UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL

NATÁLIA MEDEIROS DO NASCIMENTO

EQUAÇÕES DIOFANTINAS E O MÉTODO DAS SECANTES E TANGENTES DE FERMAT

FORTALEZA
2014

NATÁLIA MEDEIROS DO NASCIMENTO

EQUAÇÕES DIOFANTINAS E O MÉTODO DAS SECANTES E TANGENTES DE FERMAT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Alberto Duarte Maia.
Coorientador: Prof. Dr. Francisco Régis Vieira Alves.

FORTALEZA
2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

N196e Nascimento, Natália Medeiros do
Equações diofantinas e o método das secantes e tangentes de Fermat / Natália Medeiros do Nascimento. - 2014
45 f. : enc.; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2014.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Dr. José Alberto Duarte Maia.
Coorientação: Prof. Dr. Francisco Régis Vieira Alves.

1. Equações diofantinas. 2. Fermat, Último teorema de. I. Título.

CDD 512.72

NATÁLIA MEDEIROS DO NASCIMENTO

EQUAÇÕES DIOFANTINAS E O MÉTODO DAS SECANTES E TANGENTES DE FERMAT

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 26 / 04 / 2014.

BANCA EXAMINADORA

José Alberto Duarte Maia

Prof. Dr. José Alberto Duarte Maia (Orientador)

Universidade Federal do Ceará (UFC)

Prof. Dr. Marcelo Ferreira de Melo

Universidade Federal do Ceará (UFC)

Prof. Dr. Francisco Régis Vieira Alves

Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

AGRADECIMENTOS

A Deus, pela vida.

A minha família, pelo incentivo e compreensão nos momentos de ausência.

Ao meu orientador, Professor Dr. José Alberto Duarte Maia, pela grande ajuda e dedicação.

Aos professores do mestrado, que além de terem transmitido um pouco do muito que sabem, estiveram sempre dispostos a esclarecer dúvidas e ajudar.

A CAPES, pela bolsa de auxílio que recebi por dois anos.

A SBM, pela criação desse projeto, o PROFMAT, e a UFC que ao aceitar a parceria contribuiu significativamente para o meu desenvolvimento profissional.

Aos colegas de turma pelo companheirismo incondicional e disponibilidade de ajudar sempre ao longo desses dois anos e meio.

Aos professores participantes da banca pelas valiosas sugestões para o aprimoramento deste trabalho.

Ao colega Marcio Pereira da Silva pela ajuda na formatação deste trabalho.

RESUMO

Ao longo das últimas décadas, a transmissão do conhecimento matemático na Educação Básica sofreu diversas mudanças. "O Ensino Tradicional" da matemática era baseado na memorização de fórmulas, havendo assim uma mecanização no processo de resolução de problemas, onde o discente era visto como um ser passivo. A nova visão de ensino, que busca significar o que conteúdo exposto em sala, motivou a escolha desse tema, visto que situações problemas envolvendo equações diofantinas podem ser facilmente percebidas em nosso cotidiano. O objetivo deste trabalho é oportunizar a realização de uma leitura consultiva para o professor do Ensino Básico, e asseverar que essas equações podem ser aplicadas na Educação Básica como uma ferramenta que instiga o pensamento lógico, o raciocínio, a compreensão e a interpretação matemática. A formulação desse material que está dividido em cinco capítulos se deu através de levantamento bibliográfico por meio de pesquisas descritivas. A introdução compõe o primeiro capítulo. O segundo capítulo versa sobre o Legado de Diofanto: vida e obras, ressaltando sua obra titulada "Arithmetica" que contribuiu significativamente para o desenvolvimento da teoria dos números. O terceiro capítulo trata das equações diofantinas lineares de n variáveis. O quarto capítulo aborda as ternas pitagóricas, o Método das Secantes e Tangentes de Fermat na busca de soluções racionais para equações, com coeficientes racionais, da forma $ax^2 + by^2 = c$, e um caso particular do Último Teorema de Fermat. O quinto capítulo é composto de problemas sobre equações diofantinas lineares.

Palavras-chave: Equações diofantinas lineares. Ternas pitagóricas. Método das secantes e tangentes de Fermat. Último teorema de Fermat.

ABSTRACT

Over the past decades, the transmission of mathematical knowledge in basic education has undergone several changes. The "Teaching Traditional" math was based on memorizing formulas, so there mechanization in problem solving where the student was seen as a liability to be process. The new vision of education that seeks to signify exposed to room content, motivated the choice of this theme, as diophantine equations involving situations problems can be easily noticed in our daily lives. The objective of this work is an opportunity for a realization of an advisory reading for the teacher of basic education, and assert that these equations can be applied in basic education as a tool that encourages the logical thinking, reasoning, understanding and mathematical interpretation. The formulation of this material which is divided into five chapters was through literature review through descriptive research. The introduction comprises the first chapter. The second chapter deals with the Legacy of Diophantus: life and works, emphasizing his work entitled "Arithmetica" which contributed significantly to the development of number theory. The third chapter deals with linear Diophantine equations in n variables. The fourth chapter discusses the Pythagorean tender, Fermat's of secants and Tangents method, in finding rational solutions to equations with rational coefficients, of the form $ax^2 + by^2 = c$ and a particular case Fermat's Last Theorem. The fifth chapter is composed of problems on linear diophantine equations.

Keywords: Linear diophantine equations. Pythagorean tender. Method of secants and tangents of Fermat. Fermat's last theorem.

SUMÁRIO

1 INTRODUÇÃO

Observando a nossa volta é possível notar diversos padrões e sequências. A matemática surgiu a partir da necessidade humana de entender esses padrões e obter certo controle sobre algo. Alguns povos antigos, por exemplo, se baseavam nas fases da lua para ter uma noção de cheias de rios ou de períodos chuvosos, mesmo sem possuir um sistema numérico a noção de contagem estava implícita.

Um dos artefatos matemáticos mais antigos, datado com cerca de 20 mil anos, é o osso de Ishango, exposto no Museu de Ciências Naturais, em Bruxelas. Ele possui traços associados a alguma espécie de contagem, e devido à forma como aparecem os agrupamentos, certamente quem os fez estava realizando algum tipo de conta. Esse osso de macaco encontrado no Congo é mais antigo que a escrita, o que nos mostra a importância do processo de contagem desde os primórdios dos tempos (MOL[1], 2013; BOYER[2], 1974).

Outro artefato datado em 30 mil anos atrás, um osso de lobo com vestígios de marcações, considerado como prova da existência do processo de contagem na época do período Paleolítico, foi encontrado em 1937 por Karl Absalom na antiga Tchecoslováquia (ALMEIDA[3], 2002).

Mas o que teria levado os homens pré-históricos a realizarem marcações em pedações de ossos? Uma possível explicação para tal atitude é que: *"Grupos de pedras são demasiado efêmeros para conservar informação: por isso o homem pré-histórico às vezes registrava um número fazendo marcas em um bastão ou pedaço de osso"* (BOYER[2], 1974, p.3).

Os números foram fundamentais para a organização e o desenvolvimento da vida em sociedade, mas quando e onde se iniciou a ideia de atribuir um valor numérico a um grupo de objetos ou a seres, por exemplo, é um mistério. É difícil imaginar civilizações antigas que não tenham uma noção, mesmo que implícita, de contagem. Os Aua Piri, povo aborígene que habita o interior da Austrália, não utilizam números no seu idioma, possuem uma palavra que significa a unidade, somente. Eles conseguiram viver sem a necessidade de um sistema de numeração até recentemente. Os Sumérios há 6000 anos, no entanto, provavelmente por viverem em cidades sentiram a necessidade não somente de contar, mas de realizarem divisões, multiplicações e subtrações. Durante muitos séculos os números foram utilizados com a finalidade de realizar contas e medições. Posteriormente, começou-se a pensar sobre a natureza e as propriedades que os números carregam. Foi assim que surgiu a Teoria dos Números!

Essa teoria ocupa-se no estudo dos números inteiros e recebeu ao longo da história a atenção de matemáticos famosos como Pitágoras, Euclides, Diofanto e Pierre de Fermat.

---

[1]MOL, Rogério Santos. Introdução à História da Matemática. Belo Horizonte: CAED-UFMG, 2013. Disponível em: www.mat.ufmg.br. Acessado em 05/01/2014.

[2]BOYER, Carl B. História da matemática. São Paulo: Editora E. Blucher, 1974.

[3]Para mais detalhes, veja M. C. Almeida, *Talhas Numéricas e o Antigo Testamento.* Revista Brasileira de História da Matemática. Vol. 2, nº 4 , 2002. Disponível em: http://www.rbhm.org.br/vo2-no4.html. Acessado em 10/03/2014.

Os livros que abordam história da matemática costumam atribuir aos pitagóricos, membros da escola fundada por Pitágoras, o início do estudo das propriedades numéricas no conjunto dos inteiros positivos, por volta de 600 a.C.. Além de estudos matemáticos, a escola pitagórica também se dedicava ao estudo da filosofia. É importante salientar que não há nenhum documento original que comprove as descobertas atribuídas aos pitagóricos, visto que todos os membros faziam o juramento de manter os conhecimentos adquiridos e descobertos em segredo (EVES[4], 1995).

Os pitagóricos classificaram os números em pares e ímpares, estudaram os números perfeitos, amigáveis, figurados, entre outros. Como podemos observar, a matemática era tratada por eles também de um modo abstrato, esse estudo teórico era denominado por eles de "aritmética", enquanto os cálculos práticos eram conhecidos como "logístico" (EVES[4], 1995).

Para Pitágoras só havia números inteiros ou números formados pela razão entre eles (sendo considerados somente os positivos). Essa concepção foi profundamente abalada quando na aplicação do Teorema de Pitágoras percebeu-se que a hipotenusa de um triângulo retângulo com catetos iguais a um não era um número inteiro, e nem formado pela razão entre inteiros. Esse famoso teorema está escrito e demonstrado na obra "Os Elementos" de Euclides. O estudo de soluções naturais ou racionais para equações quadráticas foi um dos interesses de Diofanto séculos depois, este dedicou parte de sua vida a estudar equações indeterminadas, realizando algumas publicações. E foi observando esse mesmo teorema em uma das traduções da obra "Arithmetica" de Diofanto que surgiu o mais intrigante teorema, relacionado à teoria dos números de todos os tempos: O Último Teorema de Fermat.

A teoria dos números tem seus encantos, alguns de seus enunciados, apesar de serem bem simples e de fácil entendimento, são extremamente difíceis de demonstrar, um exemplo clássico desse tipo de enunciado é o Último Teorema de Fermat que perdurou mais de 300 anos até que alguém conseguisse uma demonstração sem falhas.

[4]EVES, Howard Whitley. Introdução a História da Matemática. Campinas,SP: Ed. da UNICAMP, 1995.

2 O LEGADO DE DIOFANTO

2.1 Vida e obra de Diofanto

Considerado o mais importante algebrista grego, Diofanto nasceu em algum ano situado entre 150 a.C. e 364 da nossa era. Sabe-se que ele viveu por um período em Alexandria, principal centro de estudos matemáticos da Grécia antiga, onde sua carreira floresceu. Sua vida é desconhecida, a única informação que temos é quanto tempo ele viveu, 84 anos, isso graças a um enigma gravado na lápide de seu túmulo que segundo a tradução contida no livro O Último Teorema de Fermat dizia o seguinte:

> *"Deus lhe concedeu graça de ser um menino pela sexta parte de sua vida. Depois, por um doze avos, ele cobriu seu rosto com a barba. A luz do casamento iluminou-o após a sétima parte e cinco anos depois do casamento Ele concedeu-lhe um filho. Ah! criança tardia e má, depois de viver metade da vida de seu pai o destino frio a levou. Após consolar sua mágoa em sua ciência dos números, por quatro anos, Diofante terminou sua vida"* .
>
> (SINGH[1], 2001, p.71)

Para solucionarmos este enigma chamaremos de x a quantidade de anos vivido por Diofanto, assim temos:

$$x = \frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4 \Rightarrow x = \frac{14x+7x+12x+42x+756}{84} \Rightarrow 84x = 75x-756$$

$$\Rightarrow 9x = 756 \Rightarrow x = \frac{756}{9} \Rightarrow x = 84 \text{ anos.}$$

2.2 A obra de Diofanto

De acordo com historiadores, Diofanto escreveu três obras:

- Porismas − que foi perdido ao longo do tempo. Estudiosos acreditam que ele teria escrito nessa obra alguns fundamentos teóricos e teoremas sobre a teoria dos números. O que é certo é que em sua obra "Arithmetica" Diofanto utiliza certas proposições como auxílio e as chama de porismas.

- Sobre Números Poligonais − Dessa obra restou apenas um fragmento, nela a representação dos números é geométrica, assim como o processo das investigações realizadas.

- Arithmetica − Esta é sem dúvida seu maior legado! Dos treze trabalhos escritos, apenas seis sobreviveram, inspirando grandes matemáticos como Pierre de Fermat.

[1]SINGH, Simon. O Último teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos. 10. ed. Rio de Janeiro: Record, 2001.

A "Arithmetica" aborda analiticamente a teoria algébrica dos números, contém mais de 100 problemas cujas soluções são detalhadas por ele, e resultam em equações de primeiro ou segundo grau, havendo também casos em que a resolução resulta em equações de grau maior que dois, equações algébricas como por exemplo $ax+by = c$, $a^2+b^2 = c^2$, $a^4+b^4+c^4 = x^4$. Os problemas diofantinos, assim como ficaram conhecidos, só possuíam soluções entre os números racionais positivos. Na maioria das vezes uma só resposta era suficiente para contentar Diofanto (EVES[2], 1995).

2.3 Alguns problemas propostos por Diofanto em sua obra, Arithmetica

Abaixo seguem cinco problemas pertencentes a "Arithmetica" de Diofanto, e suas respectivas soluções em notação atual.

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

Solução:

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

Por (iii), temos $x = 27-w-z$, e (iv) resulta em $y = 20-w-z$. Assim, substituindo em (ii), resulta em:

$27 - w - z + 20 - w - z + w = 24$, donde $23 = 2z + w(v)$.

Substituindo (iii) e (iv) em (i), teremos:

$27 - w - z + 20 - w - z + z = 22$, onde $25 = z + 2w$.

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

Assim, $3z = 21$, ou seja $z = 7$ e por (v), $w = 9$.

Como $x = 27 - w - z$ e $y = 20 - w - z$, temos que $x = 11$ e $y = 4$.

Logo, a solução é $4, 7, 9, 11$.

Livro II- problema 20: "Encontrar dois números tais que o quadrado de qualquer um somado ao outro dá um quadrado".

