Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Equações Diofantinas Lineares, Quadráticas e Aplicações

Romario Sidrone de Souza

Dissertação apresentada ao Programa de Pós-Graduação em Matemática como requisito parcial para a obtenção do grau de Mestre

Orientadora
Profa. Dra. Carina Alves

2017

512.7 Souza, Romario Sidrone de
S729e Equações diofantinas lineares, quadráticas e aplicações / Romario Sidrone de Souza. - Rio Claro, 2017
75 f. : il., figs., gráfs., tabs.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientador: Carina Alvez

1. Teoria dos números. 2. Álgebra. 3. Diofanto. 4. Equações quadráticas. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Romario Sidrone de Souza

Equações Diofantinas Lineares, Quadráticas e Aplicações

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação em Matemática do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Carina Alves
Orientadora

Profa. Dra. Eliris Cristina Rizziolli
Depto. de Matemática -UNESP/Rio Claro

Profa. Dra. Cintya Wink de Oliveira Benedito
UNESP/São João da Boa Vista

Rio Claro, 07 de março de 2017.

A Deus.
À minha família.
Aos meus professores.
Aos meus amigos.

Agradecimentos

Agradeço a Deus por tudo que tem feito em minha vida, me protegendo e me permitindo chegar até aqui.

Agradeço a minha mãe pela educação e incentivo para nunca desistir dos meus sonhos.

Ao meus fieis amigos, que estiveram presentes, que sempre participaram dos momentos bons e ruins da minha vida, contribuindo para que os dias fossem os melhores possíveis.

À minha orientadora, Profa. Dra. Carina Alves, pela paciência e dedicação.

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

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

O sucesso é ir de fracasso em fracasso sem perder o entusiasmo.
Winston Churchill

Resumo

Este trabalho é resultado de uma pesquisa bibliográfica sobre Diofanto e as equações que levam seu nome, as equações diofantinas. Mais especificamente, apresentamos as equações diofantinas lineares e alguns casos particulares das equações diofantinas quadráticas. Ainda, abordamos um estudo sobre alguns tópicos de teoria dos números e frações contínuas, afim de facilitar o entendimento sobre os teoremas e resultados acerca do tema central deste trabalho.

Palavras-chave: Álgebra, Diofanto, Equações Diofantinas, Teoria dos Números.

Abstract

This work is the result of a bibliographical research about Diophantus and the equations that take his name, the Diophantine equations. More specifically, we present the linear diophantine equations and some particular cases of the quadratic diophantine equations. We have also studied topics about number theory and continuous fractions, in order to facilitate the understanding of theorems and results that are related to the central theme of this work.

Keywords: Algebra, Diophantus, Diophantine Equations, Number Theory.

Sumário

1 Introdução

A Teoria dos Números (ou Aritmética dos Números) é uma área da Matemática que estuda propriedades de números em geral e, particularmente, dos números inteiros. Inserido na Teoria dos Números, encontra-se o estudo das equações da forma

$$f(x_1, x_2, \ldots, x_n) = 0,$$

onde f é uma função polinomial de n variáveis, com $n \geq 2$, e $x_1, x_2, \ldots, x_n$ assumem apenas valores inteiros. Esse estudo é conhecido como, o estudo das equações diofantinas, em homenagem a Diofanto de Alexandria, matemático pouco conhecido, mas que com seu livro *Arithmetica*, ou melhor parte dele, pois se conhece apenas um percentual da coleção, introduziu o uso de símbolos na resolução de equações. Entre as "Equações Diofantinas" mais famosas, encontra-se a equação $x^n + y^n = z^n$. Muitos matemáticos estudaram essa equação ao longo da história, entre eles o matemático francês, Pierre de Fermat, que após ler a obra *Arithmetica* de Diofanto, sugeriu que as equações do tipo $x^n + y^n = z^n$, não possuem soluções com valores inteiros e positivos para x, y e z, quando n for um inteiro maior do que 2. Vale salientar que, nesse trabalho fizemos um estudo apenas das equações diofantinas lineares e alguns casos mais famosos das equações diofantinas quadráticas.

Nosso trabalho esta delineado conforme segue.

No Capítulo 2, enunciamos e demonstramos alguns resultados de Teoria dos Números, como a divisibilidade, algoritmo de Euclides, identidade de Bézout, o teorema fundamental da aritmética, congruência, entre outros, os quais foram de grande importância para compreensão de algumas demonstrações que envolveram a teoria sobre as equações diofantinas.

No Capítulo 3, apresentamos um breve apanhado histórico acerca de Diofanto e como iniciou seu trabalho sobre as equações que hoje levam seu nome. Dentre os matemáticos que estudaram a Teoria dos Números, sem dúvida, Diofanto foi um dos mais importantes. O pioneirismo de Diofanto se dá no uso sistemático de abreviações para potências de números e para relações e operações.

No Capítulo 4, definimos as equações diofantinas lineares, as quais são equações que apresentam coeficientes e soluções no conjunto dos números inteiros. Demonstramos as principais propriedades que as envolvem e aplicações que fazem uso de tais propri-

edades. Mostramos como encontrar a solução geral de uma equação diofantina linear com duas e três variáveis e também abordamos um método de resolução das equações diofantinas lineares com n variáveis. Ainda, aplicamos os conhecimentos e técnicas, apresentadas nesse capítulo, na interpretação e resolução de problemas presentes em nosso cotidiano, que envolvem tais equações.

No Capítulo 5, estudamos dois casos específicos de equações diofantinas quadráticas. Sendo o primeiro, a equação $x^2 + y^2 = z^2$ também conhecida como *Teorema de Pitágoras*, porém, como este estudo se trata das equações diofantinas, os valores de x, y e z são todos números inteiros. Já o segundo caso, se trata da *Equação de Pell*: $x^2 - Ay^2 = 1$, em que x, y são inteiros e A é um inteiro positivo diferente de zero. Para o estudo da equação de Pell, foi necessário introduzir o conceitos sobre frações contínuas, as quais nos permite representar um número racional por uma sequência finita de inteiros e também um número irracional por uma sequência infinita de inteiros.

2 Tópicos de Teoria dos Números

Neste capítulo, demos enfoque a alguns tópicos da Teoria dos Números que serviram como embasamento teórico para o estudo das equações diofantinas lineares e quadráticas. Tal estudo nos permitiu compreender os métodos algébricos que nos fornecem não apenas uma, mas todas as soluções inteiras para essas equações, sendo a fundamentação teórica baseada principalmente em [4], [7] e [11].

2.1 Princípio da Boa Ordem

O *Princípio da Boa Ordenação* ou *Princípio da Boa Ordem* diz que todo subconjunto não-vazio formado por números naturais possui um menor elemento.

Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades:

i) $a \in S$,

ii) $\forall n \in S, a \leq n$.

Se S possui um menor elemento, então ele único. De fato, se a e a' são menores elementos de S, então $a \leq a'$ e $a' \leq a$, o que implica que, $a = a'$.

Teorema 2.1. *(Princípio da Boa Ordem) Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Demonstração. Seja S um subconjunto não vazio de $\mathbb{N}$ e suponha, por absurdo, que S não possui um menor elemento.

Considere o conjunto T, complementar de S em $\mathbb{N}$. Queremos, portanto, mostrar que $T = \mathbb{N}$. Seja o conjunto

$$I_n = \{k \in \mathbb{N}; k \leq n\},$$

e considere a sentença aberta

$$P(n) : I_n \subset T.$$

Como $1 \leq n$ para todo n, segue-se que $1 \in T$, pois, caso contrário, 1 seria um menor elemento de S. Logo, $P(1)$ é verdadeira.

Suponhamos agora que $P(n)$ seja verdadeira. Se $n+1 \in S$, como nenhum elemento de I_n está em S, teríamos que $n+1$ é um menor elemento de S, o que não é permitido. Logo, $n+1 \in T$, seguindo daí que

$$I_{n+1} = I_n \cup \{n+1\} \subset T,$$

o que prova que $\forall n, I_n \subset T$. Portanto, $\mathbb{N} \subset T \subset \mathbb{N}$ e consequentemente, $T = \mathbb{N}$. Se $T = \mathbb{N}$ então S é vazio e isto é uma contradição. Portanto $\mathbb{N}$ é vazio. □

Teorema 2.2. *(Princípio da Indução Finita). Seja $P(n)$ uma sentença aberta sobre $\mathbb{N}$. Suponha que*

i. $P(1)$ é verdadeira; e

ii. qualquer que seja $n \in \mathbb{N}$, sempre que $P(n)$ é verdadeira, segue que $P(n+1)$ é verdadeira.

Então, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Exemplo 2.1. Mostramos que, para todo inteiro positivo n,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{2.1}$$

Observemos que $P(1)$ é verdadeira, já que a Equação (2.1) é trivialmente válida para $n = 1$. Suponhamos agora que, para algum n natural, $P(n)$ seja verdadeira; ou seja, que

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

Queremos provar que $P(n+1)$ é verdadeira. Somando $n+1$ a ambos os lados da igualdade acima, obtemos a igualdade também verdadeira:

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

Isso mostra que $P(n+1)$ é verdadeira, toda vez que $P(n)$ é verdadeira. Pelo Teorema (2.2), a Equação (2.1) é válida para todo número natural $n \geq 1$.

2.2 Divisibilidade em $\mathbb{Z}$

O conjunto dos números inteiros é denotado por $\mathbb{Z}$, isto é, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Este conjunto é munido de diversas propriedades e definições, porém, apresentamos apenas algumas, as quais são essenciais para o desenvolvimento deste trabalho.

Definição 2.1. *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, e escrevemos $a \mid b$, se existir $k \in \mathbb{Z}$ tal que $b = ak$. Caso a não divida b, escrevemos $a \nmid b$.*

Seja a um inteiro não nulo. Se a dividir b, dizemos que a é um divisor de b, que b é divisível por a ou ainda que b é um múltiplo de a. Se $a \mid b$ e $a > 0$, então a é um divisor positivo de b. Notemos que todo inteiro não nulo é um divisor de si mesmo e de 0.

Exemplo 2.2. $5 \mid 20$ pois existe um inteiro $k = 4$ tal que $20 = 5 \cdot 4$

Exemplo 2.3. $5 \nmid 12$ pois não existe um inteiro k tal que $12 = 5 \cdot k$

Proposição 2.1. *Se a, b e c são inteiros, tais que $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Sejam a, b e c inteiros. Como $a \mid b$ e $b \mid c$, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = bk_2$. Logo, $c = (ak_1)k_2 = a(k_1k_2)$ e, portanto, $a \mid c$. □

Exemplo 2.4. Como $2 \mid 6$ e $6 \mid 12$, então $2 \mid 12$.

Proposição 2.2. *Se a, b e c são inteiros, tais que $a \mid b$ e $a \mid c$, então $a \mid (mb + nc)$, para quaisquer $m, n \in \mathbb{Z}$.*

Demonstração. Sejam a, b e c inteiros. Como $a|b$ e $a|c$, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = ak_2$. Multiplicando ambas as equações respectivamente por m e n obtemos $mb = mak_1$ e $nc = nak_2$. Logo, $mb + nc = mak_1 + nak_2 = a(mk_1 + nk_2)$. Portanto, $a \mid (mb + nc)$. □

Exemplo 2.5. Como $4 \mid 12$ e $4 \mid 16$, então $4 \mid (5 \cdot 12 + (-3) \cdot 16) = 12$.

Teorema 2.3. *(Algoritmo da Divisão em $\mathbb{Z}$) Dados $a, b \in \mathbb{Z}, b > 0$, existe um único par de inteiros q e r que satisfazem*

$$a = q \cdot b + r, \text{ com } 0 \leq r < b.$$

Demonstração. Seja b um número inteiro positivo não nulo. Se $a \in \mathbb{Z}$, então a é múltiplo de b ou está situado entre dois múltiplos consecutivos de b, isto é, $qb \leq a < (q+1)b$. Somando $-qb$ em todos os termos da desigualdade obtemos $qb - qb \leq a - qb < qb + b - qb \rightarrow 0 \leq a - qb < b$. Desta forma, tomando $r = a - qb$, segue que $a = qb + r$, em que $0 \leq r < b$.

Suponhamos agora, que existam inteiros q_1, q_2, r_1, r_2 , onde $q_1 \neq q_2$ e $r_1 \neq r_2$ e que satisfaçam às igualdades: $a = q_1b + r_1$, com $0 \leq r_1 < b$ e $a = q_2b + r_2$, com $0 \leq r_2 < b$. Se $b > r_1$ e $b > r_2$, então $b > r_2 - r_1$ e $a = bq_1 + r_1 = bq_2 + r_2$. Dessa forma, $b(q_2 - q_1) = r_2 - r_1$. Tomando $k = (q_2 - q_1)$, segue que $r_2 - r_1 = kb$, com $k \in \mathbb{Z}$ e daí $b \mid (r_2 - r_1)$. Portanto $b \leq (r_2 - r_1)$, o que é um absurdo, pois contradiz a hipótese. Logo, $r_2 = r_1$. Concluímos que $(q_2 - q_1)b = 0$. Sendo $b \neq 0$, temos que $(q_2 - q_1) = 0$ e concluímos que $q_2 = q_1$. □

Na equação $a = q \cdot b + r$, com $0 \leq r < b$, os inteiros, q e r são chamados respectivamente de *quociente* e *resto* da divisão de a por b. Vale lembrar que b somente é divisor de a se $r = 0$. Neste caso, temos que $a = bq$ e o quociente q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$ ou a/b.

Exemplo 2.6. Sabe-se que na divisão de 326 por $b > 0$, o quociente é 14 e o resto é r. Vejamos como determinar os possíveis valores de b e r.

Sabemos que $a = qb + r, 0 \leq r < b$. Assim, substituindo os valores dados, obtemos:

$$326 = 14b + r, 0 \leq r < b \rightarrow r = 326 - 14b.$$

Logo,

$$0 \leq r < b \rightarrow 0 \leq 326 - 14b < b.$$

Resolvendo essa desigualdade temos:

$$\begin{cases} 0 \leq 326 - 14b \rightarrow b \leq 23,2; \\ 326 - 14b < b \rightarrow b > 21,7. \end{cases}$$

Dessa forma, os possíveis valores para b e r são:

$$\begin{cases} b = 22 \quad e \quad r = 18 \\ ou \\ b = 23 \quad e \quad r = 4. \end{cases}$$

Exemplo 2.7. Sejam $a = 47$ e $b = 6$. Verifiquemos se a é um múltiplo de b ou, caso não seja, determinemos os múltiplos consecutivos em que a se situa.

Como não existe um inteiro k de forma que $47 = 6 \cdot k$, concluímos que 47 não é múltiplo de 6. Assim,

$$47 = 6 \cdot (7) + 5 \rightarrow 6 \cdot (7) < 47 < 6 \cdot (8).$$

Portanto, $q = 7$ e $(q + 1) = 8$.

2.3 Máximo Divisor Comum

Quando falamos em máximo divisor comum de dois números inteiros, estamos interessados em encontrar o maior inteiro que divide esses dois números. Por exemplo, sabemos que o número inteiro 6 divide 18 e também divide 12 e, além disso, como podemos verificar, 6 é o maior número inteiro positivo com essa propriedade. Sendo assim, dizemos, que 6 é o máximo divisor comum de 18 e 12, podendo ser denotado por $(18, 12) = 6$ ou $mdc(18, 12) = 6$, isto nos leva a seguinte definição.

Definição 2.2. *O máximo divisor comum (mdc) de dois inteiros a e b (a e b diferentes de zero), denotado por $mdc(a, b)$, é o maior inteiro que divide a e b. Sendo assim, o $mdc(a, b)$ é o inteiro positivo d que satisfaz às condições:*

1. *$d \mid a$ e $d \mid b$;*

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

Pela condição 1 da Definição 2.2, d é um divisor comum de a e b, e pela condição 2 d é o maior dentre todos os divisores comuns de a e b.

Exemplo 2.8. Sejam $a = 16$ e $b = 54$. Vamos determinar $mdc(16, 54)$.

O conjunto dos divisores de $a = 16$ e de $b = 54$, os quais denotamos por D_{16} e D_{54}, são: $D_{16} = \{\pm1, \pm2, \pm3, \pm4, \pm8, \pm16\}$ e $D_{54} = \{\pm1, \pm2, \pm3, \pm6, \pm9, \pm18, \pm27, \pm54\}$. Como $mdc(12, 54)$ é o maior inteiro que divide 12 e 54, para encontrar o máximo divisor comum entre estes números, basta determinar a intersecção $D_{12} \cap D_{54}$ e tomar o maior número em módulo desse conjunto. Logo, $D_{16,54} = D_{16} \cap D_{54} = \{\pm1, \pm2, \pm3\}$, que tem máximo igual a 3, que é o $mdc(16, 54)$.

Definição 2.3. *Sejam a e b dois inteiros não nulos. Dizemos que a e b são primos entre si se, e somente se, $mdc(a, b) = 1$.*

Exemplo 2.9. Os inteiros 3 e 7, 9 e 11 são *primos entre si*, pois, temos:

$$mdc(3, 7) = mdc(9, 11) = 1.$$

Proposição 2.3. *(Identidade de Bézout[1]) Seja $d = mdc(a, b)$, então existem $n_0, m_0 \in \mathbb{Z}$ tais que $d = n_0a + m_0b$, ou seja, d é uma combinação linear de a e b.*

Demonstração. Seja o conjunto $B = \{na + mb \mid n, m \in \mathbb{Z}\}$. Veja que $B \neq \emptyset$. Sejam $n_0, m_0 \in \mathbb{Z}$ tais que $c = n_0a + m_0b$ é o menor inteiro positivo pertencente a B, vamos provar que $c \mid a$ e $c \mid b$. Para tanto, suponhamos que $c \nmid a$.

Pelo algoritmo da divisão, existem q e r inteiros, tais que $a = qc + r$, $0 \leq r < c$. Tomando $r = a - qc = a - q(n_0a + m_0b) = a(1 - n_0q) + b(-m_0q)$, ou seja, r é um número inteiro positivo e $r \in B$ uma vez que, $(1 - n_0q)$ e $(-m_0q) \in \mathbb{Z}$. Daí, temos que, $r \geq c$. Mas, do Teorema 2.3, $r < c$, o que é um absurdo. Logo, $c \mid a$. Analogamente, mostramos que $c \mid b$. Assim, c é um divisor comum, e como $d = mdc(a, b)$, temos que $c \leq d$.

