UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE ARAGUAÍNA
CURSO DE LICENCIATURA EM MATEMÁTICA

JOSÉ EURIVAN RODRIGUES DOS SANTOS JÚNIOR

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS ELEMENTARES

ARAGUAÍNA
2017

JOSÉ EURIVAN RODRIGUES DOS SANTOS JÚNIOR

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS ELEMENTARES

Monografia apresentada ao curso de Licenciatura Plena em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciado em Matemática.
Orientador: Profª. Msc. Renata Alves da Silva.

ARAGUAÍNA
2017

JOSÉ EURIVAN RODRIGUES DOS SANTOS JÚNIOR

INTRODUÇÃO ÀS EQUAÇÕES DIOFANTINAS ELEMENTARES

Monografia apresentada ao curso de Licenciatura Plena em Matemática da Universidade Federal do Tocantins, como requisito parcial para a obtenção de título de Licenciado em Matemática.
Orientador: Profª. Msc. Renata Alves da Silva.

Aprovada em: / / .

BANCA EXAMINADORA

_____
Profª. Msc. Renata Alves da Silva (orientadora)

_____
Prof. Dr. Alvaro Julio Yucra Hancco

_____
Prof. Dr. José Carlos de Oliveira Junior

AGRADECIMENTOS

A Deus, que nos concedeu forças que permitiram a conclusão deste trabalho.

Aos meus pais José Eurivan e Aldenora pelo apoio, incentivo e dedicação que contribuíram de forma significativa na busca deste sonho, cursar uma graduação.

À minha esposa Leurilene pelo apoio, incentivo e compreensão.

À Fundação Universidade Federal do Tocantins por nos oferecer condições de podermos cursar uma graduação de qualidade.

Aos meus colegas da graduação que sempre estiveram torcendo pela concretização deste trabalho.

A minha orientadora Profª. Msc. Renata Alves da Silva, pela cordial atenção a qual tem dedicada na execução deste projeto.

A profª. Msc. Fernanda Vital de Paula por ter me oportunizado trabahar como monitor do Programa de Iniciação Científica da OBEMP – PIC.

Aos professores Dr. José Carlos e Dr. Sinval de Olivera pela dedicação a causa dos discentes da nossa instituição.

Ao prof. Msc. Freud Romão pelos momentos de reflexão no que diz respeito a prática docente.

Por fim, aos meus irmãos Aline, Alan, Alice e Carlos Henrique por compartilharem deste sonho.

Os padrões criados pelo matemático, como os do pintor ou do poeta, devem ser belos; as ideias, como as cores ou as palavras, devem se encaixar de um modo harmonioso. A beleza é o primeiro desafio: não existe lugar permanente no mundo para a matemática feia.

G. H. Hardy

RESUMO

Uma equação diofantina é uma equação polinomial para a qual procuramos soluções inteiras ou racionais. É mister destacar que neste trabalho abordamos estas equações somente no universo dos números inteiros. Neste trabalho, tratamos das equações diofantinas lineares a n incógnitas e suas soluções, estudamos também várias outras equações diofantinas elementares não lineares, começando com $x^2 + y^2 = z^2$ (ternas pitagóricas), passando por vários outros polinômios particulares e concluindo com um caso particular da equação de Pell, a saber, $x^2 - 2y^2 = 1$.

Palavras-chaves: Teoria dos Números. Números Inteiros. Máximo Divisor Comum. Teorema de Pitágoras.

ABSTRACT

A Diophantine equation is a polynomial equation to which we search integer or rational solutions, it is important to highlight in this project we only approach these equations in the universe of integer number. In this paper we talk from linear Diophantine equations to n unknowns and its solutions, along with the study of other elementary non-linear Diaphontine equations, starting with $x^2 + y^2 = z^2$ (Pythagorean triples), then looking into other specific polynomials and concluding with a special case of Pell's equation $x^2 - 2y^2 = 1$.

Keywords: Number theory. Integer numbers. Maximum common divisor. Pythagoras's Theorem.

Sumário

Capítulo 1

Introdução

A busca por soluções inteiras de equações permeiam a matemática há milênios, e até hoje continua sendo um problema de grande interesse para os matemáticos.

Neste trabalho, direcionaremos nossa atenção às equações diofantinas lineares e não lineares, neste último caso, abordaremos as ternas pitagóricas e um caso particular da equação de Pell. "Os trios pitagóricos são combinações de três números inteiros que se ajustam perfeitamente à equação de Pitágoras: $x^2 + y^2 = z^2$ [10]". Devido à Aritmética[1], hoje são chamadas equações diofantinas as equações polinomiais (não importa o número de incógnitas) com coeficientes inteiros, sempre que seu estudo seja feito tomando como universo das variáveis o conjunto dos números inteiros ou dos racionais. Apesar de Diofanto só ter trabalhado com alguns poucos casos particulares dessas equações e seu universo numérico ter sido o dos números racionais estritamente positivos [2], neste trabalho, nos empenharemos em explorar estas equações no universo dos números inteiros.

Para os objetivos que este trabalho se destina, faz-se necessária uma apresentação sistemática dos pré-requisitos para compreensão das soluções destas equações, ou melhor, das ferramentas matemáticas que fundamentam tais técnicas de resolução. Faremos uma breve apresentação da teoria elementar dos números, tais como os conceitos de divisibilidade, o algoritmo da divisão, máximo divisor comum, fatoração e congruências. Os teoremas, corolários, lemas e proposições quando necessário serão demonstrados com todo o rigor matemático, mas buscaremos fazê-lo da forma mais acessível possível aos leitores.

A motivação para este trabalho surgiu a partir de experiências como monitor do Programa de Iniciação Científica da OBMEP – PIC OBMEP, em 2013. Neste programa, tive o primeiro contato com as equações diofantinas lineares a duas incógnitas e com problemas de aritmética que usam recursos simples para solução de problemas aparentemente difíceis.

Nosso trabalho está delineado conforme segue.

[1] *Aritmética* é considerado o primeiro manual de álgebra que usa símbolos para indicar incógnitas e potências, e resolve as equações indeterminadas, hoje denominadas equações diofantinas.

No capítulo 2, enunciamos e demonstramos alguns resultados da Teoria Elementar dos Números, como a divisibilidade, máximo divisor comum, algoritmo de Euclides, teorema de Bèzout, números primos e congruência e outros temas fulcrais para compreensão do tema em tela.

No Capítulo 3, buscamos apresentar a solução geral da equação diofantina linear a n incógnitas, tomando como referência a técnica apresentada por [1] e [11].

No capítulo 4, apresentamos um breve apanhado histórico acerca de Pitágoras e do famoso teorema que leva seu nome, o teorema de Pitágoras. Logo em seguida, passamos a discutir acerca de algumas equações diofantinas elementares não lineares, como as ternas pitagóricas e a equação de Pell. Discutiremos também acerca da solubilidade de alguns exemplos destas equações.

Capítulo 2

Fundamentos

O presente capítulo visa apresentar informações e resultados que possibilitarão alcançar nosso objetivo maior, a solução de *Equações Diofantinas Elementares*, em particular, as lineares e as ternas Pitagóricas. Apresentaremos, inicialmente, alguns resultados preliminares, sem demonstrarmos. Logo em seguida, os elementos teóricos e, sempre que acharmos pertinente, apresentaremos exemplos, visando à criação de possibilidade de entendimento para o leitor.

2.1 Preliminares

2.1.1 Princípio de Indução Finita (PIF)

Seja $P(n)$ uma propriedade do número natural n, por exemplo:

- n pode ser fatorado em um produto de números primos;
- $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$;
- $1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$;
- a equação $2x + 3y = n$ adminte solução com x e y inteiros positivos.

Uma maneira de porvar que $P(n)$ é verdadeira para todo natural $n \geq n_0$ é utilizar o chamado *Princípio da Indução Finita* (PIF), que é um dos axiomas que caracterizam o conjunto dos números naturais. O PIF consiste em verificar duas coisas:

1. (Base da Indução) $P(n_0)$ é verdadeira e

2. (Passo Indutivo) Se $P(n)$ é verdadeira para algum número natural $n \geq n_0$, então $P(n+1)$ também é verdadeira.

Vejamos alguns exemplos de demonstrações na qual utilizamos este princípio.

Exemplo 2.1. *Para cada $n \in \mathbb{N}$, a soma dos n primeiros quadrados perfeitos é igual a*

$$\frac{1}{6}n(n+1)(2n+1).$$

Resolução: Como o k-ésimo quadrado perfeito é o número k^2, a propriedade $P(n)$ é, neste caso,

$$P(n) : \sum_{j=1}^{n} j^2 = \frac{1}{6}n(n+1)(2n+1).$$

Agora, temos que verificar que:

i. $P(1)$ é verdadeira.

ii. $P(k)$ verdadeira $\Rightarrow P(k+1)$ verdadeira.

Verificar (i) é imediato. De fato, veja que: $1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$. Agora, para verificar (ii) supomos que $P(k)$ é verdadeira, isto é, que a igualdade valha para $n = k$ (hipótese de indução):

$$\sum_{j=1}^{k} j^2 = \frac{1}{6}k(k+1)(2k+1),$$

e queremos deduzir que $P(k+1)$ também é verdadeira, isto é, que

$$\sum_{j=1}^{k+1} j^2 = \frac{1}{6}(k+1)[(k+1)+1][2(k+1)+1].$$

Mas como estamos supondo a validez de $P(k)$, segue que

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 &= \sum_{j=1}^{k} j^2 + (k+1)^2 \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\
&= \frac{1}{6}(k+1)[k(2k+1) + 6(k+1)] \\
&= \frac{1}{6}(k+1)(k+2)(2k+3).
\end{aligned}$$

Logo,

$$\sum_{j=1}^{k+1} j^2 = \frac{1}{6}(k+1)[(k+1)+1][2(k+1)+1].$$

Portanto, por indução $P(n)$ é verdadeira para todo $n \in \mathbb{N}$. □

Observação 2.2. *Há um resultado implícito no PIF chamado* ***Princípio da Boa Ordenação (PBO)*** *dos números naturais que revela-se como uma ferramenta poderosa na resolução de problemas, bem como numa série de demonstrações. Vejamos o enunciado deste princípio: Todo conjunto não-vazio de inteiros positivos contém um elemento mínimo.*

2.1.2 Números Binomiais

Definição 2.3. *Dado um inteiro não negativo n, o **fatorial** de n é o número*

$$n! = \begin{cases} 1, & \text{se } n = 0 \\ \prod_{j=1}^{n} j, & \text{se } n \geq 1. \end{cases}$$

Definição 2.4. *Dados inteiros n e k, com $0 \leq k \leq n$, definimos o **número binomial** $\binom{n}{k}$ por*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

Para todo $n \in \mathbb{N}$, tem-se

$$\binom{n}{0} = 1, \binom{n}{1} = n, \binom{n}{2} = \frac{n(n-1)}{2}.$$

Exemplo 2.5. *Demonstre que, para quaisquer naturais $n \geq m$, o coeficiente binomial*

$$\binom{n}{m} = \frac{n!}{m!(n-m)!},$$

é inteiro.

Resolução: Procederemos por indução sobre a soma $m + n$. Se $m + n = 0$, então $m = n = 0$ e $\binom{0}{0} = 1$ é inteiro (base de indução). Para o passo indutivo, observe primeiramente que, para $0 < m < n$, temos a seguinte identidade de binomiais

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}.$$

De fato, vejamos:

$$\begin{aligned} \binom{n-1}{m} + \binom{n-1}{m-1} &= \frac{(n-1)!}{m!(n-m-1)!} + \frac{(n-1)!}{(m-1)!(n-m)!} \\ &= \frac{(n-1)!(n-m)}{m!(n-m)(n-m-1)!} + \frac{m(n-1)!}{m(m-1)!(n-m)!} \\ &= \frac{(n-m)(n-1)!}{m!(n-m)!} + \frac{m(n-1)!}{m!(n-m)!} \\ &= \frac{((n-m)+m)(n-1)!}{m!(n-m)!} \\ &= \frac{n!}{m!(n-m)!} = \binom{n}{m}. \end{aligned}$$

Agora, suponhamos que $\binom{n}{m}$ é inteiro para $m + n \leq k$ (hipótese de indução). Note que podemos supor também que $0 < m < n$, já que se $m = n$ ou $m = 0$ temos $\binom{n}{m} = 1$ e o resultado segue trivialmente. Assim, se $m + n = k + 1$, temos que $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ é inteiro também, pois cada parcela da direita é inteiro pela hipótese de indução. □

Teorema 2.6. *(*Binômio de Newton*) Para $n \in \mathbb{N}$, temos*

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j.$$

Demonstração: Encontra-se em [7], página 149. □

2.2 Divisibilidade

Definição 2.7. *Se a e b são inteiros, dizemos que a divide b, denotamos por $a \mid b$, se existir um inteiro c tal que $b = ac$.*

Se a não divide b escrevemos $a \nmid b$.
Assim, por exemplo,

$$1 \mid 8, 2 \mid 8, 4 \mid 8, 8 \mid 8, -8 \mid 8, -4 \mid 8, -2 \mid 8, -1 \mid 8.$$

Isto significa que, se $d \notin \{-8, -4, -2, -1, 1, 2, 4, 8\}$, então $d \nmid 8$.

Proposição 2.8. *Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$, por hipótese, existem inteiros k_1 e k_2 com $b = k_1 a$ e $c = k_2 b$. Daí, substituindo b em $c = k_2 b$, tem-se $c = k_2(k_1 a) = (k_1 k_2)a$, o que implica $a \mid c$. □

Exemplo 2.9. *Como $3 \mid 12$ e $12 \mid 48$, então $3 \mid 48$.*

Resolução: De fato, $12 = 4 \times 3$ e $48 = 4 \times 12$, de sorte que, $48 = 4 \times (4 \times 3) = (4 \times 4) \times 3 = 16 \times 3$ e, portanto, $3 \mid 48$. □

Proposição 2.10. *Se a, b, c, m e n são inteiros, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração: De fato, se $c \mid a$ e $c \mid b$, segue imediatamente da definição que existem inteiros k_1 e k_2 com $a = k_1 c$ e $b = k_2 c$. Assim, $ma + nb = m(k_1 c) + n(k_2 c) = (mk_1)c + (nk_2)c = (mk_1 + nk_2)c$, onde $mk_1 + nk_2 \in \mathbb{Z}$. Logo, $c \mid (ma + nb)$. □

Teorema 2.11. *Temos as seguintes propriedades válidas para $a, d, n \in \mathbb{Z}$:*
(i) $n \mid n$;
(ii) $d \mid n \Rightarrow ad \mid an$;
(iii) $ad \mid an$ *e* $a \neq 0 \Rightarrow d \mid n$;
(iv) $1 \mid n$;
(v) $n \mid 0$;
(vi) $d \mid n$ *e* $n \neq 0 \Rightarrow |d| \leq |n|$;
(vii) $d \mid n$ *e* $n \mid d \Rightarrow |d| = |n|$;
(viii) $d \mid n$ *e* $d \neq 0 \Rightarrow (n/d) \mid n$.

Demonstração: (i) Observe que $n = 1 \cdot n$. Então, segue da definição que $n \mid n$. (ii) Se $d|n$ então existe k inteiro de modo que $n = kd$. Agora, multiplicando por a a igualdade $n = kd$, temos $an = a(kd) = k(ad)$ e, portanto, $ad|an$. (iii) Se $ad|an$, então $an = k(ad) = a(kd)$ para algum inteiro k. Por outro lado, sabemos que, se $a \neq 0$, então $(1/a).a = 1$.

Assim, multiplicando $an = a(kd)$ por $1/a$ teremos $(1/a)(an) = (1/a)[a(kd)] \Leftrightarrow [(1/a)a]n = [(1/a)a](kd) \Leftrightarrow n = kd$ e, portanto, $d|n$. (iv) Como $n = 1 \cdot n = n \cdot 1$ segue da definição que $1|n$. (v) Como $0 = 0 \cdot n$, segue da definição que $n|0$. (vi) Se $d|n$ e $n \neq 0$, então $n = kd$ para algum inteiro k. Por outro lado, $n \neq 0 \Rightarrow k \neq 0$ e, daí, $|k| \geq 1$. Assim, $|n| = |kd| = |k||d| \geq |d|$. (vii) Se $d|n$ e $n|d$, então existem inteiros k_1 e k_2 com $n = k_1 d$ e $d = k_2 n$. Agora, substituindo n em $d = k_2 n$ temos que $d = k_2(k_1 d) = (k_1 k_2)d \Leftrightarrow k_1 k_2 = 1 \Leftrightarrow k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$, já que $k_1, k_2 \in \mathbb{Z}$ e, portanto, $|d| = |n|$. $(viii)$ Se $d|n$ e $d \neq 0$, então $n = kd, k \in \mathbb{Z}$,e segue que n/d é um inteiro. De fato, $(1/d)n = (1/d)kd \Leftrightarrow n/d = k[(1/d)d] = k$. Doravante, $n = (n/d) \cdot d$ segue da definição que $(n/d)|n$. □

Observação 2.12. *i. A Proposição 2.10 pode ser facilmente generalizada para provar que, se $c|a_1, ..., a_n$, então $c|a_1x_1 + \cdots + a_nx_n$, para todo $x_1, ..., x_n \in \mathbb{Z}$.*
ii. Segue do item (vi) do Teorema 2.11 que todo inteiro não nulo tem somente um número finito de divisores.