Solução:

Observando que $(x+1)^2 = x^2+2x+1$, podemos tomar x e $2x+1$ como sendo esses dois números. Deveremos agora determinar x tal que $x + (2x + 1)^2$ seja um quadrado também! Assim, $4x^2 + 5x + 1 = (2x + k)^2 \Rightarrow 5x + 1 = 4kx + k^2 \Rightarrow x(5 - 4k) = k^2 - 1$. Como x deve ser um racional positivo, temos dois casos:

[2]EVES, Howard Whitley. Introdução a História da Matemática. Campinas,SP: Ed. da UNICAMP, 1995.

1º caso: $5-4k>0$ e $k^2-1>0 \Rightarrow \frac{5}{4}>k$ e $k>1$ ou $k<-1$, logo podemos tomar por exemplo $k=\frac{6}{5}$ ou $k=-2$.

Se $k=\frac{6}{5}$ temos $5x+1=4.\frac{6}{5}.x+\left(\frac{6}{5}\right)^2 \Rightarrow 5x+1=\frac{24x}{5}+\frac{36}{25} \Rightarrow \frac{25x-24x}{5}=\frac{36-25}{25} \Rightarrow \frac{5x}{5}=11 \Rightarrow x=\frac{11}{5}$ e portanto $2x+1=\frac{27}{5}$.

Se $k=-2$ então $5x+1=-8x+4$ donde $x=\frac{3}{13}$ então $2x+1=2.\frac{3}{13}+1=\frac{6}{13}+1=\frac{19}{13}$.

2º caso: $5-4k<0$ e $k^2-1<0$, isto é, $\frac{5}{4}<k$ e $-1<k<1$. Nesse caso não há solução!

Livro III- problema 21: "Dividir um número em duas parcelas e determinar um quadrado que, quando somado a qualquer delas, dá um quadrado".

Solução:

Considere o número dado como sendo 20, teremos neste caso que $x+y=20$. Pegaremos o quadrado como sendo $(a+1)^2$, conforme a solução de Diofanto. Obtemos assim o seguinte sistema:

$$\begin{cases} x+a^2+2a+1=z^2 & (i) \\ y+a^2+2a+1=z^2 & (ii) \end{cases}$$

Note que se tomarmos $x=2a+3$ em (i) teremos o quadrado $(a+2)^2$, $y=4a+8$ em (ii) teremos o quadrado $(a+3)^2$. Dessa forma, $x+y=20 \Rightarrow 2a+3+4a+8=20 \Rightarrow 6a=9$, isto é, $a=\frac{3}{2}$.

Concluímos, portanto, que $x=2a+3 \Rightarrow x=6$, $y=4a+8 \Rightarrow y=14$ e $x+a^2+2a+1=z^2 \Rightarrow z=\frac{25}{4}$.

Livro IV- problema 1: "Decompor um número dado em dois cubos cuja soma de raízes seja dada".

Solução:

Tomemos o número dado como sendo 370, e a soma das raízes igual a 10, neste caso nosso problema gera o seguinte sistema:

$$\begin{cases} x^3 + y^3 = 370 \\ x + y = 10 \end{cases}$$

Como Diofanto só admitia soluções racionais positivas, poderemos tomar por exemplo $x=a+1$ e $y=9-a$ ou $x=a+5$ e $y=5-a$, pois $x+y$ continua valendo 10, e o que devemos procurar são os possíveis valores para a que fornecem raízes racionais positivas. Tomando $x=a+5$ e $y=5-a$ e sendo $-5<a<5$ a solução, caso exista, será racional positiva. Assim:

$(a+5)^3+(5-a)^3=370 \Rightarrow (a^3+15a^2+75a+125)+(125-75a+15a^2-a^3)=370$ $\Rightarrow 30a^2+250=370 \Rightarrow 30a^2=120$ $a^2=4 \Rightarrow a=2$.

Portanto, $x = a + 5 \Rightarrow x = 7$ e $y = 5 - a \Rightarrow y = 3$.

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

Solução:

Considere o número prescrito como sendo 60. Teremos então o seguinte sistema:

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

De $(i) + (ii)$ temos $8x + 5y + 60 = (x+y)^2$. Seja $x + y = a$, neste caso temos que $8x + 5y + 60 = a^2$. Como Diofanto buscava soluções racionais positivas, da equação acima tiramos as seguintes conclusões:

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

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

Como $a^2 - 60$ é um quadrado, podemos escrevê-lo como $(a-b)^2$, donde $-60 = -2ab + b^2$, desse modo, $a = \dfrac{60+b^2}{2b}$ e $11 \leqslant \dfrac{60+b^2}{2b} \leqslant 12$. Concluímos assim que $19 \leqslant b \leqslant 21$.

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

Por (iii) temos que $y = \dfrac{79}{12}$ e (iv) resulta em $x = \dfrac{59}{12}$.

Baseado nos problemas contidos na obra de Diofanto, é possível ter uma noção do desenvolvimento da teoria dos números até àquela época.

As equações chamadas de diofantinas possuem infinitas formas, visto que é suficiente possuir coeficientes e soluções, caso exista, no conjunto dos números inteiros.

Portanto, nos deteremos a estudar as equações diofantinas lineares no capítulo seguinte.

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

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

3 EQUAÇÕES DIOFANTINAS LINEARES

Neste capítulo apresentaremos as equações diofantinas lineares de n variáveis e veremos como encontrar a solução geral dessas equações, caso exista. Antes, na primeira seção, vamos introduzir o conceito de divisibilidade que facilitará a apresentação das seções seguintes.

3.1 Divisibilidade em $\mathbb{Z}$

No Ensino Básico a divisão com resto é tratada apenas no contexto dos números naturais $\mathbb{N}$. No entanto, essa operação pode ser considerada no domínio mais amplo dos números inteiros $\mathbb{Z}$. Essa possibilidade é estabelecida pelo algoritmo de Euclides, conforme o resultado abaixo.

Teorema 3.1.1 *(Algoritmo de Euclides) Para quaisquer* $a, b \in \mathbb{Z}$*, com* $b \neq 0$*, existe um único par de inteiros* q *e* r*, de modo que* $a = b \cdot q + r$ *e* $0 \leqslant r < |b|$.

Prova: Inicialmente vamos supor $b > 0$. Observe que se o teorema for provado com essa hipótese adicional, então o caso $b < 0$ seguirá como consequência. Com efeito, se tivermos $b < 0$, então $-b > 0$. Assim, pelo caso supostamente provado, existem $q, r \in \mathbb{Z}$ tais que

$$-a = (-b) \cdot q + r, \text{ com } 0 \leqslant r < |-b| = -b = |b|.$$

Se $r = 0$, teremos $a = b.q$. Se $r > 0$, escrevemos

$$a = b \cdot q - r = b \cdot (q+1) - b - r = b \cdot (q+1) + |b| - r.$$

É claro que $0 \leqslant |b| - r < |b|$. Passemos ao caso $b > 0$. O conjunto $\{q \in \mathbb{N} | (q+1) \cdot b > a\}$ não é vazio pois o conjunto dos múltiplos de b é ilimitado, posto que é infinito. Assim, o princípio da boa ordenação garante que esse conjunto possui elemento mínimo (único!). Em outras palavras, existe $q \in \mathbb{N}$, tal que $b \cdot q \leqslant a < b \cdot (q+1)$.

Dessa forma, definindo $r = a - b \cdot q$ segue que $0 \leqslant r < b$ e $a = b \cdot q + r$.

Por fim, para garantir a unicidade, basta observar que se $q', r' \in \mathbb{Z}$ são tais que $a = b \cdot q' + r'$, com $0 \leqslant r' < b$, então $b \cdot q' \leqslant a < b \cdot (q'+1)$. Isso nos diz que q' coincide com o elemento mínimo de $\{q \in \mathbb{N} | (q+1) \cdot b > a\}$. A unicidade de q garante a unicidade de r.

Observação 3.1.1 *No caso em que* $r = 0$*, dizemos que a divisão é exata. Também dizemos que* a *é múltiplo de* b*, ou que* b *é um divisor de* a*, ou ainda que* b *divide* a*. A notação* $b|a$ *será usada para indicar esse fato.*

3.2 O máximo divisor comum

Dado $a \in \mathbb{Z}$, o conjunto dos divisores positivos de a será denotado por $D(a)$. Portanto,

$$D(a) = \{b \in \mathbb{N}^*; b|a\}.$$

Note que dados $a, b \in \mathbb{Z}$, com $b \neq 0$, temos que $b|a$ se, e somente se, $a = b \cdot q$ para algum $q \in \mathbb{Z}$. Assim, para $a = 0$, podemos tomar $q = 0$ e concluir que $D(0) = \{1, 2, 3, 4, \ldots\}$. Por outro lado, se tivermos $a \neq 0$, então $q \neq 0$ e portanto, $|q| \geqslant 1$. Daí, segue que $|a| = |b| \cdot |q| \geqslant |b|$. Em particular, para todo $b \in D(a)$ temos $b \leqslant |a|$. Isso nos diz que $D(a)$ é limitado e portanto, finito.

Dessa forma, se $m, n \in \mathbb{Z}$ não são ambos nulos, tem-se que $D(m) \cap D(n)$ é finito e não é vazio (pois $1 \in D(a) \cap D(b)$). Portanto, $D(m) \cap D(n)$ possui elemento máximo. Esse elemento máximo é chamado de máximo divisor comum de m e n, e é denotado por $mdc(m, n)$. Assim, escrevemos:

$$mdc(m, n) = \max (D(m) \cap D(n)).$$

Observação 3.2.1 *Alguns autores também adotam a notação* (a,b) *para indicar mdc. Embora essa notação seja mais econômica, tem a desvantagem de se confundir com a notação de par ordenado.*

Teorema 3.2.1 *(Bézout) Se d é o máximo divisor comum de a e b, d = mdc(a,b), então há inteiros m, n tais que* $d = am + bn$*, e além disso* d *é o menor inteiros positivo que pode ser escrito como combinação linear de* a *e* b.

Prova: Defina $A = am + bn$, o conjunto de todas as combinações lineares de $am + bn$, com m e $n \in \mathbb{Z}$. Veja que esse conjunto possui elementos positivos, negativos e o zero. Tome $c \in A$ tal que c é o menor inteiro positivo.

Afirmação: $c|a$ e $c|b$.

Suponha inicialmente que $c \nmid a$, então pelo teorema 3.1.1 podemos escrever a de modo único como $a = qc + r$, com $0 < r < c$. Assim, $r = a - qc = a - q(am + bn) = a(1 - qm) + (-qn)b$, note que $(1 - qm)$ e $(-qn)$ são inteiros, e portanto $r \in A$, o que é uma contradição, pois $0 < r < c$, e c é o menor inteiro positivo de A. Concluímos assim que $c \mid a$. É análoga a demonstração de que $c \mid b$.

Para a segunda afirmação do teorema seja $d = mdc(a, b)$, logo $a = dx$ e $b = dy$. como $c = am + bn$, então $c = dxm + dyn \Rightarrow c = d(xm + yn) \Rightarrow d \mid c$, assim $d \leqslant c$, mas $d < c$ não pode acontecer pois d é o máximo divisor comum de a e b. Concluímos assim que $c = d$, isto é, o $d = mdc(a, b)$ é o menor número inteiro positivo contido em A.

Proposição 3.2.2 *Sejam* $a, b, n \in \mathbb{Z}$ *tais que ,* na *e* nb *não são ambos nulos, então mdc*$(na, nb) = n.mdc(a, b)$.

Prova: Tome $d = mdc(na, nb)$, pelo teorema de Bézout existem x e y em $\mathbb{Z}$ tais que $nax + nby = d$, e além disso d é o menor valor possível que pode ser escrito como combinação linear

de $nax + nby$. Como $nax + nby$ é o mesmo que $n(ax + by)$, isto é, n vezes o menor valor possível de $ax + by$ que é $n.mdc(a, b)$.

Proposição 3.2.3 *Se* $mdc(a, b) = d$, *temos que* $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Prova: Suponha que exista um número natural $c > 1$ tal que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = c$, então $c|\frac{a}{d}$ e $c|\frac{b}{d}$, mas daí $c|a$ e $c|b$ em particular, e desse modo o mdc(a,b) = *dc*, contrariando a hipótese de d ser o máximo divisor comum.

Proposição 3.2.4 *(Lema de Euclides) Para quaisquer* $a, b, c \in \mathbb{Z}$, *se* $a \mid b.c$ *e* $mdc(a, b) = 1$ *então* $a \mid c$.

Prova: Se $a \mid b.c$, então existe $n \in \mathbb{Z}$ tal que $bc = na$. Como $mdc(a, b) = 1$, pelo teorema de Bézout existem $p, q \in \mathbb{Z}$ tais que $ap + bq = 1$. Assim, temos $cap + cbq = c$ e sabendo que $bc = na$, resulta em:

$$cap + naq = c \Rightarrow c = a(cp + nq).$$

Portanto, $a \mid c$.

3.3 Equações diofantinas lineares com duas variáveis

Denominaremos equações do tipo $ax + by = c$ com os números inteiros a, b e c, bem como as soluções x e y, de equações lineares diofantinas, em homenagem a Diofanto, considerado por muitos o pai da álgebra e percussor da teoria dos números.

Equações desse tipo nem sempre possuem soluções no conjunto dos inteiros, como exemplo, observe equação $2x + 4y = 5$. Supor que há solução é supor que $2x + 4y = 2(x + 2y)$ resulta em um número ímpar, o que é um absurdo!

Observação 3.3.1 *A equação* $2x + 4y = 5$, *quando analisada analiticamente num plano, representa uma reta. Mostrar que a equação não possui soluções inteiras significa dizer que esta reta não possui pontos de coordenadas*(x, y), *com* x *e* y *inteiros.*

3.3.1 Existência de soluções

Estabeleceremos a seguir condições para que equações do tipo $ax+by = c$ possuam soluções inteiras.

Teorema 3.3.1 *A equação diofantina* $ax + by = c$, *com* $a \neq 0$ *ou* $b \neq 0$, *terá solução inteira se, e somente se,* $d = mdc(a, b)$ *divide c. Além disso,* (x_0, y_0) *é uma solução particular, então todas as soluções são dadas por* $x = x_0 + \frac{b}{d}k$, $y = y_0 - \frac{a}{d}k$, *com* $k \in \mathbb{Z}$.

Prova:

$\Rightarrow$) Admita que a equação $ax + by = c$ possui solução inteira, digamos (x_0, y_0), ou seja, $ax_0 + by_0 = c$. Assim, temos que $d|ax_0$ e $d|by_0$, pois $d|a$ e $d|b$. Logo, tem-se que $d|ax + by = c$, isto é, $d|c$.

