UNIVERSIDADE ESTADUAL DO CEARÁ

CENTRO DE CIÊNCIAS E TECNOLOGIA

CURSO DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

ANTÔNIO AÉCIO LOPES FERREIRA

EQUAÇÕES DIOFANTINAS LINEARES

QUIXADÁ - CEARÁ

2018

ANTÔNIO AÉCIO LOPES FERREIRA

EQUAÇÕES DIOFANTINAS LINEARES

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Matemática.

Orientador: Prof. Dr. Ulisses Lima Parente.

QUIXADÁ - CEARÁ

2018

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Ferreira, Antônio Aécio Lopes .
Equações diofantinas lineares [recurso eletrônico] / Antônio Aécio Lopes Ferreira. - 2019.
1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 79 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Faculdade de Educação, Ciências e Letras do Sertão Central, Mestrado Profissional em Matemática em Rede Nacional, Quixadá, 2019.
Área de concentração: Matemática.
Orientação: Prof. Dr. Ulisses Lima Parente.

1. Números. 2. Propriedades. 3. Equações Diofantinas. I. Título.

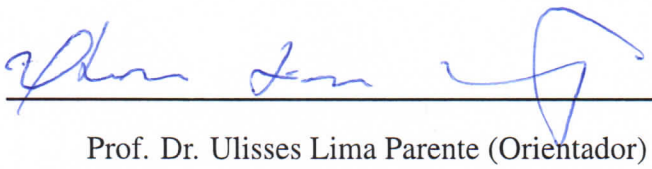
ANTÔNIO AÉCIO LOPES FERREIRA

EQUAÇÕES DIOFANTINAS LINEARES

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Matemática.

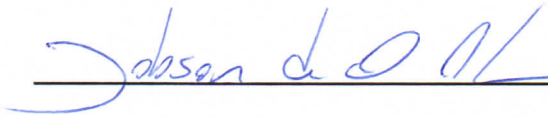
Aprovado em: 26 de abril de 2019.

BANCA EXAMINADORA



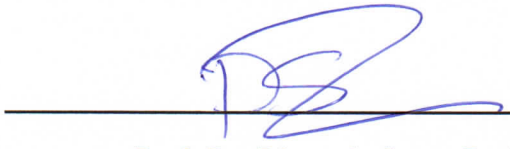
Prof. Dr. Ulisses Lima Parente (Orientador)

Universidade Estadual do Ceará – UECE



Prof. Dr. Jobson de Queiroz Oliveira

Universidade Estadual do Ceará – UECE



Prof. Dr. Diego de Sousa Rodrigues

Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE

Dedico este trabalho primeiramente a Deus, aos meus pais, Antônia Aureni Lopes Ferreira e José Rodrigues Ferreira, a minha companheira, Karoline Almeida Mesquita, e aos meus filhos, Pérola Almeida Ferreira e José Audisio Linhares Mesquita Neto.

AGRADECIMENTOS

Agradeço inicialmente a Deus, pois sem sua proteção não teria chegado até aqui.
A minha família, em especial minha mãe Antônia Aureni Lopes Ferreira, meu pai José Rodrigues Ferreira, aos meus dois filhos: Pérola Almeida Ferreira e José Audisio Linhares Mesquita Neto, minha companheira Karoline Almeida Mesquita, pelo incentivo e apoio aos meus estudos.
Sou muito grato a meu professor e mestre Crispiano Barros Uchôa, pelo incentivo ao estudo da matemática e incansáveis viradas de noite estudando essa ciência que nos desafia e encanta.
Quero agradecer também aos meus colegas da turma do PROFMAT, pela amizade e companheirismo, em especial ao amigo, Alan de Souza Sampaio.
Agradeço a CAPES, pela bolsa, pois sem ela essa conquista seria mais dificultada.
Aos professores da UECE-Quixadá com os quais ao longo desses quase três anos tive o prazer de conviver e aprender, em especial ao meu orientador Prof. Dr. Ulisses Lima Parente, pela paciência e sugestões.

"A matemática é o alfabeto com o qual DEUS escreveu o Universo".

(Pitágoras)

RESUMO

A presente pesquisa constitui-se em um conjunto de eixos temáticos e questões referentes as Equações Diofantinas Lineares, iniciamos com a história de Diofanto, grande matemático, que deu início ao estudo dessas equações, logo após, uma noção básica de números inteiros e suas propriedades que vão desde a operação de adição até a ordenação deste conjunto. Continuamos com a definição de divisão de dois números inteiros, tendo esta, uma relevante importância na demonstração de teoremas como, por exemplo, o da Divisão Euclidiana. Apresentamos a relação entre o mínimo múltiplo comum e o máximo divisor comum, onde este último junto com suas propriedades servem de base para mostrar se uma equação diofantina possui ou não solução. Tendo um papel indispensável na resolução das equações de Diofanto, o Algoritmo de Euclides, por meio da sua exposição deu continuidade a pesquisa. É feito uma breve introdução ao conjunto $\mathbb{Q}$ dos números racionais, ao conjunto dos números irracionais e ao conjunto $\mathbb{R}$ dos números reais e definimos logo na sequência, o conceito de máximo divisor comum generalizado, o qual é um dos tópicos centrais dessa pesquisa já que o mesmo possibilita resolver equações diofantinas lineares com coeficientes racionais. Todos os mecanismos citados acima, deram subsídios para a resolução de equações com duas, três, várias incógnitas e com coeficientes racionais. Finalizando o conteúdo, não podemos deixar de salientar as matrizes desse trabalho, que vão buscar de forma didática, exemplificar o estudo dessas equações e a aplicação direta das mesmas em problemas diversos, contudo é evidente que esse trabalho é sucinto e possui uma exposição teórica e prática facilitadora que encoraja o leitor a fazer bom uso do resultado dessa pesquisa.

Palavras-chave: Números. Propriedades. Equações Diofantinas.

ABSTRACT

The present research consists of a set of thematic axes and questions related to the Diophantine Linear Equations, we begin with the story of Diophantus, a great mathematician, who started the study of these equations, soon after, a basic notion of integers and their properties ranging from the addition operation to the ordering of this set. We continue with the definition of division of two integers, this being a relevant importance in the demonstration of theorems such as, for example, that of the Euclidean Division. We present the relationship between the minimum common multiple and the maximum common divisor, where the latter together with its properties serve as a basis for showing whether a diophantine equation has a solution. Having an indispensable role in the resolution of the equations of Diophantus, the Euclidean Algorithm, through its exposition continued the research. A brief introduction is made to the set $\mathbb{Q}$ of the rational numbers, to the set of irrational numbers and to the set $\mathbb{R}$ of the real numbers and then define the concept of generalized common maximum divisor, which is one of the central topics of this research since it allows to solve linear diophantine equations with rational coefficients. All the mechanisms mentioned above gave subsidies for the resolution of equations with two, three, several unknowns and with rational coefficients. Finishing the content, we must emphasize the matrices of this work, which will seek in a didactic way, to exemplify the study of these equations and the direct application of them to different problems, however it is evident that this work is succinct and has a theoretical and a facilitating practice that encourages the reader to make good use of the results of this research.

Key words: Numbers. Properties. Diophantine Equations.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Os livros didáticos brasileiros, acervo do ensino básico, não abordam na maioria das vezes, o estudo das Equações Diofantinas Lineares, resultando no corpo discente uma impotência na resolução de questões modeladas por essas equações.

O presente trabalho faz alusão a uma proposta de ampliação no currículo escolar de Ensino Fundamental II e Ensino Médio, do conteúdo de Equações Diofantinas Lineares, tendo essa pesquisa bibliográfica a intenção de expor para o leitor a importância da inclusão desse recurso algébrico para o enriquecimento do cronograma escolar de conteúdos. Podendo ser introduzido por etapas: iniciando com embasamento histórico, seguido das demonstração de teoremas e por último a aplicação em diversos problemas que retratam desde assuntos do cotidiano até os mais sofisticados, mas tendo o mesmo padrão de resolução. A utilização desse material sucinto, tanto para a compreensão do professor como para exposição didática para seu aluno, são dois fatores importantes a considerar.

O currículo compreende os conteúdos a serem ensinados e aprendidos, o planejamento pedagógico elaborados por professores, escolas e sistemas educacionais e os objetivos a serem alcançados por meio do processo de ensino, contudo, o estudo das equações diofantinas lineares por falta de influência histórica e teórica não está incluso na grade curricular do ensino básico.

As olimpíadas de matemática, assim como outras provas externas, são de gênero competitivo entre alunos do ensino básico das redes públicas e privadas, tendo como um de seus principais objetivos a interferência na melhoria do ensino de Matemática. O aluno que revela por meio de uma prova suas habilidades de fácil compreensão das questões e agilidade nas resoluções das mesmas, atingindo uma boa pontuação é motivado por ações governamentais como bolsas e premiações, porém o número de alunos beneficiados encontra-se muito abaixo da média em relação a quantidade geral de alunos participantes.

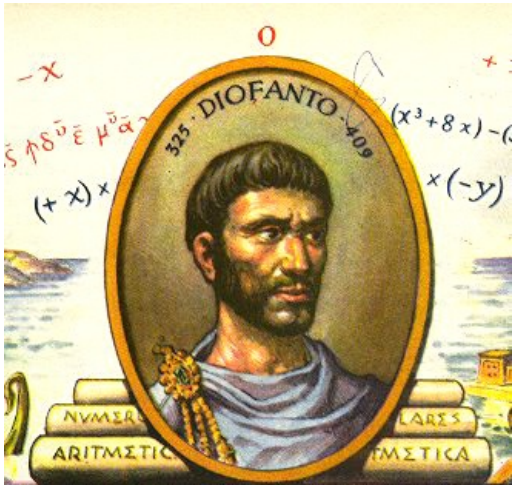
Para sanar esse déficit na média de aprovados, se faz necessário a introdução de conteúdos que uma vez que forem lecionados de acordo com a orientação didática, possam facilitar na composição de uma bagagem educacional mais sólida e o estudo das Equações Diofantinas Lineares permite um amplo olhar sobre as diferentes formas de resolver problemas, tendo como consequência, melhores resultados.

2 REFERENCIAL HISTÓRICO

Nesta seção é apresentada um pouco da história de Diofanto de Alexandria e de sua principal obra que é intitulada "Aritmética".

2.1 DIOFANTO DE ALEXANDRIA

Figura 1 – Diofanto de Alexandria



Fonte: http://www.professoramanuka.com.br.

Pouco se sabe da vida de Diofanto. Acredita-se que tenha vivido por volta de 250 d.C, em Alexandria. Considerado muitas vezes o “pai da Álgebra” por ter feito uso sistemático de abreviações para potências de números e para relações e operações. Com a sua notação, ele podia escrever polinômios numa incógnita quase tão concisamente quanto nós hoje, mas talvez seja muito mais adequado tratá-lo como precursor da moderna Teoria dos Números, cujo ponto de partida seria o trabalho de Fermat no século XVII, contudo, sua notação foi o primeiro passo na direção da álgebra simbólica, que seria desenvolvida apenas a partir do Renascimento europeu e atingiria sua maturidade com a obra de René Descartes no século XVII. O único dado pessoal sobre Diofanto encontra-se, sob forma de problema, na coleção conhecida como *Palatine* ou *Antologia Grega*, uma das melhores fontes de problemas algébricos gregos com cerca de quarenta e seis problemas que foi reunida por volta de 500 d.C, conforme a fonte consultada, o problema se enuncia da seguinte forma:

> Deus lhe 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 vigoroso rebento Lástima! O filho do mestre e sábio do mundo e vai Morreu quando da metade da idade final do pai Quatro anos mais de estudos consolam-no do pesar; Para então, deixando a terra, também ele alívio encontrar. (DARELA; CARDOSO; ROSA, 2011, p. 202).

A fim de resolver este problema, traduzindo-o na linguagem moderna, o mesmo fica representado pela equação abaixo:

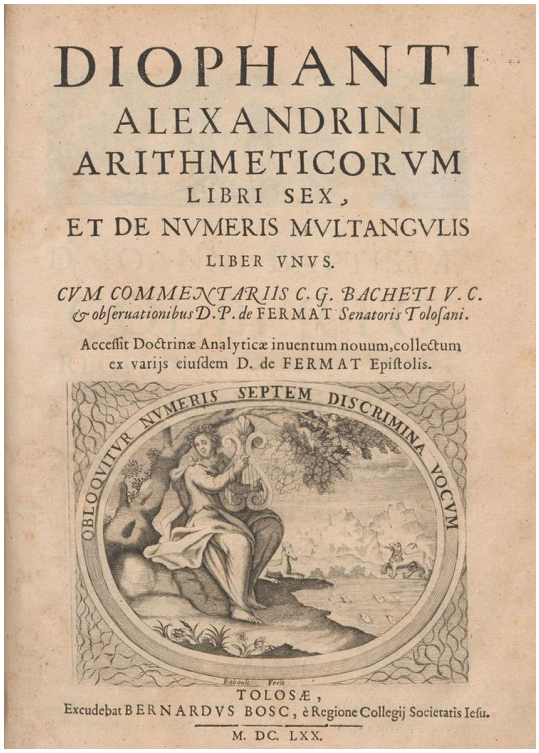
$$\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$$

Resolvendo esta equação, concluímos que Diofanto viveu 84 anos, se caso esse enigma for historicamente exato.

2.2 A OBRA DE DIOFANTO

A principal obra de Diofanto é a Aritmética.

Figura 2 – Capa do livro Aritmética



Fonte: https://en.wikipedia.org/wiki/Diophantus

A obra é tratada originalmente em 13 livros, dos quais só os seis primeiros se preservaram e chagaram aos nossos dias atuais através de manuscritos gregos de origem bizantina, tornando-se conhecidos desde o Renascimento. Possivelmente, a Aritmética, assim como os Elementos de Euclides, foi uma compilação e sistematização dos conhecimentos da época sendo este tratado caracterizado por um alto grau de habilidade matemática e de engenho, podendo ser comparado aos grandes clássicos da Idade Alexandrina anterior; no entanto quase nada tem em comum com esses ou, na verdade, com qualquer Matemática grega tradicional. Representa essencialmente um novo ramo e usa um método diferente. Devido à ênfase dada na Aritmética à solução de problemas indeterminados, o assunto, às vezes chamado análise indeterminada,

tornou-se conhecido como Análise Diofantina.

A Aritmética, é uma coleção de aproximadamente 150 problemas, todos estudados em termos de exemplos numéricos específicos, embora talvez pretendendo conseguir generalidade de método. Não é feita uma distinção clara entre problemas determinados e indeterminados, e mesmo para os últimos, para os quais o número de soluções em geral é infinito, uma só resposta é dada.

Diofanto mais do que qualquer outro apreciador da Álgebra teve uma influência sobre a Teoria dos Números, já que sua obra objetivava a exposição de problemas cuja solução fosse racional. Seu trabalho despertou um novo olhar em Fermat, político e advogado francês que deixou contribuições na Aritmética e tinha a Matemática como hobby, uma vez que possuiu a obra Aritmética traduzida em latim, resolveu fazer registros a punho nas margens do próprio livro que se tornariam uma grande revelação para uma conclusão indireta da obra. As soluções racionais eram o alvo de estudo do primeiro, quanto a resolução com diversas soluções aos números inteiros era evidenciada por Fermat.

3 CONJUNTOS NUMÉRICOS

3.1 NÚMEROS INTEIROS

Nesta subseção é feito um breve estudo sobre o conjunto dos números inteiros e suas propriedades que aqui são aceitas como verdades sem a necessidade de demonstrá-las. $\mathbb{Z}$ será o conjunto dos números inteiros, cujos elementos são dados ordenadamente como segue:

$$\{...,-3,-2,-1,0,1,2,3,...\}$$

Os números à esquerda do zero são chamados de números negativos e os à direita são chamados de números positivos. Os pares de números 1 e -1, 2 e -2, 3 e -3 etc. são chamados de números simétricos. O elemento 0, que não é nem positivo, nem negativo, é o seu próprio simétrico.

Em $\mathbb{Z}$ temos um subconjunto que merece destaque: o conjunto dos números naturais:

$$\mathbb{N} = \{1,2,3,...\}$$

O conjunto acima, cujos elementos são conhecidos como números naturais tem a sua essência caracterizada na palavra sucessor. Intuitivamente, quando $n, m \in \mathbb{N}$, dizer que m é o sucessor de n significa que m vem logo depois de n, isto é, não existem outros números naturais entre n e m. Fica claro que esta explicação apenas substitui "sucessor" por "logo depois", logo não é uma definição. O termo primitivo "sucessor" não é definido explicitamente. Contudo, no século XX, o matemático italiano Giuseppe Peano deu uma forma concisa e precisa para esses números, através da enumeração dos quatro axiomas que são conhecidos como Axiomas de Peano, abaixo enumerados:

1) Todo número natural tem um único sucessor;

2) Números naturais diferentes têm sucessores diferentes;

3) Existe um único número natural, chamado "um" e representado pelo símbolo 1, que não é sucessor de nenhum outro;

4) Seja X um conjunto de números naturais (isto é, $X \subset \mathbb{N}$). Se $1 \in X$ e se, além disso, o sucessor de todo elemento de X também pertence a X, então $X = \mathbb{N}$.

Este último axioma é conhecido como axioma da indução. Ele é a base de um eficiente método de demonstração de proposições referentes a números naturais. Enunciado em forma de propriedade em vez de conjuntos, ele se formula assim:

Seja $P(n)$ uma propriedade relativa a um número natural n. Suponhamos que:

i) P(1) é válida;

ii) Para todo $n \in \mathbb{N}$, a validade de $P(n)$ implica a validade de $P(n')$, onde n' é o sucessor de n. Então $P(n)$ é válida qualquer que seja o número natural n.

Com efeito se chamarmos de X o conjunto dos números naturais n para os quais $P(n)$ é válida, veremos que:

$1 \in X$ em virtude de (i) e que $n \in X \Rightarrow n+1 \in X$ em virtude de (ii). Logo, pelo axioma da indução, concluímos que $X = \mathbb{N}$
A proposição acima é conhecida como o princípio de indução matemática, vejamos um exemplo de sua aplicação.

Exemplo 3.1. Prove que a propriedade $P(n)$ abaixo é verdadeira para todo número natural n:

$$P(n):\ 1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

Solução. Notemos que:

$$P(1):\ 1 = \frac{1(1+1)}{2}$$

É verdadeira. Observemos também que:

$$P(n+1):\ 1+2+3+\cdots+n+(n+1) = \frac{(n+1)(n+2)}{2}$$

Agora suponhamos que para algum $n \in \mathbb{N}$, tenhamos $P(n)$ verdadeira, isto é, a fórmula

$$P(n):\ 1+2+3+\cdots+n = \frac{n(n+1)}{2}$$

é válida para tal valor de n. Somando $(n+1)$ a ambos os lados dessa igualdade, temos:

$$1+2+3+\cdots+n+(n+1) = \frac{n(n+1)}{2}+(n+1) = \frac{n(n+1)+2(n+1)}{2} = \frac{(n+1)(n+2)}{2}$$

O que mostra $P(n+1)$ também ser verdadeiro, logo pelo princípio da indução matemática $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

3.1.1 Propriedades dos Números Inteiros

Entre os números inteiros estão definidas duas operações fundamentais: a adição, que aos números a e b inteiros faz corresponder a soma $(a+b)$ e multiplicação, que lhes associa o produto $(a \cdot b)$ ou simplesmente (ab) . Abaixo temos algumas propriedades referentes a adição e multiplicação no conjunto $\mathbb{Z}$.

1) A adição e a multiplicação são bem definidas:
Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a+b = a'+b'$ e $a \cdot b = a' \cdot b'$.

2) A adição e a multiplicação são comutativas:
Para todos $a, b \in \mathbb{Z}$, $a+b = b+a$ e $a \cdot b = b \cdot a$

3) A adição e a multiplicação são associativas:
Para todos $a, b, c \in \mathbb{Z}$, $(a+b)+c = b+(a+c)$ e $(a \cdot b) \cdot c = b \cdot (a \cdot c)$

4) A adição e a multiplicação possuem elementos neutros:

Para todo $a \in \mathbb{Z}$, $a+0=a$ e $a \cdot 1 = a$

5) A adição possui elementos simétricos:
Para todo $a \in Z$, existe $b=-a$ tal que $a+b=0$

6) A multiplicação é distributiva em relação a adição:
Para todos $a,b,c \in \mathbb{Z}$, tem-se $a \cdot (b+c) = a \cdot b + a \cdot c$

7) Fechamento de $\mathbb{Z}$: O conjunto $\mathbb{Z}$ é fechado para as operações de adição e multiplicação, ou seja:
Para $a,b \in \mathbb{Z}$ tem-se que $a+b \in \mathbb{Z}$ e $ab \in \mathbb{Z}$.
O fechamento é válido para $\mathbb{N}$.

Para a e b pertencentes a $\mathbb{Z}$ diremos que a é menor do que b simbolizando $a < b$ se $b-a \in \mathbb{N}$, caso contrário diremos que b é menor do que a e simbolizaremos por $b < a$, com isso temos a propriedade (8) abaixo:

8) Tricotomia: Dados $a,b \in \mathbb{Z}$, uma, e apenas uma das seguintes possibilidades é verificada:
$i)$ $a=b$
$ii)$ $a<b$
$iii)$ $b<a$

É interessante observarmos que $a-0=a$, temos então que $a>0$ se e somente se, $a \in \mathbb{N}$. Desse modo, temos:

$$\{x \in \mathbb{Z};\ x>0\} = \mathbb{N} \quad \text{e} \quad \{x \in \mathbb{Z};\ x<0\} = -\mathbb{N}$$

Daí segue imediatamente que $a>0$ se, e somente se, $-a<0$.

9) Princípio da Boa Ordenação: Se X é um conjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então X possui um menor elemento.

3.1.2 Módulo de um Número Inteiro

Consideremos agora $a,b \in \mathbb{Z}$, diremos que a é menor ou igual do que b, ou b é maior ou igual do que a, escrevendo $a \leq b$ ou $b \geq a$, se $a<b$ ou $a=b$, com isso definimos a noção de valor absoluto.

