UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

GEOVANE DE SOUZA FERREIRA JÚNIOR

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS E APLICAÇÕES

PATOS - PB
2017

GEOVANE DE SOUZA FERREIRA JÚNIOR

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS E APLICAÇÕES

Monografia submetida à Coordenação do Curso de Licenciatura Plena em Matemática, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Me. José Ginaldo de Souza Farias.

Coorientador: Prof. Me. Arlandson Matheus Silva Oliveira.

PATOS - PB
2017

F383i Ferreira Junior, Geovane de Souza.
Introdução as Equações Diofantinas e aplicações [manuscrito] : / Geovane de Souza Ferreira Junior. - 2017
44 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2017.
"Orientação : Prof. Me. José Ginaldo de Souza Farias, Coordenação do Curso de Matemática - CCEA."
"Coorientação: Prof. Me. Arlandson Matheus Silva Oliveira, Coordenação do Curso de Matemática - CCEA.""

1. Equações Diofantinas. 2. Equações de Pell. 3. Teoria dos Números.

21. ed. CDD 512.7

Geovane de Souza Ferreira Júnior

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS E APLICAÇÕES

Trabalho de Conclusão de Curso apresentado ao Curso de Licenciatura Plena emMatemática da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Licenciado em Matemática.

Aprovado em 06 de dezembro de 2017

Prof. Me. José Ginaldo de Souza Farias (Orientador)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Wellington Candeia de Araújo (Examinador)
Universidade Estadual da Paraíba (UEPB)

Prof. Me. Alex Pereira Bezerra (Examinador)
Instituto Federal da Paraíba (IFPB)

A Manoel Bento Neto, o grande professor da minha vida, DEDICO.

RESUMO

Na Matemática, quando nos deparamos com uma equação, algumas perguntas surgem naturalmente, por exemplo: a equação tem solução? Em caso afirmativo, quantas? Ou como encontrá-las? Perguntas como essas são muito frequentes no estudo das equações diofantinas, e, nesta monografia, tenta-se responder a estas questões. Essas equações são objetos matemáticos estudados na Teoria dos Números. Este tipo de equação algébrica é da forma polinomial em que suas variáveis, bem como, os coeficientes têm valores no conjunto dos números inteiros. Nesta perspectiva, o objetivo principal deste trabalho é mostrar de forma clara a caracterização das infinitas soluções e aplicações das equações diofantinas mais conhecidas, a saber, as lineares com duas incógnitas e as clássicas equações Pitagórica e de Pell. A metodologia aplicada nesta pesquisa consiste em uma revisão da literatura matemática vinculada a esses problemas.

Palavras Chave: Equações Diofantinas; Equação de Pell; Teoria dos Números.

ABSTRACT

In Mathematics, when we find an equation, some questions arise naturally, for example: does the equation have a solution? If so, how many? Or how to find them? Questions like these are very frequent in the study of Diophantine's equations, and in this monograph we try to answer these questions. These equations are mathematical objects studied in the Theory of Numbers. This type of algebraic equation is of the polynomial form in which its variables, as well as, the coefficients have values in the set of integers. In this perspective, the main objective of this work is to clearly show the characterization of the infinite solutions and applications of the most well-known diophantine equations, namely the linear ones with two unknowns and the classical Pellagoric and Pell equations. The methodology applied in this research consists of a review of the mathematical literature linked to these problems.

Keywords: Diophantine Equations; Pell equation; Theory of Numbers.

Sumário

Introdução 6

1 Noções Preliminares **9**

1.1 Princípio da Boa Ordenação 9

1.2 Princípio de Indução Finita 10

1.3 Divisibilidade. 11

1.4 Máximo Divisor Comum 14

1.5 Números Primos 16

1.6 Congruências 18

1.7 Congruências Lineares 20

2 Equações Diofantinas **22**

2.1 Equações Diofantinas Lineares 22

2.2 Equação Pitagórica 25

2.3 Equação de Pell 27

3 Aplicações **36**

3.1 Aplicações das Equações Lineares 36

3.2 Aplicação da Equação Pitagórica 38

3.3 Aplicação da Equação de Pell 40

3.3.1 Teorema de Størmer 41

Considerações Finais 42

Referências Bibliográficas **43**

Introdução

A Teoria Elementar dos Números é um ramo que tem grandes ligações com outras partes da Matemática, além disso, é uma disciplina obrigatória no currículo de qualquer curso de licenciatura e bacharelado em Matemática. Alguns ilustres matemáticos fizeram excelentes trabalhos na teoria dos números, exemplos como Pitágoras (569-500 a.C.), Euclides ($\simeq$ 350 a.C.), Diofanto ($\simeq$ 250 d.C.), Mersenne (1588-1648), Fermat (1601-1665), Pascal (1623-1662), Euler (1707-1783), Gauss (1777-1855). Muitos resultados obtidos por estes, faz com que a Teoria dos Números seja um ramo da Matemática que se destaque em outras áreas, como na teoria dos códigos e na criptografia.

Na cidade de Alexandria, no Egito, nasceu um grande matemático conhecido por Diofanto. Deu enorme contribuição ao avanço da Matemática, principalmente no campo da Álgebra e da Teoria dos Números. Não se sabe ao certo o século que ele viveu, mas, indícios indicam que a data se distancia de um século antes ou depois do ano de 250 d.C. Um dos poucos dados sobre ele, foi encontrado em forma de enigma, no seu túmulo, enigma esse que dá pistas de como calcular o seu tempo de vida (ver [3]). O problema é o seguinte:

> Deus lhe concedeu ser menino pela sexta parte de sua vida, e somando sua duodécima parte a isso, cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz criança; depois de viver a metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números, ele terminou sua vida [Cohen e Drabkin (1958), citado por Boyer (1996, p. 121)].

Daí, segundo esse enigma histórico que pode ser modelado por uma equação polinomial de primeiro grau, conclui-se que Diofanto teria morrido com uma idade de 84 anos.

O interesse em fazer uma pesquisa sobre as Equações Diofantinas, surgiu principalmente em observar a linha de pesquisa de Diofanto. Antes dele, os matemáticos, principalmente os babilónicos, se preocupavam em caracterizar as soluções de equações aproximadas. Já a obra de Diofanto, mesmo se aproximando da Álgebra dos babilônicos, envolve equações com soluções no conjunto dos números inteiros, essas equações são denominadas de Equações Diofantinas, tema central dessa monografia, e recebe esse nome em homenagem à Diofanto.

Ademais, este estudo é dividido em três capítulos: o primeiro segue de forma preliminar, nesse sentido, são apresentados vários resultados como pré-requisitos de muita importância para o desenvolvimento de todo o estudo. No segundo capítulo, será apresentado o estudo das principais Equações Diofantinas. Iniciando com as equações lineares com duas incógnitas, e posteriormente, caracterizando as soluções da Equação Pitagórica. Por conseguinte, serão apresentadas as infinitas soluções da Equação de Pell. Finalmente, no terceiro e último capitulo, será abordado algumas aplicações sobre a temática dessas equações, onde são deixadas as considerações finais.

Capítulo 1

Noções Preliminares

Neste capitulo são apresentados vários resultados importantes para o estudo das Equações Diofantinas. Inicia-se com a apresentação de duas ferramentas usadas em demonstração de teoremas: o principio de indução finita e o princípio da boa ordem. O princípio de indução, serve como método de demonstração para muitos teoremas que envolvem o conjunto $\mathbb{N}$ dos números naturais. Em particular, as demonstrações que versam sobre propriedades dos números naturais podem ser demonstradas por indução.

1.1 Princípio da Boa Ordenação

Definição 1.1. *Seja X um subconjunto não vazio de $\mathbb{Z}$. Dizemos que X é* ***limitado inferiormente*** *quando existe um elemento $x_0 \in \mathbb{Z}$ tal que $x_0 \leqslant x$, $\forall x \in X$. Desse modo, X é limitado inferiormente por x_0. Nessas condições, um elemento $m \in X$ é chamado* ***elemento mínimo*** *de X quando*

$$m \leqslant x, \ \forall x \in X.$$

A notação para o elemento mínimo de X será indicada por

$$x_0 = \min X.$$

Axioma 1.1 (Princípio da Boa Ordenação - PBO)**.** *Todo subconjunto não vazio e limitado inferiormente X de $\mathbb{Z}$ possui menor elemento.*

Proposição 1.1. *No Axioma 1.1 , o elemento mínimo de X é único.*

Demonstração: Se x_0 e y_0 são elementos mínimos de x, então $x_0 \leqslant y_0$ e $y_0 \leqslant x_0$. Portanto, $x_0 = y_0$.[1] ■

1.2 Princípio de Indução Finita

Teorema 1.1 (Princípio de Indução finita)**.** *Seja $p(n)$ uma sentença em $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$. Então, $p(n)$ é verdadeira para todo $n \geq n_0$, desde que $p(n)$ satisfaça as seguintes condições:*

1. *$P(n_0)$ é verdadeira;*
2. *Se $P(n)$ é verdadeira para todo $n \geq n_0$, então $P(n+1)$ também é verdadeira.*

Exemplo 1.1. *Prove que* $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$, $\forall\, n \in \mathbb{N}$.