Resta ainda, mostrar que $d = n_0a + m_0b$. Vejamos que, se $d = mdc(a, b)$ então $d \mid a$ e $d \mid b$, o que implica que $a = k_1d$ e $b = k_2d$ com $k_1, k_2 \in \mathbb{Z}$. Ainda, tomando $c = n_0a + m_0b = n_0(k_1d) + m_0(k_2d) = d(n_0k_1 + m_0k_2)$, resulta em $d \mid c$. Além disso, $c \neq 0 \rightarrow| \ d \ |\leq| \ c \ |$ e como não é possível termos $d < c$, uma vez que $d = mdc(a, b)$, então $d = c$, ou seja, $d = n_0a + m_0b$. □

Proposição 2.4. *Sejam a e b números inteiros positivos. Se existem inteiros q e r tais que $a = bq + r, 0 \leq r < b$, então $mdc(a, b) = mdc(b, r)$.*

Demonstração. Sejam

[1]Étienne Bézout (1730-1783 d.C.): Matemático francês, nascido em 31 de Março de 1930 na cidade Avon-França. Em 1758 Bézout foi eleito adjunto em mecânica da Académie dês Sciences. Dentre diversos outros trabalhos, escreveu Théorie générale des équations algébriques, publicado em Paris, em 1779 (JOHN & EDMUND, 1997).

$$d_1 = mdc(a, b) \text{ e } d_2 = mdc(b, r).$$

Afirmamos que $d_1 \leq d_2$. De fato, existem inteiros positivos k_1 e k_2 tais que:

$$a = d_1 k_1 \text{ e } b = d_1 k_2.$$

Substituindo a e b na equação $a = bq + r$ obtemos:

$$r = d_1 k_1 - d_1 k_2 q = d_1(k_1 - k_2 q),$$

ou seja, d_1 é um divisor comum de b e r. Mas d_2 é o maior divisor de b e r e portanto, pela Proposição 2.3, $d_1 \leq d_2$ como queríamos. Seguindo um argumento semelhante, podemos provar o inverso, ou seja, $d_2 \leq d_1$. Em outras palavras, $d_1 = d_2$. □

Teorema 2.4. *Se a e b são inteiros não nulos, então eles serão primos entre si se, e somente se, existir inteiros x e y tais que $ax + by = 1$.*

Demonstração. ($\rightarrow$) Se a e b são primos entre si, então $mdc(a, b) = 1$, consequentemente existem x e y tais que $ax + by = 1$.
($\leftarrow$) Se existem inteiros x e y, tais que $ax + by = 1$ e se $mdc(a, b) = d$, então $d \mid a$ e $d \mid b$. Logo, $d \mid (ax + by)$ e como $d \mid 1$, resulta em $d = 1$, ou seja, $mdc(a, b) = 1$. □

Corolário 2.1. *Se $mdc(a, b) = d$, então $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Demonstração. Vejamos que $\frac{a}{d}$ e $\frac{b}{d}$ são inteiros, pois d é um divisor comum de a e b. Sendo assim, se $mdc(a, b) = d$, então $d \mid a$, $d \mid b$ e existem inteiros x e y tais que $ax + by = d$. Logo, $\frac{a}{d}x + \frac{b}{d}y = 1$, o que nos leva a conclusão, pelo Teorema 2.4, que os inteiros $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si e, portanto, $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Exemplo 2.10. Observe que $mdc(16, 36) = 4$ e $mdc\left(\frac{16}{4}, \frac{36}{4}\right) = mdc(4, 9) = 1$.

Corolário 2.2. *Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração. Como $a \mid bc$, segue que $bc = ak$ com k inteiro e como a e b são primos entre si, $ax + by = 1$ para certos inteiros x e y. Multiplicando ambos os lados da igualdade por c temos

$$cax + cby = c.$$

Agora, $c = cax + aky = a(cx + ky)$ e, portanto, $a \mid c$. □

Um número natural d será dito *mdc* de dados números naturais $a_1, a_2, \ldots, a_n$ se possuir as seguintes propriedades:

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

ii) Se c é um divisor comum de $a_1, a_2, \ldots, a_n$, então $c \mid d$.

O *mdc*, quando existe, é certamente único e será representado por $mdc(a_1, a_2, \ldots, a_n)$.

Proposição 2.5. *Dados números naturais $a_1, a_2, \ldots, a_n$, existe o seu mdc e*

$$mdc(a_1, a_2, \ldots, a_n) = mdc(a_1, a_2, \ldots, mdc(a_{n-1}, a_n)).$$

Demonstração. Vamos provar a proposição por indução sobre n ($n \geq 2$). Para $n = 2$, sabemos que o resultado é válido. Suponhamos que o resultado vale para n. Para provar que o resultado é válido $n + 1$, basta mostrar que

$$mdc(a_1, a_2, \ldots, a_n, a_{n+1}) = mdc(a_1, a_2, \ldots, mdc(a_n, a_{n+1})),$$

pois isso provará também a existência.

Seja $d = mdc(a_1, a_2, \ldots, mdc(a_n, a_{n+1}))$. Logo, $d \mid a_1, \ldots, d \mid mdc(a_n, a_{n+1})$. Portanto, $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, \ldots, a_n, a_{n+1}$, teremos que c é divisor comum de $a_1, \ldots, a_{n-1}$ e $mdc(a_n, a_{n+1})$ e portanto, $c \mid d$. □

Para calcular o $mdc(a_1, \ldots, a_n)$, pode-se usar recursivamente o algoritmo de Euclides.

2.3.1 Método das Divisões Sucessivas de Euclides

Em geral, determinar o máximo divisor comum entre dois inteiros sem um método efetivo, pode tornar-se exaustivo e pouco prático quando os inteiros escolhidos forem números relativamente altos. Apresentamos um método para determinar o máximo divisor comum de dois inteiros, a e b por meio de sucessivas aplicações do algoritmo da divisão. Este método também é conhecido como algoritmo de Euclides.

Teorema 2.5. *Sejam a e b inteiros não negativos, onde $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter $r_j = q_{j+1} \cdot r_{j+1} + r_{j+2}$, $0 \leq r_{j+2} < r_{j+1}$ para $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$, então $mdc(a, b) = r_n$, que é o último resto não nulo.*

Demonstração. Começamos por executar a divisão euclidiana de a por b:

$$a = q_1 b + r_1, 0 \leq r_1 < b.$$

Em seguida, fazemos a divisão euclidiana de b por r_1.

$$b = q_2 r_1 + r_2, 0 \leq r_2 < r_1.$$

Agora executamos sucessivamente a divisão euclidiana de r_j por r_{j+1}. A sucessão (r_j) é uma sucessão estritamente decrescente de inteiros positivos ou nulos, pelo que ao fim de um número finito de n etapas, $r_n = 0$. Vejamos:

$$r_{n-4} = q_{n-2} r_{n-3} + r_{n-2}$$

$$r_{n-3} = q_{n-1}r_{n-2} + r_{n-1}$$

$$r_{n-2} = q_n r_{n-1} + 0.$$

Da última linha, temos que r_{n-1} divide r_{n-2} e portanto o $mdc(r_{n-1}, r_{n-2}) = r_{n-1}$. Aplicando sucessivamente a Proposição 2.4, resulta que $mdc(a, b) = r_{n-1}$. □

Exemplo 2.11. Utilizando o método das divisões sucessivas, vamos calcular $mdc(542, 234)$.

Usando o Teorema 2.3 dividimos 542 por 234 escrevendo:

$$542 = 234 \cdot (2) + 74; 0 \leq 74 \leq 234.$$

Como o resto da divisão não é nulo, aplicamos novamente o algoritmo da divisão para o divisor inicial e o resto da divisão anterior, ou seja,

$$234 = 74 \cdot (3) + 12; 0 \leq 12 \leq 74.$$

Repetindo este processo enquanto o resto for não nulo, obtemos:

$$74 = 12 \cdot (6) + 2; 0 \leq 2 \leq 12$$

$$12 = 2 \cdot (6) + 0; r = 0.$$

Como o resto da última divisão é nulo, então, pelo Teorema 2.5, segue que: $mdc(542, 234) = mdc(234, 74) = mdc(74, 12) = mdc(12, 2) = mdc(2, 0) = 2$.

Algoritmo de Euclides estendido: Seja $d = mdc(a, b)$ obtido a partir do Teorema 2.5. De acordo com a Proposição 2.3, podemos obter $n_0, m_0 \in \mathbb{Z}$ tal que $d = n_0 a + m_0 b$. Para tanto, basta seguirmos os passos descritos a seguir:

1. Calculemos $d = mdc(a, b)$ utilizando o método das divisões sucessivas;
2. Isolamos o resto de cada equação obtida e em seguida, fazemos sucessivas substituições partindo da equação cujo resto é o máximo divisor comum até que se obtenha a e b. Quando isso ocorrer, tem-se os valores procurados para $n_0, m_0 \in \mathbb{Z}$.

Vejamos um exemplo para ilustrar o Algoritmo de Euclides estendido.

Exemplo 2.12. Aplicamos o Algoritmo de Euclides Estendido para obter x e y na equação $36x + 28y = 4$. Aplicando o Método das Divisões Sucessivas:

$$36 = 28 \cdot (1) + 8 \tag{2.2}$$

$$28 = 8 \cdot (3) + 4 \tag{2.3}$$

$$8 = 4 \cdot (2) + 0 \tag{2.4}$$

Isolando o resto das equações (3.2) e (3.3) respectivamente, obtemos:

$$8 = 36 + 28 \cdot (-1) \tag{2.5}$$

$$4 = 28 + 8 \cdot (-3) \tag{2.6}$$

Como $mdc(36, 28) = 4$, tomamos a igualdade (3.5) e em seguida substituímos em (3.6), e assim obtemos os valores desejados:

$$4 = 28+8\cdot(-3) = 28+(36+28\cdot(-1))\cdot(-3) = 28+36\cdot(-3)+28\cdot(3) = 36\cdot(-3)+28\cdot(4).$$

Assim, um par de inteiros n_0, m_0 nas condições da Identidade de Bézout é dado por $n_0 = -3$ e $m_0 = 4$, sendo estes valores apenas uma das soluções de $36x + 28y = 4$.

2.4 O Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética sustenta que todo inteiro positivo maior que 1 pode ser escrito como produto de números primos, sendo esta decomposição única a menos de permutações dos fatores. Para tal, precisamos discursar sobre algumas preliminares de números primos.

Os números primos são os elementos mínimos da estrutura multiplicativa dos inteiros. Vejamos um exemplo:

$$165 = 3 \cdot 5 \cdot 11$$

donde 3, 5 e 11 são "mínimos", pois não podem ser fatorados.

Definição 2.4. *(i) Dizemos que um inteiro p é primo se $p \neq 0$, $p \neq 1$, $p \neq -1$, e os únicos inteiros divisores de p são 1, p, -1 e $-p$.*
(ii) Dizemos que um número inteiro n é composto se $n \neq 0$, $n \neq 1$, $n \neq -1$ e n não for primo.

Assim, um inteiro p não nulo é primo quando $p \neq \pm 1$ e seus únicos divisores positivos são 1 e $\mid p \mid$. Já um inteiro n é composto quando $n \neq 0$ e n possui divisores positivos diferentes de 1 e de $\mid n \mid$.

Indicamos por

$$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ é primo}\},$$

o conjunto de todos os números primos.

Exemplo 2.13. Temos que 2, 3, 5 e 7 são números primos, enquanto 4, 6, 8 e 10 são números compostos.

Proposição 2.6. *Seja $p \in \mathbb{P}$. Então*

$$\forall a, b \in \mathbb{N}; p \mid ab \rightarrow p \mid a \text{ ou } p \mid b,$$

ou seja, um primo divide um produto, somente se ele divide um dos fatores.

Demonstração. Suponhamos que $p \mid ab$ e $p \nmid a$. Logo, $p \nmid a \Rightarrow mdc(p, a) = 1$, portanto, pelo Corolário 3.2, $p \mid b$. □

Teorema 2.6. *Todo inteiro composto possui um divisor primo.*

Demonstração. Seja n um inteiro composto. Consideremos $A \neq 0$ o conjunto de todos os divisores positivos de n, exceto os divisores 1 e n, isto é:

$$A = \{t \mid n; 1 < t < n; t \in \mathbb{N}\}.$$

Pelo Teorema 2.1 existe um elemento $p \in A$ minimal, que vamos mostrar ser primo. Suponhamos que p seja composto, ou seja, admite pelo menos um divisor d tal que $1 < d < p$, então $d \mid p$ e $p \mid n$, o que implica $d \mid n$, isto é, p não seria o elemento mínimo de A, se fosse composto. Logo, p é primo. □

Exemplo 2.14. Veja que se $7 \mid ab$ então necessariamente um dos fatores a ou b (ou ambos) é múltiplo de 7, pois 7 é um número primo.

Teorema 2.7. *(Teorema Fundamental da Aritmética) Todo inteiro n, $n \geq 2$, pode ser escrito na forma $n = p_1 \cdot \ldots \cdot p_s$, para determinados primos positivos $p_1, \ldots, p_s$, com $s \geq 1$ e $p_1 \leq p_2 \leq \ldots \leq p_s$. Além disso, os fatores primos $p_1, \ldots, p_s$, satisfazendo as condições apresentadas, são únicos, isto é, se $q_1, \ldots, q_r$, são também primos positivos com $q_1 \leq q_2 \leq \cdots \leq q_r$ e $n = q_1 \cdot \ldots \cdot q_r$, então $r = s$ e, além disso, $p_i = q_j$, para todo $i, j \in \{1, \ldots, r\}$.*

Demonstração. Mostramos a existência da fatoração de n em primos. Se $n = p$ é um número primo, a afirmação fica clara ($r = 1$). Agora, se n é composto, então, pelo Teorema 2.6, n possui um divisor primo p_1 e temos:

$$n = p_1 \cdot n_1, \ 1 < n_1 < n.$$

Vejamos que, se na afirmação acima n_1 é primo, então esta igualdade representa n como produto de fatores primos, e se, ao invés disso, n_1 é composto, então pelo Teorema 2.6, n_1 possui divisores p_2, isto é, $n_1 = p_2 \cdot n_2$, e temos:

$$n = p_1 \cdot p_2 \cdot n_2, \ 1 < n_2 < n.$$

Assim sendo, temos a sequência decrescente:

$$n > n_1 > n_2 > \ldots > 1.$$

Como existe um número finito de inteiros positivos menores que n e maiores que 1, existe necessariamente um n_k ($k \geq 1$) que é um primo p_s ($n_k = p_s$) e por consequência teremos:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_s.$$

Por fim, mostramos a unicidade da fatoração de n, $n \geq 2$.

Suponhamos que $p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$ com $p_1, p_2, \ldots, p_s, q_1, q_2, \ldots, q_r \in \mathbb{P}$ e $p_1 \leq p_2 \leq \ldots \leq p_s$ assim como, $q_1 \leq q_2 \leq \ldots \leq q_r$. Temos que $p_1 \mid q_1 \cdot q_2 \cdot \ldots \cdot q_r$

donde concluímos, aplicando diversas vezes a Proposição 2.5, que p_1 tem que dividir pelo menos um dos fatores $q_1, q_2, \ldots, q_r$. Então existe k $(1 \leq k \leq r)$ com $p_1 \mid q_k$. Como p_1 e q_k são primos, temos que $p_1 = q_k \geq q_1$. De modo análogo, $q_1 \mid p_l$ para algum l $(1 \leq l \leq s)$ donde segue $q_1 = p_l \geq p_1$. Desta forma, $p_1 = q_1$. Agora, de $p_1 \cdot p_2 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot \ldots \cdot q_r$ segue

$$p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_r.$$

Por indução, concluímos que $s-1 = r-1$ (isto é, $s = r$) e $p_2 = q_2, p_3 = q_3, \ldots, p_s = q_r$. Como $p_1 = q_1$, vale a unicidade da fatoração. □

Outra forma de escrever a fatoração é

$$n = p_1^{e_1} \cdot \ldots \cdot p_s^{e_s} = \prod_{k=1}^{s} p_k^{a_k}.$$

Podemos ainda representar um número inteiro como

$$n = 2^{e_2} 3^{e_3} \ldots p^{e_p} \ldots$$

onde o produto é tomado sobre todos os primos. Ao longo deste trabalho escolheremos qualquer destas representações acima e as mesmas serão referidas como a fatoração canônica de n em números primos.

Exemplo 2.15. A fatoração canônica do inteiro positivo $n = 4.200$ é dada pela igualdade:

$$4.200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Lema 2.1. *Sejam $m, n \in \mathbb{N}, mdc(m,n) = 1$. Se $mn = c^2$, então existem M e N com $m = M^2$ e $n = N^2$.*

Demonstração. Sejam $m = \prod_{k=1}^{r} p_k^{a_k}$ e $n = \prod_{k=1}^{s} q_k^{b_k}$ as fatorações canônicas de m e n. Então os q_k são diferentes dos p_l pois $mdc(m,n) = 1$. Segue que $mn = p_1^{a_1} \cdot \ldots \cdot p_r^{a_r} \cdot q_1^{b_1} \cdot \ldots \cdot q_s^{b_s}$ é a decomposição primária de mn. Como $mn = c^2$ é quadrado perfeito, segue que todos os $a_1, \ldots, a_r, b_1, \ldots, b_s$ são pares. Logo, $m = M^2$ e $n = N^2$ para $M = \prod_{k=1}^{r} p_k^{a_k/2}$ e $N = \prod_{k=1}^{s} q_k^{b_k/2}$. □

2.5 Congruência Módulo m

A congruência módulo m é uma relação de equivalência no conjunto dos números inteiros, de tal forma que dados dois inteiros a e b, ao dividirmos por um número m (chamado módulo de congruência) deixam o mesmo resto. Através das propriedades de congruência, podemos encontrar o resto das divisões sem muitos esforços e de forma breve.

Definição 2.5. *Dados a, b, $m \in \mathbb{Z}$, dizemos que a é congruente a b módulo m e denotamos:*

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

se $m \mid (a-b)$, ou seja, se a e b têm o mesmo resto na divisão por m. Se a não for congruente (ou incongruente) a b, módulo m, escrevemos $a \not\equiv b \ (mod\ m)$.

Alternativamente temos que, dados três inteiros a, b e m,

$a \equiv b \ (mod\ m) \Leftrightarrow m \mid (a-b) \Leftrightarrow a - b = km \Leftrightarrow a = b + km$, para algum $k \in \mathbb{Z}$.

Exemplo 2.16. Temos que $3 \equiv 24 \ (mod\ 7)$, pois $7 \mid (3-24)$. Por outro lado, $25 \not\equiv 12 \ (mod\ 7)$, pois $7 \nmid (25-12)$.

Proposição 2.7. *Para quaisquer $a, b, c, d, m \in \mathbb{Z}$ temos:*

1. *$a \equiv a \ (mod\ m)$ (Reflexividade);*
2. *Se $a \equiv b \ (mod\ m)$, então $b \equiv a \ (mod\ m)$ (Simetria);*
3. *Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$ (Transitividade);*
4. *(Compatibilidade com a soma e diferença):*

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d (mod\ n) \end{cases} \rightarrow \begin{cases} a + c \equiv b + d \ (mod\ m) \\ a - c \equiv b - d \ (mod\ m) \end{cases}$$

   Em particular, se $a \equiv b \ (mod\ m)$, então $ka \equiv kb \ (mod\ m)$ para todo $k \in \mathbb{Z}$.