Definição 3.1. Seja $a \in \mathbb{Z}$, o número $|a|$ será chamado de módulo ou valor absoluto de a, e será dado por:

$$|a| = \begin{cases} a, & \text{se } a \geq 0 \\ -a, & \text{se } a < 0 \end{cases}$$

É interessante observar que para todo número inteiro temos $|a| \geq 0$ e que $|a|=0$, se e somente se, $a=0$.

Como o valor do módulo de a é sempre positivo ou igual a zero,, uma outra maneira

de definir o número $|a|$ é:

$$|a| = \sqrt{a^2}$$

As propriedades enunciadas anteriormente juntamente com a definição de valor absoluto servem de base para demonstração de inúmeras proposições sobre números inteiros, vejamos algumas a seguir.

Proposição 3.1. $a \cdot 0 = 0$ para todo $a \in \mathbb{Z}$

Demonstração. Temos das propriedades 4 e 6 que:

$$a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$$

Somando $-(a \cdot 0)$ aos extremos da igualdade, pelas propriedades **5, 3, 2** e **4**, obtemos:

$$0 = -(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0 + a \cdot 0) = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0$$

■

Exemplo 3.2. Para $a, b \in \mathbb{Z}$, mostre que:

$$(-a)b = -ab$$

Solução. Notemos primeiramente que:

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

Agora somando $-ab$ em ambos os lados de $(-a)b + ab = 0$, temos:

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

Como queríamos mostrar.

Exemplo 3.3. Para $a, b \in \mathbb{Z}$, mostre que:

$$(-a)(-b) = ab$$

Solução. Da mesma forma que no exemplo (3.2), observemos primeiramente que:

$$(-a)(-b) + a(-b) = -b \cdot (-a + a) = -b \cdot 0 = 0$$

Agora somando ab em ambos os lados de $(-a)(-b) - ab = 0$, pois vimos do Exemplo (3.2) que $a \cdot (-b) = -ab$, temos:

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

Como queríamos mostrar.

Proposição 3.2. A adição é compatível e vale a lei do corte:

$$\forall a,b,c \in \mathbb{Z}, a = b \Leftrightarrow a+c = b+c.$$

Demonstração. A implicação $a = b \Rightarrow a+c = b+c$ decorre de propriedade **1**. Supondo que $a+c = b+c$ e somando $-c$ a ambos os lados da igualdade temos:

$$a+c-c = b+c-c \Rightarrow a = b$$

■

Proposição 3.3. A multiplicação é compatível e vale a lei do corte:

$$\forall a,b \in \mathbb{Z}, \forall c \in \mathbb{Z}\backslash\{0\}, a = b \Leftrightarrow ac = cb.$$

Demonstração. A implicação $a = b \Rightarrow ac = bc$ decorre de propriedade **1**.
Agora supondo $ac = bc$, temos dois possíveis casos:

i) Caso $c > 0$. Se $a < b$, temos que $b-a \in \mathbb{N}$, como $c > 0$ e $c \in \mathbb{N}$ temos pelo fechamento que $c \cdot (b-a) \in \mathbb{N} \Rightarrow (cb-ac) \in \mathbb{N}$, ou seja, $ac < bc$ o que é um absurdo.
Se $b < a$, de modo análogo temos $bc < ac$ que também é um absurdo, logo só podemos ter $a = b$

ii) Caso $c < 0$. Se $a < b$, temos $(b-a) \in \mathbb{N}$ e já que $-c \in \mathbb{N}$ temos do fechamento que $-c \cdot (b-a) \in \mathbb{N} \Rightarrow (ac-bc) \in \mathbb{N}$ de onde temos $bc < ac$ o que é um absurdo.
Se $b < a$ de modo análogo temos $ac < bc$ que também é um absurdo, logo só podemos ter $a = b$

■

Proposição 3.4. Para $a,b \in \mathbb{Z}$ e $r \in \mathbb{N}$, temos:

i) $|ab| = |a| \cdot |b|$

ii) $|a| \leq r$ se, e somente se, $-r \leq a \leq r$

iii) $|a|^2 = |a^2| = a^2$

iv) Desigualdade triangular

$$|a+b| \leq |a| + |b|$$

Demonstração:

i) Temos que $|ab| = \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}\sqrt{b^2} = |a||b|$

ii) Se $a \geq 0 \Rightarrow a = |a| \leq r \Rightarrow a \leq r$.
Se $a < 0 \Rightarrow -a = |a| \leq r \Rightarrow -r \leq a$.

De $a \leq r$ e $-r \leq a$ temos:

$$-r \leq a \leq r$$

Agora supondo que $-r \leq a \leq r$, temos desta desigualdade que:

$$a \leq r \quad \text{e} \quad a \geq -r$$

Se $a \geq 0,\ |a| = a$ e, a primeira desigualdade nos dá:

$$|a| \leq r$$

Agora se $a < 0, |a| = -a$ a segunda desigualdade nos dá:

$$|a| \leq r$$

Logo,

$$-r \leq a \leq r \Rightarrow |a| \leq r$$

iii) Sendo $a^2 \geq 0$ para $\forall a \in \mathbb{Z}$, temos que:

$$|a^2| = a^2$$

Pela definição de módulo resta mostrar que $|a|^2 = a^2$.
Se $a \geq 0$, temos $|a| = a$ e, portanto, $|a|^2 = a^2$.
Se $a < 0$, $|a| = -a$ e, portanto, $|a|^2 = (-a)^2 = a^2$
Em todo caso temos $|a|^2 = a^2$.

iv) Do item *iii*) temos que:

$$|a+b|^2 = (a+b)^2 = a^2 + b^2 + 2ab \leq |a|^2 + |a|^2 + 2|a||b| \Longrightarrow |a+b|^2 = (|a| + |b|)^2 \Longleftrightarrow |a+b| \leq |a| + |b|$$

■

Proposição 3.5. Não existe nenhum inteiro n tal que $0 < n < 1$.

Demonstração. Suponhamos por absurdo que exista n tal que $0 < n < 1$. Logo, o conjunto $X = \{x \in \mathbb{Z};\ 0 < x < 1\}$ é não vazio e limitado inferiormente. Pelo Princípio da Boa Ordenação X possui um menor elemento. Seja a este elemento, onde $0 < a < 1$. Multiplicando esta última desigualdade por a, obtemos $a \cdot 0 < a \cdot a < a \cdot 1 \Rightarrow 0 < a^2 < a < 1$, logo $a^2 \in X$ e $a^2 < a$, uma contradição, pois a é o menor elemento de X. Portanto $X = \varnothing$. ■

Corolário 3.1 (Propriedade Arquimediana)**.** Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração. Como $|b| \neq 0$, da proposição (3.5), temos que $|b| \geq 1$, logo:

$$(|a|+1)|b| \geq |a|+1 > |a| \geq a$$

Agora tomando $n = |a|+1$, se $b > 0$ e $n = -(|a|+1)$, se $b < 0$ obtemos $nb > a$ que é o resultado desejado. ■

3.2 DIVISÃO DOS NÚMEROS INTEIROS

É evidente que a divisão exata entre dois números inteiros nem sempre é possível, mas quando tal fato ocorre podemos expressá-lo através da relação de divisibilidade. Vejamos a seguinte definição:

Definição 3.2. Dados $a, b \in \mathbb{Z}$ diremos que *a divide b* e escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ac$. Quando ocorrer o contrário diremos que *a não divide b* e denotaremos por $a \nmid b$.

É importante ressaltar que a notação $a \mid b$ não representa uma operação em $\mathbb{Z}$, nem uma fração e sim de uma sentença que se diz verdadeira quando existe $c \in \mathbb{Z}$ tal que $b = ac$. Nesse caso diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a ou que b é *divisível* por a. E tal sentença será falsa quando não existir o inteiro c satisfazendo a sentença.

Exemplo 3.4. Observemos que:

1) $6 \mid 12$, pois existe $c = 2 \in \mathbb{Z}$ tal que $12 = 6 \cdot 2$.

2) $3 \nmid 10$, já que não existe $c \in \mathbb{Z}$, tal que $10 = 3 \cdot c$.

Agora destacamos três consequências imediatas da definição (3.2):

1) Para todo $a \in \mathbb{Z}$, 1 divide a; já que $a = 1 \cdot a$

2) Para todo $a \in \mathbb{Z}$, a divide a; já que $a = a \cdot 1$

3) Para todo $a \in \mathbb{Z}$, a divide 0; já que $0 = a \cdot 0$

Tendo como base a definição (3.2) e suas consequências imediatas, faremos a seguir as demonstrações das proposições que servirão para demonstrações futuras no corpo do nosso texto:

Proposição 3.6. Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (a \pm b)$. Então:

$$a \mid b \Leftrightarrow a \mid c$$

Demonstração. Faremos somente o caso $a \mid (a+b)$, pois o caso $a \mid (a-b)$ é totalmente análogo. Suponhamos que $a \mid (a+b)$. Logo existe $f \in \mathbb{Z}$ tal que $b + c = fa$
Agora se $a \mid b$, temos que existe $g \in \mathbb{Z}$ tal que $b = ga$. Juntando as equações $b + c = fa$ e $b = ga$ temos:

$$ga + c = fa \Rightarrow c = (f-g) \cdot a$$

Logo $a \mid c$.
Agora, se $a \mid c$, temos que existe $x \in \mathbb{Z}$ tal que $c = xa$. Juntando as equações $b + c = fa$ e $c = xa$ temos:

$$b + xa = fa \Rightarrow b = (f - x) \cdot a$$

Logo $a \mid b$. ■

Proposição 3.7. Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$, temos:

$$a \mid (xb + yc)$$

Demonstração. $a \mid b$ e $a \mid c$, implicam que existem $\alpha, \beta \in \mathbb{Z}$ tais que $b = \alpha \cdot a$ e $c = \beta \cdot a$. Logo:

$$xb + yc = x(\alpha \cdot a) + y(\beta \cdot a) = (x\alpha + y\beta) \cdot a$$

De onde temos que $a \mid (xb + yc)$ ■

Proposição 3.8. Dados $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que:

$$a \mid b \Rightarrow |a| \leq |b|$$

Demonstração. Se $a \mid b$, então existe $c \in \mathbb{Z}$ tal que $b = ca$. Tomando módulos, temos que $|b| = |c||a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leq |c|$ e, consequentemente, $|a| \leq |a||c| = |b|$. ■

3.3 DIVISÃO EUCLIDIANA

Na subseção anterior vimos que dados $a, b \in \mathbb{Z}$ nem sempre é verdade que $a \mid b$ ou $b \mid a$. Sabemos que $5 \nmid 7$, mas podemos escrever $7 = 1 \cdot 5 + 2$, os números 1 e 2 são chamados de *quociente* e *resto* respectivamente na divisão de 7 por 5 em um processo conhecido como algoritmo da divisão, onde o mesmo foi apresentado por Euclides, nos seus elementos. De uma maneira mais geral temos:

TEOREMA 3.1 (Divisão Euclidiana)**.** Sejam a e b dois números inteiros com $b \neq 0$. Existem dois números inteiros q e r tais que:

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

Demonstração. Consideremos primeiramente o conjunto X abaixo:

$$X = \{x = a - by;\ y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$$

Existência: Temos pela Propriedade Arquimediana que existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$ logo $a - nb > 0$, isso mostra que o conjunto X é não vazio. O conjunto X é limitado inferiormente

por 0, logo pelo Princípio da Boa Ordenação X possui um menor elemento, seja r tal elemento. Suponhamos $r = a - bq$. Temos que $r \geq 0$, basta então mostrar que $r < |b|$. Para isso suponhamos por absurdo que $r \geq |b|$. Portanto existe $x \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + x$, logo $0 \leq x < r$. Mas isto contradiz o fato de r ser o menor elemento de X, pois de $r = a - bq$ e $r = |b| + x$, temos:
Para $b > 0 \Rightarrow r = a - bq \Rightarrow |b| + x = a - bq \Rightarrow b + x = a - bq \Rightarrow x = a - b(q+1) \in X$
Para $b < 0 \Rightarrow r = a - bq \Rightarrow |b| + x = a - bq \Rightarrow -b + x = a - bq \Rightarrow x = a - b(q-1) \in X$
Com $x < r$, logo $r < |b|$.
Unicidade: Suponhamos que $a = bq + r = bq_1 + r_1$, onde $q, r, q_1, r_1 \in \mathbb{Z}$, com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$.
Como:

$$0 \leq r_1 \Rightarrow 0 - r \leq r_1 - r \Rightarrow -r \leq r_1 - r \tag{1}$$

e

$$r \geq 0 \Rightarrow -r \leq 0 \Rightarrow -r + r_1 \leq 0 + r_1 \Rightarrow r_1 - r \leq r_1 \tag{2}$$

Das desigualdades $0 \leq r < |b|$ e $0 \leq r_1 < |b|$ e de (1) e (2) temos:

$$-|b| < -r \leq r_1 - r \leq r_1 < |b| \Rightarrow |r_1 - r| < |b| \tag{3}$$

Agora de $a = bq + r = bq_1 + r_1$ temos:

$$bq + r = bq_1 + r_1 \Rightarrow b(q - q_1) = r_1 - r \Rightarrow |b||q - q_1| = |r - r_1| < |b|$$

Isso nos mostra que $|r - r_1|$ é um múltiplo de $|b|$, mas $-|b| < r_1 - r < |b|$, logo o único valor que $|r - r_1|$ pode assumir é 0, logo:

$$|r - r_1| \Rightarrow r = r_1$$

De onde concluímos diretamente que $q_1 = q$. ■

Os valores q e r são chamados respectivamente de *quociente* e *resto* da divisão de a por b. Vejamos alguns exemplos:

Exemplo 3.5. Ache o quociente e o resto da divisão de:

a) 29 por 3;

b) 31 por 5.

Solução. Pelo teorema (3.1), temos que:

a) $29 = 3 \cdot 9 + 2$ de onde vem que $q = 9$ e $r = 2$

b) como $31 = 5 \cdot 6 + 1$, temos $q = 6$ e $r = 1$

Exemplo 3.6. Se a é um número natural com $a \geq 3$, então a^2 deixa resto 1 na divisão por $a - 1$. Consequentemente, $a - 1$ divide $a^2 - 1$

Solução. A identidade $a^2-1=(a-1)(a+1)$ nos mostra claramente que $a-1$ divide a^2-1. Por outro lado, temos que $a^2=(a-1)(a+1)+1$ com $1<a-1$, de onde concluímos que a^2 deixa resto um quando dividido por $a-1$.

Exemplo 3.7. Prove que o produto de dois números naturais consecutivos é sempre divisível por 2.

Solução. Como $n\in\mathbb{N}$ devemos provar que $a_n=n\cdot(n+1)$ é sempre divisível por 2. Quando fazemos a divisão de n por 2 temos duas possibilidades para o resto r: $r=0$ ou $r=1$, ou seja, n é da forma $2k$ ou da forma $2k+1$ com $k\in\mathbb{N}$.

- Se $n=2k$, temos que $a_n=n\cdot(n+1)\Rightarrow a_n=2k\cdot(2k+1)=2\cdot(2k^2+k)$ mostrando assim que a_n é divisível por 2.
- Se $n=2k+1$, temos que $a_n=n\cdot(n+1)\Rightarrow a_n=(2k+1)\cdot(2k+1+1)=2\cdot(2k+1)\cdot(k+1)$ mostrando novamente que a_n é divisível por 2.

Logo o produto de dois números naturais consecutivos é sempre divisível por 2.

Abaixo temos uma proposição muito eficiente na resolução de problemas sobre soma e produto de restos.

Proposição 3.9. A soma e o produto de quaisquer números inteiros deixam o mesmo resto que a soma e o produto dos seus restos, na divisão por um mesmo número inteiro positivo a.

Demonstração. Demonstração da soma: Seja $n_1,n_2\in\mathbb{Z}$, fazendo a divisão com o resto de ambos os números por a temos:

$$n_1=aq_1+r_1 \quad \text{e} \quad n_2=aq_2+r_2$$

Com $0\leq r_1,r_2<|a|$. Somando $n_1=aq_1+r_1$ e $n_2=aq_2+r_2$, temos:

$$n_1+n_2=a(q_1+q_2)+(r_1+r_2)=aq+(r_1+r_2) \tag{4}$$

Onde $q=q_2+q_2$. Agora dividindo r_1+r_2 por a, obtemos:

$$r_1+r_2=ap+r \quad (4), p\in\mathbb{Z}, 0\leq r\leq|a| \tag{5}$$

De (4) e (5) segue que:

$$n_1+n_2=aq+ap+r=a(q+p)+r \tag{6}$$

De (5) e (6) concluímos que os restos de n_1+n_2 e r_1+r_2 na divisão por a são iguais.
Demonstração do produto: Agora multiplicando $n_1=aq_1+r_1$ e $n_2=aq_2+r_2$, temos:

$$\begin{aligned} n_1\cdot n_2 = &\quad (aq_1+r_1)\cdot(aq_2+r_2) \\ &= a^2q_1q_2+aq_1r_2+aq_2r_1+r_1r_2 \\ &= a(aq_1q_2+q_1r_2+q_2r_1)+r_1r_2 \\ &= aq+r_1r_2 \end{aligned} \tag{7}$$

onde $q = aq_1q_2 + q_1r_2 + q_2r_1$. Agora dividimos r_1r_2 por a para obtermos:

$$r_1r_2 = ap + r, \quad p \in \mathbb{Z} \quad 0 \leq r < a. \tag{8}$$

Das igualdades (7) e (8) segue que:

$$n_1n_2 = aq + ap + r = a(p+q) + r, \quad 0 \leq r < a. \tag{9}$$

Portanto de (8) e (9) concluímos que os restos que deixam n_1n_2 e r_1r_2 na divisão por a são iguais, concluindo assim a demonstração. ■

Exemplo 3.8. Um turista brasileiro chega à Cuba e troca parte de seu dinheiro numa casa de câmbio, recebendo 175 notas de 50 pesos e 213 notas de 20 pesos. Ele decide trocar este dinheiro pela maior quantidade possível das famosas moedas de 3 pesos cubanos, porque elas têm gravada a imagem do guerrilheiro Che Guevara. Quanto sobrou do dinheiro depois de fazer a troca pelas moedas?

Solução. Para resolver este problema basta achar o resto que deixa o número $n = 175 \cdot 50 + 213 \cdot 20$ quando dividido por 3. Entretanto aplicando a proposição (3.9) o problema fica reduzido a encontrar o resto da divisão do novo número n_1 tal que:

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

Agora procurando o resto que n_1 deixa por 3, que obviamente é 2, concluímos que sobrou para o turista 2 pesos .

3.4 MÁXIMO DIVISOR COMUM

Diremos que um inteiro d é um divisor comum de dois inteiros a e b diferentes ou não se $d \mid a$ e $d \mid b$. Assim $\pm 1, \pm 2$ e ± 4 são divisores comuns de 8 e 20, já que ± 1 divide 8 e 20, ± 2 divide 8 e 20 e ± 4 divide 8 e 20.

De agora em diante consideraremos somente os divisores positivos dos números.

Definição 3.3 (Máximo Divisor Comum)**.** Sejam a e b inteiros diferentes de zero. O máximo divisor comum, resumidamente *mdc*, entre a e b é o número $d > 0$ que satisfaz as seguintes condições:

1) d é divisor comum de a e b, isto é, $d \mid a$ e $d \mid b$;

2) d é o maior inteiro positivo com a propriedade **1)**.

Observemos que **2)** poderia ser reescrito como:

- Se c é divisor comum de a e b, então $c \mid d$.

Denotaremos o *mdc* de a e b por $d = mdc(a,b)$ ou por $d = (a,b)$ ou simplesmente

por (a,b). É interessante observamos que $d=(a,b)=(b,a)$, já que a ordem de a e b não nos importa aqui. Outra observação importante é que $(a,b)=(a,-b)=(-a,b)=(-a,-b)$, o que nos permite supor a e b sempre positivos, para o cálculo do *mdc*.

Exemplo 3.9. O *mdc* de 8 e 20 é 4.

Proposição 3.10. Sejam $a,b,n \in \mathbb{Z}$. Então valem as seguintes afirmações:

i) Se a é um múltiplo de b, então $(a,b)=b$;

ii) Se $a=bq+r$, $r\neq 0$, então o conjunto dos divisores comuns dos números a e b coincide com o conjunto dos divisores comuns dos números b e r. Particularmente, $(a,b)=(b,r)$.

Demonstração:

i) Com efeito, todo divisor comum dos números a e b é divisor de b. Reciprocamente, usando que a é múltiplo de b, todo divisor de b é também um divisor de a, ou seja, um divisor comum de a e b. Portanto, o conjunto dos divisores comuns dos números a e b é igual ao conjunto dos divisores de b. Como o maior divisor de b é ele mesmo, resulta que $(a,b)=b$.

ii) Da proposição (3.6) temos que todo divisor comum de a e b também divide r e consequentemente é divisor de b e r. Pela mesma razão todo divisor comum de b e r também divide a e, consequentemente, é um divisor de a e b. Portanto os divisores comuns de a e b são os mesmos que os divisores comuns de b e r. Particularmente, também coincide o maior divisor comum, ou seja, $(a,b)=(b,r)$.

■

Apesar da definição de máximo divisor comum ser um conceito simples de se entender, calculá-lo pode não ser uma tarefa muito fácil dependendo dos números envolvidos. O teorema a seguir nos fornece um método, chamado de algoritmo de Euclides, para calcular o máximo divisor comum de dois números.

TEOREMA 3.2 (Algoritmo de Euclides)**.** Dados dois inteiros positivos, a e b, aplicamos sucessivamente a divisão euclidiana para obter as seguintes igualdades:

$$\begin{cases} b = aq_1 + r_1, & 0 \leq r_1 < a \\ a = r_1q_2 + r_2, & 0 \leq r_2 < r_1 \\ r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2 \\ \cdots \quad\quad \cdots & \quad\quad \cdots \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_nq_{n+1} & \end{cases} \tag{10}$$

Até r_n dividir r_{n-1}. Assim, o $mdc(a,b)=r_n$, ou seja, é ultimo resto não-nulo no processo de divisões anteriores.

