UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

EQUAÇÕES DIOFANTINAS: UM PROJETO PARA A SALA DE AULA E O USO DO GEOGEBRA

DISSERTAÇÃO DE MESTRADO - PROFMAT

ALEXANDRE HUNGARO VANSAN

MARINGÁ
2014

EQUAÇÕES DIOFANTINAS: UM PROJETO PARA A SALA DE AULA E O USO DO GEOGEBRA

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Alexandre Hungaro Vansan e aprovada pela comissão julgadora.

Banca Examinadora:

1. Prof. Dr. Josiney Alves de Souza (ORIENTADOR) (DMA/UEM)
2. Prof. Dr. Simão Nicolau Stelmastchuk (UNESPAR – União da Vitória)
3. Prof. Dr. Fábio Matheus Amorin Natali (DMA/UEM)

Dissertação apresentada ao Centro de Ciências Exatas, Departamento de Matemática, UEM, como requisito parcial para obtenção do Título de Mestre em Matemática.

ALEXANDRE HUNGARO VANSAN

EQUAÇÕES DIOFANTINAS: UM PROJETO PARA A SALA DE AULA E O USO DO GEOGEBRA

Trabalho de Conclusão de Curso, apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como parte dos requisitos necessários para a obtenção do título de Mestre em Matemática tendo a Comissão Julgadora composta pelos membros:

COMISSÃO JULGADORA:

Josiney Alves de Souza

Prof. Dr. Josiney Alves de Souza
DMA/Universidade Estadual de Maringá (Presidente)

Simão Nicolau Stelmastchuk

Prof. Dr. Simão Nicolau Stelmastchuk
Universidade Estadual do Paraná – União da Vitória - PR

Prof. Dr. Fábio Matheus Amorin Natali
DMA/Universidade Estadual de Maringá

Aprovada em: 24 de fevereiro de 2014.
Local de defesa: Auditório do Departamento de Matemática do Centro de Ciências Exatas, Bloco F67, campus da Universidade Estadual de Maringá.

"PREPARAR OS CAMINHOS, E TAMBÉM AS NOSSAS VIDAS,

É PRÓPRIO DE DEUS, DO AMOR DE DEUS PARA CADA UM DE NÓS"

(PAPA FRANCISCO)

Agradecimentos

Agradeço a Deus por tudo que esta fazendo em minha vida.

Agradeço a meus pais pela educação e pelo encaminhamento profissional.

Agradeço a minha esposa Veridiana Oliveira de Souza por todo o amor e companheirismo durante o período de Mestrado.

Agradeço a todos os professores do PROFMAT que me repassaram conhecimentos por todos os níveis do processo de ensino-aprendizagem.

Agradeço ao professor Doutor Josiney Alves de Souza pela orientação no trabalho.

Agradeço aos professores Simão Nicolau Stelmastchuk (UNESPAR – União da Vitória) e Fábio Matheus Amorin Natali (DMA/UEM) que, participando da banca examinadora, contribuíram de modo significativo para a conclusão desse trabalho.

Agradeço a CAPES pelo necessário e suficiente financiamento de todo o curso.

Resumo

O estudo de Teoria dos Números visa aqui nesta dissertação 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, e as Equações Diofantinas de Segunda Ordem da forma $x^2 + y^2 = z^2$, conhecidas por Ternas Pitagóricas. 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 ele poderá encontrar sugestões de atividades que poderá aplicar em sala de aula, ou até mesmo incluir em seu plano de aula as Equações Diofantinas, já que aqui ele encontrará uma sugestão de plano de trabalho docente para incluir em suas aulas.

Palavras-chaves: Equações Diofantinas. Teoria dos Números. Múltiplos. Divisores. Ternas Pitagóricas.

Abstract

The study of Theory of Numbers here in this dissertation aims to study some properties of integer multiples or divisors , emphasizing issues related to divisibility. Which will be of great importance for studies on the Diophantine equations, which in turn provide applications for use 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 whole numbers, and Diophantine Equations of Second Order in the manner $x^2 + y^2 = z^2$, known to Pythagorean Tender. 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 he can find suggestions for activities that you can apply in the classroom, or even include in their 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. Divisors. Pythagorean Tender.

Sumário

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 [2].

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 [3] afirmam que a Teoria dos Números não estuda apenas tópicos básicos e usuais (números naturais e inteiros, divisores, multiplos, mmc e mdc), como a maioria dos alunos pensam e aprendem, mas tembém incluem tópicos algébricos. A grande maioria dos problemas de Teoria dos Números não envolvem 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 a Teoria Elementar dos Números e buscar aplicações em problemas de sala de aula.

No capitulo 1 "História de Diofante", apresentamos um breve apanhado histórico sobre Diofante e como se iniciou seu trabalho sobre as equações que levam seu nome. O pioneirismo de Diofante se dá na criação de formas de expressão, passsando 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. Aqui serão enunciados e resolvidos dois problemas originais de seu livro "Arithmetica", que mostram através de exemplos numéricos a solução de problemas algébricos.

No capitulo 2 referente à "Tópicos de Teoria dos Números"vamos enunciar e demonstrar alguns resultados de Teoria dos Números, referente a múltiplos, divisores, máximo divisor comum, mínimo múltiplo comum, Algoritmo de Euclides (também chamado de algoritmo da divisão), números primos, entre outros, os quais serão de grande importância para que o leitor possa compreender algumas demonstrações que envolverão a teoria referente as Equações Diofantinas. Este capitulo servirá de apoio teórico para que o professor possa retomar no ensino médio conteúdos fundamentais da Matemática pertencentes ao ensino fundamental, e que ele (professor) possa ter um apoio científico que o ajudará em sala de aula.

No capitulo 3 definimos as Equações Diofantinas e Equações Diofantinas Lineares, que em resumo são equações que apresentam coeficientes e soluções no conjunto dos números inteiros. Iremos demonstrar os principais resultados que as envolve e apresentar problemas e soluções pertinentes a essas equações, que poderão ser desenvolvidos em sala de aula. O trabalho não discutirá a solução de uma Equação Diofantina geral, pois não existe uma forma de fazer isso, o que faremos é apresentar as equações Diofantinas Lineares e no capítulo 4 apenas um tipo de Equação Diofantina de Ordem Superior (Ternas Pitagóricas).

As Equações Diofantinas de ordem superior vão estar no capítulo 4, onde discutiremos como encontrar algumas soluções para as Ternas Pitagóricas de modo acessível para qualquer estudante do Ensino Médio.

O capítulo 5 "Projeto de Aplicação em Sala"contará com sugestões de planos de aula, onde cada plano constará de encontros que poderão ser feitos em sala de aula, ou em forma de projeto. Neste capítulo o professor encotrará uma sequência de como aplicar a teoria em sala de aula, além apresentar sugestões de atividades e de suas soluções que poderão ser utilizados pelos professores, e a utilização do software Geogebra para encontrar ou verificar as soluções dos exercícios.

Capítulo 1

História de Diofante

Segundo Boyer [1] 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, 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 abrupta 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.. Nesta coleção encontramos o seguinte problema sobre a vida de Diofante:

"Viajante! Aqui estão as cinzas de Diofanto. É milagroso que os números possam medir a extensão da sua vida. Um sexto dela foi uma bela infância. Depois de 1/12 da sua vida, a sua barba cresceu. Um sétimo da sua vida passou-se num casamento sem filhos. Mas, cinco anos após isso, nasceu o seu primeiro filho. Que viveu uma vida feliz durante apenas metade do tempo de vida do seu pai. E, em profundo pesar, o pobre velho terminou os seus dias na Terra, quatro anos após perder o seu filho".

Todas as referências históricas Boyer [1], Katz [8] e Eves [4] 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 [13], 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 como dito anteriormente, 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 (infelizmente apenas seis livros resistiram ao tempo e as guerras), contendo mais de cem problemas algébricos e suas soluções numéricas (equações algébricas) e teoria dos números, com soluções detalhadas. 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 [8], 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 [7]).

A Arithmética não é um trabalho sobre teoria das operações algébricas, ou funções algébricas ou ainda a resolução de equações algébricas, mas é 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. Cria símbolos para representar potências ao quadrado, ao cubo, a quarta potência (onde ele chama de quadrado-quadrado), a quinta potência (quadrado-cubo) e sexta potência (cubo-cubo).

Lins e Gimenez [9] 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. Vamos exemplificar o método de Diofante, trazendo algumas de suas soluções, encontradas em Katz [8].

Exemplo 1.1 *Livro 1 - Problema 1 - Dividir um dado número em dois, tendo uma dada diferença.*

Solução: Diofante, em seu livro, traz uma solução em que o dado número é 100 e a diferença é 40. Tomando x como o menor dos números da solução, temos $2x + 40 = 100$, logo $x = 30$, e os números que obtemos são 30 e 70. Poderíamos também ter escolhido y como sendo o maior dos dois números da solução, então $2y - 40 = 100$, e teríamos $y = 70$, com a mesma solução 30 e 70. Diofante tomou números dados, mas esse método funciona para qualquer par de números. Se tomarmos a como sendo a solução e $b < a$ a diferença dada, então a equação será $2x + b = a$, e os números serão $\frac{a-b}{2}$ e $\frac{a+b}{2}$.

Exemplo 1.2 *Livro 1 - Problema 5 - Dividir um dado número em dois tais que dadas frações (não a mesma) de cada número, quando somadas, dão um dado número.*

Solução: Diofante em sua solução normalmente toma frações unitárias. Ele percebe que, neste problema, é necessário que $\frac{1}{s}a < b < \frac{1}{r}a$, onde u e v são soluções tais que $u + v = a$, $\frac{1}{r}u + \frac{1}{s}v = b$. Ele apresenta a solução no caso em que $a = 100$, $b = 30$, $r = 3$ e $s = 5$. Seja a segunda parte (de 100), $5x$. Então, a primeira parte é $3(30 - x)$. Assim, $90 + 2x = 100$ (veio de $3(30 - x) + 5x = 100$) e $x = 5$. Logo, as partes pedidas são 75 e 25. Esse método funciona também para qualquer escolha que satisfaça a desejada condição. Diofanto toma a sua incógnita $\frac{1}{5}$ da segunda parte. Evitando frações no resto do seu cálculo, porque $\frac{1}{3}$ da primeira parte deve então igualar $30 - x$ e a primeira parte deve ser $3(30 - x)$. Para testar a generalidade tomamos sx como sendo a segunda parte de a e $r(b - x)$ a primeira. A equação passa a ser $sx + r(b - x) = a$ ou $br + (s - r)x = a$. Donde encontramos a solução geral $x = \frac{(a - br)}{(s - r)}$. Como x deve ser positivo $a - br > 0$ ou $b < \frac{1}{r}a$. Como $s(\frac{a - br}{s - r}) < a$ deve acontecer, temos que $\frac{1}{s}a < b$, satisfazendo as duas condições que Diofanto exigiu.

Antes mesmo que Diofanto escrevesse sobre equações do tipo $ax+by = c$ e $x^2+y^2 = z^2$, os babilônios já tinham escritos esse assunto. E o matemático hindu Brahmagupta (628 d.C.), ao contrário de Diofanto, deu todas as soluções inteiras da Equação Linear Diofantina (Boyer [1]). Os trabalhos que Diofanto escreveu serviram de inspiração para muitos matemáticos da Renascença ou contemporâneos a ela, incluído al-Karaji, Rafael Bombelli, e Pierre de Fermat, o qual chegou a vários resultados que Diofante só sugerira. Um fato importente é que os trabalhos de Diofante eram exclusivamente uma análise de problemas, diferentemente de outros autores, como Euclides, que tinha seu trabalho puramente sintético.

Capítulo 2

Tópicos de Teoria dos Números

Neste capítulo 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 as Equações Diofantinas. Todos essas definições, proposições e teoremas tiveram como referências Hefez [7], Filho [5], Frohlich e Taylor [6], Martinez [10], Lins e Gimenez [9] e Santos [15].

2.1 Divisibilidade

Como a divisão de um número inteiro por outro nem sempre é possível, vamos expressar essa possíbilidade 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 2.1 *(Princípio da Boa Ordem) Todo conjunto não vazio de inteiros positivos possui um elemento minimo.*

Axioma 2.1 *(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 2.2 *(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 $a \nmid b$.*

Exemplo 2.1 *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 2.1 *(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 $b < 0$, a prova termina. □

Teorema 2.2 *(Algoritmo de Euclides) Sejam a e b dois números inteiros com $a \neq 0$. Existem e são únicos dois números inteiros q e r tais que $b = a \cdot q + r$ com $0 \leq r < |a|$.*

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 $r = r_1$. □

Exemplo 2.2 *O resto da divisão de 10^n por 9 é sempre 1, para todo $n \in \mathbb{N}$.*

Solução: Vamos mostrar por indução.

Para $n = 1$ temos que $10 = 9 \cdot 1 + 1$, onde $r = 1$.

Supomos agora que 10^n dividido por 9 tem resto 1, ou seja, $10^n = 9 \cdot q + 1$. Provemos agora que o resultado é válido para $n + 1$. De fato, consideremos a igualdade

$10^{n+1} = 10 \cdot 10^n =$

$(9 + 1) \cdot 10^n =$

$9 \cdot 10^n + 1 \cdot 10^n =$

$9 \cdot 10^n + 9 \cdot q + 1 =$

$9 \cdot (10^n + q) + 1.$

Como $(10^n + q) \in \mathbb{Z}$, concluímos que 10^n dividido por 9 tem resto 1, para todo $n \in \mathbb{N}$.

Exemplo 2.3 *Encontrar os múltiplos de* 5 *que se encontram entre* 1 *e* 386*.*

Solução: Pelo Algoritmo de Euclides temos que $386 = 5 \cdot 77 + 1$, ou seja, o maior múltiplo de 5 que cabe em 386 é $5 \cdot 77$, onde 77 é o quociente da divisão de 386 por 5.