Teorema 2.13. *(*Teorema de Eudoxius*). Dados a e b inteiros com $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$, existe um inteiro q tal que, para $b > 0$,*

$$qb \leq a < (q+1)b$$

e para $b < 0$,

$$qb \leq a < (q-1)b.$$

Demonstração: Sem perda de generalidade, considere $a > 0$ e $b > 0$ (os casos em que $a < 0$ ou $b < 0$ podem ser demonstrados de maneira análoga). Segue que

i. Se $a = qb$, para algum $q \in \mathbb{Z}$, não há o que provar, e o resultado segue;

ii. Se $a \neq qb \ \forall q \in \mathbb{Z}$, pelo (PBO) existe um inteiro k, mínimo, que satisfaz a condição: $a < kb$

Afirmamos que

$$(k-1)b < a.$$

De fato, caso $a < (k-1)b$ teríamos uma contradição, uma vez que $a < kb$ e k é o menor inteiro que isso ocorre. Deste modo, devemos ter que $(k-1)b < a < kb$. Tomando $q = k-1$, obtemos

$$qb \leq a < (q+1)b.$$

Como queríamos demonstrar. □

Exemplo 2.14. *Se* $a = 17$ *e* $b = 8$*, devemos tomar* $q = 2$*.*

$$2 \times 8 = 16 \leq 17 < 3 \times 8 = 24.$$

Para $a = -17$ *e* $b = 8$*, devemos tomar* $q = -3$*.*

$$-3 \times 8 = -24 \leq -17 < [(-3 + 1) = -2] \times 8 = -16.$$

Se $a = 17$ *e* $b = -8$*, tomamos* $q = -2$*.*

$$(-2) \times (-8) = 16 \leq 17 < [(-2 - 1) = -3] \times (-8) = 24.$$

Para $a = -17$ *e* $b = -8$*, tomamos* $q = 3$*.*

$$3 \times (-8) = -24 \leq -17 < [(3 - 1) = 2] \times (-8) = -16.$$

Apresentaremos, agora, o algoritmo euclidiano ou algoritmo da divisão, que, segundo [2], é a base da aritmética teórica (teoria dos números). Esse resultado aparece no livro VII dos Elementos de Euclides, escrito por volta do ano 300 a.C.

Teorema 2.15. *Dados dois inteiros* a *e* b*,* $b \neq 0$*, existe um único par de inteiros* q *e* r *tais que*

$$a = qb + r \text{ com } 0 \leq r < |b| \ (r = 0 \Leftrightarrow b|a)$$

Donde q *é chamado de quociente e* r *de resto da divisão de* a *por* b*.*

Demonstração: Este é um teorema típico de existência e unicidade. Assim, primeiro mostraremos que existem tais q e r satisfazendo as condições dadas. Suponha primeiro $b > 0$. Pelo Teorema de Eudoxius, existe q satisfazendo: $qb \leq a < (q + 1)b$, de modo que $0 \leq a - qb < b$. Daí, basta definirmos $r = a - qb$, para que seja garantida a existência de q e r. Agora, se $b < 0$, então $-b > 0$, e pelo Teorema de Eudoxius, tem-se que existe q satisfazendo: $qb \leq a < (q-1)b$, donde $0 \leq a - qb < (q - 1)b - qb = (qb - b) - qb = (qb - qb) - b = -b$, de sorte que, $-b > 0$ e, portanto $0 \leq a - qb < |b|$, pois condicionamos $b < 0$. Logo, basta definirmos $r = a - qb$, para que seja garantida a existência de q e r. Portanto, mostramos que existem os inteiros q e r. Mostraremos agora que estes inteiros são únicos. Para tal, vamos supor a existência de outro par q_1 e r_1 de modo que

$$a = q_1 b + r_1 \text{ com } 0 \leq r_1 < |b|.$$

Então, teremos que $qb + r = q_1 b + r_1$ e, assim, $qb - q_1 b = r_1 - r \Leftrightarrow b(q - q_1) = r_1 - r$. Agora, suponhamos por contradição que $r \neq r_1$, sem perda de generalidade, digamos $r > r_1$. Logo, $r_1 - r < 0$, por outro lado, caso $b > 0$, então $q - q_1 < 0$ e, portanto, $q_1 - q > 0$, ou melhor,

$q_1 - q \geq 1$. Agora, caso $b < 0$, então $q - q_1 > 0$ e, portanto, $q_1 - q < 0$, isto é, $q_1 - q \leq -1$. Outrossim, de $b(q - q_1) = r_1 - r$, seque que

$$r = r_1 + b(q_1 - q).$$

Daí, tem-se

(I) Levando-se em conta que $b > 0$, $r_1 \geq 0$ e $q_1 - q \geq 1$, da última igualdade, segue que $r \geq |b|$, o que é um absurdo, já que $0 \leq r < |b|$;

(II) Agora, levando-se em conta que $b < 0$, $r_1 \geq 0$ e $q_1 - q \leq -1$, da última igualdade segue que $r \geq |b|$, pois ($b < 0$, $q_1 - q \leq -1 \Rightarrow b(q_1 - q) > 0$), o que é um absurdo, haja vista que $0 \leq r < |b|$.

Portanto, de (I) e (II), temos $r = r_1$ e, assim, $qb = q_1 b$, de sorte que logo $q = q_1$, como queríamos. □

Exemplo 2.16. *Vamos determinar o quociente e o resto da divisão de* 43 *por* 5.

Resolução: Usaremos o raciocínio da demonstração. Assim, os múltiplos estritamente positivos de 5 são:

$$5, 10, 15, 20, 25, 30, 35, 40, 45, 50, ...$$

observe que, o número 43 está entre 40 e 45, de sorte que $40 = 8 \cdot 5$ e $45 = 9 \cdot 5$. Logo, o quociente é 8. De fato, $8 \cdot 5 \leq 43 < (8 + 1) \cdot 5$. Agora, seja r o resto nesta divisão. Então $r = 43 - 8 \cdot 5 = 3$. □

Exemplo 2.17. *Determine o quociente e o resto da divisão de* -171 *por* -33.

Resolução: Pelo Teorema de Eudoxius, como $b = -33 < 0$, segue que

$$q(-33) \leq -171 < (q - 1)(-33).$$

Por outro lado, pelo algoritmo da divisão, temos que existe um único $r \in \mathbb{Z}$ de modo que $0 \leq r = -171 - q(-33) < |-33| = 33$, donde q e r são, respectivamente, quociente e resto. Das condições de r, devemos ter $-q(-33) > 0$, então basta tomarmos $q > 0$. Por outro lado, estamos interessados na menor diferença possível de $-171 - q(-33)$ (positiva ou nula). Então, devemos tomar o menor múltiplo de 33 maior que 171, que neste caso é o $198 = 6 \cdot 33$. Logo, $r = -171 - 6(-33) = -171 + 198 = 27$, ou seja, $q = 6$ e $r = 27$. De fato, $6 \cdot (-33) = -198 \leq -171 < (6-1)(-33) = 5 \cdot (-33) = -165$ e $0 \leq 27 = -171 - 6 \cdot (-33) = -171 + 198 < |-33|$. □

2.3 Máximo Divisor Comum

Esta seção muito nos auxiliará no decorrer deste trabalho, em particular, na resolução de equações diofantinas lineares, pois nos fornecerá subsídios para tal finalidade.

Nesta seção, usaremos [8] como referência fundamental, pois diferentemente de [2], [3], [5] e [6], que abordam o tema em epígrafe partindo de casos particulares ou até mesmo restringido-se à abordagem a estes, [8] parte de casos gerais para, posteriormente, explorar os casos particulares, citamos, por exemplo, a definição de mdc que segue logo abaixo.

Se $a_1, a_2, \ldots, a_n$ são inteiros não nulos dados, dizemos que um inteiro d é um **divisor comum** de $a_1, a_2, \ldots, a_n$ quando $d|a_1, a_2, \ldots, d|a_n$. Note que $a_1, a_2 \ldots, a_n$ sempre têm divisores comuns: 1 e -1, por exemplo. Ademais, desde que qualquer inteiro não nulo tem apenas um número finito de divisores, $a_1, a_2, \ldots, a_n$ têm apenas um número finito de divisores comuns. Assim, a definição a seguir tem sentido.

Definição 2.18. *O **máximo divisor comum** dos inteiros não nulos $a_1, a_2, \ldots, a_n$, denotado por $mdc(a_1, a_2, \ldots, a_n)$, é o maior dentre os divisores comuns de $a_1, a_2, \ldots, a_n$. Os inteiros $a_1, a_2, \ldots, a_n$ são **primos entre si**, ou **relativamente primos**, se $mdc(a_1, a_2, \ldots, a_n) = 1$.*

Apresentaremos agora um dos resultados mais importante desta seção, para este trabalho, porque, a partir, dele decorrerá uma série de resultados que nos viabilizará solucionar equações diofantinas lineares, caso tenham soluções, como já delineamos acima. Mas, antes, apresentaremos uma notação que será introduzida neste trabalho, a saber, dado $n \in \mathbb{Z}$ denotemos por $n\mathbb{Z}$ o conjunto dos múltiplos inteiros de n, isto é,

$$n\mathbb{Z} = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}.$$

Teorema 2.19. *(*Bèzout[1]*). Sejam $a_1, a_2, ..., a_n$ inteiros não nulos dados. Se*

$$S = \left\{ \sum_{1 \leq i \leq n} a_i x_i; x_i \in \mathbb{Z}, \forall 1 \leq i \leq n \right\},$$

então $S = d\mathbb{Z}$, onde $d = mdc(a_1, a_2, ..., a_n)$. Em particular, existem números inteiros $u_1, ..., u_n$ tais que

$$mdc(a_1, a_2, ..., a_n) = a_1u_1 + a_2u_2 + \cdots + a_nu_n.$$

A demonstração aqui apresentada será a mesma de [8], porém com alguns ensejos dos autores, para facilitar a compreensão dos leitores.

Demonstração: Primeiro, observe que $S = d\mathbb{Z} \Leftrightarrow S \subset d\mathbb{Z}$ e $d\mathbb{Z} \subset S$. Assim, é ime-

[1]Étienne Bèzout, matématico francês do século XVIII, um dos precursores da área da Matemática hoje conhecida como Geometria Algébrica.

diato que todo múltiplo de um elemento de S pertence a S. Por outro lado, como d divide $a_1x_1 + a_2x_2 + \cdots + a_nx_n$ para todos $x_1, x_2, ..., x_n$, temos que $S \subset d\mathbb{Z}$. Para estabelecer a inclusão contrária, note primeiro que S contém inteiros positivos; de fato, escolhendo $x_1 = a_1$e $x_2 = \cdots = x_n = 0$, por exemplo, concluímos que

$$a_1^2 = a_1x_1 + a_2x_2 + \cdots + a_nx_n \in S.$$

Como S contém inteiros positivos, pelo PBO, existe um menor inteiro positivo d' em S. Se mostrarmos que $d' = d$, seguirá que $d \in S$ e nossa observação inicial garantirá que $d\mathbb{Z} \subset S$. Afirmamos, inicialmente, que $d'|a_1, a_2, ..., |a_n$. De fato, como $d' \in S$, existem $u_1, u_2, ..., u_n \in \mathbb{Z}$ tais que $d' = a_1u_1 + a_2u_2 + \cdots + a_nu_n$. Agora, pelo Teorema 2.15 seja $a_1 = d'q + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < d'$. Então

$$\begin{aligned} r &= a_1 - d'q \\ &= a_1 - (a_1u_1 + a_2u_2 + \cdots + a_nu_n)q \\ &= a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq), \end{aligned}$$

de sorte que $r \in S$. Se $0 < r < d'$, teríamos uma contradição ao fato de ser d' o menor inteiro positivo pertencente a S. Logo, $r = 0$ e $d'|a_1$. Analogamente, $d'|a_2, ..., |a_n$. Para concluir, como d' é um divisor comum de $a_1, a_2, ..., a_n$, para mostrarmos que $d' = d$, basta que $d' \geq d$, pois por hipótese $d > 0$. Mas, se $a_1 = dq_1, a_2 = dq_2, ..., a_n = dq_n$, com $q_1, q_2, ..., q_n \in \mathbb{Z}$, então

$$\begin{aligned} d' &= a_1u_1 + a_2u_2 + \cdots + a_nu_n \\ &= dq_1u_1 + dq_2u_2 + \cdots dq_nu_n \\ &= d(q_1u_1 + q_2u_2 + \cdots + q_nu_n), \end{aligned}$$

ou seja, $0 < d|d'$. Logo, pelo item (vi) do Teorema 2.11, temos que $d \leq d'$. □

Observação 2.20. *Na demonstração deste teorema provou-se não apenas que o máximo divisor comum de $a_1, a_2, ..., a_n$ pode ser expresso como uma combinação linear destes números mas que este número é o menor valor positivo dentre todas estas combinações lineares.*

Apresentaremos, a seguir, alguns corolários decorrentes deste teorema, que nos serão úteis.

Corolário 2.21. *Sejam $a_1, a_2, ..., a_n$ inteiros não nulos e d seu (mdc). Se $d' \in \mathbb{N}$, então $d'|a_1, a_2, ..., a_n$ se, e só se, $d'|d$.*

Demonstração: Do Teorema 2.19, segue que podemos tomar inteiros $u_1, u_2, ..., u_n$, de modo que $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$. Por outro lado, uma vez que $d'|a_1, a_2, ..., a_n$, o item (i) da Observação 2.12 garante que $d'|d$. Reciprocamente, como $d = mdc(a_1, a_2, ..., a_n)$, então

pela definição de máximo divisor comum, segue que $d|a_1, d|a_2, ..., d|a_n$. Daí, se $d'|d$, segue da Proposição 2.8 que $d'|a_1, a_2, ..., a_n$. □

Corolário 2.22. *Sejam $a_1, ..., a_n$ inteiros não nulos dados e d seu máximo divisor comum.*
(i) $d = 1$ se, e só se, existirem inteiros $u_1, u_2, ..., u_n$ tais que $a_1u_1 + \cdots + a_nu_n = 1$.
(ii) $mdc(\frac{a_1}{d}, \frac{a_2}{d}, ..., \frac{a_n}{d}) = 1$.

Demonstração: (i) Se $d = 1$, segue imediatamente do Teorema 2.19 (Teorema de Bèzout) a existência de inteiros $u_1, u_2, ..., u_n$, de modo que $a_1u_1 + a_2u_2 + \cdots + a_nu_n = 1$, conforme pede o enunciado. Reciprocamente, sejam $u_1, u_2, ..., u_n$ inteiros como no enunciado. Como $d = mdc(a_1, a_2, ..., a_n)$, então $d|a_1, a_2, ..., a_n$, daí, pelo intem (i) da Observação 2.12, segue que $d|(a_1u_1 + a_2u_2 + \cdots + a_nu_n)$, isto é, $d|1$ e, portanto, $d = 1$.
(ii) Sendo $d = a_1u_1 + a_2u_2 + \cdots + a_nu_n$, como $d > 0$, façamos $(1/d)d = (1/d)(a_1u_1 + a_2u_2 + \cdots + a_nu_n) \Leftrightarrow (\frac{a_1}{d})u_1 + (\frac{a_2}{d})u_2 + \cdots + (\frac{a_n}{d})u_n = 1$, logo, pelo item (i) o resultado segue imediatamente. □

Corolário 2.23. *Para $a_1, a_2, ..., a_n, k$ inteiros não nulos, temos:*
(i) mdc $(ka_1, ..., ka_n) = |k|mdc(a_1, a_2, ..., a_n)$,
(ii) mdc $(a_1, a_2, ..., a_n) = mdc(mdc(a_1, a_2..., a_{n-1}), a_n)$.