Solução: Seja $P(n)$ a sentença sobre $\mathbb{N}$ dada por

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

é claro que $P(n_0 = 1)$ é verdadeira (base de indução),

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

Vamos supor que para $p(k)$ seja verdadeira (hipótese de indução), com $k \geq 1$ e provaremos que a sentença $p(k+1)$ também é. Por hipótese

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}.$$

Agora, somando $(k+1)$ em ambos os lados desta igualdade, mostra-se que $P(k+1)$ é

[1] Dizemos que dois números inteiros a e b são iguais se, e somente se, $a \leqslant b$ e $b \leqslant a$.

verdadeira

$$\begin{aligned} 1+2+\cdots+k+(k+1) &= \frac{k(k+1)}{2}+(k+1) \\ &= \frac{k(k+1)+2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

e portanto, $P(n)$ vale para todos os números naturais.

1.3 Divisibilidade.

Definição 1.2. *Se a e b são inteiros, dizemos que b* ***divide*** *a. Denotamos por $b \mid a$, se existir um inteiro c tal que*

$$a = bc. \tag{1.1}$$

Se b não dividir a denotaremos por $b \nmid a$.

Lema 1.1. *Se $b \mid a$, e $a \neq 0$, então $|b| \leqslant |a|$.*

Demonstração: Se $b \mid a$, então existe $c \in \mathbb{Z}$ de tal modo que $a = bc$. logo,

$$|a| = |b| \cdot |c|.$$

Como $c \neq 0$, segue que $|c| \geq 1$, multiplicando ambos os lados dessa desigualdade por $|b|$, temos,

$$|b| \leqslant |b| \cdot |c| = |a|.$$

■

Proposição 1.2. *Em $\mathbb{Z}$ valem as seguintes propriedades:*

1. *Os únicos divisores de 1 são 1 e -1*

2. *Se $a \mid b$ e $b \mid a$, então $a = \pm b$*

Demonstração: (1) Seja b um divisor de 1, então pelo Lema 1.1, $|b| \leqslant 1$. Assim, $0 < |b| \leqslant 1$. Como não existe inteiro entre 0 e 1 concluímos que $|b| = 1$, isto é, $b = \pm 1$. (2) Se $a \mid b$ e $b \mid a$, então $a = \lambda_1 b$ e $b = \lambda_2 a$, com $\lambda_1,\ \lambda_2 \in \mathbb{Z}$. Desse modo,

$$a = (\lambda_1 \cdot \lambda_2)a.$$

Logo, $\lambda_1 \cdot \lambda_2 = 1$, pelo item (1), $\lambda_1 = \pm 1$, e implica que $a = \pm b$.

■

Teorema 1.2. *A divisibilidade tem as seguintes propriedades.*

1. *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*
2. *$a \mid b$ e $c \mid d$, então $ac \mid bd$.*
3. *$a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, $\forall\ m, n \in \mathbb{Z}$.*

Demonstração: (1) Por hipótese, $b = ak_1$ e $c = bk_2$, com $k_1, k_2 \in \mathbb{Z}$ substituindo o valor de b em $c = bk_2$, obtemos $c = a(k_1k_2)$, isto é, $a \mid c$.

(2) Sendo $b = ak_1$ e $d = ck_2$, temos $db = (ac)(k_1k_2)$, portanto $ac \mid bd$.

(3) Como $a \mid b$ e $a \mid c$, então $b = ak_1$ e $c = ak_2$. Logo, dados inteiros m e n, $mb = amk_1$ e $nc = ank_2$, logo $mb + nc = a(mk_1 + nk_2)$. assim, $a \mid (mb + nc.)$

■

O próximo teorema será uma ferramenta importante para demonstrar alguns resultado que virão, como por exemplo, na próxima seção que fala do máximo divisor comum.

Teorema 1.3 (Algoritmo da Divisão.)**.** [2] *Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que:*

$$a = qb + r, \quad com\ \ 0 \leqslant r < b.\ \ (r = 0 \Leftrightarrow b \mid a)$$

(q é chamado de quociente e r é o resto da divisão de a por b).

[2] Esse resultado costuma ser atribuído de forma errônea a Arquimedes e chamado "Principio de Arquimedes"(ver [9]).

Demonstração: Considere o conjunto

$$L = \{a - bq : \ q \in \mathbb{Z} \ e \ a - bq \geq 0\}$$

L é não vazio. De fato, desde que $b \geq 1$, então $|a| \cdot b \geq |a|$. Logo,

$$a - (-|a|) \cdot b = a + |a| \cdot b \geq a + |a| \geq 0.$$

Como $x = a - (-|a|) \cdot b$ é da forma $a - qb$, com $q = -|a|$, segue que $x \in L$.
Existência: Como L é limitado inferiormente e não vazio, pelo PBO L possui elemento mínimo, digamos $r = \min L$. Como $r \in L$, então $r \geq 0$ e

$$r = a - qb \ \text{ com } \ q \in \mathbb{Z}.$$

É notório que $r < b$. Pois do contrário, $r - b \geq 0$, teríamos

$$r - b = a - bq - b = a - b(q + 1).$$

Assim $r - b \in L$ e $r - b < r$, o que contraria a minimalidade de r. Portanto, $a = qb + r$, com $q \in \mathbb{Z}$ e $0 \leqslant r < b$, o que prova a existência dos inteiros q e r.
Unicidade: Considere $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = bq_1 + r_1, \ \text{ com } \ 0 \leqslant r_1 \leqslant b.$$

Assim, $bq + r = bq_1 + r_1$, o que implica

$$r - r_1 = b(q_1 - q),$$

ou seja, $b \mid (r - r_1.)$ Com $|r - r_1| < b$, segue que $r - r_1 = 0$, isto é, $q_1 = q$, com $b \neq 0$.

■

Teorema 1.4 (Algoritmo de Euclides)**.** *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com*

$b \neq 0$. *Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2},\ 0 \leq r_{j+2} < r_{j+1}$$

para $j = 0, 1, 2, 3, \cdots, n-1$ *e* $r_{n+1} = 0$ *então* $(a, b) = r_n$, *o último resto não-nulo.*

A demonstração desse teorema é feita com detalhes em [9] .

1.4 Máximo Divisor Comum

Nesta seção, o máximo divisor comum de dois inteiros a e b será o número natural d, denotado por $d = (a, b)$, que os divide e é divisível por todo divisor comum de a e b.

Definição 1.3. *Sejam* $a, b \in \mathbb{Z} \setminus \{0\}$. *Dizemos que* $d \in \mathbb{N}$ *é o* ***máximo divisor comum*** *de* a *e* b *quando as seguintes condições são satisfeitas:*

1. $d \mid a$ *e* $d \mid b$;
2. $c \mid a$ *e* $c \mid b$, *então* $c \mid d$.

Teorema 1.5 (Bachet-Bézout)**.** *Se* $d = (a, b)$, *então existem inteiros* x_0 *e* y_0 *tais que*

$$d = ax_0 + by_0. \tag{1.2}$$

Demonstração: Consideremos o conjunto

$$W = \{ax + by : x, y \in \mathbb{Z} \text{ e } ax + by > 0\}.$$

Note que $W \neq \emptyset$, pois para $x = y = 1$,

$$a1 + b1 = a + b > 0 \ \Rightarrow\ a + b \in W.$$

Assim pelo PBO, W possui menor elemento, digamos $\lambda = \min W$. Vamos mostrar que $\lambda =$

(a, b). Como $\lambda \in W$, existem $x_0, y_0 \in \mathbb{Z}$, tais que

$$\lambda = ax_0 + by_0. \tag{1.3}$$

Usando o algoritmo da divisão (Teorema 1.3) com os elementos a e λ temos

$$a = \lambda q + r, \ \text{ com } \ 0 \leqslant r < \lambda. \tag{1.4}$$

Substituindo o valor de λ em 1.3 na igualdade 1.4, segue que

$$\begin{aligned} r = a - \lambda q &= a - (ax_0 + by_0)q \\ &= a - aqx_0 - bqy_0. \end{aligned}$$

Daí,

$$r = a(1 - qx_0) + b(-qy_0).$$

Isso mostra que $r = au + bv$, onde $u = 1 - qx_0$ e $v = -qy_0$. Consequentemente $r = 0$, pois do contrário, para $r > 0$, $r \in W$, o que contraria o fato de λ ser mínimo de W, visto que $\lambda > r$, logo $a = \lambda q$, então $\lambda \mid a$. De forma similar, prova-se que $\lambda \mid b$. Sendo $d = (a, b)$, então $a = d\lambda_1$ e $b = d\lambda_2$. Logo por 1.4,

$$\lambda = \lambda(d\lambda_1)x_0 + (d\lambda_2)y_0 = d(\lambda_1 x_0 + \lambda y_0),$$

ou seja, $d \mid \lambda$, e como $\lambda \mid d$, pois $d = (a, b)$, segue que $d = \lambda$. Logo $d = ax_0 + by_0$.