Portanto, os múltiplos de 5 entre 1 e 386 são: $1 \cdot 5, 2 \cdot 5, 3 \cdot 5, ..., 77 \cdot 5$ que são 77 números.

2.2 Máximo Divisor Comum

Os resuldados 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 2.3 *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 2.4 *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 2.3 *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 2.4 *(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 $d = (a, b)$. □

Definição 2.5 *Um número d é dito um máximo divisor comum de $a_1, a_2, a_3, ..., a_n$ se satisfaz as seguintes propriedades:*

i) d é um divisor comum de $a_1, a_2, a_3, ..., a_n$.

ii) Se c é um divisor comum de $a_1, a_2, a_3, ..., a_n$, então $c|d$.

Neste caso, denota-se $(a_1, a_2, a_3, ..., a_n)$.

Proposição 2.5 *Dados números inteiros $a_1, a_2, a_3, ..., a_n$, não nulos, existe o seu mdc e $(a_1, a_2, a_3, ..., a_n) = (a_1, a_2, a_3, ..., (a_{n-1}, a_n))$.*

Demonstração: Para demonstrar essa propriedade, vamos usar indução. Inicialmente para $n = 2$ temos $(a_1, a_2) = (a_1, (a_1, a_2)) = (a_1, a_2)$.

Suponhamos que para algum $n \geq 2$, tenhamos, $(a_1, ..., a_n) = (a_1, ..., (a_{n-1}, a_n))$, e provemos que esta é válida para $n + 1$. Seja $d = (a_1, ..., a_{n-1}, (a_n, a_{n+1}))$. Logo, $d|a_1, ..., d|a_{n-1}, d|(a_n, a_{n+1})$. Portanto, $d|a_1, ..., d|a_{n-1}, d|a_n$. Por outro lado, seja c um divisor comum de $a_1, a_2, a_3, ..., a_n, a_{n+1}$, logo, c é um divisor comum de $a_1, a_2, a_3, ..., a_{n-1}$ e (a_n, a_{n+1}). Portanto, $c|d$, e consequentemente

$d = (a_1, ..., a_n, a_{n+1})$. □

Teorema 2.6 *(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 $d|c$. O que implica que $d \leq c$ (ambos positivos) e como $d < c$ não é possível, pois d é o máximo divisor comum, comcluímos que $d = c = n_0 \cdot a + m_0 \cdot b$. □

Proposição 2.7 *Para todo inteiro* $t > 0$, $(t \cdot a, t \cdot b) = t(a, b)$.

Demonstração: Pelo Teorema de Bezout (Teorema 2.6) $(t \cdot a, t \cdot b)$ é o menor valor positivo de $m \cdot t \cdot a + n \cdot t \cdot b$ (m e n inteiros) o qual é igual a t vezes o menor valor positivo de $m \cdot a + n \cdot b$. Logo, $(t \cdot a, t \cdot b) = t \cdot (a, b)$. □

Proposição 2.8 *Se* $c > 0$ *e* a *e* b *são divisíveis por* c, *então* $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot (a, b)$.

Demonstração: Como a e b são divisíveis por c, temos que $\frac{a}{c}$ e $\frac{b}{c}$ são inteiros. Então basta substituir a por $\frac{c}{c}$ e b por $\frac{b}{c}$ na proposição anteiror e tomar $t = c$. □

Corolário 2.9 *Se* $(a, b) = d$ *então* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Teorema 2.10 *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 2.2 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 2.2 $d|(b + a \cdot x)$ 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 2.11 *Se $a|b \cdot c$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Como $(a, b) = 1$ e pelo Teorema de Bezout (Teorema 2.6) existem inteiros n_0 e m_0, tais que $n_0 \cdot a + m_0 \cdot b = 1$. Multiplicando os dois lados dessa igualdade por c, obtemos: $n_0 \cdot (a \cdot c) + m_0 \cdot (b \cdot c) = c$. Como $a|a \cdot c$ e $a|b \cdot c$ temos que $a|c$. □

Teorema 2.12 *Sejam a, b inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração: Pelo Teorema 2.10, da relação $a = q \cdot b + r$, obtemos $(a, b) = (b, a - q \cdot b) = (b, r)$. □

2.3 Algoritmo de Euclides

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

Teorema 2.13 *(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 $a > r_1 > r_2 > r_3 > ...$, 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 $(a, b) = r_n$. $\square$

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 possivel temos:

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

Exemplo 2.4 *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:

$2 = 170 \cdot 1 - 12 \cdot 14 =$

$170 \cdot 1 - (182 - 170 \cdot 1) \cdot 14 =$

$170 \cdot 15 - 182 \cdot 14 =$

$(352 - 182 \cdot 1) \cdot 15 - 182 \cdot 14 =$

$352 \cdot 15 - 182 \cdot 29.$

Exemplo 2.5 *Calcular o mdc entre* 210 *e* 300*.*

Usando o procedimento do Algoritmo de Euclides, obtemos

-	1	2	3
300	210	90	**30**
90	30	0	

Logo, o $mdc(300, 210) = 30$.

2.4 Números Primos

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

Definição 2.6 *Dois números naturais a e b são ditos primos entre si, ou coprimos, se* $(a, b) = 1$*.*

Definição 2.7 *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.*

Exemplo 2.6 *O número inteiro 7 é primo porque seus fatores positivos são 1 e 7. Já o número 9 é composto, pois é dividido por 3.*

Teorema 2.14 *(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 minimo 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

$\dfrac{n}{p_1} = p_2 \cdots p_m = q_2 \cdots q_{m'}$

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. □

Exemplo 2.7 *As fatorações em primos dos números* 200, 551, 641, 999 *e* 512, *são dadas por:*

$$\begin{aligned}
&200 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 2^3 \cdot 5^2\\
&551 = 19 \cdot 29\\
&641 = 641\\
&999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37\\
&512 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^9
\end{aligned}$$

2.5 Mínimo Múltiplo Comum

A seguir definimos mínimo múltiplo comum, e apresentamos alguns resultados que serão base para o projeto.

Definição 2.8 *Um número m é um mínimo múltiplo comum (mmc) de a e b, com $a,\ b,\ m \in \mathbb{Z}$, se possuir as seguintes propriedades:*

a) m é um múltiplo comum de a e b;

b) Se c é um múltiplo comum de a e b, então $m | c$.

Se m é o mmc de a e b segue que $m \leq c$, para qualquer múltiplo comum c de a e b. Logo, m é o menor entre os múltiplos comuns de a e b, e será denotado por $[a, b]$, ou ainda por mmc(a, b) que é mais usado na educação básica.

Teorema 2.15 *Dados dois múmeros $a, b \in \mathbb{Z}_*$ (números inteiros diferentes de zero), existe o mmc $[a, b]$ e temos que $[a, b] \cdot (a, b) = a \cdot b$.*

Demonstração: Ponhamos $m = \dfrac{a \cdot b}{(a, b)}$. Como

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

temos que $a|m$ e $b|m$.

Agora, seja $c \in \mathbb{Z}$, um múltiplo comum de a e b. Logo, $c = n \cdot a = n_1 \cdot b$. Segue daí que

$$n \cdot \frac{a}{(a, b)} = n_1 \cdot \frac{b}{(a, b)}.$$

Como $\dfrac{a}{(a, b)}$ e $\dfrac{b}{(a, b)}$ são primos entre si, segue-se que $\dfrac{a}{(a, b)}$ divide n_1, e, portanto, $m = \dfrac{a}{(a, b)} \cdot b$ divide $n_1 \cdot b$ que, é igual a c. □

Definição 2.9 *Um número m é o mmc de $a_1, ..., a_n$ se m é múltiplo comum entre $a_1, ..., a_n$ e se c é um múltiplo de $a_1, ..., a_n$ então $m|c$.*

Aplicando o processo de indução a partir da existência do mmc de a_1 e a_2, mostra-se que o $[a_1, ..., a_n]$ existe e pode ser calculado recursivamente $[a_1, ..., a_n] = [[a_1, a_2], ..., a_n]$.

Corolário 2.16 *Se a e b são números primos entre si, então $[a, b] = |a \cdot b|$.*

Demonstração: Segue imediantamente do último teorema. □

Proposição 2.17 *Sejam $a, b, c \in \mathbb{N}$. Mostre que $[a, b, c] = \dfrac{a \cdot b \cdot c}{(a \cdot b, a \cdot c, b \cdot c)}$.*

Demonstração: Note que

$$[a, b, c] \cdot (a \cdot b, a \cdot c, b \cdot c) =$$

$$[a, [b, c]] \cdot ((a \cdot b, a \cdot c), b \cdot c) =$$

$$\frac{a \cdot [b,c]}{(a,[b,c])} \cdot (a \cdot (b,c), b \cdot c) =$$
$$\frac{a[b,c]}{(a,[b,c]} \cdot (a(b,c),[b,c](b,c)) =$$
$$\frac{a \cdot [b,c]}{(a,[b,c])} \cdot (b,c) \cdot (a,[b,c]) =$$
$$a \cdot [b,c] \cdot (b,c) =$$
$$a \cdot b \cdot c.$$

Portanto, obtemos o resultado. □

Proposição 2.18 *Sejam a e b não identicamente nulos. Então $(a,b) = [a,b]$ se, e somente se $a = b$.*

Demonstração: Se $(a,b) = [a,b] = d$, então existem $p, q, x, y \in \mathbb{N}$ tais que $a = x \cdot d$, $b = y \cdot d$ e $d = q \cdot a = p \cdot b$. Daí, $b = y \cdot q \cdot a$ implica que $a|b$ e $a = x \cdot p \cdot b$ implica que $b|a$. Logo, se $a|b$ e $b|a$ temos que $a = b$.

Se $a = b$ então $(a,b) = (a,a) = a = [a,a] = [a,b]$. □

Capítulo 3

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-lás em sala que o professor trabalhará alguns conteúdos referentes a Teoria dos Números. O conteúdo a seguir será baseado nas referências Hefez [7], Filho [5], Lins e Gimenez [9], Santos [15] e Nagell [11].

3.1 Equações Diofantinas Lineares

Vamos iniciar essa seção com a definição de Equação Diofantina Linear, e seguiremos com resultados de grande utilidade para o desenvolvimento de sua teoria.

Definição 3.1 *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 3.1 *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* $Y = -6$*.*

Exemplo 3.2 *Existem Equações Diofantinas Lineares com duas incógnitas que não tem solução. Por exemplo, a equação* $2X + 4Y = 7$ *não tem solução, pois* $2X + 4Y$ *é um* *inteiro par quaisquer que sejam os valores inteiros de X e Y, enquanto que 7 é um número inteiro ímpar.*

Proposição 3.1 *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 2.6). O que implica $c = dt = (aX_0 + bY_0)t = a(tX_0) + b(tY_0)$, isto é, o par de inteiros $X = tX_0 = \frac{c}{d}X_0$ e $Y = tY_0 = \frac{c}{d}Y_0$ é uma solução da equação $aX + bY = c$. □

OBS: A equação $aX + bY = c$ pode ser reduzida para a forma $\frac{a}{(a,b)}X + \frac{b}{(a,b)}Y = \frac{c}{(a,b)}$. Note que $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$. Assim, é suficiente estudar as equações $aX + bY = c$, com $(a, b) = 1$.

Definição 3.2 *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 3.2 *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 3.3 *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 seguinte 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 tráz 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.

Exemplo 3.4 *Determinar o menor número natural que tem restos* 11 *e* 35 *quando dividido, respectivamente, por* 37 *e* 48*.*

Se chamarmos de N esse número natural, podemos representar esse problema por:

$$N = 37 \cdot X + 11 \text{ e } N = 48 \cdot Y + 35.$$

Donde obtemos: $37X + 11 = 48Y + 35$ implica que $37X - 48Y = 24$ implica que $48Y - 37X = -24$.

Usando o Algoritmo de Euclides.

Dividindo 48 por 37, obtemos a seguinte igualdade:

$$48 = 37 \cdot 1 + 11.$$

Agora, dividindo 37 por 11 (resto na igualdade anterior), temos

$$37 = 11 \cdot 3 + 4.$$

E seguindo o mesmo procedimento, encontramos

$$11 = 4 \cdot 2 + 3$$

e

$$4 = 3 \cdot 1 + 1.$$

Logo, substituindo as igualdades anteriores de tráz pra frente,

$1 = 4 - 3 =$

$4 - (11 - 4 \cdot 2) =$

$4 \cdot 3 - 11 \cdot 1 =$

$3 \cdot (37 - 11 \cdot 3) - 11 \cdot 1 =$

$37 \cdot 3 - 11 \cdot 10 =$

$37 \cdot 3 - (48 - 37 \cdot 1) \cdot 10 =$

$-48 \cdot 10 + 37 \cdot 13.$

Agora, multiplicando a igualdade por -24, temos

$-24 = 48 \cdot 240 - 37 \cdot 312.$

Assim, $X_0 = 312$ e $Y_0 = 240$.

Portanto, $N = 37 \cdot X + 11 \implies N = 37 \cdot 312 + 11 = 11555$, que é o número procurado.

Proposição 3.3 *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 a divisão euclidiana, 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

$0 = na + mb - n_1a - m_1b = mb - m_1b = b(m - m_1)$,

o que implicaria $m - m_1 = 0$, e portanto $m = m_1$.

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

$0 = na - mb - (n_1a - m_1b) = -(mb + m_1b) = b(-(m + m_1))$,

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

Proposição 3.4 *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 3.4 *Definimos o conjunto das lacunas de $S(a, b)$ como sendo o conjunto $L(a, b) = \mathbb{N} \setminus S(a, b)$.*

Corolário 3.5 *Temos que $L(a, b) = \{na - mb \in \mathbb{N};\ n, m \in \mathbb{N},\ n < b\}$.*

Teorema 3.6 *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. $\square$

Proposição 3.7 *Suponha que a equação $aX + bY = c$, com $(a, b) = 1$, tenha soluçã o 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 que $x = n + tb$. E fazendo a substituição obtemos $m - y = ta$. Como queríamos demonstrar. $\square$

Exemplo 3.5 *Determinar para quais valores de $c \in \mathbb{N}$ a equação $11X + 7Y = c$ tem soluções em $n \in \mathbb{N}$.*

O conjunto das lacunas de $S(11, 7)$ é o conjunto

$$L(11, 7) = \{(n11 - m7) \in \mathbb{N};\ n, m \in \mathbb{N}, n < 7\}.$$

Agora, encontrando os valores de m obtemos:

Se $n = 1$ então $(1 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1$.