Demonstração: (i) Denotemos $d = mdc(a_1, a_2, ..., a_n)$ e $d' = mdc(ka_1, ka_2, ..., ka_n)$. Assim, provaremos que $d' = |k|d$. Como $d|a_1, ..., a_n$, temos que $|k|d \mid ka_1, ..., ka_n$. Isto significa que, $|k|d$ é um divisor comum positivo de $ka_1, ..., ka_n$. Por outro lado, como d' é o maior dentre tais divisores comuns, segue que $|k|d \leq d'$. Reciprocamente, como k divide d' e d' divide $ka_1, ..., ka_n$, temos que $\frac{d'}{|k|}$ é um inteiro positivo que divide $a_1, ..., a_n$; de fato, como $d'|ka_1, ..., ka_n \Rightarrow \frac{d'}{|k|} \mid \frac{k}{|k|}a_1, ..., \frac{k}{|k|}a_n$, isto é, $\frac{d'}{|k|}|a_1, a_2, ..., a_n$, ou seja, $\frac{d'}{|k|}$ é um divisor comum de $a_1, ..., a_n$. Logo, $\frac{d'}{|k|} \leq d$, pois $d = mdc(a_1, a_2..., a_n)$ o que é o mesmo que $d' \leq |k|d$. Finalmente, $d' = |k|d$. Como queríamos.
(ii) Com efeito, pelo Teorema 2.19, temos que existem u e v inteiros tais que

$$mdc(mdc(a_1, a_2, ..., a_{n-1}), a_n) = mdc(a_1, a_2..., a_{n-1})u + a_nv.$$

e, como existem inteiros $y_1, y_2, ..., y_{n-1}$ com

$$a_1y_1 + a_2y_2 + \cdots + a_{n-1}y_{n-1} = mdc(a_1, a_2, ..., a_{n-1}).$$

Denotemos $d = mdc(a_1, ..., a_n)$ e $d' = mdc(mdc(a_1, ..., a_{n-1}), a_n)$. Provaremos que $d = d'$. Pela Observação 2.20 segue que $d' \geq d$. Por outro lado, $d \mid a_1, a_2, ..., a_n$, então pelo item (i) da Observação 2.12 $d \mid a_1y_1 + a_2y_2 + ... + a_{n-1}y_{n-1} + a_nv$, assim $d \mid mdc(a_1, ..., a_{n-1})$ e $d \mid a_n$. Logo, pelo Corolário 2.21 $d \mid d'$, donde segue que $d \leq d'$. Portanto, $d = d'$. □

Até agora apresentamos alguns resultados importantes a respeito do **máximo divisor comum** de n inteiros, todos decorrentes da definição de (mdc), e do Teorema de Bèzout. Agora, com esses resultados, vamos tentar calcular $mdc(82, 719, 3021)$. Pela definição de máximo divisor comum poderíamos listar todos os divisores comuns de 82, 719 e 3021 e decidir qual o maior dentre eles. Por outro lado, o Teorema de Bèzout garante que existem u, v e w inteiros, de modo que $mdc(82, 719, 3021) = 82u + 719v + 3021w$.

No entanto, listar os divisores comuns de 82, 719 e 3021 pode ser uma tarefa trabalhosa e, portanto, impraticável do nosso ponto de vista. Observe também que $mdc(82, 719, 3021) = mdc(mdc(82, 719), 3021)$, conforme Corolário 2.23 item (ii). Por esses motivos, a partir de agora, especializaremos nossa discussão ao máximo divisor comum de dois inteiros não nulos, para que possamos subsidiar um algoritmo útil para encontrarmos efetivamente o (mdc) de dois inteiros de maneira razoável e eficiente. Mas, antes, veja que: dados a, b inteiros não nulos, com $d = mdc(a, b)$, o Teorema de Bèzout garante a existência de inteiros u e v tais que $d = au + bv$.

Proposição 2.24. *Para a, b e c inteiros não nulos, temos que:*
(i) Se $c|ab$ e $mdc(b, c) = 1$, então $c|a$;
(ii) Se $a + bc \neq 0$, então $mdc(a + bc, b) = mdc(a, b)$;
(iii) Se $mdc(a, c) = 1$, então $mdc(a, bc) = mdc(a, b)$;
(iv) Se $c|b$ e $mdc(a, b) = 1$, então $mdc(a, c) = 1$.

Demonstração: (i) De $mdc(b, c) = 1$, segue que existem inteiros u, v, de modo que

$$bu + cv = 1 \Leftrightarrow a(bu + cv) = a \Leftrightarrow (ab)u + c(av) = a,$$

Uma vez que $c|ab$, segue da Proposição 2.10 que $c|a$.
(ii) Sejam $d = mdc(a+bc, b)$ e $d' = mdc(a, b)$. Daí, segue que $d'|a, b$, o que implica $d'|a, a+bc$. Portanto, pelo Corolário 2.21, tem-se que $d'|d$. Reciprocamente, como $d|(a + bc)$ e $d|b$, temos que $d|[(a + bc) - bc] = a$. Isso implica que $d|a, b$. Portanto, pelo Corolário 2.21, temos que $d|d'$ e, assim, $d = d'$.
(iii) Sejam $d = mdc(a, b)$ e $d' = mdc(a, bc)$. Como $d|b$, segue que $d|bc$. Donde, $d|a$ e $d|bc$, então $d|mdc(a, bc) = d'$. Agora, precisamos mostrar que $d'|d$, para que tenhamos $d = d'$. Como $mdc(a, c) = 1$, segue do Teorema de Bèzout que existem inteiros u, v tais que $au + cv = 1 \Leftrightarrow b(au + cv) = b$ e, assim, $a(bu) + (bc)v = b$; mas $d'|a$ e $d'|bc$, logo $d'|b$ e, portanto, $d'|a, b$. Segue que $d'|mdc(a, b) = d$, o que resulta em $d = d'$.
(iv) Como $c|b$, segue que $\exists k \in \mathbb{Z}$, de modo que $b = ck$. Por outro lado, como $mdc(a, b) = 1$, pelo Teorema de Bèzout, existem $u, v \in \mathbb{Z}$ tais que $au+bv = 1$. Agora, Substituindo $b = ck$ em $au + bv = 1$, temos $au + c(kv) = 1$ e segue do item (i) do Corolário 2.22 que $mdc(a, c) = 1$.
□

2.3.1 Algoritmo de Euclides

É chegada a hora de podermos calcular o (mdc) de dois inteiros não nulos a, b com eficiência, mas como já dissemos, até o momento, sabemos apenas que é possível escrever $mdc(a, b) = au + bv$, para algum par de inteiros u, v e, por outro lado, que podemos listar os divisores comuns de a, b e decidir qual é o maior, como fazíamos nas séries iniciais. Entretanto, se a, b forem números grandes esse método se torna muito trabalhoso e, portanto, impraticável ou até impossível. Por exemplo, encontre $mdc(2^{100} - 1, 2^{120} - 1)$. Mas antes de apresentarmos o algoritmo propriamente, vejamos o seguinte lema:

Lema 2.25. *Se $a = qb + r$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração: Sejam $d = mdc(a, b)$ e $d' = mdc(b, r)$. Como $d|a, b$, segue da Proposição 2.10 que $d|(a - qb) = r$. Logo, pelo Corolário 2.21, tem-se que $d|d'$. Reciprocamente, como $d'|b, r$ segue que $d'|[(a - qb) + qb] = a$, conforme Proposição 2.10 e, assim, novamente pelo Corolário 2.21, temos que $d'|d$ e, portanto, $d = d'$. □

Veja que, empregando esse lema uma sucessão de vezes, poderemos diminuir a lista dos divisores comuns de a, b à lista dos divisores comuns de r_{j-1}, r_j em que $r_j \mid r_{j-1}$ ao ponto de decidirmos com precisão o $mdc(a, b)$. Vejamos um exempo:

Exemplo 2.26. *Vamos calcular $mdc(a, b)$, onde $a = 372$ e $b = 162$, utilizando os argumentos acima, ou seja, empregando o Lema 2.25 uma sucessão de vezes.*

Pelo algoritmo da divisão temos que

$$372 = 2 \times 162 + 48 \Leftrightarrow 48 = 372 - 2 \times 162.$$

Assim,

$$mdc(372, 162) = mdc(162, 48).$$

Apliquemos o mesmo argumento ao par $b = 162$ e $r_1 = 48$:

$$162 = 3 \times 48 + 18 \Leftrightarrow 18 = 162 - 3 \times 48.$$

Desse modo,

$$mdc(162, 48) = mdc(48, 18)$$

Aplicando novamente o mesmo argumento ao par $r_1 = 48$ e $r_2 = 18$, tem-se

$$48 = 2 \times 18 + 12 \Leftrightarrow 12 = 48 - 2 \times 18.$$

Logo,

$$mdc(48, 18) = mdc(18, 12).$$

Novamente, o mesmo argumento para o par $r_2 = 18$ e $r_3 = 12$, assim:

$$18 = 1 \times 12 + 6 \Leftrightarrow 6 = 18 - 1 \times 12.$$

Portanto, temos que

$$mdc(372, 162) = mdc(48, 18) = mdc(18, 12) = mdc(12, 6).$$

Agora, listemos os divisores comuns positivos, já que estamos interessados no maior divisor comum de 12 e 6, que são:

$$1, 2, 3, 6.$$

Portanto, reduzimos a lista dos divisores comuns de 372 e 162 a $\{1, 2, 3, 6\}$. E, finalmente

$$mdc(372, 162) = 6.$$

Veja que $r_4 = 6$. Agora, observe que $r_4 | r_3$, de fato $12 = 2 \times 6$. Daí, caso fizéssemos mais uma sucessão, teríamos $r_5 = 0$. Agora, vamos fundamentar o algoritmo do qual viemos falando. Esse algoritmo consiste na aplicação reiterada do lema acima. Vejamos!

Teorema 2.27. *(*Algoritmo de Euclides*) Dados a e b inteiros tais que $a, b > 0$ e $a > b$. Se queremos calcular $mdc(a, b)$, então dividimos a por b, achamos o resto r_1. Se $r_1 \neq 0$, dividimos b por r_1, achamos o resto r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2, achamos o resto r_3. E assim sucessivamente. O último resto, diferente de zero, desta sequência é o máximo divisor comum entre a e b.*

Demonstração: Tendo em mente o exemplo anterior, fica fácil a vizualização e compreesão do enunciado do teorema. Repetindo esse processo e fazendo divisões sucessivas, teremos:

$$\begin{aligned}
Passo\ 1 : a &= q_1 b + r_1 \quad 0 < r_1 < b \\
Passo\ 2 : b &= q_2 r_1 + r_2 \quad 0 < r_2 < r_1 \\
Passo\ 3 : r_1 &= q_3 r_2 + r_3 \quad 0 < r_3 < r_2 \\
&\cdots\cdots \\
Passo\ j : r_{j-2} &= q_j r_{j-1} + r_j \quad 0 < r_j < r_{j-1} \\
Passo\ j+1 : r_{j-1} &= q_{j+1} r_j + 0.
\end{aligned}$$

Note que a execução do algoritmo para, após um número finito de passos. De fato, os restos diminuem a cada passo e, por outro lado, $r_1, r_2, ...$ são inteiros para os quais $b > r_1 > r_2 > r_3 > \cdots \geq 0$, e, portanto, deve existir natural j tal que r_j é o último resto não nulo no processo

de divisões acima. Doravante, pelo Lema 2.25, temos sucessivamente

$$\begin{aligned} mdc(a,b) &= mdc(a-q_1b,b) = mdc(r_1,b) \\ &= mdc(r_1,b-q_2r_1) = mdc(r_1,r_2) \\ &= mdc(r_1-q_3r_2,r_2) = mdc(r_3,r_2) \\ &\quad ... \\ &= mdc(r_{j-1},r_j) = r_j. \end{aligned}$$

Donde utilizamos, na última igualdade, o fato de que $r_j|r_{j-1}$. □

Exemplo 2.28. *Calcule* $mdc(1001, 109)$.

Resolução: Realizando as divisões sucessivas, conforme acima, temos

$$\begin{aligned} 1001 &= 9\times 109+20 \\ 109 &= 5\times 20+9 \\ 20 &= 2\times 9+2 \\ 9 &= 4\times 2+1. \end{aligned}$$

Assim, temos $mdc(1001,109) = mdc(109,20) = mdc(20,9) = mdc(9,2) = mdc(2,1) = 1$. □

Exemplo 2.29. *Encontre* $mdc(2^{120}-1, 2^{100}-1)$.

Resolução: Realizando as divisões sucessivas, temos

$$\begin{aligned} 2^{120}-1 &= 2^{20}\times(2^{100}-1)+(2^{20}-1) \\ 2^{100}-1 &= 2^{80}\times(2^{20}-1)+(2^{80}-1) \\ 2^{80}-1 &= 2^{60}\times(2^{20}-1)+(2^{60}-1) \\ 2^{60}-1 &= 2^{40}\times(2^{20}-1)+(2^{40}-1) \\ 2^{40}-1 &= 2^{20}\times(2^{20}-1)+(2^{20}-1). \end{aligned}$$

Logo, temos que

$$\begin{aligned} mdc(2^{120}-1,2^{100}-1) &= mdc(2^{100}-1,2^{20}-1) = mdc(2^{80}-1,2^{20}-1) \\ &= mdc(2^{60}-1,2^{20}-1) = mdc(2^{40}-1,2^{20}-1) \\ &= mdc(2^{20}-1,2^{20}-1) = 2^{20}-1. \end{aligned}$$

□

O Teorema de Bèzout garante que existem u, v tais que $mdc(a, b) = au + bv$, como já vimos. Agora, já temos condições de encontrarmos esses inteiros u, v, porque está embutido no algoritmo de Euclides um método para tal finalidade. Esse método consite em utilizar o algoritmo de Euclides de trás para frente. Vejamos como proceder através do Exemplo 2.28.

Das igualdades apresentadas na solução do Exemplo 2.28 podemos escrever:

$$\begin{aligned} 1 &= 9 - 4 \times 2 \\ 2 &= 20 - 2 \times 9 \\ 9 &= 109 - 5 \times 20 \\ 20 &= 1001 - 9 \times 109. \end{aligned}$$

Agora, faremos algumas substituições com o objetivo de escrever o resultado 1 como combinação linear de 1001 e 109. Substituiremos os resto de cima para baixo, tomando o cuidado de manter o próximo, ou seja, substituiremos primeiro o 2, organizaremos os resultados e depois substituiremos o 9 e assim sucessivamente. Veja:

$$\begin{aligned} 1 = 9 - 4 \times 2 &= 9 - 4(20 - 2 \times 9) \\ &= 9 \times 9 - 4 \times 20 \\ &= 9(109 - 5 \times 20) - 4 \times 20 \\ &= 9 \times 109 - 49 \times 20 \\ &= 9 \times 109 - 49(1001 - 9 \times 109) \\ &= 1001 \times (-49) + 109 \times 450. \end{aligned}$$

Concluímos ao final desse processo que $u = -49$ e $v = 450$.

Esse método nos permitirá encontrar soluções particulares de equações diofantinas lineares, caso tenham soluções.

2.4 Números Primos

Esta seção nos ajudará muito neste trabalho, pois nos fornecerá alguns subsídios para resolução de exercícios, bem como para fundamentação de algumas demonstrações.

Definição 2.30. *Um número inteiro p é chamado número primo se as seguintes condições se verificam:*
(i) $p \neq 0$;
(ii) $p \neq \pm 1$;
(iii) Os únicos divisores de p são ± 1, $\pm p$.

Um número inteiro $a \neq 0, \pm 1$ é chamado *número composto* se tem outros divisores, além dos triviais[2].

Exemplo 2.31. *Determine todos os números primos que podem ser expressos na forma* $n^2 - 1$.

Resolução: Seja p um primo tal que $p = n^2 - 1 \Leftrightarrow p = (n-1)(n+1)$. Então, pela Definição 2.30, segue que os únicos divisores de p são $\pm 1, \pm p$.
Daí, temos que
(i) $(n-1) = 1$ e $n + 1 = p \Rightarrow n = 2$ e, assim, $p = 3$ ou $(n-1) = p$ e $n + 1 = 1 \Rightarrow n = 0 \Rightarrow p = -1$.
(ii) $(n-1) = -p$ e $n + 1 = -1 \Rightarrow n = -2$ e, assim, $p = 3$ ou $(n-1) = -1$ e $n + 1 = -p \Rightarrow n = 0 \Rightarrow p = -1$.
Portanto, de (i) e (ii), temos que $p = 3$, já que por definição $p \neq \pm 1$. □

Proposição 2.32. *Sejam* $a, b, p \in \mathbb{Z}$. *Se* p *é primo e* $p \mid ab$, *então* $p \mid a$ *ou* $p \mid b$.