$\Leftarrow$) Suponha que $d = mdc(a, b)$ divide c, mostraremos agora que a equação diofantina tem solução nos conjuntos dos números inteiros. Como $d|c$, então existe um inteiro k tal que $c = kd$, e como $d = mdc(a, b)$, pelo teorema de Bézout existem inteiros m e n tais que $am + bn = d$. Temos que $k(am + bn) = kd$, donde $akm + bkn = c$. Como km e kn são inteiros tome $km = x$ e $kn = y$, logo o par (km, kn) é uma solução da equação $ax + by = c$.

Provaremos agora a segunda parte do teorema, isto é, uma vez constatado que a equação diofantina $ax + by = c$ possui uma solução (x_0, y_0), todas as demais soluções dessa equação são da forma $x = x_0 + \frac{b}{d}k$, $y = y_0 - \frac{a}{d}k$, com $k \in \mathbb{Z}$.

Seja (x, y) uma solução de $ax+by = c$, como (x_0, y_0) é uma solução particular, isto é $ax_0+by_0 = c$, temos que $ax+by-(ax_0+by_0) = 0$, donde segue que $(x-x_0)+b(y-y_0) = 0$. Concluímos daí que $a(x - x_0) = b(y - y_0)$, dividindo os dois membros por d ficamos com:

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

Como o $mdc(\frac{a}{d}, \frac{b}{d}) = 1$ segue do lema de Euclides que $\frac{b}{d}|(x - x_0)$. Assim deve existir um k inteiro tal que $x = x_0 + \frac{b}{d}k$. Substituindo x pela expressão equivalente temos:

$$\frac{a}{d}(x_0 + \frac{b}{d}k - x_0) = \frac{b}{d}(y - y_0) \Rightarrow \frac{a}{d} \cdot \frac{b}{d}k = \frac{b}{d}y - y_0 \Rightarrow \frac{a}{d}k = (y - y_0) \Rightarrow y = y_0 - \frac{a}{d}k,$$

como queríamos demonstrar.

Observação 3.3.2 *Um argumento alternativo para a parte final da demonstração anterior é observar que a equação*

$$a(x - x_0) + b(y - y_0) = 0$$

revela que o vetor $(x-x_0, y-y_0)$ *é ortogonal ao vetor* (a, b). *Como o complementar ortogonal em* $\mathbb{R}^2$ *do espaço gerado por* (a, b) *é o espaço gerado por* $(-b, a)$, *segue que existe* $\lambda \in \mathbb{R}$ *tal que* $(x - x_0, y - y_0) = \lambda(-b, a)$. *Como estamos tratando de soluções inteiras, concluímos que* $\lambda \in \mathbb{Q}$. *Assim, podemos escrever* $\lambda = \frac{m}{n}$, *com* $mdc(m, n) = 1$. *Por fim, basta notar que as igualdades*

$$x - x_0 = -\frac{m}{n}b \text{ e } y - y_0 = \frac{m}{n}a$$

implicam que n *divide* a *e também divide* b. *Logo, temos que* $n|d$ *e* λ *pode ser reescrito na forma* $\lambda = \frac{k}{d}$, *com* $k = m \cdot \frac{d}{n} \in \mathbb{Z}$.

Abaixo seguem alguns exemplos da utilização desse teorema .

Exemplo 1 *: Carlos sacou RS* $50,00$ *no caixa automático. Sabendo que esse caixa só possuía notas de RS* $5,00$ *e de RS* $10,00$, *de quantas formas poderá vir esse valor?*

Solução: Se x denota a quantidade de notas de 5 reais e y a quantidade de notas de 50 reais, então a equação correspondente é $5x + 10y = 50$. O problema é resolvido determinando-se todas as soluções não negativas e inteiras.

Sendo o $mdc(5, 10) = 5$, e $5 \mid 50$, nossa equação possui solução! Escrevendo o $mdc(5, 10)$ como combinação linear de 5 e 10, temos que $5 = (-1).5 + (1).10$. Como queremos resolver a equação $5x + 10y = 50$, vamos multiplicar ambos os lados por 10. Assim, $5.(-10) + 10.(10) = 50$, logo $x_0 = -10$ e $y_0 = 10$ é uma solução particular da equação.

A solução geral é da forma:

$$x = -10 + \frac{10}{5}k \text{ e } y = 10 - \frac{5}{5}k \text{ , com } k \in \mathbb{Z}.$$

Isto é, $x = -10+2k$ e $y = 10-k$. Como nos interessa soluções inteiras não negativas, devemos ter $-10 + 2k \geqslant 0$ e $10 - k \geqslant 0 \Rightarrow k \geqslant 5$ e $10 \geqslant k$, respectivamente. Assim:

$$k = 5 \Rightarrow x = 0 \text{ e } y = 5$$
$$k = 6 \Rightarrow x = 2 \text{ e } y = 4$$
$$k = 7 \Rightarrow x = 4 \text{ e } y = 3$$
$$k = 8 \Rightarrow x = 6 \text{ e } y = 2$$
$$k = 9 \Rightarrow x = 8 \text{ e } y = 1$$
$$k = 10 \Rightarrow x = 10 \text{ e } y = 0.$$

Concluímos assim que há 6 maneiras distintas de Carlos sacar RS 50, 00.

Exemplo 2 *: Sofia encomendou laranjas e maçãs para abastecer seu mercantil, gastou um total de 158 reais. Sabendo que ela comprou 38 dúzias de maçãs e 22 dúzias de laranjas, e que o preço de cada dúzia é um número inteiro positivo, quais os possíveis preços das dúzias de cada fruta?*

Solução: Se x denota o preço da dúzia da maçã e y refere-se ao preço da dúzia da laranja, então a equação correspondente é $38x + 22y = 158$. O problema é resolvido determinando-se todas as soluções positiva e inteiras. Podemos determinar o $mdc(38, 22)$ da seguinte forma:

	1	*1*	*2*	*1*	*2*
38	*22*	*16*	*6*	*4*	*2*
16	*6*	*4*	*2*	*0*	

Assim temos que $mdc(38, 22) = 2$, e como $2 \mid 158$, nossa equação possui solução! Usando o algoritmo da divisão temos as seguintes igualdades:

$$38 = 22.1 + 16$$
$$22 = 16.1 + 6$$
$$16 = 6.2 + 4$$
$$6 = 4.1 + 2$$
$$4 = 2.2$$

Podemos escrever o $mdc(38,22) = 2$ como combinação linear de 38 e 22, temos nesse caso que:

$$\begin{aligned}
2 &= 6 - 4.1 \\
2 &= 6 - (16 - 6.2).1 = 3.6 - 16.1 \\
2 &= 3 - (22 - 16.1) - 16.1 = 3.22 - 4.16 \\
2 &= 3.22 - 4.(38 - 22.1) = -4.38 + 7.22
\end{aligned}$$

Logo, $2 = -4.38 + 7.22(i)$.

Como queremos resolver a equação $38x + 22y = 158$, vamos multiplicar ambos os lados de (i) por 79. Assim, $158 = -316.38 + 553.22$, logo $x_0 = -316$ e $y_0 = 553$ é uma solução particular da equação.

A solução geral é da forma:

$$x = -316 + \frac{22}{2}k \quad \text{e} \quad y = 553 - \frac{38}{2}k \text{ , com } k \in \mathbb{Z}.$$

Isto é, $x = -316 + 11k$ e $y = 553 - 19k$. Como nos interessa soluções inteiras positivas, devemos ter $-316+11k > 0$ e $553-19k > 0 \Rightarrow k > \frac{316}{11}$ e $\frac{553}{19} > k$, respectivamente. Assim, $k = 29$ é o único inteiro dentro das condições do problema. Concluímos, portanto, que o preço da dúzia da maçã é $x = -316 + 11k = 3$ reais e o preço da dúzia da laranja é $y = 553 - 19k = 2$ reais.

3.4 Equações diofantinas lineares com três variáveis

As equações do tipo $ax + by + cz = t$, com os números inteiros a, b, c e t, bem como as soluções x, y e z, são denominadas equações diofantinas lineares de três variáveis. Estudaremos a seguir a existência de soluções.

3.4.1 Solução particular

Afirmação: *A equação* $ax + by + cz = t$ *admite solução se, e somente se,* $d = mdc(a,b,c)$ *divide* t.

É claro que se a equação possuir solução então $d|t$, a verificação segue o mesmo raciocínio utilizado na demonstração do teorema 3.3.1. Reciprocamente, se $d|t$, considere $d' = mdc(a,b)$ e observe que $d = mdc(d',c)$. Nesse caso, pelo teorema de Bézout da seção anterior $\exists u, v, k$ e w, tais que $d' = au + vb$ e $d = kd' + cw$, isto é:

$$d = (ua + vb)k + cw \Rightarrow d = auk + bvk + cw.$$

Tomando $uk = x_0$, $vk = y_0$ e $w = z_0$, teremos $d = ax_0 + by_0 + cz_0$. Daí, como $d|t$, existe um número inteiro q, tal que $t = dq$.

Veja que:

$$d = ax_0 + by_0 + cz_0 \Rightarrow t = dq = aqx_0 + bqy_0 + cqz_0.$$

Logo, (qx_0, qy_0, qz_0) é uma solução particular de $ax + by + cz = t$.

Exemplo 3 *: Determine uma solução particular para a equação* $30x + 27y + 15z = 6$.

Solução: Calculemos inicialmente o $mdc(30, 27)$ usando o algoritmo da divisão, da seguinte forma:

	1	*9*
30	*27*	*3*
3	*0*	

Logo, $30 = 27.1 + 3 \Rightarrow 3 = 30 - 27.1$. Assim, o $mdc(30, 27) = 3$. Aplicando novamente o algoritmo da divisão para calcular o $mdc(3, 15)$ temos:

	5
15	*3*
0	

Assim, $15 = 3.5 + 0$ e portanto o $mdc(3, 15) = 3$. Escrevendo o mdc como combinação linear de 30, 27 e 15 temos $3 = 1.30 - 27.1 + 0.15$, multiplicando por 2 ambos os lados, resulta em $6 = 2.30 - 2.27 + 0.15$, portanto, $(2, -2, 0)$ é uma solução particular da equação dada.

3.4.2 Solução geral

Seguindo a linha de raciocínio apresentada por CAMPOS[1], sejam a, b e $c \in \mathbb{Z}$ e não nulos simultaneamente, e $t \in \mathbb{Z}_+$, sabemos que a equação $ax + by + cz = t$ possuirá solução se, e somente se, $d = mdc(a, b, c)|t$. Considere inicialmente $ax + by = k$, logo teremos uma nova equação, da forma $k + cz = t$ que possui solução, pois $d' = mdc(1, c) = 1$ e $1 \mid t$. Pelo teorema 3.3.1 sabemos ainda que a solução geral dessa equação é da forma:

$$k = k_0 + \frac{c}{d'}l,\ z = z_0 - \frac{1}{d'}l, \text{ com } l \in \mathbb{Z}.$$

Temos portanto $k = k_0 + cl$ e $z = z_0 - cl$ pois $d' = 1$. Observemos agora que $ax + by = k = k_0 + cl$ e note que a escolha de certa de l é fundamental, visto que o $mdc(a, b)$ deve dividir $k = k_0 + cl$.

Por fim, $ax + by = k$ tem como solução geral, devido ao teorema 3.3.1:

$$x = x_0 + \frac{b}{mdc(a, b)}l',\ y = y_0 - \frac{a}{mdc(a, b)}l', \text{ com } l' \in \mathbb{Z}.$$

[1]CAMPOS, G. D. M. Equações Diofantinas Lineares. Disponível em: bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/558/2011_00462_GISELI_DUARDO_ MACIANO _ CAMPOS.pdf. Acessado em 15/01/2014.

Concluímos que a solução geral da equação $ax + by + cz = t$, caso exista, é da forma:

$$(\ x = x_0 + \frac{b}{mdc(a,b)}l',\ y = y_0 - \frac{a}{mdc(a,b)}l'\ ,\ z = z_0 - \frac{1}{d'}l) \textit{ com } l, l' \in \mathbb{Z}.$$

Exemplo 4 *: Determine a solução geral para a equação* $30x + 27y + 15z = 6$.

Solução: Seja $k = 30x + 27y$, então $1.k + 15.z = 6$. Como o $mdc(1,15) = 1$ e $1 \mid 6$, a equação tem solução. Podemos escrever o $mdc(1,15)$ como combinação linear de 1 e 15, isto é, $1 = 1.(-14) + 15.(1)$, multiplicando ambos os lados por 6 temos:

$6 = 1.(-84) + 15.(6)$. Sendo $(-84, 6)$ uma solução particular, o teorema 3.3.1 nos diz que a solução geral é da forma:

$k = k_0 + \frac{15}{1}l$ e $z = z_0 - \frac{1}{1}l$, com $l \in \mathbb{Z}$, o que resulta em $k = -84 + 15l$ e $z = 6 - l$.

Analisemos agora $k = 30x + 27y = -84 + 15l$, observe que obrigatoriamente o $mdc(30, 27) = 3$ deve dividir $-84 + 15l$, como $3 \mid 84$ e $3 \mid 15$, não precisaremos nos preocupar com o l. Sabemos pelo exemplo anterior que $3 = 30.1 + 27.(-1)$, donde multiplicando ambos os lados por $\frac{-84+15l}{3}$ obtemos a seguinte expressão:

$$\left(\frac{-84+15l}{3}\right).3 = 30.1.\left(\frac{-84+15l}{3}\right) + 27.(-1).\left(\frac{-84+15l}{3}\right).$$

Assim, $-84 + 15l = 30(-28 + 5l) + 27.(28 - 5l)$. Concluímos novamente pelo teorema 3.3.1 que a solução geral dessa equação é:

$x = x_0 + \frac{27}{3}l'$ *e* $y = y_0 - \frac{30}{3}l'$ *, com* $l' \in Z$ *, isto é,* $x = -28 + 5l + 9l'$ *e* $y = 28 - 5l - 10l'$.

Portanto, a solução geral é da forma :

$$(-28 + 5l + 9l', 28 - 5l - 10l', 6 - l).$$

3.5 Equações diofantinas lineares com n variáveis

Denomina-se equações diofantinas lineares com n variáveis, expressões do tipo $a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + ... + a_nx_n = y$, onde $a_1, ..., a_n$ não são simultaneamente nulos e pertencem aos inteiros. Nosso interesse é determinar a solução geral no conjunto dos inteiros, se existir, $x_1, ..., x_n$.

Aplicando o mesmo procedimento de CAMPOS[1], cuja ideia está na demonstração do teorema 3.3.1, constatamos que esse tipo de equação possui solução se o $mdc(a_1...a_n) \mid y$.