Se $n = 2$ então $(2 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1, 2, 3$.

Se $n = 3$ então $(3 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1, 2, 3, 4$.

Se $n = 4$ então $(4 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1, 2, 3, 4, 5, 6$.

Se $n = 5$ então $(5 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1, 2, 3, 4, 5, 6, 7$.

Se $n = 6$ então $(6 \cdot 11 - m7) \in \mathbb{N}$ se $m = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

Assim, o conjunto das lacunas é $L(11, 7) = \{1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, 16, 17, 19, 20, 23, 24, 2$

Portanto, a equação $11X + 7Y = c$ admite solução em $\mathbb{N} \cup \{0\}$ se, e somente se $c \notin L(11, 7)$.

CAPÍTULO 4

Equações Diofantinas de Ordem Superior

Equações Diofantinas de Ordem Superior são equações algébricas de grau maior ou igual a dois com solução no conjunto dos números inteiros. Neste capítulo vamos estudar as Equações Diofantinas de Segunda ordem na forma $x^2 + y^2 = z^2$, as quais são chamadas Ternas Pitagóricas. Tais equações serão definidas nas próximas páginas e servirão para aplicações que os professores podem fazer em sala de aula. Para este capítulo usamos como referências Filho [5].

4.1 Equações Diofantinas de Segunda Ordem

Pitágoras e seus seguidores ligaram os números inteiros à geometria e, dessa forma, iniciaram a Teoria dos Números. Por volta de 1700 a.C. foram encontradas, na Babilônia, tabelas contendo listas de ternas de números inteiros com a propriedade de que um dos números quando elevado ao quadrado era igual á soma dos quadrados dos outros dois. Existem registros que mostram a existência e uso destas tabelas no Egito antigo. Os Pitagóricos estavam interessados nos triângulos retângulos cujos catetos têm comprimento inteiro x e y e o comprimento z da hipotenusa também é inteiro, e se relaciona com x e y de modo que $x^2+y^2 = z^2$. Procurar todos os inteiros positivos que satisfazem o Teorema de Pitágoras é o mesmo que determinar todos os triângulos retângulos que têm lados com medidas interias. Por volta de 600 a.C., os pitagóricos foram os primeiros a criar métodos para determinar ternas desse tipo, as quais receberam o nome de Ternas Pitagóricas. Platão (430 até 349 a.C.) também encontrou formas de determinar tais ternas (somatematica [16]).

Neste capítulo vamos demonstrar que algumas dessas ternas podem ser encontradas através de fórmulas de fácil compreensão, e também verificar que tais ternas são infinitas, ou seja, vamos estudar as soluções (x, y, z) da equação $X^2 + Y^2 = Z^2$, com $x, y, z \in \mathbb{Z}$

diferentes de zero. Iniciamos com a definição de Ternas Pitagóricas, e apresentamos os primeiros resultados.

Definição 4.1 *As triplas de números inteiros positivos* (x, y, z) *que satisfazem a equação* $X^2+Y^2 = Z^2$ *são denominadas Triplas ou Ternas Pitagóricas, já que correspondem aos comprimentos dos lados de um triângulo retângulo de lados inteiros pelo Teorema de Pitágoras.*

Exemplo 4.1 *São Ternas Pitagóricas:* $(3, 4, 5)$, $(5, 12, 13)$ *e* $(12, 35, 37)$, *pois*

$3^2 + 4^2 = 9 + 16 = 25 = 5^2$,

$5^2 + 12^2 = 25 + 144 = 169 = 13^2$ *e*

$12^2 + 35^2 = 144 + 1225 = 1369 = 37^2$.

Definição 4.2 *Chama-se Terna Pitagórica primitiva toda Terna Pitagórica* (x, y, z) *tal que* $mdc(x, y) = 1$. *Ou seja, Terna Pitagórica primitiva é toda terna tal que* x *e* y *são primos entre si.*

Proposição 4.1 *Se* (x, y, z) *é uma Terna Pitagórica, então* (cx, cy, cz), *em que* $c > 1$ *é um inteiro positivo qualquer, é uma Terna pitagórica.*

Demonstração: Basta tomarmos cx e cy no lugar de x e y, respectivamente na equação $X^2 + Y^2 = Z^2$, e verificamos o resultado da seguinte forma:

$(cx)^2 + (cy)^2 = c^2x^2 + c^2y^2 = c^2(x^2 + y^2) = c^2(z^2) = (cz)^2$. □

Exemplo 4.2 *Sabemos que* $(12, 35, 37)$ *é uma Terna Pitagórica. Se tomarmos* $c = 5$, *obtemos* $(60, 175, 185)$, *que é uma Terna Pitagórica, pois*

$60^2 + 175^2 = 3600 + 30625 = 34225 = 185^2$.

4.1.1 Fórmulas que fornecem Ternas Pitagóricas

Proposição 4.2 *As fórmulas de Pitágoras:*

$x = 2n + 1$, $y = 2n^2 + 2n$ *e* $z = 2n^2 + 2n + 1$,

em que n *é um inteiro positivo qualquer, são soluções da equação* $X^2 + Y^2 = Z^2$.

Demonstração: Vamos substituir os valores de x e y no lado esquerdo da equação pitagórica:

$x^2 + y^2 =$

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

$(4n^2+4n+1) + (4n^4+8n^3+4n^2) =$

$4n^4 + 8n^3 + 8n^2 + 1.$

Por outro lado, substituindo o valor de z, temos:

$z^2 =$

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

$4n^4 + 4n^3 + 2n^2 + 4n^3 + 4n^2 + 2n + 2n^2 + 2n + 1 =$

$4n^4 + 8n^3 + 8n^2 + 1.$

Portanto, temos o resultado. □

Exemplo 4.3 *Seja* $n = 8$, *temos* $x = 17$, $y = 144$ *e* $z = 145$, *que é uma terna pitagórica, pois*

$$17^2 + 144^2 = 289 + 20736 = 21025 = 145^2.$$

Proposição 4.3 *As fórmulas de Platão:*

$x = 2mn$, $y = m^2 - n^2$ *e* $z = m^2 + n^2$,

são soluções da equação $X^2 + Y^2 = Z^2$, *quando* m *e* n *são números inteiros positivos quaisquer e* $m > n$.

Demonstração: Basta substituirmos os valores na equação pitagórica:

$x^2 + y^2 =$

$(2mn)^2 + (m^2 - n^2)^2 =$

$(4m^2n^2) + (m^4 - 2m^2n^2 + n^4) =$

$m^4 + 2m^2n^2 + n^4.$

Por outro lado temos:

$z^2 =$

$(m^2 + n^2)^2 =$

$m^4 + 2m^2n^2 + n^4.$

Portanto, temos o resultado. □

Exemplo 4.4 *Tomando $m = 9$ e $n = 5$, temos $x = 56$, $y = 90$ e $z = 106$, que é uma Terna Pitagórica, pois*

$$56^2 + 90^2 = 3136 + 8100 = 11236 = 106^2.$$

Proposição 4.4 *As fórmulas:*

$x = \dfrac{n^2-1}{2}$, $y = n$ e $z = \dfrac{n^2+1}{2}$,

fornecem Ternas Pitagóricas com n inteiro positivo ímpar maior do que 1.

Demonstração: A hipótese de n ser ímpar e maior que 1, serve para garantirmos que x e y sejam números inteiros positivos, e $x \neq 0$. De fato, para x temos:

(i) Se n for um número par, da forma $2p$ com p um número natural diferente de 0, temos:

$\dfrac{n^2-1}{2}$ implica que $\dfrac{(2p)^2-1}{2} = \dfrac{4p^2-1}{2} = 2p^2 - \dfrac{1}{2}$,

que não é um número inteiro.

(ii) Se n for um número ímpar, da forma $2p+1$ com p um número natural diferente de 0, temos:

$\dfrac{n^2-1}{2}$ implica que $\dfrac{(2p+1)^2-1}{2} = \dfrac{(4p^2+2p+1)-1}{2} = p^2 + p$,

que é um número inteiro.

Agora, para z temos:

(i) Se n for um número par, da forma $2p$ com p um número natural diferente de 0, temos:

$\dfrac{n^2+1}{2}$ implica que $\dfrac{(2p)^2+1}{2} = \dfrac{4p^2+1}{2} = 2p^2 + \dfrac{1}{2}$,

que não é um número inteiro.

(ii) Se n for um número ímpar, da forma $2p+1$ com p um número natural diferente de 0, temos:

$\dfrac{n^2+1}{2}$ implica que $\dfrac{(2p+1)^2+1}{2} = \dfrac{(4p^2+2p+1)+1}{2} = p^2 + p + 1$,

que é um número inteiro.

Agora provaremos que as fórmulas fornecem ternas pitagóricas.

Primeiro, substituindo x e y na fórmula de Pitágoras:

$x^2+y^2 =$

$\dfrac{1}{4}(n^2-1)^2 + n^2 =$

$\frac{n^4}{4} - \frac{n^2}{2} + \frac{1}{4} + n^2 =$

$\frac{n^4}{4} + \frac{n^2}{2} + \frac{1}{4}.$

Por outro lado, substituindo z na fórmula de Pitágoras:

$z^2 =$

$\left(\frac{n^2+1}{2}\right)^2 =$

$\frac{n^4+2n^2+1}{4} =$

$\frac{n^4}{4} + \frac{n^2}{2} + \frac{1}{4}.$

Provando que as fórmulas fornecem Ternas Pitagóricas. □

Exemplo 4.5 *Seja $n = 13$, temos $x = 84$, $y = 13$ e $z = 85$, que é uma Terna Pitagórica, pois*

$$84^2 + 13^2 = 7056 + 169 = 7225 = 85^2.$$

Proposição 4.5 *Se (x, y, z) formam uma Terna Pitagórica não primitiva, isto é, $mdc(x, y) = d \neq 1$, então $d|z$, e os quocientes:*

$x_1 = \frac{x}{d}$, $y_1 = \frac{y}{d}$ *e* $z_1 = \frac{z}{d}$

formam uma Terna Pitagórica primitiva (x_1, y_1, z_1).

Demonstração: Temos que:

$(x_1)^2 + (y_1)^2 = \left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \frac{x^2+y^2}{d^2} = \frac{z^2}{d^2} = \left(\frac{z}{d}\right)^2 = (z_1)^2,$

com $mdc(x_1, y_1) = 1$, pois $mdc(x_1, y_1) = mdc\left(\frac{x}{d}, \frac{y}{d}\right) = \frac{1}{d}mdc(x, y) = \frac{1}{d}d = 1.$ □

Obs: De qualquer Terna Pitagórica não primitiva pode-se obter uma Terna Pitagórica Primitiva, multiplicando-se os seus elementos por um número convenientemente escolhido, número esse inteiro e positivo maior do que 1. Isto é, todas as soluções de $X^2 + Y^2 = Z^2$, resultam daquelas de $x_1^2 + y_1^2 = z_1^2$, onde $mdc(x_1, y_1) = 1$.

Teorema 4.6 *Para todo inteiro positivo $x > 2$, existem inteiros positivos y e z tais que (x, y, z) é uma Terna Pitagórica.*

Demonstração: Suponhamos primeiro que o inteiro $x > 2$ é par. Então, $2|x$ e $4|x^2$, de modo que

$$y = \frac{x^2 - 4}{4} \text{ e } z = \frac{x^2 + 4}{4}$$

são dois inteiros positivos. E como

$$x^2 + y^2 = x^2 + \frac{x^4 - 8x^2 + 16}{16} = \frac{x^4 + 8x^2 + 16}{16} = \left(\frac{x^2 + 4}{4}\right)^2 = z^2.$$

Segue-se que (x, y, z) é uma Terna Pitagórica.

Agora, suponhamos que $x > 2$ é ímpar. Então x é da forma $2k+1$, com $k \in \mathbb{N}$. Logo, as formas pitagóricas

$$x = 2n + 1,\ y = 2n^2 + 2n \text{ e } z = 2n^2 + 2n + 1,$$

dão a Terna Pitagórica (x, y, z). $\square$

Capítulo 5

Projeto de Aplicação em Sala

Nesse capítulo apresentaremos atividades que podem ser aplicadas em sala de aula com alunos do 9^o ano 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 [7], Filho [5], Lins e Gimenez [9], Santos [15], Rosen [14] e Nagell [11].

5.1 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 mmc (mínimo múltiplo comum), números primos, decomposição em fatores primos e Algoritmo de Euclides. Tais conceitos podem ser definidos da seguinte forma para os alunos:

Divisores Podemos utlizar a Definição 2.2 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 5.1 *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) $D(32) =\ 1,\ 2,\ 4,\ 8,\ 16,\ 32.$

Máximo Divisor Comum Usamos para definir Máximo Divisor Comum as Definições 2.3 e 2.4. Aqui, podemos introduzir uma simbologia, que servirá para facilitar a notação de mdc, que é (a, b). (Definição 2.4)

Exemplo 5.1 *Encontrar o Máximo Divisor Comum entre* 36 *e* 64*.*

Nesse exemplo o professor deverá lembrar que um dos caminho 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.

Divisão Euclidiana (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 $o \leq r < |a|$. Temos como referências os Teoremas 2.2, 2.4 e 2.13.

