões entre estas duas grandezas resultam em um número racional.

Definição 4.7. Dizemos que $a \in \mathbb{R}$ é um múltiplo inteiro de $b \in \mathbb{R}$, ou que $b \in \mathbb{R}$ é um divisor inteiro de $a \in \mathbb{R}$, quando existe $c \in \mathbb{Z}$ tal que $a = bc$.

A definição a seguir é sobre o *mdcg*, ou seja, o máximo divisor comum generalizado de dois números reais comensuráveis, ou ainda, o maior número que divide ao mesmo tempo dois números reais comensuráveis.

Definição 4.8. Sejam $a, b \in \mathbb{R}$ comensuráveis e não nulos. Dizemos que d é o máximo divisor comum generalizado *mdcg* de a e b, indicando por $d = mdcg(a, b)$, se

i) d é um divisor inteiro comum de a e b; e

ii) d' é divisor inteiro comum de a e b, então $d' \leqslant d$.

Teorema 4.2. *Sejam $a, b \in \mathbb{R}$ comensuráveis e não nulos. Então, temos que*

$$mdcg(a,b) = \frac{a}{e} = \frac{b}{f},$$

onde $\frac{e}{f}$ é a fração irredutível do número racional $\frac{a}{b}$.

Demonstração: Primeiramente, consideremos $g, h, i, j \in \mathbb{Z}$. Se $ag = bh \Rightarrow \frac{a}{b} = \frac{h}{g}$ e $ai = bj \Rightarrow \frac{a}{b} = \frac{j}{i}$, então temos que

$$\frac{a}{b} = \frac{h}{g} = \frac{j}{i}.$$

Sabemos que os menores naturais g, h que satisfazem $ag = bh$ são obtidos quando tomamos o numerador e o denominador da fração irredutível que representa o racional $\frac{a}{b}$.

Daí temos que, pela definição de $mdcg$, se $\frac{e}{f}$ é esta fração irredutível, então

$$mdcg(a,b) = \frac{a}{e} = \frac{b}{f}.$$

Portanto, sendo a, b dois números reais comensuráveis e não nulos, então, temos que $mdcg(a,b) = \frac{a}{e} = \frac{b}{f}$, onde $\frac{e}{f}$ é a fração irredutível do número racional $\frac{a}{b}$. ■

Se $a, b \in \mathbb{Q}$, então podemos reescrever a fórmula demonstrada no Teorema 4.2 através de frações irredutíveis como descrito e demonstrado no Teorema 4.3 a seguir.

Teorema 4.3. *Sejam $a, b \in \mathbb{Q}^*$ e $c, d, e, f \in \mathbb{Z}^*$, tais que $a = \frac{c}{d}$, $b = \frac{e}{f}$ e $\frac{c}{d}$ e $\frac{e}{f}$ são frações irredutíveis. Então, temos que*

$$mdcg(a,b) = \frac{mdc(c,e)}{mmc(d,f)}.$$

Demonstração: Primeiramente, como $mdc(c,d) = mdc(e,f) = 1$, temos que

$$\frac{a}{b} = \frac{\frac{c}{d}}{\frac{e}{f}} = \frac{cf}{de} = \frac{c'f'}{d'e'},$$

onde $c' = \frac{c}{mdc(c,e)}$, $d' = \frac{d}{mdc(d,f)}$, $e' = \frac{e}{mdc(c,e)}$ e $f' = \frac{f}{mdc(d,f)}$.

Sabemos que a fração $\frac{c'f'}{d'e'}$ é irredutível e daí, temos que, por definição,

$$mdcg(a,b) = \frac{a}{c'f'} = \frac{\frac{c}{d}}{\frac{c}{mdc(c,e)} \cdot \frac{f}{mdc(d,f)}} = \frac{mdc(c,e) \cdot mdc(d,f)}{d \cdot f}.$$

Agora, pela Proposição 2.11, como temos que $\frac{d \cdot f}{mdc(d,f)} = mmc(d,f) \Rightarrow \frac{mdc(d,f)}{d \cdot f} = \frac{1}{mmc(d,f)}$, então

$$mdcg(a,b) = \frac{mdc(c,e) \cdot mdc(d,f)}{d \cdot f} = \frac{mdc(c,e)}{mmc(d,f)}.$$

Portanto, sendo $a, b \in \mathbb{Q}^*$ e $c, d, e, f \in \mathbb{Z}^*$, tais que $a = \frac{c}{d}$ e $b = \frac{e}{f}$ são frações irredutíveis, então, temos que $mdcg(a, b) = \frac{mdc(c, e)}{mmc(d, f)}$. ■

Exemplo 4.15. Determinar o $mdcg(0,9; 1,5)$.

Solução: Pelo o Teorema 4.3, temos que $0,9 = \frac{9}{10}$ e $1,5 = \frac{15}{10} = \frac{3}{2}$. Daí

$$mdcg(0,9; 1,5) = \frac{mdc(9,3)}{mmc(10,2)} = \frac{3}{10} = 0,3.$$

Portanto, o $mdcg(0,9; 1,5) = 0,3$. □

Exemplo 4.16. Determinar o $mdcg(a, b)$, com $a = \frac{3}{4}$ e $b = \frac{5}{2}$.

Solução: Pelo o Teorema 4.3, temos que $a = \frac{3}{4}$ e $b = \frac{5}{2}$. Daí

$$mdcg(a, b) = \frac{mdc(3,5)}{mmc(4,2)} = \frac{1}{4}.$$

Portanto, sendo $a = \frac{3}{4}$ e $b = \frac{5}{2}$, temos que $mdcg(a, b) = \frac{1}{4}$. □

Exemplo 4.17. Um total de 600 litros de álcool 70 ° INPM será armazenado em garrafas de 0,9l e de 1,5l, para serem distribuídas nas escolas públicas estaduais do Ceará, no intuito de ajudar na prevenção ao covid-19. Determine quais o maior e o menor números de garrafas que serão usadas no armazenamento do álcool, sabendo que um mínimo de 100 garrafas de cada quantidade devem ser utilizadas.

Solução: Primeiramente, observemos aqui que podemos transformar os coeficientes racionais da equação $0,9x + 1,5y = 600$ em coeficientes inteiros da equação $9x + 15y = 6000$, ou ainda, nos coeficientes inteiros da equação $3x + 5y = 2000$, pois estas equações são equivalentes. E assim chegaríamos no resultado final obtido que também é solução para a equação $0,9x + 1,5y = 600$.

Solucionando o exemplo pela equação com os coeficientes racionais, temos que o $mdcg(0,9; 1,5) = 0,3$ e, pelo Algoritmo de Euclides,

$$0,3 = 0,9 \cdot (2) + 1,5 \cdot (-1),$$

e multiplicando ambos os lados da igualdade por 2000, obtemos

$$0,3 = 0,9 \cdot (2) + 1,5 \cdot (-1) \Rightarrow 600 = 0,9 \cdot (4000) + 1,5 \cdot (-2000),$$

onde $x_0 = 4000$, $y_0 = -2000$, $x = x_0 + 1,5 \cdot z \Rightarrow x = 4000 + 1,5 \cdot z$ e $y = y_0 - 0,9 \cdot z \Rightarrow y = -2000 - 0,9 \cdot z$, com $z \in \mathbb{Z}$.

Como a questão solicita o cálculo do maior e do menor números de garrafas que serão usadas no armazenamento do álcool, utilizando um mínimo de 100 garrafas de cada quantidade, podemos fazê-lo apenas com as quantidades máxima e mínima de cada garrafa, ou seja, x máximo + y mínimo e y máximo + x mínimo, que nos dá os valores

de $100 + 340 = 440$ e $500 + 100 = 600$, sendo 440 a quantidade mínima de garrafas e 600 a quantidade máxima de garrafas, valores estes obtidos da seguinte forma:

$\twoheadrightarrow$ para $x = 100$, $0,9x + 1,5y = 600 \Rightarrow 0,9 \cdot 100 + 1,5y = 600 \Rightarrow 1,5y = 600 - 90 \Rightarrow y = \dfrac{510}{1,5} \Rightarrow y = 340$; e

$\twoheadrightarrow$ para $y = 100$, $0,9x + 1,5y = 600 \Rightarrow 0,9x + 1,5 \cdot 100 = 600 \Rightarrow 0,9x = 600 - 150 \Rightarrow x = \dfrac{450}{0,9} \Rightarrow x = 500$.

Portanto, 440 é a quantidade mínima de garrafas e 600 é a quantidade máxima de garrafas a serem utilizadas. □

Exemplo 4.18. A moeda de um determinado país é o dynamund e suas moedas são apenas de $0,4$ *dynamumds* e de $0,7$ *dynamumds*. A partir de quantos *dynamunds* é possível pagar qualquer quantia sem receber troco?

Solução: Pelo Exemplo 4.6, podemos solucionar o problema resolvendo a equação linear $0,4x + 0,7y = c$, com $x, y \in \mathbb{N} \cup \{0\}$, onde x representaria a quantidade de moedas de $0,4$ *dynamunds* e y representaria a quantidade de moedas de $0,7$ *dynamunds*.

Solucionando o exemplo pela equação com os coeficientes racionais, temos que, pelo Teorema 4.3, $0,4 = \dfrac{4}{10}$ e $0,7 = \dfrac{7}{10}$, e daí

$$mdcg(0,4; 0,7) = \frac{mdc(4,7)}{mmc(10,10)} = \frac{1}{10} = 0,1,$$

e, pelo Algoritmo de Euclides,

$$0,1 = 0,4 \cdot (2) + 0,7 \cdot (-1),$$

onde $x_0 = 2$, $y_0 = -1$, $x = x_0 + 0,7 \cdot z \Rightarrow x = 2 + 0,7 \cdot z$ e $y = y_0 - 0,4 \cdot z \Rightarrow y = -1 - 0,4 \cdot z$, com $z \in \mathbb{Z}$.

Ampliando o Corolário 4.2 ao conjunto $\mathbb{Q}_+^*$, temos que

- $a = 0,4$;
- $b = 0,7$;
- $mdcg(0,4; 0,7) = 0,1$;
- $c = (a - 0,1) \cdot (b - 0,1) = (0,4 - 0,1) \cdot (0,7 - 0,1) = 0,3 \cdot 0,6 = 0,18$;
- $c - 0,1 = 0,18 - 0,1 = 0,17$.

Com isto, podemos afirmar que a partir de $0,18$ *dynamunds* não existem mais lacunas no conjunto solução da equação $0,4x + 0,7y = c$ e que a maior lacuna é o valor de $0,17$ *dynamunds*.

Portanto, a partir de $0,18$ *dynamunds* é possível pagar qualquer quantia sem receber troco neste país. □

Exemplo 4.19. A bebezinha Aila guarda em seu cofrinho apenas moedas de $R\$0,25$ e $R\$0,50$. Quantas moedas são necessárias, no mínimo, tendo pelo menos 6 moedas de cada valor, para que a bebezinha Aila junte uma quantia de $R\$50,00$?

Solução: Podemos solucionar o problema resolvendo a equação $0,25x + 0,50y = 50$, com $x, y \in \mathbb{N}^*$, onde x representaria a quantidade de moedas de $R\$0,25$ e y representaria a quantidade de moedas de $R\$0,50$.

Solucionando o exemplo pela equação com os coeficientes racionais, temos que, pelo Teorema 4.3, $0,25 = \dfrac{25}{100} = \dfrac{1}{4}$ e $0,50 = \dfrac{50}{100} = \dfrac{1}{2}$, e daí

$$mdcg(0,25; 0,50) = \frac{mdc(1,1)}{mmc(4,2)} = \frac{1}{4} = 0,25,$$

e, pelo Algoritmo de Euclides,

$$0,25 = 0,25 \cdot (-1) + 0,5 \cdot (1),$$

e multiplicando ambos os lados da igualdade por 200, obtemos

$$0,25 \cdot 200 = 0,25 \cdot (-1) \cdot 200 + 0,5 \cdot (1) \cdot 200 \Rightarrow 50 = 0,25 \cdot (-200) + 0,5 \cdot (200),$$

onde $x_0 = -200$, $y_0 = 200$, $x = x_0 + \dfrac{0,5}{0,25} \cdot z \Rightarrow x = -200 + 2 \cdot z$ e $y = y_0 - \dfrac{0,25}{0,25} \cdot z \Rightarrow y = 200 - z$, com $z \in \mathbb{Z}$.

Para calcularmos os limites do valor de z possíveis, devemos fazer:

1) $-200 + 2 \cdot z \geqslant 6 \Rightarrow 2 \cdot z \geqslant 6 + 200 \Rightarrow 2 \cdot z \geqslant 206 \Rightarrow z \geqslant 103$; e

2) $200 - z \geqslant 6 \Rightarrow -z \geqslant 6 - 200 \Rightarrow z \leqslant 194$.

Com isto, calculando os valores de x e y para

i) $z = 103$, temos que $x = -200 + 2 \cdot z \Rightarrow x = -200 + 2 \cdot 103 \Rightarrow x = -200 + 206 \Rightarrow x = 6 \Rightarrow$ e $y = 200 - z \Rightarrow y = 200 - 103 \Rightarrow y = 97$; e

ii) $z = 194$, temos que $x = -200 + 2 \cdot z \Rightarrow x = -200 + 2 \cdot 194 \Rightarrow x = -200 + 388 \Rightarrow x = 188 \Rightarrow$ e $y = 200 - z \Rightarrow y = 200 - 194 \Rightarrow y = 6$.

Sendo assim, podemos perceber que o número mínimo de moedas $x + y$ ocorre quando $z = 103$.

Portanto, são necessárias 103 moedas, sendo 6 moedas de $R\$0,25$ e 97 moedas de $R\$0,50$, para que a bebezinha Aila junte uma quantia de $R\$50,00$. □

Exemplo 4.20. Vovó Mazé quer doar maçãs e laranjas de um modo igual para 15 pessoas. Cada maçã custa $R\$0,50$ e cada laranja custa $R\$0,20$. Se a vovó Mazé dispõe de $R\$30$ e deseja comprar um mínimo de 20 frutas de cada tipo, qual é o número máximo de frutas que cada pessoa irá receber?

Solução: Podemos solucionar o problema resolvendo a equação $0,50x + 0,20y = 30$, com $x, y \in \mathbb{N}^*$, onde x representaria a quantidade de maçãs e y representaria a quantidade de laranjas.

Solucionando o exemplo pela equação com os coeficientes racionais, temos que, pelo Teorema 4.3, $0,50 = \dfrac{50}{100} = \dfrac{1}{2}$ e $0,20 = \dfrac{20}{100} = \dfrac{1}{5}$, e daí

$$mdcg(0,50; 0,20) = \frac{mdc(1,1)}{mmc(2,5)} = \frac{1}{10} = 0,1,$$

e, pelo Algoritmo de Euclides,

$$0,1 = 0,5 \cdot (1) + 0,2 \cdot (-2),$$

e multiplicando ambos os lados da igualdade por 300, obtemos

$$0,1 \cdot 300 = 0,5 \cdot (1) \cdot 300 + 0,2 \cdot (-2) \cdot 300 \Rightarrow 30 = 0,5 \cdot (300) + 0,2 \cdot (-600),$$

onde $x_0 = 300$, $y_0 = -600$, $x = x_0 + \dfrac{0,2}{0,1} \cdot z \Rightarrow x = 300 + 2 \cdot z$ e $y = y_0 - \dfrac{0,5}{0,1} \cdot z \Rightarrow y = -600 - 5z$, com $z \in \mathbb{Z}$.

Para calcularmos os limites do valor de z possíveis, devemos fazer:

1) $300 + 2 \cdot z \geqslant 20 \Rightarrow 2 \cdot z \geqslant 20 - 300 \Rightarrow 2 \cdot z \geqslant -280 \Rightarrow z \geqslant -140$; e

2) $-600 - 5z \geqslant 20 \Rightarrow -5z \geqslant 20 + 600 \Rightarrow -5z \geqslant 620 \Rightarrow z \leqslant -124$.

Com isto, calculando os valores de x e y para

i) $z = -140$, temos que $x = 300 + 2 \cdot z \Rightarrow x = 300 + 2 \cdot (-140) \Rightarrow x = 300 - 280 \Rightarrow x = 20 \Rightarrow$ e $y = -600 - 5z \Rightarrow y = -600 - 5 \cdot (-140) \Rightarrow y = -600 + 700 \Rightarrow y = 100$; e

ii) $z = -124$, temos que $x = 300 + 2 \cdot z \Rightarrow x = 300 + 2 \cdot (-124) \Rightarrow x = 300 - 248 \Rightarrow x = 52 \Rightarrow$ e $y = -600 - 5z \Rightarrow y = -600 - 5 \cdot (-124) \Rightarrow y = -600 + 620 \Rightarrow y = 20$.

Logo, podemos perceber que o número máximo de frutas $x+y = 20+100 = 120$ ocorre quando $z = -140$. E como este total será dividido igualmente para 15 pessoas, então cada pessoa receberá $120 \div 15 = 8$ frutas.

Portanto, a vovó Mazé conseguirá doar 120 frutas, sendo 20 maçãs e 100 laranjas e cada pessoa receberá 8 frutas. □

Observemos que o valor $z = -124$ quando substituído na solução geral determinada nos fornece o valor mínimo possível de $x + y = 52 + 20 = 72$ frutas a serem doadas, sendo 52 maçãs e 20 laranjas juntando um total de 72 frutas, que não conseguiríamos dividir igualmente para 15 pessoas. Com isto, deveríamos utilizar $z = -125$, de onde obteríamos $x = 50$ e $y = 25$ e dividiríamos igualmente para 15 pessoas, com cada pessoa recebendo $75 \div 15 = 5$ frutas.

4.3 EQUAÇÕES DIOFANTINAS LINEARES COM COEFICIENTES IRRACIONAIS

O conjunto $\mathbb{I}$, conhecido como conjunto dos números irracionais, é um conjunto numérico formado pelos números decimais infinitos e não-periódicos, os quais não podem ser representados por meio de frações.

Sendo assim, se o número c for um número irracional, então c não pode ser escrito na forma de uma fração, ou seja, não pode ser escrito na forma $\dfrac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$. Como exemplo de números irracionais podemos citar as dízimas não periódicas.