■

Teorema 1.6. *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração: Como $(a, b) = 1$ pelo Teorema anterior, existem inteiros n e m tais que $na + mb = 1$. Multiplicando-se os dois lados dessa igualdade por c temos: $n(ac) + m(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ então, pelo Teorema 1.2, $a \mid c$.

■ .

1.5 Números Primos

Definição 1.4. *Todo número $p \in \mathbb{Z} \setminus \{-1, 0, 1\}$ é primo quando seus únicos divisores são* 1 *e* $|p|$.

Observação 1.1. *Se p não é um número primo dizemos que p é composto.*

Proposição 1.3. *Se $p \mid ab$, p primo, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \nmid a$ então $(a, p) = 1$, o que implica, pelo Teorema 1.6, $p \mid b$.

■

Corolário 1.1. *Se p é primo e $p \mid a_1 a_2 \cdots a_n$, então $p \mid a_i$ para algum $i = 1, 2, \cdots n$.*

Demonstração: Provaremos usando indução em n. Para $n = 1$, o resultado é imediato. Suponhamos, que o resultado seja válido para $n \geq 1$. Logo, para $a_1 a_2 \cdots a_n a_{n+1} \in \mathbb{Z}$, temos

$$\begin{aligned} p \mid a_1 a_2 \cdots a_n a_{n+1} &\Rightarrow p \mid (a_1 a_2 \cdots a_n) a_{n+1} \\ &\Rightarrow p \mid a_1 a_2 \cdots a_n \text{ ou } p \mid a_{n+1}. \end{aligned}$$

Se $p \mid a_{n+1}$, o resultado segue. Se $(p \mid a_1 a_2 \cdots a_n)$, então, por hipótese de indução, $p \mid a_i$, para algum $i = 1, 2, \cdots, n$.

■

Corolário 1.2. *Se $p, q_1, q_2, \cdots, q_r$ são todos primos e $p \mid q_1 q_2 \cdots q_r$, então $p = q_i$ para algum $i = 1, 2, \cdots, r$.*

Teorema 1.7 (Fundamental da Aritmética - TFA.)**.** *Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de primos.*

Demonstração: Há duas coisas a serem provadas: a existência dos primos, e a unicidade da fatoração.

Existência: Consideremos o conjunto

$$M = \{a \in \mathbb{N} : a > 1 : a \neq p_1 p_2 \cdots p_n\}.$$

Para primos $p_1, p_2, \cdots, p_n$. Se mostramos que $m = \emptyset$, então a demonstração está provada. Por absurdo, se $M \neq \emptyset$, então pelo PBO, M possui elemento mínimo m. Como m não pode ser primo e, por isso, é composto, isto é,

$$m = bc, \text{ com } a < b, c < m.$$

como $b < m$ e $c < m$, então $b \notin M$ e $c \notin M$, pois $m = \min M$. Assim, sendo $b > 1$ e $c > 1$, segue que estes números são primos ou são produtos de primos. Logo, $m = bc$ é um produto de primos, o que é uma contradição. Portanto, $M = \emptyset$.

Unicidade: Suponha que

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

com $p_1, p_2 \cdots p_n, q_1, q_2 \cdots q_m$ todos primos. Logo,

$$p_1 \mid q_1 q_2 \cdots q_m$$

e, pelo Corolário 1.2, temos $p_1 = q_j$ para algum $j = 1, 2, \cdots m$, digamos que $p_1 = q_1$. Assim, segue que

$$p_2 \cdots p_n = q_2 \cdots q_m.$$

Seguindo de forma análoga, tem-se $p_2 = q_j$ para algum $j = 2, 3, \cdots, m$. Sem perda de generalidade, suponhamos $p_2 = q_2$, obtemos

$$p_3 \cdots p_n = q_3 \cdots q_m.$$

Continuando o processo, e assumindo $n > m$, temos

$$1 = p_{m+1} \cdots p_n$$

o que é um absurdo. E supondo $n < m$,

$$1 = p_{n+1} \cdots p_m$$

O que também é um absurdo. Assim, $m = n$ e $q_i = p_i$, $\forall i = 1, 2, \cdots, n$.

■

Teorema 1.8. *Se dois inteiros positivos a e b possuem as fatorações*

$$a = \prod_{i=1}^{\infty} p_i^{a_i}, \quad b = \prod_{i=1}^{\infty} p_i^{b_i}$$

então o máximo divisor comum de a e b é igual a :

$$(a, b) = \prod_{i=1}^{\infty} p_i^{c_i}, \quad \textit{onde} \;\; c_i = \min\{a_i, b_i\}. \tag{1.5}$$

Demonstração: Para que um produto de fatores primos comuns sejam um divisor comum, nenhum expoente c_i de p_i poderá superar nem a_i e nem b_i. Como estamos interessados no maior dos divisores positivos, basta tomarmos, para c_i, o menor desses dois.

■

Exemplo 1.2. *Sendo $a = 360 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^0$ e $b = 640332 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^2 \cdot 11^2$, então*

$$(a, b) = (360, 640332) = (640332, 360) = 2^2 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^0 = 36.$$

1.6 Congruências

Definição 1.5. *Se a e b são inteiros dizemos que a **é congruente a** b **módulo** m $(m > 0)$ se $m \mid (a - b)$. Denotamos isto por $a \equiv b \,(mod\, m)$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m, ou simplesmente que a não é congruente a b módulo m, e neste caso, denotamos $a \not\equiv b \,(mod\, m)$.*

Proposição 1.4. *Se a e b são inteiros, temos que $a \equiv b \,(mod\, m)$ se, e somente se, existir um número inteiro k tal que $a = b + kb$.*

Demonstração: Se $a \equiv b \pmod{m}$, então $m \mid (a - b)$ o que implica na existência de um número inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial, basta observar que $a = b + km$, temos $km = a - b$, ou seja, $m \mid (a - b)$, isto é, $a \equiv b \pmod{m}$.

■

Proposição 1.5. *Dados a, b, m e c inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv b \ (mod\, m)$

2. *Se* $a \equiv b \ (mod\, m)$, *então* $a \equiv b \ (mod\, m)$.

3. *Se* $a \equiv b \ (mod\, m)$ *e* $b \equiv c \ (mod\, m)$, *então* $a \equiv c \ (mod\, m)$.

Demonstração: (1) Como $m \mid 0$, então $m \mid (a - a)$, implica que $a \equiv a \pmod{m}$.

(2) Se $a \equiv b \pmod{m}$, então $a - b = mk$, com $k \in \mathbb{Z}$. Logo, $b - a = m(-k)$ e $-k \in \mathbb{Z}$, isto é, $b \equiv a \pmod{m}$.

(3) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem k_1 e k_2 tais que

$$a - b = mk_1 \ \text{ e } \ b - c = mk_2.$$

Somando-se, membro a membro, estas últimas equações, obtemos $a - c = (k_1 + k_2)m$. O que implica $a \equiv c \pmod{m}$. ■

Teorema 1.9. *Se a, b, c, d e m são inteiros tais que* $a \equiv b \ (mod\, m)$ *e* $c \equiv d \ (mod\, m)$, *então*

1. $a + c \equiv b + d \ (mod\, m)$ *e* $ac \equiv bd \ (mod\, m)$.

2. $a + c \equiv b + c \ (mod\, m)$ *e* $ac \equiv bc \ (mod\, m)$.

3. $a^k \equiv b^k \ (mod\, m)$ *para qualquer* $k \in \mathbb{N}$.

Demonstração: (1) De $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ temos $a - b = k_1 m$ e $c - d = k_2 m$. Somando membro a membro estas equações, obtemos que

$$a + c = b + d + (k_1 + k_2)m,$$

Assim, $(a + c) \equiv (b + d) \pmod{m}$. Agora, multiplicando membro a membro as mesmas equações

$$ac = (b + k_1 m)(d + k_2 m) = bd + k_3 m,$$

em que $k_3 = bk_2 + dk_1 + k_1 k_2 m$. Portanto, $ac \equiv bd \pmod{m}$.

(2) Como $a \equiv b \pmod{m}$, por hipótese, e como $c \equiv c \pmod{m}$, segue do item (1) que

$$a + c \equiv b + c \pmod{m} \text{ e } ac \equiv bc \pmod{m}.$$

(3) Vamos usar indução para provar que $a^k \equiv b^k \pmod{m}$ para todo inteiro $k \geq 1$. Como por hipótese, $a \equiv b \pmod{m}$, então o resultado é válido para $k = 1$. Suponhamos que por hipótese de indução que $a^k \equiv b^k \pmod{m}$ para $k \geq 1$. Como $a \equiv b \pmod{m}$, então multiplicando membro a membro estas duas congruências, segue do item (1) que $a^{k+1} \equiv b^{k+1} \pmod{m}$. Portanto, $a^k \equiv b^k \pmod{m}$ para todo $k \geq 1$

(4) Por hipótese $(a + c) \equiv (b + c) \pmod{m}$. Como $-c \equiv -c \pmod{m}$, então do item (1), obtemos que $a \equiv b \pmod{m}$.