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 5.2 *Encontrar o quociente e o resto da divisão de* 330 *por* 20*.*

Solução: Efetuando a divisão de 330 por 20 obtemos quaciente 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 2.13. Tal processo pode ser encontrado na página 13.

Exemplo 5.3 *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 proceguimos 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.

Números Primos Para definir números primos, temos como referências as Definições 2.6 e 2.7 e o Teorema 2.14. Assim, os primeiros números primos são $\{2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ ...\}$, os quais são usados na fatoração dos números naturais.

Exemplo 5.4 *Escreva os números* 120, 300 *e* 220 *na forma de fatores primos.*

Solução:

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

$300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5^2.$

$220 = 2 \cdot 2 \cdot 5 \cdot 11 = 2^2 \cdot 5 \cdot 11.$

Múltiplo Um número inteiro a será chamado múltiplo de um número inteiro b diferente de zero, quando a for divisível por b ou b for divisor de a. Ou ainda, temos como referência a Definição 2.8.

Exemplo 5.5 *Quais são os 8 primeiros múltiplos dos números abaixo:*

Solução:

a) $M(6) = 0,\ 6,\ 12,\ 18,\ 24,\ 30,\ 36,\ 42.$

b) $M(30) = 0,\ 30,\ 60,\ 90,\ 120,\ 150,\ 180,\ 210,\ 240.$

Mínimo Múltiplo Comum Dados dois ou mais números inteiros não-nulos, denomina-se mínimo múltiplo comum desses números o menor de seus múltiplos comuns que seja diferente de zero. Ou ainda, temos como referência a Definição 2.8.

Exemplo 5.6 *Determinar o mmc entre* 50 *e* 32*.*

Solução:

O professor poderá seguir o mesmo modelo de Algoritmo que o aluno pratica desde os anos iniciais do Ensino Fundamental, usando o seguinte diagrama:

50	32	2
25	16	2
25	8	2
25	4	2
25	2	2
25	1	5
5	1	5
1	1	

Logo, o mmc entre 50 e 32 é o produto $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 = 800$.

5.2 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. As referências para a resolução dos exercícios estão na página 31.

Exercício 5.2 *Verifique:*

a) se 109 é divisível por 3.

Solução: Usando o Algoritmo de Euclides temos: $109 = 3 \cdot 36 + 1$. Em que 109 não é divisível por 3.

b) se 119 é divisível por 9.

Solução: Usando o Algoritmo de Euclides temos: $119 = 9 \cdot 13 + 2$. Em que 119 não é divisível por 9.

c) se 143 é divisível por 12.

Solução: Usando o Algoritmo de Euclides temos: $143 = 12 \cdot 11 + 11$. Em que 143 não é divisível por 12.

d) se 310 é divisível por 5.

Solução: Usando o Algoritmo de Euclides temos: $310 = 5 \cdot 62 + 0$. Em que 310 é divisível por 5.

Exercício 5.3 *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, basta encontrar os divisores de 60, e verificar 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 5.4 *Qual é o maior múltiplo de* 13 *menor que* 300*?*

Solução: Os primeiros múltiplos de 13 são: $m(13) = 0, 13, 26, 39, ...$ Mas, não precisamos procurar todos os múltiplos de 13 até chegar no 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, temos

$$299 = 23 \cdot 13 + 0.$$

Logo, 299 é o maior múltiplo de 13 menor que 300.

Exercício 5.5 *Achar os elementos do conjunto* $A = \{1, 2, 3, 4, 5\}$ *que são primos com* 8.

Solução: Os primos com 8 são aqueles que não têm fatores primos iguais aos fatores primos de 8. Como 8 só tem fator primo igual a 2 ($8 = 2^3$), e os únicos que não apresentam o fator 2 na decomposição são: 1, 3 e 5. Portanto, esses são os primos com 8.

Exercício 5.6 *O número* 173 *é um número primo?*

Solução: Aqui o professor deverá apresentar o resultado de que os divisores de um número inteiro positivo são menores que sua raiz quadrada. Para saber se 173 é primo, devemos primeiro procurar seus divisores. Assim, calculamos a raiz quadrada de 173 e obtemos $\sqrt{173} \cong 13,15$. Assim, vamos calcular os divisores de 173, até chegar no número 13.

Temos que $173 = 86 \cdot 2 + 1$, de onde verificamos que 2 não é divisor de 173.

Também temos que $173 = 57 \cdot 3 + 2$, de onde verificamos que 3 não é divisor de 173.

Fazendo 173 dividido por 5 temos que $173 = 34 \cdot 5 + 3$, de onde verificamos que 5 não é divisor de 173.

Continuando esse mesmo processo para outros números primos, temos que $173 = 24 \cdot 7 + 5$, de onde verificamos que 7 não é divisor de 173.

Para $173 = 15 \cdot 11 + 8$, verificamos que 11 não é divisor de 173.

E por fim, para $173 = 13 \cdot 13 + 4$, verificamos que 13 não é divisor de 173.

Portanto, não existem divisores de 173 diferentes de 1 e de 173, logo 173 é um número primo.

Exercício 5.7 *Decomponha o número* 234 *em fatores primos.*

Solução: Temos que $234 = 2 \cdot 3 \cdot 3 \cdot 13$ ou $234 = 2 \cdot 3^2 \cdot 13$.

O professor poderá também apresentar a fatoração da seguinte forma:

234	2
117	3
39	3
13	13
1	

Exercício 5.8 *A fatoração completa do número* 1200 *é* $2^a \cdot 3^b \cdot 5^c$. *Qual é o valor de* $a + b + c$*?*

Solução: Fatorando 1200 obtemos:

$1200 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^4 \cdot 3 \cdot 5^2$.

Ou ainda fatoramos usando o diagrama:

1200	2
600	2
300	2
150	2
75	3
25	5
5	5
1	

Logo, $a = 4$, $b = 1$ e $c = 2$. Portanto, $a + b + c = 4 + 1 + 2 = 7$.

Exercício 5.9 *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 comuns.

Exercício 5.10 *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 5.11 *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 5.12 *Vovó foi viajar com a Turma da Melhor Idade do bairro. Quantas pessoas haviam na viagem, se podemos contá-los de* 8 *em* 8 *ou de* 10 *em* 10*?*

Solução: Como as pessoas podem ser contadas em múltiplos de 8 e em múltiplos de 10, então para encontar o número de pessoas que viajaram, devemos procurar o minimo múltiplo comum entre 8 e 10. Assim, $[8, 10] = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5 = 40$, pois podemos calcular o mmc usando o diagrama:

8	10	2
4	5	2
2	5	2
1	5	5
1	1	

Logo, viajaram 40 pessoas.

Exercício 5.13 *Um relógio A bate a cada* 15 *minutos, outro relógio B bate a cada* 25 *minutos, e um terceiro relógio C bate a cada* 40 *minutos. Qual é, em horas, o menor intervalo de tempo decorrido entre duas batidas simultâneas dos três relógios?*

Solução: Como as batidas dos relógios são contadas em múltiplos de 15, 25 e 40 minutos, então para encontrar o intervalo entre duas batidas simultâneas dos três relógios basta calcular o minimo múltiplo comum entre os três valores. Assim, $[15, 25, 40] = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^3 \cdot 3 \cdot 5^2 = 600$, pois podemos calcular o mmc usando o diagrama:

15	25	40	2
15	25	20	2
15	25	10	2
15	25	5	3
5	25	5	5
1	5	1	5
1	1	1	

Portanto, temos 600 minutos de intervalo, ou ainda 10 horas.

Exercício 5.14 *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:

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

$D(24) = 1,\ 2,\ 3,\ 4,\ 6,\ 8,\ 12,\ 24.$

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 5.15 *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 5.16 *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 $mdc(357, 187)$

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 $mdc(153, 17)$

$153 = 17 \cdot 9$ implica que $mdc(153, 17) = 17$.

Portanto, o número é 17, usando o Teorema 2.13.

Exercício 5.17 *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 temos:

$mdc(4869, 4416)$

Dividindo 4896 por 4416, 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 $n = 48$.

5.3 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 do Números.

Encaminhamentos Metodológicos: Conceituar Equações Diofantinas 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.

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 conjuntos dos números inteiros (Definição 3.1). O professor deverá alertar o aluno com relação as 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.

Exercícios 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 5.18 *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) $15X + 27Y = 1$.

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 $y = 6$.

h) $15X - 51Y = 41$.

Solução: Não apresenta soluções inteiras.

i) $5X + 6Y = 1$.

Solução: Por exemplo: $x = -1$ e $y = 1$; $x = 5$ e $y = -4$; $x = -7$ e $y = 6$.

j) $2X + 3Y = 4$.

Solução: Por exemplo: $x = -4$ e $y = 4$; $x = 8$ e $y = -4$.

Exercício 5.19 *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 5.20 *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 5.21 *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 5.22 *(Problema adaptado de Pommer [12]) 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 5.23 *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 5.24 *(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 facilitada usando outros argumentos.

5.4 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: Primeiramente, o professor deverá retomar a definição das Equações Diofantinas Lineares (Definição 3.1), e apresentar alguns resultados que garantirão a 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.

Segundo, o professor introduzirá a ajuda do software Geogebra para verificar as soluções encontradas, ou ainda procurar soluções.

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 $d = (a, b)$. Tal resultado pode ser encontrado na Proposição 3.1.

Exemplo 5.7 *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 3.1, 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 3.1, 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 3.1, temos que a equação $14x + 35y = 9$ não tem solução em $\mathbb{Z}$.

Exemplo 5.8 *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 3.1, 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 tráz 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 3.2 , 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 3.2, para explicar como é que encontramos a solução geral de uma Equação Diofantina Linear.

Introdução ao Geogebra Nesta parte do trabalho vamos introduzir algumas ferramentas que servirão para o uso do Geogebra nos próximos encontros.

Na Figura 1, vemos o ambiente do Geogebra, com a Entrada, a qual digitamos a equação que será representada na Janela de Visualização, e na Janela de Álgebra aparecerá essa equação.

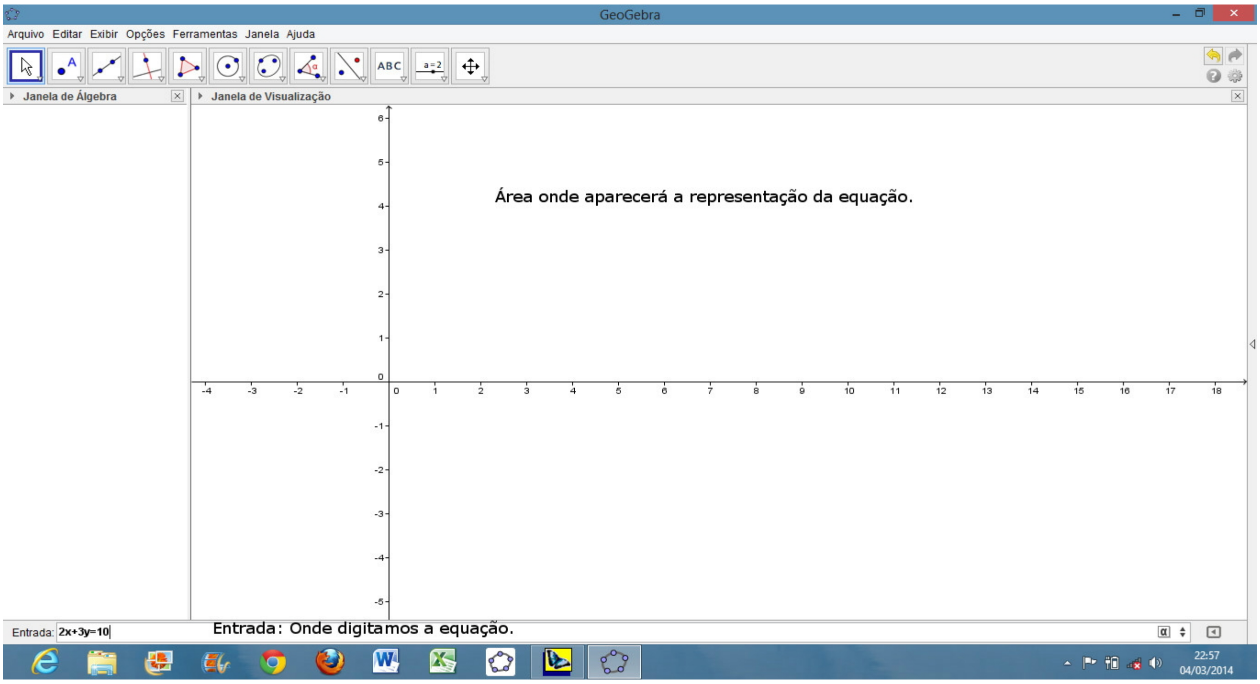

Figura 1 - Apresentação do Geogebra.

Após essa primeira parte, devemos clicar no botão "mover janela de visualização", que na Figura 2 percebemos a sua localização.

