Ciência e Natura, Santa Maria, v. 37 Ed. Especial PROFMAT, 2015, p. 532–554
Revista do Centro de Ciências Naturais e Exatas - UFSM
ISSN impressa: 0100-8307 ISSN on-line: 2179-460X

CIÊNCIA e NATURA 35 anos

Equações Diofantinas: um projeto para a sala de aula e o uso do Geogebra

Diophantine Equations: a project for the classroom and using Geogebra

Alexandre Hungaro Vansan[1]

[1]Mestre em Matemática pela Universidade Estadual de Maringá, Brasil(2014)
Professor do Secretaria de Educação do Estado do Paraná , Brasil
alexandrevansan@hotmail.com

Resumo

O estudo de Teoria dos Números visa aqui neste artigo estudar algumas propriedades dos números inteiros, como múltiplos e divisores, enfatizando questões ligadas à divisibilidade, a qual será de grande importância para os estudos das Equações Diofantinas, que por sua vez fornecerão aplicações para o uso do software Geogebra. As Equações Diofantinas são equações algébricas que apresentam solução no conjunto dos números inteiros, onde neste trabalho vamos discutir as Equações Diofantinas Lineares com duas incógnitas da forma, $ax + by = c$ com a, b, c números Inteiros. Em que elas são aplicadas como caminho alternativo para que o aluno encontre soluções de problemas que ele se depara durante sua vida escolar. Este trabalho destina-se a formação complementar de professores que estão na docência no Ensino Fundamental e Médio, onde poderá encontrar sugestões de atividades que poderá aplicar em sala de aula, ou até mesmo incluir em seu plano de aula as Equações Diofantinas.

Palavras-chaves: Equações Diofantinas. Teoria dos Números. Múltiplos. Geogebra. Plano de Aula

Abstract

The study of Number Theory here in this article aims to study some properties of integer multiples or divisors, emphasizing issues related to divisibility, which will be of great importance for the study of Diophantine equations, which in turn will provide for applications using Geogebra software. The Diophantine equations are algebraic equations that show the solution set of integers, which in this paper we will discuss the Linear Diophantine equations with two unknowns of the form $ax + by = c$ with a, b, c integers. In which they are applied as an alternative way for students to find solutions to problems he faced during his school life. This work is intended to further training of teachers who are teaching in the elementary and high school, where you can find suggestions for activities that you can apply in the classroom, or even include in your lesson plan Diophantine equations, since here he will find a suggestion of teaching work plan to include in their classes.

Keywords: Diophantine Equations. Theory of Numbers, Multiples. Geogebra. Lesson Plan

submissão: 2014-06-29 Aceito: 2014-12-17

1 Introdução

O currículo de Matemática do Ensino Fundamental apresenta tópicos da Teoria Elementar dos Números estudando os números naturais e inteiros: propriedades e operações básicas, decomposição em fatores primos, algoritmo da divisão, estudo da divisibilidade, múltiplos, divisores, máximo divisor comum, mínimo múltiplo comum, Algoritmo de Euclides, números primos, critérios de divisibilidade e o Teorema Fundamental da Aritmética. Porém, depois que o aluno estuda esses tópicos, a não ser com alguma pequena aplicação em operações, ele não volta a estudá-los de forma mais profunda e muito menos aplica algum desses conhecimentos para resolver problemas que ele enfrenta no restante do Ensino Fundamental ou no Ensino Médio. Muitas vezes o próprio professor deixa de lado esses assuntos, dando preferência ao que está rigorosamente descrito no currículo, deixando de lado a oportunidade de aplicar a Teoria dos Números. No ciclo básico, a aprendizagem da Matemática pode ser colocada na forma de um projeto de ensino, desde que dê possibilidade ao aluno de se expressar e argumentar em diferentes linguagens (natural, numérica, algébrica, gráfica), enfrentando situações-problema e decidindo caminhos que extrapolem o que é original, examinando e aplicando outras possibilidades nos contextos e outros pontos de vista sobre o que esta estudando, papeis ressaltados na proposta do ENEM, conforme BRASIL (2009).

Como sabemos, a Teoria dos Números é uma área que trata de problemas, que facilitam o pensamento dos alunos, para desenvolver estratégias de resolução, sem que haja a necessidade de uso dos algoritmos. Na Teoria dos Números podemos trabalhar de modo complementar com a Álgebra, onde muitos problemas podem ser resolvidos de modo a utilizar as duas áreas em conjunto. Alguns autores Campbell e Zazkis (2002) afirmam que a Teoria dos Números não estuda apenas tópicos básicos e usuais (números naturais e inteiros, divisores, múltiplos, mínimo múltiplo comum e máximo divisor comum), como a maioria dos alunos pensa e aprende, mas também incluem tópicos algébricos. A grande maioria dos problemas de Teoria dos Números não envolve a aplicação direta de algoritmos, mas precisam de raciocínio, interpretação e habilidades de manipular os dados para desenvolver conjecturas e encontrar soluções.

No Ensino Fundamental há uma predominação do estudo dos números naturais, inteiros e racionais não negativos, e aos poucos isso vai se transformando num estudo dos números reais, deixando uma separação entre o que é discreto e o que é contínuo. Alguns estudos feitos com números reais, que poderiam ser usados no conjunto dos números inteiros, não são, na maioria das vezes, abordados. As Equações Diofantinas,

por exemplo, não são abordadas como tema curricular, mas em algumas situações podem ser contextualizadas em problemas do Ensino Básico, fazendo uma ligação entre o que é Teoria dos Números e Álgebra. Para ajudar o professor a entender que essa abordagem poderá ser feita durante vários momentos vida escolar do aluno, é que vamos introduzir alguns conceitos referentes à Teoria Elementar dos Números e buscar aplicações em problemas de sala de aula.

O pioneirismo de Diofante se dá na criação de formas de expressão, passando de um estágio, anterior a ele, que saia de uma despreocupação com a estrutura das teorias, para um nível mais preocupado com essa estrutura, em que Diofante passou a utilizar símbolos nessa nova fórmula. Um exemplo são os problemas envolvendo geometria, que nas suas soluções apresenta uma manipulação algébrica, sem usar figuras para isso.

Segundo Boyer (1974) a Matemática grega não tinha um desenvolvimento elevado, pois após o período de grandes conquistas do século III A.C., os gregos tiveram um período de declínio que foi interrompido por Ptolomeu, e que continuou nesse declínio até os anos de 250 a 350 D.C. aproximadamente. Nesse período encontramos Diofante de Alexandria, que em sua obra mostra-nos uma quebra da tradição clássica grega, em que seus textos não se assemelhavam em nada com os textos de outros matemáticos. Encontramos poucos escritos da vida de Diofante, além de uma coleção de problemas chamada Antologia Grega, que foram escritos entre os Séculos cinco e seis D.C.

As referências históricas Boyer (1974) e Katz (2010) desconhecem a data do seu nascimento, a data de sua chegada a Alexandria, ou ainda seu país de nascimento. Algumas aproximações para uma provável data foi feita através da leitura dos seus escritos, onde ele cita Hipsicles (240-170 A.C.), e também encontramos outros indícios pesquisando os trabalhos de Theon de Alexandria (335 .405 D.C.), onde ele cita uma das definições de Diofante. Assim, determinamos uma data, não muito precisa, no período de 500 anos entre Hipsicles e Theon de Alexandria, para uma possível época da data dos escritos de Diofante. Estudando Rocque e Pitombeira (1991), percebemos que as obras de Diofante não são a base da álgebra elementar moderna, e também não trazem nada de semelhante à álgebra geométrica de Euclides, e Diofante não seguia a tradição grega para os textos matemáticos. A maior de suas obras que conhecemos é a Arithmética, uma coleção de treze livros contendo mais de cem problemas algébricos e suas soluções numéricas (equações algébricas) e teoria dos números. Diofante também escreveu outras duas obras, uma sobre Números Poligonais, que restou apenas um fragmento, e Porismas, que se perdeu pelo tempo. Em Arithimética, Diofante inicia o uso de símbolos para facilitar a escrita e os cálculos matemáticos. Segundo Katz (2010), os símbolos criados por ele (Diofante) fizeram com

que as expressões escritas somente com palavras, pudessem ser representadas com abreviações ou símbolos. Como Diofante viveu numa época muito tumultuada, presenciando, por exemplo, a queda do Império Romano, a Matemática teve seu desenvolvimento interrompido por causa do clima de guerra que se criou e pela destruição de muitas bibliotecas, fazendo com que esses símbolos de Diofante não saíssem da fase inicial. As coleções de problemas com equações não determinadas fizeram a fama de Diofante crescer muito, e como esses problemas envolvem números inteiros, eles são conhecidos por "Equações Diofantinas". Diofante tinha um maior interesse nas equações de ordem superior, mas, em homenagem a ele, as equações lineares receberam também o nome de Diofantinas (Hefez (2005)). Ainda em Arithmética encontramos uma coleção de problemas, solucionados por meio de exemplos numéricos, embora sendo possível a generalização do método. Diofante não desenvolve proposições, teoremas ou corolários, nem se esforça para encontrar todas as soluções possíveis, não faz distinção entre problemas com resultados determinados e indeterminados, e quando as soluções são infinitas, ele dá uma única solução. Há um uso grande de abreviações para potências de números, para relações e operações. Lins e Gimenez (2005) dizem que Diofante resolvia problemas envolvendo vários números desconhecidos expressando todas as quantidades desconhecidas, quando possível, em termos de apenas uma, sem recorrer à teorização.