3.5.1 Solução particular

Para a obtenção de uma solução particular de $a_1x_1+a_2x_2+a_3x_3+a_4x_4+...+a_nx_n = y$ observemos que:

Se $d_1 = mdc(a_1, a_2)$, então existe b_1 e $b_2 \in \mathbb{Z}$ tais que $a_1 = b_1 d_1$ e $a_2 = b_2 d_1$. Tome agora $d_2 = mdc(d_1, a_3)$, então existe b_3 e $b_4 \in \mathbb{Z}$ tais que $d_1 = b_3 d_2$ e $a_3 = b_4 d_2$. Em particular, percebe-se que $d_2 \mid a_1, a_2, a_3$.

Fazendo $d_3 = mdc(d_2, a_4)$, então existe b_5 e $b_6 \in \mathbb{Z} \in$ tais que $d_2 = b_5 d_3$ e $a_4 = b_6 d_3$. Note que $d_3 \mid a_1, a_2, a_3, a_4$. Continuando esse processo, percebemos por indução que $d_{n-1} = mdc(d_{n-2}, a_n)$. Assim, $d_{n-1} \mid a_1, a_2, a_3, ..., a_n$, e como $d_{n-1} = mdc(d_{n-2}, a_n)$ então $d = d_{n-1} = mdc(a_1, a_2, a_3, ..., a_n)$, isto é, podemos escrever d como combinação linear dos a_s da seguinte forma:

$$d = a_1 x_{1'} + a_2 x_{2'} + a_3 x_{3'} + a_4 x_{4'} + ... + a_n x_{n'}.$$

E como $d \mid y$, existe um $p \in \mathbb{Z}$ tal que:

$$dp = y = a_1 x_{1'} p + a_2 x_{2'} p + a_3 x_{3'} p + a_4 x_{4'} p + ... + a_n x_{n'} p.$$

Concluímos assim que, caso exista, $(x_{1'} p, x_{2'} p, ..., x_{n'} p)$ é um solução particular de $a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + ... + a_n x_n = y$.

3.5.2 Solução geral

Tomando como base o método aplicado por CAMPOS[2], vemos que o mesmo processo utilizado na determinação da solução geral de equações diofantinas lineares de três variáveis pode ser usado para encontrar a solução geral quando o números de variáveis é n. Inicialmente chamamos $a_1 x_1 + a_2 x_2 + a_3 x_3 + a_4 x_4 + ... + a_{n-1} x_{n-1} = k_1$ e resolvemos a equação em duas variáveis resultante, isto é, $1.k_1 + a_n x_n = y$, onde $1 = d_1 = mdc(1, a_n) \mid y$, e a solução geral é da forma:

$$k_1 = k_{1_0} + \frac{a_n}{mdc(1, a_n)} l_n,\ x_n = x_{n_0} - \frac{1}{mdc(1, a_n)} l_n \text{ ,com } l_n \in \mathbb{Z}.$$

Após n-1 aplicações obteremos os valores dos x_s, e portanto a solução geral que se apresenta do seguinte modo:

$$\begin{gathered} x_1 = x_{1_0} + \frac{a_2}{mdc(a_1, a_2)} l, \\ x_2 = x_{2_0} - \frac{a_1}{mdc(a_1, a_2)} l, \\ x_3 = x_{3_0} - l_3 \\ . \\ . \\ . \\ x_n = x_{n_0} - l_n \end{gathered}$$

[2]CAMPOS, G. D. M. Equações Diofantinas Lineares. Disponível em: bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/558/2011_00462_GISELI_DUARDO_ MACIANO _ CAMPOS.pdf. Acessado em 15/01/2014.

com $l, l_i \in \mathbb{Z}, 3 \leqslant i \leqslant n$.

Exemplo 5 *: Determine a solução geral de* $2u + 16v - 14x + 4y - 6z = 8$.

Solução: Observando inicialmente que o $mdc(2, 16, 14, 4, 6) = 2$ e que $2 \mid 8$, constatamos que essa equação possui solução no conjunto dos inteiros.

Tome $2u + 16v - 14x + 4y = k_1$, teremos então uma nova equação diofantina em duas variáveis, a saber $1.k_1 - 6z = 8$. Como $mdc(1, 6) = 1$ e $1 \mid 8$, ela possui solução. Em particular podemos escrever o $mdc(1, 6)$ como combinação linear de 1 e 6. Assim temos $1 = 1.(7) - 6.(1)$. Como nos interessa a solução da equação $1.k_1 - 6z = 8$, multiplicaremos ambos os lados por 8, obtendo assim $8 = 1.(56) - 6.(8)$. Note que $k_1 = 56$ e $z = 8$ é uma solução particular da equação. A solução geral é portanto:

$$k_1 = 56 + (-6)l_1;$$
$$z = 8 - l_1 \text{ , com } l_1 \in \mathbb{Z} \text{ .}$$

Assim, temos que $2u + 16v - 14x + 4y = k_1 = 56 + (-6)l_1$, isto é, resolveremos agora $2u + 16v - 14x + 4y = 56 + (-6)l_1$.

Tome $2u + 16v - 14x = k_2$, logo temos $1k_2 + 4y = 56 + (-6)l_1$, como $mdc(1, 4) = 1$ e $1 \mid 56 + (-6)l_1$, essa equação possui solução. Escrevendo como combinação linear do $mdc(1, 4) = 1$ teremos $1 = 1.(-3) + 4.(1)$, multiplicando ambos os lados por $\dfrac{56 + (-6)l_1}{mdc(1,4)}$ teremos:

$$(56 - 6.l_1).1 = 1.(-3).(56 - 6.l_1) + 4.(1).(56 - 6.l_1), \text{ que resulta em}$$
$$56 - 6.l_1 = 1.(-168 + 18l_1) + 4.(56 - 6.l_1).$$

Note que $k_2 = -168 + 18l_1$ e $y = 56 - 6.l_1$ é uma solução particular da equação. A solução geral é da forma:

$$k_2 = -168 + 18l_1 + \frac{4}{mdc(1,4)}l_2;$$
$$y = 56 - 6.l_1 - \frac{1}{mdc(1,4)}l_2, \text{ com } l_2 \in \mathbb{Z} \text{ .}$$

Assim, temos que $2u + 16v - 14x = k_2 = -168 + 18l_1 + 4l_2$, isto é, resolveremos $2u + 16v - 14x = -168 + 18l_1 + 4l_2$. Tome $2u + 16v = k_3$, logo temos $1k_3 - 14x = -168 + 18l_1 + 4l_2$. Como $mdc(1, 14) = 1$ e $1 \mid -168 + 18l_1 + 4l_2$, essa equação possui solução. Escrevendo como combinação linear do $mdc(1, 14) = 1$ teremos $1 = 1.(15) - 14.(1)$, multiplicando ambos os lados por $\dfrac{-168 + 18l_1 + 4l_2}{mdc(1,14)}$ teremos:

$(-168 + 18l_1 + 4l_2).1 = 15.(-168 + 18l_1 + 4l_2) - 14.(-168 + 18l_1 + 4l_2)$, que resulta em
$-168 + 18l_1 + 4l_2 = 1.(-2520 + 270l_1 + 60l_2) - 14.(-168 + 18l_1 + 4l_2)$.

Note que $k_3 = -2520 + 270l_1 + 60l_2$ e $x = -168 + 18l_1 + 4l_2$ é uma solução particular da equação. A solução geral é da forma:

$$k_3 = -2520 + 270l_1 + 60l_2 + \frac{-14}{mdc(1,14)}l_3;$$
$$x = -168 + 18l_1 + 4l_2 - \frac{1}{mdc(1,14)}l_3, \text{ com } l_3 \in \mathbb{Z}\,.$$

Assim, temos que $2u + 16v = k_3 = -2520 + 270l_1 + 60l_2 - 14l_3$, resolveremos portanto $2u + 16v = -2520 + 270l_1 + 60l_2 - 14l_3$. Como $mdc(2,16) = 2$ e $2 \mid -2520 + 270l_1 + 60l_2 - 14l_3$, essa equação possui solução. Escrevendo como combinação linear do $mdc(2,16) = 2$ teremos $2 = 2.(9) + 16.(-1)$, multiplicando ambos os lados por $\left(\frac{-2520 + 270l_1 + 60l_2 - 14l_3}{mdc(2,16)}\right)$ teremos:

$$\left(\frac{-2520 + 270l_1 + 60l_2 - 14l_3}{2}\right) \times 2 =$$
$$2 \times 9 \times \left(\frac{-2520 + 270l_1 + 60l_2 - 14l_3}{2}\right) + 16.(-1).\left(\frac{-2520 + 270l_1 + 60l_2 - 14l_3}{2}\right),$$

que resulta em:

$-2520 + 270l_1 + 60l_2 - 14l_3 = 2.(-1134 + 1215l_1 + 270l_2 - 63l_3) + 16(1260 - 135l_1 - 30l_2 + 7l_3)$.

Note que $u = -1134 + 1215l_1 + 270l_2 - 63l_3$ e $v = 1260 - 135l_1 - 30l_2 + 7l_3$ é uma solução particular da equação. A solução geral é da forma:

$$u = -1134 + 1215l_1 + 270l_2 - 63l_3 + \frac{16}{2}l_4;$$
$$v = 1260 - 135l_1 - 30l_2 + 7l_3 - \frac{2}{2}l_4, \text{com } \; l_4 \in \mathbb{Z}\,.$$

Concluímos assim que as soluções da equação diofantina linear $2u + 16v - 14x + 4y - 6z = 8$, com 5 variáveis é:
$u = -1134 + 1215l_1 + 270l_2 - 63l_3 + 8l_4;$
$v = 1260 - 135l_1 - 30l_2 + 7l_3 - l_4;$
$x = -168 + 18l_1 + 4l_2 - l_3;$
$y = 56 - 6.l_1 - l_2;$
$z = 8 - l_1$, com $l_i \in \mathbb{Z}, i = 1,2,3,4\,.$

Finalizamos assim o estudo das equações diofantinas lineares para uma quantidade n de variáveis.

No capítulo seguinte estudaremos uma equação diofantina quadrática especial, conhecida mundialmente como Teorema de Pitágoras. Abordaremos também uma equação diofantina quadrática específica: $ax^2 + by^2 = c$, e na procura por soluções utilizaremos o método das secantes e tangentes de Fermat.

4 PONTOS RACIONAIS DE UMA CÔNICA IRREDUTÍVEL

Neste capítulo faremos um estudo sobre as equações diofantinas quadráticas conhecidas como ternas pitagóricas, veremos como obter todas as soluções inteiras e utilizaremos o método das secantes e tangentes de Fermat para a obtenção de pontos racionais sobre cônicas irredutíveis, a saber a elipse, a parábola e a hipérbole. Analisaremos por fim uma equação diofantina especial, conhecida como o último teorema de Fermat.

4.1 Equações diofantinas quadráticas: as clássicas ternas pitagóricas

Embora haja provas de que muito antes de Pitágoras os babilônios já sabiam e utilizavam o fato de que o quadrado da hipotenusa é igual à soma dos quadrados dos catetos num triângulo retângulo, a sua primeira demonstração foi dada provavelmente por Pitágoras e hoje esse resultado é conhecido mundialmente por teorema de Pitágoras.

Os estudos de Pitágoras e sua irmandade eram focalizados nos números inteiros e frações, isto é, o que conhecemos por números racionais.

Analisaremos agora as soluções inteiras (x, y, z) da equação diofantina da forma $x^2 + y^2 = z^2$, onde x, y, e z são não nulos. Consideremos inicialmente o terno composto pelos números inteiros $(3, 4, 5)$, esses termos constituem os lados de um triângulo retângulo, pois satisfaz a equação de Pitágoras $x^2 + y^2 = z^2$, e chamado por esse motivo de triplas ou ternas pitagóricas.

4.1.1 A infinitude das ternas Pitagóricas (Demonstração de Euclides)

Segundo SINGH[1], Euclides, nascido no ano de 330 a.C., demonstrou que a quantidade de ternas pitagóricas era infinita da seguinte forma:

Observou primeiramente que uma terna pitagórica é formada por três números inteiros, onde um número ao quadrado é resultado da soma de dois outros números, ambos ao quadrado, e também que a diferença entre dois quadrados consecutivos é sempre um número ímpar, isto é:

$$1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16, \quad 5^2 = 25, \quad 6^2 = 36...$$
$$\text{e} \quad 4 - 1 = 3, \quad 9 - 4 = 5, \quad 16 - 9 = 7, \quad 25 - 16 = 9, \quad 36 - 25 = 11...$$

Observando a sequência infinita de ímpares gerada $(3, 5, 7, 9, 11, ...)$, ele concluiu que cada um desses infinitos ímpares podem ser somados a um número ao quadrado de forma que outro número ao quadrado é criado, isto é, $3 + 1^2 = 4$, $5 + 2^2 = 9$, $7 + 3^2 = 16$, e assim sucessivamente. Como parte desses ímpares são números também ímpares ao quadrado, por

[1]SINGH, Simon. O Último teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos. 10. ed. Rio de Janeiro: Record, 2001.

exemplo, $3^2 = 9$, $5^2 = 25$ e $7^2 = 49$, e sabendo que uma parte desses infinitos números também são infinitos, ele concluiu que deve existir uma quantidade infinita de ternos pitagóricos.

Afirmação: *Todo natural ímpar maior que dois faz parte de alguma terna pitagórica.*

De fato, se n é ímpar, então pelo raciocínio de Euclides, n é o resultado da diferença de dois quadrados consecutivos, isto é, existe um $x \in \mathbb{N}$ tal que $n^2 = (x+1)^2 - x^2$, logo $n^2 = x^2 + 2x + 1 - x^2 \Rightarrow x = \dfrac{n^2-1}{2}$. Assim, teremos: $n^2 = \left(\dfrac{n^2-1}{2} + 1\right)^2 - \left(\dfrac{n^2-1}{2}\right)^2 \Rightarrow$ $n^2 = \left(\dfrac{n^2+1}{2}\right)^2 - \left(\dfrac{n^2-1}{2}\right)^2$, mostrando que todo $n \neq 1$ faz parte de alguma terna pitagórica. Caso $n = 1$, temos $1^2 = 1^2 + 0^2$.

4.1.2 Caracterização das ternas Pitagóricas (Fórmula geral)

Quando os elementos de um terno pitagórico são primos entre si, tomados dois a dois, dizemos que a terna é primitiva.

Umas das grandes contribuições dos matemáticos gregos foi a criação e demonstração de uma fórmula que nos dá todos os ternos pitagóricos primitivos. Antes de enunciarmos e demonstrarmos esse teorema, faremos algumas considerações interessantes para a prova do resultado.