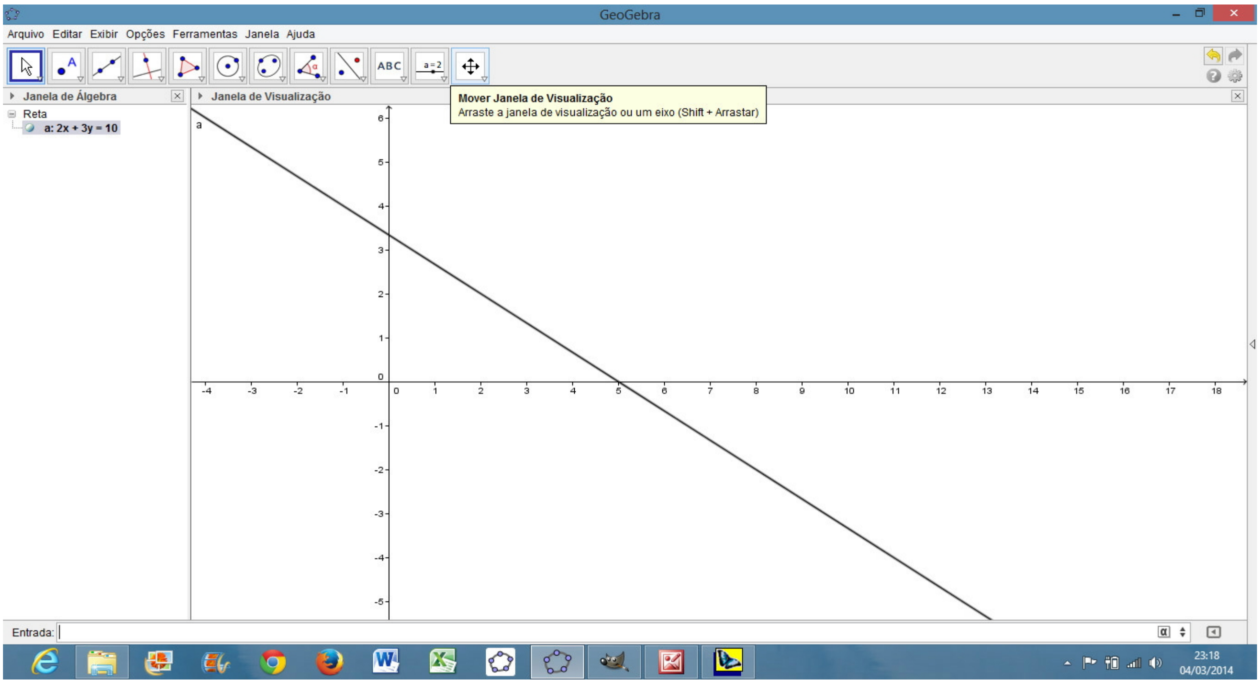

Figura 2 - Botão "mover janela de visualização".

De acordo com a Figura 3, devemos clicar com o botão esquerdo do mouse na Janela de Visualização e ativar a malha, para que possamos facilitar a visualização dos números inteiros. E na Figura 4, visualizamos a malha.

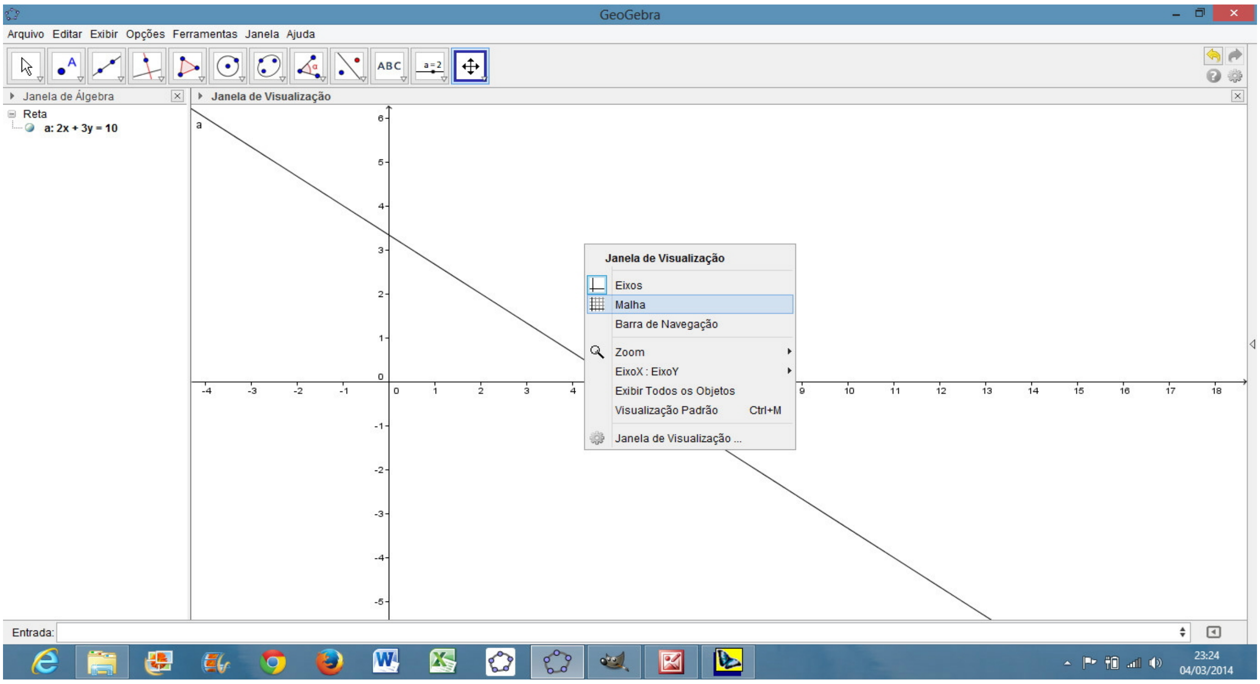

Figura 3 - Ativação da malha.

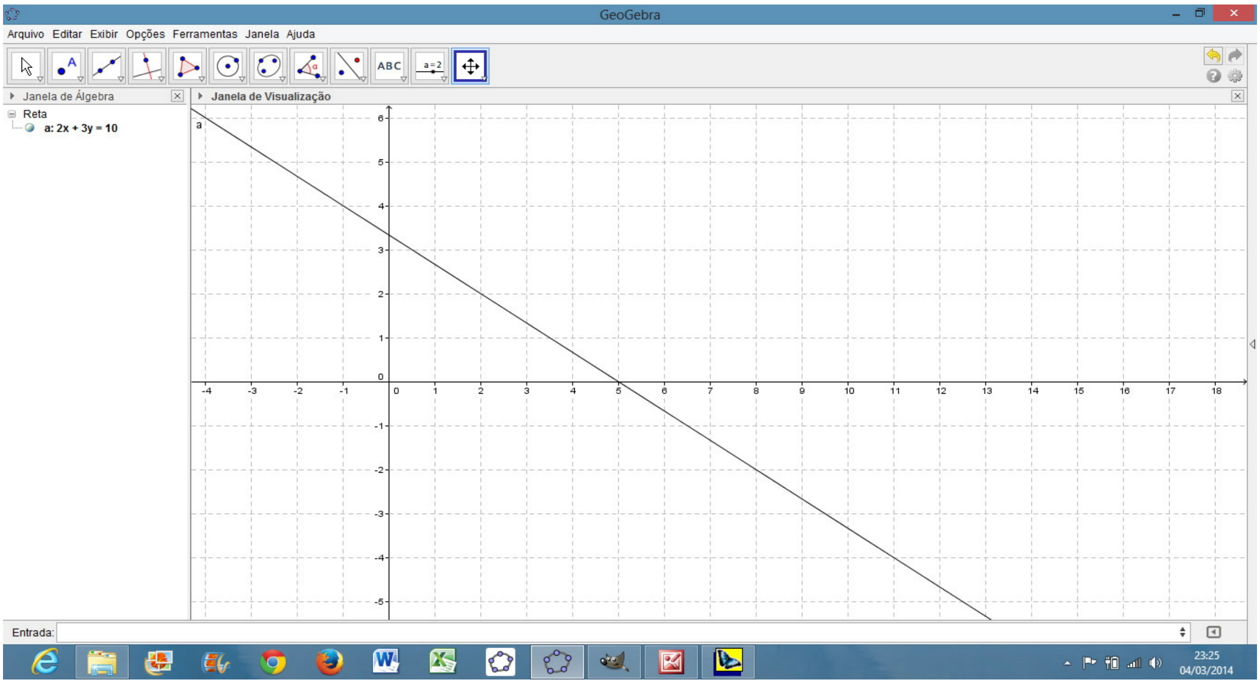

Figura 4 - Visualização da malha.

5.5 Quinto Encontro

Número de Aulas: Duas Aulas.

Objetivos: Encontrar soluções gerais para as Equações Diofantinas Lineares utilizando para isso 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: Resolução de exercícios com aplicação das Equações Diofantinas Lineares e o uso do Geogebra na verificação das soluções de alguns dos problemas.

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

Exercício 5.25 *Explique porque as equações podem ou não ter soluções inteiras, e caso tenham solução, encontrá-las.*

a) $3X + 4Y = 20$.

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:

$$4 = 1 \cdot 3 + 1 \text{ ou ainda } 1 = 1 \cdot 4 - 1 \cdot 3.$$

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 $x = -20 + 4 \cdot t$ 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 5.

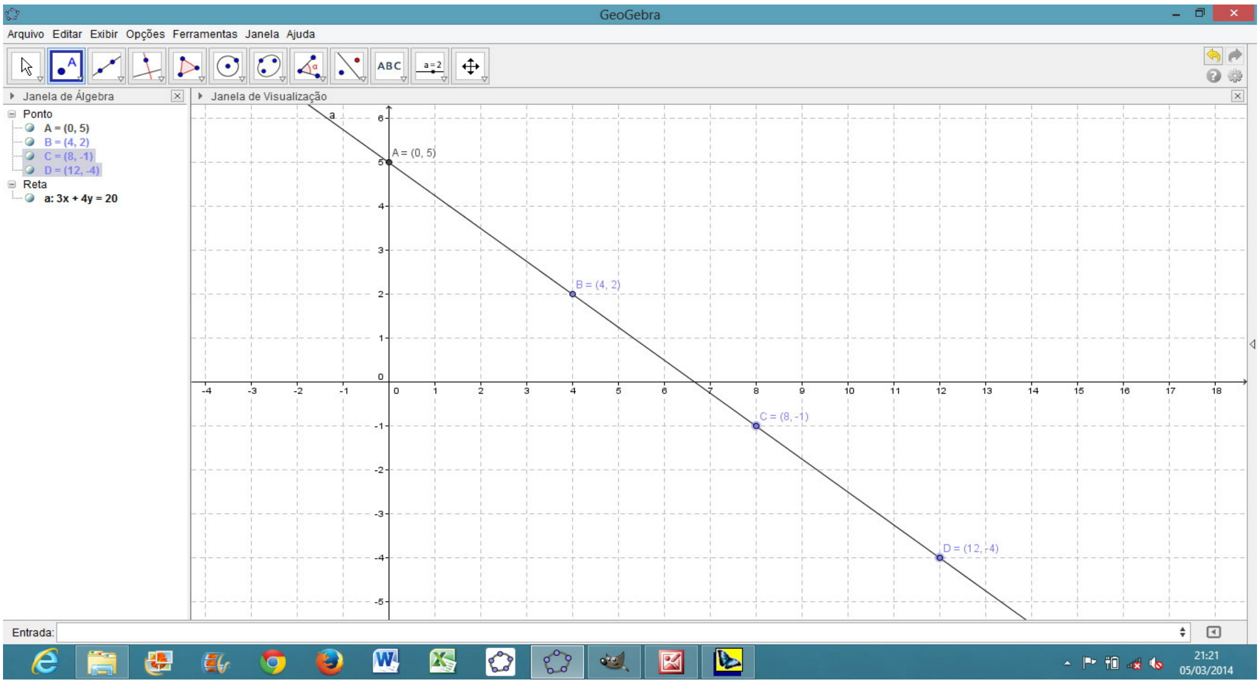

Figura 5 - Representação da equação $3X + 4Y = 20$.

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 podemos verificar que a equação não tem solução inteira. Mas devemos tomar cuidado, pois estamos visualizando apenas uma parte da representação da equação.

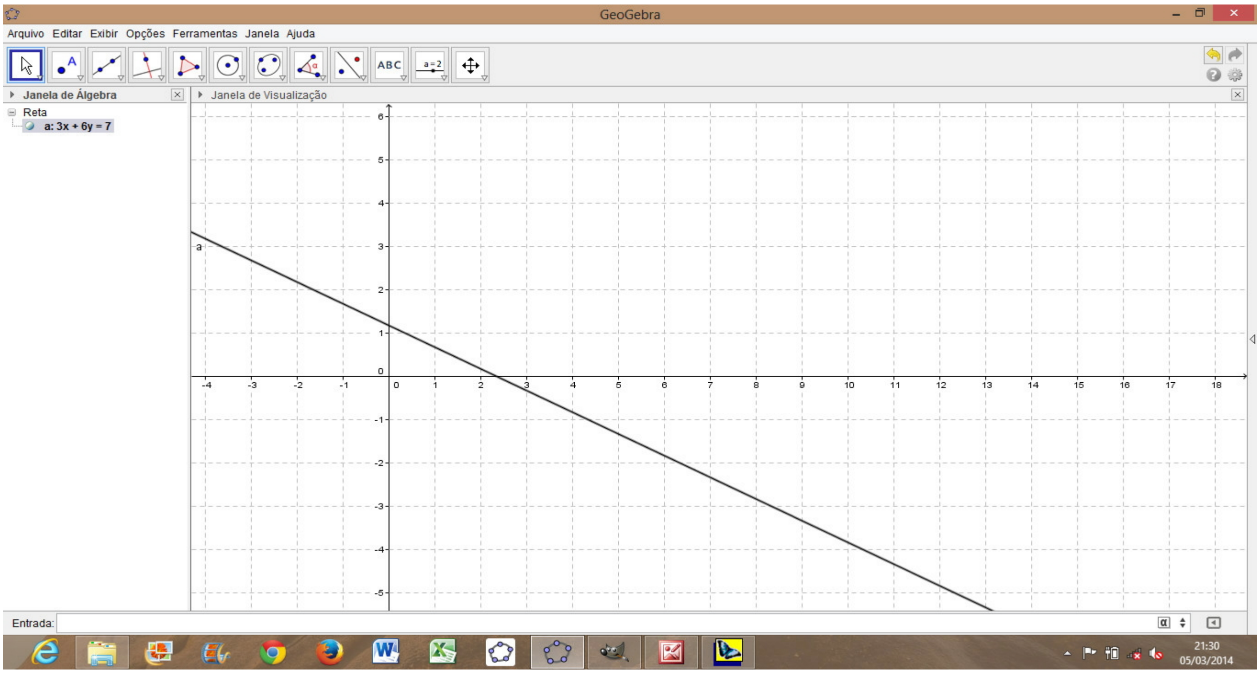

Figura 6 - Representação da equação $3X + 6Y = 7$.