2 Tópicos de Teoria dos Números

Nesta seção introduziremos as teorias que serão de grande importância para o professor que irá aplicar o projeto em sala de aula. Iniciaremos com conceitos que envolvem divisibilidade, máximo divisor comum, algoritmo de Euclides, números primos e mínimo múltiplo comum. Esses conceitos serão fundamentais para provar as teorias referentes às Equações Diofantinas. Todas essas definições, proposições e teoremas tiveram como referências Hefez (2005), Filho (1985), Frohlich (1994), Martinez (2011), Lins (2005) e Santos (2012).

Como a divisão de um número inteiro por outro nem sempre é possível, vamos expressar essa possibilidade por meio da divisibilidade. Veremos mais a frente que, quando não existir essa relação de divisibilidade entre dois números inteiros, ainda assim, será possível efetuar uma divisão, chamada de Divisão Euclidiana (aqui neste trabalho usaremos o nome Algoritmo de Euclides).

Definição 1 (Princípio da Boa Ordem). Todo conjunto não vazio de inteiros positivos possui um elemento mínimo.

Axioma 1 (Princípio da Indução Finita). Seja A um subconjunto dos

inteiros positivos. Se A possui as seguintes propriedades:
(i) $1 \in A$
(ii) $k + 1 \in A$ sempre que $k \in A$,
então A contém todos os inteiros positivos.

Definição 2 (Divisor). Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a|b$, quando existir c inteiro tal que $b = c \cdot a$. Neste caso, diremos também que a é um divisor de b, ou ainda, que b é um múltiplo de a. A negação dessa sentença significa que não existe nenhum número inteiro c tal que $b = c \cdot a$, a qual denotamos por $a \nmid b$.

Exemplo 1. Temos que 14|0, 3|9, 7|35, $12 \nmid 10$ e $4 \nmid 9$.
Temos que $0 = 0 \cdot 14$, $9 = 3 \cdot 3$ e $35 = 5 \cdot 7$. Mas não existe $c_1, c_2 \in \mathbb{Z}$ tal que $10 = c_1 \cdot 12$ e $9 = c_2 \cdot 4$.

Proposição 1. (Propriedade Arquimediana) Se $a, b \in \mathbb{Z}$ com $b \neq 0$, então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração. De fato, como $|b| > 0$, temos que $|b| \geq 1$, (pois o conjunto $\{x \in \mathbb{Z}; 0 < x < 1\}$ é vazio), logo $(|a| + 1)|b| \geq |a| + 1 > |a| \geq a$.
Escrevendo $n = |a| + 1$ se $b > 0$, ou escrevendo $n = -(|a| + 1)\ se\ b < 0$, temos o resultado desejado.

■

Teorema 1. (Algoritmo de Euclides) Sejam a e b dois números inteiros com a≠0. Existem e são únicos dois números inteiros q e r tais que b=a·q+r com 0≤r<|a|.

Demonstração. Considere o conjunto $S = \{x = b - ay, y \in \mathbb{Z}\} \cap \mathbb{N}$.
Existência: Pela Propriedade Arquimediana, escrevemos $n \in \mathbb{Z}$ tal que $n(-a) > -b$, logo $b - na > 0$, o que mostra $S \neq \emptyset$. O conjunto S é limitado inferiormente por 0, logo, pelo Principio da Boa Ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = b - a$, com $q \in \mathbb{Z}$. Como $r \geq 0$, vamos mostrar que $r < |a|$. Suponhamos $r \geq |a|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |a| + s$, logo $0 \leq s < r$. O que contradiz r ser o menor elemento de S, pois $s = b - (q \pm 1)a \in S$, com $s < r$.
Unicidade: Suponha que $b = aq + r = aq_1 + r_1$, onde $q, r, q_1, r_1 \in \mathbb{Z}$, com $0 \leq r < |a|$ e $0 \leq r_1 < |a|$. Assim, temos $-|a| < -r \leq r_1 - r < |a|$. Logo $|r_1 - r| < |a|$. Por outro lado, $a(q - q_1) = r_1 - r$, o que implica que $|a||q - q_1| = |r_1 - r| < |a|$, o que é possível se $q = q_1$ e $r = r_1$.

■

2.1 Máximo Divisor Comum

Os resultados sobre máximo divisor comum serão importantes para resolver o Algoritmo de Euclides e também para verificar se uma Equação Diofantina Linear tem ou não solução inteira.

Definição 3. Dados dois números inteiros a e b, não simultaneamente nulos, diremos que o número inteiro $d \in \mathbb{Z}$ é um divisor comum de a e b se $d|a$ e $d|b$.

Definição 4. Diremos que um número d é o máximo divisor comum (mdc)

de a e b, não simultaneamente nulos, se possuir as seguintes propriedades:
i) d é um divisor comum de a e b.
ii) d é divisível por todo divisor comum de a e b.
Representamos o mdc de a e b por $(a,b) = (b,a)$ ou ainda por $mdc(a,b)$, que é mais comum na educação básica.

Proposição 2. Se a, b, c, m e n são inteiros tais que $c|a$ e $c|b$ então $c|(ma + nb)$.

Demonstração. Se $c|a$ e $c|b$ então existem inteiros d e f tais que $a = d \cdot c$ e $b = f \cdot c$. Multiplicando essas equações por m e n, respecitivamente, teremos:
$m \cdot a = m \cdot d \cdot c$ e $n \cdot b = n \cdot f \cdot c$.
Somando membro a membro obtemos:
$m \cdot a + n \cdot b = m \cdot d \cdot c + n \cdot f \cdot c \Rightarrow m \cdot a + n \cdot b = c \cdot (m \cdot d + n \cdot f)$.
Assim concluímos que $c|(m \cdot a + n \cdot b)$.

■

Lema 1. (Lema de Euclides) Sejam $a, b, n \in \mathbb{Z}$ com $a < n \cdot a < b$. Se existe $(a, b - n \cdot a)$, então (a,b) existe e $(a,b) = (a, b - n \cdot a)$.

Demonstração. Seja $d = (a, b - n \cdot a)$, ou seja, $d|a$ e $d|(b - n \cdot a)$. Segue que, como $d|n \cdot a$, então $d|b$. Logo, d é um divisor comum de a e b. Seja c divisor comum de a e b, então $c|(b - n \cdot a)$. Assim, $c|a$ e $c|(b - n \cdot a)$ e, portanto, $c|d$. Isso prova que $d = (a,b)$.

■

Teorema 2. (Teorema de Bézout) Seja d o máximo divisor comum entre a e b, então existem inteiros m_0 e n_0 tais que $d = n_0 \cdot a + m_0 \cdot b$.

Demonstração. Seja A o conjunto de todas as combinações lineares $\{n \cdot a + m \cdot b\}$ em que n e m são inteiros. Este conjunto contém números positivos, negativos e também o zero. Vamos escolher m_0 e n_0 tais que $c = n_0 \cdot a + m_0 \cdot b$, seja o menor inteiro positivo pertencente ao conjunto A. Vamos provar que $c|a$ e $c|b$. Vamos provar por contradição que $c|a$. Suponha que $c \nmid a$. Neste caso, pelo Algoritmo de Euclides existem q e r tais que $a = q \cdot c + r$ com $0 < r < c$. Portanto,
$r = a - q \cdot c = a - q \cdot (n_0 \cdot a + m_0 \cdot b) = (1 - q \cdot n_0) \cdot a + (-q \cdot m_0) \cdot b$.
Isto mostra que $r \in A$, pois $(1 - q \cdot n_0)$ e $(-q \cdot m_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ é o menor elemento positivo de A. Logo, $c|a$, e de forma análoga se prova que $c|b$.

Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1 \cdot d$ e $b = k_2 \cdot d$ e, portanto,
$c = n_0 \cdot a + m_0 \cdot b = n_0 \cdot k_1 \cdot d + m_0 \cdot k_2 \cdot d = d \cdot (n_0 \cdot k_1 + m_0 \cdot k_2)$,
o que implica que $d|c$. Daí, temos que $d \leq c$ (ambos positivos) e como $d < c$ não é possível, pois d é o máximo divisor comum, concluímos que $d = c = n_0 \cdot a + m_0 \cdot b$.

■

Teorema 3. Para $a, b, x \in \mathbb{Z}$, temos $(a,b) = (a, b + a \cdot x)$.

Demonstração. Seja $d = (a,b)$ e $f = (a, b + a \cdot x)$. Então existem n_0 e m_0 tais que $d = n_0 \cdot a + m_0 \cdot b$, e como essa expressão pode ser escrita como $d = a \cdot (n_0 - x \cdot m_0) + (b + a \cdot x) \cdot m_0$ concluímos pelo Teorema 1 que o máximo divisor f de a e $b + a \cdot x$ é

divisor de d. Tendo mostrado que $f|d$, mostraremos que $d|f$.

Novamente pelo Teorema 1, $d|(b + a \cdot x)$ e todo divisor comum de a e $b + a \cdot x$ é um divisor de f. Provando que $d|f$, logo $d = f$, pois ambos são positivos.

■

Teorema 4. Sejam $a, b \in \mathbb{Z}$ e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.

Demonstração. Pelo Teorema 3, da relação $a = q \cdot b + r$, obtemos $(a, b) = (b, a - q \cdot b) = (b, r)$.