5. *(Compatibilidade com o produto) Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{cases} \rightarrow \ ac \equiv bd \ (mod\ m)$$

   Em particular, se $a \equiv b \ (mod\ m)$, então $a^k \equiv b^k \ (mod\ m)$ para todo $k \in \mathbb{Z}$.

6. *(Cancelamento) Se $ac \equiv bc \ (mod\ m)$ e $mdc(c, m) = d$, então $a \equiv b \ \left(mod\ \frac{m}{d}\right)$.*

Demonstração. Para a, b e c, inteiros, temos:

1. $m \mid 0 \Rightarrow m \mid (a-a) \Rightarrow a \equiv a \ (mod\ m)$.
2. $a \equiv b \ (mod\ m) \Rightarrow m \mid (a-b) \Longleftrightarrow m \mid -(a-b) \Rightarrow m \mid (b-a) \Rightarrow b \equiv a \ (mod\ m)$.
3. $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m) \Rightarrow m \mid (a-b)$ e $m \mid (b-c) \Rightarrow m \mid [(a-b)+(b-c)] \Rightarrow m \mid (a-c) \Rightarrow a \equiv c \ (mod\ m)$.

4. $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m) \Rightarrow m \mid (a-b)$ e $m \mid (c-b) \Rightarrow m \mid [(a-b)+(c-d)] \Rightarrow m \mid [(a+c)-(b+d)] \Rightarrow a+c \equiv b+d \ (mod\ m)$. A compatibilidade com a diferença segue de modo análogo.

5. Como $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, podemos concluir que existem inteiros s, t tais que $a = b + sm$ e $c = d + tm$, então $ac = (b+sm).(d+tm) = bd+btm+dsm+smtm = bd+(bt+ds+stm)m$, que por definição de congruência, $ac \equiv bd \ (mod\ m)$.

6. Se $ac \equiv bc \ (mod\ m)$, então $ac - bc = (a-b)c = km$, com $k \in \mathbb{Z}$. Ainda, se $mdc(c,m) = d$, existem inteiros r e s tais que $c = dr$ e $m = ds$, onde r e s são primos entre si. Portanto:

$$(a-b)dr = kds \text{ ou } (a-b)r = ks,$$

o que implica que, $s \mid (a-b)r$, com $mdc(r,s) = 1$. Logo, pelo Corolário 2.2, $s \mid (a-b)$ e daí $a \equiv b \ (mod\ s)$. Como $s = \dfrac{m}{d}$ segue que $a \equiv b \ \left(mod\ \dfrac{m}{d}\right)$.

□

Exemplo 2.17. Como $12 \equiv 22 \ (mod\ 5)$ e $8 \equiv 13 \ (mod\ 5)$ segue que

$$12 + 8 \equiv 22 + 13 \ (mod\ 5), \text{ ou seja, } 20 \equiv 35 \ (mod\ 5)$$

e

$$12 \cdot 8 \equiv 22 \cdot 13 \ (mod\ 5), \text{ ou seja, } 96 \equiv 286 \ (mod\ 5).$$

Exemplo 2.18. Vejamos que $31 \mid 20^{15} - 1$.

Para verificar a expressão acima é suficiente mostrar que $20^{15} \equiv 1 \ (mod\ 31)$. Para tal, observemos que

$$20 \equiv -11 \ (mod\ 31) \tag{2.7}$$

e com isso, $20^2 \equiv (-11)^2 \ (mod\ 31) \leftrightarrow 20^2 \equiv 121 \ (mod\ 31)$. Como $121 \equiv -3 \ (mod\ 31)$ temos

$$20^2 \equiv -3 \ (mod\ 31). \tag{2.8}$$

Multiplicando (2.7) e (2.8) membro a membro, obtemos $20^3 \equiv 33 \ (mod\ 31)$ e, como $33 \equiv 2 \ (mod\ 31)$,

$$20^3 \equiv 2 \ (mod\ 31). \tag{2.9}$$

Por fim, elevando (2.9) à potência 5, temos que $(20^3)^5 \equiv 2^5 \ (mod\ 31) \rightarrow 20^{15} \equiv 32 \ (mod\ 31)$ e como $32 \equiv 1 \ (mod\ 31)$, obtemos $20^{15} \equiv 1 \ (mod\ 31)$.

3 Equações Diofantinas: Uma Abordagem Histórica

O estudo das equações diofantinas é um dos mais belos e interessantes, e também um dos mais difíceis, pois em sua essência encontram-se as ligações profundas e sutis que a Teoria dos Números mantém com a Lógica, a Geometria Algébrica, e a Teoria das Aproximações Diofantinas. Por outro lado, não existe um método geral que decida se uma equação arbitrária possui ou não soluções inteiras, ou um método que estabeleça quantas soluções a equação admite. Cada equação tem sua especificidade, o que explica, em parte, porque essa área de pesquisa é tão difícil. Neste capítulo, o objetivo é abordar um pouco do contexto histórico das equações diofantinas. As principais referências utilizadas para o desenvolvimento deste capítulo foram [2] e [5].

3.1 Introdução

Sabe-se que as equações diofantinas lineares do tipo $ax + by = c$, em que a, b e c são números inteiros, tiveram sua abordagem somente em um período mais recente, diferentemente dos problemas cujas soluções envolviam equações determinadas, encontrados em diversos textos antigos, como os babilônicos, os quais tratam de alguns problemas lineares ligados com o cálculo de áreas e que são tratados com uma abordagem geométrica, [5].

Assim como os babilônios, os indianos, chineses e gregos também se preocupavam com problemas de natureza concreta e, dessa forma, os problemas indeterminados ou impossíveis, raramente eram foco desses matemáticos, os quais, mesmo demonstrando curiosidades, acreditavam que as equações hoje conhecidas como diofantinas se tratavam de erros de enunciados. A maioria dos problemas assim tratados pelas civilizações antigas admitiam uma única solução como, por exemplo, as equações polinomiais do segundo grau.

De acordo com [2], alguns problemas de indeterminação linear foram encontrados nos manuscritos de Aryabhata, um astrônomo e matemático hindu que viveu em cerca de 500 d.C. Esses manuscritos indicam que foi o matemático e astrônomo Brahmagupta (598-665 d.C.) o primeiro a encontrar a solução geral para a equação polinomial

do segundo grau em números inteiros (as diofantinas) e também a dar a solução geral da equação diofantina linear $ax + by = c$. Além disso, para as equações indeterminadas, Brahmagupta admitia não somente as soluções positivas, mas também soluções negativas, [2].

Os problemas de indeterminação linear também foram abordados posteriormente pelo matemático Bhaskara (1114-1185 d.C.) e, de acordo com [2], em suas obras *Lilavati* e *Vija-ganita*, pode-se encontrar diversos problemas sobre equações lineares, equações quadráticas determinadas, indeterminadas e ternas pitagóricas.

Um dos textos mais antigos envolvendo equações diofantinas é um manuscrito do século X, em que, segundo [5], o rei Carlos Magno (742-814 d.C.) havia convidado o inglês Alcuíno de York (735-804 d.C.) para desenvolver seu ambicioso projeto educacional. Alcuíno, além de escrever sobre diversos tópicos matemáticos, também desenvolveu uma coleção de problemas em forma de quebra-cabeças que exerceu forte influência em autores de textos escolares por muitos séculos.

3.2 Diofanto e as Equações Diofantinas

As equações diofantinas recebem este nome devido ao matemático grego Diofanto, que se interessou em resolver problemas cujas soluções fossem números inteiros ou racionais. De acordo com [5] nada se sabe sobre a nacionalidade de Diofanto e da época exata em que viveu, levando os historiadores a situá-lo no século III. Diofanto de Alexandria-Egito, teve uma enorme importância no desenvolvimento da Álgebra influenciando fortemente os europeus que posteriormente se dedicaram à Teoria dos Números.

Um possível dado pessoal sobre Diofanto pode ser encontrado em um dos problemas algébricos gregos antigos apresentados na coleção conhecida como *Palatine* ou *Antologia grega*, que contém 46 problemas numéricos em forma epigramática, uma composição poética de um determinado fato colocado em lápides ou estatuetas na Grécia. Esta obra foi reunida por volta de 500 d.C. em que, um de seus problemas, caso este seja historicamente correto, trata-se do epitáfio de Diofanto:

> *Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando sua duodécima parte a isso cobriu-lhe as faces de penugem. Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! Infeliz, criança; depois de viver à metade da vida de seu pai, o destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números, ele terminou sua vida*, [2].

Através da resolução deste epigrama podemos desvendar qual a idade de Diofanto na época de sua morte. Para tal, faremos a seguir a resolução desse enigma.

Seja x o número de anos vividos por Diofanto. Assim,

- Juventude (Deus lhe concedeu ser um menino pela sexta parte de sua vida) $= \frac{x}{6}$;
- Adolescência (e somando sua duodécima parte a isso cobriu-lhe as faces de penugem) $= \frac{x}{12}$;
- Antes do nascimento do filho (Ele lhe acendeu a lâmpada nupcial após uma sétima parte) $= \frac{x}{7}$;
- Até o nascimento do filho (e cinco anos após seu casamento concedeu-lhe um filho) $= 5$;
- Até a morte do filho (Ai! Infeliz, criança; depois de viver à metade da vida de seu pai, o Destino o levou) $= \frac{x}{2}$;
- Até a morte de Diofanto (Depois de se consolar de sua dor durante quatro anos com a ciência dos números, ele terminou sua vida) $= 4$.

A soma de todos esses itens nos fornece a idade de Diofanto à época de sua morte. Então:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 \Rightarrow x = 84.$$

Dessa forma, presume-se que Diofanto viveu oitenta e quatro anos.

Diofanto teve um grande impacto no mundo da matemática, sendo que muitas vezes ele é referido como o "Pai da Álgebra" de acordo com [2], devido as suas contribuições para a teoria dos números e a notação matemática utilizada em seus escritos. Ele produziu apenas algumas obras, mas a sua influência sobre a matemática era de longo alcance. Ao todo escreveu três trabalhos: *Arithmetica*, que tinha originalmente 13 livros, mas somente seis deles chegaram até nós; *Números Poligonais*, do qual restou apenas um fragmento; e *Porismas*, que se perdeu.

De acordo com [5], a obra *Arithmetica* é uma abordagem analítica da teoria algébrica dos números que eleva o autor à condição de gênio e ainda, na parte do trabalho dedicada à resolução de problemas, apresenta 130 problemas variados que abordam equações polinomiais do primeiro e segundo grau. Em sua obra *Arithmetica*, Diofanto sempre esteve satisfeito com um número racional positivo para a solução de seus problemas, descartando a necessidade de estudar soluções envolvendo números inteiros. No caso das equações quadráticas, ele não trabalhava com soluções negativas, e quando a equação apresentava duas raízes positivas considerava apenas a maior como sendo solução para a equação.

O desenvolvimento histórico da linguagem algébrica deu-se em três etapas: o primitivo ou retórico, em que tudo era completamente escrito em palavras, um intermédio ou sincopado, em que foram adaptadas algumas abreviaturas e convenções, e um final ou simbólico, em que são usados somente símbolos, [2]. Diofanto se encaixa no período

sincopado, pois introduziu um simbolismo algébrico que usou uma notação abreviada para as operações que ocorrem com frequência e uma abreviatura para um número desconhecido hoje chamado de incógnita e também para as potências.

De acordo com [2] nas obras preservadas de Diofanto há um uso sistemático de abreviações para potências de números e para relações e operações, sendo que, um número desconhecido é representado por um símbolo parecido com a letra grega ζ; o quadrado disto parece como Δ^{γ}, o cubo com κ^{γ}, a quarta potência, dita quadrado-quadrado, como $\Delta^{\gamma}\Delta$, a quinta potência ou quadrado-cubo, como $\Delta\kappa^{\gamma}$; a sexta potência ou cubo-cubo como $\kappa^{\gamma}\kappa$ e a igualdade como ι. O símbolo Λ era utilizado para representar o sinal de menos, sendo que, todos os termos negativos de uma expressão eram reunidos e antes deles era escrito o símbolo de menos. Já para indicar a adição de termos não utilizou nenhum símbolo específico, pois a mesma era feita por justaposição e os termos independentes eram indicados pelo símbolo μ seguido de seu coeficiente numérico. E por fim, os coeficientes sempre eram representados após o símbolo que representava a incógnita, [8].

Como pode-se notar, o simbolismo que Diofanto introduziu pela primeira vez, sem dúvida, concebeu-se em um meio curto e facilmente compreensível de expressar uma equação. Faremos a seguir uma breve comparação de como expressamos uma equação hoje e como a mesma seria expressa por Diofanto.
Equação atual:

$$x^3 + 9x - 5x^2 - 1 = x.$$

Possível equação expressa por Diofanto:

$$\kappa^{\gamma}\alpha\zeta\theta\Lambda\Delta^{\gamma}\varepsilon\Lambda\mu\alpha\iota\zeta.$$

Embora tenha feito avanços importantes no simbolismo, ele ainda não tinha a notação necessária para expressar métodos mais gerais. Isso fez com que Diofanto estivesse mais preocupado com problemas particulares ao invés de situações gerais. Uma vez que, em suas equações faltavam símbolos para a operação de multiplicação e para um número geral n, [6]. A Álgebra ainda tinha um longo caminho a percorrer antes que os problemas mais gerais pudessem ser escritos e resolvidos de forma sucinta.

De acordo com [9], alguns séculos após os trabalhos de Diofanto, não se registou um avanço qualitativo no ponto de vista teórico da aritmética. Houve, nesse intervalo de tempo, a criação do sistema de numeração decimal posicional e a introdução do zero pelos hindus, a sua adoção pelos árabes e a sua utilização, ainda que tardia, na Europa. Também nesse longo período, foram aperfeiçoados os algoritmos para se efetuar as operações, as frações e a aritmética financeira.

A atenção para a teoria dos números foi despertada novamente, apenas no século XVII pelos trabalhos do matemático francês Pierre de Fermat (1601-1665), [9]. Muitas das contribuições de Fermat para a teoria dos números se deram na forma de enunciados e notas escritos nas margens de um exemplar do livro *Arithmetica* escrito por Diofanto,

os quais foram estudados por outros matemáticos. A sua obra de maior relevância ficou conhecida como o *Último Teorema de Fermat* onde afirmou, sem demonstrar, que a equação $x^n + y^n = z^n$ para $n > 2$ não admitia soluções em inteiros positivos, a qual foi demonstrada somente em 1994, pelo matemático Andrew Wiles. A partir de então, o teorema passou a ser chamado de *Teorema de Fermat-Wiles*.

4 Equações Diofantinas Lineares

Pelos estudos pioneiros de Diofanto, denomina-se equação diofantina uma equação da forma

$$f(x_1, x_2, \ldots, x_n) = 0, \tag{4.1}$$

onde f é uma função polinomial de n variáveis, com $n \geq 2$, e $x_1, x_2, \ldots, x_n$ assumem apenas valores inteiros. Neste capítulo, estudamos alguns casos particulares da equações (4.1), que são as equações diofantinas lineares, aprendemos a reconhecer quando esse tipo de equação possui solução e como encontrar todas elas. As principais referências utilizadas para o desenvolvimento deste capítulo, foram [4], [11] e [12].

4.1 Equações Diofantinas Lineares com Duas Variáveis

Uma equação diofantina é linear se esta estiver na forma

$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n = c, \tag{4.2}$$

em que seus coeficientes $a_1, a_2, \ldots, a_n$ são números inteiros. Isto significa escrever c como combinação linear inteira de todos os a_i $(1 \leq i \leq n)$. Deste modo, determinar uma solução para a Equação (4.2) implica em encontrar um conjunto de valores inteiros $\alpha_1, \alpha_2, ..., \alpha_n$ tais que, ao serem substituídos nos respectivos lugares da *n-upla* $(x_1, x_2, ..., x_n)$, a Condição (4.2) é verificada.

Tratamos, nesta seção, de equações desse tipo, nos restringindo somente àquelas com duas variáveis x e y, com coeficientes $a_1 = a$ e $a_2 = b$. Ou seja, as equações do tipo:

$$ax + by = c, \text{ com } a, b \text{ e } c \in \mathbb{Z};\ a \neq 0 \text{ ou } b \neq 0.$$

O termo "diofantina" se refere a qualquer equação cujos coeficientes são números inteiros, enquanto que o termo "linear" é uma referência ao fato de que a equação acima representa uma reta no plano cartesiano, ou seja, resolver uma equação diofantina do tipo $ax + by = c$, nas variáveis x, $y \in \mathbb{Z}$, pode ser visto como sendo o problema de determinar pontos da reta que contêm coordenadas inteiras.

Por exemplo, embora haja uma infinidade de pontos cujas coordenadas são números reais pertencentes à reta $6x + 21y = 2$, não há ponto cujas coordenadas são números inteiros, que satisfaça essa equação, pois como $x, y \in \mathbb{Z}$, temos que o membro esquerdo da igualdade $6x + 21y = 2$ é múltiplo de 3, enquanto que o direito não.

Muitas das equações diofantinas em que suas soluções são limitadas pelo problema matemático proposto, podem ser resolvidas por tentativa, método muito utilizado na idade média. Vejamos a seguir um exemplo.

Exemplo 4.1. Em um evento do curso de matemática da UNESP, há 120 participantes. Para realizar uma dinâmica, a comissão organizadora do evento deseja separar os participantes em grupos de 6 e 12 pessoas. Quantos grupos de 6 pessoas e 12 pessoas será possível montar de modo que todos participem da dinâmica?

Representando o problema matematicamente, obtemos a equação diofantina em duas variáveis $6x + 12y = 120$. Esta equação pode ser representada por uma reta no plano cartesiano por: $y = \dfrac{120 - 6x}{12} \rightarrow y = \dfrac{20 - x}{2}$.

Vejamos que, para este problema é fácil determinar todas as possíveis soluções inteiras, pois x deve ser um múltiplo de 2 na equação $y = \dfrac{20 - x}{2}$, com $0 \leq x \leq 20$ (pois queremos soluções inteiras e positivas). Dessa forma, teremos 11 soluções para o problema, sendo elas: $(0, 10)$, $(2, 9)$, $(4, 8)$, $(6, 7)$, $(8, 6)$, $(10, 5)$, $(12, 4)$, $(14, 3)$, $(16, 2)$, $(18, 1)$, $(20, 0)$, conforme apresentado na Figura 4.1 através da representação geométrica para o problema.

Figura 4.1: Soluções inteiras e positivas da equação linear $6x + 12y = 120$.

Embora seja interessante a resolução dessas equações pelo método de tentativa, nem sempre esse é eficiente. No Exemplo 4.1 vimos claramente todas as soluções inteiras e positivas para o problema proposto, já que as coordenadas são compostas por inteiros relativamente pequenos e suas soluções são limitadas. Porém, como determinaríamos a solução de um problema, cujas coordenadas correspondessem a inteiros grandes? Certamente, utilizando o método de tentativa, nem teríamos certeza de quantas soluções

inteiras o problema teria. Por exemplo, encontrar todas as soluções inteiras da equação $7x + 11y = 100$. Sabemos que uma das soluções é dada por $x = -300$ e $y = 200$, tornando-se inviável o método. Sendo assim, de modo geral, torna-se essencial conhecer a resolução algébrica de uma equação diofantina linear em duas variáveis, a qual é apresentada a seguir.