Para as outras alternativas o professor poderá seguir da mesma forma.

c) $24X + 138Y = 18$.

Solução: Tem solução inteira pois $(24, 138) = 6$ e 6 divide 18, pois podemos usar o Algoritmo de Euclides e escrever $18 = 6 \cdot 3 + 0$.

Assim, vamos encontrar a solução usando o Algoritmo de Euclides e considerando a equação da forma $4X + 23Y = 3$, donde dividindo 23 por 4, encontramos

$$23 = 5 \cdot 4 + 3.$$

E fazendo a divisão de 4 por 3, obtemos

$$4 = 1 \cdot 3 + 1.$$

Agora, substituindo uma igualdade na outra, encontramos

$1 = 1 \cdot 4 - 1 \cdot 3 =$

$1 \cdot 4 - 1 \cdot (23 - 5 \cdot 4) =$

$-1 \cdot 23 + 6 \cdot 4,$

ou seja $1 = -1 \cdot 23 + 6 \cdot 4$. Multiplicando a igualdade por 3 temos $3 = -3 \cdot 23 + 18 \cdot 4$. Logo, $x_0 = 18$ e $y_0 = -3$ é uma solução particular, e consequentemente $x = 18 + 23t$ e $y = -3 - 4t$ com $t \in \mathbb{Z}$ é solução geral da equação.

Na Figura 7 temos a representação da equação $24X + 138Y = 18$, e sua solução particular $x_0 = 18$ e $y_0 = -3$. O professor poderá também mostrar outras soluções da equação.

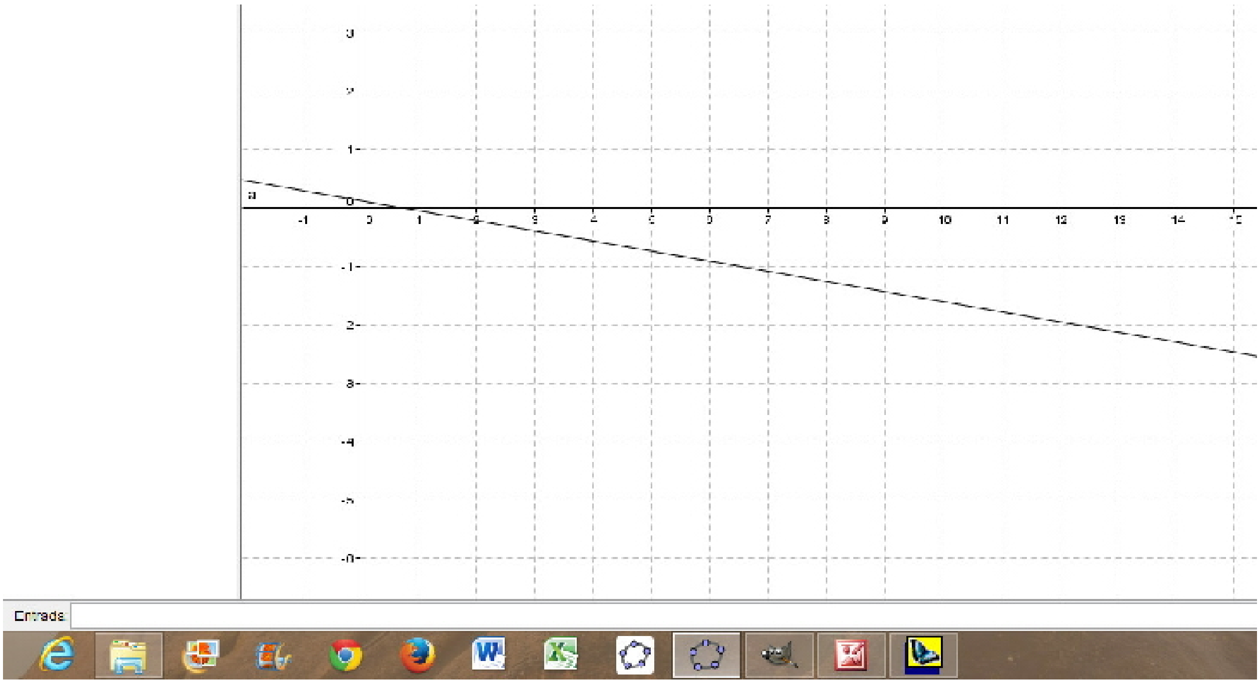

Figura 7 - Representação da equação $24X + 138Y = 18$.

d) $5X + 10Y = 3$.

Solução: Não tem solução inteira, pois $(5, 10) = 5$, e 5 não divide 3.

Aqui podemos verificar que a equação não tem solução inteira. Mas novamente devemos tomar cuidado, pois estamos visualizando apenas uma parte da representação da equação (Figura 8).

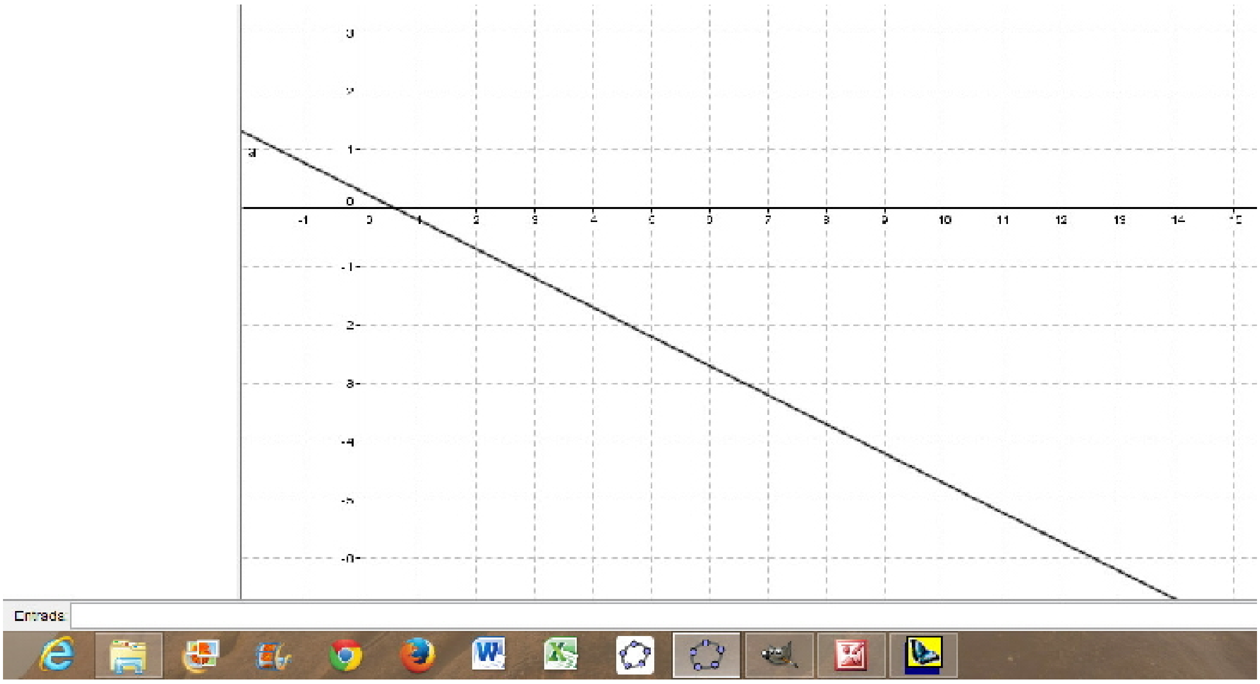

Figura 8 - Representação da equação $5X + 10Y = 3$.

e) $56X + 72Y = 40$.

Solução: Calculando o $mdc(72, 56)$, usando o Algoritmo de Euclides, obtemos a divisão de 72 por 43 da forma

$$72 = 56 \cdot 1 + 16.$$

Continuando a divisão, agora de 56 por 16, obtemos

$$56 = 16 \cdot 3 + 8,$$

e também dividindo 16 por 8, temos

$$16 = 8 \cdot 2 + 0.$$

Substituindo as igualdades anteriores de tráz pra frente e escrevendo de forma conveniente, encontramos

$8 = 56 + 16 \cdot (-3) =$

$56 + (72 + 56 \cdot (-1)) \cdot (-3) =$

$56 \cdot 4 - 72 \cdot 3 =$

$56 \cdot (4) + 72 \cdot (-3)$.

Donde obtemos:

$40 = 8 \cdot 5 =$

$56 \cdot (4 \cdot 5) + 72 \cdot (-3 \cdot 5) =$

$56 \cdot (20) + 72 \cdot (-15)$,

ou seja $40 = 56 \cdot (20) + 72 \cdot (-15)$.

Assim, a solução particular é $x_0 = 20$ e $y_0 = -15$.

Todas as soluções são: $x = 20 + (72/8)t = 20 + 9t$ e $y = -15 - (56/8)t = -15 - 7t$.

Na Figura 9 temos a representação da equação $56X + 72Y = 40$, e sua solução particular $x_0 = 20$ e $y_0 = -15$. O professor poderá também mostrar outras soluções da equação.

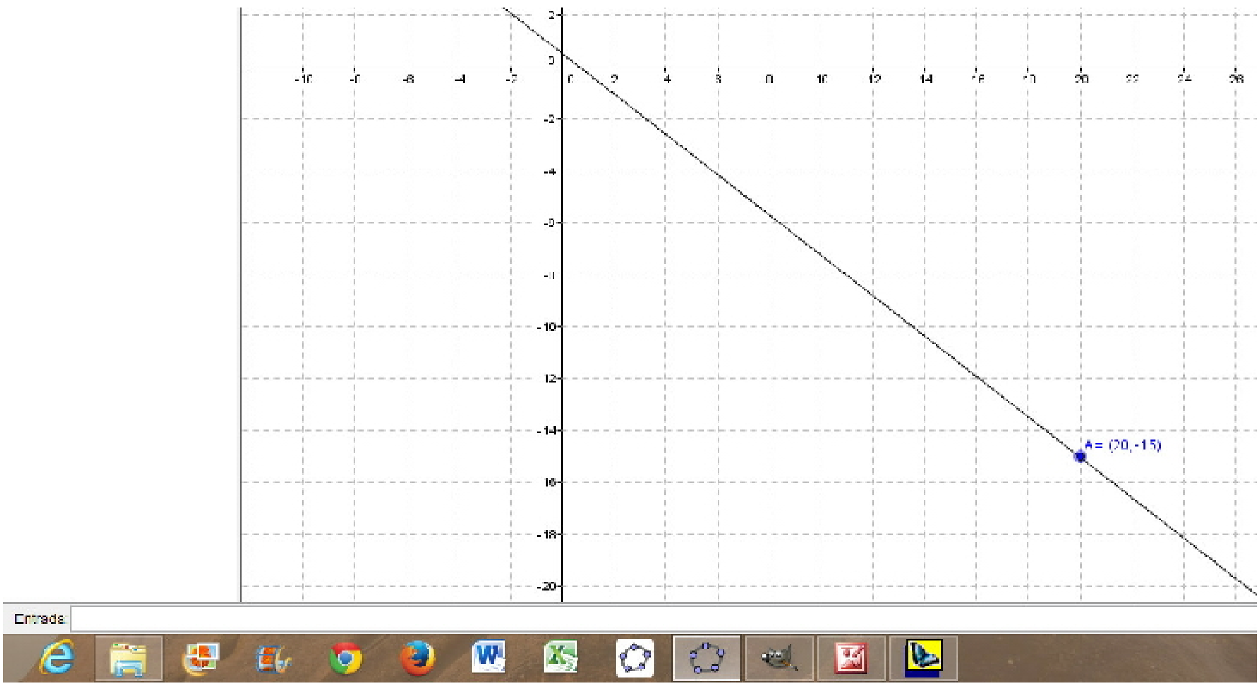

Figura 9 - Representação da equação $56X + 72Y = 40$.

Exercício 5.26 *(Euler) Divida* 100 *em* 2 *parcelas positivas, de modo que uma seja divisível por* 7 *e a outra por* 11*.*

Solução: Como visto no encontro 3, na página 44, 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,

$x = -300 + 11t > 0$, ou seja, $t > 27....$

Logo, $t \geq 28$. Tomando $t = 28$, temos como solução $x = 8$ e $y = 4$, confirmando assim a resposta tomada na página 44.

Na Figura 10 temos a representação da equação e de sua solução.

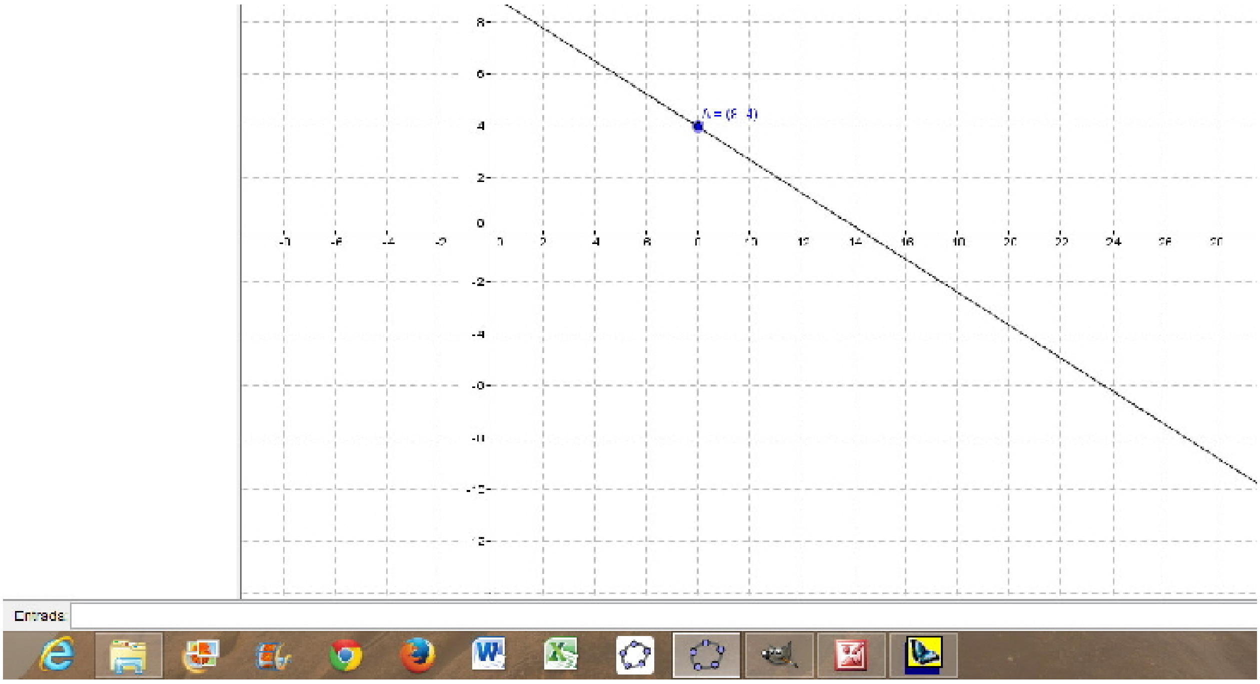

Figura 10 - Representação da equação $7X + 11Y = 100$.