■

2.2 Algoritmo de Euclides

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

Teorema 5. (Teorema do Algoritmo de Euclides) Sejam $a, b \in \mathbb{N}$, com $b \neq 0$. Se o Algoritmo de Euclides for aplicado sucessivamente, então o ultimo resto não nulo r_n, satisfaz $(a, b) = r_n$.

Demonstração. Dados $a, b \in \mathbb{Z}$, podemos supor $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda $a|b$, temos que $(a, b) = a$. Suponhamos, então, que $1 < a < b$ e que $a \nmid b$. Logo, pelo Algoritmo de Euclides, podemos escrever $b = aq_1 + r_1$ com $0 < r_1 < a$. Temos duas possibilidades:

a) Se $r_1|a$ e, em tal caso, $r_1 = (a, r_1) = (a, b - q_1 \cdot a) = (a, b)$ e termina o algoritmo, ou

b) Se $r_1 \nmid a$, e, em tal caso, podemos efetuar a divisão de a por r_1, obtendo $a = r_1 q_2 + r_2$ com $0 < r_2 < r_1$.

Novamente temos duas possibilidades:

a_1) Se $r_2|r_1$, em tal caso temos $r_2 = (r_1, r_2) = (r_1, a - r_1 \cdot q_2) = (r_1, a) = (b - q_1 \cdot a, a) = (b, a) = (a, b)$.

b_1) Se $r_2 \nmid r_1$, então efetuamos a divisão de r_1 por r_2, obtendo $r_1 = r_2 \cdot q_3 + r_3$ com $0 < r_3 < r_2$.

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

■

2.2.1 Procedimento do Algoritmo de Euclides

O algoritmo demonstrado anteriormente pode ser sintetizado e realizado na prática, como mostraremos a seguir. Inicialmente, efetuamos a divisão $b = a \cdot q_1 + r_1$ e escrevemos o seguinte diagrama:

-	q_1
b	a
r_1	

A seguir efetuamos $a = r_1 \cdot q_2 + r_2$ e escrevemos os números no próximo diagrama:

-	q_1	q_2
b	a	r_1
r_1	r_2	

Prosseguindo enquanto isso for possível temos:

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

Exemplo 2. Calcular o mdc entre 352 e 182.
Usando o procedimento do Algoritmo de Euclides, obtemos:

-	1	1	14	6
352	182	170	12	2
170	12	2	0	

Logo, o $mdc(352,182) = 2$. Observe que neste exemplo, o Algoritmo de Euclides, quando usado de trás para frente, nos fornece $2 = (352,181)$, o qual foi obtido da seguinte forma: $2 = 170 \cdot 1 - 12 \cdot 14 = 170 \cdot 1 - (182 - 170 \cdot 1) \cdot 14 = 170 \cdot 15 - 182 \cdot 14 = (352 - 182 \cdot 1) \cdot 15 - 182 \cdot 14 = 352 \cdot 15 - 182 \cdot 29$.

2.3 Números Primos

Esta seção definirá números primos e demonstrará um importante resultado, o Teorema Fundamental da Aritmética.

Definição 5. Dois números naturais a e b são ditos primos entre si, ou coprimos, se $(a,b) = 1$. Se $n > 1$ é um número inteiro possuindo somente dois divisores 1 e n, então esse número é chamado de primo. Quando $n > 1$ não é primo, ele é chamado de composto.

Teorema 6. (Teorema Fundamental da Aritmética) Todo número natural n maior do que 1 pode ser escrito de forma única (a menos da ordem) como um produto de fatores primos, ou seja

$$n = p_1 \cdots p_m$$

em que $m \geq 1$ é um número natural e $p_1 \leq \cdots \leq p_m$ são primos.

Demonstração. (Existência) Mostramos a existência da fatoração de n em primos por indução. Se n é um número primo não há o que provar, basta tomar $m = 1$ e $p_1 = n$. Se n é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$, $1 < b < n$. Por hipótese de indução, a e b se decompõem como produto de primos. Arrumando as fatorações de a e b de forma a organizar os fatores, obtemos uma fatoração de n.
(Unicidade) Suponhamos por absurdo que n possui duas fatorações diferentes, ou seja, $n = p_1 \cdots p_m = q_1 \cdots q_{m'}$ com $p_1 \leq \cdots \leq p_m$, $q_1 \leq \cdots \leq q_{m'}$ e que n é o mínimo com tal propriedade. Como $p_1 | q_1 \cdots q_{m'}$ temos que $p_1 | q_i$ para algum valor de i. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas, $\frac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_{m'}$ admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações.

■

2.4 Equações Diofantinas Lineares

As Equações Diofantinas são equações algébricas com uma ou mais variáveis, a serem resolvidas no conjunto dos números inteiros. Neste capítulo vamos introduzir conceitos sobre as Equações Diofantinas Lineares com duas incógnitas. Essas equações serão de grande importância

nesse trabalho, pois será com o objetivo de aplica-las em sala que o professor trabalhará alguns conteúdos referente a Teoria dos Números. O conteúdo a seguir será baseado nas referências Hefez, Filho, Lins, Santos e Nagell.

Definição 6. As equações Diofantinas Lineares são as equações na forma $aX + bY = c$, com $a, b, c \in \mathbb{Z}$. Se $c = 0$, as Equações Diofantinas admitem pelo menos a solução trivial $X = 0$ e $Y = 0$. Todo par de inteiros X_0, Y_0 tais que $aX_0 + bY_0 = c$ diz-se uma solução inteira ou apenas solução da equação $aX + bY = c$.

Exemplo 3. Dada a Equação Diofantina $3X + 6Y = 18$, algumas soluções possíveis são:
$3 \cdot 4 + 6 \cdot 1 = 18$ em que $X = 4$ e $Y = 1$.
$3 \cdot 2 + 6 \cdot 2 = 18$ em que $X = 2$ e $Y = 2$.
$3 \cdot 18 + 6 \cdot (-6) = 18$ em que $X = 18$ e $Y = -6$.

Proposição 3. Sejam $a, b \in \mathbb{Z}$ não nulos e $c \in \mathbb{Z}$. A equação $aX + bY = c$ admite soluções inteiras se, e somente se, $(a, b)|c$, com $d = (a, b)$.

Demonstração. Suponhamos que a equação $aX + bY = c$ tem uma solução, isto é, que existe um par de inteiros X_0 e Y_0 tais que $aX_0 + bY_0 = c$. Ponhamos $(a, b) = d$, logo existem inteiros r e s tais que $a = dr$ e $b = ds$, e temos $c = aX_0 + bY_0 = drX_0 + dsY_0 = d(rX_0 + sY_0)$. Como $rX_0 + sY_0$ é um número inteiro, segue-se que d divide c.

Reciprocamente, suponhamos que d divide c, isto é, que $c = dt$, onde t é um inteiro. Como $(a, b) = d$, existem inteiro X_0 e Y_0 tais que $d = aX_0 + bY_0$ (Teorema de Bezout). O que implica $c = dt = (aX_0 + bY_0)t = a(tX_0) + b(tY_0)$, isto é, o par de inteiros $X = tX_0 = (c/d)X_0 \; e \; Y = tY_0 = (c/d)Y_0$ é uma solução da equação $aX + bY = c$.

■

Definição 7. Uma solução particular da equação $aX - bY = c$, em que $(a, b) = 1$, é uma solução X_0, Y_0 tal que, se X_1, Y_1 é solução, então $X_0 \leq X_1$ e $Y_0 \leq Y_1$.

Proposição 4. Seja X_0, Y_0 a solução particular da equação $aX - bY = c$, em que $(a, b) = 1$. As soluções $X, Y \in \mathbb{N}$, são da forma $X = X_0 + tb$ e $Y = Y_0 + ta$ com $t \in \mathbb{N}$.
Demonstração. Suponha que $X = X_0 + tb$ e $Y = Y_0 + ta$, então $aX - bY = a(X_0 + tb) - b(Y_0 + ta) = aX_0 + atb - bY_0 - bta = aX_0 - bY_0 = c$. Logo, X e Y são soluções da equação. Reciprocamente, suponha que X, Y é uma solução. Então, $aX - bY = c = aX_0 - bY_0$. Daí, $aX - aX_0 = bY - bY_0$ implica que $a(X - X_0) = b(Y - Y_0)$. Como $(a, b) = 1$ e $b|a(X - X_0)$, segue que $b|(X - X_0)$ de onde existe $t \in \mathbb{N}$ tal que $X - X_0 = tb$, isto é, $X = X_0 + tb$. Além disso, temos $atb = b(Y - Y_0)$, de onde segue que $Y = Y_0 + ta$. Segue que a equação acima $aX + bY = c$, com $(a, b) = 1$, admite infinitas soluções em $\mathbb{Z}$.

■

Exemplo 4. Determinar todas as soluções da Equação Diofantina Linear $172X + 20Y = 1000$.