Observação 4.1.1 *A partir de agora, usaremos a notação* (x, y, z) *para designar a igualdade* $x^2 + y^2 = z^2$ *ou* $y^2 + x^2 = z^2$*, isto é, a ordem* $(x, y, z) = (y, x, z)$.

Proposição 4.1.1 *Considere* (x, y, z) *uma terna Pitagórica qualquer, e seja d=* $mdc(x, y, z)$*. Tomando* $x' = \dfrac{x}{d}$*,* $y' = \dfrac{y}{d}$ *e* $z' = \dfrac{z}{d}$ *obteremos uma terna pitagórica primitiva, a saber* (x', y', z').

Prova: Como $d = mdc(x, y, z)$, temos que $mdc(x', y', z') = mdc\left(\dfrac{x}{d}, \dfrac{y}{d}, \dfrac{z}{d}\right) = \dfrac{1}{d} mdc(x, y, z) =$ 1, e portanto, primitiva. De fato, podemos dividir cada termo da equação $x^2 + y^2 = z^2$ por d^2, daí teremos $\left(\dfrac{x}{d}\right)^2 + \left(\dfrac{y}{d}\right)^2 = \left(\dfrac{z}{d}\right)^2 = x'^2 + y'^2 = z'^2$, uma terna primitiva.

Proposição 4.1.2 *Considere* (x, y, z) *uma terna Pitagórica qualquer primitiva. Teremos necessariamente nesse caso que x é par e y é ímpar, ou vice-versa, e z é ímpar.*

Prova: Sendo a terna (x, y, z) primitiva, não podemos ter x e y ambos pares pois $mdc(x, y) = 1$, e nem ambos ímpares, pois nesse caso, tomando $x = 2a+1$ e $y = 2b+1$, com a e b pertencente aos naturais, teríamos $z^2 = x^2 + y^2$ $z^2 = 4(a^2 + b^2 + a + b) + 2$, isto é, $z^2 = 4k + 2$, com k natural. Observe que $2|z^2$ e como 2 é primo então $2|z \Leftrightarrow 4|z^2$, o que é um absurdo!

Concluímos assim que se x é par então y é necessariamente ímpar.

Proposição 4.1.3 *Considere* (x, y, z) *uma terna Pitagórica qualquer primitiva. Então os termos* x, y *e* z *são primos entre si, tomados dois a dois, ou seja,* $mdc(x, y) = mdc(x, z) = mdc(y, z) = 1$.

Prova: Seja $d = mdc(x, y)$, então $d^2|x^2$ e $d^2|y^2$, isto é, $d^2|x^2 + y^2 = z^2$, portanto $d|z$, mas $mdc(x, y, z) = 1$ por se tratar de uma terna primitiva, logo $d = 1$. Analogamente mostramos que $mdc(x, z) = mdc(y, z) = 1$.

Proposição 4.1.4 *Considere os números naturais m, n e c, com* $mn = c^2$ *e* $mdc(m, n) = 1$. *Então deve existir números naturais M e N tais que* $m = M^2$ *e* $n = N^2$.

Prova: Considere as fatorações de m e n em números primos como $m = p_1^{a_1}.p_2^{a_2}...$ e $n = q_1^{b_1}.q_2^{b_2}....$ Como $mdc(m, n) = 1$, temos que os $p_i^{a_i}$ são distintos dos $q_j^{b_j}$. Assim, $mn = p_1^{a_1}.p_2^{a_2}...q_1^{b_1}q_2^{b_2}....$ Como $mn = c^2$, todos os expoentes dos p_i e dos q_j são pares. Assim, $m = M^2$ e $n = N^2$, com $M = p_1^{\frac{a_1}{2}}p_2^{\frac{a_2}{2}}...$ e $N = q_1^{\frac{b_1}{2}}q_1^{\frac{b_2}{2}}...$).

Teorema 4.1.5 *Todas as ternas pitagóricas primitivas* (x, y, z) *podem ser obtidas através da forma* $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, *onde m e n são naturais tais que* $mdc(m, n) = 1$, $m > n$ *e* $m + n$ *é ímpar, isto é, m e n tem paridades distintas.*

Prova: Suponha x, y e z diferentes de zero. Como a terna pitagórica é primitiva, temos pela proposição 4.1.3 que os termos x, y e z são primos entre si, e pela proposição 4.1.2 podemos tomar x par e y ímpar, logo $y^2 = z^2 - x^2 = (z-x)(z+x)$ é ímpar. Observe que $mdc(z-x, z+x) = 1$, pois se $d|z - x$ e $d|z + x$ teremos que $d|z - x + z + x = 2z$ e $d| - z + x + z + x = 2x \Rightarrow d|2z$ e $d|2x \Rightarrow d|mdc(2z, 2x) = 2mdc(x, z) = 2$, mas x e z são ímpares logo $d = 1$. Concluímos assim que $z - x$ e $z + x$ não possuem fatores primos em comum, e como $(z - x)(z + x)$ é um quadrado, pela proposição 4.1.4 cada um é um quadrado, isto é, existe a e b naturais tais que $mdc(a, b) = 1$, ímpares onde $z + x = a^2$ e $z - x = b^2$, assim $2z = a^2 + b^2$, $2x = a^2 - b^2$ e $y^2 = a^2b^2$. Logo a terna (x, y, z) é da forma $\left(\frac{a^2 - b^2}{2}, ab, \frac{a^2 + b^2}{2}\right)$.

Podemos reorganizar a solução do seguinte modo:

Seja $a+b = 2m$ e $a-b = 2n$, nesse caso teremos $a^2-b^2 = 4mn, 2a^2+2b^2 = 4m^2+4n^2$, $ab = m^2-n^2$, isto é, $\frac{a^2 - b^2}{2} = 2mn$, $\frac{a^2 + b^2}{2} = m^2+n^2$ e $ab = m^2-n^2 \Rightarrow (2mn, m^2-n^2, m^2+n^2)$, com $(m, n) = 1$ e m , n de paridades distintas.

Afirmação: *Todo natural par maior que dois faz parte de alguma terna pitagórica.*

Se n é par, pelo teorema anterior tome $n = 2ab$, $p = a^2 + b^2$ e $q = a^2 - b^2$. Tomando $b = 1$ teremos $(2a)^2 = (a^2 - 1)^2 = (a^2 + 1)^2$.

Observação 4.1.2 *Como consequência desse teorema podemos notar que dada uma terna pitagórica primitiva, x é sempre um número ímpar maior que 1 e y é sempre múltiplo de 4.*

4.1.3 Obtenção de infinitas ternas primitivas

O teorema 4.1.5 nos fornece a fórmula para a obtenção de infinitas ternas primitivas. Abaixo segue uma tabela que nos mostra como obtê-las.

m	n	$x = m^2 - n^2$	$y = 2mn$	$z = m^2 + n^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61
7	2	45	28	53
7	4	33	56	65
7	6	13	84	85
.	.	.	.	.
.	.	.	.	.

4.2 O Método das secantes e tangentes de Fermat para cônicas irredutíveis.

Denominamos cônicas toda curva algébrica plana cuja equação é um polinômio de grau dois.

Cônicas irredutíveis são aquelas cujo polinômio que as determinam não pode ser fatorado em polinômios de grau menores. As únicas cônicas irredutíveis são as elipses, parábolas e hipérboles. Faremos uma analise do conjunto solução em $\mathbb{Q}$ das cônicas irredutíveis utilizando o método das tangentes e secantes de Fermat para cônicas.

4.2.1 O método

Segundo GONDIM[2], o método das tangentes e secantes de Fermat para cônicas afirma o seguinte:

Dada uma cônica C e um ponto $A \in C$, tome uma reta l, onde A não pertence a l. Seja l' paralela a l, onde $A \in l'$ e $C \cap l' = \{A, B\}$ onde A pode ser igual a B. Traçando por A uma reta tangente a C, defina A' como a intercessão entre a reta tangente e l. Obtemos uma função $\gamma : C - \{A, B\} \longrightarrow l - \{A'\}$, onde todo ponto P em $C - \{A, B\}$ possui um correspondente $P' = \overrightarrow{AP} \cap l$.

[2]GONDIM, R. Aritmética em Retas e Cônicas. Disponível em: http : //www.sbm.org.br/2013 − 04 − 29 − 17 − 34 − 54/publicacoes − dos − coloquios. Acessado em 12/02/2014.

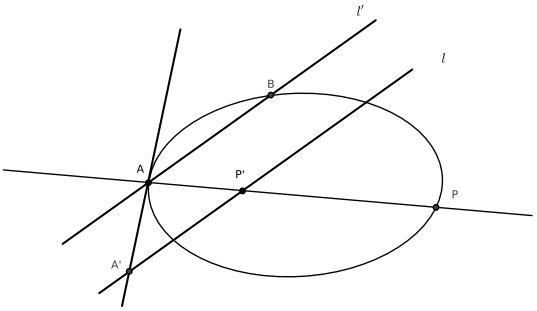

Figura 1

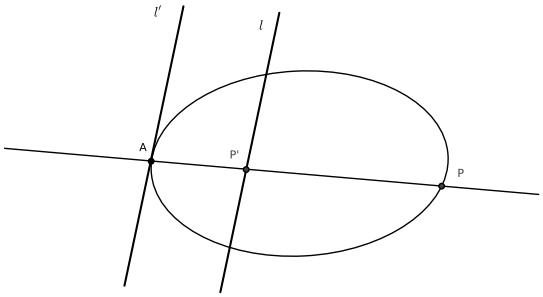

Figura 2

Observando a figura 1, veja que essa função possui uma inversa $\gamma^{-1} : l - \{A'\} \longrightarrow C - \{A, B\}$. O $C - \{A, B\}$ deve-se ao fato de que $\overrightarrow{AB}$ é um segmento de l', que é paralelo a l. Assim, todo ponto $P' \in l$ possui um único correspondente na curva C obtido quando traçamos a reta $\overrightarrow{P'A}$. Analisando a segunda situação que corresponde à figura 2, temos a inversa $\gamma^{-1} : l \longrightarrow C - \{A\}$, onde todo ponto em l continua possuindo um único correspondente $P = \overrightarrow{P'A} \cap l$. Portanto, γ é bijetiva.

Teorema 4.2.1 *Seja* C *uma cônica irredutível com coeficientes racionais e* $P \in C$ *um ponto racional. Se* l *é uma reta paralela e não coincidente com a tangente de* C *em* P *e possui pelo menos um ponto racional, então a função T:* $C - \{P\} \to l$*, definida por* $T(A) = \overrightarrow{PA} \cap l$ *determina uma bijeção entre os pontos racionais de* $C \setminus \{P\}$ *e os pontos racionais de* l.

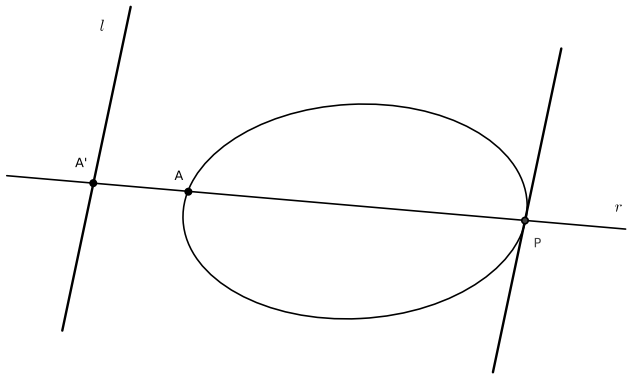

Figura 3

Prova: Se $A \in C - \{P\}$ é um ponto racional, temos que a equação de reta $\overrightarrow{PA}$ possui coeficientes racionais. Por outro lado, como l é paralela a $T_P C$ temos que o coeficiente angular de l coincide com o coeficiente angular de $T_P C$, o qual é racional pois P é racional e o referido coeficiente é dado por $\frac{dy}{dx}(P)$ obtido por derivação implícita a partir da equação da cônica. Portanto a equação de l também tem coeficientes racionais, haja vista que o coeficiente angular é racional e l passa por P, que é racional. Assim, o ponto $T(A)$ é a solução de um sistema linear com coeficientes racionais. Logo a regra de Cramer garante que $T(A)$ é racional.

Agora, observamos que a inversa de T é dada por $T^{-1}(A') = \overrightarrow{PA'} \cap (C - \{P\})$. Portanto, $T^{-1}(A')$ é obtido resolvendo-se o sistema linear de duas variáveis, sendo uma equação linear, de $\overrightarrow{PA'}$, e outra quadrática, de C. Dessa forma, tomando $A' \in l$, um ponto racional, teremos que a equação de $\overrightarrow{PA'}$ se escreve na forma $y = mx + n$, com m, n racionais. Substituindo y na equação de C teremos uma equação do segundo grau na incógnita x, da forma $ax^2 + bx + c = 0$, com a, b, c racionais, pois os coeficientes de C o são. Como P é racional, uma das raízes (abscissa de P) da equação $ax^2 + bx + c = 0$ é racional, mas então a outra também será (abscissa de A'), visto que a soma de um racional com outro número resultará em um racional, $\frac{c}{a}$, somente se esse outro número também pertence a $\mathbb{Q}$. Isso garante que $T^{-1}(A')$ é um ponto racional de $C \setminus \{P\}$.

Proposição 4.2.2 *Sejam C uma cônica irredutível com coeficientes racionais, $P \in C$ um ponto racional, L_p o conjunto das retas que passam por P e têm coeficiente angular racional e l_p a única reta vertical que passa por P. Temos um bijeção entre o conjunto dos pontos racionais de C e o conjunto $L_p \cup \{l_p\}$.*

Prova: A bijeção é obtida, definindo $\alpha : C \to \{$ retas passando por $P\}$ por

$$\alpha(Q) = \begin{cases} \overrightarrow{PQ}, \text{ se } P \neq Q \\ T_P C, \text{ se } P = Q \end{cases}$$

É claro que se Q for um ponto racional então a equação da reta $\overrightarrow{PQ}$ terá coeficiente angular racional, exceto, se for uma reta vertical, no qual caso teremos $\alpha(Q) = l_p$. Observamos que essa ultima igualdade ocorre para exatamente um ponto $Q \in C$. De fato, se $P = (x_0, y_0)$ então substituindo x por x_0 na equação da cônica ficaremos com uma equação do segundo grau em y, com coeficientes racionais, da qual y_0 é uma solução. Portanto, a outra solução, digamos y_1, também será racional. Logo, temos um ponto racional $Q = (x_0, y_1)$ tal que $\alpha(Q) = l_P$. Além disso, como $T_p C = \alpha(P)$ e $T_P C \in L_P \cup \{l_P\}$ (vide demonstração do teorema anterior), concluímos que α leva os pontos racionais de C em $L_p \cup \{l_P\}$. Por outro lado, se uma reta com coeficiente angular racional tem um ponto racional segue que o coeficiente linear também racional. Assim, cada elemento $l \in L_p$ é tal que sua equação tem coeficientes racionais. Daí, pelo mesmo argumento usado na prova do teorema acima, segue que $Q_l := l \cap (C \setminus \{P\})$ é um ponto racional de C. Explicitamente, o que se tem é que os coeficientes da equação de l são racionais e P é um ponto racional na interseção $l \cap C$, o referido argumento garante que o outro ponto de interseção, Q_l, também será racional. Dessa forma, para todo $l \in L_P$, com $l \neq T_P C$, temos $l = \alpha(Q_l)$. Logo, os pontos racionais de C são levados sobrejetivamente em $L_P \cup \{l_P\}$. Portanto, a injetividade de α garante a bijeção desejada.