Demonstração. Primeiro observamos que o processo de divisão em (10) é finito, já que a sequência de números r_k, com $k = 1,2,3\ldots,n$, é estritamente decrescente e está contida no conjunto $\{r \in \mathbb{Z}, 0 < r < a\}$, portanto não pode conter mais do que a inteiros positivos. Agora examinando as igualdades de (10) e usando a proposição (3.10) item (ii), temos que:

$$(a,b) = (a,r_1) = (r_1,r_2) = \ldots = (r_{n-1},r_{n-2}) = (r_{n-1},r_n) = r_n$$

■

O algoritmo descrito pelo teorema acima pode ser resumido e realizado na prática como mostraremos a seguir.

Inicialmente efetuamos a divisão de b por a obtendo $b = aq_1 + r_1$ e colocamos os números envolvidos no diagrama abaixo:

	q_1	
b	a	
r_1		

Continuando a divisão, agora de b por r_1 temos $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama abaixo como se segue:

	q_1	q_2	
b	a	r_1	
r_1	r_2		

E prosseguindo até que r_n divida r_{n-1}, teremos:

	q_1	q_2	q_3	$\ldots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\ldots$	r_{n-2}	r_{n-1}	$r_n = (a,b)$
r_1	r_2	r_3	r_4	$\ldots$	r_n		

Vejamos um exemplo de como aplicar o algoritmo de Euclides o usando método descrito acima:
Exemplo 3.10. Calcular o *mdc* de 8840 e 485:
Solução. Começando com a divisão de 8840 por 485, temos:

	18	4	2	2	4
8840	485	110	45	20	5
110	45	20	5	0	

Logo o *mdc* de 8840 e 485 é 5.
Observando o exemplo acima, o Algoritmo de Euclides nos dá:
$5 = 45 - 2 \cdot 20$
$20 = 110 - 2 \cdot 45$

$45 = 485 - 4 \cdot 110$
$110 = 8840 - 18 \cdot 485$
De onde temos:
$5 = 45 - 2 \cdot 20 = 45 - 2 \cdot (110 - 2 \cdot 45) = 5 \cdot 45 - 2 \cdot 110 = 5 \cdot (485 - 4 \cdot 110) - 2 \cdot 110 = 5 \cdot 485 - 22 \cdot 110 = 5 \cdot 485 - 22 \cdot (8840 - 18 \cdot 485) = 401 \cdot 485 - 22 \cdot 8840$
Logo:

$$(8840, 485) = 5 = 401 \cdot 485 + (-22) \cdot 8840$$

Notemos que, usando o Algoritmo de Euclides de trás para frente, conseguimos escrever o *mdc* de 8840 e 485 como múltiplo de 485 mais um múltiplo de 8840. Veremos na próxima subseção que o processo acima sempre pode ser realizado sendo uma ferramenta bastante útil para encontrarmos inteiros m e n tais que $(a,b) = ma + nb$.

Definição 3.4. Diremos que dois números inteiros a e b são primos entre si, se $(a,b) = 1$, ou seja, se o máximo divisor comum de ambos for igual a 1.

Exemplo 3.11. Mostre que a fração abaixo é irredutível para todo $n \in \mathbb{N}$.

$$\frac{2n+8}{4n+15}$$

Solução. Usando o Algoritmo de Euclides, temos:
$4n + 15 = (2n + 8) \cdot 1 + 2n + 7$
$2n + 8 = (2n + 7) \cdot 1 + 1$
$2n + 7 = 1 \cdot (2n + 7) + 0$
De onde temos que o $mdc(4n + 15, 2n + 8) = 1$ e portanto $4n + 15$ e $2n + 8$ são primos entre si, de onde vem que $\frac{2n+8}{4n+15}$ é irredutível para todo n natural.

3.4.1 Propriedades do Máximo Divisor Comum

O teorema a seguir nos fornece uma importante ferramenta na resolução de problemas que envolvem o máximo divisor comum de dois números e será de grande valia no decorrer do texto. O mesmo foi provado pela primeira vez por Claud-Gaspard Bachet de Méziriac(1581-1638) e logo mais tarde generalizado por Étienne Bézout (1730-1783), matemático francês.

TEOREMA 3.3 (Teorema de Bachet-Bézout)**.** Se d é o máximo divisor comum de a e b, então existem números inteiros m e n tais que $d = (a,b) = am + bn$.

Demonstração. Consideremos a combinação linear $am + bn$, onde $m, n \in \mathbb{Z}$. Este conjunto de inteiros, denotado por:

$$C(a,b) = \{am + bn;\ m,n \in \mathbb{Z}\}$$

Possui elementos positivos e negativos. Além disso, escolhendo $m = n = 0$, vemos que $0 \in$

$C(a,b)$.

Pelo princípio da Boa Ordenação, podemos escolher m_0 e n_0 de tal modo que $\lambda = am_0 + bn_0$ seja o menor inteiro positivo em $C(a,b)$.
Mostraremos primeiramente que $\lambda \mid a$.
Suponhamos por absurdo que $\lambda \nmid a$, logo pela divisão Euclidiana, existem inteiros q e r tais que $a = \lambda q + r$ com $0 < r < \lambda$. Portanto:

$$r = a - \lambda q = a - q(am_0 + bn_0) = a \cdot (1 - qm_0) + b \cdot (-qn_0)$$

De onde vemos que $r \in C(a,b)$, o que contradiz o fato de λ ser o menor elemento positivo em $C(a,b)$.

Da mesma forma suponhamos por absurdo que $\lambda \nmid b$, logo pela divisão Euclidiana, existem inteiros q_1 e r_1 tais que $a = \lambda q_1 + r_1$ com $0 < r_1 < \lambda$. Logo:

$$r_1 = b - \lambda q_1 = b - q_1(am_0 + bn_0) = b - q_1 \cdot am_0 - q_{1n_0} = a \cdot (-q_1 m_0) + b \cdot (1 - q_1 n_0)$$

E isso nos mostra agora que $r_1 \in C_{a,b}$, contrariando novamente o fato de λ ser o menor elemento positivo em $C(a,b)$. Logo $\lambda \mid a$ e $\lambda \mid b$.

Resta agora provar que $\lambda = d$. Como $d = (a,b)$ existem $a_1, b_1 \in \mathbb{Z}$, tais que $a = da_1$ e $b = db_1$, logo:

$$\lambda = am_0 + bn_0 = da_1 m_0 + db_1 n_0 = d(a_1 m_0 + b_1 n_0)$$

De onde temos que que $\lambda \mid d$. Logo pela proposição (3.8), concluímos que $d \leq \lambda$, mas $d < \lambda$ é impossível pois d é o máximo divisor comum de a e b, portanto $d = \lambda = am_0 + bn_0$. ■

Corolário 3.2. Sejam $a, b, \in \mathbb{Z}$ e $c \in \mathbb{N}$ temos que:

$$\text{Se } c \mid a \text{ e } c \mid b, \text{ então } c \mid (a,b).$$

Demonstração. Como $c \mid a$ e $c \mid b$ existem $a_1, b_1, \in \mathbb{Z}$, tais que $a = ca_1$ e $b = cb_1$ e sabendo que:

$$(a,b) = am + bn, \text{ com } m,n \in \mathbb{Z}$$
$$(a,b) = ca_1 m + cb_1 n$$
$$(a,b) = c(a_1 m + b_1 n)$$

De onde temos que $c \mid (a,b)$. ■

Corolário 3.3. Quaisquer que sejam $a, b \in \mathbb{N}$, não ambos nulos, e $\lambda \in \mathbb{Z}$, tem-se que:

$$(\lambda a, \lambda b) = \lambda (a,b)$$

Demonstração. Primeiramente observamos que:

$$\lambda am + \lambda bn = \lambda (am + bn), \text{ onde } m,n \in \mathbb{Z}$$

Usando o corolário 3.2 e o fato de λ ser positivo da igualdade acima temos que:

$$\begin{aligned}(\lambda a, \lambda b) &= min\{\lambda am + \lambda bn; m,n \in \mathbb{Z}\} \\ &= \lambda \cdot min\{am + bn; m,n \in \mathbb{Z}\} \\ &= \lambda \cdot (a,b)\end{aligned}$$

■

Corolário 3.4. Dados $a, b \in \mathbb{Z}$, ambos não nulos, tem-se que:

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

Demonstração. Pelo corolário 3.3, temos que:

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

De onde temos que a igualdade acima só se verifica se tivermos:

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

■

Proposição 3.11. Dois números inteiros a e b são primos entre si se, e somente se, existirem m e n inteiros tais que $ma + nb = 1$.

Demonstração. Supondo que a e b são primos entre si, temos pela definição (3.4) que $(a,b) = 1$. Agora pelo teorema de Bachet-Bézout existem inteiros m e n tais que $ma + nb = (a,b) = 1$. Logo a primeira parte da proposição fica demonstrada.

Agora supondo que existam m e n tais que $ma + nb = 1$. Se $(a,b) = d$, temos que $d \mid (am + bn)$, o que mostra que $d \mid 1$, e, portanto, $d = 1$. Provando assim a segunda parte da proposição. ■

TEOREMA 3.4. Sejam a, b e c inteiros. Se $a \mid bc$ e $(a,b) = 1$, então $a \mid c$.

Demonstração. Se $a \mid bc$ então existe $\lambda \in \mathbb{Z}$ tal que $bc = a\lambda$.
Se $(a,b) = 1$, então pela proposição (3.11), temos que existem $m,n \in \mathbb{Z}$ tais que:

$$ma + nb = 1$$

Multiplicando por c ambos os lados da igualdade acima, temos que:

$$c = mac + nbc$$

Substituindo bc por $a\lambda$ nesta última igualdade, temos que:

$$c = mac + na\lambda = a(mc + n\lambda)$$

De onde temos que $a \mid c$. ■

3.5 GENERALIZAÇÃO DO MÁXIMO DIVISOR COMUM

A definição de máximo divisor comum pode se generalizada. Vejamos isso na definição a seguir:

Definição 3.5. Um número natural d será dito o *mdc* de dados números inteiros $a_1, \ldots, a_n$, não nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, \ldots, a_n$;

ii) Se c é um divisor comum de $a_1, \ldots, a_n$, então $c \mid d$.

O máximo divisor comum dos números $a_1, \ldots, a_n$, quando existir, será único e representaremos por:

$$(a_1, \ldots, a_n)$$

A proposição a seguir nos fornece um método para o cálculo do *mdc* de n inteiros dados.

Proposição 3.12. Dados números inteiros $a_1, \ldots, a_n$, não todos nulos, existe o *mdc* e:

$$(a_1, \ldots, a_n) = (a_1, \ldots, (a_{n-1}, a_n))$$

Demonstração. Façamos a prova por indução sobre $n \geq 2$. Para $n = 2$, não há o que se provar. Suponhamos que o resultado é válido para n. Provaremos que é válido para $n+1$, para isso basta mostrar que se d é o *mdc* de $a_1, \ldots, a_n, a_{n+1}$, pois isso provará também a existência. Seja d o *mdc* de $a_1, \ldots, (a_n, a_{n+1})$. Logo, $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid (a_n, a_{n+1})$. Portanto, $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$

Agora seja c um divisor comum de $a_1, \ldots, a_n, a_{n+1}$; Logo, c é divisor comum de $a_1, \ldots, a_{n-1}$ e (a_n, a_{n+1}); e portanto $c \mid d$. ■

Quando tivermos o máximo divisor comum dos números acima igual a 1, diremos que os números $a_1, \ldots, a_n$ são primos entre si.

O teorema de Báchet-Bézout também pode ser generalizado como veremos a seguir.

TEOREMA 3.5 (Generalização Báchet-Bézout)**.** Sejam $a_1, \ldots, a_n$, números inteiros, então existem $x_1, \ldots, x_n \in \mathbb{Z}$ tais que:

$$(a_1, \ldots, a_n) = x_1 a_1 + \cdots + x_n a_n = \sum_{i=1}^{n} a_i x_i$$

Demonstração. Sejam $a_1, \ldots, a_n \in \mathbb{Z}$. Consideremos o seguinte conjunto:

$$I(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} a_i x_i;\ x_i \in \mathbb{Z}\ \forall\ 1 \leq i \leq n \right\}$$

Notemos que $I(a_1, \ldots, a_n) \cap \mathbb{N} \neq \varnothing$, pois tomando $x_i = a_i$, com $i = 1, \ldots, n$, obtemos:

$$\sum_{i=1}^{n} a_i a_i = \sum_{i=1}^{n} a_i^2 \in I(a_1, \ldots, a_n) \cap \mathbb{N}$$

Seja $d = \sum_{i=1}^{n} a_i x_i^{'}$, o menor elemento da interseção acima, afirmamos que d divide todo elemento de $I(a_1, \ldots, a_n)$, pois se d não os dividisse teríamos um elemento $m = \sum_{i=1}^{n} a_i x_i$ tal que $d \nmid m$ e pela divisão euclidiana existiriam $q, r \in \mathbb{Z}$ tal que $m = dq + r$ com $0 \leq r < d$. Assim:

$$\begin{aligned} r = &\ m - dq \\ = &\ \sum_{i=1}^{n} a_i x_i - q \cdot \sum_{i=1}^{n} a_i x_i^{'} \\ = &\ \sum_{i=1}^{n} a_i x_i - \sum_{i=1}^{n} q a_i x_i^{'} \\ = &\ \sum_{i=1}^{n} (a_i x_i - q a_i x_i^{'}) \in I(a_1, \ldots, a_n) \end{aligned}$$

Mas $r < d$ e d é o menor elemento positivo de $I(a_1, \ldots, a_n)$, portanto r deve ser igual a 0, de onde temos que $d \mid m$, assim como tínhamos afirmado anteriormente d divide todo elemento de $I(a_1, \ldots, a_n)$, ou seja, $d \mid a_i,\ \forall\ 1 \leq i \leq n$.

Notemos agora que como d é o menor elemento positivo de $I(a_1, \ldots, a_n)$, necessariamente temos $d \leq (a_1, \ldots, a_n)$, por outro lado $(a_1, \ldots, a_n)$ divide todos os elementos de $I(a_1, \ldots, a_n)$ em especial $(a_1, \ldots, a_n) \mid d$ e isso só pode ocorre quando $d = (a_1, \ldots, a_n)$. ■

Seja $d = (a_1, \ldots, a_n)$ e consideremos o conjunto:

$$d\mathbb{Z} = \{ld;\ l \in \mathbb{Z}\}$$

Afirmamos que $I(a_1, \ldots, a_n) = d\mathbb{Z}$. De fato, como todo elemento de $I(a_1, \ldots, a_n)$ é divisível por d, temos que $I(a_1, \ldots, a_n) \subset d\mathbb{Z}$. Por outro lado para $ld \in d\mathbb{Z}$, temos que:

$$ld = l(x_1 a_1 + \cdots + x_n a_n) = (lx_1)a_1 + \cdots + (lx_n)a_n \in I(a_1, \ldots, a_n)$$

E, portanto, $d\mathbb{Z} \subset I(a_1, \ldots, a_n)$. Logo, temos que $d\mathbb{Z} = I(a_1, \ldots, a_n)$.

3.6 MÍNIMO MÚLTIPLO COMUM

Vimos da definição 3.2 que quando a sentença $a \mid b$ é verdadeira existe $c \in \mathbb{Z}$ tal que $b = ac$, neste caso, dizemos que b é um múltiplo de a.

Se um número inteiro é um múltiplo simultâneo de dois números inteiros dados, então o mesmo é chamado de múltiplo comum desses dois números.

Definição 3.6 (Mínimo Múltiplo Comum)**.** Dados a e b inteiros diferente de zero. O mínimo múltiplo comum, resumidamente *mmc*, entre a e b é o inteiro $m \geq 0$ satisfazendo as seguintes propriedades:

i) m é um múltiplo comum de a e b, isto é, $a \mid m$ e $b \mid m$;

ii) se c é um múltiplo comum de a e b, então $m \mid c$.

Neste caso denotaremos o *mmc* entre a e b por $m = mmc(a,b)$ ou simplesmente por $m = [a,b]$.

Exemplo 3.12. 30 é um múltiplo comum de 3 e 5, mas não é o *mmc* desses números. O número 15 é o *mmc* de 3 e 5.

A proposição a seguir nos fornece um meio para o cálculo do *mmc* e dois números inteiros não nulos.

Proposição 3.13. Dados dois números inteiros não nulos a e b, temos que:

$$[a,b] \cdot (a,b) = |ab|$$

Demonstração. Podemos supor sem perda de generalidade a e b positivos devido a:

$$[a,b] = [a,-b] = [-a,b] = [-a,-b]$$

Seja $m = [a,b]$ e ponhamos $m = \dfrac{ab}{(a,b)}$. Basta então mostrar que m satisfaz as propriedades **i)** e **ii)** da definição (3.6). Como:

$$m = a \cdot \frac{b}{(a,b)} = b \cdot \frac{a}{(a,b)}$$

Temos que $a \mid m$ e $b \mid m$, ou seja, m é um múltiplo comum de a e b.

Seja c um múltiplo comum de a e b, provemos que $m \mid c$.

Como c é um múltiplo comum de a e b existe x, y inteiros positivos tais que $c = ax$ e $c = by$, de onde temos que:

$$x \cdot \frac{a}{(a,b)} = y \cdot \frac{b}{(a,b)}$$

Sabemos do corolário (3.4) que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$ segue então do lema de Gaus que $\frac{a}{(a,b)}$ divide

y, e, portanto, $m = \frac{a}{(a,b)} \cdot b$ divide $yb = c$. Logo:

$$[a,b] = \frac{ab}{(a,b)} \Rightarrow [a,b] \cdot (a,b) = ab$$

■

Exemplo 3.13. Calcule o *mmc* de 143 e 77.

Solução. Usando o algoritmo de Euclides para encontrar $(143,77)$, temos:
$143 = 77 \cdot 1 + 66$
$77 = 66 \cdot 1 + 11$
$66 = 11 \cdot 6 + 0$
Logo, $(143,77) = 11$. Agora usando a proposição (3.13), temos:
$[143,77] \cdot (143,77) = |143 \cdot 77|$
$[143,77] \cdot 11 = 11011$
$[143,77] = 1001$

Exemplo 3.14. Mostre que $[ca,cb] = |c|[a,b]$.

Solução. Usando a proposição (3.13), temos:

$$[ca,cb] \cdot (ca,cb) = |cacb|$$

$$[ca,cb] \cdot c \cdot (a,b) = |c^2| \cdot |ab|$$

Como $[a,b] \cdot (a,b) = |ab|$ e $|c^2| = c^2$, temos:

$$[ca,cb] \cdot c \cdot (a,b) = c^2 \cdot [a,b] \cdot (a,b)$$

$$[ca,cb] = c \cdot [a,b]$$

Como o *mmc* é um número positivo, temos:

$$[ca,cb] = |c| \cdot [a,b]$$

3.7 O CONJUNTO $\mathbb{Q}$ DOS NÚMEROS RACIONAIS

Devido às cheias no rio Nilo, as cercas usadas pelos habitantes que viviam às suas margens para demarcarem seus terrenos eram destruídas. Sendo assim, eram necessárias novas medições, as quais eram efetuadas pelos esticadores de cordas, encarregados do governo. As cordas usadas nas medições tinham uma unidade de medida marcada na própria corda. A medição era feita verificando quantas vezes aquela unidade de medida estava contida no lado

do terreno. Dificilmente a unidade cabia um número inteiro de vezes, foi por essa razão que os egípcios criaram os números fracionários, cuja representação é uma fração.

Hoje é comum nos depararmos diante de situações que envolvem frações e números decimais, como por exemplo, o manuseio de dinheiro, onde deve-se ter a noção de décimos e centésimos. Até mesmo no preparo de receitas de cozinha ou comer uma pizza com os amigos, necessitamos ter um conhecimento prévio de frações.

No ambiente escolar principalmente nos últimos anos do ensino Fundamental e inicias do Ensino Médio o conjunto $\mathbb{Z}$ dos números inteiros juntamente com o conjunto $\mathbb{Q}$ dos números racionais são os conjuntos mais numéricos mais trabalhados, pois servem de base para a maioria dos conteúdos e problemas abordados.

O conjunto $\mathbb{Q}$ mencionado anteriormente é representado simbolicamente por:

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a,\ b \in \mathbb{Z} \text{ e } b \neq 0 \right\}$$

a fração $\frac{a}{b}$ é irredutível, ou seja, $(a,b) = 1$

No conjunto $\mathbb{Q}$ são definidas as operações de adição $(+)$, subtração $(-)$, multiplicação $(\cdot)$ e divisão $(\div)$, descritas na definição a seguir.

Definição 3.7. A adição, subtração, multiplicação e divisão de racionais, são definidas, respectivamente, por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$
$$\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d},$$
$$\frac{a}{b} \div \frac{c}{d} = \frac{a}{b} \cdot \frac{d}{c},$$

para quaisquer racionais $\frac{a}{b}$ e $\frac{c}{d}$.

Exemplo 3.15. Dados os racionais $\frac{1}{3}$ e $\frac{2}{5}$, encontre o racional correspondente a:

a) $\frac{1}{3} + \frac{2}{5}$

b) $\frac{1}{3} - \frac{2}{5}$

c) $\frac{1}{3} \cdot \frac{2}{5}$

d) $\frac{1}{3} \div \frac{2}{5}$

Solução. Pela definição (3.7), temos:

a) $\frac{1}{3} + \frac{2}{5} = \frac{1 \cdot 5 + 3 \cdot 2}{3 \cdot 5} = \frac{5+6}{15} = \frac{11}{15}$

b) $\frac{1}{3} - \frac{2}{5} = \frac{1 \cdot 5 - 3 \cdot 2}{3 \cdot 5} = \frac{5-6}{15} = \frac{-1}{15}$

c) $\frac{1}{3} \cdot \frac{2}{5} = \frac{1 \cdot 2}{3 \cdot 5} = \frac{2}{15}$

d) $\frac{1}{3} \div \frac{2}{5} = \frac{1}{3} \cdot \frac{5}{2} = \frac{1 \cdot 5}{3 \cdot 2} = \frac{5}{6}$

Um número racional $\frac{a}{b}$ também pode ser representado na forma decimal, para isto basta efetuar a divisão de a por b. A forma decimal pode ser finita (decimais exatos) ou infinita (dízimas periódicas).

Exemplo 3.16. Represente as frações $\frac{2}{5}$ e $\frac{5}{6}$ em sua forma decimal.

Solução. Efetuando a divisão, temos:

- $\frac{5}{6} = 0,4$
- $\frac{5}{6} = 0,8333\ldots$

Também podemos representar um número decimal em forma de fração, para isto agimos de acordo com o exemplo a seguir.