Vamos primeiramente determinar o $mdc(172,20)$ pelo Algoritmo de Euclides. Dividindo 172 por 20, obtemos a igualdade $172 = 20 \cdot 8 + 12$. Agora, dividindo 20 por 12 (resto na igualdade anterior), temos $20 = 12 \cdot 1 + 8$. E seguindo o mesmo procedimento, encontramos $12 = 8 \cdot 1 + 4$ e $8 = 4 \cdot 2 + 0$. Portanto, o $mdc(172,20) = 4$, pois o último resto diferente de 0 é o 4, e como $4|1000$, segue-se que a equação tem solução. Agora dividindo a equação por 4, obtemos $43X + 5Y = 250$. Para achar uma solução particular X_0, Y_0, vamos usar novamente o Algoritmo de Euclides, dividindo agora 43 por 5, donde obtemos $43 = 5 \cdot 8 + 3$. Agora, dividindo 5 por 3 (resto na igualdade anterior), temos $5 = 3 \cdot 1 + 2$. E seguindo o mesmo procedimento, encontramos $3 = 2 \cdot 1 + 1$. Substituindo as igualdades anteriores de trás pra frente, obtemos:

$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \cdot 1 = (43 - 5 \cdot 8) \cdot 2 - 5 \cdot 1 = 43 \cdot 2 - 5 \cdot 17.$

Com isso temos $1 = 43 \cdot 2 - 5 \cdot 17$. Multiplicando a igualdade por 250, de forma conveniente, encontramos $250 = 43 \cdot 500 - 5 \cdot 4250$ ou ainda $250 = 500 \cdot 43 - 4250 \cdot 5$. Logo, $X_0 = 500$ e $Y_0 = -4250$ é solução particular e consequentemente $X = 500 + t \cdot 5$ e $Y = -4250 - t \cdot 43$, com $t \in \mathbb{Z}$ é solução da equação.

Proposição 5. Sejam $a, b \in \mathbb{N}$, com $(a, b) = 1$. Todo número natural c pode ser escrito de modo único de uma e somente uma das formas: $c = na + mb$, ou $c = na - mb$, com $n < b$ e $n, m \in \mathbb{N}$.

Demonstração. Existência: Sabemos que existem $u, v \in \mathbb{N}$ tais que $ua - vb = (a, b) = 1$. Se multiplicarmos ambos os membros dessa igualdade por c, obtemos $auc - bvc = c$. Usando o Algoritmo de Euclides, temos que existem $q, n \in \mathbb{N}$ com $n < b$ tais que $uc = qb + n$. Substituindo uc na igualdade acima, temos:
$c = na + qab - vcb$. Se $qa \geq vc$, pondo $m = qa - vc$, temos que $c = na + mb$. No caso em que $vc \geq qa$, pondo $m = vc - qa$, temos que $c = na - mb$.
Unicidade: Suponhamos que existem $n_1, m_1 \in \mathbb{N}$, tais que $na \pm mb = n_1 a \pm m_1 b$, com $n, n_1 < b$. Teremos três possibilidades para analisar:
I- $na + mb = n_1 a - m_1 b$;
II- $na + mb = n_1 a + m_1 b$;
III- $na - mb = n_1 a - m_1 b$.

Primeiro, vamos mostrar que a possibilidade I só ocorre quando $n = n_1$ e $m = m_1 = 0$. Para isto, basta mostrar que $n = n_1$, pois teríamos $0 = na + mb - (n_1 a - m_1 b) = mb + m_1 b = b(m + m_1)$, o que implicaria em $m + m_1 = 0$, e portanto $m = m_1 = 0$. Agora, suponhamos por absurdo que $n \neq n_1$. Logo, devemos ter $n_1 > n$. Portanto, $(n_1 - n)a = (m + m_1)b$. Como $(a, b) = 1$, temos que $a|(m + m_1)$ e, assim, $m + m_1 = ra$. Logo, $(n_1 - n)a = (m + m_1)b = rab$. Daí segue que $(n_1 - n) = rb$, o que é absurdo, pois $n_1 - n < b$ e $rb \geq b$. Portanto, $n = n_1$.

Segundo, vamos mostrar que a possibilidade II ocorre quando $n = n_1$ e $m = m_1$. Para isto, basta mostrar que $n = n_1$, pois teríamos $0 = na + mb - n_1 a - m_1 b = mb - m_1 b = b(m - m_1)$, o que implicaria $m - m_1 = 0$, e assim $m = m_1$. Suponhamos por absurdo

que $n \neq n_1$. Logo, devemos ter $n_1 > n$. Portanto, $(n_1 - n)a = (m - m_1)b$. Como $(a, b) = 1$, temos que $a|(m - m_1)$ e, assim, $m - m_1 = ra$. Logo, $(n_1 - n)a = (m - m_1)b = rab$. Daí segue que $(n_1 - n) = rb$, o que é absurdo, pois $n_1 - n < b$ e $rb \geq b$. Portanto, $n = n_1$.

Por último, vamos mostrar que a possibilidade III ocorre quando $n = n_1$ e $m = m_1 = 0$. Para isto, basta mostrar que $n = n_1$, pois teríamos $0 = na - mb - (n_1 a - m_1 b) = -(mb + m_1 b) = b(-(m + m_1))$, o que implicaria $-(m + m_1) = 0$, e portanto $m = m_1 = 0$. Agora, suponhamos por absurdo que $n \neq n_1$. Logo, devemos ter $n_1 > n$. Portanto, $(n_1 - n)a = (-m + m_1)b$. Como $(a, b) = 1$, temos que $a|(-m + m_1)$ e, assim, $-m + m_1 = ra$. Logo, $(n_1 - n)a = (-m + m_1)b = rab$. Daí segue que $(n_1 - n) = rb$, o que é absurdo, pois $n_1 - n < b$ e $rb \geq b$. Portanto, $n = n_1$.

■

Definição 8. Sejam $a, b \in \mathbb{N}$. Definimos o conjunto $S(a, b) = \{xa + yb;\ x, y \in \mathbb{N} \cup \{0\}\}$.

Proposição 6. Existe $c \in S(a, b)$ se, e somente se, existem $m, n \in \mathbb{N}$, com $n < b$ tais que $c = na + mb$.

Demonstração. Se $c \in S(a, b)$, então $c = xa + yb$, com $x, y \in \mathbb{N}$. Pelo Algoritmo de Euclides, $x = bq + n$, com $n < b$. Logo, $c = (bq + n)a + yb = bqa + na + yb = na + (qa + y)b$. Assim, obtemos $c = na + mb$, com $n < b$, e $m = aq + y$. Obviamente se $c = na + mb$, então $c \in S(a, b)$.

■

Definição 9. Definimos o conjunto das lacunas de $S(a, b)$ como sendo o conjunto $L(a, b) = \mathbb{N} \setminus S(a, b)$.

Corolário 1. Temos que $L(a, b) = \{na - mb \in \mathbb{N};\ n, m \in \mathbb{N}, n < b\}$.

Teorema 7. A equação $aX + bY = c$, onde $(a, b) = 1$, tem solução em números naturais se, e somente se, $c \notin L(a, b) = \{na - mb \in \mathbb{N};\ n, n \in \mathbb{N}, n < b\}$.

Demonstração. Sabemos que a equação $aX + bY = c$ tem solução se, e somente se, $c \in S(a, b)$. Assim, o resultado segue do corolário anterior.

■

Proposição 7. Suponha que a equação $aX + bY = c$, com $(a, b) = 1$, tenha solução e seja $X_0 = n$, $Y_0 = m$ a solução particular. As soluções x e y da equação são dadas pelas fórmulas $x = n + tb$ e $y = m - ta$, com $t \in \mathbb{N} \cup \{0\}$, $m - ta \geq 0$.

Demonstração. Temos que $an + bm = ax + by = c$ implica que $a(x - n) = b(m - y)$. Como $(a, b) = 1$, segue que $b|(x - n)$. Logo, $x - n = tb$, $t \in \mathbb{N}$. O que implica em $x = n + tb$. E fazendo a substituição obtemos $m - y = ta$. Como queríamos demonstrar.

■

3 Projeto de aplicação em sala de aula

Nessa seção apresentaremos atividades que podem ser aplicadas em sala de aula com alunos do 9º ano do Ensino Fundamental e do primeiro ano do Ensino Médio. Essas atividades serão desenvolvidas em forma de um

pequeno plano de aula, onde sugerimos o caminho a ser percorrido pelo professor, com toda a teoria que deverá ser aplicada, e ainda solucionar problemas dos mais simples aos mais complexos usando Equações Diofantinas Lineares e de segunda ordem. Nesta parte do trabalho utilizamos como referências Hefez, Filho, Lins, Santos, Rosen e Nagell.

3.1 Primeiro Encontro

- Números de Aulas: Duas Aulas.
- Objetivos: Revisar conceitos da Teoria dos Números.
- Conteúdos: Números primos, noções de divisibilidade, múltiplos e Algoritmo de Euclides.
- Encaminhamentos Metodológicos: Definir o conceito divisão, e relembrar como encontrar os divisores de um número. Conceituar os múltiplos de um número, e como calcular os seus respectivos múltiplos. Explicar a divisão euclidiana e como é feito o seu algoritmo.
- Teoria e Atividades: Em primeiro lugar o professor deverá iniciar sua aula motivando os alunos a relembrarem os conceitos que serão trabalhados nesse encontro. Conceitos esses que são divisores, múltiplos, mdc (máximo divisor comum) e Algoritmo de Euclides. Tais conceitos podem ser definidos das formas a seguir para os alunos.

3.1.1 Divisores

Podemos utilizar a Definição 2, onde encontramos que, dados dois números inteiros a e b, diremos que a divide b, escrevendo $a|b$, quando existir c inteiro tal que $b = c \cdot a$. Neste caso, diremos também que a é um divisor de b, ou ainda, que b é um múltiplo de a.