4.1.1 Solução Algébrica

Antes de procurar uma solução para uma equação diofantina, é importante saber se essa solução existe. Sendo assim, esboçaremos aqui uma série de resultados que nos possibilitarão responder à algumas indagações que surgem acerca das equações diofantinas:

- Quais são as condições para que as mesmas possuam solução?
- Quantas são as soluções?
- Caso existam, como calcular todas elas?

O resultado apresentado a seguir nos traz a condição necessária e suficiente para a existência de soluções de uma dada equação diofantina linear com duas variáveis.

Teorema 4.1. *Sejam a e b inteiros e $d = mdc(a, b)$. Se $d \nmid c$, então a equação $ax + by = c$ não possui solução inteira. Se $d \mid c$, então possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções podem ser dadas por:*

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ \\ y = y_0 - \dfrac{a}{d}t \end{cases} ; t \in \mathbb{Z}$$

Demonstração. Se $d \nmid c$, então a equação $ax + by = c$ não possui solução inteira, pois, como $d = mdc(a, b)$ segue que:

$d \mid a$ e $d \mid b \rightarrow d|ax$ e $d \mid by \rightarrow d \mid (ax + by) \rightarrow d \mid c$, contrariando a hipótese de que $d \nmid c$.

Se $d \mid c$ então $ax + by = c$ possui infinitas soluções. Para isso, basta tomar $d = mdc(a, b)$ e daí, como $d \mid c$, existe um inteiro k tal que $c = dk$. Pelo teorema de Bézout $d = n_0a + m_0b; n_0, m_0 \in \mathbb{Z}$. Multiplicando ambos os termos dessa equação por k resulta em: $kd = kn_0a + km_0b$. Como $c = dk$, então teremos $c = (kn_0)a + (km_0)b$ e, dessa forma $x = kn_0$ e $y = km_0$, onde $k = \dfrac{c}{d}$, pois $c = dk$.

Logo,

$$\begin{cases} x = x_0 = \dfrac{c}{d}n_0 \\ \\ y = y_0 = \dfrac{c}{d}m_0 \end{cases}$$

ou seja, (x_0, y_0) é uma solução particular para a equação diofantina dada. Agora, vamos mostrar que todas as soluções da equação diofantina $ax + by = c$ são dadas pela fórmula

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ \\ y = y_0 - \dfrac{a}{d}t \end{cases} ; t \in \mathbb{Z}$$

Sejam

$$\begin{cases} ax + by = c \quad (1) \\ ax_0 - by_0 = c \quad (2) \end{cases}$$

duas equações diofantinas com $a, b \in \mathbb{Z}$.
Subtraindo (2) de (1), temos

$$(ax + by) - (ax_0 + by_0) = 0 \rightarrow (x - x_0)a + (y - y_0)b = 0 \rightarrow (x - x_0)a = (y_0 - y)b.$$

Como

$$d = mdc(a, b) \rightarrow \frac{d}{d} = mdc\left(\frac{a}{d}, \frac{b}{d}\right) \rightarrow 1 = mdc\left(\frac{a}{d}, \frac{b}{d}\right).$$

Assim,

$$(x - x_0)a\frac{1}{d} = (y_0 - y)b\frac{1}{d} \rightarrow (x - x_0)\frac{a}{d} = (y_0 - y)\frac{b}{d}.$$

Resultando,

- $\dfrac{a}{d} \mid \dfrac{b}{d}(y_0 - y)$ e, como $mdc\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, pelo Corolário 2.1, segue que $\dfrac{a}{d} \mid (y_0 - y) \rightarrow y_0 - y = \dfrac{a}{d}t; t \in \mathbb{Z} \rightarrow y = y_0 - \dfrac{a}{d}t; t \in \mathbb{Z}$.
- $\dfrac{b}{d} \mid \dfrac{a}{d}(x - x_0)$ e, como $mdc\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$, pelo Corolário 2.1, segue que $\dfrac{b}{d} \mid (x - x_0) \rightarrow x - x_0 = \dfrac{b}{d}t; t \in \mathbb{Z} \rightarrow x = x_0 + \dfrac{b}{d}t; t \in \mathbb{Z}$.

Portanto,

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ \\ y = y_0 - \dfrac{a}{d}t \end{cases} ; t \in \mathbb{Z}$$

é a equação geral que determina as infinitas soluções da equação diofantina $ax + by = c$. □

Exemplo 4.2. Resolvemos a equação $5x + 12y = 81$, com soluções pertencentes ao conjunto dos números inteiros.

Iniciaremos fazendo uso do algoritmo de Euclides, para encontrar $mdc(12, 5)$. Sendo assim,

$$12 = 5 \cdot (2) + 2 \tag{4.3}$$

$$5 = 2 \cdot (2) + 1 \tag{4.4}$$

$$2 = 1 \cdot (2) + 0.$$

Logo, $mdc(12, 5) = 1$ e pelo Teorema (4.1), como $mdc(12, 5) = 1$ então a equação tem solução. Agora, isolamos os restos de (4.3) e (4.4), desconsiderando a última expressão, já que tem resto 0 e, portanto, não será substituída em nenhuma outra expressão. Logo,

$$2 = 12 + 5 \cdot (-2) \tag{4.5}$$

$$1 = 5 \cdot (1) + 2 \cdot (-2). \tag{4.6}$$

Substituindo (4.5) em (4.6), temos a expressão procurada:

$$= 5 \cdot (1) + (5 \cdot (-2) + 12) \cdot (-2) = 5 \cdot (5) + 12 \cdot (-2). \tag{4.7}$$

Multiplicando a Equação (4.7) por 81, segue que

$$81 = 5 \cdot (405) + 12 \cdot (-162).$$

Portanto, uma solução da equação $5x+12y = 81$ é $x_0 = 405$ e $y_0 = -162$. Deste modo, temos que a solução geral no conjunto dos inteiros, será dada por:

$$S = \{(405 + 12t, -162 - 5t), \text{ com } t \in \mathbb{Z}\}.$$

4.2 Equações Diofantinas Lineares com Três Variáveis

Daremos início a ideia de como encontrar a solução particular e geral de uma equação diofantina linear com n variáveis. Para tal, estudaremos aqui as equações diofantinas lineares com três variáveis

$$a_1x + a_2y + a_3z = c, \tag{4.8}$$

onde $a_1, a_2, a_3 \in \mathbb{Z}$ e ambos são diferentes de zero.

O mesmo argumento usado para demonstrar o Teorema 4.1, garante que a Equação (4.8) admite soluções se, $d = mdc(a_1, a_2, a_3)$ divide c. Na Seção 2.3 vimos que é possível calcular mdc de uma quantidade finita de números, então, primeiro analisaremos $mdc(a_1, a_2) = d_1$ e a partir deste, $mdc(d_1, a_3) = d$.

Se $d_1 = mdc(a_1, a_2)$, com $d_1 \in \mathbb{Z}$, então existem k_1, $k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. Como $d = mdc(d_1, a_3)$, então existem $k, z_0 \in \mathbb{Z}$ tal que $d = d_1k + a_3z_0$. Assim,

$$d = (a_1k_1 + a_2k_2)k + a_3z_0 \rightarrow d = a_1(k_1k) + a_2(k_2k) + a_3z_0.$$

Tomando $k_1k = x_0$ e $k_2k = y_0$, teremos

$$d = a_1x_0 + a_2y_0 + a_3z_0. \tag{4.9}$$

Daí, como $d \mid c$, existe um número inteiro q, tal que $c = dq$. Agora, multiplicando a Equação (4.9) por q, obtemos

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

Logo, (x_0q, y_0q, z_0q) é uma das soluções particulares da Equação (4.8).

4.2.1 Solução Geral

Para se obter a solução geral para a Equação (4.8), devemos inicialmente reduzir essa equação para duas variáveis. Considerando, $a_1x + a_2y = k$, temos

$$k + a_3z = c, \tag{4.10}$$

e evidentemente a Equação (4.10) possui solução, pois $d_1 = mdc(1, a_3) = 1$ e $1 \mid c$. Dessa forma, concluímos pelo Teorema 4.1, que a solução geral da Equação (4.10) é dada por

$$\begin{cases} k = k_0 + \dfrac{a_3}{d_1}t_1 \\ \\ \qquad\qquad ; t_1 \in \mathbb{Z} \\ \\ z = z_0 - \dfrac{1}{d_1}t_1 \end{cases}$$

e como $d_1 = mdc(1, a_3) = 1$, segue que, $k = k_0 + a_3t_1$ e $z = z_0 - t_1$. Vejamos agora que $a_1x + a_2y = k = k_0 + a_3t_1$, sendo assim, devemos escolher um valor conveniente para t_1, que satisfaça

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

Por fim, a equação $a_1x + a_2y = k$, pelo Teorema 4.1, terá como solução

$$\begin{cases} x = x_0 + \dfrac{a_2}{d_2}t_2 \\ \\ \qquad\qquad ; t_2 \in \mathbb{Z} \\ \\ y = y_0 - \dfrac{a_1}{d_2}t_2 \end{cases}$$

Assim, podemos concluir que o conjunto solução da equação $a_1x + a_2y + a_3z = c$ é

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

Exemplo 4.3. Encontremos uma solução para a equação diofantina $120x + 84y + 144z = 60$.

Como $mdc(120, 84, 144) = 12$ e $12 \mid 60$, a equação dada possui solução. Observe que, a equação $120x+84y+144z = 60$ equivale a $10x+7y+12z = 5$ e $mdc(10, 7, 12) = 1$ e $1 \mid 5$. Assim, calculando $mdc(10, 7)$ através do algoritmo de Euclides obtemos:

$$10 = 7 \cdot (1) + 3 \tag{4.11}$$

$$7 = 3 \cdot (2) + 1 \tag{4.12}$$

$$3 = 1 \cdot (3) + 0.$$

Isolando os restos das Igualdades (4.11) e (4.12) teremos

$$3 = 10 + 7 \cdot (-1) \tag{4.13}$$

$$1 = 7 + 3 \cdot (-2). \tag{4.14}$$

Tomando a Igualdade (4.13) e substituindo em (4.14) obtemos os valores procurados

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

Aplicando novamente o algoritmo de Euclides para calcular $mdc(1, 12)$ temos

$$12 = 1 \cdot (11) + 1 \tag{4.15}$$

$$11 = 1 \cdot (11) + 0$$

Assim, $12 = 1 \cdot (11) + 1$ e portanto $mdc(1, 12) = 1$. Devemos agora escrever $mdc(7, 10, 12) = 1$ como combinação linear de 10, 7 e 12. Para isso, basta isolar o resto da Igualdade (4.15) que teremos $1 = 1 \cdot (-11) + 12$ e como $1 = 10 \cdot (-2) + 7 \cdot (3)$ segue que

$$1 = (10 \cdot (-2) + 7 \cdot (3)) \cdot (-11) + 12.$$

$$1 = 10 \cdot (22) + 7 \cdot (-33) + 12.$$

Multiplicando o resultado por 5 resulta em:

$$5 = 10 \cdot (110) + 7 \cdot (-165) + 12 \cdot (5).$$

Logo a terna $(110, -165, 5)$ é uma solução particular para a equação $10x+7y+12z = 5$ e consequentemente, é uma solução particular para a equação original do problema dada por $120x + 84y + 144z = 60$.

Exemplo 4.4. Determinemos todas as soluções inteiras da equação $10x+7y+12z = 5$.

Já vimos no Exemplo 4.3 que a equação acima possui solução. Vamos agora encontrar sua solução geral, para isso, tomamos $k = 10x+7y$, então teremos $k+12z = 5$, que

também possui solução, pois $mdc(1, 12) = 1$ e $1 \mid 5$. Podemos escrever $mdc(1, 12) = 1$, como combinação linear de 1 e 12. Para tal, observe que

$$1 = 1 \cdot (-11) + 12.$$

Multiplicando por 5 ambos os lados da igualdade, teremos

$$5 = 11 \cdot (-55) + 12 \cdot (5).$$

Sendo $(-55, 5)$ uma solução particular de $k + 12z = 5$, segue do Teorema 4.1 que a solução geral é dada por

$$S_1 = \{(-55 + 12t_1, 5 - t_1), \text{ com } t_1 \in \mathbb{Z}\}.$$

Analisamos agora $10x + 7y = k = -55 + 12t_1$. É importante notar que neste caso $mdc(7, 10) = 1$ e $1 \mid (-55 + 12t_1)$, isto é, t pode assumir qualquer valor inteiro, pois $1 \mid -55$ e $1 \mid 12$. No Exemplo 4.3 vimos que $1 = 10 \cdot (-2) + 7 \cdot (3)$, donde multiplicando ambos os lados por $(-55 + 12t_1)$ temos

$$(-55 + 12t_1) \cdot 1 = 10 \cdot (-2) \cdot (-55 + 12t_1) + 7 \cdot (3) \cdot (-55 + 12t_1)$$

$$-55 + 12t_1 = 10 \cdot (110 - 24t_1) + 7 \cdot (-165 + 36t_1)$$

onde concluímos novamente, pelo Teorema 4.1, que a solução geral dessa equação é dada por

$$S_2 = \{(110 - 24t_1 + 7t_2, -165 + 36t_1 - 10t_2), \text{ com } t_1 \text{ e } t_2 \in \mathbb{Z}\}.$$

Portanto, a solução geral da equação $10x + 7y + 12z = 5$ é da forma

$$S = \{(110 - 24t_1 + 7t_2, -165 + 36t_1 - 10t_2, 5 - t_1), \text{ com } t_1 \text{ e } t_2 \in \mathbb{Z}\}.$$

Exemplo 4.5. Encontremos todas as soluções inteiras de $10x + 6y + 5z = 8$.

Como $mdc(10, 6, 5) = 1$ e $1 \mid 8$ então a equação possui solução. Faremos agora a redução da equação $10x + 6y + 5z = 8$ em duas novas equações, sendo elas $10x + 6y = k$ e $k + 5z = 8$. Para a equação $k + 5z = 8$ temos que $mdc(1, 5) = 1$ e $1 \mid 8$. Escrevendo 1 como combinação linear de 1 e 5, temos

$$1 = 1 \cdot (-9) + 5 \cdot (16).$$

Multiplicando por 8 ambos os lados da igualdade, resulta

$$8 = 1 \cdot (-72) + 5 \cdot (16).$$

Logo, $(-72, 16)$ é uma solução particular, o que nos leva a solução geral

$$S_1 = \{(-72 + 5t_1, 16 - t_1), \text{ com } t_1 \in \mathbb{Z}\}.$$

Para encontrar a solução da equação original, devemos agora encontrar a solução geral da equação

$$10x + 6y = k = -72 + 5t_1.$$

Para que essa equação possua solução, $2 = mdc(10, 6)$ deve dividir $-72 + 5t_1$. Neste caso, o parâmetro t não pode ser arbitrário, como no Exemplo 4.4, pois $2 \mid (-72+5t_1)$, mas $2 \mid -71$ e $2 \nmid 5$. Portanto t_1 precisa ser da forma $2l$ com $l \in \mathbb{Z}$. Aplicando o algoritmo de Euclides para encontrar $mdc(10, 6)$ temos que

$$10 = 6 \cdot (1) + 4 \tag{4.16}$$

$$6 = 4 \cdot (1) + 2 \tag{4.17}$$

$$4 = 2 \cdot (2) + 0.$$

Isolando os restos das Igualdades (4.16) e (4.17) segue

$$4 = 10 + 6 \cdot (-1) \tag{4.18}$$

$$2 = 6 + 4 \cdot (-1). \tag{4.19}$$

Tomando a Igualdade (4.18) e substituindo em (4.19) obtemos os valores procurados

$$2 = 6+4\cdot(-1) = 6+(10+6\cdot(-1))\cdot(-1) = 6\cdot(2)+10\cdot(-1) \rightarrow 2 = 10\cdot(-1)+6\cdot(2)$$

que ao multiplicarmos ambos os lados da igualdade acima por $\left(\frac{-72+5t_1}{2}\right)$ teremos

$$2 = 10 \cdot (-1) + 6 \cdot (2)$$

$$\left(\frac{-72+5t_1}{2}\right) \cdot 2 = 10 \cdot (-1) \cdot \left(\frac{-72+5t_1}{2}\right) + 6 \cdot (2) \cdot \left(\frac{-72+5t_1}{2}\right)$$

$$-72 + 5t_1 = 10 \cdot \left(\frac{72-5t_1}{2}\right) + 6 \cdot (-72 + 5t_1),$$

onde concluímos que a solução geral da equação $10x + 6y = -72 + 5t_1$ é dada por

$$S_2 = \left\{ \left(\frac{72-5t_1}{2} + \frac{6}{2}t_2, -72 + 5t_1 - 10t_2 \right), com \quad t_1 \in \mathbb{Z} \right\}.$$

Portanto, a solução geral da equação $10x + 6y + 5z = 8$ é da forma

$$S = \left\{ \left(\frac{72-5t_1}{2} + 3t_2, -72 + 5t_1 - 10t_2, 16 - t_1 \right), com \quad t_1 = 2l; t_1, t_2 \quad e \quad l \in \mathbb{Z} \right\}.$$

4.3 Equações Diofantinas Lineares com n Variáveis

Mostramos a seguir um método que nos permite encontrar não só uma solução particular de uma equação diofantina linear com n variáveis, mas também todas as suas soluções. Para tal, consideramos a equação diofantina linear em n variáveis

$$a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n = c, \tag{4.20}$$

onde nos interessa encontrar um conjunto de *n-uplas* $(x_1, x_2, \ldots, x_n)$ inteiras em que a Condição (4.20) é verificada. Para isso, faremos uso da ideia aplicada na Seção que consiste em reduzir a equação diofantina linear com mais de duas variáveis em um equação diofantina linear de duas variáveis. Ainda, a mesma argumentação usada para provar o Teorema 4.1, garante que a Equação (4.20) admite solução inteira se, e somente se, $d = mdc(a_1, a_2, \ldots, a_n)$ e $d \mid c$. O conteúdo a seguir foi inspirado pelos autores [1] e [3].