A descoberta dos números irracionais é considerada um marco para a geometria, visto que preencheu várias lacunas, como a medida da diagonal de um quadrado que possui lado medindo uma unidade de comprimento.

Exemplo 4.21. Calcular a diagonal de um quadrado que possui lado igual a $1cm$.

Solução: Como sabemos a fórmula que calcula a diagonal de um quadrado é $d = l\sqrt{2}$. Sendo assim, como $l = 1cm$, então $d = l\sqrt{2} \Rightarrow d = 1cm \cdot \sqrt{2} \Rightarrow d = \sqrt{2}cm$. □

> E quanto é $\sqrt{2}$? Não podemos dizer exatamente. O que sabemos é que não é possível representá-lo em forma de fração, pois há infinitas casas depois da vírgula e não é uma dízima periódica. Com isso, houve a necessidade de criar mais um conjunto, o Conjunto dos Números Irracionais. Tal conjunto é formado por todos os números que, ao contrário dos racionais, não podem ser representados por uma fração. Simbolizamos esse conjunto por $\mathbb{I}$. (PARAIZO, 2016, p. 61).

Como mencionamos nos tópicos anteriores, podemos relacionar os coeficientes a e b de uma equação diofantina linear $ax + by = c$ com números irracionais somente no caso de a e b serem números comensuráveis. Daí, podemos utilizar a generalização do mdc e dos próprios coeficientes da equação diofantina linear para solucionar estas equações que envolvem números irracionais.

Vale observarmos aqui, que todos o conjunto dos números irracionais é apresentado no ensino fundamental e trabalhados e desenvolvidos tanto no ensino fundamental quanto no ensino médio. Porém é um conteúdo menos debatido que os demais.

> A importância dos números irracionais, segundo esse documento, deve-se ao seu potencial para uma discussão referente à ampliação da noção de número e para o despertar da curiosidade dos alunos sobre questões relacionadas ao infinito. Em relação à abordagem dos números irracionais, os PCN (BRASIL, 1998) sugerem não seguir por um caminho formal, evitar a associação com radicais, discutir sobre a notação decimal infinita e não periódica e a aproximação por números racionais, além de discutir a necessidade e as consequências do arredondamento de um número com infinitas casas decimais. (BROETTO; SANTOS-WAGNER, 2019, p. 731).

Exemplo 4.22. Determinar o $mdcg\left(\frac{1}{\pi}; \frac{1}{2\pi}\right)$.

Solução: Ampliando os Corolários 2.3 e 2.4 aos números reais comensuráveis e pelo Teorema 4.3, temos que

$$mdcg\left(\frac{1}{\pi}; \frac{1}{2\pi}\right) = \frac{1}{\pi} \cdot mdcg\left(1; \frac{1}{2}\right) = \frac{1}{\pi} \cdot \left(\frac{mdc(1,1)}{mmc(1,2)}\right) = \frac{1}{\pi} \cdot \frac{1}{2} = \frac{1}{2\pi}.$$

Portanto, o $mdcg\left(\frac{1}{\pi}; \frac{1}{2\pi}\right) = \frac{1}{2\pi}$. □

Exemplo 4.23. Determinar o $mdcg\left(\frac{2}{3} \cdot \pi; \frac{3}{4} \cdot \pi\right)$.

Solução: Ampliando os Corolários 2.3 e 2.4 aos números reais comensuráveis e pelo Teorema 4.3, temos que

$$mdcg\left(\frac{2}{3} \cdot \pi; \frac{3}{4} \cdot \pi\right) = \pi \cdot mdcg\left(\frac{2}{3}; \frac{3}{4}\right) = \pi \cdot \left(\frac{mdc(2,3)}{mmc(3,4)}\right) = \pi \cdot \frac{1}{12} = \frac{1}{12} \cdot \pi.$$

Portanto, o $mdcg\left(\frac{2}{3}\cdot\pi;\frac{3}{4}\cdot\pi\right)=\frac{1}{12}\cdot\pi$. □

Exemplo 4.24. Uma empresa de construção civil possui vigas com medidas de comprimento de $20\sqrt{2}m$ e de $12\sqrt{2}m$. Um construtor deseja cortar uma viga de cada medida em pedaços de mesmo comprimento de modo que os cortes tenham o maior tamanho possível e comum às vigas. Qual deve ser a medida de comprimento dos pedaços a serem cortados?

Solução: Para solucionar o problema, devemos determinar o $mdcg(20\sqrt{2};12\sqrt{2})$. Ampliando os Corolários 2.3 e 2.4 aos números reais comensuráveis e pelo Teorema 4.3, temos que

$$mdcg(20\sqrt{2};12\sqrt{2})=4\sqrt{2}\cdot mdc(5,3)=4\sqrt{2}\cdot 1\Rightarrow mdcg(20\sqrt{2};12\sqrt{2})=4\sqrt{2}.$$

Portanto, a medida de comprimento dos pedaços a serem cortados das vigas é de $4\sqrt{2}m$. □

Exemplo 4.25. Um retângulo possui medidas de $5,5\pi cm$ e de $3,5\pi cm$. Deseja-se dividir este retângulo em quadrados com as maiores medidas possíveis, de forma que estes quadrados completem toda a superfície do retângulo. Que medida deverá ter o lado destes quadrados?

Solução: Para solucionar o problema, devemos determinar o $mdcg(5,5\pi;3,5\pi)$. Ampliando os Corolários 2.3 e 2.4 aos números reais comensuráveis e pelo Teorema 4.3, temos que

$$mdcg(5,5\pi;3,5\pi)=0,5\pi\cdot mdc(11,7)=0,5\pi\cdot 1\Rightarrow mdcg(5,5\pi;3,5\pi)=0,5\pi.$$

Portanto, o lado destes quadrados deve possuir medida de $0,5\pi cm$. □

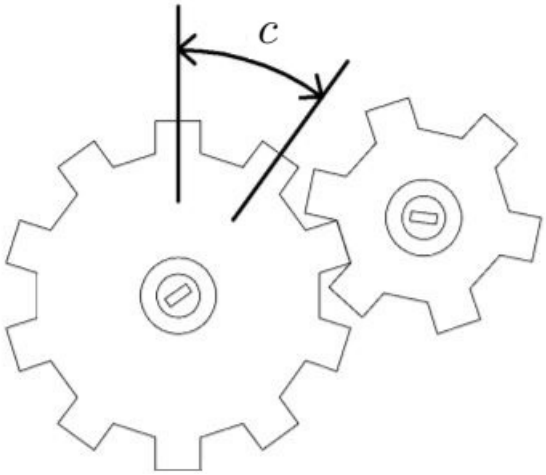
Exemplo 4.26. Duas rodas dentadas formam um sistema de engrenagem. Sabendo que todos os dentes possuem o mesmo tamanho, qual deve ser a medida do comprimento do arco compreendido por um dente e um espaço entre dois dentes vizinhos deste par de rodas para que haja um desgaste mínimo nesta engrenagem?

Solução: Solucionando geometricamente o problema, sabemos que se dois segmentos $\overline{AB}$ e $\overline{CD}$ possuem respectivamente medidas comensuráveis a e b, então o $mdcg(a,b)$ é a medida do maior segmento ou irá proporcionar medidas com valores inteiros para $\overline{AB}$ e $\overline{CD}$ quando for escolhido para ser utilizado como nova unidade de medida para medir segmentos de reta. Devemos então aplicar esta ideia ao ajuste desta engrenagem.

No intuito do desgaste sobre as rodas da engrenagem ser mínimo, como cada roda possui uma quantidade inteira de dentes, então os comprimentos das circunferências ou de seus raios devem ser comensuráveis.

Agora, denotando por c, conforme Figura 3 o arco compreendido por um dente e um espaço entre os dentes e por r_1 e r_2 os raios das duas rodas, temos que existem $d,e\in\mathbb{N}$ tais que $2\pi r_1=c\cdot d$ e $2\pi r_2=c\cdot e$ se, e somente se,

Figura 3 – Rodas Dentadas



Fonte: Adaptada de Ripoll J., Ripoll C. e Sant'Ana (2006, p.14).

$$\frac{2\pi r_1}{2\pi r_2} = \frac{c \cdot d}{c \cdot e} \Rightarrow \frac{r_1}{r_2} = \frac{d}{e} \Rightarrow e \cdot r_1 = d \cdot r_2,$$

ou seja, se e somente se, r_1 e r_2 forem comensuráveis.

Portanto, a medida do comprimento do arco compreendido por um dente e um espaço entre dois dentes vizinhos deste par de rodas, ou seja, o valor de c é exatamente $mdcg(2\pi r_1; 2\pi r_2) = 2\pi mdcg(r_1, r_2)$. □

Observemos aqui que se, na prática, este comprimento c for inviável por razão da curvatura deste arco ser muito grande, então, para podermos minimizar o desgaste, devemos tomar comprimentos iguais a $\frac{c}{f}$, com $f \in \mathbb{N}$. E, caso as medidas dos comprimentos dos dois raios forem incomensuráveis, então ocorrerá um desgaste inevitável sobre as rodas dentadas, o qual se tornará mínimo quando utilizarmos frações contínuas para calcularmos o valor de c.

4.4 EQUAÇÕES DIOFANTINAS QUADRÁTICAS

Uma equação diofantina quadrática é uma equação polinomial do segundo grau com duas ou mais variáveis que possuem apenas soluções no conjunto dos números inteiros. Aqui, abordaremos algumas das propriedades e aplicações das Equações Pitagóricas e da Equação de Pell.

4.4.1 *A Equação Pitagórica e seus Ternos Pitagóricos*

Iniciaremos esta parte do trabalho com uma observação a título de curiosidade. Segundo Domingues (1991, p.9), a distinção entre números pares e ímpares devemos aos pitagóricos (estudiosos da Escola Pitagórica), os quais conheciam os seguintes teoremas: a soma de dois números pares tem como resultado um número par; o produto de dois números ímpares tem como resultado um número ímpar; e quando um número ímpar

divide um número par, também divide sua metade.

Definição 4.9. Um terno Pitagórico é um terno de números inteiros positivos (x, y, z), tais que:

$$x^2 + y^2 = z^2.$$

Esta definição é equivalente às definições de Domingues e de Alencar Filho. Para Domingues (1991, p.13), temos que a definição de terno pitagórico é um terno (a, b, c), com $a, b, c \in \mathbb{N}$, onde tais números obedecem a relação $a^2 + b^2 = c^2$. E para Alencar Filho (1981, p.296), um terno pitagórico é toda e qualquer solução inteira e positiva da equação diofantina quadrática $x^2 + y^2 = z^2$.

De acordo com Kamers (2008, p. 7-8) e Souza (2017, p. 48), esta nomenclatura foi dada em homenagem a Pitágoras da Ilha de Samos, filósofo e matemático grego, nascido em Samos por volta de 570 a.C. e falecido provavelmente em 497 a.C. em Metaponto, no sul da Itália, mas sem precisão de datas, por ter descoberto uma interessante relação que envolvia os comprimentos dos lados dos triângulos retângulos, o Teorema de Pitágoras, onde, dado um triângulo retângulo com as medidas c para a hipotenusa, a e b para os catetos, temos que $a^2 + b^2 = c^2$, e, se $a, b, c \in \mathbb{N}$, chamamos este triângulo retângulo de Triângulo Pitagórico.

> A tradição é unânime em atribuir a Pitágoras a descoberta independente do teorema sobre triângulos retângulos hoje universalmente conhecido pelo seu nome — que o quadrado sobre a hipotenusa de um triângulo retângulo é igual à soma dos quadrados sobre os catetos. Já vimos que este teorema era conhecido pelos babilônios dos tempos de Hamurabi, mais de um milênio antes, mas sua primeira demonstração geral pode ter sido dada por Pitágoras. Muitas conjeturas têm sido feitas quanto à demonstração que Pitágoras poderia ter dado, mas ao que parece foi uma demonstração por decomposição[...] (EVES, 2011, p. 103).

Pitágoras formulou um conjunto de soluções para este tipo de equação que foi expresso por:

$$x = \frac{n^2 - 1}{2},\ y = n,\ z = \frac{n^2 + 1}{2},$$

com n sendo um número inteiro ímpar e $n > 1$.

Estas fórmulas foram obtidas da seguinte forma: se a é um número ímpar, então seu quadrado também é ímpar; daí $2b + 1 = a^2 \Rightarrow b = \dfrac{a^2 - 1}{2} \Rightarrow b + 1 = \dfrac{a^2 - 1}{2} + 1 \Rightarrow b + 1 = \dfrac{a^2 + 1}{2}$; como $(b + 1)^2 = b^2 + 2b + 1$, então

$$(b+1)^2 = b^2 + b + b + 1 \Rightarrow$$
$$\left(\frac{a^2+1}{2}\right)^2 = \left(\frac{a^2-1}{2}\right)^2 + \frac{a^2-1}{2} + \frac{a^2+1}{2}$$
$$\left(\frac{a^2+1}{2}\right)^2 = \left(\frac{a^2-1}{2}\right)^2 + \frac{a^2}{2} - \frac{1}{2} + \frac{a^2}{2} + \frac{1}{2}$$

$$\left(\frac{a^2+1}{2}\right)^2 = \left(\frac{a^2-1}{2}\right)^2 + a^2.$$

Segundo Hefez (2013, p.109), estas soluções elaboradas por Pitágoras não conseguem nos fornecer todas as soluções possíveis, como, por exemplo, o terno pitagórico $(8, 15, 17)$, pois vejamos que

$$(8, 15, 17) \to 8^2 + 15^2 = 17^2 \Rightarrow 64 + 225 = 289 \Rightarrow 289 = 289,$$

o que confirma ser um terno pitagórico, mas não se encontra este terno através do método desenvolvido por Pitágoras.

Observemos que n é um número inteiro ímpar e $n > 1$, então $n \in \{3, 5, 7, 9, ...\}$. Daí, para

- $n = 3$, temos que os valores de x, y e z são: $x = \dfrac{n^2-1}{2} = \dfrac{3^2-1}{2} = \dfrac{8}{2} \Rightarrow x = 4$, $y = n \Rightarrow y = 3$ e $z = \dfrac{n^2+1}{2} = = \dfrac{3^2+1}{2} = \dfrac{10}{2} \Rightarrow z = 5$, que indica o terno $(4, 3, 5)$;
- $n = 5$, temos que os valores de x, y e z são: $x = \dfrac{n^2-1}{2} = \dfrac{5^2-1}{2} = \dfrac{24}{2} \Rightarrow x = 12$, $y = n \Rightarrow y = 5$ e $z = \dfrac{n^2+1}{2} = = \dfrac{5^2+1}{2} = \dfrac{26}{2} \Rightarrow z = 13$, que indica o terno $(12, 5, 13)$;
- $n = 7$, temos que os valores de x, y e z são: $x = \dfrac{n^2-1}{2} = \dfrac{7^2-1}{2} = \dfrac{48}{2} \Rightarrow x = 24$, $y = n \Rightarrow y = 7$ e $z = \dfrac{n^2+1}{2} = = \dfrac{7^2+1}{2} = \dfrac{50}{2} \Rightarrow z = 25$, que indica o terno $(24, 7, 25)$;
- $n = 9$, temos que os valores de x, y e z são: $x = \dfrac{n^2-1}{2} = \dfrac{9^2-1}{2} = \dfrac{80}{2} \Rightarrow x = 40$, $y = n \Rightarrow y = 9$ e $z = \dfrac{n^2+1}{2} = = \dfrac{9^2+1}{2} = \dfrac{82}{2} \Rightarrow z = 41$, que indica o terno $(40, 9, 41)$,

ou seja, o terno $(8, 15, 17)$ não é encontrado com este método.

Observemos também que

i) se não relacionarmos a equação $x^2+y^2 = z^2$ aos lados de um triângulo retângulo, temos que as únicas soluções possíveis com uma das coordenadas igual a 0 são $(x, 0, x)$, $(x, 0, -x)$, $(-x, 0, x)$, $(-x, 0, -x)$, $(0, y, y)$, $(0, -y, y)$, $(0, y, -y)$ e $(0, -y, -y)$, com $x, y \in \mathbb{Z}$; e

ii) como todas as incógnitas em questão estão elevadas a expoentes pares, no caso 2, então basta determinarmos as soluções em $\mathbb{N}$.

Além disto, dizemos que um terno pitagórico (x, y, z) é denominado primitivo se $mdc(x, y) = 1$, $mdc(x, z) = 1$ e $mdc(y, z) = 1$, ou seja, $mdc(x, y, z) = 1$, ou ainda, de acordo com Hefez (2013, p.110), um triângulo pitagórico é chamado primitivo, quando as medidas de seus lados são números naturais coprimos dois a dois.

Proposição 4.5. *Temos que (x, y, z) é um terno pitagórico primitivo se, e somente se, $mdc(x, y) = mdc(y, z) = mdc(x, z) = 1$, ou seja, se, e somente se, x, y e z são coprimos*

dois a dois.

Demonstração: Suponhamos primeiramente que $d = mdc(x, y) = 1$. Se $d > 1$, então deve existir um divisor e primo para d. Logo, $e \mid x$ e $e \mid y \Rightarrow e \mid x+y \Rightarrow e \mid x^2+y^2 = z^2 \Rightarrow e \mid z$, o que é uma contradição, pois $e \leqslant mdc(x, y) = 1$.

Suponhamos agora que $f = mdc(x, z) = 1$. Se $f > 1$, então deve existir um divisor g primo para f. Logo, $g \mid x$ e $g|z \Rightarrow g \mid z - x \Rightarrow g \mid z^2 - x^2 = y^2 \Rightarrow g \mid y$, o que é uma contradição, pois $g \leqslant mdc(x, z) = 1$.

Suponhamos por fim que $h = mdc(y, z) = 1$. Se $h > 1$, então deve existir um divisor i primo para h. Logo, $i \mid y$ e $i|z \Rightarrow i \mid z - y \Rightarrow i \mid z^2 - y^2 = x^2 \Rightarrow i \mid x$, o que é uma contradição, pois $i \leqslant mdc(y, z) = 1$.

Por outro lado, se x, y, z são coprimos dois a dois, então

$$mdc(x, y) = mdc(y, z) = mdc(x, z) = 1,$$

não existindo primo j tal que $j \mid mdc(x, y)$ e/ou $j \mid mdc(x, z)$ e/ou $j \mid mdc(y, z)$. Daí, temos que x, y, z formam um terno pitagórico primitivo (x, y, z).