Exercício 1. Encontrar os divisores dos números 12, 30 e 32.

a) $D(12) = 1, 2, 3, 4, 6, 12.$

b) $D(30) = 1, 2, 3, 5, 6, 10, 15, 30.$

c) $D(32) = 1, 2, 4, 8, 16, 32.$

3.1.2 Máximo Divisor Comum

Usamos para definir Máximo Divisor Comum as Definições 3 e 4. Aqui, podemos introduzir uma simbologia, que servirá para facilitar a notação de mdc, que é (a, b). (Definição 4).

Exemplo 5. Encontrar o Máximo Divisor Comum entre 36 e 64.

Nesse exemplo o professor deverá lembrar que um dos caminhos para encontrar o mdc de dois ou mais números é calcular todos os divisores, e através de uma observação, encontrar qual é o maior deles. Nesse caso, temos $D(36) = 1, 2, 3, 4, 6, 9, 12, 18, 36$ e $D(64) = 1, 2, 4, 8, 16, 32, 64.$ Onde obtemos que os divisores comuns são: 1, 2 e 4, e o maior deles é o 4. Portanto, o mdc entre 36 e 64 é 4, ou seja $(36,64) = 4.$

3.1.3 Algoritmo de Euclides

Também conhecido como Algoritmo da Divisão, o Algoritmo de Euclides nada mais é que efetuar a divisão de dois números inteiros a e b, resultando num número que é o quociente q e outro que é o resto r, o qual escrevemos da forma $b = a \cdot q + r$, com $q \in \mathbb{Z}$, e $0 \leq r < |a|$. Temos como referências os Teoremas Divisão Euclidiana, Euclides e do Algoritmo de Euclides. Aqui o professor deverá mostrar ao aluno que a metodologia que ele resolve a divisão desde os anos iniciais do ensino fundamental continua a ser praticada, mas nesse instante ele irá apenas escrever a divisão de forma mais elegante, a qual ajudará na prática de alguns exercícios.

Exemplo 6. Encontrar o quociente e o resto da divisão de 330 por 20.
Solução. Efetuando a divisão de 330 por 20 obtemos quociente 16 e resto 10. Assim, podemos escrever da seguinte forma $330 = 20 \cdot 16 + 10$. Visto a Divisão Euclidiana, o professor deverá introduzir ao aluno que para encontrar o mdc de dois números inteiros basta resolver um processo que se chama Procedimento do Algoritmo de Euclides, que consiste em efetuar divisões sucessivas entre o quociente e o resto da divisão, até não encontrarmos resto, e o último resto diferente de 0 será o mdc, de acordo com o Teorema 1 (Teor. Algoritmo de Euclides).

Exemplo 7. Qual é o mdc entre 300 e 135?
Solução. Primeiro efetuamos a divisão de 300 por 135, em que obtemos quociente 2 e resto 30, que pode ser colocado no diagrama:

-	2	
300	135	30
30		

Feito isso, agora prosseguimos com a divisão de 135 por 30, em que obtemos quociente 4 e resto 15, que pode ser colocado no diagrama:

-	2	4	
300	135	30	15
30	15		

Como ainda não obtemos resto 0, devemos continuar esse processo, agora dividindo 30 por 15, o qual obtemos quociente 2 e resto 0.

-	2	4	2	
300	135	30	15	0
30	15	0		

Como o último resto diferente de 0 é o 15, então o mdc entre 300 e 135 é 15.

3.2 Segundo Encontro

- Números de Aulas: Duas Aulas.
- Objetivos: Revisar conceitos da Teoria dos Números.
- Conteúdos: Números primos, noções de divisibilidade, múltiplos e Algoritmo de Euclides.
- Encaminhamentos Metodológicos: Verificar se os alunos compreenderam os conceitos pertencentes aos divisores, múltiplos e o Algoritmo da divisão.
- Teoria e Atividades: Feito todo esse trabalho de retomada de

conteúdo no encontro anterior, o professor poderá aplicar os exercícios a seguir para que o aluno possa compreender e praticar aquilo que ele viu em sala de aula.

Exercício 2. Verifique:
a) se 109 é divisível por 3.
Solução. Usando o Algoritmo de Euclides temos: $109 = 3 \cdot 36 + 1$. Logo, 109 não é divisível por 3.

b) se 119 é divisível por 9.
Solução. Usando o Algoritmo de Euclides temos: $119 = 9 \cdot 13 + 2$. Logo, 119 não é divisível por 9.

c) se 143 é divisível por 12.
Solução: Usando o Algoritmo de Euclides temos: $143 = 12 \cdot 11 + 11$. Logo, 143 não é divisível por 12.

d) se 310 é divisível por 5.
Solução. Usando o Algoritmo de Euclides temos: $310 = 5 \cdot 62 + 0$. Logo, 310 é divisível por 5.

Exercício 3. A idade de Janete corresponde ao maior divisor par de 60, sem ser o próprio 60. Qual é a idade de Janete?
Solução. Para resolver, encontramos os divisores de 60, e verificamos quais deles são pares, e qual é o maior diferente de 60. Assim, $d(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$. Logo, a idade de Janete é 30 anos.

Exercício 4. Qual é o maior múltiplo de 13 menor que 300?
Solução. Os primeiros múltiplos de 13 são: $m(13) = 0,13,26,39,\ldots$. Mas, não precisamos procurar todos os múltiplos de 13 até chegar em 300. Como queremos um múltiplo menor que 300, vamos usar o Algoritmo de Euclides para verificar qual número menor que 300 é divisível por 13. Assim, fazendo a divisão de 300 por 13, obtemos $300 = 23 \cdot 13 + 1$. E continuando fazendo a divisão, mas agora a divisão de 299 por 13 nos dá $299 = 23 \cdot 13 + 0$. Logo, 299 é o maior múltiplo de 13 menor que 300.

Exercício 5. Calcule o mdc de 637 e 2877.
Solução. Usando o Algoritmo de Euclides temos:

-	4	1	1	14	1	2
2877	637	329	308	21	14	7
329	308	21	14	7	0	

Assim, o mdc de 637 e 2877 é 7.

Poderíamos ter resolvido também na forma mais utilizada pelos professores no ensino fundamental, que é a decomposição simultânea dos números considerando apenas os fatores primos comum.

Exercício 6. Calcule o mdc de 3568 e 988.
Solução: Usando o Algoritmo de Euclides temos:

-	3	1	1	1	1	2	1	13
3568	988	604	384	220	164	56	52	4
604	384	220	164	56	52	4	0	

Assim, o mdc de 3568 e 988 é 4.

Exercício 7. Seja o conjunto $A = \{1,2,3,4,5,6\}$. Enumerar os elementos do conjunto $X = \{x \in A \mid mdc(x,6) = 1\}$.
Solução. Se $mdc(x,6) = 1$, x e 6 são primos entre si, e como os fatores de 6

são 2 e 3, temos que os elementos de A que na decomposição não apresentam os fatores 2 e 3 são 1 e 5.

Exercício 8. Dona Maria precisa de 30 m de fita verde e 24 m de fita amarela. Ela quer cortar essas fitas de modo que os pedaços tenham o mesmo tamanho, que sejam o maior possível e que não sobre pedaços da fita. Quantos metros deve ter cada pedaço de fita?

Solução. Para descobrir quantos metros tem cada pedaço de fita, e que esses pedaços tenham o mesmo tamanho e que esse tamanho seja o maior possível, devemos encontrar o maior divisor comum a essas duas medidas das fitas, ou seja, vamos encontrar o mdc de 30 e 24. Não vamos usar o Algoritmo de Euclides (que também poderia ser usado), vamos encontrar os divisores de cada número e depois encontrar o maior comum:

$D(30) = 1, 2, 3, 5, 6, 10, 15, 30$ e $D(24) = 1, 2, 3, 4, 6, 8, 12, 24$.

Assim, temos que os divisores comuns são: 1, 2, 3, 6. O maior deles é o 6. Portanto, cada fita deve ser cortada com 6 metros.

Exercício 9. Se um número qualquer divide o produto de outros dois números inteiros quaisquer, ele necessariamente divide um dos fatores?

Solução. Não, pois podemos tomar esses números com $a > b > c$, e vemos que $a|b \cdot c$, mas $a \nmid b$ e $a \nmid c$. Por exemplo, $25|10 \cdot 5$, mas $25 \nmid 10$ e $25 \nmid 5$.

Exercício 10. Achar o maior inteiro positivo pelo qual se devem dividir os inteiros 160, 198 e 370 para que os restos sejam respectivamente 7, 11 e 13.

Solução. Se 7, 11 e 13 são os restos, a divisão de $160 - 7 = 153$, $198 - 11 = 187$ e $370 - 13 = 357$ pelo inteiro positivo é exata. Como esse inteiro é o maior inteiro positivo, esse número é o $mdc(153, 187, 357)$. Calculando o mdc:

Primeiro, calculamos $mdc(357, 187)$. Usando o Algoritmo de Euclides na divisão de 357 por 187, obtemos $357 = 187 \cdot 1 + 170$. E ainda 187 dividido por 170, encontramos $187 = 170 \cdot 1 + 17$. E por último 170 dividido por 17 escrevemos $170 = 17 \cdot 10 + 0$ implica que $mdc(357,187) = 17$.

Segundo calculamos $mdc(153,17)$. Usando o Algoritmo de Euclides na divisão de 153 por 17, obtemos $153 = 17 \cdot 9$, o que implica em $mdc(153,17) = 17$. Portanto, o número é 17, usando o Teorema 1 (Teor. Algoritmo de Euclides).