4.3.1 Solução Particular

Para obter uma solução particular para (4.20) observemos que, se $d_1 = mdc(a_1, a_2)$, então existem $k_1, k_2 \in \mathbb{Z}$ para os quais $a_1k_1 + a_2k_2 = d_1$. Tomemos agora $d_2 = mdc(d_1, a_3)$, então existem $k_3, k_4 \in \mathbb{Z}$ para os quais $d_1k_3 + a_3k_4 = d_2$. Sendo assim, podemos observar que $d_2 \mid (a_1, a_2, a_3)$. Continuando este processo, de modo análogo, chegaremos que $d_{n-1} = mdc(d_{n-2}, a_n)$, donde segue, $d_{n-1} \mid (a_1, a_2, \cdots, a_n)$, e como $d_{n-1} = mdc(d_{n-2}, a_n)$ então teremos que $d = d_{n-1} = mdc(a_1, a_2, \cdots, a_n)$, ou seja, podemos escrever d como combinação linear dos a_s da seguinte forma

$$a_1x_1^{'} + a_2x_2^{'} + \cdots + a_{n-1}x_{n-1}^{'} + a_nx_n^{'} = d.$$

E como $d \mid c$, então existe $q \in \mathbb{Z}$ tal que:

$$a_1(x_1^{'}q) + a_2(x_2^{'}q) + \cdots + a_{n-1}(x_{(n-1)}^{'}q) + a_n(x_n^{'}q) = d.q = c,$$

o que nos mostra que

$$(x_1^{'}q, x_2^{'}q, \cdots, x_{(n-1)}^{'}q, x_n^{'}q)$$

é uma solução particular da Equação (4.20).

4.3.2 Solução Geral

Para encontrar a solução geral para a Equação (4.20) devemos utilizar o processo de reduzi-la em uma equação diofantina linear em duas variáveis, isto é, $a_1x_1 + a_2x_2 + \cdots + a_{n-1}x_{n-1} = k_1$ e $k_1 + a_nx_n = c$, onde $d_1 = mdc(1, a_n) = 1$ e $1 \mid c$, sendo que, pelo Teorema 4.1 a solução geral é da forma

$$k_1 = k_1^{'} + \frac{a_n}{d_1}t_1, x_n = x_n^{'} - \frac{1}{d_1}t_1, \text{ com } t_1 \in \mathbb{Z},$$

e portanto a solução geral da Equação (4.20) pode ser dada por

$$x_1 = x_1^{'} + \frac{a_2}{d_{n-1}} t_{n-1},$$

$$x_2 = x_2^{'} - \frac{a_1}{d_{n-1}} t_{n-1},$$

$$x_3 = x_3^{'} - t_{n-2},$$

$$\vdots$$

$$x_n = x_n^{'} - t_1$$

que pode ser representada da seguinte forma

$$S = \left\{ \left(x_1^{'} + \frac{a_2}{d_{n-1}} t_{n-1}, x_2^{'} - \frac{a_1}{d_{n-1}} t_{n-1}, x_3^{'} - t_{n-2}, \ldots, x_n^{'} - t_1 \right) \right\},$$

sendo $d_{n-1} = mdc(a_1, a_2)$ e $t_i \in \mathbb{Z}$, com $i = 1, 2, 3, \cdots, n-1$.

Exemplo 4.6. Determinemos todas as soluções da equação diofantina $4x + 7y + 5z + 11w = 7$.

Note que a equação acima possui solução, pois $mdc(4, 5, 7, 11) = 1$ e $1 \mid 7$. Fazendo a redução da equação $4x + 7y + 5z + 11w = 7$ em duas novas equações, teremos $4x + 7y + 5z = k_1$ e $k_1 + 11w = 7$. É evidente que a equação $k_1 + 11w = 7$ possui solução, pois $mdc(1, 11) = 1$ e $1 \mid 7$. Sendo assim, conseguimos encontrar sua solução particular e geral. Escrevendo 1 como combinação linear de 1 e 7, teremos

$$1 = 1 \cdot (-10) + 11 \cdot (1).$$

Multiplicando por 7 ambos os lados da igualdade, resulta

$$7 = 1 \cdot (-70) + 11 \cdot (7).$$

Disso temos que $(-70, 7)$ é uma solução particular de $k_1 + 11w = 7$. A solução geral é portanto

$$S_1 = \{(-70 + 11t_1, 7 - t_1), \text{ com } t_1 \text{ e } t_2 \in \mathbb{Z}\}.$$

Assim, temos que $4x+7y+5z = k_1 = -70+11t_1$, para t_1 arbitrário, pois $mdc(4, 5, 7) = 1$ e $1 \mid (-70 + 11t_1)$. Resolvemos agora $4x + 7y + 5z = -70 + 11t_1$, fazendo uma nova redução. Para tal, tome $4x + 7y = k_2$, logo temos $k_2 + 5z = -70 + 11t_1$, que também possui solução, pois $mdc(1, 5) = 1$ e $1 \mid (-70 + 11t_1)$. Escrevendo como combinação linear $mdc(1, 5) = 1$ temos

$$1 = 1 \cdot (-4) + 5 \cdot (1).$$

Multiplicando por $(-70 + 11t_1)$ ambos os lados da igualdade, segue que

$$(-70 + 11t_1) \cdot (1) = 1 \cdot (-4) \cdot (-70 + 11t_1) + 5 \cdot (1) \cdot (-70 + 11t_1)$$

$$-70 + 11t_1 = 1 \cdot (240 + 44t_1) + 5 \cdot (-70 + 11t_1),$$

onde concluímos que a solução particular de $k_2 + 5z = -70 + 11t_1$ é $(240 + 44t_1, -70 + 11t_1)$ e portanto sua solução geral é dada por

$$S_2 = \{(240 + 44t_1 + 5t_2, -70 + 11t_1 - t_2), \text{ com } t_2 \text{ e } t_1 \in \mathbb{Z}\}.$$

Por fim, encontramos a solução geral de $4x + 7y = k_2 = 240 + 44t_1 + 5t_2$, que possui solução para quaisquer valores de t_1 e t_2, pois $mdc(4, 7) = 1$ e $1 \mid (240 + 44t_1 + 5t_2)$. Utilizando o algoritmo de Euclides para escrever $mdc(4, 7) = 1$, temos

$$7 = 4 \cdot (1) + 3$$

$$4 = 3 \cdot (1) + 1$$

$$3 = 1 \cdot (3) + 0.$$

Isolando os restos nas igualdades acima, segue que

$$3 = 4 \cdot (-1) + 7$$

$$1 = 4 + 3 \cdot (-1).$$

Logo,

$$1 = 4 + (7 + 4 \cdot (-1)) \cdot (-1) = 4 + 7 \cdot (-1) + 4 \cdot (1) = 4 \cdot (2) + 7 \cdot (-1).$$

Multiplicando por $(240 + 44t_1 + 5t_2)$ ambos os lados da igualdade, obtemos

$$1 = 4 \cdot (2) + 7 \cdot (-1)$$

$$(240 + 44t_1 + 5t_2) \cdot (1) = 4 \cdot (2) \cdot (240 + 44t_1 + 5t_2) + 7 \cdot (-1) \cdot (240 + 44t_1 + 5t_2)$$

$$240 + 44t_1 + 5t_2 = 4 \cdot (480 + 88t_1 + 10t_2) + 7 \cdot (-240 - 44t_1 - 5t_2),$$

ou seja, $(x_0, y_0) = (480 + 88t_1 + 10t_2, -240 - 44t_1 - 5t_2)$ e a solução geral é

$$S_3 = \{(480 + 88t_1 + 10t_2 + 7t_3, -240 - 44t_1 - 5t_2 - 4t_3), \text{ com } t_1, t_2 \text{ e } t_3 \in \mathbb{Z}\}.$$

Portanto, a solução geral de $4x + 7y + 5z + 11w = 7$ é da forma:

$$S = (480 + 88t_1 + 10t_2 + 7t_3, -240 - 44t_1 - 5t_2 - 4t_3, -70 + 11t_1 - t_2, 7 - t_1),$$

com t_1, t_2 e $t_3 \in \mathbb{Z}$.

4.4 Algumas Aplicações Práticas

Nesse capítulo, fizemos um estudo sobre as equações diofantinas lineares analisando suas condições de existência, sua admissão de soluções e como encontra-las. Agora, exibiremos algumas das diversas aplicações dessas equações em situações reais, no nosso dia a dia, mostrando onde e como usamos as equações diofantinas lineares.

Exemplo 4.7. Em um evento beneficente em prol de crianças com câncer que ocorreu no Centro Cultural Roberto Palmari em 2017 no Município de Rio Claro - SP, foram vendidos R$ $720,00$ em ingressos. Sabendo que o valor do ingresso para homens custava R$ $15,00$ e para mulheres R$ $8,00$, quantos homens e quantas mulheres participaram do evento?

Solução: Seja H o número de homens e M o número de mulheres que participaram do evento, segue que, a quantidade de homens presentes pode ser expressa por $15H$, enquanto a quantidade de mulheres por $8M$. Deste modo o problema acima pode ser representado pela equação $15H + 8M = 720$. Para resolver este problema, primeiro devemos verificar se ele possui solução. Como o $mdc(15, 8) = 1$ e $1 \mid 720$, então a equação diofantina $15H + 8M = 720$ possui solução. Agora, determinaremos uma solução particular para essa equação. Para tal, aplicamos o algoritmo de Euclides para calcular o $mdc(10, 7)$. Logo,

$$15 = 8 \cdot (1) + 7 \tag{4.21}$$

$$8 = 7 \cdot (1) + 1 \tag{4.22}$$

$$7 = 1 \cdot (3) + 0.$$

Como o $mdc(10, 7) = 1$, devemos isolar os restos das Igualdades (4.21) e (4.22). Sendo assim,

$$7 = 15 + 8 \cdot (-1) \tag{4.23}$$

$$1 = 8 + 7 \cdot (-1). \tag{4.24}$$

Tomando a Igualdade (4.23) e substituindo em (4.24) obtemos os valores procurados

$$1 = 8 + (15 + 8 \cdot (-1)) \cdot (-1) = 8 + 15 \cdot (-1) + 8 \cdot (1) = 15 \cdot (-1) + 8 \cdot (2).$$

Multiplicando a igualdade acima por 720, segue que

$$720 = 15 \cdot (-720) + 8 \cdot (1440).$$

Logo obtemos $(-720, 1440)$ como sendo a solução particular para a equação dada. Vejamos que a solução particular $(-720, 1440)$, não serve como solução para o problema, tendo em vista que os valores para H e M precisam ser todos positivos. Portanto precisamos encontrar a solução geral para a equação e limitar um intervalo de valores, que seja válido como solução para o problema.

t	$H = -720 + 8t$	$M = 1440 - 15t$
90	0	90
91	8	75
92	16	60
93	24	45
94	32	30
95	40	15
96	48	0

Tabela 4.1: Soluções do Exemplo 4.7, com $90 \leq t \leq 96$.

Para encontrar todas as soluções da equação dada, basta substituir os valores obtidos na fórmula a seguir:

$$\begin{cases} H = H_0 + \dfrac{b}{d}t \to H = -720 + \dfrac{8}{1}t \\ \\ M = M_0 - \dfrac{a}{d}t \to M = 1440 - \dfrac{15}{1}t \end{cases} ; t \in \mathbb{Z}.$$

Portanto, as soluções para a equação $15H + 8M = 720$ são dadas por

$$S = \{(-720 + 8t, 1440 - 15t), \text{ com } t \in \mathbb{Z}\}.$$

Vejamos que, para o problema proposto as soluções precisam ser inteiras e positivas, ou seja, com $90 \leq t \leq 96$. As soluções desejadas para o problema podem ser visualizadas na Tabela 4.4.

Exemplo 4.8. Um fazendeiro pretende comprar filhotes de codorna e de galinha, gastando um total de R$ 1.770,00. O filhote de codorna custa R$ 31,00 e o de galinha custa R$ 21,00. Quantos filhotes de aves o fazendeiro poderá comprar?

Solução: Vamos modelar o problema da seguinte forma:

$$31C + 21G = 1770 \tag{4.25}$$

onde C representa o número filhotes de codornas e G representa o número filhotes de galinhas a serem compradas. Como $mdc(31, 21) = 1$ e 1 divide 1770 segue que a equação tem solução. Vamos encontrar uma solução particular. Para isso, usamos o algoritmo da Euclides:

$$31 = 21 \cdot (1) + 10 \tag{4.26}$$

$$21 = 10 \cdot (2) + 1. \tag{4.27}$$

Isolado os restos das igualdades (4.26) e (4.27) obtemos

$$10 = 31 + 21 \cdot (-1) \tag{4.28}$$

$$1 = 21 + 10 \cdot (-2). \tag{4.29}$$

Fazendo as devidas substituições temos

$$1 = 21+10\cdot(-2) = 21+(31-21)\cdot(-2) = 21\cdot(3)+31\cdot(-2) \Longrightarrow 1 = 31\cdot(-2)+21\cdot(3).$$

Multiplicando ambos os lados por 1770, obtemos

$$1770 = 31 \cdot (-3540) + 21 \cdot (5310).$$

Portanto, uma solução particular é $C_0 = -3540$ e $G_0 = 5310$. A solução geral da equação é dada por

$$S = \{(-3540 + 21t, 5310 - 31t), \text{ com } t \in \mathbb{Z}\}.$$

Observe que estamos interessados somente nas soluções positivas ou nulas, pois representam as quantidades das aves a serem compradas. Assim, temos que impor as seguintes condições

$$-3540 + 21t \geq 0 \text{ e } 5310 - 31t \geq 0.$$

Portanto, $21t \geq 3540$ e $31t \leq 5310$, que é o mesmo que $t \geq 168,57$ e $t \leq 171,29$. Assim, como t é um número inteiro, temos que $169 \leq t \leq 171$. Desse modo, as soluções são:

$$\begin{array}{llll} C = -3540 + 21 \cdot 169 = 9 & \text{e} & G = 5310 - 31 \cdot 169 = 71, & \text{ou} \\ C = -3540 + 21 \cdot 170 = 30 & \text{e} & G = 5310 - 31 \cdot 170 = 40, & \text{ou} \\ C = -3540 + 21 \cdot 171 = 51 & \text{e} & G = 5310 - 31 \cdot 171 = 9. & \end{array}$$

Através desses resultados podemos ver que o fazendeiro tem três alternativas para efetuar a compra de suas aves, são elas: 9 codornas e 71 galinhas ou 30 codornas e 40 galinhas, ou 51 codornas e 9 galinhas.

Exemplo 4.9. Um agricultor deve fazer uma plantação de eucaliptos e pinus. Cada muda de eucalipto custa R$ 0,40 e cada muda de pinus custa R$ 0,75. Sabendo que o agricultor dispõe de R$ 3500,00 para comprar mudas e que irá plantar no mínimo 1000 mudas de cada espécie, qual é o número máximo e o número mínimo de mudas que se pode comprar?

Solução: A equação que podemos extrair do problema é $0,75P + 0,40E = 3500$, sendo E o número de eucaliptos e P o número de pinus. Para resolver o problema deve-se achar uma equação diofantina equivalente a original, mas com coeficientes inteiros. Neste caso, uma multiplicação de toda equação por 100 resolverá a situação, isto é, $750P + 400E = 350.000$. Agora vamos calcular *mdc* dos coeficientes.

$$750 = 400 \cdot (1) + 350$$

$$400 = 350 \cdot (1) + 50$$

$$350 = 50 \cdot (7) + 0.$$

Como $mdc(750, 400) = 50$ e $50 \mid 350$ a equação $750P + 400E = 3500$ possui soluções inteiras. Isolando os restos nas igualdades acima e fazendo as devidas substituições, obtemos

$$50 = 400 + 350 \cdot (-1) = 400 + (750 - 400) \cdot (-1) = 750 \cdot (-1) + 400 \cdot (2).$$

Multiplicando a igualdade acima por 70.000, encontramos uma solução particular

$$350.000 = 750 \cdot (-70.000) + 400 \cdot (140.000).$$

Através da solução particular encontramos a solução geral do problema, dada por

$$S = \{(-70.000 + 8t, 140.000 - 15t), \text{ com } t \in \mathbb{Z}\}.$$

Agora vamos usar as informações do problema para delimitar os possíveis valores de t que fornecem as respostas exigidas do problema. Assim temos,

$$P = -70.000 + 8t \geq 0 \Longrightarrow t \geq 8875 \text{ e } E = 140.000 - 15t \geq 0 \Longrightarrow t \leq 9266.$$

O cálculo acima mostra que os valores de t que satisfazem as condições do problema são $8875 \leq t \leq 9266$.

Quanto menor o valor de t, maior será o número de mudas de eucalipto e menor o número de mudas de pinus, ou seja, quando $t = 8875$. Substituindo este valor na solução geral temos

$$P = -70.000 + 8 \cdot (8875) = 1000 \text{ e } E = 140.000 - 15 \cdot (8875) = 6875.$$

Totalizando 7875 mudas.

E quanto maior o valor de t, maior será o número de mudas de pinus e menor será o número de mudas de eucalipto, ou seja, quando $t = 9266$. Assim,

$$P = -70.000 + 8 \cdot (9266) = 4128 \text{ e } E = 140.000 - 15 \cdot (9266) = 1010.$$

Totalizando 5138 mudas.

Ao que vemos, o número máximo de mudas a serem plantadas será de 7875 e o número mínimo será de 5138 mudas.

Exemplo 4.10. O conteúdo de um barril de álcool destilado de 600 litros será distribuído em garrafas de $0,9l$ e de $1,5l$. Determine qual o maior e o menor número de garrafas que serão utilizadas, sabendo que devem ser usadas no mínimo 100 garrafas de cada quantidade.

Solução: Modelamos o problema através da equação diofantina $0,91x + 1,51y = 600$, onde x representa o número de garrafas de $0,9l$ e y representa o número de garrafas de $1,51l$. Tornando os coeficientes da equação pertencente ao conjunto dos números

inteiros, temos $9x + 15y = 6000$, que equivale a $3x + 5y = 2000$.
Aplicando o dispositivo prático do algoritmo de Euclides, obtemos

$$5 = 3 \cdot (1) + 2$$

$$3 = 2 \cdot (1) + 1.$$

Isolando os restos nas igualdades acima e fazendo as devidas substituições, temos

$$1 = 3 \cdot (-1) + 2 \cdot (-1) = 3 + (3 - 5) \cdot (-1) = 3 \cdot (2) + 5 \cdot (-1).$$

Multiplicando o resultado acima por 2000, obtemos

$$2000 = 3 \cdot (4000) + 5 \cdot (-2000),$$

onde $x_0 = 4000$ e $y_0 = -2000$. E, de modo semelhante aos cálculos realizados anteriormente, encontramos a solução geral do problema:

$$S = \{4000 + 5t, -2000 - 3t), \text{ com } t \in \mathbb{Z}\}.$$

Notemos que, é preciso restringir os valores de t, pois o número mínimo de cada garrafa deve ser 100 unidades. Logo,

$$x = 4000 + 5t \geq 100 \Longrightarrow t \geq -780 \text{ e } y = -2000 - 3t \geq 0 \Longrightarrow t \leq -700.$$

Analisando os valores extremos da variável t, o número máximo de garrafas ocorrerá quando $t = -700$. Vejamos

$$x = 4000 + 5 \cdot (-700) = 500 \text{ e } y = -2000 - 3 \cdot (-700) = 100.$$

Agora, o número mínimo de garrafas ocorrerá quando $t = -780$. Assim,

$$x = 4000 + 5 \cdot (-780) = 100 \text{ e } y = -2000 - 3 \cdot (-780) = 340.$$

Portanto as duas possibilidades exigidas no problema são: 500 garrafas de $0,9l$ e 100 de $1,5l$ ou 100 garrafas de $0,9l$ e 340 de $1,5l$.