■

Teorema 1.10. *Se a, b, c, e m são inteiros e $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{m/d}$ onde $d = (c, m)$.*

Demonstração: De $ac \equiv bc \pmod{m}$ temos $ac - bc = c(a - b) = km$. Se dividirmos os dois membros por d, teremos $(m/a) \cdot (a - b) = k(m/d)$. Logo $(m/a) \mid (c/d)(a - b)$ e, como $(m/d, c/d) = 1$, então $(m/d) \mid (a - b)$ o que implica que $a \equiv b \pmod{m/d}$. ■

1.7 Congruências Lineares

Definição 1.6. *Dados a e b inteiros, com $a \neq 0$, uma congruência da forma*

$$ax \equiv b \pmod{m}$$

*é chamada **congruência linear,** em que x é uma incógnita.*

Teorema 1.11. *A congruência linear $ax \equiv b \pmod{m}$ tem solução inteira se, e somente se, $d \mid b$, em que $d = (a, m)$.*

Demonstração: Suponhamos que x_0 seja solução de $ax \equiv b \pmod{m}$ e $d = (a, m)$. Assim, $ax_0 - b = km$, isto é, $b = ax_0 - km$. Como $d \mid a$ e $d \mid m$, então $d \mid b$.

Reciprocamente, vamos supor que $d \mid b$. Pelo Teorema de Bachet-Bézout, existem r e s inteiros, tais que

$$d = a \cdot r + s \cdot m$$

como $b = dt$, com $t \in \mathbb{Z}$, então

$$b = (ar + sm)t = art + smt,$$

ou seja, $a(rt) \equiv b \pmod{m}$, $x_0 = rt$ é solução de $ax \equiv b \pmod{m}$. ■

Teorema 1.12. *Se x_0 é uma solução da congruência linear $ax \equiv b \,(mod\, m)$, então todas as soluções desta congruência são da forma*

$$x = x_0 + \frac{m}{d} \quad com \quad k \in \mathbb{Z}, \tag{1.6}$$

em que $d = (a, m)$.

Demonstração: Inicialmente, vamos provar que $x = x_0 + (m/d)k$, com $d = (a, m)$, é uma solução de $ax \equiv b \pmod{m}$ para cada inteiro k. Desde que $ax_0 \equiv b \pmod{m}$, ou seja, $ax_0 = b + \lambda m$, com $\lambda \in \mathbb{Z}$, temos

$$ax = a(x_0 + (m/d)k) = ax_0 + a(m/d)k = b + m(\lambda + ak/d).$$

Portanto, $ax \equiv b \pmod{m}$, pois $ak/d \in \mathbb{Z}$.

Agora, sejam $x_1 \in \mathbb{Z}$ tal que $ax_1 \equiv b \pmod{m}$. Como $ax_0 \equiv ax_1 \pmod{m}$. Então, pelo Teorema 1.10, $x_0 \equiv x_1 \pmod{m/d}$, ou seja, $x_1 = x_0 + \frac{m}{d}k$ com $k \in \mathbb{Z}$. ■

Capítulo 2

Equações Diofantinas

O estudo que segue, aborda o objeto matemático central deste trabalho, as Equações Diofantinas. Neste capítulo, serão apresentados as principais equações.

Definição 2.1. *Uma* ***equação diofantina*** *é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas.*

2.1 Equações Diofantinas Lineares

Definição 2.2. *Uma* ***equação diofantina linear*** *é uma equação da forma*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{2.1}$$

onde $a_1, \cdots, a_n$ *são inteiros dados, denominados coeficientes,* b *também é um inteiro, e* $x_1, \cdots, x_n$ *são as incógnitas.*

Nessa seção serão estudadas as equações diofantinas lineares com apenas duas incógnitas, isto é, equações da forma

$$ax + by = c. \tag{2.2}$$

Observação 2.1. *A equação 2.2 nos guia à congruência linear*

$$ax \equiv c \,(mod\, b).$$

Teorema 2.1. *A equação diofantina $ax + by = c$ tem soluções inteiras se, e somente se, $d \mid c$, com $d = (a, b)$. Além disso, se x_0 e y_0 é uma solução particular desta equação, então sua solução geral é dada por*

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

em que k é um inteiro.

Demonstração: Como $ax + by = c$ se, e somente se, $ax \equiv c \pmod{b}$, então, pelo Teorema 1.11 , $ax + by = c$ tem solução inteira se, e somente se, $d \mid c$, com $d = (a, b)$.
Agora, se x_0 e y_0 é uma solução particular. Então

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

também o é, pois $ax_0 + by_0 = c$, isto é,

$$\begin{aligned} ax' + by' &= a[x_0 + (b/d)k] + b[y_0 - (a/d)k] \\ &= (ax_0 + by_0) + (ab/d - ab/d)k \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Agora, seja x' e y' outra solução para $ax + by = c$. Assim,

$$ax_0 + by_0 = ax' + by' = c,$$

mas, temos

$$a(x' - x_0) = b(y_0 - y') \tag{2.3}$$

se $d = (a, b)$, então $a = dk_1$ e $b = dk_2$, com $(k_1, k_2) = 1$. Substituindo estes valores em 2.3 e cancelando o fator comum d, tem-se

$$k_1(x' - x_0) = k_2(y_0 - y'). \tag{2.4}$$

Isto é, $k_1 \mid k_2(y_0 - y')$, Como $(k_1, k_2) = 1$, segue que $k_1 \mid (y_0 - y')$, ou seja, $y_0 - y' = k_1 k$ para algum inteiro k. Substituindo este valor em, 2.4. Obtemos $x' - x_0 = k_2 k$. Portanto,

$$\begin{aligned} x' &= x_0 + kk_2 = x_0 + (b/d)k, \\ y' &= y_0 - kk_1 = y_0 - (a/d)k. \end{aligned}$$

■

Exemplo 2.1. *Resolva a seguinte equação diofantina*

$$6x + 15y = 225.$$

Solução: Como $(6, 15) = 3$ e 3 divide 225, então esta equação tem solução inteiras, e dividindo toda a equação por $3 = (6, 15)$, tem-se a equação equivalente à seguir

$$2x + 5y = 75.$$

Agora, basta observar que $(2, 5) = 1$. Devemos encontrar n e m inteiros tais que

$$2n + 5m = 1.$$

Logo, $n = -2$ e $m = 1$ é solução. Agora, basta multiplicar toda a equação por 75, dai segue que

$$2 \cdot (-150) + 5 \cdot (75) = 75,$$

então, $x_0 = -150$ e $y_0 = 75$, portanto a solução geral da equação diofantina é

$$x = -150 + 5k \quad \text{e} \quad y = 75 - 2k, \;\; k \in \mathbb{Z}.$$

2.2 Equação Pitagórica

Nessa seção, trataremos da **equação pitagórica,** nosso principal objetivo é determinar todas as soluções da equação

$$x^2 + y^2 = z^2. \tag{2.5}$$

Com x, y e $z \in \mathbb{Z}$. Nesse sentido, todas as soluções da equação 2.5, são denominadas de **ternos pitagóricos.**[1] Por exemplo, $(3, 4, 5)$ e $(6, 8, 10)$ são uns dos ternos pitagóricos mais conhecidos.

Definição 2.3. *Um terno de inteiros (a, b, c) satisfazendo*

$$a^2 + b^2 = c^2$$

é chamado ***terno pitagórico primitivo*** *se $(a, b, c) = 1$.*

Observe que se (a, b, c) é um terno pitagórico, então é muito fácil notar que (ka, kb, kc), com $k \in \mathbb{Z}$, também será um terno pitagórico.

Lema 2.1. *Se (a, b, c) é um terno pitagórico primitivo, então $(a, b) = (a, c) = (b, c) = 1$.*

Demonstração: Suponhamos que p é um número primo divisor comum de a e b, então é claro que p também é divisor comum de $a^2 + b^2 = c^2$ e, conseguintemente de c, mas isso contradiz o fato de (a, b, c) ser solução primitiva. Portanto, $(a, b) = 1$. Usando o mesmo argumento, $(a, c) = (b, c) = 1$. ■

Lema 2.2. *Se (a, b, c) é um terno pitagórico primitivo, então a e b são de paridades distintas. Em particular, c é impar.*

Demonstração: Se a e b são ambos pares, $2 \mid a^2 + b^2 = c^2$, ou seja, $2 \mid c$. Logo, $(a, b, c) \neq 1$, o que contradiz o fato de (a, b, c) ser um terno pitagórico primitivo. Por outro lado, se a e b são ambos ímpares, então $a = 2\alpha + 1$ e $b = 2\beta + 1$, com $\alpha, \beta \in \mathbb{Z}$, assim

$$c^2 = a^2 + b^2 = (2\alpha + 1)^2 + (2\beta + 1)^2 = 4k + 2,$$

[1] Esta denominação vem do fato desses inteiros corresponderem aos comprimentos dos lados de um triângulo retângulo

com k inteiro. Isso implica que $c^2 \equiv 2 \pmod 4$, ou seja, c^2 é divisível por 2, mas não é por 4. Mas, isso é um absurdo, pois, se c^2 é divisível por 2, c também o é; daí, c^2 é divisível por 4. Portanto, a e b têm paridade distinta. Em particular, c é ímpar, pois c^2 é ímpar. ■

Lema 2.3. *Sejam m e n inteiros tais que $(m, n) = 1$. Se $mn = k^2$, então m e n são ambos quadrados perfeitos.*

Para detalhes da demonstração desse resultado, veja [11].