Exercício 11. Os restos das divisões dos inteiros 4933 e 4435 por um inteiro positivo n são respectivamente 37 e 19. Achar o inteiro n.

Solução. Como os restos são 37 e 19, temos que $4933 - 37 = 4896$ e $4435 - 19 = 4416$ são múltiplos comuns de n. Portanto, n é divisor comum de 4896 e 4416, isto implica que n é divisor do $mdc(4869,4416)$.

Calculando o $mdc(4869,4416)$, dividimos 4896 por 4416, e obtemos $4896 = 4416 \cdot 1 + 480$, e ainda 4416 dividido por 480, encontramos

$4416 = 480 \cdot 9 + 96$, e por fim, 480 dividido por 96, obtemos $480 = 96 \cdot 5 + 0$ implica que $mdc(4896,4416) = 96$. Logo, N é um divisor de 96, maior que 37 que é o resto da divisão de 4933 por n. Portanto, $n = 96$ ou $n = 48$.

3.3 Terceiro Encontro

- Número de Aulas: Duas Aulas.
- Objetivos: Definir as Equações Diofantinas Lineares e desenvolver o método de tentativa e erro.
- Conteúdos: Equações Diofantinas Linerares e máximo divisor comum, além de outros conceitos de Teoria dos Números.
- Encaminhamentos Metodológicos: Conceituar Equações Diofan-tinas Lineares e fazer com que o aluno pense nas possíveis soluções das equações apresentadas.
- Teoria e Atividades: Apresentamos aqui uma lista de equações e problemas que ajudarão o professor a iniciar essa exposição das Equações Diofantinas Lineares. Essa primeira aula será apenas para que o aluno tenha conhecimento desse tipo de equação, qual o seu conjunto de soluções, e se todas as equações na forma linear apresentam solução.

3.3.1 Equações Diofantinas Lineares

As Equações Diofantinas Lineares são as equações da forma $aX + bY = c$, com $a, b, c \in \mathbb{Z}$, cujas soluções pertencem ao conjunto dos números inteiros (Definição 6). O professor deverá alertar o aluno com relação às soluções, pois ele poderá encontrar infinitas soluções que não sejam inteiras, mas no conjunto dos números inteiros nem sempre uma Equação Diofantina Linear tem solução.

Neste momento apresentamos uma série de exercícios que podem ser resolvidos pelo método de tentativa e erro. Esse método consiste em procurar algumas das possíveis soluções dos problemas, ou ainda perceber que uma equação não tem solução sem utilizar um algoritmo para isso, apenas testando possíveis soluções. Após esse método, poderemos questionar se essa é a única forma de procurar as soluções, o que será resolvido no próximo encontro.

Exercício 12. Usando o método de tentativa e erro, encontre algumas soluções para as equações a seguir:

a) $2X + 6Y = 10$. Solução. Por exemplo: $x = 2$ e $y = 1$; $x = 5$ e $y = 0$; $x = 8$ e $y = -1$.

b) $5X + 3Y = 12$. Solução. Por exemplo: $x = 0$ e $y = 4$; $x = 3$ e $y = -1$; $x = -3$ e $y = 9$.

c) $4X + 8Y = 9$. Solução. Não apresenta solução inteira.

d) $6X - 3Y = 12$. Solução. Por exemplo: $x = 2$ e $y = 0$; $x = 5$ e $y = 6$; $x = -4$ e $y = -12$.

e) $10X + 5Y = 6$. Solução. Não apresenta solução inteira.

f) $15X - 51Y = 41$. Solução. Não apresenta soluções inteiras.

g) $5X + 6Y = 1$. Solução. Por exemplo: $x = -1$ e $y = 1$; $x = 5$ e $y = -4$; $x = -7$ e $y = 6$.

Exercício 13. Suponhamos que só existam notas de 15 e de 7 reais e que se queira pagar (em dinheiro) uma certa quantia em reais. Será que é sempre possível? E se existissem somente notas de 12 e de 30 reais?
Solução. Primeiro, percebemos que o problema pode ser resolvido para a quantia de 1 real, pois para obter outras quantias, basta multiplicar o seu resultado. Por exemplo, para pagar 1 real podemos usar uma nota de 15 e receber de troco duas notas de 7. Deste modo, se quisermos pagar 23 reais podemos usar 23 notas de 15 e receber de troco 46 notas de 7. Entretanto, seria mais simples pagar com 2 notas de 15 e receber de troco uma nota de 7. Agora, tendo pensado em possíveis soluções, podemos conseguir equacionar o problema. Ou seja, estamos tentando encontrar soluções inteiras para a equação $7X + 15Y = 1$. No segundo caso, devemos perceber que a solução seria um múltiplo de 6, já que 12 e 30 são múltiplos de 6. E da mesma forma que no primeiro caso, aqui bastaria repetir o pagamento de 6 reais quantas vezes fossem necessárias para encontrar soluções múltiplas de 6, ou seja, devemos encontrar soluções para a equação $30X - 12Y = 6$. Por exemplo, uma solução seria $x = 1$ e $y = 2$.

Exercício 14. Suponhamos que duas crianças vão comprar sorvete e recebem de seus pais R$10,00. Se cada sorvete custa R$2,00 quando é bola simples, e R$3,00 quando é bola dupla, quais as possíveis combinações de sorvete que eles podem comprar gastando todo o dinheiro? E se tivessem recebido R$15,00?
Solução. Pensando nas possíveis combinações para os R$10,00, vamos perceber que as crianças podem comprar:

- 5 sorvetes de bola simples e 0 sorvetes de bola dupla;
- 2 sorvetes de bola simples e 2 sorvetes de bola dupla;

Agora, para R$15,00 temos:

- 0 sorvetes de bola simples e 5 sorvetes de bola dupla;
- 6 sorvetes de bola simples e 1 sorvete de bola dupla;
- 3 sorvetes de bola simples e 3 sorvete de bola dupla;

O aluno também pode escrever as equações que caracterizam esse problema: $2X + 3Y = 10$ e $2X + 3Y = 15$, onde x é o número de sorvetes de bola simples e y é o número de sorvetes de bola dupla.

Exercício 15. Um supermercado vende pacotes de leite do tipo "C" e do tipo "B". Se em um mês Carlos comprou R$48,00 em leite, quais as possíveis combinações, se o supermercado vende cada leite tipo "C" a R$2,00, e cada leite tipo "B" a R$3,00?
Solução: Nesse problema a várias possibilidades, dentre elas:

- 12 leites do tipo "C" e 8 leites do tipo "B";
- 24 leites do tipo "C" e 0 leites do tipo "B";
- 0 leites do tipo "C" e 16 leites do tipo "B";
- 15 leites do tipo "C" e 6 leites do tipo "B".

Entre outras soluções.

Exercício 16. (Problema adaptado de Pommer) Ana gosta muito de música, e todos os meses utiliza de seu salário R$270,00 para comprar CD´s ou DVD´s. Se cada CD que ela compra custa R$18,00 e cada DVD custa R$30,00, quais as possibilidades que ela tem de compra? Se depois de alguns meses, Ana passou a utilizar R$130,00 do seu salário, quais as possíveis possibilidades, se os CD´s passaram a custar R$20,00 e os DVD´s R$32,00?
Solução. As possíveis soluções para a primeira situação são:

- 10 CD´s e 3 DVD´s;
- 15 CD´s e 0 DVD´s;
- 0 CD´s e 9 DVD´s;

Para a segunda situação não temos solução inteira, levando-nos a fazer alguns cálculos desnecessários, e que no próximo encontro saberemos como verificar se esse problema tem ou não solução.

Exercício 17. Uma caixa contém besouros e aranhas. Existem 46 patas na caixa. Quantos são os besouros e quantas são as aranhas?
Solução. Lembrando que cada aranha tem 8 patas e cada besouro tem 6 patas. A equação que representa a situação do problema é $8A + 6B = 46$, onde A representa o número de aranhas, e B representa o número de besouros. Assim, encontrando a solução por tentativa e erro, encontramos os valores de A e de B (que devem ser positivos):

- $A = 2$ e $B = 5$, onde o número de aranhas são 2, e de besouros são 5.
- $A = 5$ e $B = 1$, onde o número de aranhas são 5, e de besouros são 1.

Exercício 18. (Euler) Divida 100 em 2 parcelas positivas, de modo que uma seja divisível por 7 e a outra por 11.
Solução. A situação do exercício é representada pela seguinte equação: $7X + 11Y = 100$. Procurando a solução por tentativa e erro, encontramos $x = 8$ e $y = 4$.

No próximo encontro vamos perceber que encontrar a solução desse problema é facilitado usando outros argumentos.

3.4 Quarto Encontro

- Número de Aulas: Duas Aulas.
- Objetivos: Encontrar soluções gerais para as Equações Diofantinas Lineares utilizando os conceitos dos primeiros encontros. Utilizar o software Geogebra como ferramenta para verificar se as soluções dos problemas são realmente verdadeiras, ou até mesmo encontrar outras soluções diferentes.
- Conteúdos: Equações Diofantinas Linerares e máximo divisor comum além de outros conceitos de Teoria dos Números e software Geogebra.
- Encaminhamentos Metodológicos: Fazer com que o aluno utilize Equações Diofantinas Lineares para resolver diversos problemas, e que ele procure as possíveis soluções das equações e dos problemas apresentados.