Exemplo 4.11. Para transportar 31 estudantes de Rio Claro-SP a um evento que ocorreria em Campinas-SP, a Universidade Estadual Paulista (UNESP) disponibilizou 3 tipos de veículos, A, B e C, com capacidade de 4, 5 e 7 passageiros, respectivamente. Qual o número mínimo de veículos necessários para levar todos os estudantes de modo que pelo menos um veículo de cada tipo seja utilizado e todos os assentos sejam ocupados.

Solução: Sejam x, y e z respectivamente o números de veículos do tipo A, B e C, que foram disponibilizados pela UNESP. Como o veículo A tem capacidade para 4 passageiros, B para 5 passageiros e C, representamos o número de veículos do tipo A

por $4x$, do tipo B por $5y$ e do tipo C por $7z$. Assim, vemos que o número de veículos necessários para levar os estudantes pode ser representado pela expressão

$$4x + 5y + 7z = 31. \tag{4.30}$$

Para resolver este problema devemos, inicialmente, verificar se ele possui solução. Como $mdc(4, 5, 7) = 1$ e $1 \mid 31$, então a Equação (4.30) possui solução. Iniciamos buscando uma solução para a equação $4x + 5y = k$. Como $mdc(4, 5) = 1$, podemos escreve-lo como combinação linear

$$1 = 4 \cdot (-1) + 5 \cdot (1).$$

Multiplicando por k ambos os lados da igualdade, resulta

$$1k = 4 \cdot (-1k) + 5 \cdot (1k).$$

onde $x_0 = -1k$ e $y_0 = 1k$ é uma solução particular de $4x + 5y = k$. Sendo assim, a solução geral é dada por

$$S_1 = \{(-k + 5t_1, k - 4t_1), \text{ com } t_1 \in \mathbb{Z}\}.$$

Agora, vamos tomar a equação $k + 7z = 31$. Como $mdc(1, 7) = 1$, efetuando a combinação linear, obtemos

$$1 = 1 \cdot (8) + 7 \cdot (-1).$$

Para encontrarmos os inteiros k_0 e z_0 basta multiplicar ambos os membros da equação por 31, donde segue

$$31 = 1 \cdot (248) + 7 \cdot (-31).$$

Portanto, $k_0 = 248$ e $z_0 = -31$. Temos então que a solução geral da equação $k+7z = 31$ é dada por

$$S_2 = \{(248 + 7t_2, -31 - t_2), \text{ com } t_2 \in \mathbb{Z}\}.$$

Substituindo o valor de $k = 248 + 7t_2$ na solução geral S_1, encontrada para a equação $4x + 5y = k$, temos que

$$x = -k + 5t_1 \Longrightarrow -248 + 5t_1 - 7t_2 \text{ e } y = k - 4t_1 \Longrightarrow 248 - 4t_1 + 7t_2.$$

Concluímos então, que a solução geral da equação $4x + 5y + 7z = 31$ é:

$$S = \{(-248 + 5t_1 - 7t_2, 248 - 4t_1 + 7t_2, -31 - t_2), \text{ com } t_1, t_2 \in \mathbb{Z}\}.$$

Notemos que o problema requer soluções inteiras maiores que zero para x, y e z. Dessa forma, as soluções para este problema estão compreendidas no intervalo $-35, 4 < t_2 < -31$, que quando substituído na solução geral da equação $4x+5y+7z = 31$, geram todas as soluções do problema. Vejamos,

- Para $t_2 = -32$, temos que

$$x = -248 + 5t_1 - 7 \cdot (-32) > 0 \Longrightarrow t_1 > 4,8$$

e

$$y = 248 - 4t_1 + 7 \cdot (-32) > 0 \Longrightarrow t_1 < 6.$$

Logo $4,8 < t_1 < 6$ e como t_1 tem que ser inteiro tomamos $t_1 = 5$. Assim temos $x = 1, y = 4, z = 1$.

- Para $t_2 = -33$, segue

$$x = -248 + 5t_1 - 7 \cdot (-33) > 0 \Longrightarrow t_1 > 3,4$$

e

$$y = 248 - 4t_1 + 7 \cdot (-33) > 0 \Longrightarrow t_1 < 4,25.$$

Como t_1 tem que ser inteiro tomamos $t_1 = 4$. Assim temos $x = 3, y = 1, z = 2$.

- Para $t_2 = -34$, obtemos

$$x = -248 + 5t_1 - 7 \cdot (-34) > 0 \Longrightarrow t_1 > 2$$

e

$$y = 248 - 4t_1 + 7 \cdot (-34) > 0 \Longrightarrow t_1 < 2,5.$$

Podemos observar, que não existe inteiro t_1 no intervalo $2 < t_1 < 2,5$. Portanto, $t_2 = -34$ não é solução.

- Para $t_2 = -35$, temos

$$x = -248 + 5t_1 - 7 \cdot (-35) > 0 \Longrightarrow t_1 > 0,6$$

e

$$y = 248 - 4t_1 + 7 \cdot (-34) > 0 \Longrightarrow t_1 < 0,75.$$

Não exite inteiro t_1 no intervalo $0,6 < t_1 < 0,75$. Portanto, $t_2 = -34$ também não é solução.

Sendo assim, será necessário no mínimo 6 veículos para levar todos os estudantes ao evento, de modo que pelo menos um veículo de cada tipo seja utilizado e todos os assentos dos veículos utilizados sejam ocupados. Esse valor é obtido pela soma dos elementos da tripla ordenada $(1, 4, 1)$ e $(3, 1, 2)$ provenientes das soluções do problema. Portanto, o transporte dos estudantes pode ocorrer de duas maneira: 1 veículo do tipo A, 4 do tipo B e 1 do tipo C ou 3 veículos do tipo A, 1 do tipo B e 2 do tipo C.

5 Equações Diofantinas Quadráticas

Equações diofantinas quadráticas são equações algébricas em que o expoente de maior grau é igual a dois e cujas soluções então contidas no conjunto dos números inteiros. Tratamos aqui, apenas algumas dessas equações e veremos suas propriedades e aplicações. As principais referências utilizadas para o desenvolvimento deste capítulo foram [7] e [10].

5.1 Ternas Pitagóricas

Pitágoras da Ilha de Samos (atual Grécia) foi um filósofo e matemático grego que nasceu em Samos no ano de 570 a.C. e morreu provavelmente em 497 a.C em Metaponto (região sul da Itália). Ele descobriu uma relação muito interessante envolvendo o tamanho dos lados de triângulos retângulos, relação essa, hoje conhecida como Teorema de Pitágoras, o qual afirma que, dado um triângulo retângulo com as medidas c para a hipotenusa, a e b para os outros lados, então

$$a^2 + b^2 = c^2. \tag{5.1}$$

A fórmula para gerar todas as ternas (a, b, c) da Equação (4.21) foi conhecida desde a antiguidade e acha-se provada na obra *Arithmetica* de Diofanto. Mostramos que algumas dessas ternas podem ser encontradas através de fórmulas de fácil compreensão, e também vimos que tais ternas são infinitas. De modo geral, 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.

Definição 5.1. *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 $mdc(x, y, z) = 1$.

Exemplo 5.1. São ternas pitagóricas

$$(3, 4, 5),\ (10, 24, 26) \text{ e } (5, 12, 13)$$

pois temos:

$3^2 + 4^2 = 5^2$, $10^2 + 24^2 = 26^2$ e $5^2 + 12^2 = 13^2$, respectivamente.

Proposição 5.1. *Se (x, y, z) é uma terna pitagórica, com $k \geq 1$, então (xk, yk, zk) também será uma terna pitagórica.*

Demonstração. Tomando nos lugares de x e y os respectivos valores xk e yk, temos

$$(xk)^2 + (yk)^2 = x^2k^2 + y^2k^2 = (x^2 + y^2)k^2 = z^2k^2 = (zk)^2.$$

□

Exemplo 5.2. Tomemos a terna pitagórica $(5, 12, 13)$. Note que para $k = 3$ teremos $(15, 36, 39)$, que também é uma terna pitagórica, pois

$$15^2 + 36^2 = 225 + 1296 = 1521 = 39^2.$$

Exemplo 5.3. Vejamos que,

- $(3, 4, 5), (6, 8, 10), ..., (3k, 4k, 5k), ...$
- $(12, 35, 37), (24, 70, 74), ..., (12k, 35k, 37k), ...$

Note que, todas são ternas pitagóricas, sendo que $(3, 4, 5)$ e $(12, 35, 37)$ são primitivas, pois $mdc(3, 4, 5) = mdc(12, 35, 37) = 1$.

Proposição 5.2. *Seja (x, y, z) uma terna pitagórica primitiva. Então*

$$mdc(x, y) = mdc(y, z) = mdc(x, z) = 1.$$

O que significa que x, y e z são relativamente primos dois a dois.

Demonstração. Seja $d = mdc(x, y) = 1$. Se $s > 1$, então existe um divisor p primo de d. Logo, $p \mid x$ e $p \mid y$, então $p \mid x^2 + y^2 = z^2$ e também $p \mid z$. O que nos leva à contradição $p \leq mdc(x, y) = 1$. Da mesma forma se prova que $(y, z) = (x, z) = 1$. □

Proposição 5.3. *Sejam (x, y, z) uma terna pitagórica qualquer, $d = mdc(x, y, z)$ e os quocientes $x_1 = \frac{x}{d}, y_1 = \frac{y}{d}, z_1 = \frac{z}{d}$. Então (x_1, y_1, z_1) formam uma terna pitagórica primitiva e vale (dx_1, dy_1, dz_1).*

Demonstração. Sabemos que o $mdc(x_1, y_1, z_1) = 1$ e vale $(x, y, z) = (dx_1, dy_1, dz_1)$. Além disso,

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

mostrando que (x_1, y_1, z_1) é uma terna pitagórica primitiva. □

Portanto, é possível obter qualquer terna pitagórica não primitiva de uma terna pitagórica primitiva, bastando multiplicar os seus elementos por um inteiro positivo maior do que 1, ou seja, todas as soluções de $x^2 + y^2 = z^2$ resultam daquelas de (x_1, y_1, z_1), onde $mdc(x_1, y_1, z_1) = 1$.

Exemplo 5.4. Vejamos que a terna pitagórica $(16, 30, 34)$ não é primitiva, pois $mdc(16, 30) = 2 \neq 1$, porém, podemos encontrar a sua primitiva. De fato, basta dividir a terna pitagória $(16, 30, 34)$ pelo $mdc(16, 30) = 2$, donde obtemos sua primitiva $(8, 15, 17)$.

Teorema 5.1. *Se (x, y, z) é uma terna pitagórica primitiva então exatamente um dos números x ou y é par, o outro é impar e z é ímpar.*

Demonstração. Suponhamos x e y ambos pares. Então $z^2 = x^2 + y^2$ e também z é par, o que exclui a possibilidade de x e y serem pares.

Suponhamos agora, x e y ambos ímpares, digamos $x^2 = 4k + 1$ e $y^2 = 4l + 1$. Segue $z^2 = x^2 + y^2 = 4(k + l) + 2 \equiv 2 \ (mod\ 4)$, o que é impossível para um quadrado, pois os mesmos são congruentes a 0 ou a 1 módulo 4. Vejamos:

- Caso em que z for ímpar:

$$z^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \ (mod\ 4).$$

- Caso em que z for par

$$z^2 = (2k)^2 \equiv 0 \ (mod\ 4),$$

o que nos leva a concluir que x e y têm paridades distintas e z é ímpar. □

Para eliminar possíveis confusões, a partir deste momento fixamos x como sendo par e y ímpar quando (x, y, z) é uma terna pitagórica primitiva.

Teorema 5.2. *1. As ternas pitagóricas primitivas (x, y, z) da equação*

$$x^2 + y^2 = z^2 \tag{5.2}$$

são da forma

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

com $mdc(m, n) = 1$ e $m - n$ é ímpar.

2. Qualquer terna pitagórica primitiva é obtida pelo método do item 1.

Demonstração. 1. Primeiro assumiremos $x^2 + y^2 = z^2$ e que $x = 2mn, y = m^2 - n^2, z = m^2 + n^2$. Sendo assim temos:

$$x^2 + y^2 = (2mn)^2 + (m^2 - n^2)^2 = 4m^2n^2 + m^4 + n^4 - 2m^2n^2 =$$

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

o que nos mostra que (x, y, z) é uma terna pitagórica.

Suponhamos agora, que $p \mid mdc(x, y, z)$ para algum p primo. Então p é ímpar e de $p \mid 2mn$, donde segue que $p \mid m$ ou $p \mid n$. Observe que $z = m^2 + n^2$ (ou de $y = m^2 - n^2$) segue então que $p \mid m$ e $p \mid n$, resultando em $p \leq mdc(m, n) = 1$, o que é um absurdo.

Portanto, (x, y, z) é uma terna primitiva.

2. Seja (x, y, z) uma terna pitagórica primitiva qualquer, com x par e y ímpar. Reescrevendo a equação (4.22), temos

$$x^2 = z^2 - y^2 = (z + y)(z - y)$$

e daí

$$\frac{x^2}{4} = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right). \tag{5.3}$$

Então

$$\left(\frac{x}{2}\right)^2 = uv \quad com \quad u = \frac{z+y}{2} \quad e \quad v = \frac{z-y}{2}. \tag{5.4}$$

Se $d = mdc(u, v)$, então $d \mid u \pm v$. Mas, $u + v = \dfrac{z+y}{2} + \dfrac{z-y}{2} = z$ e $u - v = \dfrac{z+y}{2} - \dfrac{z-y}{2} = y$, daí $d \mid mdc(y, z)$. Como (x, y, z) é primitiva, segue que $mdc(x, y) = mdc(y, z) = mdc(x, z) = 1$. Logo, $mdc(u, c) = 1$. Pelo Lema 2.1, sabemos que tanto u quanto v são individualmente quadrados perfeitos. Sendo assim, podemos tomar $u = m^2$ e $v = n^2$ com $m, n \in \mathbb{N}$. Temos então $mdc(m, n) = mdc(u, v) = 1$ e $m - n$ é ímpar. Além disso, $m^2 - n^2 = u - v = y$ e $m^2 + n^2 = u + v = z$. Por fim, podemos concluir de (5.3) e (5.4) que $\dfrac{x^2}{4} = uv = n^2m^2$ donde segue $x = \sqrt{4n^2m^2} = 2mn$. □

Como resultado da demonstração acima temos que as ternas pitagóricas, tanto primitivas quanto as não-primitivas, podem ser obtidas por

$$(x, y, z) = (2mnk, (m^2 - n^2)k, (m^2 + n^2)k),$$

onde $m, n, k \in \mathbb{N}$ com $m > n \geq 1$, $mdc(m, n) = 1, m - n$ ímpar.

Exemplo 5.5. Encontrar todas as soluções inteiras da equação $x^2 + y^2 = 2z^2$.

Vejamos que, na equação

$$x^2 + y^2 = 2z^2, \tag{5.5}$$

devemos ter x e y com a mesma paridade, pois caso contrário $x^2 + y^2$ seria um número ímpar, o que não pode ocorrer, já que $2z^2$ é par. Sendo assim, existem inteiros $u = \dfrac{1}{2}(x + y)$ e $v = \dfrac{1}{2}(x - y)$ tais que

$$x = u + v, y = u - v,$$

que ao serem substituídos na Equação (5.5) resulta,

$$x^2 + y^2 = (u + v)^2 + (u - v)^2 = 2u^2 + 2v^2 = 2z^2 \rightarrow u^2 + v^2 = z^2,$$

ou seja,

$$x^2 + y^2 = 2z^2 \Longleftrightarrow u^2 + v^2 = z^2.$$

Observamos que a última equação é correspondente a Equação de Pitágoras. Então, de acordo com o Teorema 5.2, podemos afirmar

$$(u, v, z) = (2mnk, (m^2 - n^2)k, (m^2 + n^2)k),$$

onde $m, n, k \in \mathbb{N}$ com $m > n \geq 1$, $mdc(m, n) = 1, m - n$ ímpar. Segue daí que as soluções (x, y, z) da Equação (5.5) são do tipo,

$$(x, y, z) = (2mnk + (m^2 - n^2)k, 2mnk - (m^2 - n^2)k, (m^2 + n^2)k)$$

onde m, n e k satisfazem às mesmas condições do Teorema 5.2.

5.2 Frações Contínuas

Apresentamos, a seguir, um estudo sobre frações contínuas, o qual nos permite representar um número racional por uma sequência finita de inteiros e também um número irracional por uma sequência infinita de inteiros. Tais representações permitem encontrar uma aproximação de um número irracional por um número racional, tão próximo quanto desejarmos. Essa seção foi fundamental para o estudo da equação de Pell, e grande parte das exposições desta seção é baseada em [10] e [11].

Definição 5.2. *(Frações Contínuas) Seja α um número real. Uma expressão finita ou infinita da forma*

$$\alpha = [a_0; a_1, a_2, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}, \forall i \in \mathbb{N} \tag{5.6}$$

onde a_i são números reais, com $a_1, a_2, \ldots \geq 1$, se chama representação por frações contínuas de α. Os números a_i são chamados de quocientes parciais da fração contínua.

A fração contínua (5.6) é chamada simples se os quocientes parciais a_i são todos inteiros. Ela será finita se ela terminar, isto é, se for da forma

$$\alpha = [a_0; a_1, a_2, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}, \forall n \in \mathbb{N}.$$

Caso contrário será infinita.

Denotamos a_0 como sendo a parte inteira de α, ou seja, $a_0 = \lfloor \alpha \rfloor \in \mathbb{Z}$. Observe que o termo a_0 é separado por ponto e vírgula para evidenciar a parte inteira do número representado.

Definição 5.3. *A fração contínua infinita* $\alpha = [a_0; a_1, a_2, a_3, \ldots]$ *será chamada de fração contínua periódica quando* a_n *começar a repetir para um determinado* $n = 0, 1, 2, \ldots$, *ou seja, quando estiver da forma* $\alpha = [a_0; a_1, a_2, r, s, r, s, \cdots] = [a_0; a_1, a_2, \overline{r, s}]$, *com* $r, s \in \mathbb{N}$. *Sendo que, quando o período iniciar em* a_0 *essa fração contínua será chamada de fração contínua periódica pura.*

Vejamos que, se a representação por frações contínuas de α for finita então α é claramente racional. Observamos que, para obtermos uma fração contínua de certo número racional, basta aplicar o algoritmo da divisão de Euclides sucessivamente numa divisão de inteiros. Por exemplo, tomemos um racional $\alpha = \dfrac{p}{q}$, $mdc(p, q) = 1$ com $q > 0$, temos que existem únicos a_0 e r_1 tais que $p = a_0 q + r_1$, com $0 \leq r_1 < q$, logo

$$\alpha = \frac{p}{q} = \frac{a_0 q}{q} + \frac{r_1}{q} = a_0 + \frac{r_1}{q} = a_0 + \frac{1}{\frac{q}{r_1}}.$$

Para q e r_1, obtemos únicos a_1 e r_2 tal que $q = a_1 r_1 + r_2$, com $0 \leq r_2 < r_1$, logo

$$\alpha = \frac{p}{q} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_2}}.$$

Repetindo esse processo sucessivamente, obtemos

$$x = \frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} = [a_0; a_1, ..., a_n].$$

Sabemos que o algoritmo da divisão de Euclides é um processo finito, sendo assim, esse também o é, e esta última expressão é a fração contínua que representa o número racional $\alpha = \dfrac{p}{q}$.