Teorema 2.2. *Todos os ternos pitagóricos primitivos (a, b, c), com $a > 0$, $b > 0$ e $c > 0$, são da forma*

$$a = 2mn, \;\; b = m^2 - n^2 \;\; e \;\; c = m^2 + n^2,$$

em que $(m, n) = 1$, $m > n > 0$ e $m + n$ é ímpar.

Demonstração: Sem perda de generalidade, considere a e b par e ímpar, respectivamente, de modo que c é ímpar. Assim, $c - b$ e $c + b$ são ambos pares, isto é,

$$c - b = 2u \;\; \text{e} \;\; c + b = 2v.$$

Note que os inteiros u e v são primos entre si, pois se $(u, v) = d$, então $d \mid u + v$ e $d \mid u - v$. Mas, $2u + 2v = 2c$ e $2u - 2v = 2b$, ou seja, $d \mid c$ e $d \mid b$, o que de acordo com o Lema 2.1, $d = 1$. Agora, vamos escrever a equação $a^2 + b^2 = c^2$ da seguinte forma

$$a^2 = c^2 - b^2 = (c - b)(c + b).$$

Daí,

$$\left(\frac{a}{2}\right)^2 = \frac{a^2}{4} = \frac{(c - b)(c + b)}{4} = \frac{2u2v}{4} = uv.$$

Ou melhor,

$$\left(\frac{a}{2}\right)^2 = uv,$$

como $(u, v) = 1$ e uv é um quadrado perfeito, segue do Lema 2.3 que u e v são ambos quadrados perfeitos, isto é,

$$u = n^2 \;\; \text{e} \;\; v = m^2, \;\; \text{com} \;\; m, n \in \mathbb{N}.$$

Assim, $c = u + v = n^2 + m^2$ e $b = v - u = m^2 - n^2$ e $a = 4uv = 4n^2m^2$, ou seja, $a = 2mn$, portanto

$$a = 2mn, \;\; b = m^2 - n^2 \;\text{ e }\; c = n^2 + m^2.$$

Se $(m, n) = d$, então $d \mid b$ e $d \mid c$, assim, $d = 1$. Além disso, se m e n têm a mesma paridade, então $c = m^2 + n^2$ e $b = m^2 - n^2$ são ambos pares, o que contradiz o fato de $(b, c) = 1$. Portanto, m e n são de paridades distintas, ou seja, $m + n$ é ímpar. Logo,

$$(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$$

é de fato um terno pitagórico. A fim de mostrar que este é primitivo, suponhamos que $(a, b, c) = d > 1$. Logo, existe um primo p tal que $p \mid d$, com $p \mid b$, então $p \neq 2$, pois b é ímpar. Assim, $p \mid c$, de modo que $p \mid b + c$ e $p \mid c - b$, isto é, $p \mid 2m^2$ e $p \mid 2n^2$, assim, $p \mid m$ e $p \mid n$, mas isso é absurdo, pois $(m, n) = 1$. Assim $d = 1$ e concluímos que (a, b, c) é um terno pitagórico primitivo.

■

2.3 Equação de Pell

Definição 2.4. *Chama-se* ***equação de Pell*** *toda equação diofantina da forma*

$$x^2 - dy^2 = 1, \tag{2.6}$$

onde $x, y \in \mathbb{Z}$, *com* $d \in \mathbb{N}$, $\sqrt{d} \notin \mathbb{N}$.

Observação 2.2. *Se* $d < 1$, *então* $-d = a > 1$, *ou seja,* $x^2 + ay^2 = 1$ *admite apenas as soluções triviais* $x = \pm 1$ *e* $y = 0$.

Observação 2.3. *Se* $d = -1$, *as soluções de* $x^2 + y^2 = 1$ *são:* $x = \pm 1$ *e* $y = 0$ *ou* $x = 0$ *e* $y = \pm 1$.

Observação 2.4. *Se* d *é um quadrado perfeito, isto é,* $\sqrt{d} \in \mathbb{N}$, *então* $d = a^2$, $a > 0$, *então*

$$x^2 - (ay)^2 = (x - ay)(x + ay) = 1.$$

Então as únicas soluções dessa equação, são $(x-ay)=(x+ay)=1$ *ou* $(x-ay)=(x+ay)=-1$. *Daí,* $x=\pm 1$ *e* $y=0$.

Nas Observações 2.2, 2.3 e 2.4, tem-se apenas casos em que a equação de Pell tem soluções triviais. Mas, as coisas ficam mais interessantes quando na Equação 2.6 podemos encontrar suas soluções não triviais.

Se $d>1$ e não é um quadrado perfeito, ou seja, $\sqrt{d}\notin\mathbb{N}$, então $\sqrt{d}\in\mathbb{R}\setminus\mathbb{Q}$. De fato, se $\sqrt{d}=\dfrac{p}{q}$, com $p,q\in\mathbb{N}$ e $(p,q)=1$, então podemos ter $d=\dfrac{p^2}{q^2}$, com $(p^2,q^2)=1$, segue que $q^2=1$ e, assim, $d=p^2$, o que é uma contradição. Portanto, $\sqrt{d}$ é irracional.

Agora, considere o conjunto[2]

$$\mathbb{Z}[\sqrt{d}]=\{x+y\sqrt{d}\ :\ x,y\in\mathbb{Z}\}.$$

Observe que $0=0+0\sqrt{d}$, e assim, $0\in\mathbb{Z}[\sqrt{d}]$. Portanto, $\mathbb{Z}[\sqrt{d}]\neq\emptyset$. Em particular, $\mathbb{Z}\subset\mathbb{Z}[\sqrt{d}]$, pois se c é um número inteiro, então $c=c+0\sqrt{d}$.

Podemos definir em $\mathbb{Z}[\sqrt{d}]$ as operações de adição " $+$ " e multiplicação " $\cdot$ " da seguinte forma: dados $\alpha=x_1+b_1\sqrt{d}$ e $\beta=x_2+y_2\sqrt{d}$, em que $a_1,a_2,b_1,b_2\in\mathbb{Z}$, então

$$\alpha+\beta=(a_1+a_2)+(b_1+b_2)\sqrt{d}$$

e

$$\alpha\cdot\beta=(a_1a_2+db_1b_2)+(a_1b_2+a_2b_1)\sqrt{d}.$$

Observação 2.5. *Se* $\alpha\in\mathbb{Z}[\sqrt{d}]$, *então existe um único par de inteiros* x *e* z *tais que* $\alpha=x+y\sqrt{d}$. *De fato, se* $\alpha=x+y\sqrt{d}=\beta=z+w\sqrt{d}$, *com* $x,y,z,w\in\mathbb{Z}$, *então, se* $y=z$ *e* $x+y\sqrt{d}=z+w\sqrt{d}$, *isso implica* $x=z$. *Mas, se* $y\neq w$, *e* $x-z\sqrt{d}=w-y\sqrt{d}$, *então*

$$\sqrt{d}=\frac{x-z}{w-y}\in\mathbb{Q}.$$

o que é um absurdo. Logo $w=y$ *e* $x=z$.

[2]Sendo d um natural que não é um quadrado perfeito, então o conjunto $A=\mathbb{Z}[\sqrt{d}]$ com as operações de adição " $+$ " e multiplicação " $\cdot$ " é um anel comutativo com unidade. O leitor com interesse pode ver a referência [10].

Definição 2.5. *Dado $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, chamamos de* ***conjugado*** *de α, o elemento $\overline{\alpha} = x - y\sqrt{d}$.*

Observemos que a partir dessa definição

$$\alpha \cdot \overline{\alpha} = (x + y\sqrt{d}) \cdot (x - y\sqrt{d}) = x^2 - y^2\sqrt{d}. \tag{2.7}$$

$$\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}, \ \ \forall \alpha, \beta \in \mathbb{Z}[\sqrt{d}]. \tag{2.8}$$

E usando indução em n, pode-se provar que

$$\overline{\alpha^n} = \overline{\alpha}^n, \ \ \forall \alpha \in \mathbb{Z}[\sqrt{d}] \ \text{ e } \ n \in \mathbb{N}. \tag{2.9}$$

Por fim, mostra-se que se $(x + y\sqrt{d})^n \in \mathbb{Z}[\sqrt{d}]$, então

$$(x + y\sqrt{d})^n = x_n + y_n\sqrt{d}, \tag{2.10}$$

para cada $n \in \mathbb{N}$, sendo x_n e y_n inteiros.