Portanto, temos que (x, y, z) é um terno pitagórico primitivo se, e somente se, $mdc(x, y) = mdc(y, z) = mdc(x, z) = 1$, ou seja, se, e somente se, x, y e z são coprimos dois a dois. ■

Temos também que os ternos pitagóricos primitivos (x, y, z) geram todos os ternos pitagóricos, ou seja, sendo (x_1, y_1, z_1) um terno pitagórico, então

$$\left(\frac{\mid x_1 \mid}{mdc(x, y, z)}, \frac{\mid y_1 \mid}{mdc(x, y, z)}, \frac{\mid z_1 \mid}{mdc(x, y, z)}\right),$$

é um terno pitagórico primitivo, ou ainda, todas as soluções não triviais da equação pitagórica $x^2 + y^2 = z^2$ é um terno pitagórico primitivo que possui suas coordenadas multiplicadas por um número natural.

Proposição 4.6. *Sejam (x, y, z) um terno pitagórico, $d = mdc(x, y, z)$ e os quocientes $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$ e $z_1 = \frac{z}{d}$. Então temos que (x_1, y_1, z_1) é um terno pitagórico primitivo, valendo (dx_1, dy_1, dz_1).*

Demonstração: Temos que

1) o $mdc(x_1, y_1, z_1) = 1$;
2) vale $(x, y, z) = (dx_1, dy_1, dz_1)$, pois $x_1 = \frac{x}{d} \Rightarrow x = x_1 \cdot d$, $y_1 = \frac{y}{d} \Rightarrow y = y_1 \cdot d$ e $z_1 = \frac{z}{d} \Rightarrow z = z_1 \cdot d$; e
3) $x_1^2 + y_1^2 = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = \left(\frac{z}{d}\right)^2 = z_1^2$, o que prova (x_1, y_1, z_1) ser um terno pitagórico primitivo.

Portanto, sendo (x, y, z) um terno pitagórico, $d = mdc(x, y, z)$ e os quocientes $x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$ e $z_1 = \frac{z}{d}$, então temos que (x_1, y_1, z_1) é um terno pitagórico primitivo, valendo (dx_1, dy_1, dz_1). ■

Logo, podemos obter um terno pitagórico primitivo a partir de um não primi-

tivo, bastando dividir suas coordenadas pelo *mdc* de duas das coordenadas do terno não primitivo.

Exemplo 4.27. Como o terno pitagórico $(12, 16, 20)$ não é terno primitivo, pois temos que $mdc(12, 16) = 4 \neq 1$, então podemos determinar o terno pitagórico primitivo que gerou $(12, 16, 20)$ bastando dividirmos as coordenadas de $(12, 16, 20)$ pelo $mdc(12, 16) = 4$, de onde obtemos $(3, 4, 5)$, que é um terno pitagórico primitivo, pois $mdc(3, 4, 5) = 1$.

Daí, também podemos obter um terno pitagórico não primitivo a partir de um outro primitivo ou não primitivo, bastando multiplicar suas coordenadas por um inteiro positivo maior do que 1, ou seja, todas os ternos pitagóricos (x, y, z) que são soluções de $x^2 + y^2 = z^2$ resultam da multiplicação das coordenadas de (x_1, y_1, z_1), com $mdc(x_1, y_1, z_1) = 1$ por um número natural maior do que 1.

Corolário 4.3. *Seja (x, y, z) um terno pitagórico e $a \in \mathbb{N}$. Temos que (ax, ay, az) também é um terno pitagórico.*

Demonstração: Multiplicando x e y por a, elevando os dois resultados ao quadrado e somando estes últimos resultados, temos que

$(a\cdot x)^2+(a\cdot y)^2 = a^2\cdot x^2+a^2\cdot y^2 = a^2\cdot(x^2+y^2) = a^2\cdot z^2 = (a\cdot z)^2 \Rightarrow (a\cdot x)^2+(a\cdot y)^2 = (a\cdot z)^2.$

Portanto, sendo (x, y, z) um terno pitagórico e $a \in \mathbb{N}$, temos que (ax, ay, az) também é um terno pitagórico. ■

Exemplo 4.28. Seja o terno pitagórico $(8, 15, 17)$. Então $(40, 75, 85)$ também é um terno pitagórico, pois

$40^2 + 75^2 = (5\cdot 8)^2 + (5\cdot 15)^2 = 5^2\cdot 8^2 + 5^2\cdot 15^2 = 5^2\cdot(8^2 + 15^2) = 5^2\cdot 17^2 = (5\cdot 17)^2 = 85^2.$

Exemplo 4.29. Observemos que como $(3, 4, 5)$ e $(8, 15, 17)$ são ternos pitagóricos primitivos, então

- $\surd$ $(3, 4, 5) = (1\cdot 3, 1\cdot 4, 1\cdot 5)$, $(6, 8, 10) = (2\cdot 3, 2\cdot 4, 2\cdot 5)$, $(9, 12, 15) = (3\cdot 3, 3\cdot 4, 3\cdot 5)$, ..., $(a\cdot 3, a\cdot 4, a\cdot 5)$, ..., também são ternos pitagóricos; e
- $\surd$ $(8, 15, 17) = (1\cdot 8, 1\cdot 15, 1\cdot 17)$, $(16, 30, 34) = (2\cdot 8, 2\cdot 15, 2\cdot 17)$, $(24, 45, 51) = (3\cdot 8, 3\cdot 15, 3\cdot 17)$, ..., $(a\cdot 8, a\cdot 15, a\cdot 17)$, ..., também são ternos pitagóricos.

Como em um terno pitagórico primitivo temos coprimalidade duas a duas de suas coordenadas, então devemos ter duas das coordenadas ímpares, sendo que uma destas duas ímpares é a maior das três coordenadas.

Teorema 4.4. *Seja (a, b, c) um terno pitagórico primitivo, com $c > a$ e $c > b$. Então temos que a e b são um número par e um número ímpar, ou um número ímpar e um número par. Temos também que c é um número ímpar.*

Demonstração: Suponhamos primeiramente por absurdo que a e b são números ímpares e, por isto, podem ser escritos na forma: $a = 2d + 1$ e $b = 2e + 1$, com $d, e \in \mathbb{Z}$. Como a e b são números ímpares, então seus respectivos quadrados também serão números ímpares, implicando em c ser um número par, pois a soma de dois números ímpares resulta em um

número par.

Daí, pelo Teorema de Pitágoras, temos que

$$c^2 = a^2 + b^2 \Rightarrow$$
$$c^2 = (2d+1)^2 + (2e+1)^2 \Rightarrow$$
$$c^2 = 4d^2 + 4d + 1 + 4e^2 + 4e + 1 \Rightarrow$$
$$c^2 = 4 \cdot (d^2 + d + e^2 + e) + 2 \Rightarrow$$
$$c^2 = 4 \cdot f + 2,$$

com $f = (d^2 + d + e^2 + e) \in \mathbb{Z}$.

Isto nos mostra que quando dividimos c^2 por 4 o resto desta divisão é 2, o que é um absurdo, pois c sendo ímpar, então $c = 2h + 1 \Rightarrow c^2 = 4h^2 + 4h + 1 \Rightarrow c^2 = 4 \cdot (h^2 + h) + 1 \Rightarrow c^2 = 4i + 1$, com $h, i \in \mathbb{Z}$ e $i = (h^2 + h)$ ou seja, c par deixa resto 1 na divisão por 4.

Daí, não podemos ter a e b ímpares ao mesmo tempo.

Suponhamos agora por absurdo que a e b são números pares, então chegamos a um absurdo, pois pela Proposição 4.5, a e b são coprimos, ou seja, $mdc(a, b) = 1$.

Suponhamos por fim e sem perda de generalidade, que a é um número par e b é um número ímpar e, por isto, podem ser escritos na forma: $a = 2p$ e $b = 2q + 1$, com $p, q \in \mathbb{Z}$. Como a é um número par e b é um número ímpar, então seus respectivos quadrados também serão um número par e número ímpar, implicando em c ser um número ímpar, pois a soma de um número par com um número ímpar resulta em um número ímpar.

Daí, pelo Teorema de Pitágoras, temos que

$$c^2 = a^2 + b^2 \Rightarrow$$
$$c^2 = (2p)^2 + (2q+1)^2 \Rightarrow$$
$$c^2 = 4p^2 + 4q^2 + 4q + 1 \Rightarrow$$
$$c^2 = 4 \cdot (p^2 + q^2 + q) + 1 \Rightarrow$$
$$c^2 = 4 \cdot r + 1,$$

com $r = (p^2 + q^2 + q) \in \mathbb{Z}$.

Isto nos mostra que quando dividimos c^2 por 4 o resto desta divisão é 1, o que pode acontecer, pois c sendo ímpar, então $c = 2t + 1 \Rightarrow c^2 = 4t^2 + 4t + 1 \Rightarrow c^2 = 4u + 1$, com $t, u \in \mathbb{Z}$ e $u = 4 \cdot (t^2 + t)$ ou seja, c par deixa resto 1 na divisão por 4.

Daí, temos que a é um número par, b é um número ímpar e c é um número ímpar ou a é um número ímpar, b é um número par e c é um número ímpar, o que é justificado e reforçado pelo fato de a, b e c serem coprimos dois a dois.

Portanto, sendo (a, b, c) um terno pitagórico, com $c > a$ e $c > b$. Então temos que a e b são um número par e um número ímpar, ou um número ímpar e um número par e c é um número ímpar. ■

Exemplo 4.30. Mostrar que em um triângulo retângulo pitagórico, a área é um número

inteiro positivo.

Solução: Primeiramente, temos que todo triângulo retângulo pitagórico possui lados com medidas inteiras positivas e, pelo Teorema de Pitágoras, $a^2 + b^2 = c^2$, com a, b sendo os catetos e c sendo a hipotenusa e $a \leqslant b < c$.

Associamos então a este triângulo retângulo o terno pitagórico (a, b, c), como solução da equação $a^2 + b^2 = c^2$.

Em concordância com PEREIRA (2015, p. 4), podemos calcular a área (A) deste triângulo pela expressão

$$A = \frac{cateto \cdot cateto}{2} = \frac{a \cdot b}{2}$$

e, para provarmos que a área deste triângulo é um número inteiro, basta mostrarmos que a ou b é um número par.

Daí, pelo Teorema 4.4, temos que, em um terno pitagórico (a, b, c), com $c > a$ e $c > b$, a e b são um número par e um número ímpar.

Sendo a par, temos que é da forma $a = 2 \cdot d$, com $d \in \mathbb{Z}_+^*$ e substituindo em $A = \frac{a \cdot b}{2}$, obtemos

$$A = \frac{a \cdot b}{2} \Rightarrow A = \frac{2 \cdot d \cdot b}{2} \Rightarrow A = d \cdot b,$$

e, como b e d são números inteiros positivos, então a área do triângulo também é um número inteiro positivo.

Sendo b par, temos que é da forma $b = 2\cdot$, com $e \in \mathbb{Z}_+^*$ e substituindo em $A = \frac{a \cdot b}{2}$, obtemos

$$A = \frac{a \cdot b}{2} \Rightarrow A = \frac{a \cdot 2 \cdot e}{2} \Rightarrow A = a \cdot e,$$

e, como a e e são números inteiros positivos, então a área do triângulo também é um número inteiro positivo.

Portanto, em um triângulo retângulo pitagórico, a área é um número inteiro positivo. □

Em seu livro Elementos, Euclides construiu e determinou a existência de infinitos ternos pitagóricos primitivos, ao mostrar e demonstrar uma fórmula que gera todos os ternos pitagóricos primitivos.

Lema 4.1. *Sejam $a, b \in \mathbb{N}$ coprimos. Se $a \cdot b$ é um quadrado, então tanto a quanto b são quadrados também.*

Demonstração: Suponhamos que $a \cdot b = c^2$, com $c \in \mathbb{N}$ e consideremos $d = mdc(a, b)$.

Daí, temos que, $a = a_1 \cdot d$, $c = c_1 \cdot d$ e, pelo Corolário 2.3, $mdc(a_1, c_1) = 1$. Substituindo em $a \cdot b = c^2$, obtemos

$$a \cdot b = c^2 \Rightarrow a_1 \cdot d \cdot b = (c_1 \cdot d)^2 \Rightarrow a_1 \cdot b = c_1^2 \cdot d.$$

Como $mdc(a_1, c_1) = 1$, então, pela propriedade $(viii)$ do mdc, temos que $mdc(a_1, c_1^2) = 1$.

Logo, $c_1^2 \mid b$ e $b = c_1^2 \cdot e$, para algum $e \in \mathbb{N}$. Agora, substituindo este resultado em $a_1 \cdot b = c_1^2 \cdot d$, obtemos

$$a_1 \cdot b = c_1^2 \cdot d \Rightarrow a_1 \cdot c_1^2 \cdot e = c_1^2 \cdot d \Rightarrow a_1 \cdot e = d.$$

Agora, como $d \mid a$ e $e \mid b$, então temos que $mdc(d, e) \mid mdc(a, b)$. Como $mdc(a, b) = 1$, então $mdc(d, e) = 1$. Como $a_1 \cdot e = d$ e $mdc(d, e) = 1$, então $d \mid a_1$, ou seja, $a_1 = f \cdot d$, com $f \in \mathbb{N}$. Substituindo este resultando em $a_1 \cdot e = d$, obtemos

$$a_1 \cdot e = d \Rightarrow f \cdot d \cdot e = d \Rightarrow f \cdot e = 1 \Rightarrow f = e = 1.$$

Logo, temos que $a_1 \cdot e = d \Rightarrow a_1 = d$, $a = a_1 \cdot d \Rightarrow a = d \cdot d \Rightarrow a = d^2$ e $b = c_1^2 \cdot e \Rightarrow b = c_1^2$.

Portanto, sendo $a, b \in \mathbb{N}$ coprimos, se $a \cdot b$ é um quadrado, então tanto a quanto b são quadrados também. ■

Teorema 4.5. (Fórmulas de Euclides) *Sejam dois números naturais d, e, com $e > d$, o terno (a, b, c), onde:*

$$a = 2 \cdot d \cdot e,\ b = e^2 - d^2,\ c = e^2 + d^2$$

é pitagórico primitivo se, e somente se, d, e forem coprimos e possuírem paridades distintas.

Demonstração: Pelo Teorema de Pitágoras, temos que

$$\begin{gathered} c^2 = a^2 + b^2 \Rightarrow \\ c^2 - b^2 = a^2 \Rightarrow \\ (c+b) \cdot (c-b) = a^2 \Rightarrow \\ \frac{c+b}{2} \cdot \frac{c-b}{2} = \frac{a^2}{2 \cdot 2} \Rightarrow \\ \frac{c+b}{2} \cdot \frac{c-b}{2} = \left(\frac{a}{2}\right)^2. \end{gathered}$$

Supondo a par e b ímpar , como temos que b e c são ímpares, então $\frac{c+b}{2}$ e $\frac{c-b}{2}$ são positivos e coprimos, visto que $mdc\left(\frac{c+b}{2}, \frac{c-b}{2}\right)$ tem que dividir a soma $\frac{c+b}{2} + \frac{c-b}{2} = c$ e também a diferença $\frac{c+b}{2} - \frac{c-b}{2} = b$ que são coprimos.

Daí, pelo Lema 4.1, temos que existem dois números $d, e \in \mathbb{N}$ com $e > d$ e $mdc(d, e) = 1$ e de paridades distintas, tais que $\frac{c+b}{2} = e^2$, e $\frac{c-b}{2} = d^2$, ou seja,

$\angle\ e^2 + d^2 = \frac{c+b}{2} + \frac{c-b}{2} = c$;

$\angle\ e^2 - d^2 = \frac{c+b}{2} - \frac{c-b}{2} = b$; e

$\angle\ \frac{c+b}{2} \cdot \frac{c-b}{2} = \frac{a^2}{2 \cdot 2} \Rightarrow \frac{c^2 - b^2}{4} = \frac{a^2}{4} \Rightarrow \frac{(e^2+d^2)^2 - (e^2-d^2)^2}{4} = \frac{a^2}{4} \Rightarrow \frac{4 \cdot e^2 \cdot d^2}{4} = \frac{a^2}{4} \Rightarrow e^2 \cdot d^2 = \frac{a^2}{4} \Rightarrow 4 \cdot e^2 \cdot d^2 = a^2 \Rightarrow 2 \cdot e \cdot d = a.$

Por outro lado, dados dois números $d, e \in \mathbb{N}$ com $e > d$ e $mdc(d, e) = 1$ e de paridades distintas, fazendo $c = e^2 + d^2$, $b = e^2 - d^2$ e $a = 2 \cdot e \cdot d$, temos que (a, b, c) é

um terno pitagórico primitivo, pois

$$c^2 = a^2 + b^2 \Rightarrow$$
$$(e^2 + d^2)^2 = (2 \cdot e \cdot d)^2 + (e^2 - d^2)^2 \Rightarrow$$
$$e^4 + 2 \cdot e^2 \cdot d^2 + d^4 = 4 \cdot e^2 \cdot d^2 + e^4 - 2 \cdot e^2 \cdot d^2 + d^4 \Rightarrow$$
$$2 \cdot e^2 \cdot d^2 = 2 \cdot e^2 \cdot d^2,$$

o que é uma sentença verdadeira.

Suponhamos agora que existe $f \mid mdc(a, b, c)$, com f sendo um número primo. Como a é par e b e c são ímpares, então f é ímpar, pois $f \mid a = 2 \cdot e \cdot d$, de onde podemos dizer que $f \mid d$ ou $f \mid e$, $f \mid b = e^2 - d^2$, de onde podemos dizer que $f \mid d$ e $f \mid e$ e $f \mid c = e^2 + d^2$, de onde podemos dizer que $f \mid d$ e $f \mid e$. Como consequência destes dois últimos fatos, temos que $f \leqslant mdc(d, e) = 1$, o que é um absurdo. Logo, como $mdc(a, b) = mdc(a, c) = mdc(b, c) = 1$, ou seja, são coprimos dois a dois, então $mdc(a, b, c) = 1$.