Demonstração: Se $p \nmid a$, então $mdc(a, p) = 1$. De fato, os divisores de p são ± 1 e $\pm p$ e assim, os divisores comuns de a e p são apenas ± 1 e, portanto, pelo item (i) da Proposição 2.24, segue que $p|b$. Agora, se $p \nmid b$, então $mdc(b, p) = 1$, donde segue imediatamente que $p|a$. Como queríamos. □

Teorema 2.33. (Teorema Fundamental da Aritmética). *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

Demonstração: Caso o leitor esteja interessado na demonstração deste Teorema, veja [6], página 26. □

Teorema 2.34. *Existem infinitos primos.*

Demonstração: Vamos supor que a sequência dos primos seja finita. Sejam, pois, $p_1, p_2, ..., p_n$ a lista de todos os primos positivos. Consideramos o número $R = p_1 \cdot p_2 \cdot ... \cdot p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas, pelo Teorema Fundamental da Aritmética, ou R é primo ou possui algum fator primo, e isto implica na existência de um primo que não pertence à nossa lista. Portanto, a sequência dos números primos não pode ser finita. □

Lema 2.35. *Se* $a_1, ..., a_n \in \mathbb{N}$ *e* p *é um primo tal que* $p \mid a_1 a_2 ... a_n$, *então existe* $1 \leqslant i \leqslant n$ *tal que* $p \mid a_i$. *Em particular, se* $a_1, ..., a_n$ *forem todos primos, então existe* $1 \leqslant i \leqslant n$ *tal que* $p = a_i$.

Demonstração: Veja [8], página 39. □

[2]Um número inteiro $a \neq 0, \pm 1$ tem pelo menos quatro divisores: ± 1 e $\pm a$. Esses são os *divisores triviais* de a.

2.5 Congruência

Definição 2.36. *Sejam a, b e n inteiros dados, sendo $n > 1$. Dizemos que a é* ***congruente*** *a b, módulo n, e denotamos $a \equiv b \pmod{n}$, se $n|(a-b)$. Se a não for congruente a b módulo n, denotamos $a \not\equiv b \pmod{n}$.*

Exemplo 2.37. $9 \equiv 5 \pmod{2}$, *pois* $2|(9-5)$. *Como* $7 \nmid 16$ *e* $16 = 29 - 13$ *temos que* $29 \not\equiv 13 \pmod{7}$.

Proposição 2.38. *Sejam a e n inteiros dados, com $n > 1$.*
(a) Se a deixa resto r na divisão por n, então $a \equiv r \pmod{n}$. Em particular, todo inteiro é congruente, módulo n, a exatamente um dos números $0, 1, 2, ..., n-2, n-1$.
(b) $a \equiv b \pmod{n} \Leftrightarrow a$ e b deixam um mesmo resto na divisão por n.

Demonstração: (a) Suponhamos que a deixa resto r quando dividido por n. Assim, pelo algoritmo da divisão, segue que $a = qn + r$ para algum inteiro q. Daí, $a - r = qn$, ou seja, $n \mid (a-r)$. Logo, pela definição de congruêcia, tem-se $a \equiv r \pmod{n}$. O restante é imediato.
(b) Se $a \equiv b \pmod{n}$, então $n \mid (a-b)$. Por outro lado, pelo algoritmo da divisão, segue que existem $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leqslant r_1, r_2 < n$, unicamente determinados, tais que $a = q_1 n + r_1$ e $b = q_2 n + r_2$. Então,

$$a - b = (q_1 n + r_1) - (q_2 n + r_2) = (q_1 - q_2)n + (r_1 - r_2),$$

e como $n \mid (a-b)$ e $n \mid (q_1 - q_2)n$, segue da Proposição 2.10 que n divide $r_1 - r_2 = (a-b) - (q_1 - q_2)n$. Por outro lado, $0 \leqslant r_1, r_2 < n \Rightarrow |r_1 - r_2| < n$ e, portanto, a única possibilidade é $|r_1 - r_2| = 0$, isto é, $r_1 = r_2$.
Reciprocamente, se a, b deixam um mesmo resto r na divisão por n, então podemos escrever $a = q_1 n + r$ e $b = q_2 n + r$, com $q_1, q_2 \in \mathbb{Z}$. Logo, $a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$, donde $n \mid (a-b)$ e, portanto, $a \equiv b \pmod{n}$. □

Proposição 2.39. *Dados inteiros a, b, c e n, sendo $n > 1$, temos:*
(a) $a \equiv a \pmod{n}$;
(b) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$;
(c) $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Demonstração: (a) Esse resultado é imediato, pois, como $n \mid 0$, então $n \mid (a-a)$, o que resulta pela definição de congruência em $a \equiv a \pmod{n}$. (b) Se $a \equiv b \pmod{n}$, então $n \mid (a-b)$. Por outro lado, $b - a = -a + b = -(a-b)$, assim, pela Definição 2.7, temos que $n \mid (b-a)$, o que implica em $b \equiv a \pmod{n}$. (c) Se $n \mid (a-b)$, $n \mid (b-c)$, então $a \equiv b \pmod{n}$, $b \equiv c \pmod{n}$, respectivamente. Pela Proposição 2.10, segue que $n \mid (a-b) + (b-c) = a - c$, o que implica em $a \equiv c \pmod{n}$. □

Proposição 2.40. *Sejam a, b, c, d, m e n inteiros dados, com $m, n > 1$.*
(a) Se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a + c \equiv b + d \pmod{n}$ e $ac \equiv bd \pmod{n}$. Em particular, $ac \equiv bc \pmod{n}$;
(b) Se $a \equiv b \pmod{n}$, então $a^k \equiv b^k \pmod{n}$, para todo $k \in \mathbb{N}$;
(c) Se $c_0, c_1, \ldots, c_m \in \mathbb{Z}$ e $f(x) = c_m x^m + \cdots + c_1 x + c_0$, então

$$a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n};$$

(d) Se $a \equiv b \pmod{n}$, então $mdc(a, n) = mdc(b, n)$;
(e) Se $a + c \equiv b + c \pmod{n}$, então $a \equiv b \pmod{n}$;
(f) Se $ac \equiv bc \pmod{n}$ e $mdc(c, n) = d$, então $a \equiv b \pmod{\frac{n}{d}}$. Em particular, se $mdc(c, n) = 1$, então $a \equiv b \pmod{n}$;
(g) Se $a \equiv b \pmod{mn}$, então $a \equiv b \pmod{n}$.

Demonstração: (a) Como $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $n \mid (a - b)$ e $n \mid (c - d)$. Segue da Proposição 2.10 que $n \mid [(a-b)+(c-d) = (a+c)-(b+d)]$, mas isso é o mesmo que $a + c \equiv b + c \pmod{n}$. Por outro lado, segue da Observação 2.12 item (i), que $n \mid (a - b)d$ e $n \mid (c-d)a$, de sorte que, pela Proposição 2.10, tem-se que $n \mid [(a-b)d+(c-d)a = ac-bd]$, o que implica $ac \equiv bd \pmod{n}$. Por fim, como $c \equiv c \pmod{n}$, conforme item (a)da Proposição 2.39, segue do resultado anterior que $ac \equiv bc \pmod{n}$. (b) Se $a \equiv b \pmod{n}$, assim, para $k = 1$, o resultado é imediato. Agora, veja que, fazendo $c = a$ e $d = b$ na segunda parte do item (a), obtemos $a^2 \equiv b^2 \pmod{n}$. Assumimos, agora, a validade da mesma para $k = t$ e utilizando a segunda parte do item (a) mostraremos que a congruência em epígrafe também se verifica para $k = t + 1$. Com efeito, tomemos $c = a^t$ e $d = b^t$, daí

$$a^{t+1} = a \cdot a^t \equiv b \cdot b^t = b^{t+1} \pmod{n}.$$

Logo, pelo Princípio de Indução Finita, podemos concluir que esta proposição é verdaderia para todo $k \in \mathbb{N}$. (c) Se $a \equiv b \pmod{n}$, temos, a partir dos itens (a) e (b), que $c_k a^k \equiv c_k b^k \pmod{n}$, para $0 \leq k \leq m$. Portanto, segue da Observação 2.41 que

$$f(a) = \sum_{0 \leq k \leq m} c_k a^k \equiv \sum_{0 \leq k \leq m} c_k b^k = f(b) \pmod{n}.$$

(d) Como $a \equiv b \pmod{n}$, existe $q \in \mathbb{Z}$ tal que $a = b + nq$. De fato, pois $n \mid (a - b) \Rightarrow \exists q \in \mathbb{Z}$, de modo que $a - b = nq \Rightarrow a = b + nq$. Queremos, pois, mostrar que

$$mdc(b + nq, n) = mdc(b, n).$$

Mas isso é imediato a partir do item (ii) da Proposição 2.24. (e) Se $a+c \equiv b+c \pmod{n}$, então $n \mid [(a+c)-(b+c) = a-b]$, mas isto é implica $a \equiv b \pmod{n}$. (f) Sejam $n = dn'$ e $c = dc'$, com c' e n' inteiros primos entre si. De $ac \equiv bc \pmod{n}$, segue que $n \mid (ac - bc = c(a - b))$,

ou seja, $(dn') \mid [dc'(a-b)]$, ou, ainda, que $n' \mid c'(a-b)$. Mas, como $mdc(n', c') = 1$, segue do intem (i) da Proposição 2.24 que $n' \mid (a-b)$. Note que $n' = \frac{n}{d}$, daí, segue que $a \equiv b \pmod{\frac{n}{d}}$. O resto é imediato. (g) Se $a \equiv b \pmod{mn}$, então $mn \mid (a-b)$, e daí, $m \mid (a-b)$. Mas essa última relação equivale a $a \equiv b \pmod{m}$; analogamente, $a \equiv b \pmod{n}$. □

Observação 2.41. *O item (a) da proposição acima pode ser generalizado para provar que, se $m, n > 1$ são naturais e $a_1, \ldots, a_m, b_1, \ldots, b_m$ são inteiros tais que $a_k \equiv b_k \pmod{n}$ para $1 \leqslant k \leqslant m$, então*

$$\sum_{1\leq k\leq m} a_k \equiv \sum_{1\leq k\leq m} b_k \pmod{n} \quad e \quad \prod_{1\leq k\leq m} a_k \equiv \prod_{1\leq k\leq m} b_k \pmod{n}.$$

Exemplo 2.42. *Mostre que todo número da forma $19^{8n} - 1$ é divisível por 17.*

Resolução: Isto equivale a demonstrar que $17 \mid (19^{8n} - 1)$, de sorte que isto é equivalente a $19^{8n} \equiv 1 \pmod{17}$. Para isso, observemos que

$$19 \equiv 2 \pmod{17}$$

e, assim, $19^4 \equiv 2^4 \pmod{17} \Leftrightarrow 19^4 \equiv 16 \pmod{17}$. De sorte que $16 \equiv -1 \pmod{17}$. Temos

$$19^4 \equiv -1 \pmod{17}.$$

Elevando ambos os membros ao quadrado, temos que $19^8 \equiv 1 \pmod{17}$ e, portanto, $19^{8n} \equiv 1^n = 1 \pmod{17}$, como queríamos mostrar. □

Exemplo 2.43. *Para $N \in \mathbb{N}$, mostremos, utilizando congruência, que o resto da divisão de N por 9 é igual ao resto da divisão da soma dos algarismos da representação decimal de N por 9.*

Resolução: Se $N = (a_n a_{n-1} \cdots a_1 a_0)_{10}$ é a representação decimal do natural N, podemos escrever

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_{10} + a_0 = \sum_{0\leq k\leq n} a_k 10^k.$$

Como $10 \equiv 1 \pmod{9}$, aplicando as propriedades da Proposição 2.40, temos que $10^k \equiv 1 \pmod{9}$, donde

$$N = \sum_{0\leq k\leq n} a_k 10^k \equiv \sum_{0\leq k\leq n} a_k \pmod{9}.$$

Portanto, segue que N e a soma de seus dígitos na base 10 possuem o mesmo resto na divisão por 9. □

Teorema 2.44. *(*Fermat*). Para $a, p \in \mathbb{Z}$, com p primo, temos $a^p \equiv a \pmod{p}$. Em particular, se $mdc(a,p) = 1$, então*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{2.1}$$

Demonstração: Se $a^p \equiv a \pmod{p}$, então p divide $a^p - a = a(a^{p-1} - 1)$; portanto, se $mdc(a,p) = 1$, segue do item (a) da Proposição 2.24 que $p \mid (a^{p-1} - 1)$ e segue (2.1). Assim, basta, pois, mostrarmos que $a^p \equiv a \pmod{p}$, para todo $a \in \mathbb{Z}$. Se $p = 2$ o resultado é óbvio, uma vez que $a^2 - a = a(a-1)$, sendo o produto de dois inteiros consecutivos e, portanto, par. Suponhamos, que $p > 2$ e provaremos o resultado, primeiramente para $a > 0$, por indução sobre a. Para $a = 1$ nada há a fazer. Suponha por hipótese de indução, o teorema válido para um certo valor natural de a, isto é, suponha que $k^p \equiv k \pmod{p}$, para algum $k \in \mathbb{N}$. Para $a = k + 1$, temos

$$\begin{aligned}
(k+1)^p - (k+1) &= \left(\sum_{0 \le j \le p} \binom{p}{j} k^{p-j} \right) - (k+1) \\
&= \left[\binom{p}{0} k^p + \binom{p}{1} k^{p-1} + \cdots + \binom{p}{p-1} k + \binom{p}{p} k^0 \right] - (k+1) \\
&= \left[k^p + \binom{p}{1} k^{p-1} + \cdots + \binom{p}{p-1} k + 1 \right] - (k+1) \\
&= \left[(k^p + 1) - (k+1) \right] + \left[\binom{p}{1} k^{p-1} + \cdots + \binom{p}{p-1} k \right] \\
&= (k^p - k) + \sum_{1 \le j \le p-1} \binom{p}{j} k^{p-j}.
\end{aligned}$$

Mas, como $p \mid (k^p - k)$ (pela hipótese de indução) e $p \mid \binom{p}{j}$ para $1 \le j \le p-1$, de fato, uma vez que o número

$$\binom{p}{j} = \frac{p!}{j!(p-j)!} = \frac{p(p-1)\ldots(j+1)}{(p-j)!}$$

é um inteiro, temos que $(p-j)! \mid (p(p-1)\ldots(j+1))$. Como p é primo, segue que $p \nmid 1, 2, 3, \ldots, p-j$, de sorte que o Lema 2.35 garante que $p \nmid (p-j)!$, assim $mdc(p, (p-j)!) = 1$. Portanto, pelo item (i) da Proposição 2.24, concluímos que $(p-j)!$ divide $p(p-1)\ldots(j+1)$ e, daí, $\binom{p}{j}$ é um múltiplo de p. Logo, deste resultado, segue que p divide $(k+1)^p - (k+1)$, ou seja, que $(k+1)^p \equiv (k+1) \pmod{p}$.

Analisaremos, agora, o caso $a \le 0$: se $a = 0$, nada há a fazer; se $a < 0$, então, uma vez que p é ímpar, segue do que fizemos acima que

$$a^p = -(-a)^p \equiv -(-a) = a \pmod{p}.$$

□

Exemplo 2.45. *Determine o resto da divisão de $2^{5379249}$ por 11.*

Resolução: Utilizando os resultados já apresentados e o teorema acima, vamos calcular o resto da divisão de $2^{5379249}$ por 11. Primeiramente, note que, sem a utilização do teorema acima, devíamos efetuar uma quantidade enorme de potências módulo 11 para encontrarmos o resto em questão. De sorte que, pelo resultado anterior, tem-se $2^{10} \equiv 1 \pmod{11}$. De fato, veja que: $11 \mid [(2^{10} - 1) = 1024 - 1 = 1023 = 93 \cdot 11]$. Por outro lado, $13 \equiv 2 \pmod{11}$, então

$$13^{5379249} \equiv 2^{5379249} = (2^{10})^{537924} \cdot 2^9 \equiv 1^{537924} \cdot 2^9 \pmod{11}.$$

Mas, $2^9 \equiv 6 \pmod{11} \Rightarrow 2^{5379249} \equiv 6 \pmod{11}$. Portanto, o resto em questão é 6. □

Exemplo 2.46. *Mostre que* $2222^{5555} + 5555^{2222}$ *é múltiplo de* 7.