Exercício 5.27 *Determinar todas as soluções inteiras e positivas das seguintes Equações Diofantinas Lineares:*

(a) $5X - 11Y = 29$.

Solução: De modo que $11 = 5 \cdot 2 + 1$ temos $mdc(5, 11) = 1$.

Para $5X - 11Y = 1$ temos a solução particular $x = -2$ e $y = -1$. Para $5X - 11Y = 29$, temos $x = -2 \cdot 29 = -58$ e $y = -1 \cdot 29 = -29$.

As demais soluções inteiras são das formas $x = -58 + (-11/1)t = -58 - 11t$ e $y = -29 - (5/1)t = -29 - 5t$.

Como as soluções devem ser positivas, então $-58 - 11t > 0$ implica que $-11t > 58$, ou ainda $11t < -58$ que implica em $t < -58/11$ ou $t < -6$ (t deve ser inteiro).

Por outro lado, $-29 - 5t > 0$ implica que $-5t > 29$ implica que $5t < -29$, ou seja $t < -29/5$ então $t < -6$, com $t \in \mathbb{Z}$.

(b) $32X + 55Y = 771$

Solução: Como $mdc(32, 55) = 1$, e usando o Algoritmo de Euclides de forma do procedimento da página 13.

Fazendo 55 dividido por 32 obtemos

$$55 = 32 \cdot 1 + 23.$$

E continuando o processo de divisão entre o quociente e o resto, encontramos

$$32 = 23 \cdot 1 + 9,$$
$$23 = 9 \cdot 2 + 5,$$
$$9 = 5 \cdot 1 + 4,$$

E por último temos

$$5 = 4 \cdot 1 + 1.$$

Agora, tomando as igualdades anteriores e substituindo umas nas outras de trás para frente obtemos, de forma conveniente:

$1 = 5 - 4 \cdot 1 =$

$5 - (9 - 5 \cdot 1) \cdot 1 =$

$5 \cdot 2 - 9 \cdot 1 =$

$(23 - 9 \cdot 2) \cdot 2 - 9 \cdot 1 =$

$= 23 \cdot 2 - 9 \cdot 5 =$

$23 \cdot 2 - (32 - 23 \cdot 1) \cdot 5 =$

$23 \cdot 7 - 32 \cdot 5 =$

$(55 - 32 \cdot 1) \cdot 7 - 32 \cdot 5 =$

$32 \cdot (-12) + 55 \cdot (7)$

Assim encontramos

$771 = 771 \cdot 1 = 32 \cdot (-12 \cdot 771) + 55 \cdot (771 \cdot 7) = 32 \cdot (-9252) + 55 \cdot (5397),$

ou seja

$771 = 32 \cdot (-9252) + 55 \cdot (5397).$

Encontramos a solução particular $x_0 = -9252$ e $y_0 = 5397$. De onde tiramos a solução geral: $x = -9252 + (55/1)t = -9252 + 55t$ e $y = 5397 - (32/1)t = 5397 - 32t$.

Para soluções positivas $-9252+55t > 0$ implica $t > 168$, e por outro lado $5397-32t > 0$ implica $t < 168$, o que não é possível. Portanto, não existem soluções positivas inteiras.

Exercício 5.28 *Temos duas balanças: uma que marca massas múltiplas de* 10 *e outra que marca massa múltiplas de* 13*. Como é que com essas balanças podemos medir* 107 *gramas?*

Solução: Temos que encontrar as soluções possíveis para a equação $13X+10Y = 107$. Como $(13, 10) = 1$, podemos então encontrar essa solução iniciando pelo Algoritmo de Euclides, dividindo primeiro 13 por 10 e encontrando

$13 = 10 \cdot 1 + 3$

e depois dividindo 10 por 3 e obtemos

$10 = 3 \cdot 3 + 1.$

Substituindo essas igualdades uma na outra de tráz pra frente e obtemos:

$1 = 10 - 3 \cdot 3,$

$1 = 10 - 3 \cdot (13 - 10 \cdot 1)$ e assim

$1 = -3 \cdot 13 + 4 \cdot 10.$

Multiplicando por 107 encontramos $107 = -321 \cdot 13 + 428 \cdot 10$

Assim obtemos $x_0 = -321$ e $y_0 = 428$. Logo, podemos medir 428 gramas na balança múltipla de 13, e descontar 321 gramas na balança múltipla de 10. Ou ainda, encontrar solução na forma:

$$x = -321 - 10t \text{ e } y = 428 + 13t, \text{ com } t \in \mathbb{N}.$$

Exercício 5.29 *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 11 a representação da equação e da sua solução.

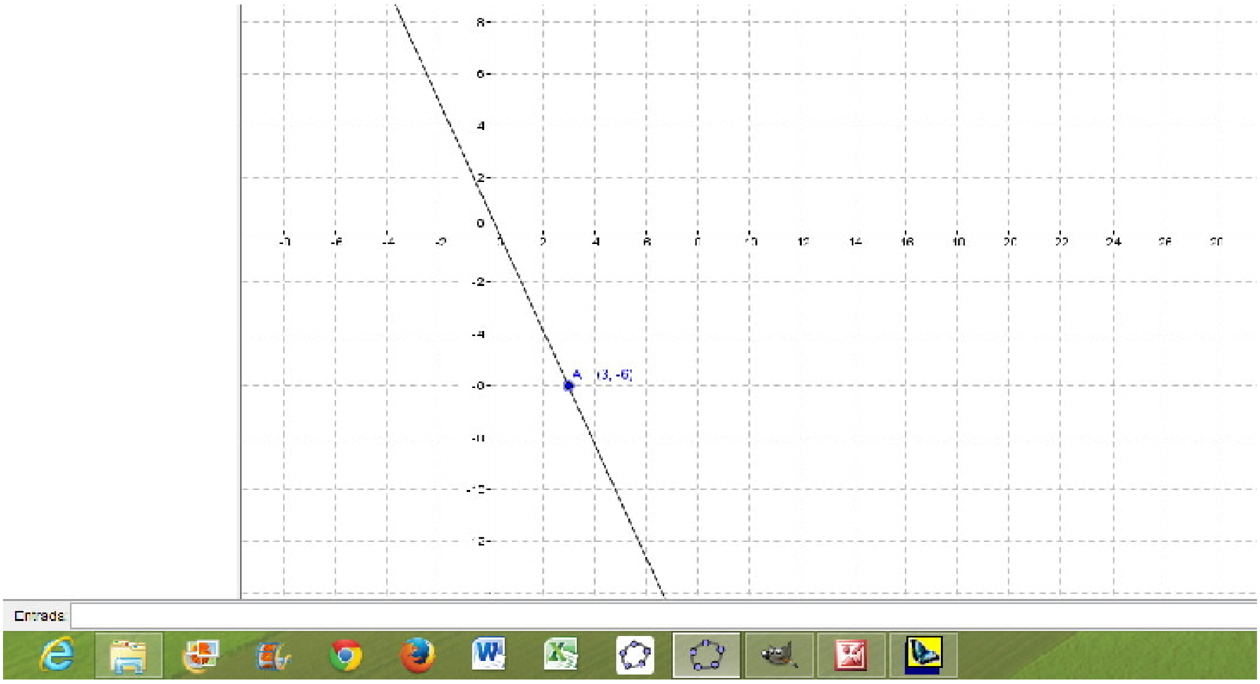

Figura 11 - Representação da equação $11X + 5Y = 3$.

Exercício 5.30 *Uma caixa contém besouros e aranhas. Existem* 46 *patas na caixa. Quantos são os besouros e quantas são as aranhas?*

Solução: As soluções encontradas na página 44 são:

$A = 2$ 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.

Sabendo que a equação é $8A + 6B = 46$. Trocando A por X e B por Y, podemos verificar essas soluções também usando o Geogebra como na Figura 12.

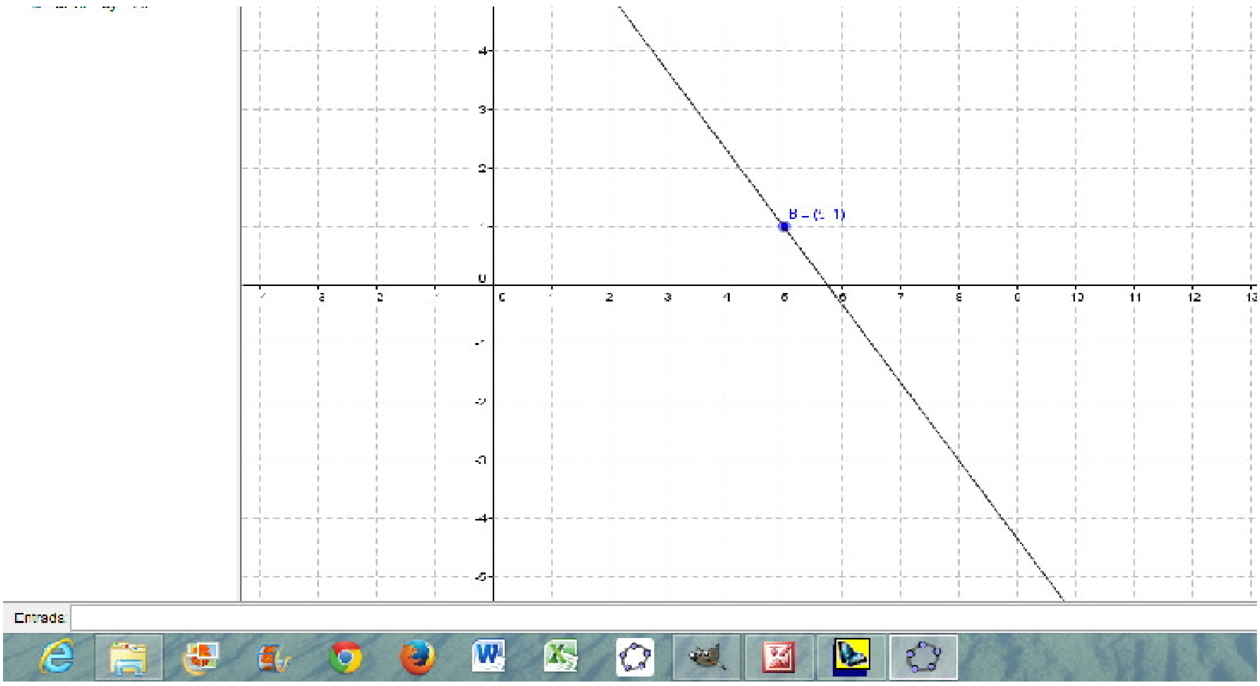

Figura 12 - Representação da equação $8X + 6Y = 46$.

Exercício 5.31 *Encontrar todos os números inteiros N, tais que o resto da divisão de N por 37 é 9, e o resto da divisão de N por 52 é 15.*

Solução: Devemos encontrar a solução para o sistema com as equações $N = 37X + 9$ e $N = 52Y + 15$, e obtemos $37X + 9 = 52Y + 15$ o que implica em $37X - 52Y = 6$, então $52Y - 37X = -6$.

Podemos encontrar a solução usando o Algoritmo de Euclides para dividir 52 por 37, e assim temos

$$52 = 1 \cdot 37 + 15.$$

E depois dividimos 37 por 15 temos

$$37 = 2 \cdot 15 + 7.$$

E por último dividimos 15 por 7 para encontrar

$$15 = 2 \cdot 7 + 1.$$

Agora substituindo uma igualdade na outra de tráz para frente de forma conveniente, obtemos:

$1 = 15 - 2 \cdot 7$

$1 = 15 - 2 \cdot (37 - 2 \cdot 15) = -2 \cdot 37 + 5 \cdot 15$

$1 = -2 \cdot 37 + 5 \cdot (52 - 1 \cdot 37) = 5 \cdot 52 - 7 \cdot 37$

Multiplicando a ultima igualdade por 6, temos:

$$6 = -(-30) \cdot 52 - 42 \cdot 37$$

Assim, uma solução é $y_0 = -30$ e $x_0 = -42$. Fazendo $x = 52t - 42$ e $y = 37t - 30$, encontramos solução para

$37 \cdot (37t - 30) - 37 \cdot (52t - 42) = 6$, para todo $t \in \mathbb{Z}$.

Assim, a equação $37x - 52y = 6$, tem uma infinidade de soluções inteiras para $x = 52t - 42$ e $y = 37t - 30$.

Podemos agora encontrar as soluções naturais da equação. Para isso devemos ter $x = 52t - 42 \geq 0$ e $y = 37t - 30 \geq 0$. Assim temos duas condições: $52t \geq 42$ e $37t \geq 30$, que são válidas se, e somente se $t \geq 1$. Portanto, qualquer $t \in \mathbb{N}$ satisfaz a equação.