Exemplo 3.17. Represente em forma de fração os seguintes números decimais:

a) 0,3

b) 0,777...

c) 1,212121...

Solução:

a) Seja x a fração que representa 0,3, logo:

$$x = 0,3$$

Multiplicando a igualdade acima por 10, temos:

$$10x = 3 \Rightarrow x = \frac{3}{10}$$

b) Seja x a fração que representa 0,777..., logo:

$$x = 0,777\ldots$$

Multiplicando a igualdade acima por 10, temos:

$$10x = 7,777\ldots$$

$$10x = 7 + 0,777\ldots$$

$$10x = 7 + x$$

$$x = \frac{7}{9}$$

c) Observemos que $1,212121\ldots = 1 + 0,212121\ldots$, seja então x a fração que representa 0,212121..., logo:

$$x = 0,212121\ldots$$

Multiplicando a igualdade acima por 100, temos:

$$100x = 21,2121\ldots$$

$$100x = 21 + 0,212121\ldots$$

$$100x = 21 + x$$

$$99x = 21$$

$$x = \frac{21}{99} = \frac{7}{33}$$

De onde temos que a fração que representa o número 1,212121... é dada por:

$$1 + \frac{7}{33} = \frac{33+7}{33} = \frac{40}{33}$$

3.8 O CONJUNTO DOS NÚMEROS IRRACIONAIS

Como foi visto anteriormente, um número racional é equivalente a número decimal finito ou infinito periódico (dízimas periódicas), porém há números decimais que são infinitos e não periódicos, como por exemplo, $\sqrt{2} = 1,41421356237309504\ldots$, tais números, são chamados de irracionais e representados por $\mathbb{R}^1 \setminus \mathbb{Q}$. Observemos que os elementos de $\mathbb{R} \setminus \mathbb{Q}$ não podem ser escritos na forma $\frac{a}{b}$ com a e b inteiros e $b \neq 0$. Uma outra observação é que $\mathbb{Q} \cup \mathbb{R} \setminus \mathbb{Q} = \mathbb{R}$. Segundo (DARELA; CARDOSO; ROSA, 2011, p. 94) a descoberta dos números irracionais:

> [...] é devida aos pitagóricos, que deram conta que nem todas as medidas são inteiras. Ao estudarem a relação dos lados de um quadrado de medida uma unidade, deu-se conta por meio do teorema de Pitágoras, que não havia nenhum número conhecido que correspondesse a tal medida.

Alguns números irracionais são bastante conhecidos, por exemplo, os números $\Phi = \frac{1+\sqrt{5}}{2} \approx 1,618033$, $\pi \approx 3,1415$ (razão entre o comprimento da circunferência e seu diâmetro), $e \approx 2,718281$ (número de Euler), etc...

Exemplo 3.18. Mostre que $\sqrt{2}$ é irracional.

Solução. Suponhamos que $\sqrt{2}$ seja racional, então existem m e n inteiros com $n \neq 0$ tal que $\sqrt{2} = \frac{m}{n}$, com m e n primos entre si. Elevando ao quadrado ambos os lados dessa igualdade

[1] $\mathbb{R}$ denota o conjunto dos números reais.

temos:

$$(\sqrt{2})^2 = \left(\frac{m}{n}\right)^2 \Rightarrow 2n^2 = m^2 \tag{11}$$

Como m^2 é um número par, temos que m também é par, pois se m fosse ímpar teríamos m^2 ímpar, o que é uma contradição.

Portanto $m = 2k$, com $k \in \mathbb{Z}$. Logo $m^2 = 4k^2$. Substituindo $m^2 = 4k^2$ em (11), temos:

$$2n^2 = 4k^2 \Rightarrow n^2 = 2k^2 \tag{12}$$

De (12) temos que n^2 é um número par, o que implica n par. Mas isso é um absurdo, pois m e n são primos entre si, logo $\sqrt{2}$ não pode ser racional, sendo assim, $\sqrt{2}$ deve ser irracional.

3.9 O CONJUNTO $\mathbb{R}$ DOS NÚMEROS REAIS

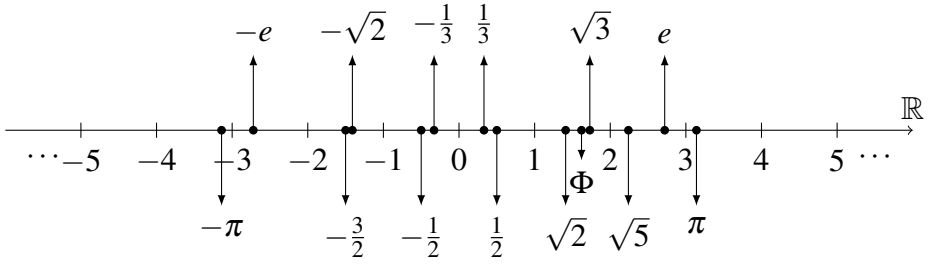
Introduziremos a seguir o conceito de número real. Não faremos aqui uma definição rigorosa desse conjunto, para uma abordagem mais aprofundada o leitor poderá consultar (LIMA, E, L., 2008).

A reunião do conjunto dos números racionais com o conjunto dos números irracionais forma o conjunto dos números reais, isto é, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$. Ou seja, o conjunto dos números reais é dado por:

$$\mathbb{R} = \{x; x \in \mathbb{Q} \text{ ou } x \in \mathbb{I}\}.$$

Segundo (LIMA et al., 1997) o conjunto $\mathbb{R}$ pode ser visto como modelo aritmético de uma reta, enquanto esta, por sua vez, é o modelo geométrico de $\mathbb{R}$ conforme ilustra a Figura (3). Esta reta numerada será chamada de reta real. O referido autor afirma ainda que tal propriedade é o que garante a continuidade da reta.

Figura 3 – Representação dos Reais



Fonte: Elaborado pelo autor.

No conjunto dos números reais estão definidas duas operações, adição (+) e multiplicação ($\cdot$), que satisfazem as seguintes propriedades:

P1. *Comutatividade*: Para todos $a, b \in \mathbb{R}$, temos:

$a + b = b + a$ e $a \cdot b = b \cdot a$

P2. *Associatividade*: Para todos $a,b,c \in \mathbb{R}$, temos:
$(a+b)+c = b+(a+c)$ e $(a\cdot b)\cdot c = b\cdot(a\cdot c)$

P3. *Distributividade*: Para todo $a,b,c \in \mathbb{R}$, temos:
$a\cdot(b+c) = a\cdot b + a\cdot c$

P4. *Elemento neutro*: Existem únicos números reais, indicados por 0 e 1, tais que, para qualquer $a \in \mathbb{R}$, temos:
$a+0 = a$ e $a\cdot 1 = a$

P5. *Existência de inversos aditivo e multiplicativo*: Para todo $a,b \in \mathbb{R}$, temos:
$a+b = 0$, e se $b \neq 0$ temos, $a\cdot b = 1$

P6. *Lei do cancelamento*: Se $a,b \in \mathbb{R}$ são tais que $a\cdot b = 1$, então $a = 0$ ou $b = 0$

A propriedade **P5** acima nos garante a existência de um inverso aditivo e um inverso multiplicativo. Na proposição a seguir veremos que os mesmos são únicos.

Proposição 3.14. Os inversos aditivo e multiplicativo do conjunto $\mathbb{R}$ são únicos.
Demonstração:
Unicidade do inverso aditivo:Sejam $a,b,b^{'} \in \mathbb{R}$ tais que $a+b = 0$ e $a+b^{'} = 0$, então a associatividade e a comutatividade da adição, juntamente com o elemento neutro dessa operação, nos dão:

$$b = b+0 = b+(a+b^{'}) = (b+a)+b^{'} = (a+b)+b^{'} = 0+b^{'} = b^{'}$$

De onde temos que o número real a possui um único inverso aditivo, o qual denotaremos por $-a$.
Unicidade do inverso multiplicativo: Sejam $a,b,b^{'} \in \mathbb{R}$ com $a \neq 0$ tais que $a\cdot b = 1$ e $a\cdot b^{'} = 1$, então a associatividade e a comutatividade da multiplicação, juntamente com o elemento neutro dessa operação, nos dão:

$$b = b\cdot 1 = b\cdot(a\cdot b^{'}) = (b\cdot a)\cdot b^{'} = (a\cdot b)\cdot b^{'} = 1\cdot b^{'} = b^{'}$$

De onde temos que o número real a possui um único inverso multiplicativo, o qual denotaremos por a^{-1}.

■

Podemos definir ainda as operações de subtração (-) e divisão $(\div)$ no conjunto $\mathbb{R}$. Basta colocarmos

$$a-b = a+(-b) \qquad \text{e} \qquad a\div b = a\cdot b^{-1},$$

com $b \neq 0$ no último caso, onde a e b são números reais.

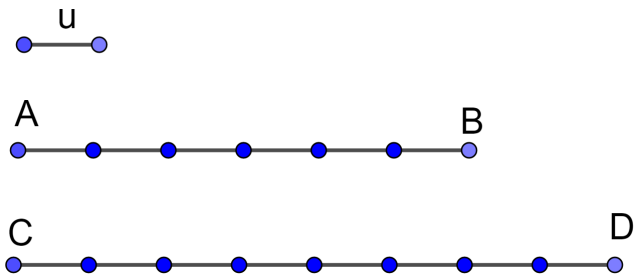
3.10 O CONCEITO DE MÁXIMO DIVISOR COMUM GENERALIZADO

Antes de definirmos o conceito de máximo divisor comum generalizado, necessitamos de algumas definições.

Definição 3.8. Sejam AB e CD dois segmentos de reta. Se existir um segmento de medida u e dois números naturais m e n tais que $\overline{AB}$[2]$= m \cdot u$ e $\overline{CD} = n \cdot u$, diremos que AB e CD são comensuráveis.

Exemplo 3.19. Na Figura 4, temos que os segmentos AB e CD são comensuráveis, pois tomando o segmento de medida u, temos $\overline{AB} = 6 \cdot u$ e $\overline{CD} = 8 \cdot u$.

Figura 4 – Segmentos comensuráveis



Fonte: Elaborado pelo autor.

Apesar da comensurabilidade ter sua essência através da geometria, essa definição pode ser estendida aos números reais, é o que nos mostra a definição a seguir.

Definição 3.9. Dois números reais r e s são comensuráveis se existirem inteiros não nulos m e n tais que $m \cdot r = n \cdot s$.

O conceito de múltiplo e divisor de um número real qualquer também pode ser definido como veremos a seguir.

Definição 3.10. Dizemos que um número real r é *múltiplo inteiro* de um número real s, ou que s é um *divisor inteiro* de r, se existir $a \in \mathbb{Z}$ tal que $r = a \cdot s$.

A partir das definições acima, temos a seguinte proposição

Proposição 3.15. Sejam r e s dois reais não nulos. As seguintes afirmações são equivalentes:

a) r e s são comensuráveis;

b) o quociente $\frac{r}{s}$ é um número racional;

c) existe um real t que é múltiplo inteiro comum de r e de s;

d) existe um real u que é divisor inteiro comum de r e de s.

Demonstração:

(**a**) $\Rightarrow$ (**b**): Se r e s são comensuráveis então existem $m,n \in \mathbb{Z} - \{0\}$, tais que $m \cdot r = n \cdot s$. Consequentemente $\frac{r}{s} = \frac{m}{n} \in \mathbb{Q}$.

(**b**) $\Rightarrow$ (**c**): Suponhamos que $\frac{r}{s} \in \mathbb{Q}$, digamos, $\frac{r}{s} = \frac{m}{n}$ com $m,n \in \mathbb{Z}$. Então multiplicando esta última igualdade por $s \cdot m$ obtemos que $t = m \cdot r = n \cdot s$ é múltiplo inteiro comum de r e de s, com $t \in \mathbb{R}$.

(**c**) $\Rightarrow$ (**d**): Seja $t \in \mathbb{R}$ um múltiplo inteiro comum de r e de s, digamos $t = m \cdot r = n \cdot s$, com

[2] AB representa o segmento de reta e $\overline{AB}$ representa sua medida.

$m,n \in \mathbb{Z} - \{0\}$. Então, o número $u = \frac{r}{n} = \frac{s}{m}$ é um inteiro comum de r e de s.
(**d**) $\Rightarrow$ (**a**): Seja u um divisor comum de r e de s, digamos $r = u \cdot m$ e $s = u \cdot m$, com $m,n \in \mathbb{Z} - \{0\}$. Então, temos que $m \cdot r = n \cdot s$ o que conclui a demonstração.

■

De posse das definições anteriores, podemos definir finalmente o conceito de máximo divisor comum generalizado.

Definição 3.11 (Máximo Divisor Comum Generalizado)**.** Sejam r e s dois números reais comensuráveis não nulos. Dizemos que u é o máximo divisor comum generalizado $(mdcg)$ e escrevemos $u = mdcg(r,s)$, se:

a) u é um divisor inteiro comum de r e s.

b) se $u^{'}$ é um divisor inteiro comum de r e s, então $u^{'} < u$.

Uma vez definido o conceito de máximo divisor comum generalizado, seria interessante termos uma maneira de calcular tal resultado. Os dois teoremas a seguir nos fornecem uma maneira para calcular o *mdcg* para quaisquer dois números reais comensuráveis.

TEOREMA 3.6. Sejam r e s dois números reais comensuráveis não nulos. Então

$$mdcg(r,s) = \frac{r}{s} = \frac{s}{v},$$

onde $\frac{u}{v}$ é a forma irredutível do racional $\frac{r}{s}$.

Demonstração. Consideremos aqui apenas o caso em que r e s são positivos. Para isso, observando inicialmente que a,b,c,d são inteiros tais que $ar = bs$ e $cr = ds$ então

$$\frac{a}{b} = \frac{d}{c},$$

e estas frações são frações equivalentes de $\frac{r}{s}$, portanto, os menores números naturais a e b que satisfazem a igualdade $ar = bs$ são encontrados quando analisamos o numerador e o denominador da fração irredutível que representa o número racional $\frac{r}{s}$. Daí, pela definição de *mdcg*, se $\frac{u}{v}$ é tal fração irredutível, então

$$mdcg(r,s) = \frac{r}{u} = \frac{s}{v},$$

completando assim a demonstração. ■

Observemos que caso r e s sejam números racionais, a fórmula dada no teorema 3.6 pode ser reescrita em termos das representações racionais em frações irredutíveis, como podemos ver no corolário a seguir.

Corolário 3.5. Sejam r e s racionais não nulos e sejam a,b,c,d inteiros tais que $\frac{a}{b}$ e $\frac{c}{d}$ são as representações para r e s, respectivamente, na forma de fração irredutível. Então:

$$mdcg(r,s) = \frac{(a,c)}{[b,d]}$$

Demonstração. Novamente aqui provaremos somente o caso em que r e s são positivos. Como $(a,b) = 1 = (c,d)$, temos:

$$\frac{r}{s} = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc} = \frac{a_1 d_1}{b_1 c_1}$$

Onde

$$a_1 = \frac{a}{(a,c)},\ b_1 = \frac{b}{(b,d)},\ c_1 = \frac{c}{(a,c)},\ d_1 = \frac{d}{(b,d)}$$

Como a fração $\frac{a_1 d_1}{b_1 c_1}$ é irredutível, do teorema 3.6, temos:

$$mdcg(r,s) = \frac{r}{a_1 \cdot d_1} = \frac{a}{b} \cdot \frac{(a,c)}{a} \cdot \frac{(b,d)}{d} = (a,b) \cdot \frac{(b,d)}{b \cdot d} = \frac{(a,c)}{\frac{b \cdot d}{(b,d)}}$$

Temos da proposição 3.13 que:

$$[a,b] = \frac{ab}{(a,b)}$$

Substituindo esta última igualdade em $mdcg(r,s) = \frac{(a,c)}{\frac{b \cdot d}{(b,d)}}$, temos:

$$mdcg(r,s) = \frac{(a,c)}{[b,d]}$$

Concluindo assim a demonstração. ■

Exemplo 3.20. Determine o *mdcg* para $0,25$ e $0,10$.

Solução. Pelo corolário 3.5, temos:

$$mdcg(0,25;0,10) = mdcg\left(\frac{25}{100}, \frac{10}{100}\right) = mdcg\left(\frac{1}{4}, \frac{1}{10}\right) = \frac{(1,1)}{[4,10]} = \frac{1}{20} = 0,05$$

Usaremos o conceito de máximo divisor comum generalizado mais adiante, este, será usado para possibilitar a resolução de equações diofantinas com coeficiente racionais, possibilitando assim resolver esse tipo de equação diretamente sem empregar artifícios matemáticos. Vale ressaltar que a definição 3.11 só tem sentido quando adotada como referência única e exclusiva a definição 3.10.

4 EQUAÇÕES DIOFANTINAS LINEARES

Consideremos o problema a seguir:

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

Afim de modelar o problema acima, seja X e Y as quantidades de selos de cinco e três reais respectivamente, logo a solução do problema se reduz em determinar o número de soluções inteiras e positivas da equação:

$$5X + 3Y = 50 \tag{13}$$

Equações do tipo (13) são chamadas de equações diofantinas em homenagem a Diofanto de Alexandria (aprox. 300 d.C). Estas nos dão uma base bastante sólida para solucionar problemas de aritmética, sendo assim se tornam uma ferramenta poderosa para resolver problemas como o descrito acima. A seguir faremos a definição formal das equações diofantinas de duas variáveis.

4.1 EQUAÇÕES DIOFANTINAS EM DUAS VARIÁVEIS

Segui agora a definição formal de equação diofantina linear em duas variáveis.

Definição 4.1. Uma equação diofantina linear de duas variáveis é uma equação do tipo:

$$aX + bY = c \tag{14}$$

Com $a, b, c \in \mathbb{Z}$, sendo X e Y variáveis a ser determinadas em $\mathbb{Z}$.
Quando nos deparamos com equações do tipo de (14) é comum nos perguntarmos:

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

Exemplo 4.1. Consideremos as equações diofantinas abaixo:

a) $2X + 5Y = 3$

b) $2X + 4Y = 5$

Notemos que na equação do item (a) temos $(2,5) \mid 3$ e é visível que $x_0 = -1$ e $y_0 = 1$ é uma solução para $2X + 5Y = 3$, esta solução não é única, já que $x_0 = 4$ e $y_0 = -1$ é outra solução para a mesma equação.
Agora observando a equação do item (b), vemos que $(2,4) \nmid 5$ e também podemos perceber que não existem inteiros x e y, tais que $2x + 4y = 5$ uma vez que $2x + 4y$ é um número par e, portanto, nunca igual a 5.

A proposição e o teorema a seguir nos fornecerão respostas mais gerais para os

questionamentos acima.

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

Demonstração. Suponhamos que a equação admita uma solução $x_0,\ y_0$. Então vale a igualdade $ax_0 + by_0 = c$. Como o $(a,b) \mid a$ e $(a,b) \mid b$, segue que ele divide $ax_0 + by_0$, logo divide c.

Agora, suponhamos que $(a,b) \mid c$, ou seja, $c = (a,b) \cdot \lambda$, com $\lambda \in \mathbb{Z}$. Por outro lado, o teorema de Bachet-Bézout nos garante que existem inteiros m e n tais que:

$$(a,b) = am + bn$$

Multiplicando ambos os lados da igualdade acima por λ, obteremos:

$$c = (a,b) \cdot \lambda = a \cdot (m\lambda) + b \cdot (n\lambda)$$

Logo, a equação $aX + bY = c$ admite pelo menos uma solução $x_0 = m\lambda$ e $y_0 = n\lambda$ ■

Consideremos que na equação $aX + bY = c$, com $a \neq 0$ ou $b \neq 0$ tenhamos $(a,b) \mid c$. Dividindo esta equação por (a,b), temos:

$$\frac{aX}{(a,b)} + \frac{bY}{(a,b)} = \frac{c}{(a,b)}$$

Fazendo:

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

Teremos:

$$a_1X + b_1Y = c_1$$

Que é uma equação equivalente a $aX + bY = c$ e do corolário (3.4), $(a_1, b_1) = 1$ e da proposição (3.11) esta equação sempre tem solução.

Exemplo 4.2. Mostre que a equação $2X + 3Y = 5$ sempre tem solução em $\mathbb{Z}$ e determine um par de números x e y que satisfaça a equação.

Solução. Como $(2,3) = 1$ e $1 \mid 5$, temos pela proposição que $2X + 3Y = 5$ admite solução em $\mathbb{Z}$. Claramente o par de inteiros $x = 1$ e $y = 1$ é solução da equação $2X + 3Y = 5$.

No exemplo (4.2) poderíamos encontrar outras soluções para $2X + 3Y = 5$ como por exemplo os pares de números $x = -2$, $y = 3$ e $x = -5$ e $y = 3$. Na verdade se tivermos uma equação diofantina linear $aX + bY = c$, com $(a,b) = 1$ ela terá infinitas soluções é o que o próximo teorema nos garante.

TEOREMA 4.1. Seja x_0 e y_0 uma solução da equação $aX + bY = c$, onde $(a,b) = 1$. Então, as

soluções x e y em $\mathbb{Z}$ da equação são:

$$x = x_0 + bt, \quad y = y_0 - at; \quad t \in \mathbb{Z}.$$

Demonstração. Consideremos x e y uma solução de $aX + bY = c$, logo:

$$\begin{aligned} ax + by = \ & c = ax_0 + by_0 \\ ax + by &= ax_0 + by_0 \\ ax - ax_0 &= by_0 - by \\ a(x - x_0) &= b(y_0 - y) \end{aligned}$$

Como $(a,b) = 1$, temos que $b \mid (x - x_0)$, logo:

$$x - x_0 = tb \Rightarrow x = x_0 + tb \text{ com } t \in \mathbb{Z}$$

Substituindo $x - x_0 = tb$ em $a(x - x_0) = b(y_0 - y)$, temos:

$$\begin{aligned} a(x - x_0) &= b(y_0 - y) \\ atb &= b(y_0 - y) \\ at &= y_0 - y \\ y &= y_0 - at \end{aligned}$$

Provando que as soluções da equação são do tipo proposto.