Resolução: De sorte que isto equivale a mostrar que $2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$, de fato, isto é o mesmo que $7 \mid (2222^{5555} + 5555^{2222})$. Como 7 é primo e $mdc(2222, 7) = 1$ e $mdc(5555, 7) = 1$, pelo Teorema de Fermat, temos que

$$2222^6 \equiv 1 \pmod{7} \quad e \quad 5555^6 \equiv 1 \pmod{7}.$$

Por outro lado, pelo algoritmo da divisão, tem-se:

$$5555 = 925 \times 6 + 5 \quad e \quad 2222 = 370 \times 6 + 2$$

Então,

$$\begin{aligned}
2222^6 &\equiv 1 \pmod{7} \Rightarrow \\
(2222^6)^{925} &\equiv 1 \pmod{7} \Rightarrow \\
(2222^6)^{925} \cdot 2222^5 &\equiv 2222^5 \pmod{7} \Rightarrow \\
2222^{5555} &\equiv 3^5 \pmod{7} \Rightarrow \\
2222^{5555} &\equiv 243 \pmod{7} \Rightarrow \\
2222^{5555} &\equiv 5 \pmod{7}.
\end{aligned}$$

A última equação nos diz que o resto da divisão de 2222^{5555} por 7 é 5. Outrossim:

$$\begin{aligned}
5555^6 &\equiv 1 \pmod{7} \Rightarrow \\
(5555^6)^{370} &\equiv 1 \pmod{7} \Rightarrow \\
5555^{2220} \cdot 5555 &\equiv 5555 \pmod{7} \Rightarrow \\
5555^{2220} \cdot 5555 &\equiv 4 \pmod{7} \Rightarrow \\
5555^{2220} \cdot 5555^2 &\equiv 4^2 \pmod{7} \Rightarrow \\
5555^{2222} &\equiv 2 \pmod{7}.
\end{aligned}$$

A última equação nos diz que o resto da divisão de 5555^{2222} por 7 é 2. Donde segue que

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 = 7 \pmod{7} \Leftrightarrow 2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}.$$

Portanto, $2222^{5555} + 5555^{2222}$ é múltiplo de 7. □

Capítulo 3

Equações Diofantinas Lineares

Neste capítulo, tomando como base [1] , [2], [3], [4] e [11], mostraremos como encontrar uma solução particular e a solução geral de equações diofantinas lineares com n incógnitas. Para tal finalidade, iniciaremos abordando acerca das equações diofantinas lineares a duas incógnitas, logo em seguida, a três incógnitas, e finalmente as equações a n incógnitas. Buscamos, desta forma, compreender melhor como se dá o processo de resolução de equações diofantinas lineares, a partir da técnica apresentada por [1], bem como possibilitar uma compreensão mais consistente por parte do leitor.

3.1 Equações Diofantinas Lineares a duas Incógnitas

Esse tipo de equação com duas incógnitas se apresenta da seguinte forma: $ax + by = c$ com $a, b, c \in \mathbb{Z}$, onde a e b são inteiros não nulos simultaneamente.

Para determinar uma solução da equação $ax + by = c$, devemos procurar inteiros x_0 e y_0, de forma que $ax_0 + by_0 = c$ seja verdadeira.

Dada uma equação, as perguntas naturais que se colocam são as seguintes:

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

No que segue, buscaremos responder a estes questionamentos.

Proposição 3.1. *Uma equação diofantina linear $ax + by = c$, em que $a \neq 0$ ou $b \neq 0$, tem solução se, e somente se, $d = mdc(a, b)$ é um divisor de c.*

Demonstração: Se (x_0, y_0) é uma solução, vale a igualdade

$$ax_0 + by_0 = c.$$

Como $d \mid a$ e $d \mid b$, então $d \mid c$, este resultado segue da Proposição 2.10. Reciprocamente, se $d = mdc(a, b)$, então pelo Teorema de Bèzout, podem-se determinar $x_0, y_0 \in \mathbb{Z}$, de modo que, $ax_0 + by_0 = d$. Por hipótese, por hipótese, $d \mid c$ e, portanto, $c = qd$ para algum inteiro q, tem-se

$$c = dq = (ax_0 + by_0)q = (ax_0)q + (by_0)q = a(x_0q) + b(y_0q),$$

Portanto, o par (x_0q, y_0q) é solução da equação em epígrafe. □

Proposição 3.2. *Seja (x_0, y_0) uma solução particular da equação diofantina linear $ax+by = c$, onde $a \neq 0$ e $b \neq 0$. Então, essa equação admite infinitas soluções, e o conjunto dessas soluções é:*

$$S = \left\{ \left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t \right) | \; t \in \mathbb{Z} \right\},$$

onde $d = mdc(a, b)$.

Demonstração: Primeiramente, mostraremos que, todo par $(x_0+(b/d)t, y_0-(a/d)t)$ é solução da equação considerada. De fato,

$$\begin{aligned} a(x_0 + (b/d)t) + b(y_0 - (a/d)t) &= (ax_0 + a(b/d)t) + (by_0 - b(a/d)t) \\ &= (ax_0 + by_0) + (a(b/d)t - b(a/d)t) \\ &= (ax_0 + by_0) + [(ab - ba)/d]t \\ &= ax_0 + by_0 = c, \end{aligned}$$

já que (x_0, y_0) é solução, por hipótese. Agora, seja (x', y') uma solução genérica da equação em tela. Então,

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

donde

$$a(x' - x_0) = b(y_0 - y').$$

Por outro lado, como $d \mid a$ e $d \mid b$, existem inteiros r e s tais que $a = dr$ e $b = ds$, de modo que $mdc(r, s) = 1$. Assim,

$$dr(x' - x_0) = ds(y_0 - y'),$$

e, portanto,

$$r(x' - x_0) = s(y_0 - y').$$

Dessa última igualdade, segue que $r \mid s(y_0 - y')$. De sorte que r e s são primos entre si, pelo item (i) da Proposição 2.24, $r \mid y_0 - y'$. Logo, para algum $t \in \mathbb{Z}$, tem-se

$$y_0 - y' = rt \Leftrightarrow y' = y_0 - rt. \tag{3.1}$$

Agora, note que, em consequência,

$$r(x' - x_0) = s(y_0 - y') = srt,$$

donde

$$r(x' - x_0) = srt,$$

e, portanto,

$$x' - x_0 = st \Leftrightarrow x' = x_0 + st. \tag{3.2}$$

Por fim, façamos $r = a/d$ e $s = b/d$. Logo, de (3.1) e (3.2), obtemos

$$y' = y_0 - \left(\frac{a}{d}\right)t,$$
$$x' = x_0 + \left(\frac{b}{d}\right)t.$$

□

Exemplo 3.3. *Vejamos como achar as soluções de* $172x + 20y = 1000$.

Resolução: Dividindo os coeficientes da equação $172x+20y = 1000$ por 4, obtemos a equação equivalente $43x + 5y = 250$. Como $mdc(43, 5) = 1$, esta última equação é compatível, isto é, tem solução portanto, o mesmo ocorrendo com a equação dada. Por outro lado, notemos que se (x_0, y_0) é solução de $43x + 5y = 1$, então o par $(250x_0, 250y_0)$ é solução de $43x + 5y = 250$, de fato, basta multiplicar $43x + 5y = 1$ por 250. Mas uma solução de $43x + 5y = 1$ pode ser achada, conforme já pontuamos na subseção 2.3.1, basta utilizarmos o algoritmo de Euclides de trás para frente. Vejamos!

$$43 = 5 \cdot 8 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1.$$

Das divisões sucessivas, obtém-se

$$\begin{aligned} 1 = 3 - 2 \cdot 1 &= 3 - (5 - 3 \cdot 1) \\ &= 3 \cdot 2 + 5 \cdot (-1) \\ &= (43 - 5 \cdot 8) \cdot 2 + 5 \cdot (-1) \\ &= 43 \cdot 2 + 5 \cdot (-17). \end{aligned} \tag{3.3}$$

Segue que $(x_0, y_0) = (2, -17)$ é solução da equação $43x + 5y = 1$. Logo, $(250x_0, 250y_0) = (500, -4250)$ é uma solução particular da equação dada.

Consequentemente, sua solução geral é expressa da seguinte forma:

$$\begin{aligned} x &= 500 + 5t, \\ y &= -4250 - 43t, \end{aligned}$$

onde $t \in \mathbb{Z}$.
Por fim, o conjunto dessas soluções é:

$$S = \{(500 + 5t, -4250 - 43t) | t \in \mathbb{Z}\}.$$

□

Conforme pontua [4], o único verdadeiro trabalho que se tem para resolver uma equação diofantina linear $ax + by = c$ é calcular $mdc(a, b)$ para verificar se divide ou não c e descobrir uma solução particular x_0, y_0. Vejamos mais exemplos.

Exemplo 3.4. *Decomponha o número* 100 *em duas parcelas positivas tais que uma é múltiplo de* 7 *e a outra de* 11. *(Problema do matemático L. Euler [1707-1738].)*

Resolução: A equação a ser resolvida é $7x+11y = 100$, que possui solução, pois $mdc(7, 11) = 1$ e $1 \mid 100$. Por outro lado, notemos que, se (x_0, y_0) é solução de $7x + 11y = 1$, então o par $(100x_0, 100y_0)$ é solução de $7x + 11y = 100$. Para encontrarmos o par (x_0, y_0), procederemos conforme exercício anterior. Assim, segue-se:

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1. \end{aligned}$$

Das divisões sucessivas, temos que

$$\begin{aligned} 1 = 4 - (3 \cdot 1) &= 4 - (7 - 4 \cdot 1) \\ &= 4 \cdot 2 - 7 \\ &= (11 - 7 \cdot 1) \cdot 2 - 7 \\ &= 11 \cdot 2 - 7 \cdot 3 \\ &= 7 \cdot (-3) + 11 \cdot 2. \end{aligned}$$

Logo, $(x_0, y_0) = (-3, 2)$. Assim, $(100x_0, 100y_0) = (-300, 200)$ é uma solução particular da equação dada. Portanto, a solução geral é da forma: $x = -300+11t$ e $y = 200-7t$ com $t \in \mathbb{Z}$. No entanto, note que, estamos interessados em soluções positivas, isto é, $x, y > 0$. Então,

$$-300 + 11t > 0 \Leftrightarrow t > \frac{300}{11}, \tag{3.4}$$

$$200 - 7t > 0 \Leftrightarrow t < \frac{200}{7}. \tag{3.5}$$

Desde que $300 = 27 \cdot 11 + 3$ e $200 = 28 \cdot 7 + 4$. Assim, de (3.4) e (3.5), segue que

$$\frac{300}{11} = 27 + \frac{3}{11} < t < \frac{200}{7} = 28 + \frac{4}{7}. \tag{3.6}$$

Logo, de (3.6), devemos ter $t = 28$. Portanto, $x = -300 + 11 \cdot 28 = -300 + 308 = 8$ e $y = 200 - 7 \cdot 28 = 200 - 196 = 4$. Finalmente, $7 \cdot 8 = 56$ e $11 \cdot 4 = 44$ são as parcelas procuradas. □

Exemplo 3.5. *Mostre que nenhum inteiro pode deixar resto* 5 *quando dividido por* 12 *e resto* 4 *quando dividido por* 15.

Resolução: Por absurdo, suponha que exista um inteiro positivo n satisfazendo tais condiçõe. Então, $n = 12y + 5$ e $n = 15x + 4$, o que nos conduz a equação $15x - 12y = 1$. Daí, $mdc(15, 12) \mid 1$, isto é, $3 \mid 1$. Absurdo! Portanto, não existe nenhum inteiro positivo satisfazendo tais condições. □

3.2 Equações Diofantinas Lineares a três Incógnitas

Consideremos agora a equação $a_1x + a_2y + a_3z = b$, onde cada a_i, com $i = 1, 2, 3$, sejam inteiros não nulos simultaneamente. A mesma argumentação usada para provar a Proposição 3.1 garante que essa equação admite soluções se, e somente se, $d = mdc(a_1, a_2, a_3)$ divide b. Com efeito, pelo item (ii) do Corolário 2.23, tem-se que $mdc(a_1, a_2, a_3) = mdc(mdc(a_1, a_2), a_3)$. Assim, se $mdc(a_1, a_2) = d_1$, então existem $u_1, u_2 \in \mathbb{Z}$ para os quais $a_1u_1 + a_2u_2 = d_1$, conforme Teorema de Bèzout. Como $d = mdc(a_1, a_2, a_3) = mdc(d_1, a_3)$, existem $v, z_0 \in \mathbb{Z}$ tais que $d = d_1v + a_3z_0$. Daí,

$$d = d_1v + a_3z_0 = (a_1u_1 + a_2u_2)v + a_3z_0 = a_1(u_1v) + a_2(u_2v) + a_3z_0.$$

Fazendo $a_1u_1 = x_0$ e $a_2u_2 = y_0$, temos que

$$a_1x_0 + a_2y_0 + a_3z_0 = d.$$

Assim, se $a_1x + a_2y + a_3z = b$ admite solução, como $b = dq$ para algum $q \in \mathbb{Z}$, então:

$$a_1(x_0q) + a_2(y_0q) + a_3(z_0q) = dq = b.$$

O que mostra que (x_0q, y_0q, z_0q) é uma de suas soluções particulares.

Exemplo 3.6. *Vejamos como encontrar uma solução particular de*

$$120x + 84y + 144z = 60.$$

Resolução: Como $mdc(120, 84, 144) = 12$ e $12 \mid 60$, então essa equação é compatível, ou seja, admite solução. Consideremos sua forma equivalente:

$$10x + 7y + 12z = 5.$$

Seja $d_1 = mdc(10, 7)$, pelo Algoritmo de Euclides, temos que

$$10 = 7 \cdot 1 + 3$$
$$7 = 3 \cdot 2 + 1$$
$$3 = 1 \cdot 3 + 0.$$

Então, $d_1 = 1$.
Daí,

$$1 = 7 - 3 \cdot 2 = 7 - (10 - 7 \cdot 1) \cdot 2 = 10 \cdot (-2) + 7 \cdot 3.$$

Agora, veja que o $mdc(1, 12) = 1$. Então, tomando $z_0 = 0$, teremos que:

$$10 \cdot (-2) + 7 \cdot 3 + 12 \cdot 0 = 1.$$

Logo o terno $(-10, 15, 0)$ é uma solução da equação dada. De fato, $120 \cdot (-10) + 84 \cdot 15 + 144 \cdot 0 = -1200 + 1260 + 0 = 60$. □

3.2.1 Solução Geral

Para encontrar a solução geral de uma equação diofantina linear a três incógnitas, caso seja compatível, utilizaremos os seguintes passos:
(i) Por meio de uma substituição, reduziremos a equação original a uma equação com duas incógnitas e resolveremos essa equação.
(ii) A partir dessa solução, retornaremos na substituição feita inicialmente e resolveremos mais uma equação a duas incógnitas, obtendo, assim, a solução geral.

Considere a equação $a_1x + a_2y + a_3z = b$, onde $a_1, a_2, a_3 \in \mathbb{Z}$ e os três são direfentes de zero. Se a equação possui solução, então $d = mdc(a_1, a_2, a_3) \mid b$. Considerando, $a_1x + a_2y = k$, temos

$$k + a_3z = b, \tag{3.7}$$

Que, evidendimente, a Equação (3.7) possui solução. Uma vez que $d_1 = mdc(1, a_3) = 1$ e $1 \mid b$. Pela Proposição 3.2, segue que a solução geral da Equação (3.7) é dada por

$$S_1 = \left\{ \left(k_0 + \frac{a_3}{d_1}t_1, z_0 - \frac{1}{d_1}t_1 \right) | \; t_1 \in \mathbb{Z} \right\},$$

como $mdc(1, a_3) = 1$, segue que

$$S_1 = \{(k_0 + a_3t_1, z_0 - t_1 | \; t_1 \in \mathbb{Z})\}.$$

Agora, vejamos que $a_1x + a_2y = k = k_0 + a_3t_1$ e, sendo assim, devemos escolher valores convenientes para t_1, que satisfaça

$$d_2 = mdc(a_1, a_2) \mid (k_0 + a_3t_1).$$

Pela Proposição 3.2, segue que a solução geral de $a_1x + a_2y = k$ é da forma

$$S_2 = \left\{ \left(x_0 + \frac{a_2}{d_2}t_2, y_0 - \frac{a_1}{d_2}t_2 \right) | \; t_2 \in \mathbb{Z} \right\}.$$

Por fim, podemos concluir que o conjunto solução da equação $a_1x + a_2y + a_3z = b$ é dado por

$$S = \left\{ \left(x_0 + \frac{a_2}{d_2}t_2, y_0 - \frac{a_1}{d_2}t_2, z_0 - t_1 \right) | \; t_1, t_2 \in \mathbb{Z} \right\}.$$

Exemplo 3.7. *Determinemos todas as soluções inteiras da equação* $120x + 84y + 144z = 60$.