4.2.2 Determinação dos pontos racionais de uma cônica irredutível com coeficientes racionais

Podemos parametrizar a partir de um ponto racional sobre uma cônica com coeficientes racionais o conjunto solução dessa cônica em Q.

Teorema 4.2.3 *Dada uma cônica em* $\mathbb{R}^2$ *com equação* $C : ax^2 + by^2 = c$*, onde* a*,* b *e* c *pertencem aos racionais, e dado um ponto racional* (x_0, y_0)*, então todos os outros pontos são do tipo:*

$$\left(\frac{bm^2x_0 - 2bmy_0 - ax_0}{bm^2 + a}, \frac{-bm^2y_0 - 2amx_0 + ay_0}{bm^2 + a}\right)$$

sendo $bm^2 + a \neq 0$, $m \in \mathbb{Q}$ e $(x_0, -y_0)$ o único ponto que não obtemos a partir da fórmula para solução geral descrita acima.

Prova: Tome todas as retas que passam por (x_0, y_0), assim a equação de uma reta qualquer dessas é $l : y - y_0 = m(x - x_0)$, veja que ela varia de acordo com o parâmetro racional m que é o coeficiente angular da reta.

Afirmamos que, sendo os coeficientes de l racionais, ela será secante a cônica em outro ponto também racional, devido ao fato de que a solução do sistema gerado pela equação da cônica e da reta, ambas com coeficientes racionais, gera soluções racionais. Esse resultado é devido ao método desenvolvido por Fermat e foi demonstrado no teorema anterior. Resta-nos obter a solução geral substituindo a equação da reta l na equação da cônica C. Tomemos então $C : ax^2 + by^2 = c$, e $l : y - y_0 = m(x - x_0)$, assim notamos que ao substituir $y = y_0 + m(x - x_0)$ em C teremos:

$$ax^2 + b(y_0 + m(x - x_0))^2 = c$$

$$\Rightarrow ax^2 + b(y_0^2 + 2y_0m(x - x_0) + m^2x^2 - 2m^2xx_0 + m^2x_0^2) = c$$

$$\Rightarrow ax^2 + by_0^2 + 2by_0mx - 2by_0mx_0 + bm^2x^2 - 2bm^2xx_0 + bm^2x_0^2 - c = 0$$

$$\Rightarrow (a + bm^2)x^2 + (2by_0m - 2bm^2x_0)x + (by_0^2 - 2by_0mx_0 + bm^2x_0^2 - c) = 0.$$

Veja que $by_0^2 - c = -ax_0^2$, logo temos:

$(a + bm^2)x^2 + (2by_0m - 2bm^2x_0)x + x_0(bm^2x_0 - 2by_0m - ax_0) = 0$. Obtemos portanto uma equação do segundo grau na variável x, e das relações de Girard[3] concluímos que se x_0 e x' são as raízes, então:

$$x_0x' = x_0\left(\frac{bm^2x_0 - 2by_0m - ax_0}{a + bm^2}\right).$$

[3]Albert Girard: Matemático francês, nascido em 1595, seus trabalhos contribuíram para o desenvolvimento da álgebra, aritmética e trigonometria.

Logo, $x' = \left(\frac{bm^2x_0 - 2by_0m - ax_0}{a + bm^2}\right)$, cuja coordenada y' é da forma

$$y' = y_0 + m\left(\frac{bm^2x_0 - 2by_0m - ax_0}{a + bm^2} - x_0\right)$$

$$\Rightarrow y' = y_0 + m\left(\frac{bm^2x_0 - 2by_0m - ax_0 - ax_0 - bm^2x_0}{a + bm^2}\right)$$

$$\Rightarrow y' = \left(\frac{-bm^2y_0 - 2amx_0 + ay_0}{a + bm^2}\right).$$

A solução geral é então da forma:

$$\left(\frac{bm^2x_0 - 2bmy_0 - ax_0}{bm^2 + a}, \frac{-bm^2y_0 - 2amx_0 + ay_0}{bm^2 + a}\right).$$

Por fim, observe que se $(x_0, y_0) \in C$ então $(x_0, -y_0)$ também pertencerá, porém, $-y_0 = y_0 + m(x_0 - x_0) \Leftrightarrow -2y_0 = m.0 \Leftrightarrow y_0 = 0$, isto é, para que solução geral determine o ponto $(x_0, -y_0)$ deveríamos ter $(x_0, 0)$.

Exemplo 6 *: Considere a hipérbole de equação* $H : x^2 - 3y^2 = 4$, *determine todos os pontos racionais de* H.

Solução: Tome $B(2, 0) \in H$, assim:

$a = 1$, $b = -3$, $c = 4$, $x_0 = 2$ e $y_0 = 0$.

Logo temos $\left(\frac{-3m^2.2 - 2.(-3).m.0 - 1.2}{-3m^2 + 1}, \frac{-(-3).m^2.0 - 2.1.m.2 + 1.0}{-3.m^2 + 1}\right) \Rightarrow$

$$\left(\frac{-6m^2 - 2}{-3m^2 + 1}, \frac{-4m}{-3m^2 + 1}\right),$$

com $m \in \mathbb{Q}$.

Tomando $m = -\frac{1}{2}$ por exemplo obtemos o ponto racional $A(-14, 8)$.

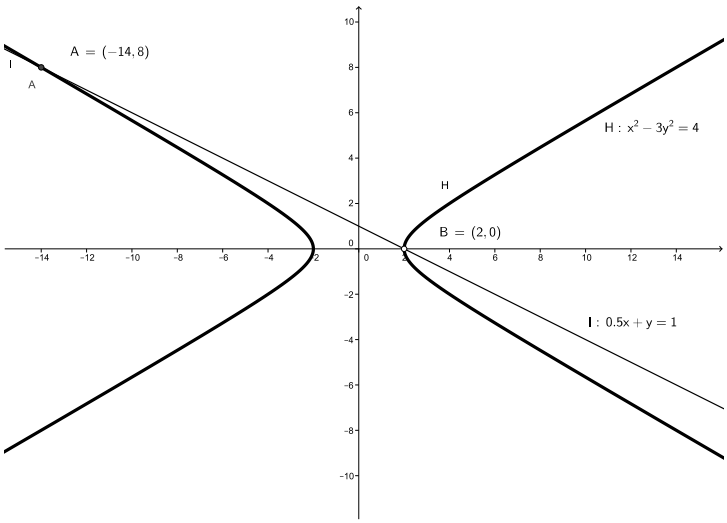

Figura 4

Veja que como tomamos $y_0 = 0$ então há de fato todos os pontos racionais.

Exemplo 7 *: Considere a elipse de equação* $E : x^2 + 3y^2 = 4$*, determine todos os pontos racionais de* E.

Solução: Tome novamente $B(2,0) \in E$, assim:

$a = 1$, $b = 3$, $c = 4$, $x_0 = 2$ e $y_0 = 0$.

Logo temos $\left(\frac{3m^2.2 - 2.3.m.0 - 1.2}{3m^2+1}, \frac{-3.m^2.0 - 2.1.m.2 + 1.0}{3.m^2+1}\right) \Rightarrow$

$$\left(\frac{6m^2-2}{3m^2+1}, \frac{-4m}{3m^2+1}\right),$$

com $m \in \mathbb{Q}$.

Tomando $m = -\frac{1}{2}$ por exemplo obtemos o ponto racional $A\left(-\frac{2}{7}, \frac{8}{7}\right)$ que em decimais é aproximadamente $A(-0.29, 1.14)$.

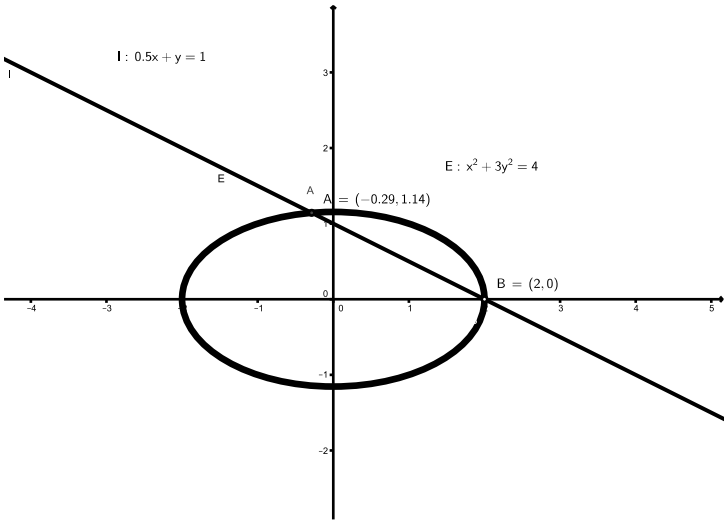

Figura 5

Como $y_0 = 0$ temos todos os pontos racionais.

4.2.3 Caso particular: o círculo unitário centrado na origem

Consideremos agora a equação diofantina $a^2 + b^2 = c^2$, onde a, b, e c são inteiros não simultaneamente nulos. Dividindo ambos os lados por c^2 obteremos $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$, onde $\left(\frac{a}{c}\right)$ e $\left(\frac{b}{c}\right) \in \mathbb{Q}$. Note que $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ é a equação de um círculo cujo raio é 1. Faça $\frac{a}{c} = x$ e $\frac{b}{c} = y$, nesse caso nosso interesse é achar todas as soluções racionais da equação $x^2 + y^2 = 1$, isto é, todos os pontos racionais pertencentes ao círculo unitário:

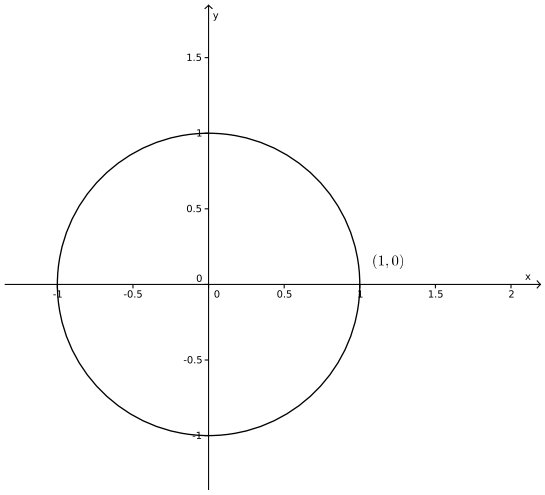

Figura 6

Inicialmente notemos que (1,0) é solução, pois $1^2+0^2 = 1$. Podemos traçar por $(1,0)$ uma reta que intercepta o círculo em outro ponto. Veremos que também este outro ponto é um par de números racionais. A reta gerada por estas duas coordenadas racionais é denominada reta racional.

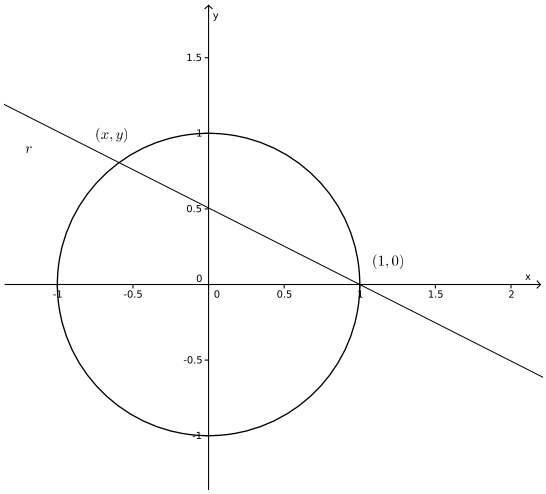

Figura 7

Seja r a reta que passa por $(1,0)$ e intercepta o círculo no ponto (u,w), logo r é da forma $r : y = m(x-1)$, onde m é a tangente do ângulo de inclinação da reta com o eixo OX. Tomaremos m como uma de declividade racional.

Se o ponto (u,v) pertence a reta e ao círculo, então: $\begin{cases} w = m(u-1) \\ u^2+w^2 = 1 \end{cases}$. Assim, $u^2+(m(u-1))^2 = 1 \Rightarrow u^2+m^2u^2-2m^2u+m^2 = 1 \Rightarrow u^2(1+m^2)-u(2m^2)+(m^2-1) = 0$. Resolvendo essa equação do segundo grau em u teremos:

$$u = \frac{2m^2 \pm \sqrt{(2m)^2-4(1+m^2)(m^2-1)}}{2(1+m^2)}$$

$$u = \frac{2m^2 \pm \sqrt{4m^4 - 4m^2 + 4 - 4m^4 + 4m^2}}{2(1+m^2)}$$

$$u = \frac{2m^2 \pm 2}{2(1+m^2)}$$

$$u = \frac{m^2 \pm 1}{1+m^2}$$

Portanto, $w = m\left(\frac{m^2 \pm 1}{1+m^2} - 1\right)$. Note que se tomarmos $u = \left(\frac{m^2+1}{1+m^2}\right)$, teremos $w = 0$ e $u = 1$, por isso consideraremos $u = \left(\frac{m^2-1}{1+m^2}\right)$, donde $w = m\left(\frac{m^2-1-1-m^2}{1+m^2}\right)$. O conjunto solução é, portanto:

$$u = \left(\frac{m^2-1}{1+m^2}\right)$$
$$w = m\left(\frac{-2}{1+m^2}\right).$$

Por $w = m(u-1)$ vemos que m é racional, logo tomemos $m = \frac{t}{k}$, com $mdc(t,k) = 1$ então:

$$P_{(\frac{t}{k})} = \left(\frac{\frac{t^2}{k^2} - 1}{1 + \frac{t^2}{k^2}}, \frac{\frac{-2t}{k}}{1 + \frac{t^2}{k^2}}\right) \Rightarrow \left(\frac{t^2-k^2}{k^2+t^2}, \frac{-2tk}{k^2+t^2}\right).$$

Tomando $a = t^2 - k^2$, $b = -2tk$ e $c = k^2 + t^2$, teremos a solução em $\mathbb{Z}$ de $a^2 + b^2 = c^2$.