Como:

$$\begin{aligned} ax + by &= a(x_0 + tb) \\ &= ax_0 + atb + by_0 - bta \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

Provando que os números x e y são soluções da equação $aX + bY = c$. ■

Observação 4.1. Se caso tivéssemos $(a,b) = d$ no teorema 4.1, então teríamos as soluções x e y de $aX + bY = c$, dadas por:

$$x = x_0 + \frac{b}{d}t \quad \text{e} \quad y = y_0 - \frac{a}{d}t$$

De fato, seja x e y uma solução de $aX + bY = c$ da mesma forma que x_0 e y_0, logo:

$$ax + by = ax_0 + by_0 \Rightarrow a(x - x_0) = b(y_0 - y)$$

Dividindo esta última equação por $(a,b) = d$, temos:

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \tag{15}$$

Assim, $\frac{b}{d} \mid (x - x_0)$, já que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Logo $\exists\, t \in \mathbb{Z}$ tal que $x - x_0 = \frac{b}{d}t \Rightarrow x = x_0 + \frac{b}{d}t$. Substi-

tuindo $x - x_0$ por $\frac{b}{d}t$ na equação (15), obtemos de modo análogo $y_0 - \frac{a}{d}t$.

Se os valores de $|a|$, $|b|$ e $|c|$ forem pequenos fica fácil encontrar uma solução particular por inspeção. Caso contrário poderemos recorrer ao método descrito abaixo.

Dada a equação $aX + bY = c$, com $(a,b) \mid c$, vimos que é possível tomar uma equação $a_1X + b_1Y = c_1$ equivalente a $aX + bY = c$, com $(a,b) = 1$.
Agora usando o algoritmo de Euclides de trás para frente, é possível determinar $m, n \in \mathbb{Z}$ tais que:

$$ma + nb = 1$$

Multiplicando ambos os lados da igualdade acima por c_1, obtemos:

$$c_1ma + c_1nb = c_1$$

De onde temos que $x_0 = c_1m$ e $y_0 = c_1n$ é uma solução particular da equação dada.

Exemplo 4.3. Resolva a equação diofantina $20x + 12y = 8$.

Solução. A equação tem solução pois $(20,12) = 4 \mid 8$. Dividindo ambos os lados da equação por $4 = (20,12)$, obtemos:

$$5x + 3y = 4$$

Agora vamos achar uma solução particular x_0 e y_0 para esta última equação. Usando o algoritmo de Euclides, temos:

$$\begin{array}{l} 5 = 3 \cdot 1 + 2 \\ 3 = 2 \cdot 1 + 1 \end{array} \Rightarrow \begin{array}{l} 2 = 5 - 3 \cdot 1 \\ 1 = 3 - 2 \cdot 1 \end{array}$$

De onde temos que:

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

Multiplicando essa última igualdade por 2, temos:

$$4 = 5 \cdot 2 + 3 \cdot (3)$$

De onde temos $x_0 = 2$ e $y_0 = -2$, logo as soluções são:

$$x = 2 + 3t \quad \text{e} \quad y = -2 - 5t, \quad \text{com} \quad t \in \mathbb{Z}$$

4.1.1 Resolução de uma Equação Diofantina em Duas Variáveis nos Naturais

Há alguns problemas, como o apresentado no início desta seção, que se faz necessário resolver a equação diofantina em $\mathbb{N} \cup \{0\}$, ou seja, as equações do tipo $aX + bY = c$, onde $a,\ b,\ c \in \mathbb{N}$ e $X,\ Y \in \mathbb{N} \cup \{0\}$, contudo, para conseguirmos resolver equações desse tipo

precisamos do seguinte resultado.

Proposição 4.2. Sejam $a,\ b \in \mathbb{N}$, com $(a,b) = 1$. Todo número inteiro c pode ser escrito de modo único da forma:

$$c = ma + nb, \quad \text{com} \quad 0 \leq m < b \quad \text{e} \quad n \in \mathbb{Z}$$

Demonstração. Existência: Pelo teorema de Báchet-Bêzout, sabemos que existem $\alpha, \beta \in \mathbb{Z}$ tais que:

$$\alpha a + \beta b = (a,b) = 1$$

Multiplicando ambos os lados da igualdade acima por c, temos que:

$$\alpha ac + \beta bc = c$$

Da divisão euclidiana, sabemos que existem $q, m \in \mathbb{Z}$ com $0 \leq m < b$ tais que $\alpha c = qb + m$. Substituindo esse valor de αc na igualdade acima, obtemos:

$$\begin{aligned} c &= \alpha ac + \beta bc \\ &= a(qb + m) + \beta bc \\ &= aqb + am + \beta bc \\ &= am + b(aq + \beta c) \end{aligned}$$

Agora tomando $n = aq + \beta c \in \mathbb{Z}$, obtemos:

$$c = ma + nb, \text{ com } 0 \leq m < b \text{ e } n \in \mathbb{Z}$$

Unicidade: Suponhamos que:

$$ma + nb = m_1 a + n_1 b, \text{ com } 0 \leq m, m_1 < b$$

Logo,

$$\begin{aligned} ma - m_1 a &= n_1 b - nb \\ a(m - m_1) &= b(n_1 - n) \end{aligned}$$

Temos que $|m - m_1| < b$. Como $(a,b) = 1$ devemos ter $b \mid (m - m_1)$, o que só é possível quando $m - m_1 = 0 \Rightarrow m = m_1$, de onde temos imediatamente que $n = n_1$. ■

Consideremos a partir de agora o conjunto:

$$S(a,b) = \{xa + yb;\ x, y \in \mathbb{N}\} \cup \{0\}$$

onde $a, b \in \mathbb{N}$.
A proposição a seguir caracteriza os elementos de $S(a,b)$.

Proposição 4.3. Tem-se que $c \in S(a,b)$ se, e somente se, existem inteiros $m, n \in \mathbb{N} \cup \{0\}$ únicos, com $m < b$ tais que $c = ma + nb$.

Demonstração. Se $c = ma + nb$, com $m, n \in \mathbb{N} \cup \{0\}$, então $c \in S(a,b)$.
Agora, se $c \in S(a,b)$, então existem $x, y \in \mathbb{N} \cup \{0\}$ tal que $c = xa + yb$. Pela divisão euclidiana, temos $x = bq + m$ com $0 \leq m < b$, substituindo o valor de x nesta última igualdade, temos:

$$c = (bq + m)a + yb = ma + (aq + y)b$$

Tomando $n = aq + y \in \mathbb{N} \cup \{0\}$, temos:

$$c = am + nb$$

É verdade que m e n são únicos. A veracidade dessa afirmação decorre imediatamente da proposição (4.2). ■

Definição 4.2. O conjunto de lacunas de $S(a,b)$ é o conjunto:

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

Proposição 4.4. Temos que:

$$L(a,b) = \{ma - nb \in \mathbb{N};\ m, n \in \mathbb{N},\ m < b\}$$

Demonstração. Seja $l \in L(a,b)$. Notemos que l não pode ser escrito como $ma + nb$, pois não existem $m, n \in \mathbb{N} \cup \{0\}$ tal que $l = ma + nb$. Se m e n fossem determinados então $l \in S(a,b)$ que é um absurdo. No entanto, a proposição (4.2) garante que existe um inteiro $n^{'}$ tal que $l = ma + n^{`'}b$. Tomemos então $n^{'} = -n$, com $n \in \mathbb{Z}$. Logo, $l = ma - nb$. ■

TEOREMA 4.2. A equação $aX + bY = c$, onde $(a,b) = 1$, tem solução em $\mathbb{N}$ se, e somente se,

$$c \notin L(a,b) = \{ma - nb \in \mathbb{N};\ m, n \in \mathbb{N},\ m < b\}$$

Demonstração. Como a equação $aX + bY = c$ tem solução se, e somente se, $c \in S(a,b)$ e já que $L(a,b) = \mathbb{N} \backslash S(a,b)$, temos que $c \notin L(a,b)$. ■

Corolário 4.1. Seja $a, b \in \mathbb{N}$ tais que $(a,b) = 1$. Tem-se que $(a-1)(b-1)$ é o menor inteiro tal que $c \in S(a,b)$ para todo $c \geq (a-1)(b-1)$.

Demonstração. Como $L(a,b)$ é finito e o seu maior elemento ocorre quando $m = (b-1)$ e $n = 1$, temos que:

$$\text{Max}L(a,b) = (b-1)a - b$$

Portanto se,

$$\begin{aligned} c \geq (b-1)a - b + 1 &= ab - a + 1 \\ &= a(b-1) - (b-1) \\ &= (a-1)(b-1) \end{aligned}$$

a equação $aX + bY = c$ admite solução em $\mathbb{N}$. Agora se $c = (a-1)(b-1) - 1$, ela não admite solução em $\mathbb{N}$. ■

Diante dos resultados apresentados fica fácil determinar se a equação $aX + bY = c$ admite solução.

Se $(a,b) \nmid c$, a equação não tem solução em $\mathbb{Z}$, logo não tem solução em $\mathbb{N}$. Se $(a,b) \mid c$, a equação é equivalente a outra da forma $a_1X + b_1Y = c_1$, com:

$$a_1 = \frac{a}{(a,b)},\ b_1 = \frac{b}{(a,b)},\ c_1 = \frac{c}{(a,b)} \quad \text{e} \quad (a_1,b_1) = 1$$

Pelo algoritmo de Euclides, escrevemos:

$$1 = (a_1,b_1) = m_1a - n_1b$$

Logo:

$$c = cm_1a - cn_1b$$

Agora, usando a divisão euclidiana, escrevemos $cm_1 = qb + m$ com $m < b$, logo:

$$c = \begin{cases} ma + (qa - cn_1)b \in S(a,b), & \text{se} \quad qa \geq cn_1 \\ ma - (cn_1 - qa)b \in L(a,b), & \text{se} \quad cn_1 \geq qa \end{cases}$$

Vimos que no segundo casso a equação $a_1X + b_1Y = c_1$ não tem solução.

No primeiro caso a equação tem solução. Definimos então a solução minimal m e n da equação $a_1X + b_1Y = c_1$, com $m < b$, minimal no sentido de que se x e y são soluções, então $x \geq m$.

Com isso, enunciamos o resultado a seguir.

Proposição 4.5. Suponhamos que a equação $aX + bY = c$ com $(a,b) = 1$, tenha solução e seja $x_0 = m$ e $y_0 = n$ a solução minimal. As soluções x e y da equação são dadas por:

$$x = m + tb, \text{ e } y = n - ta,\ t \in \mathbb{N}, \text{ com } n - ta \geq 0$$

Exemplo 4.4. Determinar quais valores de $c \in \mathbb{N}$ a equação $7X + 3Y = c$ admite solução em $\mathbb{N} \cup \{0\}$.

Solução. Como o conjunto das lacunas de $S(7,3)$ é:

$$L(a,b) = \{7m - 3n \in \mathbb{N},\ m,n \in \mathbb{N},\ m < 3\} = \{1,2,4,5,8,11\}$$

Portanto, a equação $7X+3Y=c$ admite solução em $\mathbb{N}\cup\{0\}$ se, e somente se, $c\notin L(7,3)$.

Exemplo 4.5. Resolva a equação $7X+3Y=13$ em $\mathbb{N}\cup\{0\}$.

Solução. Do exemplo anterior $13\notin L(7,3)$, logo a equação possui soluções em $\mathbb{N}\cup\{0\}$. Usando o algoritmo de Euclides, temos:
$7=3\cdot 2+1\Rightarrow 1=7-3\cdot 2\Rightarrow 13=7\cdot 13-3\cdot 26\Rightarrow 13=7\cdot(3\cdot 4+1)-3\cdot 26\Rightarrow 13=$
$3\cdot 28+7\cdot 1-3\cdot 26\Rightarrow 13=7\cdot 1+3\cdot 2$
De onde segue que $x_0=1$ e $y_0=2$ é a solução minimal da equação, logo, as soluções são:

$$x=1+3t,\ y=2-7t,\ \text{com } t\in\mathbb{N}\cup\{0\}$$

Portanto a equação tem $x_0=1$ e $y_0=2$ como a única solução natural.

Ressaltamos que não se faz necessário usar toda a técnica desenvolvida acima, pois sendo b pequeno, é mais oportuno encontrarmos as soluções por inspeção.
No exemplo acima, bastaríamos ter testado quais dos valores $x=0$ ou $x=1$ tornava o número $13-7X$ divisível por 3, que como vimos é quando $x=1$.

4.2 RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES COM COEFICIENTES RACIONAIS

Chamaremos de "equação do tipo diofantina linear"a equação da forma $\alpha X+\beta Y=\gamma$ com α, β e γ números racionais em sua forma decimal ou fracionária, X e Y inteiros a serem determinados.

Observemos que se $\alpha=\frac{m}{n}$, $\beta=\frac{p}{q}$ e $\gamma=\frac{r}{s}$, com $m,n,p,q,r,s\in\mathbb{Z}$, podemos tomar uma equação $aX+bY=c$ equivalente a $\alpha X+\beta Y=\gamma$, com $a,b,c\in\mathbb{Z}$, com

$$a=msq,\quad b=nps\quad \text{e}\quad c=nqr.$$

Resolveremos a partir de agora alguns problemas que são modelados por equações do tipo diofantinas lineares, tomaremos como base o corolário 3.5 e a observação 4.1.

4.2.1 Problemas Modelados Por Equações Diofantinas Lineares

Problema 4.2.1. O conteúdo de um barril de vinho de 600 litros será distribuído em garrafas de 0,9l e de 1,5l. Determine qual o maior e o menor número de garrafas que serão utilizadas, sabendo que devem ser usadas no mínimo 100 garrafas de cada quantidade.

Solução. Sejam X e Y os números de garrafas com capacidades de 0,9l e 1,5l respectivamente.

Logo, pelo enunciado do problema devemos ter:

$$0,9X + 1,5Y = 600 \tag{16}$$

A equação (16) é uma equação do tipo diofantina linear, usando o conceito de máximo divisor comum generalizado, temos:

$$mdcg(0,9;1,5) = mdcg\left(\frac{9}{10}, \frac{15}{10}\right) = mdcg\left(\frac{9}{10}, \frac{3}{2}\right) = \frac{(9,3)}{[10,2]} = \frac{3}{10} = 0,3$$

Como:
$1,5 = 0,9 \cdot 1 + 0,6$
$0,9 = 0,6 \cdot 2 + 0,3$
Das igualdades acima, obtemos:

$$0,3 = 0,9 - 0,6 \cdot 1 = 0,9 - 1 \cdot (1,5 - 0,9 \cdot 1) = 0,9 - 1,5 + 0,9 \Rightarrow 0,3 = 0,9 \cdot 2 + 1,5 \cdot (-1)$$

Multiplicando a última igualdade acima por 2000, temos:

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

De onde concluímos que $x = 4000$ e $y = -2000$ é uma solução da equação (16). Pensando agora como na observação 4.1, temos:

$$x = 4000 + \frac{1,5}{0,3}t \Rightarrow x = 4000 + 5t, \quad \text{com} \quad t \in \mathbb{Z}$$

$$y = -2000 - \frac{0,9}{0,3}t \Rightarrow y = -2000 - 3t, \quad \text{com} \quad t \in \mathbb{Z}$$

Devemos ter no mínimo 100 garrafas de cada quantidade, vem que x e y devem ser maiores do que ou iguais a 100, logo:

$$x \geq 100 \Rightarrow 4000 + 5t \geq 100 \Rightarrow 5t \geq 3900 \Rightarrow t \geq -780$$
$$y \geq 100 \Rightarrow -2000 - 3t \geq 100 \Rightarrow -3t \geq 2100 \Rightarrow t \leq -700$$

Ou seja, $-780 \leq t \leq -700$.
Como, quanto maior o valor de t, maior será o número de garrafas de 0,9l e menor será o número de garrafas de 1,5l, temos:

$$x = 4000 + 5 \cdot (-700) \Rightarrow x = 500$$
$$y = -2000 - 3 \cdot (-700) \Rightarrow y = 100$$

E, quanto menor o valor de t, maior será o número de garrafas de 1,5l e menor será o número de

garrafas de 0,9l, temos:

$$x = 4000 + 5 \cdot (-780) \Rightarrow x = 100$$
$$y = -2000 - 3 \cdot (-780) \Rightarrow y = 340$$

Concluímos então, que o maior número de garrafas utilizadas é $500 + 100 = 600$ e o menor é $100 + 340 = 440$.

Problema 4.2.2. Um piscicultor pretende iniciar uma criação de tucunarés e tilápias. Cada tucunaré custa R$ 0,80 e cada tilápia R$ 0,60. Sabendo que o piscicultor dispõe de R$ 3000,00 para a compra das duas espécies e quer começar com no mínimo de 1000 peixes de cada espécie, qual o número máximo de peixes que ele pode comprar?

Solução. Sejam X e Y os números de tucunarés e tilápias respectivamente. O problema nos dá a seguinte equação:

$$0,8X + 0,6Y = 3000 \tag{17}$$

A equação acima é do tipo diofantina linear. Usando o corolário 3.5, para encontrar o máximo divisor comum generalizado de $0,8$ e $0,6$, temos:

$$mdcg(0,8;0,6) = mdcg\left(\frac{8}{10}, \frac{6}{10}\right) = mdcg\left(\frac{4}{5}, \frac{3}{5}\right) = \frac{(4,3)}{[5,5]} = \frac{1}{5} = 0,2$$

Como:

$$0,8 = 0,6 \cdot 1 + 0,2 \Rightarrow 0,2 = 0,8 + 0,6 \cdot (-1)$$

Multiplicando esta última igualdade por 1500, temos:

$$3000 = 0,8 \cdot (1500) + 0,6 \cdot (-1500)$$

Logo, $x = 1500$ e $y = -1500$ é uma solução para a equação (17), pensando como na observação 4.1, temos:

$$x = 15000 + \frac{0,6}{0,2}t \Rightarrow x = 15000 + 3t, \quad \text{com} \quad t \in \mathbb{Z} \tag{18}$$
$$y = -15000 - \frac{0,8}{0,2}t \Rightarrow y = -15000 - 4t, \quad \text{com} \quad t \in \mathbb{Z} \tag{19}$$

Como devemos ter um número mínimo de 1000 peixes para cada espécie, temos:

$$x \geq 1000 \Rightarrow 15000 + 3t \Rightarrow t \leq -4666,666\ldots \Rightarrow t \leq -4666$$
$$y \geq 1000 \Rightarrow -15000 - 4t \geq 1000 \Rightarrow t \leq -4000$$

Analisando as equações 18 e 19 concluímos que t deve ser igual a -4666 para que o número de peixes seja máximo, substituindo esse valor nas referidas equações, temos:

$$x = 15000 + 3 \cdot (-4666) = 1002$$

$$y = 15000 - 4 \cdot (-4666) = 3664$$

De onde temos que o número máximo de peixes é $1002 + 3664 = 4666$.

Problema 4.2.3. Em uma livraria o custo de uma impressão simples (preto e branco) é de R$ 0,15 e de uma impressão colorida é de R$ 0,35. Qual o número máximo de impressões feitas em um dia, sabendo que o total arrecadado foi de R$ 40,00?

Solução. Seja X o número de impressões simples e Y o número de impressões coloridas. O problema nos fornece a seguinte equação:

$$0,15X + 0,35Y = 40 \tag{20}$$

A equação (20) é do tipo diofantina linear. Usando o corolário 3.5, para encontrar o máximo divisor comum generalizado de $0,15$ e $0,35$, temos:

$$mdcg(0,15;0,35) = mdcg\left(\frac{15}{100}, \frac{35}{100}\right) = mdcg\left(\frac{3}{20}, \frac{7}{20}\right) = \frac{(3,7)}{[20,20]} = \frac{1}{20} = 0,05$$

Agora, como:

$$0,35 = 2 \cdot 0,15 + 0,05 \Rightarrow 0,05 = 0,15 \cdot (-2) + 0,35$$

Multiplicando essa última desigualdade por 800, temos:

$$40 = 0,15 \cdot (-1600) + 0,35 \cdot 800$$

De onde temos que $x = -1600$ e $y = 800$ é uma solução da equação (20). Pensando como na observação 4.1, temos que:

$$x = -1600 + \frac{0,35}{0,05}t \Rightarrow x = -1600 + 7t, \quad \text{com} \quad t \in \mathbb{Z} \tag{21}$$

$$y = 800 - \frac{0,15}{0,05}t \Rightarrow y = 800 - 3t, \quad \text{com} \quad t \in \mathbb{Z} \tag{22}$$

Para termos um número máximo de impressões, devemos ter o número de impressões coloridas menor possível e isso só acontece quando $y \geq 0$, ou seja:

$$800 - 3t \geq 0 \Rightarrow t \leq \frac{800}{3} \Rightarrow t \leq 266,666\ldots \Rightarrow t = 266$$

Substituindo esse valor de t nas equações (21) e (22), temos:

$$x = -1600 + 7 \cdot 266 = 262$$
$$y = 800 - 3 \cdot 266 = 2$$

De onde concluímos que o número máximo de impressões foi $262 + 2 = 264$.

Problema 4.2.4. Uma caminhonete transporta telhas e tijolos de uma fábrica. Sabe-se que cada telha tem 2,8 kg de massa e cada tijolo tem 0,5 kg. O peso líquido máximo que a caminhonete pode transportar é de 9000 kg. Sabendo que em cada carga deve-se ter no mínimo 1000 telhas, descubra qual a quantidade máxima de cada produto que poderá ser transportado.