Resolução: Já vimos no Exemplo 3.6 que a equação acima possui solução. Por outro lado, vimos também que, a equação $120x + 84y + 144z = 60$ equivale a $10x + 7y + 12z = 5$. Vamos agora encontrar a solução geral da equação em epígrafe a partir da equação equivalente $10x + 7y + 12z = 5$. Para isso, tomamos $k = 10x + 7y$. Daí teremos $k + 12z = 5$ que, também, possui solução, pois $mdc(1, 12) = 1 \mid 5$. Pelo Teorema de Bèzout, segue que existem $u, v \in \mathbb{Z}$ de modo que $mdc(1, 12) = u + 12v$, ou seja, podemos escrever 1 como combinação linear de 1 e 12. Para tal, observe que

$$1 = 1 \cdot (-11) + 12. \tag{3.8}$$

Multiplicando por 5 ambos os lados de (3.8), teremos

$$5 = 1 \cdot (-55) + 12 \cdot (5).$$

Sendo, pois, $(-55, 5)$ uma solução particular de $k + 12z = 5$, segue da Proposição 3.2 que a solução geral de $k + 12z = 5$ é dada por

$$S_1 = \{(-55 + 12t_1, 5 - t_1) | t_1 \in \mathbb{Z}\}. \tag{3.9}$$

Analisaremos agora $10x + 7y = k = -55 + 12t_1$. Note que, $mdc(10, 7) = 1$ e $1 \mid (-55 + 12t_1)$. Assim, t_1 pode assumir qualquer valor inteiro. No Exemplo (3.6), vimos que

$$1 = 10 \cdot (-2) + 7 \cdot (3). \tag{3.10}$$

Daí, multiplicando ambos os lados de (3.10) por $(-55 + 12t_1)$, teremos

$$\begin{aligned} (-55 + 12t_1) \cdot 1 &= 10 \cdot (-2) \cdot (-55 + 12t_1) + 7 \cdot (3) \cdot (-55 + 12t_1) \\ -55 + 12t_1 &= 10 \cdot (110 - 24t_1) + 7 \cdot (-165 + 36t_1). \end{aligned}$$

Pela Proposição 3.2, segue que a solução geral de $10x + 7y = -55 + 12t_1$ é dada por

$$S_2 = \{((110 - 24t_1) + 7t_2, (-165 + 36t_1) - 10t_2) | \; t_1, t_2 \in \mathbb{Z}\}. \tag{3.11}$$

Portanto, de (3.9) e (3.11), segue que o conjunto de todas as soluções da equação $10x + 7y + 12z = 5$ é

$$S = \{(110 - 24t_1 + 7t_2, -165 + 36t_1 - 10t_2, 5 - t_1) | \; t_1, t_2 \in \mathbb{Z}\}. \tag{3.12}$$

Finalmente, os elementos de S são as soluções gerais da equação dada. □

Exemplo 3.8. *Encontre todas as soluções inteiras de* $8x + 18y + 20z = 1034$.

Resolução: Como $mdc(8, 18, 20) = 2$ e $2 \mid 1034$, então a equação possui solução. Por outro lado, observe que, a equação $8x + 18y + 20z = 1034$ equivale a $4x + 9y + 10z = 517$ e $mdc(4, 9, 10) = 1 \mid 517$, como esperado, e a equação equivalente é compatível. Faremos agora a redução da equação $4x + 9y + 10z = 517$ em duas novas equações, sendo elas $4x + 9y = k$ e $k + 10z = 517$. Para a equação $k + 10z = 517$ temos que $mdc(1, 10) = 1$ e $1 \mid 517$. Agora, vamos escrever 1 como combinação linear de 1 e 10. Temos

$$1 = 1 \cdot (-9) + 10 \cdot (1). \tag{3.13}$$

Multiplicando por 517 ambos os lados de (3.13), temos que

$$517 = 1 \cdot (-4653) + 10 \cdot (517).$$

Logo, $(-4653, 517)$ é uma solução particular da equação $k + 10z = 517$ e, portanto, pela Proposição 3.2, segue que a solução geral é da forma

$$S_1 = \{(-4653 + 10t_1, 517 - t_1) |\, t_1 \in \mathbb{Z}\}. \tag{3.14}$$

Agora, precisamos encontrar a solução da segunda equação, ou seja, de $4x+9y = k$. Mas, antes, veja que $4x+9y = k = -4653+10t_1$. Desde que $mdc(4, 9) = 1$ e $1 \mid (-4653+10t_1), \forall t_1 \in \mathbb{Z}$, de fato, $1 \mid -4653$ e $1 \mid 10$. Como fizemos em (3.13), vamos escrever $mdc(4, 9) = 1$ como combinação linear de 4 e 9. Assim, segue-se:

$$1 = 4 \cdot (-2) + 9 \cdot (1). \tag{3.15}$$

Multiplicando ambos os lados de (3.15) por $-4653 + 10t_1$, teremos

$$-4653 + 10t_1 = 4 \cdot (9306 - 20t_1) + 9 \cdot (-4653 + 10t_1). \tag{3.16}$$

Logo, de (3.16), segue que $(9306 - 20t_1, -4653 + 10t_1)$ é uma solução particular da equação $4x + 9y = k$, e portanto, pela Proposição 3.2, temos que a solução geral desta equação é da forma

$$S_2 = \{((9306 - 20t_1) + 9t_2, (-4653 + 10t_1) - 4t_2 |\, t_2 \in \mathbb{Z}\}. \tag{3.17}$$

Portanto, de (3.14) e (3.17), tem-se que a solução geral da equação $4x + 9y + 10z = 517$ é dada por

$$S = \{(9306 - 20t_1 + 9t_2, -4653 + 10t_1 - 4t_2, 517 - t_1 |\, t_1, t_2 \in \mathbb{Z}\}.$$

□

3.3 Equações Diofantinas Lineares a n Incógnitas

Mostraremos nesta seção um método que nos permite encontar tadas as soluções de uma equação diofantina linear a n incógnitas. Para tal, consideremos a equação diofantina linear a n incógnitas

$$a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} + a_nx_n = b, \tag{3.18}$$

onde nos interessa encontrar um conjunto de n-uplas $(x_1, x_2, ..., x_n)$ de inteiros em que a condição (3.18) é verificada. Este método consiste em reduzir a equação diofantina linear com mais de duas incógnitas em uma equação diofantina linear de duas incógnitas, conforme fizemos na seção anterior. Por outro lado, a mesma argumentação usada para provar a Proposição 3.1 garante que a Equação (3.18) admite solução inteira se, e somente se, $d = mdc(a_1, a_2, ..., a_n)$ e $d \mid b$. Os resultados que se seguem têm como base [1] e [11].

3.3.1 Solução Particular

Para obter uma solução particular para (3.18), observemos que, se $d_1 = mdc(a_1, a_2)$, então pelo Teorema de Bèzout segue que existem $u_1, u_2 \in \mathbb{Z}$ para os quais $a_1u_1 + a_2u_2 = d_1$. Tomemos agora $d_2 = mdc(d_1, a_3)$. Novamente pelo Teorema de Bèzout, existem $u_3, u_4 \in \mathbb{Z}$ de modo que $d_1u_3 + a_3u_4 = d_2$. Veja que $d_2 \mid a_1, a_2, a_3$, pois $mdc(a_1, a_2, a_3) = mdc(mdc(a_1, a_2), a_3) = mdc(d_1, a_3) = d_2$, conforme item (ii) do Corolário 2.23. Procedendo de forma análoga $n - 1$ vezes, chegaremos em $d = mdc(d_{n-1}, a_n)$, ou seja, podemos escrever d como combinação linear dos $a_{i's}$ da seguinte forma

$$a_1x'_1 + a_2x'_2 + \cdots + a_{n-1}x'_{n-1} + a_nx'_n = d.$$

Vide Teorema de Bèzout. E como $d \mid b$, então existe $q \in \mathbb{Z}$ tal que, $b = dq$.
Donde,

$$a_1(x'_1q) + a_2(x'_2q) + \cdots + a_{n-1}(x'_{n-1}q) + a_n(x'_nq) = d \cdot q = b.$$

Portanto,

$$(x'_1q, x'_2q, \cdots, x'_{n-1}q, x'_nq),$$

é uma solução particular da Equação (3.18).

3.3.2 Solução Geral

Para encontrar a solução geral da Equação (3.18), devemos utilizar o processo de reduzi-la a uma equação diofantina linear a duas incógnitas. Conforme segue, $a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} = k_1$ e $k_1 + a_nx_n = b$, de modo que $d_1 = mdc(1, a_n) = 1$, e $1 \mid b$. Assim, pela Proposição 3.2, a solução geral de $k_1 + a_nx_n = b$ é da forma

$$k_1 = k'_1 + \frac{a_n}{d_1}t_1, x_n = x'_n - \frac{1}{d_1}t_1, \text{com } t_1 \in \mathbb{Z}.$$

Repetido o mesmo argumento, agora para $a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} = k_1$, teremos $a_1x_1 + a_2x_2 + \cdots + a_{n-2}x_{n-2} = k_2$ e $k_2 + a_{n-1}x_{n-1} = k_1$. Note que $d_1 = mdc(1, a_{n-1}) = 1$ e $1 \mid k_1$. Logo, pela Proposição 3.2, a solução geral de $k_2 + a_{n-1}x_{n-1} = k_1$ é da forma

$$k_2 = k_2' + \frac{a_{n-1}}{d_2}t_2, x_{n-1} = x_{n-1}' - \frac{1}{d_2}t_2, \text{com } t_2 \in \mathbb{Z}.$$

Faremos o mesmo para a equação $a_1x_1 + a_2x_2 + \cdots + a_{n-2}x_{n-2} = k_2$, então façamos, $a_1x_1 + a_2x_2 + \cdots + a_{n-3}x_{n-3} = k_3$ e $k_3 + a_{n-2}x_{n-2} = k_2$, de modo que $d_3 = mdc(1, a_{n-2}) = 1$ e $1 \mid k_2$. Daí, da Proposição 3.2, segue que a solução geral de $k_3 + a_{n-2}x_{n-2} = k_2$ é da forma

$$k_3 = k_3' + \frac{a_{n-2}}{d_3}t_3, x_{n-2} = x_{n-2}' - \frac{1}{d_3}t_3, \text{com } t_3 \in \mathbb{Z}.$$

Seguindo estes argumentos, podemos concluir que a solução geral da Equação (3.18) é dada por

$$\begin{aligned} x_1 &= x_1' + \frac{a_2}{d_{n-1}}t_{n-1}, \\ x_2 &= x_2' - \frac{a_1}{d_{n-1}}t_{n-1}, \\ x_3 &= x_3' - t_{n-2}, \\ &\vdots \\ x_n &= x_n' - t_1, \end{aligned}$$

Para $t_1, t_2, ..., t_{n-1} \in \mathbb{Z}$ que pode ser representada da seguinte forma

$$S = \left\{ \left(x_1' + \frac{a_2}{d_{n-1}}t_{n-1}, x_2' - \frac{a_1}{d_{n-1}}t_{n-1}, x_3' - t_{n-2}, \ldots, x_n' - t_1 \right) | \, t_i \in \mathbb{Z}, i = 1, 2, 3, \cdots, n-1 \right\},$$

sendo $d_{n-1} = mdc(a_1, a_2)$.

Exemplo 3.9. *Determine todas as soluções da equação diofantina* $8x+18y+20z+80w = 648$.

Resolução: Note que a equação dada possui solução, pois $mdc(8, 18, 20, 80) = 2$ e $2 \mid 648$. Por outro lado, a equação $8x + 18y + 20z + 80w = 648$ equivale a $4x + 9y + 10z + 40w = 324$, veja que $mdc(4, 9, 10, 40) = 1$ e $1 \mid 324$ como esperado. Agora, façamos a redução da equação $4x + 9y + 10z + 40w = 324$ em duas novas equações. Assim, teremos $4x + 9y + 10z = k_1$ e $k_1+40w = 324$. É evidente que a equação $k_1+40w = 324$ possui solução, pois, $mdc(1, 40) = 1$ e $1 \mid 324$. Portanto, conseguimos encontrar uma solução particular e geral, conforme fizemos na seção anterior. Para encontrarmos uma solução particular de $k_1 + 40w = 324$, basta, pois, escrevermos 1 como combinação linear de 1 e 40, de sorte que o Teorema de Bèzout garante a existência de $u, v \in \mathbb{Z}$, tais que $1 = 1 \cdot u + 40 \cdot v$. Com efeito, vejamos:

$$1 = 1 \cdot (-39) + 40 \cdot (1). \tag{3.19}$$

Multiplicando por 324 ambos os lados de (3.19), resulta

$$324 = 1 \cdot (-12636) + 40 \cdot (324). \tag{3.20}$$

De (3.20) temos que $(-12636, 324)$ é uma solução particular de $k_1 + 40w = 324$. Segue, portanto, da Proposião 3.2 que a solução geral desta equação é da forma

$$S_1 = \{(-12636 + 40t_1, 324 - t_1) |\, t_1 \in \mathbb{Z}\}. \tag{3.21}$$

Veja que $4x + 9y + 10z = k_1 = -12636 + 40t_1$ e como $mdc(4, 9, 10) = 1 \mid (-12636 + 40t_1), \forall\, t_1 \in \mathbb{Z}$, assim, podemos tomar t_1 arbitário. Resolvemos agora $4x + 9y + 10z = k_1 = -12636+40t_1$, fazendo uma nova redução. Para tal, tome $4x+9y = k_2$. Logo, temos $k_2+10z = -12636 + 40t_1$, que também possui solução, pois $mdc(1, 10) = 1$ e $1 \mid (-12636 + 40t_1)$. Portanto, escrevendo como combinação linear $mdc(1, 10) = 1$, tem-se

$$1 = 1 \cdot (-9) + 10 \cdot (1). \tag{3.22}$$

Multiplicando ambos os lados de (3.22) por $(-12636 + 40t_1)$, temos que

$$\begin{aligned} (-12636 + 40t_1) \cdot 1 &= 1 \cdot (-9) \cdot (-12636 + 40t_1) + 10 \cdot (1) \cdot (-12636 + 40t_1) \\ -12636 + 40t_1 &= 1 \cdot (113724 - 360t_1) + 10 \cdot (-12636 + 40t_1), \end{aligned}$$

donde concluímos que a solução particular de $k_2 + 10z = -12636 + 40t_1$ é

$$(113724 - 360t_1, -12636 + 40t_1),$$

de modo que sua solução geral é dada por

$$S_2 = \{(113724 - 360t_1 + 10t_2, -12636 + 40t_1 - t_2) |\, t_1, t_2 \in \mathbb{Z}\}. \tag{3.23}$$

Falta, portanto, encotrarmos a solução geral de $4x + 9y = k_2 = 113724 - 360t_1 + 10t_2$, que possui solução para quaisquer valores de t_1 e t_2. De fato, temos que $mdc(4, 9) = 1$ e $1 \mid (113724 - 360t_1 + 10t_2)$. De (3.15), segue que

$$1 = 4 \cdot (-2) + 9 \cdot (1). \tag{3.24}$$

Multiplicando ambos os lados de (3.24) por $113724 - 360t_1 + 10t_2$, obtemos

$$\begin{aligned} 113724 - 360t_1 + 10t_2 &= 4 \cdot (-2) \cdot (113724 - 360t_1 + 10t_2) + 9 \cdot (113724 - 360t_1 + 10t_2) \\ &= 4 \cdot (-227448 + 720t_1 - 20t_2) + 9 \cdot (113724 - 360t_1 + 10t_2). \end{aligned}$$

Logo,

$$(-227448 + 720t_1 - 20t_2, 113724 - 360t_1 + 10t_2)$$

é uma solução particular de $4x + 9y = k_2 = 113724 - 360t_1 + 10t_2$, e a solução geral é dada por

$$S_3 = \{(-227448 + 720t_1 - 20t_2 + 9t_3, 113724 - 360t_1 + 10t_2 - 4t_3) |\, t_1, t_2, t_3 \in \mathbb{Z}\}. \tag{3.25}$$

Portanto, de (3.21), (3.23) e (3.25), segue que a solução geral de $4x + 9y + 10z + 40w = 324$ é da forma

$$S = \{(-227448 + 720t_1 - 20t_2 + 9t_3, 113724 - 360t_1 + 10t_2 - 4t_3, -12636 + 40t_1 - t_2, 324 - t_1)\},$$

com $t_1, t_2, t_3 \in \mathbb{Z}$.
Finalmente,o conjunto S é a solução geral da equação dada. □

Capítulo 4

Equações Diofantinas Elementares não Lineares

4.1 As Ternas Pitagóricas

4.1.1 Um Pouco da História

Pitágoras nasceu na ilha de Samos por volta do ano 560 a.C.. Quando jovem, visitou demoradamente o Egito, a Índia e a Mesopotâmia, onde, a par da Matemática, certamente absorveu muito do misticismo desses lugares. Voltando ao mundo greto, fundou em Crotona (sudeste da Itália de hoje) uma escola, na verdade uma sociedade secreta, dedicada ao estudo da Matemática e Filosofia, principalmente.