- Teoria e Atividades: O professor deverá retomar a definição das Equações Diofantinas Lineares (Definição 6), e apresentar alguns resultados que garantirão uma forma de verificar se uma equação tem ou não solução. E só depois disso poderá mostrar como encontrar a solução usando a teoria já apresentada. Uso do Geogebra na verificação das soluções de alguns dos problemas.

3.4.1 Equações Diofantinas Lineares

As Equações Diofantinas Lineares apresentam solução nos números inteiros quando o mdc entre os coeficientes a e b da equação for divisor do termo independente c. Ou seja, quando $d|c$ (d divide c), sendo $d = (a, b)$

Exemplo 7. Verificar se as equações abaixo apresentam ou não soluções inteiras.
a) $2X + 3Y = 10$.
Solução. Calculando (2,3), encontramos 1 como sendo o mdc. Como 1 é divisor de 10, pois usando o Algoritmo de Euclides podemos escrever $10 = 1 \cdot 10 + 0$, então usando a Proposição 3, temos que a equação $2x + 3y = 10$ tem solução em $\mathbb{Z}$.
b) $4X + 10Y = 16$.
Solução. Calculando (4,10), encontramos 2 como sendo o mdc. Como 2 é divisor de 16, pois usando o Algoritmo de Euclides podemos escrever $16 = 2 \cdot 8 + 0$, então usando a Proposição 3, temos que a equação $4x + 10y = 16$ tem solução em $\mathbb{Z}$.
c) $14X + 35Y = 9$.
Solução. Calculando (14,35), encontramos 7 como sendo o mdc. Como 7 não é divisor de 9, pois usando o Algoritmo de Euclides podemos escrever $9 = 7 \cdot 1 + 2$, então usando a Proposição 3, temos que a equação $14x + 35y = 9$ não tem solução em $\mathbb{Z}$.

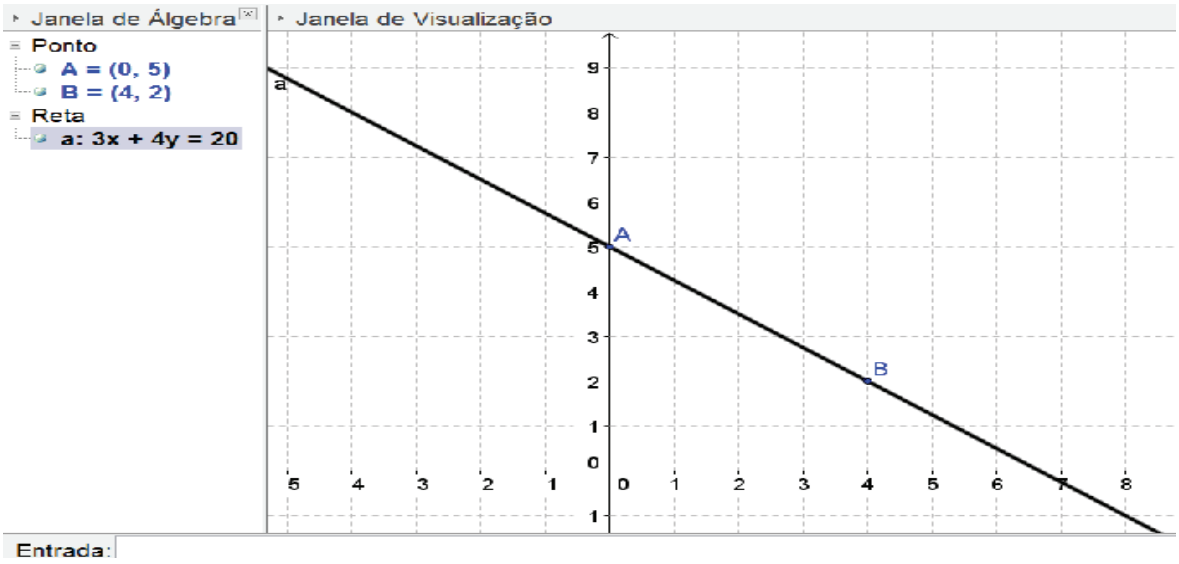
Exemplo 8. Encontrar as soluções particulares e gerais para a Equação Diofantina $6X + 10Y = 26$.
Solução. Primeiramente, devemos verificar se tal equação possui solução em $\mathbb{Z}$. De fato, como $(6,10) = 2$, e 2 divide 26, pois usando o Algoritmo de Euclides podemos escrever $26 = 2 \cdot 13 + 0$, então usando a Proposição 3, temos que a equação $6X + 10Y = 26$ tem solução em $\mathbb{Z}$.

Agora, podemos procurar as soluções da equação. Vamos simplificar a equação, dividindo ela pelo mdc 2, e obtemos a equação $3X + 5Y = 13$. Depois disso, vamos usar o procedimento do Algoritmo de Euclides para encontrar as soluções. Donde obtemos a divisão de 5 por 3 e escrevemos $5 = 3 \cdot 1 + 2$. E fazendo a divisão de 3 por 2, obtemos $3 = 2 \cdot 1 + 1$. Logo, substituindo as igualdades anteriores de trás pra frente, $1 = 3 \cdot 1 - 2 = 3 \cdot 1 - (5 - 3 \cdot 1) = 3 \cdot 2 - 5 \cdot 1$. De onde obtemos $2 \cdot 3 + (-1) \cdot 5 = 1$. Agora, multiplicando a igualdade por 13 de forma conveniente, temos $26 \cdot 3 + (-13) \cdot 5 = 13$. Assim uma solução particular é, $X_0 = 26$ e $Y_0 = -13$. E usando a Proposição 4, podemos encontrar as soluções da forma $X = X_0 + tb$ e $Y = Y_0 + ta$ com $t \in \mathbb{Z}$, que neste exemplo são: $X = 26 + 5t$ e $Y = -13 - 3t$, com $t \in \mathbb{Z}$. É

neste momento que o professor deverá introduzir a Proposição 4, para explicar como é que encontramos a solução geral de uma Equação Diofantina Linear.

Neste momento o professor deverá resolver as atividades usando os métodos feitos no encontro anterior e deverá aplicar o Geogebra na solução dos problemas.

Solução: Tem solução inteira, pois $(3,4) = 1$ e 1 divide 20, pois $20 = 1 \cdot 20 + 0$. Assim, vamos encontrar a solução usando o Algoritmo de Euclides. Escrevemos a igualdade $4 = 1 \cdot 3 + 1$ ou ainda $1 = 1 \cdot 4 - 1 \cdot 3$. Multiplicando a igualdade por 20, obtemos $20 = 20 \cdot 4 - 20 \cdot 3$. Então, $x_0 = -20$ e $y_0 = 20$ é uma solução particular, e consequentemente



Exercício 19. Explique porque as equações podem ou não ter soluções inteiras, e caso tenham solução, encontrá-las.
a) $3X + 4Y = 20$.

Figura 1

b) $3X + 6Y = 7$.
Solução: Não tem solução inteira, pois $(3,6) = 3$ e 3 não divide 7, pois podemos usar o Algoritmo de Euclides e escrever $7 = 3 \cdot 2 + 1$. Aqui $x = -20 + 4 \cdot t$ e $y = 20 - 3 \cdot t$ para $t \in \mathbb{Z}$ é solução geral da equação. Tomando por exemplo $t = 5$ obtemos o ponto (0,5), e se $t = 6$ obtemos o ponto (4,2), que podem ser representados na Figura 1. podemos verificar que a equação não tem solução inteira. Mas devemos tomar cuidado, pois estamos visualizando apenas uma parte da representação da equação.

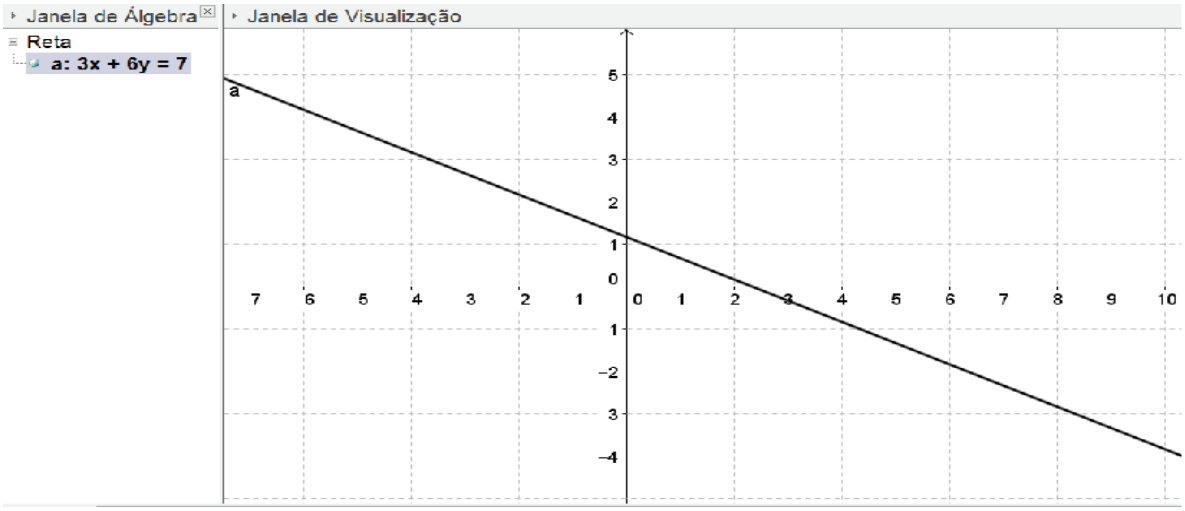


Figura 2

Exercício 20. (Euler) Divida 100 em 2 parcelas positivas, de modo que uma seja divisível por 7 e a outra por 11.