Solução. Seja X o número de telhas e Y o número de tijolos. o problema nos fornece a seguinte equação:

$$2,8X + 0,5Y = 9000 \tag{23}$$

A equação (23) é do tipo diofantina linear. Usando o corolário 3.5 para calcular o *mdcg* de $2,8$ e $0,5$, temos:

$$mdcg(2,8;0,5) = mdcg\left(\frac{28}{10}, \frac{5}{10}\right) = mdcg\left(\frac{14}{5}, \frac{1}{2}\right) = \frac{(14,1)}{[5,2]} = \frac{1}{10} = 0,1$$

Como:
$2,8 = 0,5 \cdot 5 + 0,3 \Rightarrow 0,3 = 2,8 - 0,5 \cdot 5$
$0,5 = 0,3 \cdot 1 + 0,2 \Rightarrow 0,2 = 0,5 - 0,3 \cdot 1$
$0,3 = 0,2 \cdot 1 + 0,1 \Rightarrow 0,1 = 0,3 - 0,2 \cdot 1$
De onde temos:
$0,1 = 0,3 - 1 \cdot (0,5 - 0,3 \cdot 1) = 0,3 - 0,5 + 0,3 = 0,3 \cdot 2 - 0,5 = 2 \cdot (2,8 - 0,5 \cdot 5) - 0,5 =$
$2,8 \cdot 2 - 0,5 \cdot 10 - 0,5 \Rightarrow 0,1 = 2,8 \cdot 2 + 0,5 \cdot (-11)$
Multiplicando esta última igualdade por 18000, temos:

$$9000 = 2,8 \cdot 36000 + 0,5(-198000)$$

Logo, $x = 36000$ e $y = -198000$ é uma solução da equação (23), pensando agora como na observação 4.1, temos:

$$x = 36000 + \frac{0,5}{0,1}t \Rightarrow x = 36000 + 5t, \quad \text{com} \quad t \in \mathbb{Z} \tag{24}$$

$$y = -198000 - \frac{2,8}{0,1}t \Rightarrow y = -198000 - 28t, \quad \text{com} \quad t \in \mathbb{Z} \tag{25}$$

Como cada carga deve ter no mínimo 1000 tijolos, devemos ter $y \geq 1000$, ou seja:

$$-198000 - 28t \geq 1000 \Rightarrow -28t \geq 199000 \Rightarrow t \leq -7107,14286 \Rightarrow t = -7108$$

Substituindo esse valor de t nas equações (24) e (25), obtemos:

$$x = 36000 + 5 \cdot (-7108) = 460$$
$$y = -198000 - 28 \cdot (-7108) = 1024$$

Concluímos então que a quantidade máxima de cada produto é 460 telhas e 1024 tijolos.

Problema 4.2.5. Marta deseja comprar maçãs e peras para distribuir entre os seus 15 familiares. Sabendo que cada maçã custa R$ 0,50 e que cada pera R$ 0,75 e que Marta pretende comprar no mínimo 10 frutas de cada tipo, qual é a quantidade máxima de frutas que Marta conseguirá comprar com R$ 40,00?

Solução. Seja X o número de maçãs e Y o número de peras, pelo enunciado do problema, temos a seguinte equação:

$$0,50X + 0,75Y = 40 \tag{26}$$

A equação (26) é do tipo diofantina linear. Usando o corolário 3.5 para determinar o máximo divisor comum generalizado entre $0,50$ e $0,75$, temos:

$$mdcg(0,50;0,75) = mdcg\left(\frac{50}{100}, \frac{75}{100}\right) = mdcg\left(\frac{1}{2}, \frac{3}{4}\right) = \frac{(1,3)}{[2,4]} = \frac{1}{4} = 0,25$$

Como:
$0,75 = 0,50 \cdot 1 + 0,25 \Rightarrow 0,25 = 0,50 \cdot (-1) + 0,75$
Multiplicando esta última igualdade por 160, temos:

$$40 = 0,50 \cdot (-160) + 0,75 \cdot 160$$

De onde temos que $x = -160$ e $y = 160$ é uma solução da equação (26). Agindo agora como na observação 4.1, temos:

$$x = -160 + \frac{0,75}{0,25}t \Rightarrow x = -160 + 3t, \quad \text{com} \quad t \in \mathbb{Z} \tag{27}$$

$$y = 160 - \frac{0,50}{0,25}t \Rightarrow y = 160 - 2t, \quad \text{com} \quad t \in \mathbb{Z} \tag{28}$$

Como Marta pretende comprar um número mínimo de 10 frutas de cada tipo, devemos ter $x \geq 10$ e $y \geq 10$, ou seja:

$$-160 + 3t \geq 10 \Rightarrow 3t \geq 170 \Rightarrow t \geq 56,666\ldots \Rightarrow t \geq 57$$
$$160 - 2t \geq 10 \Rightarrow -2t \geq -150 \Rightarrow t \leq 75$$

Analisando as equações (27) e(28), concluímos que temos o maior número de frutas quando $t = 75$, substituindo esse valor nas referidas equações, obtemos:

$$x = -160 + 3 \cdot 75 \Rightarrow x = 65$$
$$y = 160 - 2 \cdot 75 \Rightarrow y = 10$$

Logo, o maior número de frutas que Marta conseguirá comprar é $65 + 10 = 75$.

4.3 EQUAÇÕES DIOFANTINAS EM TRÊS VARIÁVEIS

Definição 4.3. Uma equação diofantina linear de três variáveis é uma equação do tipo:

$$aX + bY + cZ = k$$

Onde $a, b, c, k \in \mathbb{Z}$ e X, Y e Z variáveis a serem determinadas em $\mathbb{Z}$.

De modo semelhante às equações diofantinas em duas variáveis, as de três varáveis admitem solução se, e somente se, $(a,b,c) \mid k$. De fato, seja $d = (a,b,c)$ e suponhamos que a equação admita uma solução x_0, y_0, z_0, valendo a igualdade $ax_0 + by_0 + cz_0 = k$, como $d \mid a$, $d \mid b$ e $d \mid c$, temos que existem a_1, b_1 e c_1 inteiros tais que:

$$a = a_1 d,\ b = b_1 d \quad \text{e} \quad c = c_1 d$$

Substituindo esses valores em $ax_0 + by_0 + cz_0 = k$, obtemos:

$$\begin{aligned} a_1 d x_0 + b_1 d x_0 + c_1 z_0 &= k \\ d(a_1 x_0 + b_1 x_0 + c_1 z_0) &= k \end{aligned}$$

Isso mostra que $d \mid k$.

Suponhamos agora que $d \mid k$ e portanto $k = qd$ com $q \in \mathbb{Z}$. A generalização do teorema de Báchet-Bézout garante que existem m, n e t inteiros tais que:

$$am + bn + ct = d$$

Multiplicando ambos os membros desta igualdade por q, temos:

$$a(mq) + b(nq) + c(tq) = qd = k$$

De onde $x_0 = mq$, $y_0 = nq$ e $z_0 = tq$ é uma solução particular da equação diofantina $aX + bY + cZ = k$.

Provamos assim o seguinte resultado.

Proposição 4.6. A equação diofantina $aX + bY + cZ = k$ com a, b, c inteiros não nulos e k um inteiro qualquer admite solução se, e somente se, $(a,b,c) \mid k$.

Para determinar as soluções da equação definida acima, reduziremos a mesma para duas variáveis, que sabemos resolver utilizando os resultados aqui desenvolvidos. Vejamos como proceder na resolução de tais equações na proposição a seguir.

Proposição 4.7. Seja x_0, y_0 e z_0 uma solução particular da equação $aX + bY + cZ = k$, com $(a,b,c) \mid k$ e a, b e c inteiros não nulos. A equação admite infinitas soluções que são dadas da

forma:

$$x = x_0(l_0 - cq) + \frac{bt}{d}$$
$$y = y_0(l_0 - cq) - \frac{at}{d}$$
$$z = dq + r_0$$

Com $d = (a,b)$ e $r_0, l_0, q, t \in \mathbb{Z}$.

Demonstração. Observemos primeiramente que a equação $aX + bY + cZ = k$ pode ser reescrita como:

$$aX + bY = k - cZ \tag{29}$$

Para que a equação acima tenha solução, devemos ter $d \mid (k - cZ)$. Consideremos que $z = dq + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < q$, logo:

$$\begin{aligned} k - cZ &= k - c(dq + r) \\ &= k - cdq + cr \\ &= (k - cr) - cdq \end{aligned} \tag{30}$$

Como $d \mid cdq$, temos que ter $d \mid (k - cr)$. Assim, existe $l \in \mathbb{Z}$ tal que:

$$k - cr = dl \Rightarrow dl + cr = k \tag{31}$$

Observemos que a equação acima possui solução, uma vez que $(d,c) = (a,b,c)$ e $(a,b,c) \mid k$. Seja r_0 e l_0 uma solução particular da equação (31), logo:

$$dl_0 + cr_0 = k \Rightarrow k - cr_0 = dl_0 \tag{32}$$

Como:

$$\begin{aligned} k - cZ &= (k - cr) - cdq \\ &= dl_0 - cdq \\ &= d(l_0 - cq) \end{aligned} \tag{33}$$

Substituindo (33) em (29), obtemos:

$$aX + bY = d(l_0 - cq)$$

Que possui solução para $\forall\ q \in \mathbb{Z}$. Seja agora x_0 e y_0 uma solução particular de $aX + bY = d$, ou seja, $ax_0 + by_0 = d$, multiplicando esta última igualdade por $(l_0 - cq)$, obtemos:

$$a(x_0(l_0 - cq)) + b(y_0(l_0 - cq)) = d(l_0 - cq)$$

De onde segue que:

$$x = x_0(l_0 - cq) + \frac{bt}{d}$$
$$y = y_0(l_0 - cq) - \frac{at}{d}$$
$$z = dq + r_0$$

Com $d = (a,b)$ e $r_0, l_0, q, t \in \mathbb{Z}$. ■

Exemplo 4.6. Determine a solução geral da equação diofantina $14X + 35Y + 11Z = 255$

Solução. Podemos reescrever a equação $14X + 35Y + 11Z = 255$ como:

$$14X + 35Y = 255 - 11Z$$

Onde a mesma admite solução se, e somente se, $(35,14) = 7 \mid (255 - 11Z)$. Pela divisão euclidiana, consideremos $Z = 7q + r$ com $q, r \in \mathbb{Z}$ e $0 < r < 7$, de modo que $7 \mid (255 - 11(7q + r))$.
Como:
$255 - 11(7q + r) = (36 \cdot 7 + 3) - 11 \cdot (7q + r) = 36 \cdot 7 + 3 - 11 \cdot 7q + 11r =$
$7 \cdot (36 - 11q) + (3 - 11r)$
Logo $7 \mid (255 - 11Z)$ se

$$7 \mid (7 \cdot (36 - 11q) + (3 - 11r))$$

Ou seja,

$$7 \mid (3 - 11r)$$

Como $0 < r < 7$, o único valor possível é $r = 6$. Assim, $Z = 7q + 6$ de onde temos que:

$$\begin{aligned} 14X + 35Y &= 255 - 11(7q + 6) \\ &= 255 - 77q - 66 \\ &= 189 - 77q \end{aligned}$$

Dividindo $14X + 35Y = 189 - 77q$ por 7, temos:

$$7X + 5Y = 29 - 11q$$

Determinamos agora uma solução particular, usando o algoritmo de Euclides, para esta última equação:

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

Multiplicando esta última igualdade por $27 - 11q$, temos:

$$27 - 11q = 2(-54 + 22q) - 5(27 - 11q)$$

Logo, a solução geral de $14X + 35Y + 11Z = 255$ é:

$$\begin{aligned} x &= -54 + 22q + 5t \\ y &= 27 - 11q - 2t \qquad\qquad \text{com } q,t \in \mathbb{Z} \\ z &= 7q + 6 \end{aligned}$$

Uma outra forma de resolver a equação $aX + bY + cZ = k$ é tomarmos $p = aX + bY$ e resolver a equação $p + cZ = k$, obtendo $p = p_0 + ct$ e $z = z_0 - t$, depois resolvemos:

$$aX + bY = p_0 + ct$$

Determinando os valores x e y.
Ilustramos esse processo no exemplo a seguir.

Exemplo 4.7. Resolva a equação diofantina $3X + 5Y + 8Z = 46$.

Solução. Como $(3,5,8) = 1 \mid 46$ a equação possui solução. Agora, seja $p = 3X + 5Y$, logo:

$$p + 8Z = 46$$

É óbvio que a equação acima tem solução, e é fácil ver que $p = 6$ e $z_0 = 5$ é uma solução particular da mesma, logo sua solução geral é dada por:

$$p = 6 + 8t \quad \text{e} \quad z = 5 - t \quad \text{com} \quad t \in \mathbb{Z}$$

De onde temos:

$$3X + 5Y = 6 + 8t$$

Como $(3,5) \mid (6 + 8t)$ a equação acima também tem solução. Usando o algoritmo de Euclides, temos:

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

Logo:
$1 = 3 - 2 \cdot 1 = 3 - 2 \cdot (5 - 3 \cdot 1) = 3 - 5 \cdot 1 + 3 \cdot 1 \Rightarrow 1 = 3 \cdot 2 + 5 \cdot (-1)$
Multiplicando a última igualdade acima por $6 + 8t$, temos:

$$3(12 + 16t) + 5(-6 - 8t) = 6 + 8t$$

De onde temos que a solução geral da equação $3X + 5Y + 8Z = 46$ é:

$$\begin{aligned} x &= 12 + 16t + 5t_1 \\ y &= -6 - 8t - 3t_1 \qquad\qquad \text{com } t, t_1 \in \mathbb{Z} \\ z &= 5 - t \end{aligned}$$

4.4 GENERALIZAÇÃO: EQUAÇÕES DIOFANTINAS EM VARIAS VARIAVÉIS

Definição 4.4. Uma equação diofantina em n variáveis é uma equação da forma:

$$a_1X_1 + \cdots + a_nX_n = k$$

Com $a_i \in \mathbb{Z} \setminus \{0\}$, para $\forall\, i = 1, \ldots, n$.

De modo similar as equações diofantinas apresentadas anteriormente, a equação acima tem solução se, e somente se, $(a_1, \ldots, a_n) \mid k$, este resultado é mostrado na proposição a seguir.

Proposição 4.8. A equação diofantina $a_1X_1 + \cdots + a_nX_n = k$, $a_i \in \mathbb{Z}$, com $a_i \neq 0$ para $\forall\, i = 1, \ldots, n$, e $k \in \mathbb{Z}$ admite solução se, e somente se, $(a_1, \ldots, a_n) = d \mid k$.

Demonstração. Da generalização do teorema de Báchet-Bézout, sabemos que:

$$I(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} a_i x_i;\ x_i \in \mathbb{Z} \right\} = d\mathbb{Z}$$

A equação $a_1X_1 + \cdots + a_nX_n = k$ possui solução se, e somente se, $k \in I(a_1, \ldots, a_n)$ o que é equivalente a $k \in d\mathbb{Z}$, ou seja;

$$ld = k \text{ para algum } l \in \mathbb{Z}$$

esta última igualdade mostra que $d \mid k$ ■

4.4.1 Solução Geral

Apresentaremos aqui um método, indutivo, para solucionar as equações diofantinas de n variáveis, tendo a mesma solução. O método consiste basicamente em reduzir a equação dada em outra de duas variáveis, a qual sabemos resolver. Assim, determinaremos o valor da n-ésima variável. Após, devemos solucionar uma equação de $n-1$ variáveis, e, procedendo analogamente, obteremos o valor da variável de índice $n-1$. Repetindo esse processo, paramos quando chegarmos em uma equação diofantina de duas variáveis, ou seja, uma equação da forma $a_1X_1 + a_2X_2 = k$, a qual sabemos resolver. Vejamos na prática como proceder.

Consideremos a equação diofantina

$$a_1X_1 + \cdots + a_nX_n = k, \tag{34}$$

com $(a_1, \ldots, a_n) \mid k$.
Tomemos $p^{(1)} = a_1X_1 + \cdots + a_{n-1}X_{n-1}$. Assim, a equação (34) pode ser representada por:

$$p^{(1)} + a_nX_n = k \tag{35}$$

Como $(1,a_n) = 1 \mid k$ a equação (35) tem solução e esta é dada por:

$$\begin{aligned} p^{(1)} &= p_1 + a_n t_1 \\ x_n &= x_n^{'} - t_1 \end{aligned} \qquad \text{com } t_1 \in \mathbb{Z}$$

Onde $p_1, x_n^{'}$ é uma solução particular da equação (35).
Agora devemos resolver a equação $p^{(1)} = p_1 + a_n t_1$, a qual pode ser reescrita como,

$$a_1 X_1 + \cdots + a_{n-1} X_{n-1} = p_1 + a_n t_1 \tag{36}$$

notemos que (36) só possui solução se $(a_1,\ldots,a_{n-1}) \mid (p_1 + a_n t_1)$, escolhemos então, $t_1 = t_1^{'}$, de modo que $(a_1,\ldots,a_{n-1}) \mid (p_1 + a_n t_1^{'})$. Devemos observar, no entanto, que que quando $t_1 = t_1^{'}$, a variável x_n será escrita como $x_n = x_n^{'} - t_1^{'}$. Na verdade, devemos ter $t_1^{'} = (a_1,\ldots,a_{n-1})q_1 + r_1$, com $0 \leq r_1 < (a_1,\ldots,a_{n-1})$, onde r_1 é um inteiro determinado e q_1 é um inteiro qualquer, logo:

$$a_1 X_1 + \cdots + a_{n-1} X_{n-1} = l_1 + a_n(a_1,\ldots,a_{n-1})q_1 \quad \text{com} \quad l_1 = p_1 + a_n r_1$$

Prosseguindo de modo análogo ao passo anterior, seja $p^{(2)} = a_1 X_1 + \cdots + a_{n-2} X_{n-2}$, logo:

$$p^{(2)} + a_{n-1} X_{n-1} = l_1 + a_n(a_1,\ldots,a_{n-1})q_1 \tag{37}$$

Como $(1,a_{n-1}) = 1 \mid (l_1 + a_n(a_1,\ldots,a_{n-1}))$ a equação (37) possui solução e são dadas por:

$$\begin{aligned} p^{(2)} &= p_2 + a_{n-1} t_2 \\ x_{n-1} &= x_{n-1}^{'} - t_2 \end{aligned} \qquad \text{com } t_2 \in \mathbb{Z}$$

Onde $p_2, x_{n-1}^{'}$ é uma solução particular da equação (37).
Devemos agora resolver a seguinte equação:

$$a_1 X_1 + \cdots + a_{n-2} X_{n-2} = p_2 + a_{n-1} t_2 \tag{38}$$

A equação (38) só possui solução se $(a_1,\ldots,a_{n-2}) \mid (p_2 + a_{n-1} t_2)$. Tomemos então $t_2 = t_2^{'}$ onde $t_2^{'} = (a_1,\ldots,a_{n-2})q_2 + r_2$, com $0 \leq r_2 < (a_{1,\ldots},a_{n-2})$, onde r_2 é um inteiro determinado e q_2 um inteiro qualquer. Substituindo esse valor de $t_2^{'}$ na equação (38), temos:

$$a_1 X_1 + \cdots + a_{n-2} X_{n-2} = l_2 + a_{n-1}(a_1,\ldots,a_{n-2})q_2 \quad \text{com} \quad l_2 = p_2 + a_{n-1} r_2$$

Basta, então, tomarmos $p^{(3)} = a_1 X_1 + \cdots + a_{n-3} X_{n-3}$ e procedermos como nos passos anteriores.

Concluímos, então, que o método consiste em repetirmos o processo $n-2$ vezes, no qual determinamos os valores das variáveis X_k, com $k = 3,\ldots,n$. E, a partir do i-ésimo passo é necessário determinarmos os valores t_i para que $(a_1,\ldots,a_{n-i}) \mid (p_i + a_{n-i+1} t_i)$ com $1 \leq i \leq n-2$.

Agindo dessa forma chegaremos a seguinte equação:

$$a_1X_1 + a_2X_2 = l_{n-3} + a_4(a_1,a_2,a_3)q_{n-3}; \quad \text{com} \quad l_{n-3} = p_{n-3} + a_4r_{n-3} \tag{39}$$

Com r_{n-3} determinado no passo anterior de modo que $t_{n-3} = t'_{n-3} = (a_1,a_2,a_3)q_{n-3} + r_{n-3}$ e tenhamos $(a_1,a_2,a_3) \mid (p_{n-3} + a_4t_{n-3})$. Resolvendo a equação (39), temos:

$$x_1 = x'_1 + \frac{a_2}{(a_1,a_2)}t_{n-1}$$

$$x_2 = x'_2 + \frac{a_2}{(a_2,a_2)}t_{n-1}$$

Onde $t_{n-1} \in \mathbb{Z}$.

Concluímos então, que a solução geral de (34) é dada por:

$$x_1 = x'_1 + \frac{a_2}{(a_1,a_2)}t_{n-1}$$

$$x_2 = x'_2 + \frac{a_2}{(a_2,a_2)}t_{n-1}$$

$$x_3 = x'_3 - t'_{n-2}$$

$$\vdots$$

$$x_n = x'_n - t'_1$$

Com $t'_i = (a_1,\ldots,a_{n-i})q_i + r_i$, onde r_i é um inteiro determinado, q_i um inteiro qualquer e $i = 1,\ldots,n-2$ é o número de passos realizados.

5 APLICAÇÃO DAS EQUAÇÕES DIOFANTINAS LINEARES

5.1 EQUAÇÕES DIOFANTINAS LINEARES E CONTEÚDOS DO ENSINO MÉDIO

É totalmente aceitável que as equações diofantinas lineares em duas variáveis podem ser facilmente entendidas por educandos do ensino básico, pois os conteúdos exigidos como pré-requisitos, o conjunto dos números inteiros, o conceito de divisibilidade entre dois inteiros e o de máximo divisor comum, são conhecidos pelos mesmos. Para facilitar ainda mais esse entendimento, alguns conteúdos lecionados na educação básica, podem ser usados para facilitar ainda mais o entendimento desses alunos a respeito de tais equações, como mostraremos a seguir.

5.1.1 Relação entre Equações Diofantinas Lineares e a Função Afim

Consideremos o seguinte exemplo:

Exemplo 5.1. Na cidade de matemáticópolis um motorista de táxi cobra uma taxa fixa de R$ 5,00 pela "bandeirada" mais R$ 3,00 por quilômetro rodado.

Se x for o número de quilômetros rodados o preço y da corrida será dado por:

$$y = 3x + 5$$

Pensando de um modo mais geral no exemplo acima, se o preço da bandeirada fosse b reais e o preço do quilômetro rodado a reais, então o preço y de uma corrida seria dado, em reais, por:

$$y = ax + b \tag{40}$$

Se tomarmos x e y números reais a equação (40) é dita função[3] polinomial do primeiro grau ou simplesmente função afim, mais formalmente:

Definição 5.1. Uma função $f : \mathbb{R} \to \mathbb{R}$ chama-se afim quando existem constantes $a, b \in \mathbb{R}$ tais que $f(x) = ax + b$.