Portanto, sendo dois números naturais d, e, com $e > d$, o terno (a, b, c), onde $a = 2 \cdot d \cdot e$, $b = e^2 - d^2$ e $c = d^2 + e^2$ é pitagórico primitivo se, e somente se, d e e forem coprimos e possuírem paridades distintas. ■

Em concordância com Souza (2017, p. 52), como consequência do Teorema 4.5 e do Corolário 4.3, temos que todos os ternos pitagóricos, tanto os primitivos quanto os não primitivos, podemos determiná-los através de

$$(a, b, c) = (f \cdot d \cdot e, f \cdot (e^2 - d^2), f \cdot (e^2 + d^2)),$$

com $d, e, f \in \mathbb{N}$, $f \geqslant 1$, $e > d \geqslant 1$, $mdc(d, e) = 1$ e d e e com paridades distintas.

Proposição 4.7. *Todo terno pitagórico primitivo (a, b, c) é representado de modo único como solução da equação $a^2 + b^2 = c^2$ e na forma $a = 2 \cdot d \cdot e,\ b = e^2 - d^2,\ c = e^2 + d^2$.*

Demonstração: Suponhamos que, $a = 2 \cdot d \cdot e = 2 \cdot f \cdot g$, $b = e^2 - d^2 = g^2 - f^2$, e $c = e^2 + d^2 = g^2 + f^2$, com $f, g \in \mathbb{N}$ e $g > f$. Pelo Teorema 4.5, f e g são coprimos e possuírem paridades distintas. Então, temos que somando as equações membro a membro $e^2 - d^2 = g^2 - f^2$ e $e^2 + d^2 = g^2 + f^2$, obtemos

$$e^2 - d^2 + e^2 + d^2 = g^2 - f^2 + g^2 + f^2 \Rightarrow 2 \cdot e^2 = 2 \cdot g^2 \Rightarrow e^2 = g^2 \Rightarrow e = g.$$

Agora, substituindo este resultado em $e^2 + d^2 = g^2 + f^2$, obtemos

$$e^2 + d^2 = g^2 + f^2 \Rightarrow g^2 + d^2 = g^2 + f^2 \Rightarrow d^2 = f^2 \Rightarrow d = f.$$

Portanto, todo terno pitagórico primitivo (a, b, c) é representado de modo único como solução da equação $a^2 + b^2 = c^2$ e na forma $a = 2 \cdot d \cdot e,\ b = e^2 - d^2,\ c = d^2 + e^2$. ■

Logo, um terno pitagórico primitivo (a, b, c) determina univocamente d e e da seguinte forma, supondo a par, então a fração reduzida equivalente à fração $\dfrac{b + c}{a}$ é

$$\frac{b + c}{a} = \frac{e^2 - d^2 + e^2 + d^2}{2 \cdot d \cdot e} = \frac{2 \cdot e^2}{2 \cdot d \cdot e} = \frac{e}{d}.$$

Exemplo 4.31. Determinar os valores d, e, com $d, e \in \mathbb{N}$ e $e > d$ para que o terno

pitagórico (8, 15, 17) satisfaça $8 = 2 \cdot d \cdot e,\ 15 = e^2 - d^2,\ 17 = e^2 + d^2$.

Solução: Pela Proposição 4.7, temos que

$$\frac{b+c}{a} = \frac{15+17}{8} = \frac{32}{8} = \frac{4}{1} = \frac{e}{d},$$

ou seja, $d = 1$ e $e = 4$.

Portanto, os valores de d, e, com $d, e \in \mathbb{N}$ e $e > d$ para que o terno pitagórico (8, 15, 17) satisfaça $8 = 2 \cdot d \cdot e,\ 15 = e^2 - d^2,\ 17 = e^2 + d^2$ são $d = 1$ e $e = 4$. □

Exemplo 4.32. Determinar todas as soluções em $\mathbb{Z}$ para a equação $x^2 + y^2 = 2z^2$.

Solução: Na equação $x^2 + y^2 = 2z^2$, como $2z^2$ é par, então temos que x e y devem possuir a mesma paridade.

Temos também que existem, em $\mathbb{Z}$, $a = \dfrac{x+y}{2}$ e $b = \dfrac{(x-y)}{2}$ tais que $x = a+b$ e $y = a-b$. Substituindo em $x^2 + y^2$, obtemos como resultado

$$x^2 + y^2 = (a+b)^2 + (a-b)^2 = a^2 + 2 \cdot a \cdot b + b^2 + a^2 - 2 \cdot a \cdot b + b^2 = 2 \cdot a^2 + 2 \cdot b^2 = 2 \cdot z^2 \Rightarrow$$

$$a^2 + b^2 = z^2,$$

que corresponde a Equação do Teorema de Pitágoras.

Daí, pelo Teorema 4.5, podemos determinar que todas as soluções para a equação $a^2 + b^2 = z^2$ são da forma

$$(a, b, z) = (2 \cdot c \cdot d \cdot e, c \cdot (e^2 - d^2), c \cdot (e^2 + d^2)),$$

com $c, d, e \in \mathbb{N}$, $c \geqslant 1$, $e > d \geqslant 1$, $mdc(d, e) = 1$ e d e e com paridades distintas.

Portanto, também pelo Teorema 4.5, temos que todas as soluções em $\mathbb{Z}$ para a equação $x^2 + y^2 = 2z^2$ são forma

$$(x, y, z) = (a+b, a-b, z) = (2 \cdot c \cdot d \cdot e + c \cdot (e^2 - d^2), 2 \cdot c \cdot d \cdot e - c \cdot (e^2 - d^2), c \cdot (e^2 + d^2)),$$

com $c, d, e \in \mathbb{N}$, $c \geqslant 1$, $e > d \geqslant 1$, $mdc(d, e) = 1$ e d e e com paridades distintas. □

Exemplo 4.33. Determinar todos os ternos (a, b, c) de números inteiros positivos tais que a^2, b^2 e c^2 estão em progressão aritmética.

Solução: Como a^2, b^2 e c^2 estão em progressão aritmética, então temos que

$$b^2 = \frac{a^2 + c^2}{2} \Rightarrow a^2 + c^2 = 2 \cdot b^2.$$

Sendo assim, é suficiente considerarmos que a, b e c sejam coprimos, da mesma forma que acontece nos ternos pitagóricos. Logo, temos que a e c possuem mesma paridade, ou seja, a e c são números ímpares e, por hipótese, possuem $mdc(a, c) = 1$, ou seja, existem $d, e \in \mathbb{Z}_+^*$ tais que $d = \dfrac{c+a}{2}$ e $e = \dfrac{c-a}{2}$, de onde obtemos

$$d + e = \frac{c+a}{2} + \frac{c-a}{2} = \frac{c+a+c-a}{2} = \frac{2c}{2} \Rightarrow c = d + e,$$

$$d - e = \frac{c+a}{2} - \frac{c-a}{2} = \frac{c+a-c+a}{2} = \frac{2a}{2} \Rightarrow a = d - e$$

e

$$2\cdot b^2 = a^2 + c^2 = (d-e)^2 + (d+e)^2 = d^2 - 2\cdot d\cdot e + e^2 + d^2 + 2\cdot d\cdot e + e^2 = 2\cdot d^2 + 2\cdot e^2 \Rightarrow$$
$$2\cdot b^2 = 2\cdot (d^2 + e^2) \Rightarrow b^2 = d^2 + e^2,$$

ou seja, o terno (d, e, b) é um terno pitagórico.

Como qualquer divisor comum de d e e também é divisor comum de a e c, então o terno pitagórico (d, e, b) é primitivo, ou seja, pelo Teorema 4.5, existem $f, g \in \mathbb{Z}_+^*$ tais que $d = 2\cdot f\cdot g$, $e = f^2 - g^2$ e $b = f^2 + g^2$.

Substituindo, agora em $a = d - e$ e $c = d + e$, obtemos

$$a = d - e = 2\cdot f\cdot g - (f^2 - g^2) \Rightarrow a = g^2 - f^2 + 2\cdot f\cdot g$$

e

$$c = d + e = 2\cdot f\cdot g + (f^2 - g^2) \Rightarrow c = f^2 - g^2 + 2\cdot f\cdot g.$$

Daí, temos que os ternos (a, b, c) da forma $(g^2 - f^2 + 2\cdot f\cdot g, f^2 + g^2, f^2 - g^2 + 2\cdot f\cdot g)$ estão em progressão aritmética, pois temos que

$$a^2 + c^2 = (g^2 - f^2 + 2\cdot f\cdot g)^2 + (f^2 - g^2 + 2\cdot f\cdot g)^2$$
$$\begin{aligned} a^2 + c^2 = \quad & g^4 - f^2\cdot g^2 + 2\cdot f\cdot g^3 - f^2\cdot g^2 + f^4 - 2\cdot f^3\cdot g + 2\cdot f\cdot g^3 - 2\cdot f^3\cdot g + \\ & 4\cdot f^2\cdot g^2 + f^4 - f^2\cdot g^2 + 2\cdot f^3\cdot g - f^2\cdot g^2 + g^4 - 2\cdot f\cdot g^3 + 2\cdot f^3\cdot g - \\ & 2\cdot f\cdot g^3 + 4\cdot f^2\cdot g^2 \end{aligned}$$
$$a^2 + c^2 = 2\cdot g^4 + 2\cdot f^4 + 4\cdot f^2\cdot g^2 = 2\cdot (f^4 + 2\cdot f^2\cdot g^2 + g^4) = 2\cdot (f^2 + g^2)^2$$
$$a^2 + c^2 = 2\cdot b^2.$$

Portanto, todos os ternos (a, b, c) de números inteiros positivos tais que a^2, b^2 e c^2 estão em progressão aritmética são da forma $(g^2 - f^2 + 2\cdot f\cdot g, f^2 + g^2, f^2 - g^2 + 2\cdot f\cdot g)$, com $f, g \in \mathbb{Z}_+^*$. □

Exemplo 4.34. Provar que para todo $a > 2$ com $a \in \mathbb{Z}$, existem $b, c \in \mathbb{Z}_+^*$ tais que

$$a^2 + b^2 = c^2.$$

Solução: Primeiramente, quando realizamos a fatoração de $a^2 + b^2 = c^2$, obtemos

$$a^2 + b^2 = c^2 \Rightarrow a^2 = c^2 - b^2 \Rightarrow a^2 = (c + b)\cdot (c - b).$$

Daí, temos duas possibilidades. Uma a sendo ímpar e outra a sendo par.

Com isto, se a for ímpar, então podemos determinar b e c tais que $c + b = a^2$ e $c - b = 1$, obtendo $(a, b, c) = \left(a, \dfrac{a^2 - 1}{2}, \dfrac{a^2 + 1}{2}\right)$ da seguinte forma: ao somarmos ambos lados das igualdades $c + b = a^2$ e $c - b = 1$, obtemos

$$c + b + c - b = a^2 + 1 \Rightarrow 2c = a^2 + 1 \Rightarrow c = \frac{a^2 + 1}{2}$$

e substituindo este resultado em $c + b = a^2$, obtemos

$$c + b = a^2 \Rightarrow \frac{a^2 + 1}{2} + b = a^2 \Rightarrow a^2 + 1 + 2b = 2a^2 \Rightarrow 2b = a^2 - 1 \Rightarrow b = \frac{a^2 - 1}{2}.$$

E, se a for par, então podemos determinar b e c tais que $c + b = \dfrac{a^2}{2}$ e $c - b = 2$, obtendo $(a, b, c) = \left(a, \dfrac{a^2 - 1}{2}, \dfrac{a^2 + 1}{2}\right)$ da seguinte forma: ao somarmos ambos lados das

igualdades $c+b=\dfrac{a^2}{2}$ e $c-b=2$, obtemos

$$c+b+c-b=\frac{a^2}{2}+2\Rightarrow 4c=a^2+4\Rightarrow c=\frac{a^2}{4}+1$$

e substituindo este resultado em $c+b=\dfrac{a^2}{2}$, obtemos

$$c+b=\frac{a^2}{2}\Rightarrow\frac{a^2}{4}+1+b=\frac{a^2}{2}\Rightarrow a^2+4+4b=2a^2\Rightarrow 4b=a^2-4\Rightarrow b=\frac{a^2}{4}-1.$$

Portanto, para todo inteiro $a>2$, existem $b,c\in\mathbb{Z}_+^*$ tais que $a^2+b^2=c^2$. □

A seguir, temos dois exemplos de soma de dois quadrados, uma utilizando a equação de uma circunferência e outra utilizando a equação de uma elipse. As equações apresentadas são da forma $ax^2+by^2=c$, com $a,b,x,y\in\mathbb{Q}$ e $c=1$. Podemos observar aqui que a forma $ax^2+by^2=c$, poderia ser tratada como $ax^2+by^2=cz^2$, com $a,b,x,y\in\mathbb{Q}$ e $c=z=1$, ou seja, não seria um terno pitagórico, pois $z=1$. Mais detalhes sobre soma de dois quadrados recomendamos as leituras de Moreira (2012, p.2-8) e Santos (2007, p.129-131).

Exemplo 4.35. Sejam $x,y\in\mathbb{Q}$. Provar que os pares (x,y) da circunferência com equação $x^2+y^2=1$ são todos da forma

$$(x,y)=(1,0)\text{ e }(x,y)=\left(\frac{c^2-1}{c^2+1},\frac{2c}{c^2+1}\right).$$

Solução: Primeiramente, consideremos a reta d que passa pelos pontos $(1,0)$ e $(0,c)$, com $c\in\mathbb{Q}$. Com isto, temos que $d: y=ax+b$ e daí, para o ponto $(1,0)$

$$y=ax+b\Rightarrow 0=a\cdot 1+b\Rightarrow a=-b$$

e para o ponto $(0,c)$

$$y=ax+b\Rightarrow c=a\cdot 0+b\Rightarrow c=b\Rightarrow a=-c,$$

ou seja, a reta d possui equação $y=ax+b\Rightarrow y=-c\cdot x+c\Rightarrow y=-c\cdot(x-1)$.

Substituindo a equação da reta d na equação da circunferência, obtemos que a reta d intercepta a circunferência em

$$x^2+y^2=1\Rightarrow$$
$$x^2+[-c\cdot(x-1)]^2=1\Rightarrow$$
$$x^2+[c^2\cdot(x^2-2x+1)]=1\Rightarrow$$
$$x^2+c^2\cdot x^2-2\cdot c^2\cdot x+c^2=1\Rightarrow$$
$$(1+c^2)\cdot x^2-2\cdot c^2\cdot x+c^2-1=0\Rightarrow$$
$$\Delta=(-2\cdot c^2)^2-4\cdot(1+c^2)\cdot(c^2-1)=4\cdot c^4-4\cdot(c^4-1)=4\cdot c^4-4\cdot c^4+4=4.$$
$$x=\frac{-(-2\cdot c^2)\pm\sqrt{4}}{2\cdot(1+c^2)}=\frac{2\cdot c^2\pm 2}{2\cdot(c^2+1)}\Rightarrow$$
$$x_1=\frac{c^2+1}{c^2+1}\Rightarrow x_1=1\Rightarrow y_1=-c\cdot(x_1-1)=-c\cdot(1-1)=0;$$

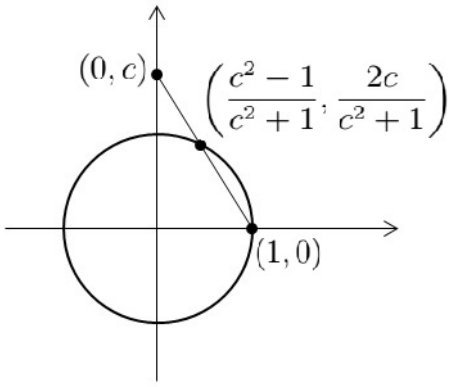
e

$$x_2 = \frac{c^2-1}{c^2+1} \Rightarrow y_2 = -c\cdot(x_2-1) = -c\cdot\left(\frac{c^2-1}{c^2+1}-1\right) = -c\cdot\left(\frac{c^2-1}{c^2+1}-\frac{c^2+1}{c^2+1}\right) \Rightarrow$$

$$y_2 = -c\cdot\left(\frac{c^2-1-c^2-1}{c^2+1}\right) = -c\cdot\left(\frac{-2}{c^2+1}\right) = \frac{2c}{c^2+1},$$

ou seja, justamente nos pontos $(x,y) = (1,0)$ e $(x,y) = \left(\frac{c^2-1}{c^2+1}, \frac{2c}{c^2+1}\right)$, conforme figura que se segue.

Figura 4 – Circunferência



Fonte: Elaborada pelo autor.

Observemos aqui que existe uma bijeção entre os pontos racionais do eixo y, do tipo $(0,c)$ e os pontos racionais da circunferência $x^2+y^2=1$, do tipo $\left(\frac{c^2-1}{c^2+1}, \frac{2c}{c^2+1}\right)$, excetuando-se o ponto $(1,0)$, determinados pela relação $(0,c) \mapsto \left(\frac{c^2-1}{c^2+1}, \frac{2c}{c^2+1}\right)$, pois temos que se $c \in \mathbb{Q}$, então $\left(\frac{c^2-1}{c^2+1}, \frac{2c}{c^2+1}\right)$ é um ponto racional da circunferência.

Por outro lado, dado um ponto racional qualquer da circunferência que seja diferente do ponto $(1,0)$, temos que a reta e, que une este ponto qualquer ao ponto $(1,0)$, possui em sua equação coeficientes racionais, ou seja, a reta e intercepta o eixo y em um ponto $(0,c)$, com $c \in \mathbb{Q}$.

Portanto, sendo $x, y \in \mathbb{Q}$, os pares cartesianos (x,y) da circunferência com equação $x^2+y^2=1$ são todos da forma $(x,y) = (1,0)$ e $(x,y) = \left(\frac{c^2-1}{c^2+1}, \frac{2c}{c^2+1}\right)$. □

De acordo com Moreira (2012, p. 2), temos que as soluções inteiras primitivas da equação $x^2+y^2=z^2$ estão em bijeção, via $(x,y,z) \mapsto (\frac{x}{z}, \frac{y}{z})$, com as soluções racionais da equação $x^2+y^2=1$ e que, quando substituimos $c = d\cdot e$, com $d, e \in \mathbb{Z}$, $e \neq 0$, $e > d$ e $mdc(d,e) = 1$, obtemos as soluções racionais $\left(\frac{e^2-d^2}{e^2+d^2}, \frac{2\cdot d\cdot e}{e^2+d^2}\right)$, as quais têm correspondência bijetiva com os ternos pitagóricos $(e^2-d^2, 2\cdot d\cdot e, e^2+d^2)$.