Solução. Já Sabemos que a solução para este problema é: $x = 8$ e $y = 4$, se $7X + 11Y = 100$. Agora vamos verificar usando Algoritmo de Euclides essa solução. De fato, fazendo 11 dividido por 7, obtemos $11 = 7 \cdot 1 + 4$. Agora, fazendo as outras divisões de 7 por 4, e de 4 por 3, temos $7 = 4 \cdot 1 + 3$ e $4 = 3 \cdot 1 + 1$. Substituindo uma igualdade na outra, temos

$1 = 4 + (-1) \cdot 3 = 4 + (-1) \cdot (7 + (-1) \cdot 4)) = 2 \cdot 4 + (-1) \cdot 7 = 2 \cdot (11 + (-1) \cdot 7) + (-1) \cdot 7 = 7 \cdot (-3) + 11 \cdot 2$, ou seja $1 = 7 \cdot (-3) + 11 \cdot 2$. Multiplicando esse resultado por 100, encontramos: $7 \cdot (-300) + 11 \cdot 200 = 100$. Assim uma solução particular é $x_0 = -300$ e $y_0 = 200$. Todas as soluções são: $x = -300 + 11t$ e $y = 200 - 7t$, com $t \in \mathbb{Z}$. Mas, como 100 é positivo, cada parcela deve ser positiva. Assim, $x = -300 + 11$, $t > 0$, ou seja, $t > 27...$ Logo, $t \geq 28$. Tomando $t = 28$, temos como solução $x = 8$ e $y = 4$. Na Figura 3 temos a representação da equação e de sua solução.

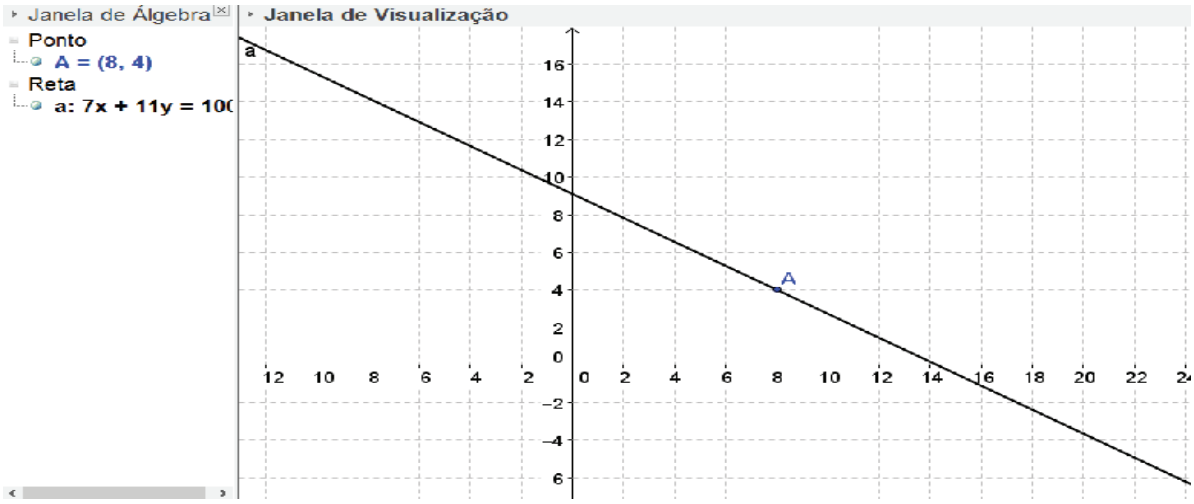


Figura 3.

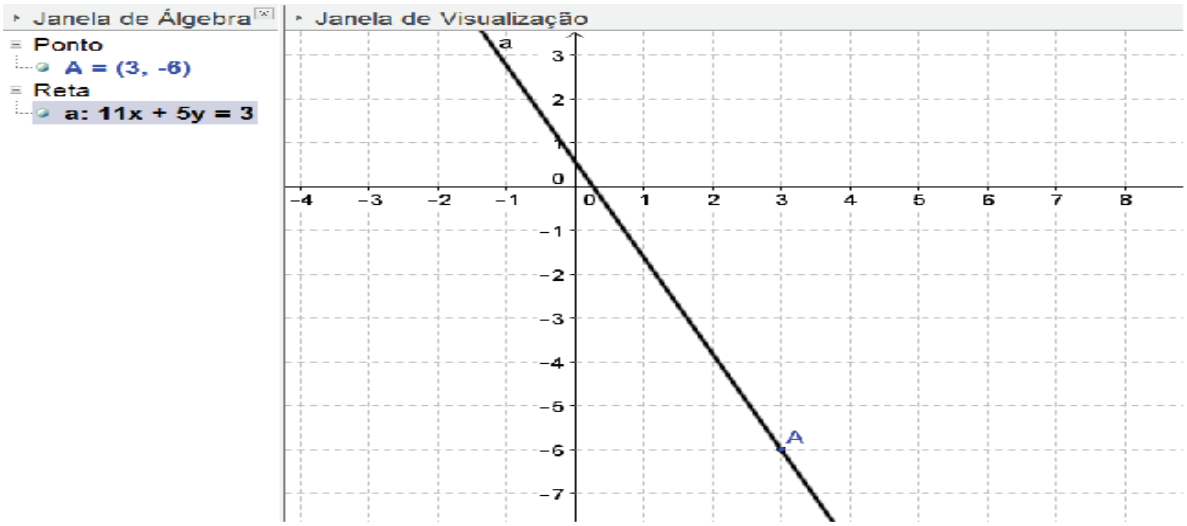


Figura 4

Exercício 21. Apenas com a utilização de dois relógios que só dão intervalos de tempo de 5 e de 11 minutos como podemos cozinhar um ovo durante 3 minutos?

Solução: Devemos encontrar as possíveis soluções para a equação $11X + 5Y = 3$. Como $(11,5) = 1$, podemos então encontrar essa solução iniciando pelo Algoritmo Euclides: $11 = 2 \cdot 5 + 1$. De onde escrevemos

$1 = 11 - 2 \cdot 5$. Assim, multiplicando por 3 obtemos $3 = 3 \cdot 11 - 6 \cdot 5$. Logo, uma solução será $x_0 = 3$ e $y_0 = -6$. Portanto, a solução para o problema será observar 6 intervalos de tempo no relógio que mostra o tempo a cada 5 minutos, e cozer o ovo até que o relógio que mostra o tempo a cada 11 minutos marque seu terceiro intervalo de tempo. Temos na Figura 4 a representação da equação e da sua solução.

Agradecimentos

Agradeço ao PROFMAT e a UEM por todo o incentivo durante o período de estudos.

Referências

BOYER, C. B. (1974) História da Matemática. Tradução: Elza F. Gomide. São Paulo. Editora Edgard Blücher.

BRASIL, Secretaria de Educação e Tecnologia do Ministério da Educação (2009). Parâmetros Curriculares Nacionais para o Ensino Médio. Brasília: SEMT/MEC, 1998. Ministério da Educação. Matriz de Referência para o ENEM. Brasília.

CAMPBELL, S.; ZAZKIS R. (2002) Toward Number Theory as a Conceptual Field. In: CAMPBELL, S., ZAZKIS, R. (org.). Learning and Teaching Number Theory. London: Ablex Publishing, 1-14p.

EVES, H., Introdução a História da Matemática. Tradução: Higyno H. Domingues. Editora Unicamp. Campinas-SP.

FILHO, E. A. (1985) Teoria Elementar dos Números. 3ª edição. Editora Livraria Nobel S. A. São Paulo – SP.

FROHLICH, A.; TAYLOR M. J. (1994) Algebric Number Theory. Cambridge studies in advanced mathematics 27. Cambridge University Press.

HEFEZ, A. (2005) Elementos da Aritmética. Rio de Janeiro. Sociedade Brasileira de Matemática.

KATZ, V. J. (2010) História da Matemática. Fundação Calouste Gulbenkian. Avenida de Berna. Lisboa.

LINS, R. C.; GIMENEZ J. (2005) Perspectivas em Aritmética e Álgebra para o século XXI. 5ª ed. Campinas-SP: Papirus.

MARINEZ, F. B, et al. (2011) Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro. Projeto Euclides. 2ª ed. Rio de Janeiro: IMPA.

NAGELL, T. (1972) Introduction to Number Theory. Chelsea Publishing Company, New York.

POMMER, W. M. (2008) Equações Diofantinas Lineares: Um desafio motivador para alunos do ensino médio. 153 f. Dissertação (Mestrado em Educação Matemática), Pontifícia Universidade Católica de São Paulo. São Paulo.

ROCQUE, G. DE LA; PITOMBEIRA, J. B. (1991) Uma Equação Diofantina e Suas Resoluções. Revista do professor de Matemática, São Paulo. V. 19, p. 39-47.

ROSEN, K. H. (2009) Matemática Discreta e Suas Aplicações. 6ª ed. McGraw-Hill Interamericana do Brasil. São Paulo – SP.

SANTOS, J. P. de O. (2012) Introdução a Teoria dos Números. Coleção Matemática Universitária. Impa. 3ª edição. Rio de Janeiro.