Observemos que a equação (40) pode ser escrita como $a_1x + b_1 = c$ com $a_1, b_1, c, x, y \in \mathbb{R}$. Logo, se torna inevitável compararmos as equações diofantinas lineares de duas variáveis com a função afim, no entanto, devemos ter cuidado com tal comparação, já que os conjuntos numéricos que são trabalhados as equações diofantinas e a função afim são diferentes. Podemos afirmar que toda equação diofantina linear em duas variáveis representa uma função afim com as variáveis x e y assumindo valores inteiros, assim, a representação geométrica da mesma seria um conjunto de pontos do plano cartesiano com coordenadas inteiras. Também podemos levar

[3] Dados dois conjuntos não vazios X e Y, uma função $f : X \to Y$ (lê-se: uma função de X em Y) é uma regra que determina como associar a cada elemento $x \in X$ um único elemento $y = f(x) \in Y$.

em conta o fato de x e y na equação diofantina pertencerem ao conjunto $\mathbb{R}$ dos números reais, obtendo assim uma função afim. Mas não podemos afirmar que toda função afim representa uma equação diofantina, se tomarmos, por exemplo, a e b números irracionais veremos isso facilmente.

Para esclarecer melhor essas diferenças e semelhanças, vejamos o exemplo a seguir.

Exemplo 5.2. Represente a solução geral da equação diofantina $2x+y=3$ no plano cartesiano e faça uma comparação com o gráfico da função $f:\mathbb{R}\to\mathbb{R}$ dada pela equação $2x+y=3$.

Solução. Podemos resolver facilmente a equação $2x+y=3$ com os conhecimentos adquiridos até o momento. Como $(2,1)=1 \mid 3$ a equação tem soluções inteiras e já que:

$$2\cdot 1+1\cdot 1=3$$

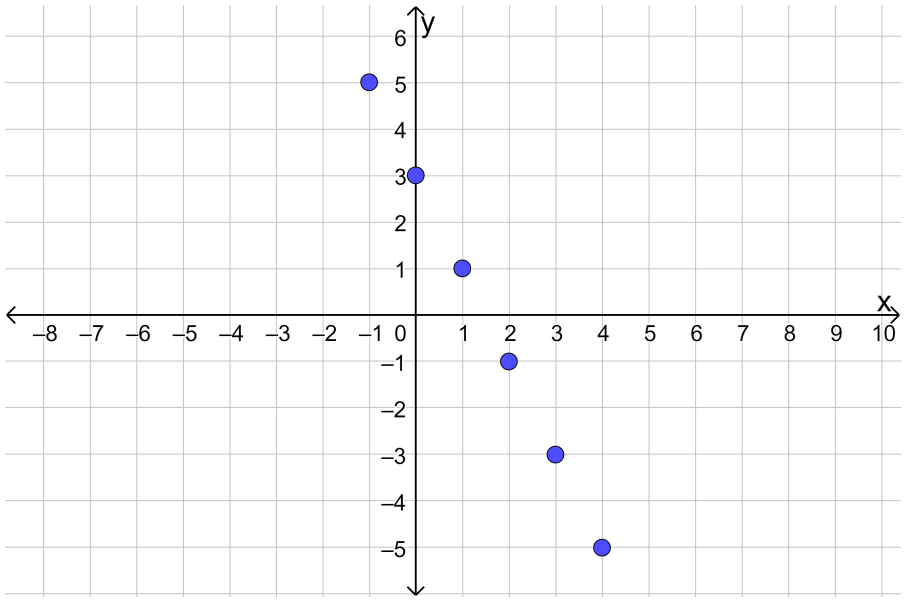
Temos que $x=1$ e $y=1$ é uma solução particular de $2x+y=3$, logo:

$$x=1+t \quad \text{e} \quad y=1-2t \quad \text{com } t\in\mathbb{Z}.$$

Tomando $t=\{-2,-1,0,1,2,3\}$ obtemos $x=\{-1,0,1,2,3,4\}$ e $y=\{5,3,1,-1,-3,-5\}$ respectivamente.

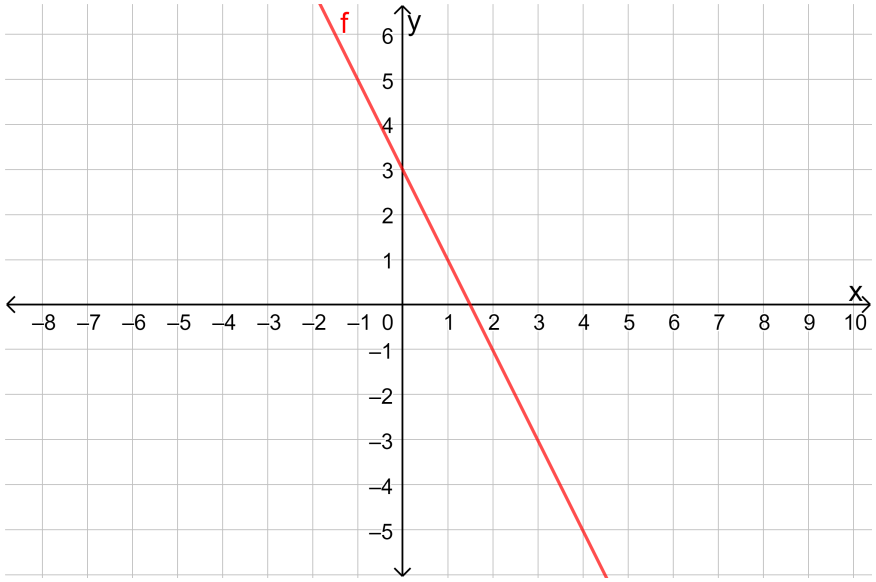
Na figura 5 encontra-se a representação dessas soluções no plano cartesiano. Já na figura 6 temos o gráfico da função afim $2x+y=3$, com $x,y\in\mathbb{R}$ o qual servirá para apontarmos algumas semelhanças e diferenças entre a função afim e a equação diofantina ambas dadas pela equação $2x+y=3$.

Figura 5 – Soluções da equação diofantina 2x+y=3



Fonte: Elaborado pelo autor

Figura 6 – Gráfico da função afim 2x+y=3

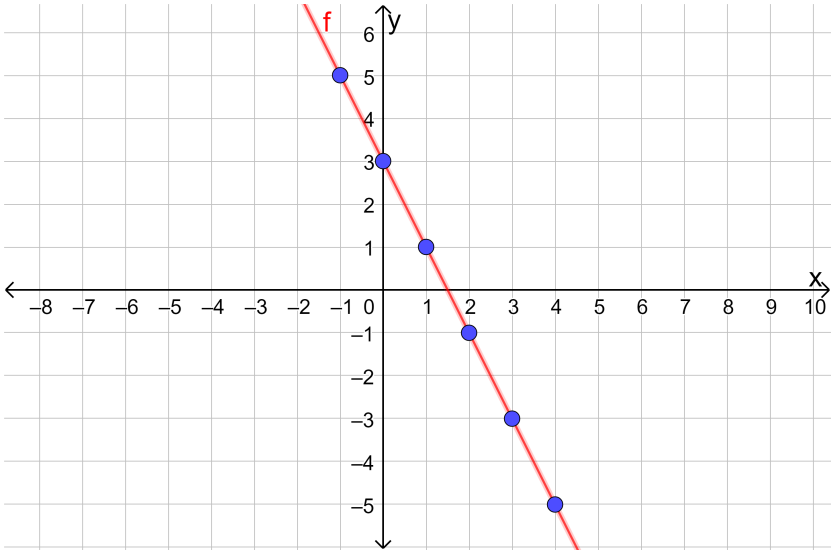


Fonte: Elaborado pelo autor

Analisando a figura 5, percebemos que as soluções da equação diofantina representam pontos do plano cartesiano onde as coordenadas x e y são números inteiros enquanto na figura 6 o gráfico da função f é representado por uma reta. Obviamente se conhecermos um ponto do gráfico das soluções da equação diofantina conseguiremos encontrar todas os outros pontos, pois cada coordenada x_n e y_n é uma solução particular da equação diofantina $2x+y=3$.

Sendo assim, as soluções de uma equação diofantina, caso existam, estão sobre o gráfico da função afim de mesma equação. Podemos ver esse fato na figura 7.

Figura 7 – Soluções da equação diofantina 2x+y=3 sobre o gráfico da função f. de mesma equação.



Fonte: Elaborado pelo autor

5.1.2 Relação entre Equações Diofantinas Lineares e Progressão Aritmética (P.A)

É comum nos depararmos com situações envolvendo grandezas que sofrem variações iguais em intervalos de tempos também iguais. Vejamos o exemplo a seguir.

Exemplo 5.3. Uma empresa produziu, em 2014, 1000 unidade de um certo produto. Quantas unidades produzirá, anualmente, de 2014 a 2019, se o aumento anual for de 200 unidades?

Podemos esquematizar a situação da seguinte forma:

- Produção de 2014: 1000
- Produção de 2015:
  (Produção de 2014) $+ 200 = 1000 + 200 = 1200$
- Produção de 2016:
  (Produção de 2015) $+ 200 = 1200 + 200 = 1400$
- Produção de 2017:
  (Produção de 2016) $+ 200 = 1400 + 200 = 1600$
- Produção de 2018:
  (Produção de 2017) $+ 200 = 1600 + 200 = 1800$
- Produção de 2019:
  (Produção de 2018) $+ 200 = 1800 + 200 = 2000$

Sendo assim, a produção anual é dada pela seguinte sequência[4] numérica:

$$(1000, 1200, 1400, 1600, 1800, 2000)$$

Observemos que no exemplo 5.3 que a diferença entre cada termo e o termo anterior é constante(200 unidades, nesta sequência).

Sequências desse tipo são chamadas de **Progressões Aritméticas (P.As)** estas são definidas formalmente a seguir.

Definição 5.2. Progressão Aritmética (P.A) é toda sequência de números na qual a diferença entre cada termo (a partir do segundo) e o termo anterior é constante. Essa diferença constante é chamada de **razão** da progressão e é representada pela letra r.

Genericamente escrevemos $(a_1, a_2, \ldots, a_n, \ldots)$ para representar a P.A, sendo cada a_n chamado de termo da P.A e $n \in \mathbb{N}$.

Pela definição 5.2 podemos calcular a razão r da seguinte forma:

$$r = a_2 - a_1 = \ldots = a_n - a_{n-1}$$

[4]Uma sequência de números reais é uma função definida em $\mathbb{N}$ e tomando valores no conjunto $\mathbb{R}$ dos números reais.

Em uma progressão aritmética $(a_1, a_2, \ldots, a_n, \ldots)$ de razão r, temos:

$$\begin{aligned} a_2 - a_1 &= r \\ a_3 - a_2 &= r \\ &\vdots \\ a_n - a_{n-1} &= r \end{aligned}$$

Somando as $n-1$ igualdades acima, temos:

$$(a_2 - a_1) + (a_3 - a_2) + \cdots + (a_n - a_{n-1}) = (n-1) \cdot r \Rightarrow a_n = a_1 + (n-1) \cdot r$$

A última igualdade acima nos dá o termo geral da P.A para um n natural qualquer. Escreveremos esta equação da seguinte forma:

$$a_n = a_1 - r + n \cdot r \tag{41}$$

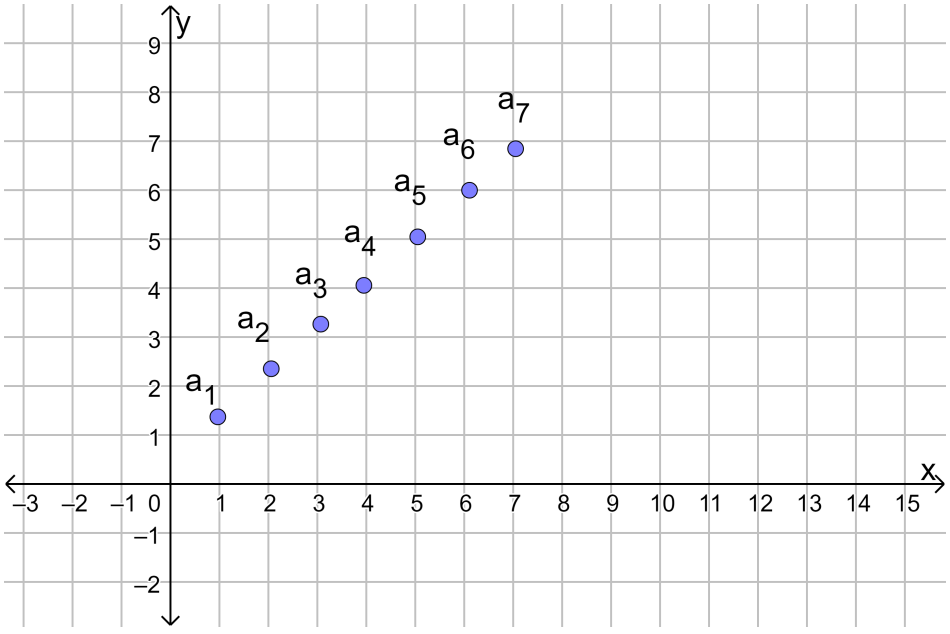
A fim de representar uma progressão aritmética no plano cartesiano podemos escrever $a_n = y$ e $n = x$, fazendo essas substituições na equação (41), temos:

$$y = a_1 - r - nx \Rightarrow -rx + y = a_1 - r$$

Com $x = n = \{1, 2, 3, \ldots\}$ e $y = a_n = \{a_1, a_2, a_3, \ldots\}$.

A figura 8 nos mostra como seria a representação da P.A $(a_1, a_2, a_3, \ldots)$ no plano cartesiano.

Figura 8 – Representação de uma P.A no plano cartesiano



Fonte: Elaborado pelo autor

A figura 8 tem uma certa semelhança com a figura 5, a qual representa a solução da equação diofantina linear $2x+y=3$, isso nos sugeri estabelecer uma relação entre P.As e Equações Diofantinas Lineares de Duas Variáveis.

A equação $-rx+y=a_1-r$ é uma equação diofantina, onde $a=-r$, $b=1$ e $c=a_1-r$. E como $(-r,1)=1 \mid (a_1-r)$ temos que a equação possui solução. A solução geral é dada por $x=x_0+t=1+t$ e $y=y_0+rt=a_1+rt$, com $t\in\mathbb{N}$, pois $x_0=1$ e $y_0=a_1$ é sempre uma solução particular desta equação.

Com isso podemos concluir que equações diofantinas da forma $ax+y=c$ onde $x\in\mathbb{N}$ e $t\in\mathbb{N}$, são também progressões aritméticas. Porém a recíproca não é verdadeira, ou seja, nem toda P.A de termo geral $a_n=a_1+(n-1)\cdot r$ gera uma equação diofantina. Podemos verificar isso facilmente tomando o primeiro termo da P.A um número decimal ou irracional.

Vejamos agora um exemplo de como podemos trabalhar a P.A juntamente com a equação diofantina linear, mostrando graficamente a correspondência entre os dois conteúdos.

Exemplo 5.4. Dada a P.A $(3,5,7,9,\ldots)$ encontre a equação diofantina correspondente a esta P.A, encontre a sua solução geral e construa o gráfico que representa esta sequência e a solução da equação diofantina correspondente simultaneamente.

Solução. Na P.A $(3,5,7,9,\ldots)$, temos $a_1=3$ e $r=a_2-a_1=5-3=2$, logo:

$$a_n=a_1+(n-1)\cdot r \Rightarrow a_n=3+(n-1)\cdot 2 \Rightarrow a_n=2n+1$$

Fazendo $a_n=y$ e $n=x$, na última equação acima, temos a equação diofantina correspondente a P.A

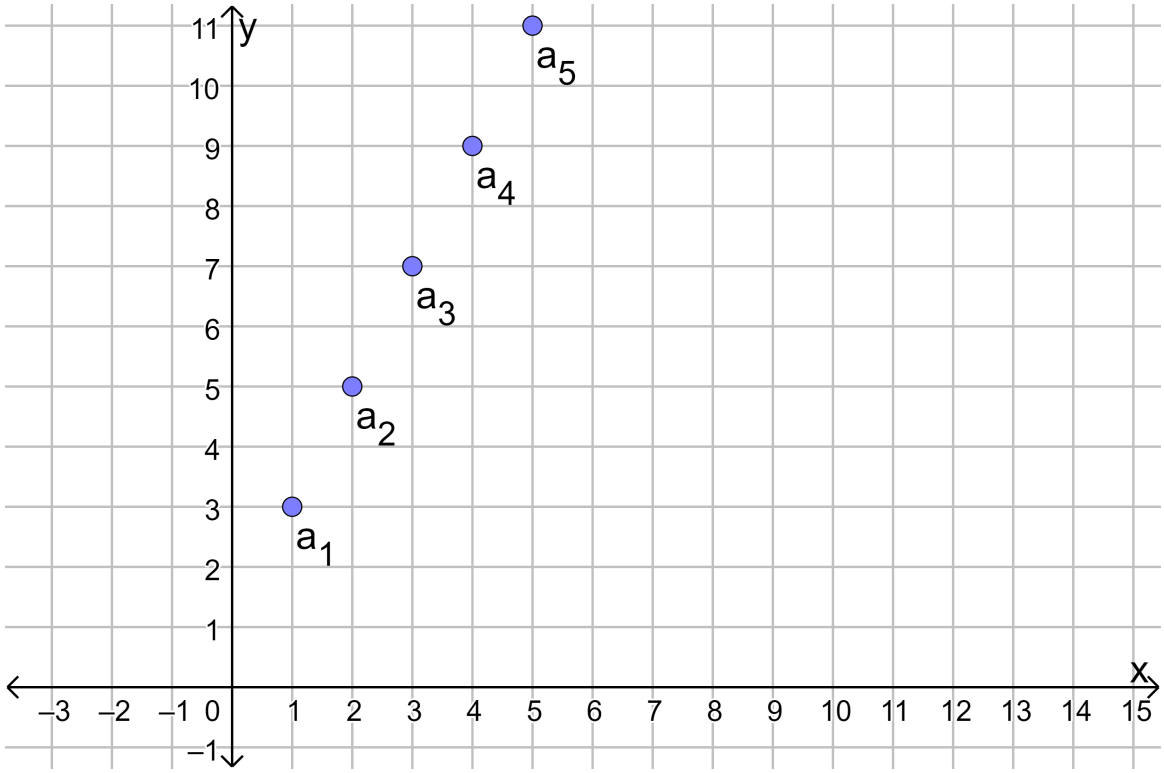
$$y=2x+1 \Rightarrow -2x+y=1$$

Como $x_0=1$ e $y_0=a_1$ sempre é uma solução particular de $-rx+y=a_1-r$, temos que $x_0=1$ e $y_0=a_1=3$ é uma solução particular de $-2x+y=1$ e sua solução geral será dada por:

$$\begin{aligned} x&=1+t, \quad \text{com} \quad t\in\mathbb{N} \\ y&=3+2t, \quad \text{com} \quad t\in\mathbb{N} \end{aligned}$$

O gráfico da figura 9 podemos ver os termos da P.A $(3,5,7,9,\ldots)$ e a solução da equação diofantina $-2x+y=1$.

Figura 9 – Gráfico da P.A $a_n = 2n+1$ e solução da equação diofantina $-2x+y=1$



Fonte: Elaborado pelo autor

5.2 PROBLEMAS ENVOLVENDO EQUAÇÕES DIOFANTINAS LINEARES

Como mencionamos anteriormente, muitos problemas são modelados pelas equações diofantinas lineares, problemas esses, que são cada vez mais cobrados em provas de olimpíadas de matemática tais como a OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), OBM (Olimpíada Brasileira de Matemática) entre outras, com base nesse pensamento resolveremos agora problemas modelados por essas equações, aplicando assim a teoria que desenvolvemos anteriormente.

Problema 5.2.1 (OBMEP 2018, primeira fase nível 3)**.** De quantas maneiras podemos trocar uma nota de R$ 20,00 por moedas de R$ 0,10 e R$ 0,25?
(A) 21 (B) 36 (C) 38 (D) 41 (E) 56

Solução (1)**.** Sejam X e Y as quantidades de moedas de R$ 0,10 e R$ 0,25 respectivamente. Logo o nosso problema fica reduzindo a determinar a quantidade de soluções da equação $0,10X+0,25Y=20$, onde $X,Y \in \mathbb{N}\cup\{0\}$. Multiplicando a equação $0,10X+0,25Y=20$ por 100, obtemos:

$$10X+25Y=2000$$

A equação acima possui solução já que $(10,25)=5 \mid 2000$, dividindo essa equação por $(10,25)=$

5, temos:

$$2X + 5Y = 400$$

Achemos agora uma solução particular para esta última equação. Usando o algoritmo de Euclides, temos:
$5 = 2 \cdot 2 + 1 \Rightarrow 1 = 2 \cdot (-2) + 5$
Multiplicando ambos os membros desta última igualdade por 400 e fazendo $-800 = -160 \cdot 5 + 0$, temos:
$400 = 2 \cdot (-800) + 5 \cdot 400 = 2 \cdot (-160 \cdot 5 + 0) + 5 \cdot 400 = -320 \cdot 5 + 2 \cdot 0 + 5 \cdot 400 = 2 \cdot 0 + 5 \cdot 80 = 400$
Onde $x_0 = 0$ e $y_0 = 80$ é a solução minimal de $2X + 5Y = 400$, logo sua solução geral é:

$$x = 5t \qquad \text{e} \qquad y = 80 - 2t \qquad \text{com} \qquad t \in \mathbb{N} \cup \{0\}$$

Como $x, y \in \mathbb{N} \cup \{0\}$ os únicos valores possíveis para t são, $0, 1, \ldots, 40$. logo temos 41 maneiras possíveis de trocar 20 reais por moedas de R$ 0,10 e R$ 0,25.