Exercício 5.32 *Determinar o menor inteiro positivo que dividido por* 8 *e por* 15 *deixa os restos* 6 *e* 13*, respectivamente.*

Solução: Seja n o número inteiro positivo. Pelo Algoritmo de Euclides temos: $n = 8X + 6$ e $n = 15Y + 13$. Como n é positivo, os quocientes X e Y devem ser positivos.

Assim, $8X + 6 = 15Y + 13$ implica em $8X - 15Y = 13 - 6$, então $8X - 15Y = 7$. Considerando que $mdc(8, 15) = 1$, temos que uma solução particular imediata dessa equação é $x = -1$ e $y = -1$.

O menor valor de n será obtido ao tomar o menor valor de X e Y que satisfaça a equação $8X - 15Y = 7$. A solução geral da equação $8X - 15Y = 7$ é $x = -1 + (-15/1)t = -1 - 15t$ e $y = -1 - (8/1)t = -1 - 8t$. Como X e Y devem ser ambos positivos, então $-1 - 15t > 0$ implica em $t < -1/15$ e $-1 - 8t < 0$ implica que $t < -1/8$.

Para satisfazer as duas condições, $t < -1/8$. O menor valor positivo de x e de y ocorre para $t = -1$. Portanto: $x = -1 - 15 \cdot (-1) = 14$ e $y = -1 - 8 \cdot (-1) = 7$.

Assim obtemos, $n = 8 \cdot 14 + 6 = 118$ ou $n = 15 \cdot 7 + 13 = 188$.

Exercício 5.33 *(Atividade adaptada de um manuscrito Árabe de 1200 d.c.) Um pato pode ser comprado por* 5 *reais, uma galinha por* 1 *real, e* 20 *codornas por* 1 *real. Você possui* 100 *reas e deseja comprar* 100 *aves. Quantas aves de cada tipo você pode adquirir?*

Solução: Chamando de X, Y e Z o número de patos, galinhas e codornas, respectivamente, obtemos as seguintes equações:

$X + Y + Z = 100$ (número de aves).

$5X + Y + \frac{Z}{20} = 100$ (valor pago pelas aves).

Assim, resolvendo o sistema que envolve as duas equações, encontramos:

$\begin{cases} X + Y + Z = 100 \\ 5X + Y + \frac{Z}{20} = 100 \end{cases}$ implica em $\begin{cases} X + Y + Z = 100 \\ 100X + 20Y + Z = 2000 \end{cases}$ implica em $99X + 19Y = 1900$

Para encontrar as soluções, temos duas condições a considarar:

i) As incógnitas tem valores inteiros; ii) Temos que conhecer o dominio de uma das incógnitas.

Agora vamos isolar y (tem menor coeficiente), daí encontramos $y = \frac{1900 - 99x}{19}$. Como todas as soluções são inteiras, devemos ter $y \geq 0$. Logo,

$\frac{1900 - 99x}{19} \geq 0$ implica em $x \leq 19,19$.

Como x também é inteiro, devemos ter $x \leq 19$. Agora, encontrando os valores de y e z, obtemos:

$(x, y, z) = (0, 100, 0)$ ou $(x, y, z) = (19, 1, 80)$.

Portanto, as soluções do problemas são 100 galinhas ou 19 patos, 1 galinha e 80 codornas.

Esse problema apresenta apenas duas soluções, o que poderia motivar o aluno a resolver o problema por tentativa e erro, entretanto o exercício a seguir mostra que nem sempre é possível resolver problemas por tentativa e erro, pois algumas equações podem ter muitas soluções.

Exercício 5.34 *(Adaptado de um problema escrito no século X, com o autor identificado por Alcuin) Quando* 100 *quilogramas de grãos são distribuídos entre* 100 *pessoas de modo que cada homem recebe* 3 *quilogramas, cada mulher recebe* 2 *quilogramas, e cada criança recebe meio quilograma, quantos homens, mulheres e crianças haviam?*

Chamando de x, y e z o número de homens, mulheres e crianças, respectivamente, obtemos as seguintes equações:

$3X + 2Y + \frac{Z}{2} = 100$ (Quantidade de quilogramas),

$X + Y + Z = 100$ (Quantidade de pessoas).

Vamos resolver o seguinte sistema de equações:

$\begin{cases} X+Y+Z=100 \\ 3X+2Y+\dfrac{Z}{2}=100 \end{cases}$ implica em $\begin{cases} X+Y+Z=100 \\ 6X+4Y+Z=200 \end{cases}$ implica em $5X+3Y=100$.

Para encontrar a solução vamos usar o método de Equações Diofantinas Lineares.

Como $(5,3)=1$, e 1 divide 100, pois $100=1\cdot 100+0$, então usando o Algoritmo de Euclides, obtemos:

$5=3\cdot 1+2$ ou ainda $2=5-3\cdot 1$. Multiplicando essa última igualdade por 50 de forma conveniente, obtemos

$100=5\cdot 50+(-50)\cdot 3$, donde encontramos a solução particular $x_0=50$ e $y_0=-50$. Assim, a solução geral é da forma $x=50-3t$, e $y=-50+5t$, com $t\in\mathbb{Z}$. Como os valores de x e y devem ser positivos, pois o número de homens e mulheres são positivos, temos que $t\leq 16$ e $t\geq 10$, quando usamos a solução geral. Assim, $10\leq t\leq 16$.

Se $t=10$, obtemos $x=20$ e $y=0$, e daí encontramos $z=80$.

Se $t=11$, obtemos $x=17$ e $y=5$, e daí encontramos $z=78$.

Se $t=12$, obtemos $x=14$ e $y=10$, e daí encontramos $z=76$.

Se $t=13$, obtemos $x=11$ e $y=15$, e daí encontramos $z=74$.

Se $t=14$, obtemos $x=8$ e $y=20$, e daí encontramos $z=72$.

Se $t=15$, obtemos $x=5$ e $y=25$, e daí encontramos $z=70$.

Se $t=16$, obtemos $x=2$ e $y=30$, e daí encontramos $z=68$.

Que representam o número de homens, mulheres e crianças respectivamente.

5.6 Sexto Encontro

Número de Aulas: Duas Aulas.

Objetivos: Apresentar os conceitos que envolvem Ternas Pitagóricas.

Conteúdos: Relações métricas nos triângulos retângulos, mmc, mdc.

Encaminhamentos Metodológicos: Fazer com que os alunos encontrem Ternas Pitagóricas encolvendo os conceitos apresentados nesse trabalho.

Teoria e Atividades: O objetivo desse encontro será desenvolver uma aula voltada as Equações Diofantinas de Segunda Ordem, que são denominas Ternas Pitagóricas de acordo com a Definição 4.1. Feita a definição, o próximo passo do professor será exemplificar as ternas pitagóricas, e quais os procedimentos que devemos fazer para obter tais equações, como nas páginas 26, 27 e 28, onde estão as Proposições 4.2, 4.3 e 4.4, e os exemplos que podem ser introduzidos na sala de aula.

Feito todos esse processo, o professor deverá aplicar os exercícios seguintes:

Exercício 5.35 *Determine todos os triângulos pitagóricos que têm um cateto* $x = 12$.

Solução: Primeiro elevamos 12 ao quadrado. Depois fatoramos 12^2 como produto de dois inteiros positivos (u e v) , distintos e de mesma paridade ($12^2 = 144 = 72 \cdot 2 = 36 \cdot 4 = 24 \cdot 6 = 18 \cdot 8$). Portanto, existem 4 triângulos pitagóricos com catetos de comprimento 12.

O comprimento do lado desses triângulos são dados por $(12, 35, 37)$; $(12, 16, 20)$; $(12, 9, 15)$; $(12, 5, 13)$.

Exercício 5.36 *Usando as fórmulas de pitágoras, verifique se existe alguma terna pitagórica em que um dos lados do triângulo retângulo vale* 220.

Solução: Sabemos que as fórmulas de pitágoras que estão na proposição 4.2 são: $x = 2n+1$ (cateto de valor impar), $y = 2n^2 + 2n$ (cateto de valor par) e $z = 2n^2 + 2n + 1$ (hipotenusa). Assim, dessas fórmulas a única que pode valer 220 é o cateto y. Então, $y = 2n^2 + 2n = 220$ implica que $n = -11$ e $n = 10$. Usando $n = -11$ encontramos $x = -21$, o qual não podemos considerar. Agora, usando $n = 10$, encontramos $x = 21$ e $z = 221$. Logo, a terna pitagórica é $(21; 220; 221)$. Verificando se é mesmo uma terna pitagórica, temos: $21^2 + 220^2 = 221^2$ implica que $441 + 48400 = 48841$. Portanto, existe uma terna pitagórica com um dos lados medindo 220.

Exercício 5.37 *Usando o mesmo valor de cateto* 220, *verifique usando as fórmulas de Platão se existe alguma terna pitagórica diferente da terna do exercicio anterior.*

Solução: Sabemos que as fórmulas de Platão são: $x = 2mn$, $y = m^2 - n^2$ e $z = m^2 + n^2$. Podemos usar a fórmula de $x = 2mn$ para verificar se existe tal terna, então podemos fazer: $x = 2mn = 220$ implica em $mn = 110$. Assim, podemos ter $110 \cdot 1 = 110$, $55 \cdot 2 = 110$ e $11 \cdot 10 = 110$, onde teremos três casos para os pares m e n.

i) Se $m = 110$ e $n = 1$, então temos $y = 12099$ e $z = 12101$, e determinamos a seguinte terna pitagórica $(220; 12099; 12101)$. Verificando se é mesmo uma terna pitagórica, obtemos:

$220^2 + 12099^2 = 12101^2$ implica que $48400 + 146385801 = 146434201$. O que confirma que $(220; 12099; 12101)$ é uma terna pitagórica.

ii) Se $m = 55$ e $n = 2$ temos $y = 3021$ e $z = 3029$, e determinamos a seguinte terna pitagórica $(220; 3021; 3029)$. Verificando se é mesmo uma terna pitagórica, obtemos: $220^2 + 3021^2 = 3029^2 \Rightarrow 48400 + 9126441 = 9174841$. O que confirma que $(220; 3021; 3029)$ é uma terna pitagórica.

iii) Se $m = 11$ e $n = 10$ temos $y = 21$ e $z = 221$, e determinamos a seguinte terna pitagórica $(220; 21; 221)$, que é a mesma terna obtida no exercicio anterior.

Portando, existem ternas pitagóricas usando as fórmulas de Platão.

Exercício 5.38 *Verifique se os números primos* $3, 5, 7, 13, 17, 19$ *fazem parte de alguma terna pitagórica.*

Solução: Tomando as fórmulas $x = \dfrac{n^2-1}{2}$, $y = n$ e $z = \dfrac{n^2+1}{2}$, podemos verificar se estes números fazem parte de uma terna pitagórica. Tomando $y = n = 3$ encontramos $x = 4$ e $z = 5$, e assim obtemos a terna $(4; 3; 5)$. Como o 5 já esta na terna anterior, podemos tomar $y = n = 7$, e encontramos $x = 24$ e $z = 25$, e temos a terna $(24; 7; 25)$. Tomando agora $y = n = 13$ encontramos $x = 84$ e $z = 85$, e obtemos a terna pitagórica $(84; 13; 85)$. Para $y = n = 17$, obtemos $x = 144$ e $z = 145$, e assim $(144; 17; 145)$ é uma terna pitagórica. Se $y = n = 19$, temos $x = 180$ e $y = 181$, e assim a terna é $(180; 19; 185)$. Portanto, todos os números primos acima pertencem a uma terna pitagórica.

Referências Bibliográficas

[1] BOYER, C. B.. **História da Matemática**. Tradução: Elza F. Gomide – São Paulo. Editora Edgard Blücher – 1974. 488p.

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

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

[4] EVES, H.**Introdução a História da Matemática**. Tradução: Higyno H. Domingues. Editora Unicamp. Campinas-SP. 843p.

[5] FILHO, E. de A. **Teoria Elementar dos Números**. 3^a edição. Editora Livraria Nobel S. A. São Paulo – SP. 1985.

[6] FROHLICH, A. e TAYLOR, M. J. **Algebric Number Theory**. Cambridge studies in advanced mathematics 27. Cambridge University Press. 1994. 355p.

[7] HEFEZ, A. **Elementos da Aritmética**. Rio de Janeiro. Sociedade Brasileira de Matemática, 2005. 169 p.

[8] KATZ, V. J. **História da Matemática**. Fundação Calouste Gulbenkian. Avenida de Berna. Lisboa – 2010.

[9] LINS, R. C.; GIMENEZ J. **Perspectivas em Aritmética e Álgebra para o século XXI**. 5^a ed. Campinas-SP: Papirus 2005. 176p.

[10] MARINEZ, F. B; MOREIRA, C. G.; SALDANHA, N.; TENGAN; E. **Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro.** Projeto Euclides. 2 ed. Rio de Janeiro: IMPA 2011. 450p.

[11] NAGELL, T. **Introduction to Number Theory**. Chelsea Publishing Company, New York. 1972. 309p.

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

[13] ROCQUE, G. de La; PITOMBEIRA, J. B. **Uma Equação Diofantina e Suas Resoluções**. Revista do professor de Matemática, São Paulo, 1991. v. 19, p. 39-47.

[14] ROSEN, K. H.; **Matemática Discreta e Suas Aplicações**. 6^a ed. McGraw-Hill Interamericana do Brasil. São Paulo - SP, 2009. 982p.

[15] SANTOS, J. P. de O.; **Introdução a Teoria dos Números**. Coleção Matemática Universitária. Impa, 3^a edição. Rio de Janeiro, 2012. 198p.

[16] Site: **http://www.somatematica.com.br/coluna/gisele/20062001.php**; Acesso em 04/03/2014.