Essa ideia de utilizar um coeficiente angular racional para uma reta e um ponto com coordenadas racionais conhecidas, contido no círculo e na reta, como sugere a proposição 4.2.2, faz com que consigamos obter todos os pontos racionais do círculo, e em particular as soluções da terna pitagórica dada inicialmente.

Observação 4.2.1 *: Sendo m um valor racional e (u,v) um ponto do círculo, concluímos ainda que há uma bijeção entre m (conjunto dos racionais) e (u,v), conjunto de pontos do círculo unitário centrado na origem, com exceção do ponto $(1,0)$.*

4.3 Das ternas pitagóricas ao último teorema de Fermat

A obra "Arithmetica" de Diofanto inspirou as gerações seguintes de matemáticos, incluindo Pierre de Fermat que exercia a profissão de magistrado. Segundo algumas fontes confiáveis, Pierre de Fermat nasceu em Beaumont de Lomagne, próximo a Toulouse, mas seu ano de nascimento é incerto, foi entre os anos de 1590 e 1608. Filho de comerciante, seus estudos começaram em casa e a matemática virou o seu hobby. Ao adquirir uma copia da obra prima de Diofanto, uma tradução em latim realizada em 1621 por Claude Gaspar Bachet de Méziriac, essa tradução tornou-se o centro de sua atenção, era com ela que Fermat se divertia nas horas vagas. A arithmetica coligia um conhecimento matemático adquirido por grandes

gênios da matemática com Euclides, autor da obra "Os elementos" e Pitágoras, conhecimento gerado nos últimos mil anos que antecederam Diofanto (SINGH[4], 2001).

Fermat não costumava publicar seus trabalhos, mas seu extraordinário talento com os números contribuiu profundamente para a criação da moderna teoria dos números. Muitas de suas anotações eram feitas nas margens de sua cópia do livro Arihtmetica, vários teoremas demonstrados posteriormente por outros matemáticos foram confirmados como verdadeiros, porém um perdurou por séculos desafiando gerações de matemáticos brilhantes como Euler, Legende e Dirichlet. O livro II da Arithmetica de Diofanto aborda o Teorema de Pitágoras e os ternos pitagóricos, e foi durante uma de suas leituras, ao lado do problema 8 que Fermat fez a seguinte afirmação:

> *"Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet"(SINGH[4], 2001, P.80).*

> *"É impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como uma soma de dois números elevados a quatro, ou, em geral, para qualquer número que seja elevado a uma potência maior do que dois ser escrito como a soma de duas potências semelhantes. Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para contê-la"(SINGH[4], 2001, P.80).*

A conjectura de Fermat, que ficou conhecida como o último teorema de Fermat, confirmada por Andrew Wilis apenas em 1994, é um problema muito difícil de resolver, mas seu enunciado é bem simples, acessível a qualquer estudante, e ganhou certa notoriedade no mundo inteiro por ser o teorema com o maior números de demonstrações incorretas publicadas. Muitos acreditam que Fermat não possuía uma demonstração como afirmava, o que é certo é que a matemática utilizada na demonstração de Wilis é muito avançada, nem de longe poderia ser a que Fermat supostamente possuía (SINGH[4], 2001).

4.3.1 Caso particular do último teorema de Fermat

Em 1637 Fermat lançou o desafio que causaria frustação em muitas mentes brilhantes ao escrever seu mais famoso teorema:

A equação $x^n + y^n = z^n$, não possui soluções inteiras, exceto a trivial, para $n > 2$.

[4]SINGH, Simon. O Último teorema de Fermat: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos. 10. ed. Rio de Janeiro: Record, 2001.

Logicamente, ao escrever essa afirmação, Fermat não estava levando em consideração o caso em que somente uma da variáveis, x ou y, é zero, visto que assim bastaria tomar o z igual ao termo não nulo, por exemplo $2^5 + 0^5 = z^5 \Rightarrow z = 2$.

Teorema 4.3.1 *(Fermat)A equação* $x^n + y^n = z^n$ *não tem solução para os inteiros* x, y *e* z *quando* $n = 4k$ *, com* $k \in \mathbb{N}$.

Prova: Veja inicialmente que $x^4 + y^4 = a^4 \Rightarrow x^4 + y^4 = (a^2)^2$. Assim, faça $(a^2)^2 = z^2$ e considere a equação $x^4 + y^4 = z^2$, seja $d = mdc(x, y)$, teremos então $x = di$, $y = dj$ e $mdc(i, j) = 1$. Logo, $x^4 + y^4 = z^2 = d^4(i^4 + j^4) \Rightarrow d^4 | z^2 \Rightarrow d^2 | z$. Tome $z = d^2 f$, então $x^4 + y^4 = z^2 \Rightarrow d^4 i^4 + d^4 j^4 = d^4 f^2 \Rightarrow i^4 + j^4 = f^2$. Podemos supor então que $mdc(x, y) = 1$, pois caso não seja conseguimos reduzi-la à uma equação do mesmo tipo com $mdc(i, j) = 1$.

Tome $(x^2)^2 + (y^2)^2 = z^2$, pelo teorema 4.1.5 existem m e p inteiros tais que $(m, p) = 1$, onde $x^2 = m^2 - p^2$, $y^2 = 2mp$, $z = m^2 + p^2$, e m e p tem paridades distintas. Então $x^2 + p^2 = m^2 \Rightarrow x^2$ é ímpar. Seja p par, então existem u e v inteiros tais que $(u, v) = 1$, onde $x = u^2 - v^2$, $p = 2uv$, $m = u^2 + v^2$, e u e v tem paridades distintas. Veja que $y^2 = 2mp = 4m\frac{p}{2}$, $\left(\frac{y}{2}\right)^2 = m\frac{p}{2}$, $mdc(m, p) = 1 \Rightarrow mdc\left(m, \frac{p}{2}\right) = 1 \Rightarrow$ existe r e s naturais tais que $m = r^2$ e $\frac{p}{2} = s^2 \Rightarrow \frac{p}{2} = uv = s^2$, $mdc(u, v) = 1$. Existe então t e w naturais com $u = t^2$ e $v = w^2$. Como $m = u^2 + v^2$, então $r^2 = u^2 + w^2 = t^4 + w^4$. Observe que $r \leqslant r^2 = m < 2mp = y^2 < z$, pois $y^4 < x^4 + y^4 = z^2$. Assim, $r < z$ e (t, w, r) é uma solução menor que (x, y, z). Esse raciocínio nos mostra que se a equação $x^n + y^n = z^n$ possuir uma solução (x, y, z) nos naturais, podemos tomar o z como o menor possível, e mesmo assim encontraremos outra solução (t, w, r) onde $r < z$, o que é um absurdo. Na verdade podemos aplicar esse procedimento infinitas vezes, obtendo resultados cada vez menores, mas sem fim. Esse método criado por Fermat é chamado de "descida infinita de Fermat".

Para concluirmos que não há solução quando $n = 4k$ basta observarmos que a equação $x^{4k} + y^{4k} = z^{4k}$ equivale a $(x^k)^4 + (y^k)^4 = (z^k)^4$, isto é, $\overline{x}^4 + \overline{y}^4 = \overline{z}^4$ (MIRANDA[5], 2007).

Finalizamos assim o estudo introdutório sobre alguns tipos de equações diofantinas. O capítulo seguinte trará aplicações das equações diofantinas lineares em problemas que poderão ser abordados na educação básica, sendo necessário um conhecimento prévio sobre as quatro operações básicas, mdc e habilidade de interpretar e escrever matematicamente situações problemas matemáticos.

[5]Para mais detalhes, veja: M.C. de Miranda,*"Heurística e Equações Diofantinas"*, FAMAT em revista, nº9, 2007. Disponível em: http : //www.portal.famat.ufu.br/node/262. Acessado em 21/01/2014.

5 APLICAÇÕES DAS EQUAÇÕES DIOFANTINAS NO ENSINO BÁSICO

Faz parte das atribuições do docente a criação de situações para que os discentes sintam-se motivados e tenham um papel ativo durante as aulas, facilitando assim o processo de ensino aprendizagem. A abordagem de problemas sobre equações diofantinas lineares nas aulas de matemática é uma boa maneira de incentivar os alunos a pensarem e desenvolverem competências e habilidades como raciocínio lógico, identificação de informações relevantes para a resolução de uma situação problema proposta, atenção e concentração.

Neste capítulo daremos alguns exemplos de problemas que podem ser facilmente solucionados quando aplicamos os conhecimentos sobre resolução de equações diofantinas lineares.

Problema 1 *: Determinar todas as soluções inteiras da seguinte equação diofantina linear:* $3x + 4y = 5$.

Solução: Como o $\mathrm{mdc}(3,4) = 1$ e $1 \mid 5$ a equação possui solução no conjunto dos $\mathbb{Z}$.

	1	3
4	3	1
1	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$4 = 3.1 + 1$

$3 = 1.3 + 0$

Escrevendo o $\mathrm{mdc}(3,4) = 1$ como combinação linear de 3 e 4, obteremos:

$1 = -3.1 + 4$

Como queremos resolver a equação $3x + 4y = 5$, vamos multiplicar ambos os lados por 5. Assim, $5 = 3(-5) + 4.5$, logo $x_0 = -5$ e $y_0 = 5$ é uma solução particular da equação.

A solução geral é da forma:

$$x = -5 + \frac{4}{1}k \text{ e } y = 5 - \frac{3}{1}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = -5 + 14k$ e $y = 5 - 3k$, com $k \in \mathbb{Z}$.

Problema 2 *: Determinar todas as soluções inteiras da seguinte equação diofantina linear:* $9x - 15y = 9$.

Solução: Como o $\mathrm{mdc}(9,15) = 3$ e como $3 \mid 9$, nossa equação possui solução!

	1	1	2
15	9	6	3
6	3	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$15 = 9.1 + 6$

$9 = 6.1 + 3$

$6 = 3.2 + 0.$

Podemos escrever o $\mathrm{mdc}(9, 15) = 3$ como combinação linear de 9 e 15, temos nesse caso que:

$3 = 9 - 6.1$

$3 = 9 - (15 - 9.1).1$

$3 = 9 - 15 + 9.1$

$3 = 9.2 - 15.1.$

Como queremos resolver a equação $9x - 15y = 9$, vamos multiplicar ambos os lados por 3. Assim, $9 = 9.6 - 15.3$, logo $x_0 = 6$ e $y_0 = 3$ é uma solução particular da equação. A solução geral é da forma:

$$x = 6 + \frac{(-15)}{3}k \text{ e } y = 3 - \frac{9}{3}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = 6 - 5k$ e $y = 3 - 3k$, com $k \in \mathbb{Z}$.

Problema 3 *: Determinar o menor inteiro positivo que ao ser dividido por 3 deixa resto 2 e quando dividido por 7 deixa resto 1.*

Solução: Seja n esse menor inteiro positivo. Então como n dividido por 3 deixa resto 2 temos que $n = 3y + 2$ com $y \in \mathbb{N}$, e como n dividido por 7 deixa resto 1 temos que $n = 7x + 1$ com $x \in \mathbb{N}$. Assim, $3y + 2 = 7x + 1 \Rightarrow 7x - 3y = 1$. Como o $\mathrm{mdc}(7, 3) = 1$ e como $1 \mid 1$, nossa equação possui solução!

	2	3
7	3	1
1	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$7 = 3.2 + 1$

$3 = 1.3 + 0$

Escrevendo o $\mathrm{mdc}(7, 3) = 1$ como combinação linear de 7 e 3, temos nesse caso que:

$1 = 7 - 3.2$

Logo, $x_0 = 1$ e $y_0 = 2$ é uma solução particular da equação.

A solução geral é da forma:

$$x = 1 + \frac{(-3)}{1}k \text{ e } y = 2 - \frac{7}{1}k \text{ , com } k \in \mathbb{Z}.$$

Isto é, $x = 1 - 3k$ e $y = 2 - 7k$, com $k \in \mathbb{Z}$.

Observando que se:

$k < 0 \Rightarrow x > 1$ e $y > 2$

$k = 0 \Rightarrow x = 1$ e $y = 2$

$k > 0 \Rightarrow x < 0$ e $y < 0$, onde n será negativo.

Concluímos que k deve ser zero, logo teremos $n = 3y + 2 \Rightarrow n = 8$. Portanto 8 é o menor inteiro positivo que dividido por 3 deixa resto 2 e dividido por 7 deixa resto 1.

Problema 4 *: Encontre as duas menores frações positivas, cujos denominadores são 5 e 9 de forma que sua soma seja igual a* $\frac{37}{45}$.

Solução: Seja $\frac{x}{5}$ e $\frac{y}{9}$ as duas menores frações positivas tais que $\frac{x}{5} + \frac{y}{9} = \frac{37}{45}$, então $\frac{9x+5y}{45} = \frac{37}{45}$. Devemos portanto procurar as soluções da equação linear diofantina $9x + 5y = 37$.

Como o $mdc(9,5) = 1$ e como $1 \mid 37$, nossa equação possui solução!

	1	1	4
9	5	4	1
4	1	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$9 = 5.1 + 4$

$5 = 4.1 + 1$

$4 = 1.4 + 0$

Escrevendo o $mdc(9,5) = 1$ como combinação linear de 9 e 5, temos nesse caso que:

$1 = -9.1 + 5.2$

Como queremos resolver a equação $9x + 5y = 37$, multiplicaremos ambos os lados por 37. Logo, $37 = 9.(-37) + 5.74$, e portanto $x_0 = -37$ e $y_0 = 74$ é uma solução particular da equação.

A solução geral é da forma:

$$x = -37 + \frac{5}{1}k \text{ e } y = 74 - \frac{9}{1}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = -37 + 5k$ e $y = 74 - 9k$, com $k \in \mathbb{Z}$.

Como x e y devem ser positivos, de $x = -37 + 5k$ temos $k > 7$ e de $y = 74 - 9k$ resulta $k < 9$.

Concluímos assim que $k = 8$ e portanto $x = 3$ e $y = 2$. Assim as frações procuradas são $\frac{3}{5}$ e $\frac{2}{9}$.

Problema 5 *: Escreva o número 91 como soma de dois inteiros positivos tais que o primeiro seja divisível por 6 e o segundo por 7.*

Solução: Devemos procurar x e y tais que $6x + 7y = 91$.

Como o $mdc(6,7) = 1$ e como $1 \mid 91$, nossa equação possui solução!