Exemplo 5.6. A representação de $\dfrac{542}{234}$ em frações contínuas é dada por $[2; 3, 6, 6]$, pois

$$\begin{aligned} \frac{542}{234} &= 2 + \frac{74}{234} = 2 + \frac{1}{\frac{234}{74}} = 2 + \frac{1}{3 + \frac{12}{74}} = 2 + \frac{1}{3 + \frac{1}{\frac{74}{12}}} = 2 + \frac{1}{3 + \frac{1}{6 + \frac{2}{12}}} \\ &= 2 + \frac{1}{3 + \frac{1}{6 + \frac{1}{\frac{12}{2}}}} = 2 + \frac{1}{3 + \frac{1}{6 + \frac{1}{6}}} = [2; 3, 6, 6]. \end{aligned}$$

Vimos que, qualquer número racional pode ser representado sob a forma de uma fração contínua

$$\frac{p}{q} = [a_1; a_1, a_2, \ldots, a_n],$$

onde $a_n \in \mathbb{Z}, \forall n \geq 0$ e $a_1, a_2, \ldots, a_n$ são todos inteiros positivos.

Consideremos as frações

$$\alpha_0 = \frac{a_0}{1}, \alpha_1 = a_0 + \frac{1}{a_1}, \alpha_2 = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}}, \ldots$$

obtidos pelas expansões das frações contínuas

$$[a_0], [a_0; a_1], [a_0; a_1; a_2], \cdots .$$

Estas frações são chamadas de primeiro, segundo, terceiro,..., convergentes, respectivamente, da fração contínua $\alpha = [a_0; a_1, a_2, \ldots, a_n]$. Sendo que, o n-ésimo termo dessa fração é chamado de n-ésima reduzida ou convergente da fração contínua de α e será igual à própria fração contínua.

Nos resultados a seguir mostraremos algumas propriedades satisfeitas pelos convergentes de uma fração contínua. Denotamos $\dfrac{p_n}{q_n}$ como sendo a n-ésima convergente da fração contínua de α.

Proposição 5.4. *Dada uma sequência (finita ou infinita)* $a_0, a_1, a_2, \cdots \in \mathbb{R}$ *tal que* $a_k > 0$*, para todo* $k \geq 1$*, definimos sequências* (p_m) *e* (q_m) *por* $p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1, p_m = a_m p_{m-1} + p_{m-2}, q_m = a_m q_{m-1} + q_{m-2}$*, para todo* $m \geq 0$*. Temos então*

$$[a_0; a_1, a_2, ..., a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} = \frac{p_n}{q_n}, \forall n \geq 0$$

Demonstração. Provamos por indução em n. Para $n = 0$ temos

$$[a_0] = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}.$$

Para $n = 1$, temos

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{p_1}{q_1}$$

e, para $n = 2$, temos

$$[a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1} = \frac{a_2(a_0a_1 + 1) + a_0}{a_1a_2 + 1}$$

$$= \frac{a_2p_1 + p_0}{a_2q_1 + q_0} = \frac{p_2}{q_2}.$$

Assumimos que a afirmação seja válida para n. Agora, estamos prontos para provar que a relação é valida para $n + 1$. Lembramos que, o $(n + 1)$-*ésimo* convergente

$[a_0; a_1, a_2, \ldots, a_n, a_{n+1}]$ é obtido substituindo na expressão do *n-ésimo* convergente $[a_0; a_1, a_2, \ldots, a_n]$ o número a_n por $a_n + \dfrac{1}{a_{n+1}}$, portanto,

$$[a_0; a_1, a_2, ..., a_n, a_{n+1}] = \left[a_0; a_1, a_2, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right].$$

Observamos que a substituição de a_n por $a_n + \dfrac{1}{a_{n+1}}$ não altera a definição dos $a_0, a_1, a_2, \ldots, a_{n-1}$ precedentes, pois,

$$\frac{p_{n-1}}{q_{n-1}} = \frac{a_{n-1}p_{n-2} + q_{n-3}}{a_{n-1}q_{n-2} + q_{n-3}}.$$

Portanto, como os números $p_{n-2}, p_{n-3}, q_{n-2}, q_{n-3}$ são independentes do quociente a_n, eles não se alteram com esta substituição. Sendo assim,

$$\begin{aligned}
[a_0; a_1, a_2, \ldots, a_n, a_{n+1}] &= \left[a_0; a_1, a_2, \ldots, a_{n-1}, a_n + \frac{1}{a_{n+1}}\right] \\
&= \frac{\left(a_n + \dfrac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \dfrac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\
&= \frac{(a_{n+1}a_n + 1)p_{n-1} + a_{n+1}p_{n-2}}{(a_{n+1}a_n + 1)q_{n-1} + a_{n+1}q_{n-2}} \\
&= \frac{a_{n+1}a_np_{n-1} + a_{n+1}p_{n-2} + p_{n-1}}{a_{n+1}a_nq_{n-1} + a_{n+1}q_{n-2} + q_{n-1}} \\
&= \frac{a_{n+1}(a_np_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_nq_{n-1} + q_{n-2}) + q_{n-1}} \\
&= \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}.
\end{aligned}$$

□

Lema 5.1. *As igualdades* $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$ *e* $p_nq_{n-2} - p_{n-2}q_n = (-1)^n a_n$, *se verificam para* $n \geq 1$, *onde* p_n *e* q_n *são, respectivamente, o numerador e o denominador do n-ésimo convergente.*

Demonstração. Mostramos por indução, a primeira igualdade. Para $n = 1$ temos

$$p_1q_0 - p_0q_1 = (a_0a_1 + 1) - a_0a_1 = 1 = (-1)^0.$$

Vamos assumir, como hipótese de indução, a validade de $p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$ e mostrar que a mesma relação também se verifica quando substituímos n por $n+1$. Na Proposição 5.4, vimos que

$$p_n = a_n p_{n-1} + p_{n-2} \text{ e } q_n = a_n q_{n-1} + q_{n-2}$$

Logo,

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= p_{n-2} q_{n-1} + a_n p_{n-1} q_{n-1} - a_n p_{n-1} q_{n-1} - p_{n-1} q_{n-2} \\ &= (-1)(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}). \end{aligned}$$

Usando a hipótese de indução, obtemos

$$p_n q_{n-1} - p_{n-1} q_n = (-1)(-1)^n = (-1)^{n-1},$$

o que conclui a demonstração da primeira igualdade.

Para demonstrar a segunda igualdade, isto é, demonstrar que $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$, fazemos

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - (a_n q_{n-1} + q_{n-2} p_{n-2} \\ &= a_n p_{n-1} q_{n-2} + p_{n-2} q_{n-2} - p_{n-2} q_{n-2} - a_n p_{n-2} q_{n-1} \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\ &= (1)^{n-2} a_n \\ &= (-1)^n a_n \end{aligned}$$

o que conclui a demonstração da segunda igualdade e, portanto, do lema. □

Corolário 5.1. *Seja α um número real. Para $n = 0, 1, 2, \ldots$ definimos recursivamente: $\alpha_0 = \alpha, a_n = \lfloor \alpha_n \rfloor, \alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$ e*

$$[a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_{n+1}] = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}.$$

Demonstração. A igualdade acima segue da Proposição 5.4 □

Observação 5.1. Notemos que, da equação $\alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$ segue que, α_n é positivo para todo $n \geq 0$, pois, $\dfrac{1}{\alpha_{n+1}} = \alpha_n - \lfloor \alpha_n \rfloor$. Assim, o lado esquerdo da equação é menor que 1 e, portanto, $\alpha_{n+1} > 1$. Portanto, a_{n+1} é um inteiro positivo e concluímos que $\alpha_n, a_n \geq 1$ para $n \geq 1$.

Corolário 5.2. *Para todo convergente $\dfrac{p_n}{q_n}$ tem-se que $mdc(p_n, q_n) = 1$.*

Demonstração. Pelo Lema 5.1, segue que $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$. Isto nos diz que qualquer divisor de p_n e q_n deve ser divisor de 1 ou -1. Logo, o máximo divisor comum de p_n e q_n deve ser igual a 1. □

Teorema 5.3. *Seja α um número irracional e $\dfrac{p_n}{q_n}$ os convergentes da expansão de α em frações contínuas. Então*

$$\alpha - \frac{p_n}{q_n} = \frac{1}{q_n(\alpha_{n+1} q_n + q_{n+1})}.$$

Demonstração. Como $\alpha = [a_0; a_1, \ldots, a_n, \alpha_{n-1}]$, segue do Corolário 5.1 que

$$\begin{aligned}
\alpha - \frac{p_n}{q_n} &= \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\
&= \frac{p_{n-1}q_n + \alpha_{n+1}p_nq_n - \alpha_{n+1}p_nq_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
&= \frac{p_{n-1}q_n - p_nq_{n-1}}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
&= \frac{(-1)(p_nq_{n-1} - q_np_{n-1})}{q_n(\alpha_{n+1}q_n + q_{n-1})}.
\end{aligned}$$

Pelo Lema 5.1,

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}.$$

□

Notemos que, $a_n \leq \alpha_n$, pois a fração contínua pode ser finita ou infinita. Além disso, como q_{-1}, q_0 e $a_n (n > 0)$ são inteiros positivos, o mesmo deve ser verdadeiro para $q_n\,(n > 0)$, por definição. Logo,

$$\begin{aligned}
\left|\alpha - \frac{p_n}{q_n}\right| &= \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} \\
&< \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} \\
&= \frac{1}{q_nq_{n+1}} < \frac{1}{q_n^2}.
\end{aligned}$$

Por definição, $q_n = a_nq_{n-1} + q_{n-2}$. Como $1 \leq a_n$ e $q_{n-2} > 0$, concluímos que q_n é estritamente crescente à medida que n aumenta. Portanto,

$$\alpha = \lim_{n\to\infty} \frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots],$$

ou seja, o limite da sequência dos convergentes da representação do irracional α sob a forma de fração contínua é igual ao próprio α.

Proposição 5.5. *Para todo $k \geq 0$, temos*

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq \alpha \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}.$$

Demonstração. O resultado segue dos seguintes fatos gerais. Para todo $n \geq 0$, temos que

$$\begin{aligned}\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} &= \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} \\ &= \frac{a_{n+2}(p_{n+1}q_n - p_nq_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{(-1)^n a_{n+2}}{q_{n+2}q_n}\end{aligned}$$

é positivo para n par e negativo para n ímpar. Além disso, para todo $n \geq 0$, temos que

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(\alpha_{n+1}q_n + q_{n-1})}$$

é positivo para n par e negativo para n ímpar. □

Corolário 5.3. *Seja α um número real com convergente $\frac{p_n}{q_n}$. Então*

$$|q_n\alpha - p_n| < |q_{n-1}\alpha - p_{n-1}|.$$

Demonstração. Pelo Teorema 5.3,

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} \Rightarrow |q_n\alpha - p_n| = \frac{1}{q_n\alpha_{n+1} + q_{n-1}}.$$

De modo similar,

$$|q_{n-1}\alpha - p_{n-1}| = \frac{1}{q_{n-1}\alpha_n + q_{n-2}}.$$

Basta agora provar a seguinte desigualdade:

$$\frac{1}{q_n\alpha_{n+1} + q_{n-1}} < \frac{1}{q_{n-1}\alpha_n + q_{n-2}}. \tag{5.7}$$

Observe que

$$\begin{aligned}1q_{n-1}\alpha_n + q_{n-2} &= \frac{1}{q_{n-1}\left(a_n + \frac{1}{\alpha_{n+1}}\right) + q_{n-2}} = \frac{1}{q_{n-1}a_n + \frac{q_{n-1}}{\alpha_{n+1}} + q_{n-2}} \\ &= \frac{\alpha_{n+1}}{q_{n-1}a_n\alpha_{n+1} + q_{n-1} + q_{n-2}\alpha_{n+1}}.\end{aligned} \tag{5.8}$$

Suponha que a Desigualdade (5.7) não seja válida. Substituindo (5.8) no lado direito de (5.7) segue, de acordo com nossa suposição, que

$$\begin{aligned}\alpha_{n+1}(q_{n-1}a_n + q_{n-2}) + q_{n-1} &> q_n\alpha_{n+1}^2 + q_{n-1}\alpha_{n+1} \\ q_n\alpha_{n+1} + q_{n-1} &> \alpha_{n+1}(q_n\alpha_{n+1} + q_{n-1}) \\ 1 &> \alpha_{n+1},\end{aligned}$$

o que é um absurdo, pela Observação 5.1. Portanto, a Desigualdade (5.7) é válida.

□

Teorema 5.4. *(Boas Aproximações) Seja α um número real com a convergente $\frac{p_n}{q_n}$ e $n \geq 2$. Se p, q são inteiros tais que $0 < q \leq q_n$ e $\frac{p}{q} \neq \frac{p_n}{q_n}$, então*

$$|q_n\alpha - p_n| < |q\alpha - p|.$$

Além disso, uma fração reduzida $\frac{p'}{q'}$ com $q' \geq q_2$ que satisfaz a última desigualdade é uma convergente.

Demonstração. Pelo Corolário 5.3, já provamos o caso em que $\frac{p_n}{q_n}$ é um convergente. Supomos agora, $q = q_n$. Daí, da hipótese segue que, $p \neq p_n$. Temos

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| = \frac{|p - p_n|}{q_n} \geq \frac{1}{q_n} \text{ e } \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{2q_n}$$

pois, $q_{n+1} \geq 3$ se $n \geq 2$ (q_n é estritamente crescente para $n \geq 1$ e $q_1 \geq q_0 = 1$). Pela desigualdade triangular, temos

$$\begin{aligned}\left|\alpha - \frac{p}{q}\right| &\geq \left|\frac{p}{q} - \frac{p_n}{q_n}\right| - \left|\alpha - \frac{p_n}{q_n}\right| \\ &> \frac{1}{q_n} - \frac{1}{2q_n} = \frac{1}{2q_n} \\ &> \left|\alpha - \frac{p_n}{q_n}\right|.\end{aligned}$$

Multiplicando ambos os lados por $q = q_n$, obtemos a desigualdade desejada. Agora supomos $0 < q < q_n$. Podemos configurar o seguinte sistema de duas equações com duas variáveis x e y:

$$\begin{cases} p_n x + p_{n-1} y = p \\ q_n x + q_{n-1} y = q. \end{cases} \tag{5.9}$$

Realizando algumas manipulações algébricas no sistema de equações acima, chegamos no seguinte resultado para x e y:

$$x = \frac{pq_{n-1} - qp_{n-1}}{p_n q_{n-1} - p_{n-1} q_n} \text{ e } y = \frac{pq_n - qp_n}{p_n q_{n-1} - p_{n-1} q_n}.$$

Pelo Lema 5.1, os denominadores se reduzem a ± 1, ou seja,

$$\begin{aligned} x &= \pm(pq_{n-1} - qp_{n-1} \\ y &= \pm(pq_n - qp_n). \end{aligned}$$

Pelo Lema 5.1, o determinante principal do sistema é ± 1 e, consequentemente, este sistema possui uma solução em inteiros x e y.

Na realidade, x e y são diferentes de zero. Isto porque se $x = 0$ teremos $q = yq_{n-1}$, o que implica $y > 0$ e $q \geq q_{n-1}$, em contradição com $q < q_n$. Se $y = 0$ então $p = xp_n, q = xq_n$ e

$$\begin{aligned}|q\alpha - p| &= |xq_n\alpha - xp_n| \\ &= |x||q_n\alpha - p_n| \geq |q_n\alpha - p_n|,\end{aligned}$$

uma vez que, $|x| \geq 1$, o que nos dá uma contradição. Novamente pelo Lema 5.1 temos que, $\alpha - \dfrac{p_n}{q_n}$ alternam os sinais, isto é, $\alpha - \dfrac{p_n}{q_n}$ e $\alpha - \dfrac{p_{n-1}}{q_{n-1}}$ possuem sinais opostos. Isso implica que $q_n\alpha - p_n$ e $q_{n-1}\alpha - p_{n-1}$ também têm sinais opostos. Portanto, $x(q_n\alpha - p_n)$ e $y(q_{n-l}\alpha - p_{n-1})$ possuem o mesmo sinal. Daí,

$$\begin{aligned} q\alpha - p &= (q_n x + q_{n-1}y)\alpha - (p_n x + p_{n-1}y) \\ &= x(q_n\alpha - p_n) + y(q_{n-1}\alpha - p_{n-1}). \end{aligned}$$

Logo,

$$\begin{aligned} |q\alpha - p| &= |x(q_n\alpha - p_n)| + |y(q_{n-1}\alpha - p_{n-1})| \\ &> |q_{n-1}\alpha - p_{n-1}| \\ &> |q_n\alpha - p_n|, \end{aligned}$$

o que conclui a demonstração. □

Teorema 5.5. *1. Dados quaisquer dois convergentes consecutivos para um número real α, pelo menos um vai satisfazer a desigualdade*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}. \tag{5.10}$$

2. Qualquer fração reduzida que satisfaça a desigualdade (5.10) é uma convergente da expansão de α.

Demonstração. 1. Pela Proposição 5.4, temos que, o número α sempre pertence ao segmento de extremos $\dfrac{p_n}{q_n}$ e $\dfrac{p_{n+1}}{q_{n+1}}$. Portanto,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\frac{p_n}{q_n} - \alpha\right|.$$

Agora, suponhamos que a desigualdade (5.10) não é verdadeira para alguns convergentes consecutivos $\dfrac{p_n}{q_n}$ e $\dfrac{p_{n+1}}{q_{n+1}}$. Pelo Lema 5.1,

$$\begin{aligned} \frac{1}{q_n q_{n+1}} &= \left|\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\frac{p_n}{q_n} - \alpha\right| \\ &\geq \frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2} = \frac{q_n^2 + q_{n+1}^2}{2q_n^2 q_{n+1}^2}. \end{aligned}$$

Logo,

$$2q_n q_{n+1} \geq q_n^2 + q_{n+1}^2 \Rightarrow 0 \geq (q_n - q_{n+1})^2.$$

Como q_n é estritamente crescente para n positivo, isso pode ser verdadeiro se, e somente se, $n = 0$ e $q_1 = q_0 = a_1 = 1$. Assim, por contradição, *1.* é verdadeiro para

todo n positivo. Por fim, só precisamos provar o caso em que $n = 0$, (sendo os dois convergentes consecutivos $\frac{p_0}{q_0}$ e $\frac{p_1}{q_1}$):

$$0 < \frac{p_1}{q_1} - \alpha \quad = a_1 a_0 + 1 - \alpha = a_0 + 1 - \alpha = a_0 + 1 - [a_0; 1, a_2, a_3, \ldots]$$

$$< 1 - \frac{1}{1 + \frac{1}{a_2}} = 1 - \frac{a_2}{a_2 + 1} \leq \frac{1}{2}.$$

O que prova o item *1.*

2. Suponhamos que $\frac{p}{q}$ satisfaça a Desigualdade (5.10). Pelo Teorema 5.4 basta mostrar que $\frac{p}{q}$ é a melhor aproximação para α. Seja $\frac{a}{b}$, tal que $\frac{a}{b} \neq \frac{p}{q}$ e $|b\alpha - a| \leq |q\alpha - p| = q\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q}$.