Exemplo 4.36. Determinar todos os pares cartesianos racionais (x,y) pertencentes a

elipse

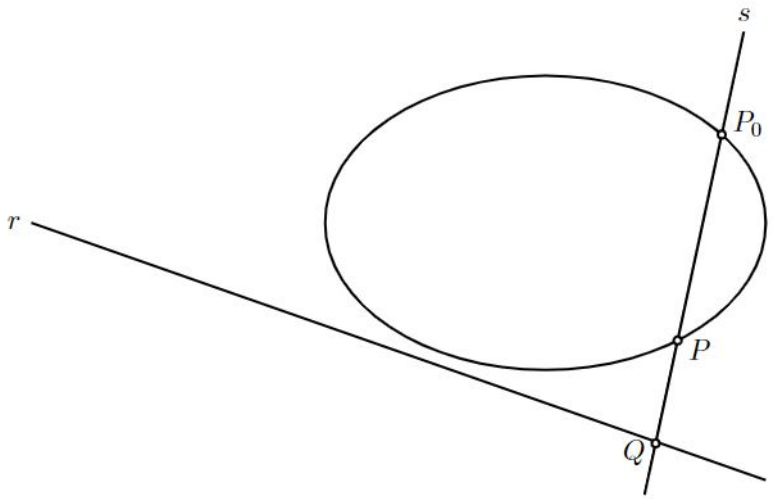
$$\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1.$$

Solução: Ao olharmos para a equação da elipse $\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1$, podemos perceber um destes pontos racionais, seja este $(x_0, y_0) = (1, 1)$, pois

$$\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = \frac{1^2}{\frac{7}{2}} + \frac{1^2}{\frac{7}{5}} = \frac{2}{7} + \frac{5}{7} = \frac{7}{7} = 1.$$

Para determinarmos todos os demais pares cartesianos racionais $Q = (x, y)$ pertencentes a elipse, primeiramente traçamos uma reta t de coeficientes racionais sendo esta paralela à reta tangente à elipse no ponto $Q_0 = (1, 1)$, conforme figura abaixo.

Figura 5 – Elipse



Fonte: Adaptada de Moreira (2012, p. 5).

Em seguida, ao derivarmos a equação da elipse $\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1$ em relação à x, obtemos $\frac{2x}{\frac{7}{2}} + \frac{2yy'}{\frac{7}{5}} = 0$ e, utilizando o ponto Q_0, temos que

$$\frac{2x}{\frac{7}{2}} + \frac{2yy'}{\frac{7}{5}} = 0 \Rightarrow \frac{2 \cdot 1}{\frac{7}{2}} + \frac{2 \cdot 1 \cdot y'}{\frac{7}{5}} = 0 \Rightarrow \frac{10y'}{7} = -\frac{4}{7} \Rightarrow y' = -\frac{2}{5},$$

que nos mostra podermos tomar a reta t definida pela equação $y = -\frac{2}{5} \cdot x - 2$.

Agora, para obtermos um outro ponto $Q \neq Q_0$ da elipse, tomemos a reta u secante a elipse que passa por Q e por Q_0. Como a reta u não é paralela à reta t, ou seja, as retas t e u são concorrentes, então elas determinam um ponto $Q' = (d, e)$ de intersecção.

Temos que a relação $Q \mapsto Q'$ é uma bijeção entre os pontos racionais da elipse,

com exceção do ponto Q_0, e os pontos racionais da reta t, pois sendo Q um ponto racional da elipse, então temos que a equação da reta u possui coeficientes racionais, mostrando que o ponto cartesiano Q' é racional, sendo intersecção das retas t e u as quais possuem equações com coeficientes racionais.

Por outro lado, suponhamos que o ponto $Q' = (d, e)$ seja um ponto cartesiano racional da reta t. Daí, a equação da reta u, determinada pelos pontos cartesianos racionais Q_0 e Q', também possuirá coeficientes racionais e será definida por:

$$\Delta y = m \cdot \Delta x \Rightarrow y - 1 = \frac{e-1}{d-1} \cdot (x-1).$$

Como, pelo enunciado, a equação da elipse possui coeficientes racionais, então a intersecção $Q \neq Q_0$ da reta u com a elipse também é um ponto cartesiano racional, pois temos que $y - 1 = \frac{e-1}{d-1} \cdot (x-1) \Rightarrow y = \frac{e-1}{d-1} \cdot (x-1) + 1$ e, substituindo na equção da elipse, obtemos

$$\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1 \Rightarrow \frac{2}{7} \cdot x^2 + \frac{5}{7} \cdot \left[\frac{e-1}{d-1} \cdot (x-1) + 1\right]^2 - 1 = 0,$$

ou seja, uma equação quadrática com coeficientes racionais, onde uma raiz é $x_0 = 1$ que é o valor da abscissa do ponto Q_0 e a outra raiz é o valor da abscissa do ponto Q que também é racional pelas relações de Girard.

Como o ponto $Q' = (d, e) \in t$, então temos que na equação já obtida da reta $t : y = -\frac{2}{5} \cdot x - 2 \Rightarrow e = -\frac{2}{5} \cdot d - 2 \Rightarrow e = \frac{-2d-10}{5}$ e substituindo na equação da elipse

$$\frac{2}{7} \cdot x^2 + \frac{5}{7} \cdot \left[\frac{e-1}{d-1} \cdot (x-1) + 1\right]^2 - 1 = 0 \Rightarrow$$

$$\frac{2}{7} \cdot x^2 + \frac{5}{7} \cdot \left[\frac{\frac{-2d-10}{5} - 1}{d-1} \cdot (x-1) + 1\right]^2 - 1 = 0 \Rightarrow$$

$$2 \cdot x^2 + 5 \cdot \left[\frac{-(2d+15)}{5 \cdot (d-1)} \cdot (x-1) + 1\right]^2 - 7 = 0 \Rightarrow$$

$$2 \cdot x^2 + \left[\frac{(2d+15)^2}{5 \cdot (d-1)^2} \cdot (x^2 - 2x + 1) - 2 \cdot \frac{2d+15}{(d-1)} \cdot (x-1) \cdot 1 + 5\right] - 7 = 0 \Rightarrow$$

$$2 \cdot x^2 + \frac{(2d+15)^2}{5 \cdot (d-1)^2} \cdot x^2 - \frac{2(2d+15)^2}{5 \cdot (d-1)^2} \cdot x + \frac{(2d+15)^2}{5 \cdot (d-1)^2} - \frac{10(2d+15)}{5 \cdot (d-1)} \cdot x + \frac{10(2d+15)}{5 \cdot (d-1)} - 2 = 0 \Rightarrow$$

$$\left[2 + \frac{(2d+15)^2}{5 \cdot (d-1)^2}\right] x^2 - \left[\frac{2(2d+15)^2}{5 \cdot (d-1)^2} + \frac{20d+150}{5 \cdot (d-1)}\right] x + \left[\frac{(2d+15)^2}{5 \cdot (d-1)^2} + \frac{20d+150}{5 \cdot (d-1)} - 2\right] = 0.$$

Pelas equações de Girard, $x_1 + x_2 = -\frac{b}{a}$ e como $x_1 = x_0 = 1$, então temos que

$$x_1 + x_2 = -\frac{b}{a} = -\frac{-\left[\frac{2(2d+15)^2}{5 \cdot (d-1)^2} + \frac{20d+150}{5 \cdot (d-1)}\right]}{\left[2 + \frac{(2d+15)^2}{5 \cdot (d-1)^2}\right]} \Rightarrow$$

$$1 + x_2 = \frac{\frac{8d^2 + 120d + 450}{5 \cdot (d-1)^2} + \frac{20d^2 - 20d + 150d - 150}{5 \cdot (d-1)^2}}{\frac{10d^2 - 20d + 10}{5 \cdot (d-1)^2} + \frac{4d^2 + 60d + 225}{5 \cdot (d-1)^2}} \Rightarrow$$

$$x_2 = \frac{28d^2 + 250d + 300}{14d^2 + 40d + 235} - 1 = \frac{28d^2 + 250d + 300}{14d^2 + 40d + 235} - \frac{14d^2 + 40d + 235}{14d^2 + 40d + 235} \Rightarrow$$

$$x_2 = \frac{28d^2 + 250d + 300 - 14d^2 - 40d - 235}{14d^2 + 40d + 235} = \frac{14d^2 + 210d + 65}{14d^2 + 40d + 235}.$$

Agora, como o ponto Q pertence à reta u a qual possui coeficientes racionais, o valor da ordenada y do ponto Q também é racional, ou seja, o ponto cartesiano Q é racional, pois substituindo o x_2 na equação da elipse obtemos

$$\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1 \Rightarrow 2x^2 + 5y^2 = 7 \Rightarrow 2 \cdot \left(\frac{14d^2 + 210d + 65}{14d^2 + 40d + 235}\right)^2 + 5y^2 = 7 \Rightarrow$$

$$5y^2 = 7 \cdot \frac{(14d^2 + 40d + 235)^2}{(14d^2 + 40d + 235)^2} - 2 \cdot \frac{(14d^2 + 210d + 65)^2}{(14d^2 + 40d + 235)^2} \Rightarrow$$

$$y^2 = 7 \cdot \frac{(196d^4 + 560d^3 + 3290d^2 + 560d^3 + 1600d^2 + 9400d + 3290d^2 + 9400d + 55225)}{5 \cdot (14d^2 + 40d + 235)^2} -$$

$$2 \cdot \frac{(196d^4 + 2940d^3 + 910d^2 + 2940^3 + 44100d^2 + 13650d + 910d^2 + 13650d + 4225)}{5 \cdot (14d^2 + 40d + 235)^2} \Rightarrow$$

$$y^2 = \frac{(1372d^4 + 7840d^3 + 57260d^2 + 131600d + 386575)}{5 \cdot (14d^2 + 40d + 235)^2} -$$

$$\frac{(392d^4 + 11760d^3 + 91840d^2 + 54600d + 8450)}{5 \cdot (14d^2 + 40d + 235)^2} \Rightarrow$$

$$y^2 = \frac{980d^4 - 3920d^3 - 34580d^2 + 77000d + 378125}{5 \cdot (14d^2 + 40d + 235)^2} \Rightarrow$$

$$y^2 = \frac{196d^4 - 784d^3 - 6916d^2 + 154000d + 75625}{(14d^2 + 40d + 235)^2} \Rightarrow$$

$$y^2 = \frac{(14d^2 - 28d - 275)^2}{(14d^2 + 40d + 235)^2} \Rightarrow y = \frac{14d^2 - 28d - 275}{14d^2 + 40d + 235}.$$

Obtemos os pontos cartesianos racionais Q da elipse quando d percorre todos os racionais $d \in \mathbb{Q}$, inclusive $d = \infty$, ou seja, o limite para $d \to \infty$, que nos fornece o ponto $Q_0 = (1, 1)$, que corresponde ao ponto de intersecção da reta t com a reta u tangente à elipse no ponto Q_0.

Portanto, as coordenadas dos pares cartesianos racionais (x, y) pertencentes a elipse determinada pela equação $\frac{x^2}{\frac{7}{2}} + \frac{y^2}{\frac{7}{5}} = 1$ são dados por

$$Q = \left(\frac{14d^2 + 210d + 65}{14d^2 + 40d + 235}, \frac{14d^2 - 28d - 275}{14d^2 + 40d + 235}\right),$$

onde $x = \dfrac{14d^2 + 210d + 65}{14d^2 + 40d + 235}$ e $y = \dfrac{14d^2 - 28d - 275}{14d^2 + 40d + 235}$. □

4.4.2 *A Equação de Pell*

Definição 4.10. A Equação de Pell é uma equação do tipo $x^2 - ny^2 = 1$, ou seja, é um caso particular das equações diofantinas quadráticas, com $x, y \in \mathbb{Z}$ e $n \in \mathbb{Z}_+^*$ diferente de um quadrado perfeito.

Na equação $x^2 - ny^2 = 1$, temos que $n \in \mathbb{Z}_+^*$ e é diferente de um quadrado perfeito, ou seja, $\sqrt{n}$ é um número irracional. Caso contrário, temos que, se $\sqrt{n} = \dfrac{a}{b}$, com $a, b \in \mathbb{Z}$, $b \neq 0$, $mdc(a, b) = 1$ e $b > 1$, então $\sqrt{n} = \dfrac{a}{b} \Rightarrow n = \dfrac{a^2}{b^2} \Rightarrow n = \left(\dfrac{a}{b}\right)^2$, ou seja, $n \in \mathbb{Q}$, não podendo ser um número inteiro, pois, como $mdc(a, b) = 1$ e $b > 1 \Rightarrow b^2 > 1 \Rightarrow mdc(a^2, b^2) = 1$. Logo, neste caso e por definição, temos que a equação $x^2 - ny^2 = 1$ é conhecida por Equação de Pell.

De acordo com Souza (2017, p. 61-62), esta nomenclatura foi dada em homenagem ao matemático inglês John Pell (1611 - 1685), que somente contribuiu com a publicação de resultados parciais obtidos por William Brouncker (1620 - 1684), em um desafio feito por Fermat e, segundo Souza (2017, p. 52), o método utilizado por Brouncker é semelhante a um método utilizado por matemáticos indianos seis séculos antes.

Euler (1707 - 1783), em sua obra "Álgebra de Euler", mostra como determinar a solução da equação de Pell. A formulação da solução em termos de Frações Contínuas, também é devido a Euler.

Joseph Louis Lagrange (1736 - 1813) foi o primeiro matemático a provar que, para a equação $x^2 - ny^2 = 1$, com n diferente de um quadrado perfeito, existem infinitas soluções inteiras distintas. Estas soluções podem ser usadas para aproximar com precisão a raiz quadrada de n por números racionais da forma $\dfrac{a}{b}$, com $a, b \in \mathbb{Z}$ e $b \neq 0$.

A equação de Pell possui

- um número finito de soluções quando temos $n < 0$ e $n > 0$, com n sendo um quadrado perfeito;
- um número infinito de soluções quando temos $n = 0$; e
- um possui um número infinito de soluções quando $n > 0$, com n diferente de um quadrado perfeito.

Sendo assim, começaremos analisando alguns casos mais simples:

i) quando $n < -1$, temos que $x^2 - ny^2 = 1 \Rightarrow x^2 = 1 + ny^2$, tomando:

1°) $y = 0$, como $1 + ny^2 = 1$ então $x^2 = 1 + ny^2 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1$; e

2°) $y \neq 0$ como $1 + ny^2$ é negativo, então $x^2 = 1 + ny^2 \Rightarrow x^2 = a \Rightarrow x = \sqrt{a}$, com $a \in \mathbb{Z}_-^*$ o que não resulta em valor em $\mathbb{Z}$ para x e, consequentemente, a equação de Pell não possui solução em $\mathbb{Z}$;

ii) quando $n = -1$, temos que $x^2 - ny^2 = 1 \Rightarrow x^2 + y^2 = 1$, tomando:

1°) $y = 0$, então $x^2 + y^2 = 1 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1$; e

2°) $x = 0$ então $x^2 + y^2 = 1 \Rightarrow y^2 = 1 \Rightarrow y = \pm 1$, resultando em quatro soluções $x = 0, y = -1$, $x = 0, y = 1$, $x = -1, y = 0$ e $x = 1, y = 0$ para a equação de Pell nestas condições;

iii) quando $n = b^2$, temos que $x^2 - ny^2 = 1 \Rightarrow x^2 - b^2 \cdot y^2 = 1 \Rightarrow (x + by) \cdot (x - by) = 1 \Rightarrow (x + by) = (x - by) = 1$ ou $(x + by) = (x - by) = -1$, de onde podemos escrever:

1°) $(x + by) = (x - by) = 1 \Rightarrow x = \dfrac{2x}{2} \Rightarrow x = \dfrac{x + x + by - by}{2} \Rightarrow x = \dfrac{(x + by) + (x - by)}{2} \Rightarrow x = \dfrac{1 + 1}{2} \Rightarrow x = \dfrac{2}{2} \Rightarrow x = 1 \Rightarrow y = 0$; e

2°) $(x + by) = (x - by) = -1 \Rightarrow x = \dfrac{2x}{2} \Rightarrow x = \dfrac{x + x + by - by}{2} \Rightarrow x = \dfrac{(x + by) + (x - by)}{2} \Rightarrow x = \dfrac{-1 - 1}{2} \Rightarrow x = \dfrac{-2}{2} \Rightarrow x = -1 \Rightarrow y = 0$, resultando em duas soluções $x = -1, y = 0$ e $x = 1, y = 0$ para a equação de Pell nestas condições; e

iv) quando $n = 0$, temos que $x^2 - ny^2 = 1 \Rightarrow x^2 = 1 \Rightarrow x = \pm 1$, tomando qualquer valor para y, resultando sempre em soluções do tipo $x = -1, \forall y \in \mathbb{Z}$ e $x = 1, \forall y \in \mathbb{Z}$ para a equação de Pell nestas condições.

Souza (2017, p. 63) afirma que o gráfico de uma Equação de Pell, ao utilizarmos o plano cartesiano, tem a forma de uma hipérbole e suas soluções sempre são um par de coordenadas (x, y), com x e $y \in \mathbb{Z}$.

Exemplo 4.37. Verifique se os pontos $(-3, 2)$, $(1, 0)$ e $(7, 4)$ são soluções da equação $x^2 - 3y^2 = 1$.

Solução: Observemos que a equação é $x^2 - 3y^2 = 1$ é uma Equação de Pell e para verificarmos se os pares ordenados são soluções inteiras da equação basta substituirmos os respectivos valores de x e y. Então,

1) para $x = -3$ e $y = 2$, temos que $x^2 - 3y^2 = (-3)^2 - 3 \cdot 2^2 = 9 - 12 = -3 \neq 1$, mostrando que $(-3, 2)$ não é solução da equação;

2) para $x = 1$ e $y = 0$, temos que $x^2 - 3y^2 = 1^2 - 3 \cdot 0^2 = 1 - 0 = 1$, mostrando que $(1, 0)$ é solução da equação; e

3) para $x = 7$ e $y = 4$, temos que $x^2 - 3y^2 = 7^2 - 3 \cdot 4^2 = 49 - 48 = 1$, mostrando que $(7, 4)$ é solução da equação.