Lema 2.4. *Se d é um inteiro positivo que não é um quadrado perfeito, existe um inteiro não nulo m tal que*

$$x^2 - dy^2 = m$$

admite infinitas soluções.

Veja a demonstração desse resultado na referência [6].

Teorema 2.3. *A equação $x^2 - dy^2 = 1$, onde d é um inteiro positivo que não é quadrado perfeito, admite solução.*

Demonstração: Conforme o Lema 2.4, onde d podemos tomar um inteiro m de modo que a equação

$$x^2 - dy^2 = m \tag{2.11}$$

admite soluções inteiras. Podemos escolher duas dessas soluções (x_1, y_1) e (x_2, y_2) de modo que $|x_1| \neq |x_2|$, e com

$$x_1 \equiv x_2 \pmod{m} \ \text{ e } \ y_1 \equiv y_2 \pmod{m}. \tag{2.12}$$

temos que

$$(x_1 + y_1\sqrt{d}) \cdot (x_2 - y_2\sqrt{d}) = (x_1x_2 - dy_1y_2) + (x_2y_1 - x_1y_2)\sqrt{d}. \tag{2.13}$$

Agora de 2.12, podemos ter

$$x_2 - x_1 = m\lambda_1 \text{ e } y_2 - y_1 = m\lambda_2, \quad \lambda_1, \lambda_2 \in \mathbb{Z}.$$

E como (x_1, y_1) é solução de 2.11, $m = x_1^2 - dy_1^2$, assim

$$\begin{aligned} x_1x_2 - dy_1y_2 &= x_1x_2 + x_1^2 - x_1^2 - dy_1^2 + dy_1^2 - dy_1y_2 \\ &= x_1(x_2 - x_1) + (x_2^2 - dy_1^2) + dy_1(y_1 - y_2) \\ &= x_1m\lambda_1 + m + dy_1m\lambda_1 \\ &= (x_1\lambda_1 + 1 + dy_1\lambda_1)m \\ &= k_1m \end{aligned}$$

e

$$\begin{aligned} x_2y_1 - x_1y_2 &= x_2y_1 - x_1y_1 + x_1y_1 - x_2y_2 \\ &= (x_2 - x_1)y_1 + (y_1 - y_2)x_1 \\ &= my_1\lambda_1 - mx_1\lambda_2 \\ &= (y_1\lambda_1 - x_1\lambda_2)m \\ &= k_2m. \end{aligned}$$

Onde, $k_1 = x_1\lambda_1 + 1 + dy_1\lambda_1$ e $k_2 = y_1\lambda_1 - x_1\lambda_2$. Desse modo

$$x_1x_2 - dy_1y_2 = k_1m \text{ e } x_2y_1 - x_1y_2 = k_2m. \tag{2.14}$$

Portanto de 2.13,

$$(x_1 + y_1\sqrt{d}) \cdot (x_2 - y_2\sqrt{d}) = m(k_1 + k_2\sqrt{d}). \tag{2.15}$$

Tomando o conjugado dos dois lados de 2.15, e usando 2.11, temos

$$(x_1 - y_1\sqrt{d}) \cdot (x_2 + y_2\sqrt{d}) = m(k_1 - k_2\sqrt{d}). \tag{2.16}$$

Multiplicando membro a membro 2.15 e 2.16

$$(x_1^2 - dy_1^2) \cdot (x_2^2 - dy_2^2) = m^2(k_1^2 - dk_2^2).$$

Como $m = x_1^2 - dy_1^2 = x_2^2 - dy_2^2$, segue que

$$m^2 = m^2(k_1^2 - dk_2^2).$$

Isto é

$$k_1^2 - dk_2^2 = 1.$$

Portanto (k_1, k_2) é solução de 2.11. Assim, a demonstração estará concluída se mostrarmos que k_1, k_2 não nulos. De fato, se $k_1 = 0$, então $-dk_2^2 = 1$, o que é um absurdo. Se $k_2 = 0$, teríamos $k_1 \pm 1$. logo de 2.13, viria

$$x_1x_2 - dy_1y_2 = \pm m \text{ e } x_2y_1 - x_1y_2 = 0.$$

Assim de 2.13, $(x_1 + y_1\sqrt{d}) \cdot (x_2 - y_2\sqrt{d}) = \pm m = \pm(x_2^2 - dy_2^2)$, por isso

$$(x_1 + y_1\sqrt{d}) = \pm(x_2 + y_2\sqrt{d}),$$

ou seja, $|x_1| = |x_2|$, o que contraria nossa hipótese sobre as soluções (x_1, y_1) e (x_2, y_2). E isso mostra que (k_1, k_2) é uma solução não nula de $x^2 - dy^2 = 1$. ■

Definição 2.6. *Chama-se de* ***solução fundamental*** *ou* ***solução base*** *da equação* $x^2 - dy^2 = 1$, *a solução positiva* (x_1, y_1) *tal que,* $x_1 + y_1\sqrt{d}$ *é o menor possível.*

Teorema 2.4. *Seja* (x_1, y_1) *uma solução da equação* $x^2 - dy^2 = 1$ *então, cada par de inteiros* x_n *e* y_n *definidos por*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

para cada $n \in \mathbb{N}$, e também uma solução da equação. Em particular essa equação admite infinitas soluções positivas.

Demonstração: De acordo com 2.10, existem x_n e y_n tais que

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

Por 2.12,

$$x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n.$$

Assim como $x_1^2 - dy_1^2 = 1$,

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + y_n\sqrt{d}) \cdot (x_n - y_n\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n \cdot (x_1 - y_1\sqrt{d})^n \\ &= (x_1^2 - dy_1^2)^n \\ &= 1^n \\ &= 1. \end{aligned}$$

Por fim, se (x_1, y_1) é solução positiva de $x^2 - dy^2 = 1$, então (x_n, y_n) obtida pela fórmula anterior, também o é. ■

O teorema anterior, garante que a equação 2.6, admite infinitas soluções positivas. No entanto, não as caracteriza. O próximo teorema nos mostra como determinar todas as soluções positivas de $x^2 - dy^2 = 1$. Antes disso, vamos fazer uso do seguinte lema:

Lema 2.5. *Seja $\theta > 1$ um número real. Então, para cada número real $x > 1$, $x \neq \theta$, existe $n \in \mathbb{N}$ tal que*

$$\theta^n < x < \theta^{n+1}.$$

Esse resultado é da análise matemática. Para mais detalhes, o leitor pode ver [11].

Teorema 2.5. *Seja (x_1, y_1) a solução fundamental de $x^2 - dy^2 = 1$. Então, cada solução positiva desta equação é dada por x_n e y_n, onde estes inteiros são dados por*

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n,$$

em que $n \in \mathbb{N}$.

Demonstração: Pelo Teorema 2.4, os inteiros x_n e y_n dados por

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$$

é uma solução de $x^2 - dy^2 = 1$. Por contradição, vamos supor que exista uma solução (a, b) que não seja obtida por $(x_1 + y_1\sqrt{d})^n$. Como $x_1 + y_1\sqrt{d} > 1$, pois $x_1 > 0$ e $y_1 > 0$, então as potências positivas de $x_1 + y_1\sqrt{d}$ tornam-se estritamente grandes, isto é,

$$\lim_{n\to\infty} (x_1 + y_1\sqrt{d})^n = \infty$$

como $a + b\sqrt{d} > 1$, então pelo Lema anterior, existe $n \in \mathbb{N}$, tal que

$$(x_1 + y_1\sqrt{d})^n < a + b\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1},$$

ou melhor

$$(x_n + y_n\sqrt{d}) < a + b\sqrt{d} < (x_n + y_n\sqrt{d})(x_1 + y_1\sqrt{d}).$$

Multiplique esta desigualdade por $x_n - y_n\sqrt{d}$, daí obtemos

$$1 < (a + b\sqrt{d})(x_n - y_n\sqrt{d}) < x_1 + y_1\sqrt{d} \tag{2.17}$$

considere $\alpha + \beta\sqrt{d} = (a + b\sqrt{d})(x_n - y_n\sqrt{d})$, com $\alpha, \beta \in \mathbb{Z}$. Logo,

$$\alpha = ax_n - bdy_n \text{ e } \beta = bx_n - ay_n,$$

de modo que

$$\begin{aligned} \alpha^2 - d\beta^2 &= (\alpha + \beta\sqrt{d})(\alpha - \beta\sqrt{d}) \\ &= (a^2 - db^2)(x_n^2 - dy_n^2) \\ &= 1 \cdot 1 \\ &= 1. \end{aligned}$$

Assim, (α, β) é uma solução de $x^2 - dy^2 = 1$. Além disso, por 2.17,

$$1 < \alpha + \beta\sqrt{d} < x_1 + y_1\sqrt{d}.$$

Agora, como $1 < \alpha + \beta\sqrt{d}$ e $(\alpha + \beta\sqrt{d})(\alpha - \beta\sqrt{d}) = 1$, temos

$$0 < \alpha - \beta\sqrt{d} < 1.$$

Daí,

$$\begin{aligned} 2\alpha &= (\alpha + \beta\sqrt{d}) + (\alpha - \beta\sqrt{d}) > 1 + 0 = 1, \\ 2\beta\sqrt{d} &= (\alpha + \beta\sqrt{d}) - (\alpha - \beta\sqrt{d}) > 1 - 1 = 0. \end{aligned}$$

Logo $\alpha, \beta > 0$. Portanto, (α, β) é uma solução positiva tal que $\alpha + \beta\sqrt{d} < x_1 + y_1\sqrt{d}$, o que contraria o fato de (x_1, y_1) ser solução fundamental. ■

Exemplo 2.2. *Determinar as soluções positivas da equação* $x^2 - 7y^2 = 1$.