O Teorema de Pitágoras é um dos mais belos e importantes teoremas da Matemática de todos os tempos e ocupa uma posição especial na história do nosso conhecimento matemático. Foi onde tudo começou. Desde o século 5 a.C. até o século 20 d.C., inúmeras demonstrações do Teorema de Pitágoras apareceram. Por outro lado, é importante destacar que, antes de Pitágoras, os babilônios antigos conheciam o Teorema de Pitágoras. Temos provas concretas deste fato, mas os matemáticos da época não estavam preocupados com demonstrações, na verdade, eles conheciam receitas que davam certo e, com elas, resolviam inúmeros problemas. Já para Pitágoras, a ideia da prova matemática era sagrada, e foi esse tipo de demonstração que permitiu que a Irmandade, escola pitagórica, descobrisse varias coisa. Segue o enunciado do Teorema de Pitágoras: **em qualquer triângulo retângulo, a área do quadrado cujo lado é a hipotenusa é igual à soma das áreas dos quadrados que têm como lado cada um dos catetos**.

Se a é a medida da hipotenusa e se b e c são as medidas dos catetos, o enunciado do Teorema de Pitágoras equivale a afirmar que

$$a^2 = b^2 + c^2. \tag{4.1}$$

Não resta dúvida que os pitagóricos viam o papel dos números no mundo de uma ma-

neira muito especial. Daí não ser surpresa que a aritmética teórica tenha nascido entre eles. Como a escola tratava a matemática de maneira muito filosófica e abstrata, desvinculada das exigências da vida prática, era natural que separassem o estudo teórico dos números, que chamavam aritmética, dos cálculos práticos, que denominavam logística, preocupando-se essencialmente apenas com o primeiro desses aspectos. Considerando o grau de preocupação dos pitagóricos no sentido de ligar os números (naturais) às coisas, especialmente à geometria, era natural esperar que procurassem determinar todos os triângulos retângulos de lados inteiros. Este problema consiste em resolver no conjunto das ternas ordenadas de números naturais não nulos a equação $x^2 + y^2 = z^2$. Uma terna (a, b, c) de números naturais não nulos tal que $a^2 + b^2 = c^2$ chama-se *terna pitagórica*.

Com isso, a escola pitagórica inaugurou o estudo de problemas indeterminados envolvendo números naturais, algo que seria retomado posteriormente, com grande fôlego, por Diofanto de Alexandria (séc. III, d.C.). É importante destacar que os próprios pitagóricos chegaram à fórmula

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

que, para m ímpar, fornece infinitas soluções dessa equação (embora não todas).

Vejamos alguns exemplos:

- Para $m = 3$, obtém-se a terna $(3, 4, 5)$, que satisfaz (4.1). De fato, veja: $3^2 + 4^2 = 9 + 16 = 25 = 5^2$;
- Para $m = 7$, obtém-se a terna $(7, 24, 25)$, que satisfaz (4.1). De fato, veja: $7^2 + 24^2 = 49 + 576 = 625 = 25^2$;
- Para $m = 13$, obtém-se a terna $(13, 84, 85)$, que satisfaz (4.1). De fato, veja: $13^2 + 84^2 = 169 + 7056 = 7225 = 85^2$;
- Para $m = 101$, obtém-se a terna $(101, 5100, 5101)$, que satisfaz (4.1). De fato, veja: $101^2 + 5100^2 = 10201 + 26010000 = 26020201 = 5101^2$.

Utilizamos como referência básica para o exposto acima [2], [10] e [12].

4.1.2 Ternas Pitagóricas

Nesta seção, apresentamos alguns resultados que nos permitem encontrar todas as ternas pitagóricas. Conforme vimos na seção anterior, os pitagóricos conheciam uma fórmula para gerar infinitas ternas pitagóricas (a, b, c). De modo geral, nesta seção, apresentamos as soluções (x, y, z) da equação diofantina $x^2 + y^2 = z^2$, com $x, y, z \in \mathbb{Z}$ e diferentes de zero. Posteriormente, utilizaremos estes resultados para resolver outras equações em números inteiros. Para o que segue, tomamos como referência [6], [8] e [11].

Definição 4.1. *Uma terna de números naturais (x, y, z) chama-se terna pitagórica se*

$$x^2 + y^2 = z^2.$$

Além disso, a terna (x, y, z) chama-se primitiva se $mdc(x, y, z) = 1$.

Como vimos acima $(3, 4, 5), (13, 84, 85)$ e $(101, 5100, 5101)$ são exemplos de ternas pitagóricas.

Proposição 4.2. *Se (x, y, z) é uma terna pitagórica, e $k \geq 1$ é um inteiro, então (kx, ky, kz) também será uma terna pitagórica.*

Demonstração: Com efeito, tomando nos lugares de x e y os valores kx e ky, temos que

$$(kx)^2 + (ky)^2 = k^2x^2 + k^2y^2 = k^2(x^2 + y^2), \tag{4.2}$$

de sorte que, por hipótese (x, y, z) é uma terna pitagórica, isto é, $x^2 + y^2 = z^2$. Assim, das igualdades em (4.2) segue que:

$$(kx)^2 + (ky)^2 = k^2x^2 + k^2y^2 = k^2(x^2 + y^2) = k^2z^2.$$

□

Exemplo 4.3. *Tomemos a terna pitagórica $(3, 4, 5)$. Note que, para $k = 5$ teremos $(15, 20, 25)$, que também é uma terna pitagórica. De fato, vejamos:*

$$15^2 + 20^2 = 225 + 400 = 625 = 25^2.$$

Proposição 4.4. *Os ternos (x, y, z) de inteiros não nulos tais que $x^2 + y^2 = z^2$ são dados por:*

$$x = 2uvd, y = (u^2 - v^2)d, z = (u^2 + v^2)d$$

ou

$$x = (u^2 - v^2)d, y = 2uvd, z = (u^2 + v^2)d,$$

onde k, u e v são inteiros não nulos, com u e v de paridades distintas e primos entre si.

Demonstração: Sem perda de generalidade, podemos supor $x, y, z > 0$. Se $d = mdc(x, y)$, então $d^2 \mid (x^2 + y^2)$, de fato, veja: $d \mid x$ e $d \mid y$, daí $d^2 \mid x^2$ e $d^2 \mid y^2$. Pela Proposição 2.10, segue que $d^2 \mid (x^2 + y^2)$, donde segue que $d^2 \mid z^2$, assim $z^2 = d^2l$ com l inteiro, como z^2 é um quadrado perfeito, então d^2l também deve ser um quadrado perfeito, desta forma $l = m^{2q}$, com m inteiro e $q \in \mathbb{N}$. Existem, portanto, inteiros não nulos a, b e c tais que $mdc(a, b) = 1$ e $(x, y, z) = (da, db, dc)$. Ademais, como

$$x^2 + y^2 = z^2 \Leftrightarrow a^2 + b^2 = c^2.$$

Daí, basta, pois, encontrarmos as soluções inteiras não nulas a, b e c da equação acima, sujeitas à condição $mdc(a, b) = 1$.

As condições $a^2+b^2 = c^2$ e $mdc(a, b) = 1$ nos fornecem os seguintes resultados $mdc(a, c) = mdc(b, c) = 1$. De fato, como a e b são primos entre si, então a^2 e b^2 também são, assim segue o resultado. Agora, vejamos que o quadrado de um inteiro t deixa resto 0 ou 1 quando dividido por 4, conforme t seja respectivamente ímpar ou par. De fato, seja $t = 2k + 1, k \in \mathbb{Z}$. Daí $t^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Agora, se $t = 2k, k \in \mathbb{Z}$, então $t^2 = (2k)^2 = 4k^2 \equiv 0 \pmod 4$. Portanto, se a e b forem ímpares, então $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, ou seja, c^2 deixará resto 2 quando dividido por 4, uma contradição, já que $c^2 \equiv 0 \pmod 4$ ou $c^2 \equiv 1 \pmod 4$. Como $mdc(a, b) = 1$, restam dois casos a considerar: a ímpar e b par ou a par e b ímpar. Analisando o primeiro, temos: Sendo a ímpar e b par, segue de $c^2 = a^2 + b^2$ que c também é ímpar. Por outro lado,

$$b^2 = c^2 - a^2 = (c - a)(c + a). \tag{4.3}$$

Agora, se $d' = mdc(c - a, c + a)$, então, pela Proposição 2.10, segue que d' divide

$$(c + a) + (c - a) = 2c \text{ e } (c + a) - (c - a) = 2a,$$

e, daí, $d' \mid mdc(2a, 2c)$. Mas $mdc(2a, 2c) = 2 \cdot mdc(a, b) = 2 \cdot 1 = 2$; então $d' \mid 2$. Uma vez que, $c - a$ e $c + a$ são ambos pares, pois a e c têm a mesma paridade, segue que $d' = 2$ e podemos escrever (4.3) como

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

Pelo item (ii) do Corolário 2.22, temos que $mdc\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$. Logo $\frac{c+a}{2}$ e $\frac{c-a}{2}$ são primos entre si e seu produto é um quadrado perfeito. Pelo Teorema Fundamental da Aritmética, cada um destes fatores deve ser o quadrado de um número natural. Assim,

$$\begin{aligned} \frac{c+a}{2} = u^2 &\Leftrightarrow c + a = 2u^2 \\ \frac{c-a}{2} = v^2 &\Leftrightarrow c - a = 2v^2 \\ b^2 = 4u^2v^2 &\Leftrightarrow b = 2uv, \end{aligned}$$

com $mdc(u, v) = 1$, pois $mdc(\frac{c-a}{2}, \frac{c+a}{2} = 1$. Escrevendo a, b e c em termos de u e v, obtemos:

$$a = u^2 - v^2, b = 2uv, c = u^2 + v^2. \tag{4.4}$$

Ademais, como $c = u^2 + v^2$ é ímpar, u e v têm paridades distintas.

Analisaremos, agora, o segundo caso, sendo, pois, a par e b ímpar, segue novamente de $c^2 = a^2 + b^2$ que c também é ímpar. Escrevamos agora

$$a^2 = (c - b)(c + b); \tag{4.5}$$

daí, se $d'' = mdc(c - b, c + b)$, então d'' divide

$$(c+b)+(c-b)=2c \text{ e } (c+b)-(c-b)=2b,$$

donde segue que $d'' \mid mdc(2b,2c)=2$. Mas como $c-b$ e $c+b$ são ambos pares, segue que $d''=2$, e podemos escrever (4.5) como

$$\left(\frac{a}{2}\right)^2=\left(\frac{c-b}{2}\right)\left(\frac{c+b}{2}\right),$$

com $mdc\left(\frac{c-b}{2},\frac{c+b}{2}\right)=1$. Logo, $\frac{c+b}{2}$ e $\frac{c-b}{2}$ são primos entre si e seu produto é um quadrado perfeito. Pelo Teorema Fundamental da Aritmética, cada um destes fatores deve ser o quadrado de um número natural. Assim,

$$\begin{aligned}\frac{c+b}{2}=u^2 &\Leftrightarrow c+b=2u^2\\ \frac{c-b}{2}=v^2 &\Leftrightarrow c-b=2v^2\\ a^2=4u^2v^2 &\Leftrightarrow a=2uv,\end{aligned}$$

com $mdc(u,v)=1$. Escrevendo a,b e c em termos de u e v, obtemos:

$$a=2uv, b=u^2-v^2, c=u^2+v^2. \tag{4.6}$$

Por outro lado, como $c=u^2+v^2$ é ímpar, u e v têm paridades distintas.

Finalmente, substituindo (4.4) na equação original, tem-se:

$$\begin{aligned}(u^2-v^2)^2+(2uv)^2 &= (u^2)^2-2u^2v^2+(v^2)^2+4u^2v^2\\ &= (u^2)^2+2u^2v^2+(v^2)^2\\ &= (u^2+v^2)^2.\end{aligned}$$

agora, substituíndo (4.6), tem-se:

$$\begin{aligned}(2uv)^2+(u^2-v^2)^2 &= 4u^2v^2+(u^2)^2-2u^2v^2+(v^2)^2\\ &= (u^2)^2+2u^2v^2+(v^2)^2\\ &= (u^2+v^2)^2.\end{aligned}$$

Portanto, concluímos que as ternas acima são realmente soluções da equação em epígrafe. □

Exemplo 4.5. *Tomemos $u=3$ e $v=2$. Assim, encontramos as ternas pitagóricas $(5,12,13)$ e $(12,5,13)$.*

Veja que:

- $(5,12,13),(10,24,26),\ldots,(5k,12k,13k),\ldots$
- $(12,5,13),(24,10,26),\ldots,(12k,5k,13k),\ldots$

todas são ternas pitagóricas, sendo que $mdc(5, 12, 13) = mdc(12, 5, 13) = 1$.

Agora, vejamos como aplicar o resultado da Proposição 4.4 para encontrar as soluções inteiras de outras equações diofantinas.

Exemplo 4.6. *Ache todas as soluções inteiras não nulas da equação* $x^2 + y^2 = 2z^2$*, com* $x \neq \pm y$*.*

Resolução: Em uma qualquer dessas soluções, x e y devem ter a mesma paridade, ou seja, devemos ter x e y ambos pares ou ambos ímpares, pois, caso contrário, $x^2 + y^2$ seria ímpar. Note que existem inteiros a e b tais que $x = a + b$ e $y = a - b$. De fato, é só fazer $a = \frac{x+y}{2}$ e $b = \frac{x-y}{2}$, com $a, b \in \mathbb{Z} \setminus \{0\}$, pois $x \neq \pm y$. Substituindo tais expressões para x e y na equação original, temos que

$$x^2 + y^2 = (a + b)^2 + (a - b)^2 = 2(a^2 + b^2) = 2z^2 \Leftrightarrow a^2 + b^2 = z^2.$$

Uma vez que essa última equação é correspondente à Equação de Pitágoras, segue da Proposição 4.4 a existência de inteiros não nulos k, u e v, com u e v primos entre si e de paridades distintas, tais que

$$a = 2uvk, b = (u^2 - v^2)k, z = (u^2 + v^2)k$$

ou

$$a = (u^2 - v^2)k, b = 2uvk, z = (u^2 + v^2)k.$$

Portanto, as soluções (x, y, z) da equação original, com $x \neq \pm y$, são de um dos tipos abaixo, onde k, u, v satisfazem as condições acima descritas:

$$x = (u^2 - v^2 + 2uv)k, y = (-u^2 + v^2 + 2uv)k, z = (u^2 + v^2)k$$

ou

$$x = (u^2 - v^2 + 2uv)k, y = (u^2 - v^2 - 2uv)k, z = (u^2 + v^2)k.$$

□

Exemplo 4.7. *Ache todas as soluções inteiras não nulas da equação* $x^2 + y^2 = 5z^2$*.*

Resolução: Primeiramente, note que podemos tomar $x = z$ e $y = 2z$. Daí, segue que

$$x^2 + y^2 = z^2 + (2z)^2 = 5z^2.$$

A igualdade acima fornece uma infinidade de soluções da equação em tela, mas não todas. De fato, a terna $(76, 82, 50)$ é solução da equação dada, veja: $76^2 + 82^2 = 5776 + 6724 = 12500 = 5 \cdot 50^2 = 5 \cdot 2500$. No entanto, não obedece à regra acima.