Solução (2)**.** Assim como na solução anterior, sejam X e Y as quantidades de moedas de R$ 0,10 e R$ 0,25 respectivamente, logo:

$$0,10X + 0,25Y = 20 \tag{42}$$

A solução do problema é o número de soluções inteiras e positivas da equação (42), a qual é do tipo diofantina linear, usando o corolário 3.5 para encontrar o máximo divisor comum generalizado de $0,10$ e $0,25$, temos:

$$mdcg(0,10; 0,25) \Rightarrow mdcg\left(\frac{10}{100}, \frac{25}{100}\right) \Rightarrow mdcg\left(\frac{1}{10}, \frac{1}{4}\right) = \frac{(1,1)}{[10,4]} = \frac{1}{20} = 0,05$$

Como:

$$0,25 = 2 \cdot 0,10 + 0,05 \Rightarrow 0,05 = 0,10 \cdot (-2) + 0,25$$

multiplicando esta última igualdade por 400, temos:

$$20 = 0,10 \cdot (-800) + 0,25 \cdot 400$$

Logo $x = -800$ e $y = 400$ é uma solução para a equação (42), pensando como na observação 4.1, temos:

$$x = -800 + \frac{0,25}{0,05}t \Rightarrow x = -800 + 5t, \quad \text{com} \quad t \in \mathbb{Z}$$

$$y = 400 - \frac{0,10}{0,05}t \Rightarrow y = 400 - 2t, \quad \text{com} \quad t \in \mathbb{Z}$$

Como devemos ter x e y maiores ou iguais a zero, temos:

$$x \geq 0 \Rightarrow -800+5t \geq 0 \Rightarrow 5t \geq 800 \Rightarrow t \geq 160$$
$$y \geq 0 \Rightarrow 400-2t \geq 0 \Rightarrow 2t \geq 400 \Rightarrow t \leq 200$$

Ou seja, t só pode assumir os valores $160, 161, \ldots, 200$. Logo temos 41 maneiras possíveis de trocar 20 reais por moedas de R$ 0,10 e R$ 0,25.

Problema 5.2.2 (OCM XVIII 1989, nível fundamental)**.** Encontre duas frações com numeradores inteiros positivos e denominadores 7 e 9 de tal modo que a soma delas seja $\frac{73}{63}$.

Solução. Sejam X e Y os numeradores de 7 e 9 respectivamente, pelo enunciado do problema, temos:

$$\frac{X}{7}+\frac{Y}{9}=\frac{73}{63}$$

Multiplicando cada membro da equação acima por 63, temos:

$$63\cdot\left(\frac{X}{7}+\frac{Y}{9}\right)=63\cdot\frac{73}{63}\Rightarrow 9X+7Y=73$$

De onde o problema fica reduzido a encontrar valores inteiros positivos X e Y satisfazendo a equação diofantina acima. Como $(9,7)=1 \mid 73$ a equação possui solução. Usando o algoritmo de Euclides, temos:

$$\begin{array}{l} 9=7\cdot 1+2 \\ 7=2\cdot 3+1 \end{array} \Rightarrow \begin{array}{l} 2=9-7\cdot 1 \\ 1=7-2\cdot 3 \end{array}$$

De onde temos que:

$1=7-3\cdot 2=7-3\cdot(9-7\cdot 1)=7-3\cdot 9+7\cdot 3\Rightarrow 1=9\cdot(-3)+7\cdot 4$

Multiplicando essa última igualdade por 73 e fazendo $-219=7\cdot(-32)+5$, temos:

$$\begin{aligned} 73 &= 9\cdot(-219)+7\cdot 292 \\ &= 9\cdot(7\cdot(-32)+5)+7\cdot 292 \\ &= 7\cdot(-288)+9\cdot 5+7\cdot 292 \\ &= 9\cdot 5+7\cdot 4 \end{aligned}$$

Logo, $x_0=5$ e $y_0=4$ é a solução minimal de $9X+7Y=73$ e sua solução geral é:

$$x=5+7t,\ y=4-9t \quad \text{com} \quad t\in\mathbb{N}\cup\{0\}$$

Onde $t=0$ é o único valor de t que satisfaz o nosso problema, para $t=0$ temos respectivamente x e y iguais a 5 e 4, logo as frações procuradas são $\frac{5}{7}$ e $\frac{4}{9}$.

Problema 5.2.3 (OBMEP 2017, primeira fase nível 3)**.** Somando 1 a um certo número natural, obtemos um múltiplo de 11. Subtraindo 1 desse mesmo número, obtemos um múltiplo de 8. Qual é o resto da divisão do quadrado desse número por 88?

(A) 0 (B) 1 (C) 8 (D) 10 (E) 80

Solução. Seja n o número natural em questão, X e Y inteiros, segundo o nosso problema devemos ter:

$$n+1 = 11X \tag{43}$$

$$n-1 = 8Y \tag{44}$$

Das equações (43) e (44), temos:

$$11X - 1 = 8Y + 1 \Rightarrow 11X - 8Y = 2$$

Onde a última equação acima é uma equação diofantina e como $(11,-8) = (11,8) = 1 \mid 2$ a mesma possui solução. Usando o algoritmo de Euclides, temos:

$$\begin{array}{lll} 11 = 8\cdot 1 + 3 & & 3 = 11 - 8\cdot 1 \\ 8 = 3\cdot 2 + 2 & \Rightarrow & 2 = 8 - 3\cdot 2 \\ 3 = 2\cdot 1 + 1 & & 1 = 3 - 2\cdot 1 \end{array}$$

De onde temos:

$1 = 3 - 2\cdot 1 = 3 - (8 - 3\cdot 2)\cdot 1 = 3 - 8 + 3\cdot 2 = -8 + 3\cdot 3 = -8 + 3\cdot(11 - 8\cdot 1) = -8 + 3\cdot 11 - 8\cdot 3 \Rightarrow 1 = 11\cdot 3 - 8\cdot 4$

Multiplicando esta última igualdade por 2, temos:

$$2 = 11\cdot 6 - 8\cdot 8$$

De onde segue que $x_0 = 6$ e $y_0 = 8$ é uma solução particular da equação $11X - 8Y = 2$, consequentemente, temos:

$$x = 6 - 8t, \quad y = 8 - 11t \quad \text{com} \quad t \in \mathbb{Z}$$

Como solução geral. Tomando $t = 0$ temos $n = 11\cdot 6 - 1 = 65$, e:

$$65^2 = 4225 = 88\cdot 48 + 1$$

O que mostra que o resto da divisão de n por 88 é 1.

Da mesma forma tomando $t = -1$, pois $n \in \mathbb{N}$, temos outro candidato a n e este é igual a $n = 11\cdot 14 - 1 = 153$. Logo:

$$153^2 = 23409 = 88\cdot 266 + 1$$

O que mostra novamente que n deixa resto 1 na divisão por 88.

De um modo mais geral, tomando $n = 11\cdot(66 - 8t) - 1 = 65 - 88t$ com $t = \{0,-1,-2,\ldots\}$,

temos:

$$\begin{aligned} n^2 = (65-88t)^2 &= 4225 - 2\cdot 66\cdot 88t + 88^2t^2 \\ &= 1 + 88\cdot 48 - 2\cdot 66\cdot 88t + 88^2t^2 \\ &= 1 + (48 - 2\cdot 66\cdot t + 88t^2)\cdot 88 \end{aligned}$$

De onde concluímos que existem infinitos candidatos a n e estes sempre deixam resto 1 na divisão por 88.

Problema 5.2.4 (OBM 2003, primeira fase nível 2)**.** Você possui muitos palitos com 6cm e 7cm de comprimento. Para fazer uma fila de palitos com comprimento total de 2 metros, o número mínimo de palitos que você precisa utilizar é:
(A) 29 (B) 30 (C) 31 (D) 32 (E) 33

Solução (1)**.** Sejam X e Y as quantidades de palitos com 6cm e 7cm de comprimento respectivamente. Como 2m correspondem a 200cm, temos:

$$6X + 7Y = 200$$

A equação acima é uma equação diofantina e a mesma possui solução já que $(7,6) = 1 \mid 200$. Usando o algoritmo de Euclides para encontrar uma solução particular, temos:

$$7 = 6\cdot 1 + 1 \Rightarrow 1 = 6\cdot(-1) + 7$$

Multiplicando esta última igualdade acima por 200 e fazendo $-200 = 7\cdot(-29) + 3$, temos:
$200 = 6\cdot(-200) + 7\cdot 200 = 6\cdot(7\cdot(-29)+3) + 7\cdot 200 = 7\cdot(-174) + 6\cdot 3 + 7\cdot 200 \Rightarrow 200 = 6\cdot 3 + 7\cdot 26$
De onde temos que $x_0 = 3$ e $y_0 = 26$ é uma solução particular de $6X + 7Y = 200$, logo sua solução geral é dada por:

$$x = 3 + 7t, \quad y = 26 - 6t \quad \text{com} \quad t \in \mathbb{N}\cup\{0\}$$

Logo os possíveis valores para x e y são:

t	x	y
0	3	26
1	10	20
2	17	14
3	24	8
4	31	2

Como queremos $x+y$ mínimo, devemos ter $x = 3$ e $y = 26$, logo o número mínimo de palitos é 29.

Solução (2)**.** Assim como na solução anterior, Sejam X e Y as quantidades de palitos com 6cm e 7cm de comprimento respectivamente. Como 6cm é igual a 0,06m e 7cm é igual a 0,07m, temos:

$$0,06X + 0,07Y = 2 \tag{45}$$

A equação acima é do tipo diofantina linear. Usando o corolário 3.5 para encontrar o *mdcg* entre $0,06$ e $0,07$, temos:

$$mdcg(0,06;0,07) \Rightarrow mdcg\left(\frac{6}{100}, \frac{7}{100}\right) \Rightarrow \frac{(6,7)}{[100,100]} = \frac{1}{100} = 0,01$$

Como:

$$0,07 = 0,06 \cdot 1 + 0,01 \Rightarrow 0,01 = 0,06 \cdot (-1) + 0,07$$

Multiplicando essa última igualdade por 200, temos:

$$2 = 0,06 \cdot (-200) + 0,07 \cdot 200$$

Logo $x = -200$ e $y = 200$ é uma solução para a equação (45), pensando agora como na observação 4.1, temos:

$$x = -200 + \frac{0,07}{0,01}t \Rightarrow x = -200 + 7t, \quad \text{com} \quad t \in \mathbb{Z}$$

$$y = 200 - \frac{0,06}{0,01}t \Rightarrow y = 200 - 6t, \quad \text{com} \quad t \in \mathbb{Z}$$

Como x e y devem ser inteiros positivos, temos:

$$x \geq 0 \Rightarrow -200 + 7t \geq 0 \Rightarrow 7t \geq 200 \Rightarrow t \geq \frac{200}{200} \Rightarrow t = 29$$
$$y \geq 0 \Rightarrow 200 - 6t \geq 0 \Rightarrow 6t \leq 200 \Rightarrow t \leq \frac{200}{6} \Rightarrow t = 33$$

Logo, $t = \{29,30,31,32,33\}$ para esses valores encontramos $x = \{3,10,17,24,31\}$ e $y = \{26,20,14,8,2\}$. Como queremos $x + y$ mínimo, devemos ter $x = 3$ e $y = 26$, ou seja, o número mínimo de palitos é 29.

Problema 5.2.5 (OBM 1999, primeira fase nível 2)**.** Contando-se os alunos de uma classe de 4 em 4 sobram 2 e contando-se de 5 em 5 sobram 1. Sabendo-se que 15 alunos são meninas e que nesta classe o número de meninas é maior que o número de meninos, o número de meninos é igual a:
(A) 7 (B) 8 (C) 9 (D) 10 (E) 11

Solução. Seja n o número de alunos e X e Y inteiros quaisquer, pelo enunciado do problema, temos:

$$n = 4Y + 2 \tag{46}$$

$$n = 5X + 1 \tag{47}$$

Das equações (46) e (47), temos:

$$5X + 1 = 4Y + 2 \Rightarrow 5X - 4Y = 1$$

A equação acima possui solução uma vez que $(5,-4) = (5,4) = 1$ e $1 \mid 1$. É fácil ver que $x_0 = 1$ e $y_0 = 1$ é uma solução particular de $5X - 4Y = 1$. Logo, sua solução geral é dada por:

$$x = 1 - 4t \quad \text{e} \quad y = 1 - 5t \quad \text{com} \quad t \in \mathbb{Z}$$

Com $t = \{0,-1,-2,-3,\ldots\}$, uma vez que n é um inteiro positivo.
Abaixo temos alguns possíveis valores para n.

t	x	y	n
0	1	1	6
-1	5	6	26
-2	9	11	46
⋮	⋮	⋮	⋮

O único valor de n que satisfaz o nosso problema é $n = 26$, uma vez que o número de meninas é maior que o número de meninos, logo, devemos ter $26 - 15 = 11$ meninos.

Problema 5.2.6 (OBM 1998, primeira fase nível 2)**.** Um fabricante de brinquedos embala bolas de ping-pong em dois tipos de caixas. Num dos tipos ele coloca 10 bolas e no outro ele coloca 24 bolas. Num certo dia foram embaladas 198 bolas e usadas mais de 10 caixas. Quantas caixas foram feitas nesse dia?
(A) 14 (B) 16 (C) 15 (D) 17 (E) 11

Solução. Sejam X e Y os tipos de caixas que são colocadas 10 e 24 bolas respectivamente, logo:

$$10X + 24Y = 198$$

A equação acima se trata de uma equação diofantina e a mesma possui solução, pois $(24,10) = 2$ e $2 \mid 198$. Dividindo $10X + 24Y = 198$ por $2 = (24,10)$, temos:

$$5X + 12Y = 99$$

Usando o algoritmo de Euclides para encontrar uma solução particular para esta última equação acima, temos:

$$\begin{array}{l} 12 = 5 \cdot 2 + 2 \\ 5 = 2 \cdot 2 + 1 \end{array} \Rightarrow \begin{array}{l} 2 = 12 - 5 \cdot 2 \\ 1 = 5 - 2 \cdot 2 \end{array}$$

De onde temos:

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 5 \cdot 2) = 5 - 2 \cdot 12 + 5 \cdot 4 \Rightarrow 1 = 5 \cdot 5 + 12 \cdot (-2)$$

Multiplicando esta última igualdade por 99 e fazendo $495 = 12 \cdot 41 + 3$, obtemos:
$99 = 5 \cdot 495 + 12 \cdot (-198)$
$99 = 5 \cdot (12 \cdot 41 + 3) + 12 \cdot (-198)$
$99 = 12 \cdot 205 + 5 \cdot 3 + 12 \cdot (-198)$
$99 = 5 \cdot 3 + 12 \cdot 7$
Logo, a solução geral de $5X + 12Y = 99$ é:

$$x = 3 + 12t \quad \text{e} \quad y = 7 - 5t \quad \text{com} \quad t \in \mathbb{N} \cup \{0\}$$

De onde concluímos que o único valor de t que satisfaz o nosso problema é $t = 1$, pois devemos ter $x + y > 10$, logo:
$x = 3 + 12 \cdot 1 = 15$
$y = 7 - 5 \cdot 1 = 2$
De onde temos que o número de caixas feitas nesse dia foram $x + y = 15 + 2 = 17$.

Problema 5.2.7 (OBM 1999, primeira fase nível 2)**.** Quantos são os pares de inteiros positivos x e y que satisfaz a equação $2x + 3y = 101$.
(A) 13 (B) 14 (C) 15 (D) 16 (E) 17

Solução. Observemos primeiramente que $(2,3) = 1$ e $1 \mid 101$, logo $2x + 3y = 101$ admite soluções inteiras.Usando o algoritmo de Euclides para escrever:
$3 = 2 \cdot 1 + 1 \Rightarrow 1 = 2 \cdot (-2) + 3$
Agora multiplicando esta última igualdade por 101 e fazendo $-101 = 3 \cdot (-34) + 1$, temos:
$101 = 2 \cdot (-101) + 3 \cdot 101$
$101 = 2 \cdot (3 \cdot (-34) + 1) + 3 \cdot 101$
$101 = 3 \cdot (-68) + 2 \cdot 1 + 3 \cdot 101$
$101 = 2 \cdot 1 + 3 \cdot 33$.
De onde temos $x_0 = 1$ e $y_0 = 33$ uma solução particular de $2x + 3y = 101$. Logo sua solução geral é dada por:

$$x = 1 + 3t \quad \text{e} \quad y = 33 - 2t \quad \text{com} \quad t \in \mathbb{N} \cup \{0\}$$

Como x e y são inteiros positivos, t só pode assumir valores ser $0, 1, 2, \ldots, 16$, logo o número de pares x e y inteiros positivos que satisfazem nosso problema são 17.

Problema 5.2.8 (OBM 2002, primeira fase nível 2)**.** O lava-rápido "Lave Bem" faz uma promoção:

Lavagem simples R$5,00
Lavagem completa R$7,00

No dia da promoção, o faturamento do lava-rápido foi de R$ 176,00. Nesse dia, qual o menor número possível de clientes que foram atendidos?
(A) 23 (B) 44 (C) 26 (D) 28 (E) 30

Solução. Sejam X e Y os números de clientes que escolheram a lavagem simples e completa

respectivamente. X e Y são inteiros positivos. Pelo enunciado do problema devemos ter:

$$5X + 7Y = 176$$

A equação acima possui solução, uma vez que $(5,7) = 1 \mid 176$. Pelo algoritmo de Euclides, temos:
$7 = 5 \cdot 1 + 2$
$5 = 2 \cdot 2 + 1$
O que é equivalente a:
$2 = 7 - 5 \cdot 1$
$1 = 5 - 2 \cdot 2$
De onde temos:
$1 = 5 - 2 \cdot (7 - 5 \cdot 1) = 5 - 2 \cdot 7 + 5 \cdot 2 \Rightarrow 1 = 5 \cdot 3 + 7 \cdot (-2)$
Multiplicando esta última igualdade por 176 e fazendo $528 = 7 \cdot 75 + 3$, temos:
$176 = 5 \cdot 528 + 7 \cdot (-352)$
$176 = 5 \cdot (7 \cdot 75 + 3) + 7 \cdot (-352)$
$176 = 7 \cdot 375 + 5 \cdot 3 + 7 \cdot (-352)$
$176 = 5 \cdot 3 + 7 \cdot 23$.
Logo, $x_0 = 3$ e $y_0 = 23$ é uma solução particular de $5X + 7Y = 176$ e sua solução geral é:

$$x = 3 + 7t \quad \text{e} \quad y = 23 - 5t \quad \text{com} \quad t \in \mathbb{N} \cup \{0\}$$

t só pode ser $\{0,1,2,3,4\}$ de onde, temos $x = \{3,10,17,24,31\}$ e $y = \{23,18,13,8,3\}$ assim concluímos que o número mínimo de clientes é 26, pois isso só acontece quando temos $x = 3$ e $y = 23$.

6 CONSIDERAÇÕES FINAIS

Pretende-se através da leitura e o estudo dessa pesquisa, motivar o leitor a ter uma nova perspectiva quanto a importância desse conteúdo, levando-o tanto a realização de uma explanação rápida como ter um plano de ação, o qual, pode ser usado como ferramenta de trabalho do professor que almeja um índice maior de aprovação de seu corpo discente, em provas externas por meio de uma aplicação no cronograma de conteúdos.

As competências e habilidades que são exigidas no Ensino Básico são decisivas no apuramento do desenvolvimento do educando, quando se trata da maneira a qual elas serão modeladas em sala levando o aluno ao aprimoramento dessas exigências curriculares. O estudo dessas equações aqui apresentadas e o perfil, o qual, se propõe na organização sequenciada de como trabalhá-las didaticamente, é perceptível que a proposta de as introduzir nas exposições didáticas, iria interferir de forma satisfatória no crescimento de novas perspectivas na avaliação das competências e habilidades do aluno.

Tendo como centro, a praticidade na exposição do conteúdo desse trabalho, o leitor terá mais autonomia em flexionar o conhecimento adquirido, formando sua própria metodologia e colocando-a em prática.

Os pilares de organização dessa pesquisa consistem em uma sequência de fatos que foram desde ao embasamento histórico e teórico até uma resolução diversificada de problemas, os quais, possuidores de referências de provas de elaboração apreciável e de grande valor não só para o sistema escolar, mas em particular no vínculo educacional professor/aluno.

REFERÊNCIAS

ANDREESCU, T; ANDRICA, D; CUCUREZEANU, I. **An Introduction Dorin Andrica to Diophantine Equations**: A Problem-Based Approach. New York: Birkhäuser, 2010. Disponível em: <https://www.academia.edu/17556966/An_Introduction_to_Diophantine_Equations>. Acesso em: 15 out. 2018.

ALENCAR FILHO, E. **Teoria Elementar dos números**. São Paulo: NOBEL, 1981.

BOYER, C. B. **História da Matemática**; tradução Elza F. Gomide. 2. ed. São Paulo: EDGARD BLUCHERLTDA, 1996.

CARNEIRO, E.; CAMPOS, O.; MAX, P. **Olimpíadas Cearenses de Matemática**: Nível Fundamental. Rio de Janeiro: SBM, 2014.

DARELA, E.; CARDOS, M.; ROSA, R. C. **História da Matemática**: Livro didático. 3. ed. Palhaça: Unisulvirtual, 2011. Disponível em: <https://docplayer.com.br/83186238-Historia-da-matematica.html >. Acesso em : 11 nov. 2018.

HEFEZ, A. **Aritmética**.2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016.

LIMA, E. L. **Curso de Análise**. 12. ed. Rio de Janeiro: IMPA, 2008.

LIMA, Elon Lages et al. **A Matemática do Ensino Médio**. 10. ed. Rio de Janeiro: IMPA, 2012.

MUNIZ NETO, A. C. **Tópicos de matemática elementar**: teoria dos números. 2. ed. Rio de Janeiro: SBM, 2013. (Coleção do Professor de Matemática).

OLIMPÍADA BRASILEIRA DE MATEMÁTICA. **Provas e Gabaritos**. Disponível em: <https://www.obm.org.br/como-se-preparar/provas-e-gabaritos/>. Acesso em: 28 out. 2018.

OLIMPÍADA BRASILEIRA DE MATEMÁTICA DAS ESCOLAS PÚBLICAS. **Provas e soluções**. Disponível em: <http://www.obmep.org.br/provas.htm>. Acesso em: 28 out. 2018.

OLIVEIRA, K. I. M.; FERNANDEZ, A. J. C. **Iniciação à Matemática**: um curso com problemas e soluções. Rio de Janeiro: SBM, 2010.

SAVÓIS, Josias Neubert; FREITAS, Daiane. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. **Ciência e Natura**, [s.l.], v. 37, p.47-57, 7 ago. 2015. Disponível em: <http://www.redalyc.org/html/4675/467547643005/index.html>. Acesso em: 20 fev. 2018.