Solução: Através de substituições sucessivas de $y = 1, 2, \cdots$ na expressão $7y^2 + 1$ podemos

obter um quadrado perfeito. De fato,

$$\begin{aligned} y = 1 &\Rightarrow 1 + 7y^2 = 8, \\ y = 2 &\Rightarrow 1 + 7y^2 = 29, \\ y = 3 &\Rightarrow 1 + 7y^2 = 64 = 8^2. \end{aligned}$$

Logo $x_1 = 8$ e $y_1 = 3$, pelo Teorema 2.4, as soluções da equação são os pares (x_n, y_n), tal que

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n = (8 + 3\sqrt{7})^n, \quad n \in \mathbb{N}.$$

Assim, para $k \in \mathbb{N}$ tem-se

$$\begin{aligned} n = 2 &\Rightarrow (8 + 3\sqrt{7})^2 = 127 + 48\sqrt{7}, \\ n = 3 &\Rightarrow (8 + 3\sqrt{7})^3 = 2024 + 765\sqrt{7}, \\ &\vdots \\ n = k &\Rightarrow (8 + 3\sqrt{7})^k = x_k + y_k\sqrt{7}, \\ &\vdots \end{aligned}$$

Capítulo 3

Aplicações

Este capítulo tem o objetivo de mostrar algumas aplicações das equações diofantinas tratadas no capítulo anterior. As aplicações mais elementares são as que envolvem as equações diofantinas lineares, onde estão relacionadas com situações problema do nosso dia a dia.

3.1 Aplicações das Equações Lineares

Diversos problemas do nosso dia a dia podem ser respondidos usando o auxílio das equações diofantinas lineares, onde o problema é modelado até chegar em uma equação do tipo $ax + by = c$. No Exemplo 3.1, que segue, modelamos o problema e recaímos numa equação dessa forma, que para resolver esse problema, basta encontrar as soluções inteiras da equação.

Exemplo 3.1 (Aplicação das equações diofantinas lineares)**.** *Um fazendeiro deseja comprar porcos e ovelhas para sua fazenda. Ele tem exatamente R$* $17.770,00$ *para gastar nessa compra. De quantas maneiras o fazendeiro pode comprar os animais gastando exatamente o que tem, tendo em vista que os preços dos animais são R$ 310,00 e R$ 210, 00 por cabeça de porco e ovelha respetivamente?*

Solução: Considere x e y o número de cabeças de porcos e ovelhas, respetivamente. Agora, podemos resumir nosso problema a equação diofantina linear

$$310x + 210y = 17.770, \tag{3.1}$$

note que a equação 3.1 é equivalente a essa outra equação $31x+21y = 1.777$ como $(31, 21) = 1$ e $1 \mid 1777$ a equação admite solução. Pelo Teorema 1.5 , existem inteiros m e n, tais que

$$1 = 31m + 21n.$$

Daí, usando o algoritmo de Euclides podemos encontra-los

$$\begin{aligned} 31 &= 21 \cdot 1 + 10 \\ 21 &= 10 \cdot 2 + 1 \\ 10 &= 10 \cdot 1 + 0. \end{aligned}$$

Assim,

$$\begin{aligned} 1 &= 21 - 10 \cdot 2 \\ &= 21 - (31 - 21) \cdot 2 \\ &= 21 - 31 \cdot 2 + 21 \cdot 2 \\ &= 31 \cdot (-2) + 21 \cdot 3. \end{aligned}$$

Logo $m = -2$ e $n = 3$. Multiplicando toda a equação por 1777, tem-se

$$1777 = 31 \cdot (-3554) + 21 \cdot 5331.$$

Agora podemos ver que o par de inteiros $(-3554, 5331)$ é uma solução particular para equação 3.1, portanto a solução geral é dada por

$$x = -3554 + 21k \text{ e } y = 5331 - 31k.$$

Mas, a natureza desse problema nos obriga ter x e y inteiros não negativos, isto é, $x = -3554 + 21k \geqslant 0$ e $y = 5331 - 31k \geqslant 0$, fazendo os cálculos temos, $170 \leqslant k \leqslant 171$, ou seja

$$k \in \{170, 171\}.$$

Portanto o fazendeiro terá exatamente duas formas de efetuar a compra gastando todo seu dinheiro. São elas

$$\begin{aligned} k &= 170 \Rightarrow x = 16 \text{ e } y = 61; \\ k &= 171 \Rightarrow x = 37 \text{ e } y = 30. \end{aligned}$$

3.2 Aplicação da Equação Pitagórica

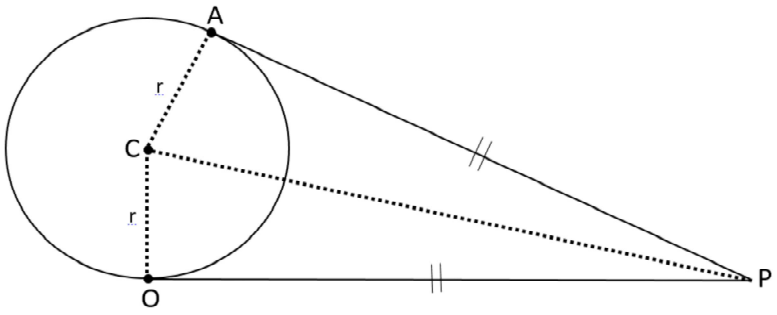
Vamos considerar nesta seção uma aplicação sobre a teoria da *equação pitagórica,* antes disso, faremos uso do seguinte resultado exposto em forma de uma proposição.

Proposição 3.1. *Se dois lados de um ângulo de vértice P são tangentes a um círculo nos pontos A e O, então $PA = PO$.*

Demonstração: Seja C o centro do círculo. Trace PC e compare os triângulos PCO e PCA. Como os ângulos PÂC= PÔC= 90^{o} os triângulos são retângulos. Como $AC = OC$ (por se tratarem do raio) e PC é comum a ambos os triângulos, então esses triângulos são semelhantes. Daí, $PA = PO$.

■

Figura 3.1: Lados de um ângulo de vértice P tangentes a um círculo nos pontos A e O.



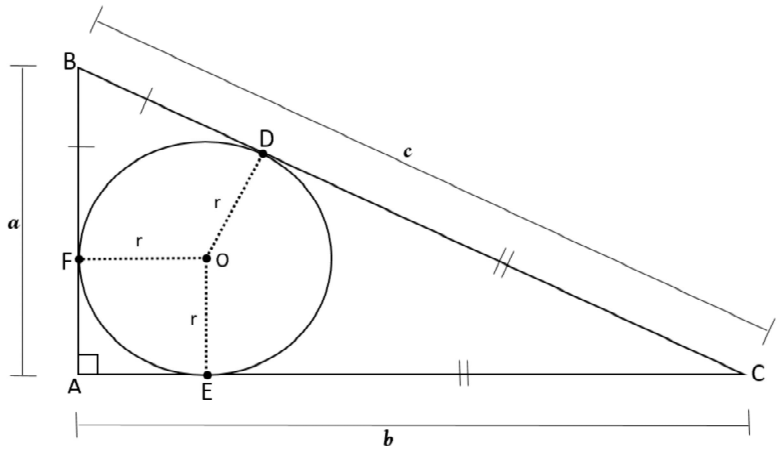
Definição 3.1. *Uma circunferência está inscrita em um triângulo se todos os lados do triângulo estão tangentes a circunferência. Quando tal coisa ocorre diz-se que o triângulo circunscreve a circunferência.*

Na Definição 3.1 podemos tirar a exigência de ser um triângulo e falar que é um polígono, como é dito em [2].