	1	6
7	6	1
1	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$7 = 6.1 + 1$ $6 = 1.6 + 0$

Escrevendo o $\mathrm{mdc}(7,6) = 1$ como combinação linear de 7 e 6, temos nesse caso que:

$1 = 7.1 - 6.1$

Como queremos resolver a equação $6x + 7y = 91$, multiplicaremos ambos os lados por 91. Logo, $91 = 6.(-91) + 7.91$, e portanto $x_0 = -91$ e $y_0 = 91$ é uma solução particular da equação.

A solução geral é da forma:

$$x = -91 + \frac{7}{1}k \text{ e } y = 91 - \frac{6}{1}k \text{ , com } k \in \mathbb{Z}.$$

Isto é, $x = -91 + 7k$ e $y = 91 - 6k$, com $k \in \mathbb{Z}$.
Como x e y devem ser positivos, de $x = -91 + 7k$ temos $k > 13$ e de $y = 91 - 6k$ resulta $k < 16$.

Concluímos assim que se $k = 14$ teremos $x = 7$ e $y = 7$. Caso tenhamos $k = 15$ então $x = 14$ e $y = 1$. Portanto temos os valores 42 e 49 ou 84 e 7 como soluções.

Problema 6 *: O valor de entrada em um parque de diversão é de RS* $8,00$ *para pessoas acima de 15 anos e RS* $6,00$ *para quem tem 15 anos ou menos. Quantas pessoas no mínimo deverão ir ao parque de maneira que a bilheteria arrecade pelo menos RS* $500,00$.

Solução: Devemos procurar x e y tais que $8x + 6y = 500$.

Como o $\mathrm{mdc}(8,6) = 2$ e como $2 \mid 500$, nossa equação possui solução no conjunto dos $\mathbb{Z}$!

	1	3
8	6	2
2	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$8 = 6.1 + 2$ $6 = 2.3 + 0$

Escrevendo o $\mathrm{mdc}(8,6) = 2$ como combinação linear de 8 e 6, temos nesse caso que:

$2 = 8.1 - 6.1$

Como queremos resolver a equação $8x + 6y = 500$, multiplicaremos ambos os lados por 250. Logo, $500 = 8.250 + 6.(-250)$, e portanto $x_0 = 250$ e $y_0 = -250$ é uma solução particular da equação.

A solução geral é da forma:

$$x = 250 + \frac{6}{2}k \text{ e } y = -250 - \frac{8}{2}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = 250 + 3k$ e $y = -250 - 4k$, com $k \in \mathbb{Z}$.

Como x e y devem ser positivos, e observando que para se ter o mínimo de pessoas de modo que a arrecadação seja pelo menos 500, o valor de x deverá ser o maior possível, pois quanto mais pessoas que pagam RS $8,00$ houver, menor será a quantidade de pessoas necessárias.

De $x = 250+3k \geqslant 0$ temos $k \geqslant -83,3$ e de $y = -250-4k \geqslant 0$ resulta $k \leqslant -62,5$, isto é, $-83,3 \leqslant k \leqslant -62,5$. O maior valor possível para x ocorre quando $k = -63$.
Concluímos assim que $x = 250 - 189 = 61$ e $y = -250 + 252 = 2$. Portanto serão necessário pelo menos 61 pessoas acima de 15 anos e 2 pessoas com 15 anos ou menos.

Problema 7 *: Uma blusa custa RS* $46,00$*, porém o cliente só possui notas de RS* $5,00$ *e o vendedor notas de RS* $2,00$*. Nessas condições, é possível efetuar a transação de modo que o comprador receba seu troco corretamente? se sim, quantas notas o comprador dará e quantas receberá como troco?*

Solução: Seja x a quantidade de notas de RS $5,00$ que o comprador dará e y a quantidade de notas de RS $2,00$ que ele receberá de troco do vendedor, então devemos procurar x e y positivos tais que $5x - 2y = 46$.

Como o $mdc(5,2) = 1$ e como $1 \mid 46$, nossa equação possui solução no conjunto dos $\mathbb{Z}$!

	2	2
5	2	1
1	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$5 = 2.2 + 1$

$2 = 1.2 + 0$

Escrevendo o $mdc(5,2) = 1$ como combinação linear de 5 e 2, temos nesse caso que:

$$1 = 5.1 - 2.2$$

Como queremos resolver a equação $5x - 2y = 46$, multiplicaremos ambos os lados por 46. Logo, $46 = 5.46 - 2.92$, e portanto $x_0 = 46$ e $y_0 = 92$ é uma solução particular da equação.
A solução geral é da forma:

$$x = 46 + \frac{(-2)}{1}k \text{ e } y = 92 - \frac{5}{1}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = 46 - 2k$ e $y = 92 - 5k$, com $k \in \mathbb{Z}$.
Como x e y devem ser positivos, de $x = 46 - 2k$ temos $23 > k$ e de $y = 92 - 5k$ resulta

$18,4 > k$.

Tomando k maior possível teremos a quantidade mínima de notas que o cliente deverá ter para efetuar o pagamento e receber o troco. Tomemos $k = 18$, então $x = 46 - 36 = 10$ e $y = 92 - 90 = 2$. Portanto a compra poderá ser efetuada se o comprador der 10 notas de RS $5,00$ e o vendedor voltar 2 notas de RS $2,00$.

Problema 8 *: Para agrupar 40 alunos em filas de 6 ou de 8, serão necessárias quantas filas no mínimo? E caso deva haver pelo menos uma fila de 6 e uma de 8, qual a solução*?

Solução: Seja x a quantidade de filas de 6 alunos e y a quantidade de filas de 8 alunos, então devemos procurar x e y não negativos tais que $6x + 8y = 40$.

Como o $mdc(6,8) = 2$ e como $2 \mid 40$, nossa equação possui solução no conjunto dos $\mathbb{Z}$!

	1	3
8	6	2
2	0	

Usando o algoritmo da divisão temos as seguintes igualdades:

$8 = 6.1 + 2$

$6 = 2.3 + 0$

Escrevendo o $mdc(6,8) = 2$ como combinação linear de 6 e 8, temos nesse caso que:

$2 = 8.1 - 6.1$

Como queremos resolver a equação $6x + 8y = 40$, multiplicaremos ambos os lados por 20. Logo, $40 = 6(-20) + 8.20$, e portanto $x_0 = -20$ e $y_0 = 20$ é uma solução particular da equação. A solução geral é da forma:

$$x = -20 + \frac{8}{2}k \text{ e } y = 20 - \frac{6}{2}k, \text{ com } k \in \mathbb{Z}.$$

Isto é, $x = -20 + 4k$ e $y = 20 - 3k$, com $k \in \mathbb{Z}$.

Como x e y devem ser não negativos, de $x = -20 + 4k \geqslant 0$ temos $k \geqslant 5$ e de $y = 20 - 3k$ resulta $\frac{20}{3} \geqslant k$. Assim, $5 \leqslant \frac{20}{3} \Rightarrow k = 5$ ou $k = 6$. Tomando k menor possível teremos y maior possível, e consequentemente a quantidade mínima de filas necessárias. Logo $k = 5 \Rightarrow x = 0$ e $y = 5$. Assim, deverão ser formadas 5 filas de 8 alunos.

No caso em que deve haver filas de 6 e de 8, obtemos solução usando $k = 6$, onde $x = 4$ e $y = 2$, sendo necessário portanto um total de 6 filas.

Problema 9 *: Determine o conjunto solução em $\mathbb{Z}$ da equação* $6x + 9y + 12z = 120$.

Solução: Calculemos inicialmente o $mdc(6,9)$ usando o algoritmo da divisão, da seguinte forma:

	1	2
9	6	3
3	0	

Logo, $9 = 6.1 + 3 \Rightarrow 3 = 6.(-1) + 9.1$. Assim, o $mdc(6,9) = 3$. Aplicando novamente o algoritmo da divisão para calcular o $mdc(3,12)$ temos:

	4
12	3
0	

Assim, $13 = 3.4 + 0$ e portanto o $mdc(3,12) = 3$. Escrevendo o mdc como combinação linear de 6, 9 e 12, temos $3 = 6.(-1) + 9.1 + 12.0$, multiplicando por 40 ambos os lados resulta em $120 = 6.(-40) + 9.40 + 12.0$. Portanto, $(40, -40, 0)$ é uma solução particular da equação dada.

Agora considere $k = 6x + 9y$, então $1.k + 12.z = 120$. Como o $mdc(1,12) = 1$ e $1 \mid 120$, a equação tem solução. Podemos escrever o $mdc(1,12)$ como combinação linear de 1 e 12, isto é, $1 = 1.(-11) + 12.(1)$, multiplicando ambos os lados por 120 temos:

$120 = 1.(-1320) + 12.(120)$. Sendo $(-1320, 120)$ uma solução particular, o teorema 3.3.1 nos diz que a solução geral é da forma:

$k = k_0 + \frac{12}{1}l$ e $z = z_0 - \frac{1}{1}l$, com $l \in \mathbb{Z}$, o que resulta em $k = -1320 + 12l$ e $z = 120 - l$.

Analisemos agora $k = 6x + 9y = -1320 + 12l$, observe que obrigatoriamente o $mdc(6,9) = 3$ deve dividir $-1320 + 12l$, como $3 \mid 1320$ e $3 \mid 12$, não precisaremos nos preocupar com o valor de l. Sabemos pelo exemplo anterior que $3 = 6.(-1) + 9.1$, donde multiplicando ambos os lados por $\frac{-1320 + 12l}{3}$ obtemos a seguinte expressão:

$$\left(\frac{-1320 + 12l}{3}\right).3 = 6.1.\frac{-1320 + 12l}{3} + 9.(1).\frac{-1320 + 12l}{3}.$$

Assim, $-1320 + 12l = 6(440 - 4l) + 9.(-440 + 4l)$. Concluímos novamente pelo teorema 3.3.1 que a solução geral dessa equação é:

$x = x_0 + \frac{9}{3}l'$ e $y = y_0 - \frac{6}{3}l'$, com $l' \in \mathbb{Z}$, isto é, $x = 440 - 4l + 3l'$ e $y = -440 + 4l - 2l'$.

Portanto, a solução geral é da forma:

$x = 440 - 4l + 3l'$;

$y = -440 + 4l - 2l'$;

$z = 120 - l$, com $l, l' \in \mathbb{Z}$.

6 CONCLUSÃO

Vimos ao longo deste trabalho que a matemática originou-se primeiramente de forma intuitiva, antecedendo a escrita que foi fundamental para o seu desenvolvimento e propagação. Conhecemos um pouco da história de alguns grandes matemáticos como Pitágoras, Fermat e Diofanto, que tanto contribuíram para o surgimento e desenvolvimento da teoria dos números.

O estudo aprofundado sobre equações diofantinas lineares nos forneceu condições necessárias e suficientes para que elas tenham solução no conjunto dos inteiros e nos mostra quão acessível e interessante pode ser sua abordagem na educação básica.

Analisamos um tipo especial de equação diofantina, conhecida no mundo inteiro como o Teorema de Pitágoras, salientando que só são consideradas equações diofantinas, aquelas cujos coeficientes e soluções pertencem ao conjunto dos inteiros. Pudemos verificar a existência de infinitas soluções para as terna pitagóricas através de observações feitas por Euclides há muitos séculos atrás, e formular expressões que resultam em seu conjunto solução, bem como as condições de existência. O método das tangentes e secantes criado por Fermat nos fornece não só as expressões, mas também uma visão analítica do comportamento do Teorema de Pitágoras quando a hipotenusa vale 1, o que nos permitiu também obter o conjunto solução de determinadas cônicas de um modo mais geral, com coeficientes e soluções nos racionais.

Fizemos um estudo sobre a observação feita por Fermat as margens de seu exemplar, uma tradução da obra "Arithmetica"escrita por Diofanto, observação essa que ficou famosa no mundo inteiro por seu enunciado bem simples mas solução extremamente complicada. Não sabemos se Fermat possuía um método engenhoso para resolvê-la, se possuía uma solução errada, ou se não possuía solução alguma, apesar de ter deixado pistas da demonstração de um caso particular de sua afirmação ao resolver um outro problema.

Por fim, encerramos este trabalho com algumas aplicações simples sobre as equações lineares diofantinas na esperança de ter despertado o interesse do leitor pelo assunto abordado e que este se sinta motivado a pesquisar sobre o tema, e caso seja professor, que possa incluir as belas equações diofantinas lineares no seu plano de aula, visto que elas podem contribuir significativamente, pois incita o discente a pensar, analisar hipóteses, e transcrever em linguagem matemática as informações contidas em situação problema.

REFERÊNCIAS

ALMEIDA, M. C. **Talhas Numéricas e o antigo testamento**. Revista Brasileira de História da Matemática. vol.2, n 4, 2002. Disponível em: <http://www.rbhm.org.br/vo2-no4.html>. Acessado em 10/03/2014.

BISPO, D. dos S. **Equações diofantinas lineares e suas aplicações**, 2013. Disponível em: <http://www.uesb.br/mat/download/Trabamonografia/2013/Dinguiston.pdf>. Acessado em 15/01/2014.

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

CAMPOS, G. D. M. **Equações diofantinas lineares**. Disponível em: <bit.profmat-sbm.org.br/xmlui/bitstream/handle/123456789/558/2011_00462_GISELI_DUARDO_ MACIANO _ CAMPOS.pdf>. Acessado em 15/01/2014.

DOMINGUES, Hygino Hugueros. **Fundamentos de aritmética**. São Paulo, SP: Atual, 1991.

EVES, Howard Whitley. **Introdução a história da matemática**. Campinas, SP: Ed. da UNICAMP, 1995.

GONDIM, R. **Aritmética em retas e cônicas**. Disponível em: <http://www.sbm.org.br/2013-04-29-17-34-54/publicacoes-dos-coloquios>. Acessado em 12/02/2014.

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

MAIER, Rudolf R. **Teoria dos números**. Versão atualizada, 2005. Disponível em: <https://www.mat.unb.br/ maierr/tnotas.pdf>. Acessado em 21/01/2014.

MIRANDA, M. C. **Heurística e equações Diofantinas**, FAMAT em revista, n9, 2007. Disponível em: <http://www.portal.famat.ufu.br/node/262>. Acessado em 21/01/2014.

MOL, Rogério Santos. **Introdução à história da matemática** - Belo Horizonte: CAED-UFMG, 2013. Disponível em: <www.mat.ufmg.br>. Acessado em 05/01/2014.

SANTOS, J. P. de O. **Introdução à teoria dos números**. 3. ed. Rio de Janeiro, RJ: IMPA, 2005.

SINGH, Simon. **O último teorema de Fermat**: a história do enigma que confundiu as maiores mentes do mundo durante 358 anos. 10. ed. Rio de Janeiro: Record, 2001.