Portanto, temos que o ponto $(-3, 2)$ não é solução da equação $x^2 - 3y^2 = 1$, enquanto os pontos $(1, 0)$ e $(7, 4)$ são soluções da equação é $x^2 - 3y^2 = 1$. □

Observemos também que como o gráfico da equação tem a forma de uma hipérbole, então os pontos cartesianos $(1, 0)$ e $(7, 4)$ pertencem à hipérbole, enquanto o ponto cartesiano $(-3, 2)$ não pertence à hipérbole.

Podemos determinar todas as soluções da equação de Pell. Para tal, deve-

mos encontrar uma solução mínima desta equação e utilizá-la juntamente com algumas aplicações de norma.

Com isto, devemos considerar o conjunto $\mathbb{Q}(\sqrt{n}) = \{x + \sqrt{n} \cdot y;\ x, y \in \mathbb{Q}\}$ inicialmente. Seja $a = x + \sqrt{n} \cdot y \in \mathbb{Q}(\sqrt{n})$, com $x, y \in \mathbb{Q}$. Definindo o conjugado de a, temos que $\bar{a} = x - \sqrt{n} \cdot y$ e, definindo a norma como a função

$$N : \mathbb{Q}(\sqrt{n}) \to \mathbb{Q}$$
$$a \mapsto N(a) = a \cdot \bar{a} = (x + \sqrt{n} \cdot y) \cdot (x - \sqrt{n} \cdot y) = x^2 - n \cdot y^2.$$

Como a função N é uma função multiplicativa, então, temos que

$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = N(b \cdot x + \sqrt{n} \cdot c \cdot x + \sqrt{n} \cdot b \cdot y + \sqrt{n} \cdot \sqrt{n} \cdot c \cdot y) \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = N((b \cdot x + n \cdot c \cdot y) + \sqrt{n} \cdot (c \cdot x + b \cdot y)) \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = (b \cdot x + n \cdot c \cdot y)^2 - n \cdot (c \cdot x + b \cdot y))^2 \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = b^2 \cdot x^2 + n^2 \cdot c^2 \cdot y^2 - n \cdot c^2 \cdot x^2 - n \cdot b^2 \cdot y^2)) \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = b^2 \cdot x^2 - n \cdot b^2 \cdot y^2 - n \cdot c^2 \cdot x^2 + n^2 \cdot c^2 \cdot y^2 \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = b^2 \cdot (x^2 - n \cdot y^2) - n \cdot c^2 \cdot (x^2 - n \cdot y^2) \Rightarrow$$
$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = (x^2 - n \cdot y^2) \cdot (b^2 - n \cdot c^2),$$

ou seja,

$$N((x + \sqrt{n} \cdot y)(b + \sqrt{n} \cdot c)) = N(x + \sqrt{n} \cdot y) \cdot N(b + \sqrt{n} \cdot c), \forall x, y, b, c \in \mathbb{Z}.$$

Devido a esta propriedade da multiplicatividade da norma, podemos observar que se a equação tem alguma solução (x_1, y_1) com $y_1 \neq 0$ então esta equação possui infinitas soluções.

Não é objetivo deste trabalho, mas, deixando como nota e fonte de pesquisa, segundo Souza (2017, p. 64), generalizando esta solução, geralmente, como, na equação Equação de Pell, $x_1^2 - ny_1^2 = \pm 1$, então

$$N((x_1 + \sqrt{n} \cdot y_1)^d) = (x_1 + \sqrt{n} \cdot y_1)^d \cdot (x_1 - \sqrt{n} \cdot y_1)^d = (\pm 1)^d,$$

com $d \in \mathbb{N}$, e substituindo este resultado em $x_d + \sqrt{n} \cdot y^d$, obtemos

$$x_d + \sqrt{n} \cdot y_d = (x_1 + \sqrt{n} \cdot y_1)^d = \sum_{e=0}^{d} \begin{pmatrix} d \\ e \end{pmatrix} (\sqrt{n})^d \cdot x_1^{d-e} \cdot y_1^d,$$

onde

$$x_d = \sum_{e=0}^{\lfloor \frac{d}{2} \rfloor} \begin{pmatrix} d \\ 2e \end{pmatrix} n^e \cdot x_1^{d-2e} \cdot y_1^2 e \quad \text{e} \quad y_d = \sum_{e=0}^{\lfloor \frac{d-1}{2} \rfloor} \begin{pmatrix} d \\ 2e+1 \end{pmatrix} n^e \cdot x_1^{d-2e-1} \cdot y_1^{2e+1},$$

e, daí, obtemos $x_d^2 - n \cdot y_d^2 = \pm 1$, $\forall d \in \mathbb{N}$.

Proposição 4.8. *Temos que o valor $x + \sqrt{n} \cdot y$ é univocamente representado, ou seja, se $x_1 + \sqrt{n} \cdot y_1 = x_2 + \sqrt{n} \cdot y_2$, com $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, então $x_1 = x_2$ e $y_1 = y_2$.*

Demonstração: Observemos que se

$$x_1 + \sqrt{n} \cdot y_1 = x_2 + \sqrt{n} \cdot y_2 \Rightarrow$$
$$\sqrt{n} \cdot y_1 - \sqrt{n} \cdot y_2 = x_2 - x_1 \Rightarrow$$
$$\sqrt{n} \cdot (y_1 - y_2) = x_2 - x_1.$$

Daí, temos que se

- $y_1 = y_2$, então $x_2 - x_1 = \sqrt{n} \cdot (y_1 - y_2) = 0$. Logo, $x_1 = x_2$; e
- $y_1 - y_2 \neq 0$, então $\sqrt{n} = \dfrac{x_2 - x_1}{y_1 - y_2} \in \mathbb{Q}$.

Então chegamos a um absurdo, já que a razão entre números racionais é sempre um número racional e n, por definição, deve ser um número inteiro positivo diferente de um quadrado perfeito, ou seja, $\sqrt{n}$ deve ser um número irracional.

Portanto, temos que o valor $x + \sqrt{n} \cdot y$ é univocamente representado. ■

Sendo assim, temos que as soluções inteiras (x, y) para a equação de Pell são os elementos do conjunto $\mathbb{Z}[\sqrt{n}] = \{x + \sqrt{n} \cdot y; x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{n})$, que possui sua norma

$$N(x + \sqrt{n} \cdot y) = x^2 - \sqrt{n} \cdot y^2 = 1.$$

Teorema 4.6. *Temos que a equação de Pell $x^2 - ny^2 = 1$, com $x, y \in \mathbb{Z}$ e $n \in \mathbb{Z}_+^*$ e diferente de um quadrado perfeito, possui solução não trivial em $\mathbb{Z}_+^*$, ou seja, possui solução com $x + \sqrt{n} \cdot y > 1$.*

Demonstração: Sabemos que $\sqrt{n}$ é um número irracional. Daí, a desigualdade

$$\left|\sqrt{n} - \frac{a}{b}\right| < \frac{1}{b^2}$$

indica infinitas soluções em $\mathbb{Q}$ para $\dfrac{a}{b}$.

Temos também que

$$N(a + \sqrt{n} \cdot b) = a^2 - n \cdot b^2 = \frac{a^2 \cdot b^2}{b^2} - n \cdot b^2 = b^2 \left(\frac{a}{b} + \sqrt{n}\right) \cdot \left(\frac{a}{b} - \sqrt{n}\right).$$

Logo, se $\left|\sqrt{n} - \dfrac{a}{b}\right| < \dfrac{1}{b^2}$, então temos que

$$\left|a^2 - n \cdot b^2\right| = b^2 \left|\left(\frac{a}{b} + \sqrt{n}\right)\right| \cdot \left|\left(\frac{a}{b} - \sqrt{n}\right)\right| < b^2 \left|\left(\frac{a}{b} + \sqrt{n}\right)\right| \cdot \frac{1}{b^2} = \left|\left(\frac{a}{b} + \sqrt{n}\right)\right|.$$

Agora, utilizando a desigualdade triangular, temos que

$$\left|\left(\frac{a}{b} + \sqrt{n}\right)\right| = \left|\left(\frac{a}{b} + \sqrt{n} + \sqrt{n} - \sqrt{n}\right)\right| \leqslant 2 \cdot \sqrt{n} + \left|\left(\frac{a}{b} - \sqrt{n}\right)\right| < 2 \cdot \sqrt{n} + \frac{1}{b^2} \leqslant 2 \cdot \sqrt{n} + 1.$$

Com isto, prova-se que existem infinitos pares (a_i, b_i), com $a_i, b_i, i \in \mathbb{Z}_+^*$, onde $\left|\sqrt{n} - \dfrac{a_i}{b_i}\right| < \dfrac{1}{b_i^2}$, $|N(a_i + \sqrt{n} \cdot b_i)| = |a_i^2 - n \cdot b_i^2| < 2 \cdot \sqrt{n} + 1$, o que implica em possibilidades finitas de $a_i^2 - n \cdot b_i^2 \in \mathbb{Z}$.

Sendo assim, podemos observar que

- deve existir $c \in \mathbb{Z}$ tal que $c = a_i^2 - n \cdot b_i^2$, com $i \in \mathbb{Z}_+^*$; e
- $c \neq 0$, caso contrário, $c = a_i^2 - n \cdot b_i^2 \Rightarrow a_i^2 - n \cdot b_i^2 = 0 \Rightarrow a_i^2 = n \cdot b_i^2 \Rightarrow n = \dfrac{a_i^2}{b_i^2} \Rightarrow$ $n = \left(\dfrac{a_i}{b_i}\right)^2 \Rightarrow \sqrt{n} = \dfrac{a_i}{b_i} \in \mathbb{Q}$, onde chegamos a um absurdo já que $\sqrt{n}$ é irracional.

E, daí, podemos construir (d_j) e (e_j), com $j \in \mathbb{N}$, duas sequências crescentes de pares de números inteiros positivos tais que

$$d_j^2 + n \cdot e_j^2 = c, \ \forall j.$$

Sabemos que o número $x + \sqrt{n} \cdot y$ possui representação única, e, pelos resultados obtidos acima, se tomarmos $j < k$, com $j, k \in \mathbb{N}$ então $d_j + n \cdot e_j \neq d_k + n \cdot e_k$.

Suponhamos, sem perda de generalidade, que $1 \leqslant d_j + \sqrt{n} \cdot e_j < d_k + \sqrt{n} \cdot e_k$ e façamos

$$x + \sqrt{n} \cdot y = \frac{d_k + \sqrt{n} \cdot e_k}{d_j + \sqrt{n} \cdot e_j} > 1 \Rightarrow$$

$$x + \sqrt{n} \cdot y = \frac{(d_k + \sqrt{n} \cdot e_k) \cdot (d_j - \sqrt{n} \cdot e_j)}{(d_j + \sqrt{n} \cdot e_j) \cdot (d_j - \sqrt{n} \cdot e_j)} > 1 \Rightarrow$$

$$x + \sqrt{n} \cdot y = \frac{(d_j \cdot d_k - d_k \cdot \sqrt{n} \cdot e_j + d_j \cdot \sqrt{n} \cdot e_k - n \cdot e_j \cdot e_k)}{(d_j^2 + n \cdot e_j^2)} > 1 \Rightarrow$$

$$x + \sqrt{n} \cdot y = \frac{(d_j \cdot d_k - n \cdot e_j \cdot e_k) + \sqrt{n} \cdot (d_j \cdot e_k - d_k \cdot e_j)}{c} > 1 \Rightarrow$$

$$x + \sqrt{n} \cdot y = \frac{d_j \cdot d_k - n \cdot e_j \cdot e_k}{c} + \sqrt{n} \cdot \frac{d_j \cdot e_k - d_k \cdot e_j}{c} > 1,$$

com $x = \dfrac{d_j \cdot d_k - n \cdot e_j \cdot e_k}{c}$ e $y = \dfrac{d_j \cdot e_k - d_k \cdot e_j}{c}$, e, como $x, y \in \mathbb{Z}$, então temos que $d_j \cdot d_k - n \cdot e_j \cdot e_k$ e $d_j \cdot e_k - d_k \cdot e_j$ são divisíveis por c e $x + \sqrt{n}y = \dfrac{d_k + \sqrt{n} \cdot e_k}{d_j + \sqrt{n} \cdot e_j} > 1$.

Por outro lado, utilizando os resultados já obtidos anteriormente, temos que

$$(x + \sqrt{n} \cdot y) \cdot (d_j + \sqrt{n} \cdot e_j) = (d_k + \sqrt{n} \cdot e_k) \Rightarrow$$

$$N(x + \sqrt{n}y) \cdot N(d_j + \sqrt{n} \cdot e_j) = N(d_k + \sqrt{n} \cdot e_k) = f,$$

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

Como $N(d_j + \sqrt{n} \cdot e_j) = N(d_k + \sqrt{n} \cdot e_k) = f$, então, consequentemente, temos que $N(x + \sqrt{n} \cdot y) \cdot N(d_j + \sqrt{n} \cdot e_j) = N(d_k + \sqrt{n} \cdot e_k) \Rightarrow N(x + \sqrt{n}y) \cdot f = f \Rightarrow N(x + \sqrt{n} \cdot y) = 1$.

Daí, obtemos que $x^2 + n \cdot y^2 = N(x + \sqrt{n} \cdot y) \Rightarrow x^2 + n \cdot y^2 = 1$.

Portanto, temos que a equação de Pell $x^2 - ny^2 = 1$, com $x, y \in \mathbb{Z}$ e $n \in \mathbb{Z}_+^*$ e diferente de um quadrado perfeito, possui solução não trivial em $\mathbb{Z}_+^*$, ou seja, possui solução com $x + \sqrt{n}.y > 1$. ■

Segundo Filipe (2020, p. 1), pelo Teorema 4.6, toda equação de Pell tem solução. Logo, dentre todas as soluções com $x + \sqrt{n} \cdot y$, podemos tomar uma solução minimal, ou seja, que possui $x + \sqrt{n} \cdot y$ mínimo.

Também, em concordância com Filipe (2020, p. 2), "um método rápido de encontrar a solução minimal é olhando para a fração contínua de $\sqrt{n}$. Escrevendo $\sqrt{n} = [a_0; a_1, a_2, a_3, ..., a_k]$". Sendo assim, descreveremos e exemplificaremos o método das frações contínuas a seguir.

Nas frações contínuas, devemos escrever $\sqrt{n} = [a_0; a_1, a_2, a_3, ..., a_b] = \dfrac{x_1}{y_1}$, onde n está definido na equação de Pell, $a_0, a_1, a_2, a_3, a_b \in \mathbb{N}$, $a_0 = \lfloor \sqrt{n} \rfloor$, x_1 e y_1 são os valores da solução mínima de uma equação de Pell.

Para fazer o cálculo da solução mínima, devemos efetuar os seguintes passos:

1 *passo*: tomamos o valor de $\sqrt{n}$, com n definido na equação de Pell;

2 *passo*: somamos e subtraímos $\lfloor \sqrt{n} \rfloor$ ao valor de $\sqrt{n}$, ou seja,

$$\sqrt{n} = \sqrt{n} + \lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n} \rfloor;$$

3 *passo*: tomamos o valor positivo de $\lfloor\sqrt{n}\rfloor$ como o a_0, enquanto $(\sqrt{n}-\lfloor\sqrt{n}\rfloor)$ multiplicamos e divididimos por $(\sqrt{n}+\lfloor\sqrt{n}\rfloor)$, ou seja,

$$\sqrt{n} = a_0 + \frac{(\sqrt{n}-\lfloor\sqrt{n}\rfloor)\cdot(\sqrt{n}+\lfloor\sqrt{n}\rfloor)}{(\sqrt{n}+\lfloor\sqrt{n}\rfloor)};$$

4 *passo*: efetuamos os cálculos possíveis na fração criada no 3° passo, e depois devemos inverter as posições das partes desta fração criando-se uma nova fração com numerador 1 e denominador sendo uma outra fração que possui numerador $(\sqrt{n}+\lfloor\sqrt{n}\rfloor)$ e denominador $c \in \mathbb{N}$ o que restou dos cálculos realizados citados no início deste passo, ou seja,

$$\sqrt{n} = a_0 + \frac{c}{\sqrt{n}+\lfloor\sqrt{n}\rfloor} = a_0 + \frac{1}{\dfrac{\sqrt{n}+\lfloor\sqrt{n}\rfloor}{c}},$$

com $c = (\sqrt{n}-\lfloor\sqrt{n}\rfloor)\cdot(\sqrt{n}+\lfloor\sqrt{n}\rfloor)$;

5 *passo*: aqui, passamos a repetir o processo a partir do 2° passo, onde devemos somar e subtrair $\lfloor\sqrt{n}\rfloor$ ao valor de $(\sqrt{n}+\lfloor\sqrt{n}\rfloor)$, ou seja,

$$\sqrt{n} = a_0 + \frac{1}{\dfrac{\sqrt{n}+\lfloor\sqrt{n}\rfloor+\lfloor\sqrt{n}\rfloor-\lfloor\sqrt{n}\rfloor}{c}};$$

6 *passo*: podemos agora extrair uma parte inteira positiva do denominador desta fração que possui numerador 1 e obtemos, com isto, o valor de $a_1 = \dfrac{d\cdot c}{c}$, com $d \in \mathbb{N}$, enquanto $(\sqrt{n}-e)$, com $e \in \mathbb{Z}$ sendo o número que restou junto à $\sqrt{n}$ em um numerador, multiplicamos e divididimos por $(\sqrt{n}+e)$, ou seja,

$$\sqrt{n} = a_0 + \frac{1}{a_1 + \dfrac{(\sqrt{n}-e)\cdot(\sqrt{n}+e)}{c\cdot(\sqrt{n}+e)}};$$

7 *passo*: efetuamos os cálculos possíveis na fração criada no 6° passo, e depois devemos inverter as posições das partes desta fração criando-se uma nova fração com numerador 1 e denominador sendo uma outra fração que possui numerador $(\sqrt{n}+e)$ e denominador $c_1 \in \mathbb{N}$ sendo o que restou dos cálculos realizados citados no início deste passo, ou seja,

$$\sqrt{n} = a_0 + \frac{1}{a_1 + \dfrac{c_1}{\sqrt{n}+e}} = a_0 + \frac{1}{a_1 + \dfrac{1}{\dfrac{\sqrt{n}+e}{c_1}}},$$

com $c_1 = \dfrac{(\sqrt{n}-e)\cdot(\sqrt{n}+e)}{c}$;

8 *passo*: devemos repetir sucessivamente este processo até conseguirmos obter em $c_i = 1$, com $i \in \mathbb{N}$, daí repetimos o 2° passo e aparecerá novamente a expressão $(\sqrt{n}-\lfloor\sqrt{n}\rfloor)$, ou seja, quando isto acontecer, o processo volta a ser igual desde o começo;

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{\sqrt{n}+e_i}{c_i}}}} \Rightarrow$$

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{\sqrt{n}+e_i+\lfloor\sqrt{n}\rfloor-\lfloor\sqrt{n}\rfloor}{1}}}} \Rightarrow$$

$$\sqrt{n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + a_b + \sqrt{n} - \lfloor\sqrt{n}\rfloor}}} = \frac{x_1}{y_1}$$

Neste momento, temos que $b \in \mathbb{N}$ e, quando b for par, devemos considerar a fração contínua até o termo a_{b-1}, ou seja,

$$\frac{x_1}{y_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{b-1}}}}}}$$

e, quando b for ímpar, devemos considerar a fração contínua até o termo a_{2b-1}, ou seja,

$$\frac{x_1}{y_1} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{2b-1}}}}}}.$$

Exemplo 4.38. Determinar a solução mínima de $x^2 - 41y^2 = 1$.