Exemplo 3.2 (Aplicação da equação pitagórica)**.** *Considere um triângulo pitagórico ABC e uma circunferência de centro O inscrita nesse triângulo. Então o raio dessa circunferência é sempre um número natural.*

Solução: Sejam a, b e c as medidas de um triângulo pitagórico ABC e r a medida do raio da circunferência inscrita. Pela Proposição 3.1, se D, E e F são os pontos da circunferência tangentes aos lados do triângulo, então $CD = CE$ e $BD = BF$, como mostra a Figura 3.2.

Figura 3.2: Triângulo pitagórico com uma circunferência inscrita.



Note que, $CD = CE = (b - r)$ e $BF = BD = (a - r)$. Daí segue que

$$\begin{aligned} c &= DC + DB \\ &= (b - r) + (a - r) \\ &= b + a - 2r. \end{aligned}$$

Logo

$$r = \frac{b + a - c}{2}. \tag{3.2}$$

Mas, $a^2 + b^2 = c^2$, pois o triângulo em questão é pitagórico, assim (a, b, c) é um terno pitagórico, e portanto, para algum $k \in \mathbb{N}$

$$a = ka_1;\ b = kb_1;\ c = kc_1$$

para (a_1, b_1, c_1) um terno pitagórico primitivo. Assim,

$$a = 2kmn,\ b = k(m^2 - n^2);\ c = k(m^2 + n^2) \tag{3.3}$$

com $(m, n) = 1,\ m > n > 0$ e $m + n$ ímpar.

Agora, substituindo os valores de a, b e c em 3.3 na Equação 3.2, tem-se

$$\begin{aligned} r &= \frac{k(m^2 - n^2) + 2kmn - k(m^2 + n^2)}{2} \\ &= \frac{km^2 - kn^2 + 2kmn - km^2 - kn^2}{2} \\ &= \frac{-2kn^2 + 2kmn}{2} \\ &= \frac{2nk(m - n)}{2} \\ &= nk(m - n) \\ &= nkv. \end{aligned}$$

Onde $n, k, v \in \mathbb{N}$ e $v = m - n$. Daí, concluímos que r é um número natural.

3.3 Aplicação da Equação de Pell

Nesta Seção será apresentado um argumento de Størmer,[1] uma bela aplicação da teoria da equação de Pell. Começaremos com a seguinte definição

[1] Carl Størmer (1874 - 1957), matemático Norueguês.

Definição 3.2. *Considere o conjunto* $S = \{p_1, p_2, \cdots, p_r\}$ *formado por* r *números primos distintos. Chama-se* ***S-número,*** *todos os inteiros* $p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ *com* $a_i \in \mathbb{N}_0 = \{0, 1, \cdots\}$ *constituídos dos primos em* S.

Nas condições da Definição 3.2, os $\{2, 3\}$-números menores que 60 são:

$$1, 2, 3, 4, 6, 8, 9, 12, 16, 17, 24, 27, 32, 36, 48, 54.$$

Para dizer que os S-números x e y são separados pela lacuna de espaço um, escrevemos a seguinte equação

$$x - y = 1. \tag{3.4}$$

Se x e y são $\{2, 3\}$-números, então a equação 3.4 diz que $2^a 3^b - 2^c 3^d = 1$.

3.3.1 Teorema de Størmer

Carl Størmer (1874 - 1957), provou que a equação 3.4, não tem infinitas soluções, ou em outras palavras, a equação tem *finitas* soluções x, y em S-números. O último teorema desse capítulo prova essa afirmação. No entanto, faremos uso do Teorema 3.1 e da seguinte definição:

Definição 3.3. *Para* $d, n \in \mathbb{N}$ *dizemos que* n *é um* **d-número** *se cada fator primo de* n *divide* d, *isto é,* n *é um S-número para* S *o conjunto de divisores primos de* d.

O teorema que segue, sem uma demonstração, afirma que cada equação de Pell tem no máximo uma solução fundamental em que y é um d-número. Na demonstração desse resultado usa-se o Teorema 2.4. Para mais detalhes [5].

Teorema 3.1 (Størmer, 1897)**.** *Cada equação*

$$x^2 - dy^2 = 1,\ d \in \mathbb{N}\ e\ \sqrt{d} \notin \mathbb{N}$$

tem no máximo uma solução $x, y \in \mathbb{N}$ *onde* y *é um d-número, isto é, todo fator primo de* y *divide* d.

Se essa tal solução existe, ela será igual a solução fundamental da equação $x^2 - dy^2 = 1$. Veja a referência [5].

Teorema 3.2 (Teorema de Størmer)**.** *Seja $S = \{p_1, p_2, \cdots, p_r\}$ sendo r primos distintos. Cada uma das duas equações*

$$x - y = 1 \quad e \quad x - y = 2$$

tem no máximo 3^r soluções em S-números x, y.

Demonstração: Esse teorema segue do Teorema 3.1. Se y e $y+1$ são ambos S-números, então eles são separados por uma lacuna de espaço um. Além disso, $2 \in S$ e $4y \cdot (y+1) = (2y+1)^2 - 1$, é um S-número. De forma parecida, se y e $y+2$ são ambos S-números, deixam uma lacuna de espaço dois, e tem-se que, $y(y+2) = (y+1)^2 - 1$ é um S-número. Essa ideia é suficiente para mostrar que no máximo 3^r S-números são da forma $a^2 - 1$. Note que todas as soluções (x, y) das equações, $x - y = 1$ e $x - y = 2$, produzem S-números da forma $a^2 - 1$, para $a \in \mathbb{N}$. Então, é suficiente mostrar que existem no máximo 3^r S-números da forma $a^2 - 1$. Seja $a^2 - 1 = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ onde $a \in \mathbb{N}$ e $a_i \in \mathbb{N}_0$. Agora, defina $b_i \in \mathbb{N}_0$ por

$$b_i = \begin{cases} a_i - 1, & \text{para } a_i \text{ impar;} \\ 0, & \text{para } a_i = 0 \text{ ou } 2; \\ a_i - 2, & \text{para } a_i \geq 4 \text{ e } a_i \text{ par.} \end{cases}$$

Considere também $d = p_1^{a_1 - b_1} p_2^{a_2 - b_2} \cdots p_r^{a_r - b_r}$ e $b = p_1^{\frac{b_1}{2}} p_2^{\frac{b_2}{2}} \cdots p_r^{\frac{b_r}{2}}$. Então

$$a^2 - db^2 = 1,$$

onde b é um d-número. Daí, nós temos no máximo 3^r escolhas para d, pois, perceba que $d = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_r^{\varepsilon_r}$, com $\varepsilon_i \in \{0, 1, 2\}$. Assim, são 3^r equações $x^2 - dy^2 = 1$, e cada uma delas, pelo Teorema 3.1, tem no máximo uma solução positiva (a, b) com b sendo um d-número. Portanto, conclui-se que existem no máximo 3^r S-números da forma $a^2 - 1$, o que prova o teorema.

■

Considerações Finais

Neste estudo, ficou clara a complexidade e a extensão do assunto, uma vez que não foram estudados todos os tipos de equações. No entanto, o objetivo de estudar algumas equações diofantinas e mostrar suas aplicações, foi, sem dúvida, alcançado. Portanto, depois de ler e analisar todo o texto, o leitor terá condições de saber se uma determinada equação diofantina, tratada nessa monografia, tem infinitas soluções sem a necessidade de resolvê-la.

Referências Bibliográficas

[1] ABRAMO, H. *Iniciação à Aritmética.* Sociedade Brasileira da Matemática. IMPA, Rio de Janeiro, 2009.

[2] BARBOSA, J. L. M. *Geometria Euclidiana Plana.* Sociedade Brasileira da Matemática, Rio de Janeiro, 1985.

[3] BOYER.C.B., MERZBACH.U.C. *História da Matemática.* 3 ed. Blucher, São Paulo, 2015.

[4] FREITAS, C. W. A. *Equações Diofantinas.* Dissertação (Mestrado em Matemática), Universidade Federal do Ceará, Fortaleza, 2015.

[5] KLAZAR, M. *Størmer's solutions of the unit equations* $x - y = 1$. Disponível em: <`http://kam.mff.cuni.cz/~klazar/stormer.pdf` >. Acesso em: 21 out. 2017.

[6] LANDAU, E. *Teoria elementar dos números.* Coleção Clássicos da Matemática. Ciência Moderna, Rio de Janeiro, 2014.

[7] MIRANDA, M. C. *Heurísticos e equações diofantinas.* Artigo, Universidade de matemática - FAMAT, Uberlândia, 2007.

[8] POMMER, W. M. *Equações Diofantinas Lineares: Um Desafio Motivador para Alunos do Ensino Médio.* Dissertação (Mestrado em Matemática), PUC - SP. São Paulo, 2008.

[9] SANTOS, J.P.O. *Introdução á teoria dos números.* 3 ed. CMU, IMPA, Rio de Janeiro, 2009.

[10] VIEIRA, V.L. *Álgebra Abstrata para Licenciatura .* 2 ed. Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.

[11] VIEIRA, V.L. *Um Curso Básico em Teoria dos Números.* Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.