Por outro lado, tomando x e y com paridades distintas, teremos z ímpar. Assim, podemos utilizar o resultado da Proposição 4.4 na solução da equação em epígrafe. De sorte que existem

inteiros a e b não nulos, de modo que $x = 2a + b$ e $y = a - 2b$. De fato, é só fazer $a = \frac{2x+y}{5}$ e $b = \frac{x-2y}{5}$, de modo que $2x + y = 5m$ e $x - 2y = 5n$, com $m, n \in \mathbb{Z} \setminus \{0\}$. Substituindo temos que

$$x^2 + y^2 = (2a + b)^2 + (a - 2b)^2 = 5(a^2 + b^2) = 5z^2 \Leftrightarrow a^2 + b^2 = z^2.$$

Observemos que a última equação é correspondente a Equação de Pitágoras se $a, b \in \mathbb{Z}$. Daí, segue da Proposição 4.4 a existência de inteiros não nulos k, u e v, com u e v primos entre si e de paridades distintas, tais que

$$a = 2uvk, b = (u^2 - v^2)k, z = (u^2 + v^2)k$$

ou

$$a = (u^2 - v^2)k, b = 2uvk, z = (u^2 + v^2)k.$$

Portanto, conseguimos novamente uma infinidade de ternas (x, y, z), não todas, da equação original que podem ser dadas de um dos tipos abaixo, onde k, u, v satisfazem as condições acima descritas:

$$x = (u^2 - v^2 + 4uv)k, y = (-2u^2 + 2v^2 + 2uv)k, z = (u^2 + v^2)k$$

ou

$$x = (2u^2 - 2v^2 + 2uv)k, y = (u^2 - v^2 - 4uv)k, z = (u^2 + v^2)k.$$

Deixamos como desafio ao leitor encontrar uma fórmula que gere todas as soluções da equação dada, a partir da equação de Pitágoras. □

4.1.3 Outras Equações Diofantinas não Lineares

Nesta seção, discutiremos acerca da solubilidade de algumas equações diofantinas elementares não lineares, para tal, utilizaremos as propriedades das congruência.

Exemplo 4.8. *Mostre que a equação $x^2+y^2 = 2z+3$ possui infinitas soluções inteiras positivas.*

Resolução: Primeiramente, veja que:

$$x^2 + y^2 = 2z + 3 \Leftrightarrow x^2 + y^2 - 2z = 3.$$

Observe que como 2 é um múltiplo de 2, qualquer solução inteira positiva da equação dada deve satisfazer

$$x^2 + y^2 - 2z \equiv 3 \pmod 2 \Leftrightarrow x^2 + y^2 \equiv 1 \pmod 2. \tag{4.7}$$

De (4.7), segue que x e y devem ter paridades distintas, pois, caso contrário, $x^2 + y^2$ seria par, e teríamos $x^2 + y^2 \equiv 0 \pmod 2$. Considere o caso em que $x = 2q$ e $y = 2q + 1$, com q inteiro positivo. Agora, substituindo esses valores na equação, original temos que

$$\begin{aligned}(2q)^2 + (2q+1)^2 = 2z + 3 &\Leftrightarrow 4q^2 + 4q^2 + 4q + 1 - 3 = 2z \\ &\Leftrightarrow z = 4q^2 + 2q - 1.\end{aligned}$$

Portanto, as ternas $(2q, 2q + 1, 4q^2 + 2q - 1)$ são soluções de $x^2 + y^2 = 2z + 3$, para todo q inteiro positivo. □

Exemplo 4.9. *Mostre que a equação $x^2 + y^2 = 4z + 3$ não possui soluções inteiras x e y.*

Resolução: Observe que como 4 é múltiplo de 4, qualquer solução inteira deve satisfazer

$$x^2 + y^2 = 4z + 3 \equiv 3 \pmod 4 \Leftrightarrow x^2 + y^2 \equiv 3 \pmod 4.$$

Por outro lado, vejamos que:

$$\begin{aligned}x \equiv 0 \pmod 4 &\Rightarrow x^2 \equiv 0 \pmod 4, \\ x \equiv 1 \pmod 4 &\Rightarrow x^2 \equiv 1 \pmod 4, \\ x \equiv 2 \pmod 4 &\Rightarrow x^2 \equiv 4 \equiv 0 \pmod 4, \\ x \equiv 3 \pmod 4 &\Rightarrow x^2 \equiv 9 \equiv 1 \pmod 4.\end{aligned}$$

o mesmo é válido para y. Logo, $x^2 + y^2$ só pode deixar resto $0, 1$ ou 2 na divisão por 4. Assim, $x^2 + y^2 \equiv 3 \pmod 4$ é impossível, e a equação não possui soluções inteiras. □

Exemplo 4.10. *Mostre que a equação $x^2 = 3y^2 + 8$ não possui soluções inteiras x e y.*

Resolução: De fato, olhando módulo 3, temos que

$$x^2 = 3y^2 + 8 \equiv 8 \pmod 3 \Leftrightarrow x^2 = 3y^2 + 8 \equiv 2 \pmod 3. \tag{4.8}$$

Por outro lado,

$$\begin{aligned}x \equiv 0 \pmod 3 &\Rightarrow x^2 \equiv 0 \pmod 3, \\ x \equiv 1 \pmod 3 &\Rightarrow x^2 \equiv 1 \pmod 3, \\ x \equiv 2 \pmod 3 &\Rightarrow x^2 \equiv 4 \equiv 1 \pmod 3.\end{aligned}$$

Portanto, conforme acima, vemos que a aquação dada não possui soluções inteiras. □

4.2 Equação de Pell

Nesta seção, discutimos um caso das equações diofantinas do tipo

$$x^2 - dy^2 = 1, \tag{4.9}$$

no caso em que d é um inteiro positivo, com x e y inteiros. Veja que, se d é um quadrado perfeito, digamos $d = k^2$, temos que $x^2 - dy^2 = (x^2 - k^2y^2) = (x + ky)(x - ky) = 1$ a equação (4.9) admite apenas as soluções $y = 0, x = \pm 1$, pois teríamos

$$x - ky = x + ky = \pm 1.$$

Neste caso,

$$x = \frac{(x + ky) + (x - ky)}{2} = \pm 1, y = 0.$$

Portanto, o caso interessante é quando d não é um quadrado perfeito, desta forma $\sqrt{d}$ é um irracional. De fato, se $\sqrt{d} = \frac{p}{q}$, com $mdc(p, q) = 1$ e $q > 1$, teríamos $d = \frac{p^2}{q^2}$ o que é um absurdo, porque por hipótese $mdc(p, q) = 1 \Rightarrow mdc(p^2, q^2) = 1$, donde segue que $\frac{p^2}{q^2}$ não pode ser inteiro. Nesse caso, a equação $x^2 - dy^2 = 1$ corresponde a pontos inteiros sobre uma hipérbole.

Segue, abaixo, o exemplo da qual nos referimos acima.

Exemplo 4.11. *A equação $x^2 - 2y^2 = 1$ possui uma infinidade de soluções inteiras positivas.*

Resolução: Primeiramente, note que $x = 3, y = 2$ e $x = 17, y = 12$ são soluções da equação em tela. De fato,

$$\begin{aligned} x = 3,\ y = 2 \ &\Rightarrow\ 3^2 - 2 \cdot 2^2 = 9 - 8 = 1, \\ x = 17,\ y = 12 \ &\Rightarrow\ 17^2 - 2 \cdot 12^2 = 289 - 288 = 1. \end{aligned}$$

Agora, seja (a, b) uma solução não nula da equação dada, ou seja, $a^2 - 2b^2 = 1$. Daí,

$$(a + b\sqrt{2})(a - b\sqrt{2}) = 1. \tag{4.10}$$

e, assim, elevando ao quadrado ambos os membros de (4.10), temos

$$(a + b\sqrt{2})^2(a - b\sqrt{2})^2 = 1.$$

Desenvolvendo os binômios, chegamos a

$$(a^2 + 2b^2 + 2ab\sqrt{2})(a^2 + 2b^2 - 2ab\sqrt{2}) = 1$$

ou, ainda, a

$$(a^2 + 2b^2)^2 - 2(2ab)^2 = 1.$$

Portanto, $(a^2+2b^2, 2ab)$ também será solução da equação.

Agora, vamos elevar ao cubo ambos os membros de (4.10). Obtemos

$$(a+b\sqrt{2})^3(a-b\sqrt{2})^3 = 1.$$

Desenvolvendo os binômios, temos

$$(a^3+3a^2b\sqrt{2}+6ab^2+2b^3\sqrt{2})(a^3-3a^2b\sqrt{2}+6ab^2-2b^3\sqrt{2}) = 1$$

$$\Updownarrow$$

$$(a^3+6ab^2+3a^2b\sqrt{2}+2b^3\sqrt{2})(a^3+6ab^2-3a^2b\sqrt{2}-2b^3\sqrt{2}) = 1$$

donde

$$(a^3+6ab^2)^2 - 2(3a^2b+2b^3)^2 = 1.$$

Logo, $(a^3+6ab^2, 3a^2b+2b^3)$ também é solução da equação.

Seguindo este raciocínio, vamos elevar a 4 ambos os membros de (4.10). Tem-se:

$$(a+b\sqrt{2})^4(a-b\sqrt{2})^4 = 1.$$

Veja que

$$\begin{aligned}(a+b\sqrt{2})^4 &= \sum_{j=0}^{n=4}\binom{n}{j}a^{n-j}(b\sqrt{2})^j \\ &= \binom{4}{0}a^4+\binom{4}{1}a^3(b\sqrt{2})+\binom{4}{2}a^2(b\sqrt{2})^2+\binom{4}{3}a(b\sqrt{2})^3+\binom{4}{4}(b\sqrt{2})^4 \\ &= a^4+4a^3b\sqrt{2}+12a^2b^2+8ab^3\sqrt{2}+4b^4, \qquad (4.11)\end{aligned}$$

$$\begin{aligned}(a-b\sqrt{2})^4 &= \sum_{j=0}^{n=4}\binom{n}{j}a^{n-j}(-b\sqrt{2})^j \\ &= \binom{4}{0}a^4-\binom{4}{1}a^3(b\sqrt{2})+\binom{4}{2}a^2(b\sqrt{2})^2-\binom{4}{3}a(b\sqrt{2})^3+\binom{4}{4}(b\sqrt{2})^4 \\ &= a^4-4a^3b\sqrt{2}+12a^2b^2-8ab^3\sqrt{2}+4b^4. \qquad (4.12)\end{aligned}$$

De (4.11) e (4.12), temos que

$$(a^4+4a^3b\sqrt{2}+12a^2b^2+8ab^3\sqrt{2}+4b^4)(a^4-4a^3b\sqrt{2}+12a^2b^2-8ab^3\sqrt{2}+4b^4) = 1$$

$$\Updownarrow$$

$$(a^4+12a^2b^2+4b^4+4a^3b\sqrt{2}+8ab^3\sqrt{2})(a^4+12a^2b^2+4b^4-4a^3b\sqrt{2}-8ab^3\sqrt{2}) = 1,$$

o que é o mesmo que

$$(a^4+12a^2b^2+4b^4)^2 - 2(4a^3b+8ab^3)^2 = 1.$$

Portanto, $(a^4 + 12a^2b^2 + 4b^4, 4a^3b + 8ab^3)$ também é uma solução da equação dada.

Finalmente,vamos elevar a n ambos os lados de (4.10). Temos

$$(a + b\sqrt{2})^n(a - b\sqrt{2})^n = 1. \tag{4.13}$$

Desenvolvendo o binômio $(a + b\sqrt{2})^n$, obtemos

$$(a + b\sqrt{2})^n = \sum_{\substack{0\leq j\leq n\\ 2|j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^j} + \sqrt{2}\sum_{\substack{0\leq j\leq n\\ 2\nmid j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^{j-1}}.$$

Fazendo

$$c = \sum_{\substack{0\leq j\leq n\\ 2|j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^j} \text{ e } d = \sum_{\substack{0\leq j\leq n\\ 2\nmid j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^{j-1}},$$

é imediato que $c, d \in \mathbb{Z}$ (uma vez que $\sqrt{2^j}$ é inteiro para j par, e $\sqrt{2^{j-1}}$ é inteiro para j ímpar, já que $j - 1$ neste caso é par).

Desenvolvendo o binômio $(a - b\sqrt{2})^n$, obtemos

$$(a - b\sqrt{2})^n = \sum_{\substack{0\leq j\leq n\\ 2|j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^j} - \sqrt{2}\sum_{\substack{0\leq j\leq n\\ 2\nmid j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^{j-1}}.$$

Agora, veja que podemos escrever (4.13) da forma

$$\begin{aligned}(a + b\sqrt{2})^n(a - b\sqrt{2})^n &= (c + d\sqrt{2})(c - d\sqrt{2})\\ &= c^2 - 2d^2 = 1.\end{aligned}$$

Portanto,

$$(c, d) = \left(\sum_{\substack{0\leq j\leq n\\ 2|j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^j}, \sum_{\substack{0\leq j\leq n\\ 2\nmid j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^{j-1}}\right),$$

é solução da equação em epígrafe.

Desses resultados podemos concluir que a equção $x^2 - 2y^2 = 1$ possui uma infinidade de soluções inteiras positivas. De fato, basta repetir o argumento acima sucessivas vezes. Veja também que, sendo a e b naturais, temos

$$a < a^2 + 2b^2 < a^3 + 6ab^3 < a^4 + 12a^2b^2 + 4b^4 < \cdots < \sum_{\substack{0\leq j\leq n\\ 2|j}} \binom{n}{j} a^{n-j}b^j\sqrt{2^j} < \cdots < \cdots .$$

□

Capítulo 5

Considerações Finais

Nesse trabalho apresentamos como é possível encontrar as soluções de uma equação diofantina linear que contenha um número qualquer de incógnitas. Sendo assim, fizemos um estudo sobre algumas propriedades aritméticas relativas a números inteiros, como a divisibilidade, o algoritmo de Euclides, o teorema de Bèzout, números primos, congruência, entre outros. Para uma melhor compreensão da técnica apresentada, iniciamos abordando as equações diofantinas lineares a duas incógnitas e a três incógnitas, para, posteriormente, generalizarmos os resultados em epígrafe.

Apresentamos também um resultado que nos permite encontrar todas as ternas pitagóricas, em números inteiros. Para tal, utilizamos uma série de resultados aqui apresentados, como, por exemplo, propriedades do máximo divisor comum, Teorema Fundamental da Aritmética, e outros. Discutimos também acerca da solubilidade de algumas equações diofantinas não lineares, desta abordagem, percebemos que cada equação apresenta característica específicas, das quais devemos buscar identificá-las.

Compreendo como relevante a discussão do tema em tela, mais ainda, pelo fato da disciplina *Teoria Elementar dos Números* não constar como obrigatória no programa do curso de Licenciatura em Matemática da Fundação Universidade Federal do Tocantins, campus de Araguaína.

Referências

[1] CAMPOS, G. D. M. **Equações diofantinas lineares**. 2013. 68f. Dissertação (Mestrado Profissional em Matemática) - Instituto de Ciências Exatas e da Terra, Universidade Federal de Mato Grosso, Cuiabá - MT. Disponível em: $< http : //bit.profmat - sbm.org.br/xmlui/bitstream/handle/123456789/558/2011\_00462\_GISELI\_DUARDO\_MACIANO\_CAMPOS.pdf?sequence = 1 >$. Acesso em, 20 de set. 2016.

[2] DOMINGUES, H. H. **Fundamentos de Aritmética**. São Paulo: Atual, 1991.

[3] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**: Volume único. 4. ed. São Paulo: Atual, 2003.

[4] HEFEZ, A. **Iniciação à Aritmética**. Rio de Janeiro: IMPA, 2015.

[5] LANDAU, E. G. H. **Teoria elementar dos números**. Tradução de Paulo Henrique Viana de Barros. Rio de Janeiro: Editora Ciência Moderna, 2002, Coleção Clássicos da Matemática.

[6] MARTINEZ, F. B. et al. **Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro**. 4. ed. Rio de Janeiro: IMPA, 2015, Projeto Euclides.

[7] MUNIZ NETO, A. C. **Tópicos de matemática elementar**. vol. 1. 2.ed. Rio de Janeiro: SBM, 2013, Coleção Professor de Matemática.

[8] MUNIZ NETO, A. C. **Tópicos de matemática elementar**. vol. 5. 2.ed. Rio de Janeiro: SBM, 2012, Coleção Professor de Matemática.

[9] SANTOS, J. P. de O. **Introdução a teoria dos números**. Rio de Janeiro: IMPA, 2006.

[10] SINGH, S. **O último teorema de Fermat**. Tradução de Jorge Luiz Calife. 7.ed. Rio de Janeiro: Record, 2000.

[11] SOUZA, R. S. de. **Equações diofantinas lineares, quadráticas e aplicações**. 2017. 75f. Dissertação (Mestrado) - Instituto de Geociências e Ciências Exatas,

Universidade Estadual Paulista, Rio Claro - SP. Disponível em: $< https : //repositorio.unesp.br/bitstream/handle/11449/149949/souza\_rs\_me\_rcla.pdf?sequence = 5isAllowed = y >$. Acesso em, 12 de abr. 2017.

[12] WAGNER, E. **Teorema de Pitágoras e Áreas**. Rio de Janeiro: IMPA, 2009.