Solução: Para fazermos isto, basta escrevermos a fração contínua de $\sqrt{41}$.

Primeiramente, somamos e subtraímos $\lfloor\sqrt{41}\rfloor$ de $\sqrt{41}$, obtendo

$$\sqrt{41} = \sqrt{41} + \lfloor\sqrt{41}\rfloor - \lfloor\sqrt{41}\rfloor = 6 + (\sqrt{41} - 6).$$

No segundo momento, multiplicamos e dividimos $(\sqrt{41} - 6)$ por $(\sqrt{41} + 6)$, obtendo

$$\sqrt{41} = 6 + \frac{(\sqrt{41}-6)\cdot(\sqrt{41}+6)}{(\sqrt{41}+6)} = 6 + \frac{5}{(\sqrt{41}+6)} = 6 + \cfrac{1}{\cfrac{\sqrt{41}+6}{5}}.$$

Agora, somamos e subtraímos $\lfloor\sqrt{41}\rfloor$ de $\sqrt{41}+6$, obtendo

$$\sqrt{41} = 6 + \cfrac{1}{\cfrac{\sqrt{41}+6+\lfloor\sqrt{41}\rfloor-\lfloor\sqrt{41}\rfloor}{5}} = 6 + \cfrac{1}{\cfrac{\sqrt{41}+6+6-6}{5}} \Rightarrow$$

$$\sqrt{41} = 6 + \frac{1}{\frac{10 + \sqrt{41} - 4}{5}} = 6 + \frac{1}{2 + \frac{\sqrt{41} - 4}{5}}.$$

Daí, multiplicamos e dividimos $\frac{\sqrt{41} - 4}{5}$ por $(\sqrt{41} + 4)$, obtendo

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{(\sqrt{41} - 4) \cdot (\sqrt{41} + 4)}{5 \cdot (\sqrt{41} + 4)}} = 6 + \frac{1}{2 + \frac{25}{5 \cdot (\sqrt{41} + 4)}} \Rightarrow$$

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{5}{\sqrt{41} + 4}} = 6 + \frac{1}{2 + \frac{1}{\frac{\sqrt{41} + 4}{5}}}.$$

Novamente, somamos e subtraímos $\lfloor \sqrt{41} \rfloor$ agora de $\sqrt{41} + 4$, obtendo

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{\frac{\sqrt{41} + 4 + \lfloor \sqrt{41} \rfloor - \lfloor \sqrt{41} \rfloor}{5}}} = 6 + \frac{1}{2 + \frac{1}{\frac{\sqrt{41} + 4 + 6 - 6}{5}}} \Rightarrow$$

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{\frac{10 + \sqrt{41} - 6}{5}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{\sqrt{41} - 6}{5}}}.$$

Agora, multiplicamos e dividimos $\frac{\sqrt{41} - 6}{5}$ por $(\sqrt{41} + 6)$, obtendo

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{(\sqrt{41} - 6) \cdot (\sqrt{41} + 6)}{5 \cdot (\sqrt{41} + 6)}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{5}{5 \cdot (\sqrt{41} + 6)}}}$$

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{41} + 6}}}.$$

Mais uma vez, somamos e subtraímos $\lfloor \sqrt{41} \rfloor$ agora de $\sqrt{41} + 6$, obtendo

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{41} + 6 + \lfloor \sqrt{41} \rfloor - \lfloor \sqrt{41} \rfloor}}} \Rightarrow$$

$$\sqrt{41} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\sqrt{41} + 6 + 6 - 6}}} = 6 + \frac{1}{2 + \frac{1}{2 + \frac{1}{12 + \sqrt{41} - 6}}}.$$

Como o próximo passo é novamente multiplicar e dividir $\sqrt{41} - 6$ por $(\sqrt{41} + 6)$, então, observemos aqui, que o processo começará a se repetir do começo.

Neste momento, podemos representar $\sqrt{41} = [6; 2, 2, 12]$, com $a_0 = 6$, $a_1 = 2$, $a_2 = 2$ e $a_3 = 12$. Como a repetição começa no $a_3 = 12$, que possui o índice ímpar, então temos que tomar o processo até o a_5 para obtermos a solução mínima, ou seja,

$$\frac{x_1}{y_1} = 6 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{12 + \dfrac{1}{2 + \dfrac{1}{2}}}}} = 6 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{12 + \dfrac{1}{\frac{5}{2}}}}} = 6 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{12 + \frac{2}{5}}}} \Rightarrow$$

$$\frac{x_1}{y_1} = 6 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{\frac{60}{5} + \frac{2}{5}}}} = 6 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{\frac{62}{5}}}} = 6 + \frac{1}{2 + \dfrac{1}{2 + \frac{5}{62}}} \Rightarrow$$

$$\frac{x_1}{y_1} = 6 + \frac{1}{2 + \dfrac{1}{\frac{129}{62}}} = 6 + \frac{1}{2 + \frac{62}{129}} = 6 + \frac{1}{2 + \dfrac{1}{\frac{124}{62} + \frac{5}{62}}} \Rightarrow$$

$$\frac{x_1}{y_1} = 6 + \frac{1}{\frac{258}{129} + \frac{62}{129}} = 6 + \frac{1}{\frac{320}{129}} = 6 + \frac{129}{320} = \frac{1920}{320} + \frac{129}{320} = \frac{2049}{320}.$$

Logo, temos que $x_1 = 2049$ e $y_1 = 320$ é a solução mínima.

Portanto, a solução mínima de $x^2 - 41y^2 = 1$ é o par $(2049, 320)$. □

Exemplo 4.39. Determinar as soluções mínima e geral de $x^2 - 19y^2 = 1$.

Solução: Para determinarmos a solução mínima, basta escrevermos a fração contínua de $\sqrt{19}$. Sendo assim, utilizando passos similares aos feitos no exemplo 4.38, temos que

$$\sqrt{19} = 4 + (\sqrt{19} - 4) = 4 + \frac{(\sqrt{19} - 4) \cdot (\sqrt{19} + 4)}{(\sqrt{19} + 4)} = 4 + \frac{3}{(\sqrt{19} + 4)} = 4 + \frac{1}{\dfrac{\sqrt{19} + 4}{3}}$$

$$\sqrt{19} = 4 + \frac{1}{\dfrac{\sqrt{19} + 4 + 4 - 4}{3}} = 4 + \frac{1}{2 + \dfrac{(\sqrt{19} - 2) \cdot (\sqrt{19} + 2)}{3 \cdot (\sqrt{19} + 2)}} = 4 + \frac{1}{2 + \dfrac{15}{3 \cdot (\sqrt{19} + 2)}}$$

$$\sqrt{19} = 4 + \frac{1}{2 + \dfrac{1}{\dfrac{\sqrt{19} + 2 + 4 - 4}{5}}} = 4 + \frac{1}{2 + \dfrac{1}{1 + \dfrac{(\sqrt{19} - 3) \cdot (\sqrt{19} + 3)}{5 \cdot (\sqrt{19} + 3)}}}$$

$$\sqrt{19} = 4 + \frac{1}{2 + \dfrac{1}{1 + \dfrac{10}{5 \cdot (\sqrt{19} + 3)}}} = 4 + \frac{1}{2 + \dfrac{1}{1 + \dfrac{1}{\dfrac{\sqrt{19} + 3 + 4 - 4}{2}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{(\sqrt{19}-3)\cdot(\sqrt{19}+3)}{2\cdot(\sqrt{19}+3)}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{10}{2\cdot(\sqrt{19}+3)}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{\cfrac{\sqrt{19}+3+4-4}{5}}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{(\sqrt{19}-2)\cdot(\sqrt{19}+2)}{5\cdot(\sqrt{19}+2)}}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{15}{5\cdot(\sqrt{19}+2)}}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{\cfrac{\sqrt{19}+2+4-4}{3}}}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{(\sqrt{19}-4)\cdot(\sqrt{19}+4)}{3\cdot(\sqrt{19}+4)}}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{3}{3\cdot(\sqrt{19}+4)}}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{19}+4+4-4}}}}}}$$

$$\sqrt{19} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{8 + \sqrt{19} - 4}}}}}}.$$

Observemos aqui que o processo começará a se repetir do começo. Neste momento, podemos representar $\sqrt{19} = [4; 2, 1, 3, 1, 2, 8]$, com $a_0 = 4$, $a_1 = 2$, $a_2 = 1$, $a_3 = 3$, $a_4 = 1$, $a_5 = 2$ e $a_6 = 8$. Com isto, podemos representar . Como a repetição começa no a_6, que possui o índice par, então temos que tomar o processo até o a_5 para

obtermos a solução mínima, ou seja,

$$\frac{x_1}{y_1} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2}}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{\cfrac{5}{2}}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{2}{5}}}}$$

$$\frac{x_1}{y_1} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cfrac{17}{5}}}} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{5}{17}}} = 4 + \cfrac{1}{2 + \cfrac{1}{\cfrac{22}{17}}}$$

$$\frac{x_1}{y_1} = 4 + \cfrac{1}{2 + \cfrac{17}{22}} = 4 + \frac{1}{\cfrac{61}{22}} = 4 + \frac{22}{61} = \frac{266}{61}.$$

Logo, temos que $x_1 = 266$ e $y_1 = 61$ é a solução mínima.

Agora, para determinarmos a solução geral de $x^2 - 19y^2 = 1$, tomemos o par (x_d, y_d), com $x_d - \sqrt{19} \cdot y_d = (x_1 - \sqrt{19} \cdot y_1)^d = (266 - \sqrt{19} \cdot 61)^d$, onde temos que $d \in \mathbb{N}$, $x_d = \dfrac{(x_1 + \sqrt{19} \cdot y_1)^d + (x_1 - \sqrt{19} \cdot y_1)^d}{2} = \dfrac{(266 + \sqrt{19} \cdot 61)^d + (266 - \sqrt{19} \cdot 61)^d}{2}$ e $y_d = \dfrac{(x_1 + \sqrt{19} \cdot y_1)^d - (x_1 - \sqrt{19} \cdot y_1)^d}{2 \cdot \sqrt{19}} = \dfrac{(266 + \sqrt{19} \cdot 61)^d - (266 - \sqrt{19} \cdot 61)^d}{2 \cdot \sqrt{19}}$.

Portanto, temos que a solução mínima é o par $(266, 61)$ e a solução geral é o par (x_d, y_d), com $x_d - \sqrt{19} \cdot y_d = (x_1 - \sqrt{19} \cdot y_1)^d = (266 - \sqrt{19} \cdot 61)^d$, onde temos que $d \in \mathbb{N}$,

$$x_d = \frac{(266 + \sqrt{19} \cdot 61)^d + (266 - \sqrt{19} \cdot 61)^d}{2}$$

e

$$y_d = \frac{(266 + \sqrt{19} \cdot 61)^d - (266 - \sqrt{19} \cdot 61)^d}{2 \cdot \sqrt{19}}$$

para a equação $x^2 - 19y^2 = 1$. □

Exemplo 4.40. Mostrar que existem infinitos a tais que a soma $1 + 2 + 3 + ... + a$ é um quadrado perfeito.

Solução: Como $1 + 2 + 3 + ... + a$ é a soma dos a primeiros termos de uma progressão aritmética de razão 1, então temos que

$$1 + 2 + 3 + ... + a = \frac{a(a+1)}{2}.$$

Daí, para esta soma poder ser um quadrado perfeito, então $\dfrac{a(a+1)}{2}$ deve ser da forma b^2. Com isto, temos que

$$\frac{a(a+1)}{2} = b^2 \Rightarrow$$

$$\frac{a^2 + a}{2} = b^2 \Rightarrow$$

$$a^2 + a = 2 \cdot b^2 \Rightarrow$$
$$4 \cdot (a^2 + a) = 4 \cdot (2 \cdot b^2) \Rightarrow$$
$$4 \cdot a^2 + 4 \cdot a = 8 \cdot b^2 \Rightarrow$$
$$4 \cdot a^2 + 4 \cdot a + 1 = 8 \cdot b^2 + 1 \Rightarrow$$
$$(2 \cdot a^2 + 1)^2 - 2 \cdot (2 \cdot b)^2 = 1,$$

que é uma equação de Pell da forma $x^2 - 2y^2 = 1$, com $x = 2 \cdot a^2 + 1$ e $y = 2 \cdot b$, ou seja, é uma equação que possui infinitas soluções.

Analisando ambos membros da equação $x^2 - 2y^2 = 1$, temos que, do lado esquerdo da igualdade, $x = 2 \cdot a^2 + 1 = 2 \cdot c + 1$ é ímpar, com $c \in \mathbb{N}$ e $c = a^2$ e $y = 2 \cdot b$ é par e $x^2 - 2y^2$ resulta em um valor ímpar, e, do lado direito da igualdade, temos um valor ímpar, o que é compatível. Logo, temos que existem infinitas soluções com x ímpar e y par.

Portanto, temos infinitos valores de a tais que a soma $1 + 2 + 3 + ... + a$ é um quadrado perfeito. □

Exemplo 4.41. Determinar todas as soluções inteiras positivas e não nulas da equação $x^2 - 2y^2 = 1$.

Solução: Nesta questão, para não calcularmos novamente uma fração contínua, no caso, a fração contínua de $\sqrt{2}$, então tentemos encontrar um par (x_1, y_1) que seja a solução mínima inteira positiva e não nula da equação $x^2 - 2y^2 = 1$. Sendo assim, verificaremos alguns pares a seguir.

Para $(x, y) = (1, 1)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 1^2 - 2 \cdot 1^2 = 1 - 2 = -1 \neq 1$, ou seja, $(1, 1)$ não é solução da equação.

Para $(x, y) = (1, 2)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 1^2 - 2 \cdot 2^2 = 1 - 8 = -7 \neq 1$, ou seja, $(1, 2)$ não é solução da equação.

Para $(x, y) = (2, 1)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 2^2 - 2 \cdot 1^2 = 4 - 2 = 2 \neq 1$, ou seja, $(2, 1)$ não é solução da equação.

Para $(x, y) = (2, 2)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 2^2 - 2 \cdot 2^2 = 4 - 8 = -4 \neq 1$, ou seja, $(2, 2)$ não é solução da equação.

Para $(x, y) = (2, 3)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 2^2 - 2 \cdot 3^2 = 4 - 18 = -14 \neq 1$, ou seja, $(2, 3)$ não é solução da equação.

Para $(x, y) = (3, 2)$, temos que $x^2 - 2y^2 = 1 \Rightarrow 3^2 - 2 \cdot 2^2 = 9 - 8 = 1$, ou seja, $(3, 2)$ é solução mínima da equação.

Agora, para podermos determinar a solução geral da equação $x^2 - 2y^2 = 1$, temos que tomar o par (x_d, y_d), com $x_d - \sqrt{2} \cdot y_d = (x_1 - \sqrt{2} \cdot y_1)^d = (3 - 2 \cdot \sqrt{2})^d$, onde temos que $d \in \mathbb{N}$, $x_d = \dfrac{(x_1 + \sqrt{2} \cdot y_1)^d + (x_1 - \sqrt{2} \cdot y_1)^d}{2} = \dfrac{(3 + 2 \cdot \sqrt{2})^d + (3 - 2 \cdot \sqrt{2})^d}{2}$ e $y_d = \dfrac{(x_1 + \sqrt{2} \cdot y_1)^d - (x_1 - \sqrt{2} \cdot y_1)^d}{2 \cdot \sqrt{2}} = \dfrac{(3 + 2 \cdot \sqrt{2})^d - (3 - 2 \cdot \sqrt{2})^d}{2 \cdot \sqrt{2}}$.

Portanto, para a equação $x^2 - 2y^2 = 1$, temos que a solução mínima é o par

$(3, 2)$ e a solução geral é o par (x_d, y_d), com

$$x_d - \sqrt{2} \cdot y_d = (x_1 - \sqrt{2} \cdot y_1)^d = (3 - 2 \cdot \sqrt{2})^d,$$

onde $d \in \mathbb{N}$, $x_d = \dfrac{(3 + 2 \cdot \sqrt{2})^d + (3 - 2 \cdot \sqrt{2})^d}{2}$ e $y_d = \dfrac{(3 + 2 \cdot \sqrt{2})^d - (3 - 2 \cdot \sqrt{2})^d}{2 \cdot \sqrt{2}}$. □

Exemplo 4.42. Demonstrar que existem infinitos ternos inteiros (a, b, c), com $a, b, c \in \mathbb{N}$, que satisfazem a relação:

$$2 \cdot a^2 + 3 \cdot b^2 - 5 \cdot c^2 = 1997.$$

Solução: Para realizarmos a resolução deste exemplo, devemos transformar a equação dada $2 \cdot a^2 + 3 \cdot b^2 - 5 \cdot c^2 = 1997$ em uma outra equação da forma $x^2 - n \cdot y^2 = 1$, ou seja, deixá-la na forma de uma equação de Pell, que possui infinitas soluções, mostrando assim que a equação inicial também possui infinitas soluções.

Primeiramente, reescreveremos a equação inicial, efetuando os seguintes passos:

passo 1**:** passamos o monônio que possui a incógnita a para o segundo membro, ou seja, $2 \cdot a^2 + 3 \cdot b^2 - 5 \cdot c^2 = 1997 \Rightarrow 3 \cdot b^2 - 5 \cdot c^2 = 1997 - 2 \cdot a^2$;

passo 2**:** substituímos a por um valor particular, determinado por $\left\lfloor \sqrt{\dfrac{1997}{2}} \right\rfloor$, que, no caso, teremos $a = \left\lfloor \sqrt{\dfrac{1997}{2}} \right\rfloor = 31$, resultando em $3 \cdot b^2 - 5 \cdot c^2 = 1997 - 2 \cdot a^2 \Rightarrow 3 \cdot b^2 - 5 \cdot c^2 = 1997 - 2 \cdot 31^2 \Rightarrow 3 \cdot b^2 - 5 \cdot c^2 = 1997 - 2 \cdot 961 \Rightarrow 3 \cdot b^2 - 5 \cdot c^2 = 1997 - 1922 \Rightarrow 3 \cdot b^2 - 5 \cdot c^2 = 75$;

passo 3**:** agora, como o segundo membro da equação é 75, temos que fazer os monômios $3 \cdot b^2$ e $5 \cdot c^2$ serem múltiplos de 75, ou seja, podemos colocar $b = 5 \cdot x$ e $c = 15 \cdot y$, obtendo $3 \cdot b^2 - 5 \cdot c^2 = 75 \Rightarrow 3 \cdot (5 \cdot x)^2 - 5 \cdot (15 \cdot y)^2 = 75 \Rightarrow 3 \cdot 25 \cdot x^2 - 5 \cdot 225 \cdot y^2 = 75 \Rightarrow 75 \cdot x^2 - 1125 \cdot y^2 = 75$; e

passo 4**:** por fim, como na equação de Pell o segundo membro deve ser 1, então dividiremos ambos membros por 75, obtendo $75 \cdot x^2 - 1125 \cdot y^2 = 75 \Rightarrow x^2 - 15y^2 = 1$.

Para determinar a solução mínima de $x^2 - 15y^2 = 1$, calculamos a fração contínua de $\sqrt{15}$. Sendo assim, utilizando passos similares aos feitos nos exemplos 4.38 e 4.39, temos que

$$\sqrt{15} = \sqrt{15} + \lfloor \sqrt{15} \rfloor - \lfloor \sqrt{15} \rfloor = 3 + (\sqrt{15} - 3) = 3 + \frac{(\sqrt{15} - 3) \cdot (\sqrt{15} + 3)}{(\sqrt{15} + 3)}$$

$$\sqrt{15} = 3 + \frac{6}{(\sqrt{15} + 3)} = 3 + \frac{1}{\dfrac{\sqrt{15} + 3}{6}} = 3 + \frac{1}{\dfrac{\sqrt{15} + 3 + \lfloor \sqrt{15} \rfloor - \lfloor \sqrt{15} \rfloor}{6}}$$

$$\sqrt{15} = 3 + \frac{1}{\dfrac{\sqrt{15} + 3 + 3 - 3}{6}} = 3 + \frac{1}{\dfrac{6 + \sqrt{15} - 3}{6}} = 3 + \frac{1}{1 + \dfrac{\sqrt{15} - 3}{6}}$$

$$\sqrt{15} = 3 + \frac{1}{1 + \frac{(\sqrt{15}-3)\cdot(\sqrt{15}+3)}{6.(\sqrt{15}+3)}} = 3 + \frac{1}{1 + \frac{6}{6.(\sqrt{15}+3)}} = 3 + \frac{1}{1 + \frac{1}{\sqrt{15}+3}}$$

$$\sqrt{15} = 3 + \frac{1}{1 + \frac{1}{\frac{\sqrt{15}+3+\lfloor\sqrt{15}\rfloor - \lfloor\sqrt{15}\rfloor}{5}}} = 3 + \frac{1}{1 + \frac{1}{\sqrt{15}+3+3-3}}$$

$$\sqrt{15} = 3 + \frac{1}{1 + \frac{1}{6 + (\sqrt{15}-3)}}.$$

Observemos aqui que o processo começará a se repetir do começo. Com isto, podemos representar $\sqrt{15} = [3; 1, 6]$. Como a repetição começa no a_2, que possui índice par, então temos que tomar o processo somente até o a_1 para obtermos a solução mínima, ou seja,

$$\frac{x_1}{y_1} = 3 + \frac{1}{1} = 3 + 1 = 4 = \frac{4}{1}.$$

Logo, temos que $x_1 = 4$ e $y_1 = 1$ é a solução mínima.

Sendo assim, a equação $x^2 - 15y^2 = 1$ possui como solução mínima o par $(4, 1)$ e como solução geral os pares (x_d, y_d), com $x_d - \sqrt{15}\cdot y_d = (x_1 - \sqrt{15}\cdot y_1)^d = (4 - \sqrt{15})^d$, onde temos que $d \in \mathbb{N}$, $x_d = \frac{(x_1 + \sqrt{15}\cdot y_1)^d + (x_1 - \sqrt{15}\cdot y_1)^d}{2} = \frac{(4+\sqrt{15})^d + (4-\sqrt{15})^d}{2}$ e $y_d = \frac{(x_1 + \sqrt{15}\cdot y_1)^d - (x_1 - \sqrt{15}\cdot y_1)^d}{2\cdot\sqrt{15}} = \frac{(4+\sqrt{15})^d - (4-\sqrt{15})^d}{2\cdot\sqrt{15}}$.

Com isto, temos que a equação inicial pode ter o formato de uma é equação de Pell, que, por sua definição e propriedades, possui infinitas soluções, ou seja, a equação inicial $2\cdot a^2 + 3\cdot b^2 - 5\cdot c^2 = 1997$ possui infinitas soluções.

Portanto, a equação $2\cdot a^2 + 3\cdot b^2 - 5\cdot c^2 = 1997$, com $a, b, c \in \mathbb{N}$, possui infinitas soluções da forma $(a, b, c) = (31, 5x, 15y)$, com $x, y \in \mathbb{N}$ e os quais satisfazem a equação $x^2 - 15y^2 = 1$, com solução mínima $(4, 1)$ e solução geral (x_d, y_d), onde temos que $d \in \mathbb{N}$ e $x_d - \sqrt{15}\cdot y_d = (x_1 - \sqrt{15}\cdot y_1)^d = (4 - \sqrt{15})^d$. □

5 CONCLUSÃO

Oportunizamos um estudo bastante significatico e criterioso sobre equações diofantinas, assunto presente na resolução de diversas situações-problema. Abordamos as equações diofantinas lineares com duas variáveis, definindo-a nos conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{I}$, mostrando que alguns teoremas, proposições e lema cujas definições se restringem apenas ao conjunto $\mathbb{Z}$, podem ser ampliadas ao conjunto $\mathbb{Q}$ e aos números reais comensuráveis, onde estão pares de números que pertencem ao conjunto $\mathbb{I}$. Abordamos também dois tipos de equações diofantinas quadráticas, as equações pitagóricas e a Equação de Pell.

Primeiramente, apresentamos alguns conteúdos matemáticos que estão intrinsicamente relacionados com a resolução das equações diofantinas e estão presentes na grade curricular de nossa educação básica, seja no ensino fundamental ou seja no ensino médio.

Em um segundo momento, foi realizado um breve histórico do pouco que se conhece sobre a vida de Diofanto, matemático grego homenageado pelo seu estudo sobre as equações diofantinas, que propiciou grande avanço na matemática ao mostrar um novo modelo de resolução algébrica, dando início à utilização de símbolos em suas resoluções e ao desenvolvimento da notação algébrica, onde, hoje em dia, nesta linguagem, são utilizados somente símbolos organizada e estruturadamente em suas representações e cálculos.

Em um terceiro momento, mostramos e demonstramos os conceitos, teoremas, proposições e lemas que proporcionam as resoluções das situações-problema por meio das equações diofantinas lineares com duas variáveis e suas aplicações. Em seguida, apresentamos um modelo onde ampliamos a aplicação das equações diofantinas lineares com duas variáveis aos conjuntos $\mathbb{Q}$ e $\mathbb{I}$, e onde fundamentamos os novos coeficientes para estas equações em um novo conceito de *mdc*, chamado de máximo divisor comum generalizado (*mdcg*).

Após isto, passamos a trabalhar as equações diofantinas quadráticas, abordando dois tipos destas: as equações pitagóricas e seus ternos pitagóricos e a equação de Pell, mostrando e demonstrando conceitos, teoremas, proposições e lemas que proporcionam as resoluções de determinadas situações-problema e suas aplicações.

Observamos em cada uma destas equações que elas podem ter solução, seja trivial ou não, ou não ter solução, dependendo de cada situação, sendo que a existência de soluções para:

- as equações que dependem do *mdc* entre seus coeficientes nos possibilitaram uma retomada e ampliação dos estudos aritméticos e algébricos e suas relações com lógica matemática, equação e função polinomial do 1° grau, com progressão aritmética e com geometria analítica;
- a ampliação das aplicações nas equações diofantinas lineares ao conjunto $\mathbb{Q}$ e aos núme-

ros reais comensuráveis nos possibilitarou uma retomada e ampliação dos estudos aritméticos e algébricos e suas relações com a lógica matemática, com as frações e os números decimais, e com geometria plana;

- as equações pitagóricas nos possibilitaram uma retomada e ampliação dos estudos aritméticos e algébricos e suas relações com geometria plana e geometria analítica; e
- a equação de Pell nos possibilitou uma retomada e ampliação dos estudos aritméticos e algébricos e suas relações com os números racionais e irracionais.

Acreditamos que a grande maioria dos conteúdos e das resoluções apresentadas neste estudo estão dentro da realidade de compreensão dos alunos do ensino básico, principalmente do ensino médio, tanto pelo entendimento e percepção, quanto pela assimilação dos conteúdos.

Em função deste trabalho, concluímos que as equações diofantinas lineares com duas incógnitas são um conteúdo matemático que pode instigar a investigação matemática, pois possui várias situações-problema onde se aplica sua teoria e pode se desenvolver o raciocínio dos educandos do ensino médio, visto que este nível de ensino possui maturidade e compreensão matemática suficientes, ao passo que a exigência aqui se restringe somente ao domínio de assuntos que são trabalhados no ensino fundamental. Esta conclusão está tão bem fundamentada, pois o próprio Enem, que é o Exame Nacional do Ensino Médio, ou seja, uma avaliação de extrema importância dos educandos do ensino médio, deste ano, trouxe uma questão sobre equação diofantina linear com duas variáveis.

Concluímos também que as equações pitagóricas e seus ternos pitagóricos podem ser trabalhados na geometria plana como uma extensão dos cálculos dos lados de um triângulo retângulo, bem como das áreas destes tipos de triângulos, além de podermos trabalhar na álgebra os valores de uma expressão e a veracidade de uma equação.

Concluímos ainda que a equação de Pell pode nos auxiliar na abordagem dos números irracionais que, dos conteúdos tratados neste trabalho, é o conteúdo menos trabalhado no ensino fundamental e médio. Podemos aqui trabalhar, fazendo uso das frações contínuas, a representação de um número racional por uma sequência finita de inteiros, a representação de um número irracional por uma sequência infinita de inteiros e a aproximação dos números irracionais em números racionais. Além disto, podemos também citar a equação de Pell na geometria analítica como exemplo de hipérbole e transformar outras equações deixando-as na forma da equação de Pell, para mostrar que aquela equação possui infinitas soluções. Esta parte do trabalho é pouco mais difícil de ser tratada no ensino fundamental e médio, pois, como foi mencionado, é um contéudo menos desenvolvido no ensino básico.

Para finalizar, notamos que o estudo das equações diofantinas nos propicia o desenvolvimento de ideias matemáticas importantes, pois à medida das realizações das demonstrações construímos a Matemática, por meio da explicação proporcionamos a compreensão, através da descoberta obtemos novos aprendizados e resultados, por intermédio

da comunicação conseguimos o significado, mediante o desafio intelectual chegamos a realização pessoal e com o auxílo da sistematização desenvolvemos a organização.

Desta forma, observamos a pouca atenção dadas atualmente nas propostas curriculares oficiais e nos livros didáticos de matemática à exploração das potencialidades acima mencionadas na nossa educação básica.

REFERÊNCIAS

ALENCAR FILHO, Edgard de. **Teoria Elementar dos Números**. 1. ed. São Paulo: Nobel, 1981.

BOYER, Carl. B. **História da Matemática**. tradução Elza F. Gomide - 2a ed.- São Paulo: EDGARD BLUCHERLTDA, 2008.

BOYER, Carl. B.; MERZBACH, Uta C. **História da Matemática**. tradução Helena Castro - 3a ed.- São Paulo: BLUCHER, 2012.

BRASIL. **Parâmetros Curriculares Nacionais:** PCN Matemática. Brasília: Ministério da Educação, 1998b.

BRASIL. **Base Nacional Comum Curricular.** Brasília: Ministério da Educação, 2018a.

BROETTO, Geraldo Claudio; SANTOS-WAGNER, Vânia Maria Pereira dos. O Ensino de Números Irracionais na Educação Básica e na Licenciatura em Matemática: um círculo vicioso está em curso? **Bolema:Boletim de Educação Matemática,** online, v. 33, n. 64, p. [728–747], 2019.

DOMINGUES, Hygino H. **Fundamentos de Aritmética**. 1. ed. São Paulo: Atual Editora LTDA, 1991.

EVES, Howard. **Introdução à História da Matemática**. tradução Hygino H. Domingues - 5. ed. - Campinas, SP: Eitora Unicamp, 2011.

FILIPE, Rafael. **Equação de Pell Generalizada.** Natal: SEMANA OLÍMPICA 2020, 2020. Disponível em: <https://www.obm.org.br/content/uploads/2020/02/23_SO_Rafael_Filipe_Equacao_de_Pell_Generalizada_Nivel_3_compressed.pdf>. Acesso em: 27 set. 2021.

FRANK, J. Swetz. Mathematical Treasures - Bachet's Arithmetic of Diophantus. *In*: **Convergence**, May 2018, 2018. Disponível em: <https://www.maa.org/press/periodicals/convergence/mathematical-treasures-bachets-arithmetic-of-diophantus>. Acesso em: 20 jan. 2022.

FREITAS, Carlos Wagner Almeida. **Equações Diofantinas** 2015. 201 f. Dissertação (Programa de Pós-graduação em Matemática em rede Nacional) – Universidade Federal do Ceará, Fortaleza, 2015.

HEFEZ, Abramo. **Elementos de Aritmética**. Textos Universitários: SBM, 2006.

HEFEZ, Abramo. **Iniciação a Aritmética**. [S.l.]: SBM, 2009.

HEFEZ, Abramo. **Aritmética**. 1. ed. Rio de Janeiro: SBM, 2013.

KAMERS, Fernando. **Pitágoras de Samos e o Teorema de Pitágoras** 2008. 43 f. Monografia (Curso de Matemática) – Universidade Federal de Santa Catarina - UFSC, Florianópolis, 2008.

MARTINEZ, Fabio Brochero; et al. **Teoria dos Números:** um passeio com primos e outros números familiares pelo mundo inteiro. 4.ed.[Projeto Euclides]: IMPA, 2018.

MILIES, Sônia Pitta, César Polcino; COELHO. **Números:** uma introdução à Matemática. 3 ed. São Paulo: Edusp, 2001.

MOREIRA, Carlos Gustavo. **Equações Diofantinas Quadráticas.** São Paulo: Pólos Olímpicos de Treinamento - Curso de Teoria dos Números - Nível 3, 2012. Disponível em: <http://docplayer.com.br/34966229-Equacoes-diofantinas-quadraticas-as-triplas-de-numeros-inteiros-positivos-a-b-c-que-satisfazem-a-equacao-a-2-b-2-c-2.html>. Acesso em: 26 set. 2021.

PARAIZO, Ricardo Ferreira. **Conjuntos numéricos II: números racionais, irracionais e reais.** Viçosa: e-Tec Brasil - Matemática Instrumental - Aula 3, 2016. Disponível em: <http://proedu.rnp.br/bitstream/handle/123456789/585/Aula_03.pdf?sequence=3&isAllowed=y>. Acesso em: 16 jan. 2022.

PEREIRA, Marivaldo Bispo. **Triângulos de Heron** 2015. 35 f. Dissertação(Mestrado Profissional em Matemática em Rede Nacional -PROFMAT) – Universidade Federal da Bahia - UFBA, Salvador, 2015.

POMMER, Wagner Marcelo; POMMER, Clarice Peres Carvalho Retroz. Equações Diofantinas Lineares: um viés histórico- epistemológico como recurso para introduzir diferentes estratégias de resolução de problemas. **Revista de Ensino de Ciências e Matemática,** São Paulo, v. 3, n. 1, p. 28–43, 2012.

RIPOLL, Jaime Bruck; RIPOLL, Cydara Cavedon; SANT'ANA, Alveri Alves. *O mínimo múltiplo comum e o máximo divisor comum generalizados.* **Matemática Universitária,** Porto Alegre, n. 40, p. 59-74, 2006.

ROCQUE, Gilda de La; PITOMBEIRA, João Bosco. Uma Equação Diofantina e Suas Resoluções. **Revista do Professor de Matemática,** Rio de Janeiro, v. 19, n. 2, 1991.

ROQUE, Tatiana. **História da Matemática:** uma visão crítica, desfazendo mitos e lendas. [S.l.]: Zahar, 2012.

ROQUE, Tatiana; PITOMBEIRA, João Bosco. **Tópicos de História da Matemática**. 1a ed. [S.l.]: SBM, 2012.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3. ed. Rio de

Janeiro: IMPA, 2007.

SAVÓIS, Josias Neubert; FREITAS, Daiane. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. **Ciência e Natura,** Santa Maria, v. 37, n. 3, p. 47–57, 2015.

SOUZA, Romario S. de. **Equações Diofantinas Lineares, Quadráticas e Aplicações** 2017. 75 f. Dissertação (Mestrado em Programa de Pós-Graduação em Matemática) – Universidade Estadual Paulista, Rio Claro, 2017.