Então,

$$\frac{1}{qb} \quad \leq \frac{|pb - aq|}{qb} = \left|\frac{p}{q} - \frac{a}{b}\right| \leq \left|\alpha - \frac{p}{q}\right| + \left|\frac{a}{b} - \alpha\right| < \frac{1}{2q^2} + \frac{1}{2qb} = \frac{q + b}{2q^2 b}$$

$$\Rightarrow 1 \quad < \frac{q + b}{2q} \Rightarrow 2q < q + b \Rightarrow q < b.$$

Portanto, $\frac{p}{q}$ é uma melhor aproximação. □

5.3 Equação de Pell

A equação de Pell é um caso particular das equações diofantinas quadráticas da forma $x^2 - Ay^2 = n$. Mais precisamente é uma equação do tipo

$$x^2 - Ay^2 = 1, \tag{5.11}$$

com x, y inteiros e A um número inteiro positivo e diferente de um quadrado perfeito. Nos casos em que $A < 0$ e $A > 0$ é um quadrado perfeito, mostramos que a Equação (5.11) possui um número finito de soluções, e para $A = 0$ um número infinito. Porém, o fato da Equação (5.11) ter um número infinito de soluções para qualquer A positivo, em que A não é um quadrado perfeito, deu origem a um teorema bastante interessante, o qual foi demonstrado após um breve apanhado histórico sobre tal equação.

Um fato bastante interessante é que, curiosamente encontramos em diversos livros a Equação (5.11) sendo chamada como equação de Pell, pois o próprio Euler (1707-1783) a denominou assim acreditando que os resultados sobre a equação tinham sido descobertos pelo matemático inglês John Pell (1811-1685), porém, a única contribuição

de Pell para o assunto foi uma publicação de alguns resultados parciais que tinham sido de fato, encontrado por William Brouncker (1620-1684), em resposta a um desafio de Fermat. De acordo com [6], o método para encontrar a solução da equação de Pell apresentado por Brouncker é substancialmente idêntico a um método conhecido por matemáticos indianos pelo menos seis séculos antes. A equação de Pell também apareceu na matemática grega, mas não houve nenhuma evidência convincente de que os gregos podiam resolver a equação. Uma exposição de como encontrar a solução da equação de Pell pode ser encontrada na obra "Álgebra de Euler" escrita por Euler em 1770. Os livros modernos geralmente dão uma formulação em termos de Frações Contínuas, o que também é devido a Euler.

Joseph Louis Lagrange (1736-1813) foi o primeiro a provar que, contanto que na equação

$$x^2 - Ay^2 = 1,$$

o valor de A não seja um quadrado perfeito, a equação de Pell tem infinitas soluções inteiras distintas. Estas soluções podem ser usadas para aproximar com precisão a raiz quadrada de A por números racionais da forma $\frac{p}{q}$. As principais referências utilizadas para o desenvolvimento desta seção foram [11] e [10].

5.3.1 Soluções Triviais da Equação $x^2 - Ay^2 = 1$

Analisamos inicialmente os casos triviais. Tomando $A < -1$, como $1 \geq |A|y^2$, obtemos

$$y = 0, x = \pm 1.$$

Tomando $A = -1$,

$$x^2 - (-1)y^2.$$

Certamente temos quatro soluções

$$x = \pm 1, y = 0; \quad x = 0, y \pm 1.$$

Tomando $A = b^2 > 0$, temos que

$$x^2 - Ay^2 = x^2 - b^2y^2 = (x + by)(x - by) = 1,$$

donde observamos que

$$(x + by) = (x - by) = \pm 1.$$

Sendo assim,

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

Tomando $A = 0$,

$$x^2 = 1,$$

neste caso a equação é verdadeira para $x = \pm 1$ e para qualquer y.

O caso interessante desta equação é exatamente quando A não é um quadrado perfeito, ou seja, $\sqrt{A}$ é um irracional (de fato, se $\sqrt{A} = \frac{p}{q}$, com $mdc(p,q) = 1$ e $q > 1$, teríamos $A = \frac{p^2}{q^2}$ o que é um absurdo, pois $mdc(p,q) = 1$ e $q > 1 \to q^2 > 1 \to mdc(p^2, q^2) = 1$, donde $\frac{p^2}{q^2}$ não pode ser inteiro). Neste caso, a equação $x^2 - Ay^2 = 1$ é conhecida como *equação de Pell.*

Definição 5.4. *A equação de Pell é uma equação diofantina da forma* $x^2 - Ay^2 = 1$ *com* $x, y \in \mathbb{Z}$*, onde* A *é um número inteiro positivo diferente de um quadrado.*

Em coordenadas cartesianas, a equação tem a forma de uma hipérbole, onde suas soluções ocorrem sempre que a curva passa por um ponto cujas coordenadas x e y são ambos números inteiros.

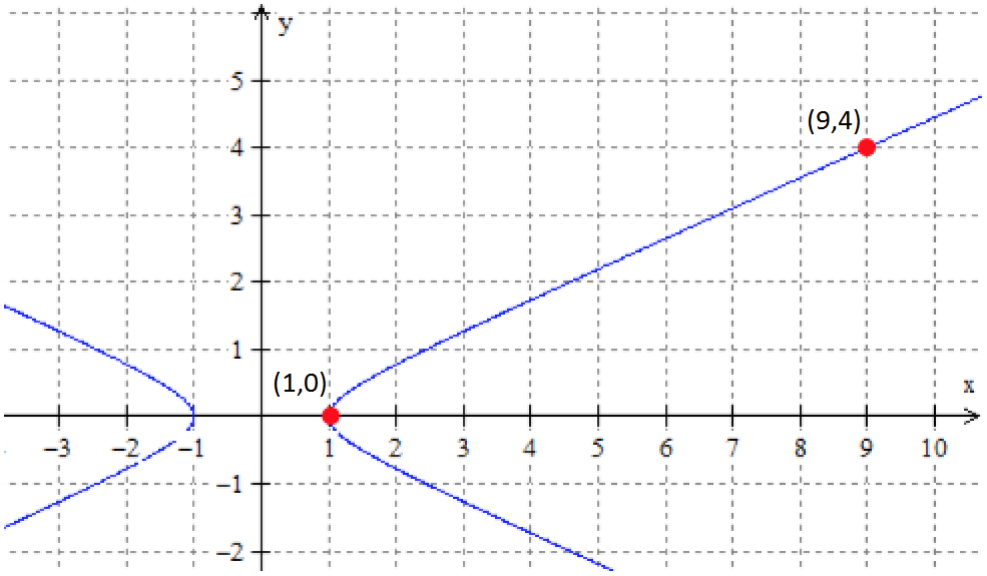

Figura 5.1: Visualização geométrica da equação $x^2 - 5y^2 = 1$.

Exemplo 5.7. Na Figura 5.1, a hipérbole é $x^2 - 5y^2 = 1$, onde é possível verificar que $(9, 4)$ é um ponto inteiro sobre a hipérbole, pois, $9^2 - 5 \cdot 4^2 = 1$. Porém o ponto $(5, 2)$ está próximo à hipérbole, mas não pertence a ela, pois, $5^2 - 5 \cdot 2^2 = 5 \neq 1$.

Para a demonstração do próximo teorema o qual nos permite encontrar todas as soluções da equação de Pell, a partir de uma solução mínima da mesma equação, usamos algumas aplicações de norma. Sendo assim, consideramos o conjunto $\mathbb{Q}(\sqrt{A}) = \{x + y\sqrt{A}; x, y \in \mathbb{Q}\}$. Dado $\delta = x + y\sqrt{A} \in \mathbb{Q}(\sqrt{A})$, com $x, y \in \mathbb{Q}$, podemos definir seu *conjugado* $\widehat{\delta} = x - y\sqrt{A}$. Definimos a norma como sendo a função

$$\begin{array}{rcl} N : \mathbb{Q}(\sqrt{A}) & \to & \mathbb{Q} \\ \delta & \longmapsto & N(\delta) = \delta\widehat{\delta} = x^2 - Ay^2. \end{array}$$

Temos que N é uma função multiplicativa, ou seja,

$$N((x+y\sqrt{A})(u+v\sqrt{A})) = N(x+y\sqrt{A})N(u+v\sqrt{A}), \forall x,y,u,v \in \mathbb{Z}.$$

De fato,

$$\begin{aligned} N((x+y\sqrt{A})(u+v\sqrt{A})) &= N((xu+Ayv)+(xv+yu)\sqrt{A}) \\ &= (xu+Ayv)^2 - A(xv+yu)^2 \\ &= x^2u^2 + A^2y^2v^2 - A(x^2v^2+y^2u^2) \\ &= (x^2-Ay^2)(u^2-Av^2). \end{aligned}$$

Devido a multiplicatividade da norma, observamos que se a equação tem alguma solução (x_1, y_1) com $y_1 \neq 0$ então ela possui infinitas. Mais geralmente, se $x_1^2 - Ay_1^2 = \pm 1$, temos

$$N((x_1+y_1\sqrt{A})^k) = (x_1-y_1\sqrt{A})^k(x_1+y_1\sqrt{A})^k = (\pm 1)^k.$$

Fazendo a substituição da solução (x_1, y_1) em $x_k + y_k\sqrt{A}$, obtemos

$$x_k + y_k\sqrt{A} = (x_1+y_1\sqrt{A})^k = \sum_{j=0}^{k} \binom{k}{j} x_1^{k-j} y_1^k (\sqrt{A})^k$$

onde

$$x_k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} x_1^{k-2j} A^j y_1^{2j} \text{ e } y_k = \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{2j+1} x_1^{k-2j-1} A^j y_1^{2j+1},$$

e obtemos $x_k^2 - Ay_k^2 = (\pm 1)^k$ para todo $k \in \mathbb{N}$.

Observamos ainda, que o valor $x + y\sqrt{A}$ possui uma única representação, ou seja, se $x_1 + y_1\sqrt{A} = x_2 + y_2\sqrt{A}$, com $x_1, y_1, x_2, y_2 \in \mathbb{Q}$, então $x_1 = x_2$ e $y_1 = y_2$. De fato,

$$x_1 + y_1\sqrt{A} = x_2 + y_2\sqrt{A} \rightarrow (y_1 - y_2)\sqrt{A} = x_2 - x_1.$$

Se $y_1 = y_2$, então $x_2 - x_1 = (y_1 - y_2)\sqrt{A} = 0$. Logo, $x_1 = x_2$. Caso contrário, $y_1 - y_2 \neq 0$ então $\sqrt{A} = \dfrac{x_2 - x_1}{y_1 - y_2} \in \mathbb{Q}$, o que é um absurdo, pois a razão entre dois números racionais é racional.

As soluções inteiras (x, y) da equação de Pell correspondem a elementos do conjunto $\mathbb{Z}[\sqrt{A}] = \{x + y\sqrt{A}; x, y \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{A})$, cuja norma $N(x + y\sqrt{A}) = x^2 - Ay^2$ é igual a 1.

Teorema 5.6. *A equação $x^2 - Ay^2 = 1$, com A diferente de um quadrado perfeito, possui solução não trivial em inteiros positivos, isto é, com $x + y\sqrt{A} > 1$.*

Demonstração. Como $\sqrt{A}$ é irracional, a desigualdade $\left|\sqrt{A} - \dfrac{p}{q}\right| < \dfrac{1}{q^2}$ tem infinitas soluções racionais $\dfrac{p}{q}$, como vimos no Teorema 5.3.

Analisando inicialmente $N(p+q\sqrt{A}) = p^2 - Aq^2$, temos

$$p^2 - Aq^2 = (p+q\sqrt{A})(p-q\sqrt{A}) = q^2\left(\frac{p}{q}+\sqrt{A}\right)\left(\frac{p}{q}-\sqrt{A}\right).$$

Notemos que, se $\left|\sqrt{A}-\frac{p}{q}\right| < \frac{1}{q^2}$ então

$$|p^2 - Aq^2| = q^2\left|\frac{p}{q}+\sqrt{A}\right|\left|\frac{p}{q}-\sqrt{A}\right| < q^2\left|\frac{p}{q}+\sqrt{A}\right|\frac{1}{q^2} = \left|\frac{p}{q}+\sqrt{A}\right|.$$

Pela desigualdade triangular, obtemos

$$\left|\frac{p}{q}+\sqrt{A}\right| \leq 2\sqrt{A} + \left|\frac{p}{q}-\sqrt{A}\right| < 2\sqrt{A} + \frac{1}{q^2} \leq 2\sqrt{A}+1.$$

Assim, existem infinitos pares de inteiros positivos (p_n, q_n) com $\left|\sqrt{A}-\frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$, em que teremos sempre $|N(p_n+q_n\sqrt{A})| = |p_n^2 - Aq_n^2| < 2\sqrt{A}+1$, portanto temos um número finito de possibilidades para o valor (inteiro) de $p_n^2 - Aq_n^2$. Consequentemente, existe $k \in \mathbb{Z}$ tal que $p_n^2 - Aq_n^2 = k$ para infinitos valores de n. Observamos ainda que $k \neq 0$, pois, se $k = 0$, teríamos

$$p^2 - Aq^2 = 0 \to p^2 = Aq^2 \to \left(\frac{p}{q}\right)^2 = \frac{p^2}{q^2} = A \to \sqrt{A} = \frac{p}{q} \in \mathbb{Q},$$

o que é um absurdo. Obtemos portanto duas sequências crescentes de pares de inteiros positivos $(u_r), (v_r), r \in \mathbb{N}$, tais que $u_r^2 - Av_r^2 = k$ para todo r.

Como há apenas $|k|^2$ possibilidades para os pares $(u_r \ (mod\ k), v_r \ (mod\ k))$, existem inteiros a e b e infinitos valores de r tais que $u_r \equiv a \ (mod\ k)$ e $v_r \equiv b \ (mod\ k)$. Vimos que o número $x+y\sqrt{A}$ só tem uma única representação, sendo assim, tomando $r < s$ com as propriedades acima, certamente $u_s + v_s\sqrt{A} \neq u_r + v_r\sqrt{A}$. Suponhamos então, sem perda de generalidade que $1 \leq u_r + v_r\sqrt{A} < u_s + v_s\sqrt{A}$ e consideremos o número $x+y\sqrt{A} = \dfrac{u_s+v_s\sqrt{A}}{u_r+v_r\sqrt{A}} > 1$, pois $r < s$. Temos,

$$x+y\sqrt{A} = \frac{u_s+v_s\sqrt{A}}{u_r+v_r\sqrt{A}} = \frac{(u_s+v_s\sqrt{A})(u_r-v_r\sqrt{A})}{u_r^2-Av_r^2} = \frac{(u_ru_s - Av_sv_r) + (u_rv_s - u_sv_r)\sqrt{A}}{u_r^2-Av_r^2}.$$

Substituindo $u_r^2 - Av_r^2 = k$ no resultado acima, obtemos

$$\frac{(u_ru_s - Av_sv_r) + (u_rv_s - u_sv_r)\sqrt{A}}{k} = \frac{u_su_r - Av_sv_r}{k} + \left(\frac{u_rv_s - u_sv_r}{k}\right)\sqrt{A}.$$

Temos ainda,

$$u_su_r - Av_sv_r \equiv u_r^2 - Av_r^2 = k \equiv 0 \ (mod\ k) \text{ e } u_rv_s - u_sv_r \equiv ab - ab = 0 \equiv 0 \ (mod\ k)$$

e portanto, $x = \dfrac{u_s u_r - A v_s v_r}{k}$ e $y = \dfrac{u_r v_s - u_s v_r}{k}$ são inteiros e $x+y\sqrt{A} = \dfrac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} > 1$. Por outro lado,

$$(x + y\sqrt{A})(u_r + v_r\sqrt{A}) = u_s + v_s\sqrt{A},$$

donde

$$k = N(u_s + v_s\sqrt{A}) = N(x + y\sqrt{A})N(u_r + v_r\sqrt{A}).$$

Como $N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A}) = k$, segue que $k = N(u_s + v_s\sqrt{A}) = N(x + y\sqrt{A})N(u_r + v_r\sqrt{A}) = kN(x + y\sqrt{A})$.
Portanto,

$$x^2 - Ay^2 = N(x + y\sqrt{A}) = \frac{k}{k} = 1.$$

□

A partir deste momento, mostraremos que dentre todas as soluções $(x, y) \in \mathbb{N}^2$ da equação de Pell $x^2 - Ay^2 = 1$ com $x + y\sqrt{A} > 1$, existe uma solução mínima ou fundamental, ou seja, com x, e portanto y e $x + y\sqrt{A}$, mínimos.

Proposição 5.6. *Se $x_1 + y_1\sqrt{A}$ é a solução mínima de $x^2 - Ay^2 = 1$, então todas as soluções de $x^2 - Ay^2 = 1$, com $x, y \in \mathbb{N}$, podem ser expressas por $x + y\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, para algum $k \in \mathbb{N}$.*

Demonstração. Representamos essa solução mínima por (x_1, y_1). Se, como antes, definimos $(x_n, y_n) \in \mathbb{N}^2$ pela relação $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, temos que $(x_n, y_n), n \geq 1$, são todas as soluções inteiras positivas da equação de Pell. De fato, já vimos que (x_n, y_n) são soluções, e se (x', y') é uma outra solução e como $x_1 + y_1\sqrt{A} > 1$ então existe $n \geq 1$ tal que

$$(x_1 + y_1\sqrt{A})^n \leq x' + y'\sqrt{A} < (x_1 + y_1\sqrt{A})^{n+1}.$$

Multiplicando ambos os lados da igualdade por $x_n - y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^{-n} > 0$, obtemos

$$1 \leq (x' + y'\sqrt{A})(x_n - y_n\sqrt{A}) = (x'x_n - y'y_nA) + (y'x_n - x'y_n)\sqrt{A} < x_1 + y_1\sqrt{A}.$$

Como $N((x' + y'\sqrt{A})(x_n - y_n\sqrt{A})) = N(x' + y'\sqrt{A})N(x_n - y_n\sqrt{A}) = 1$, temos que $(x'x_n - y'y_nA, y'x_n - x'y_n)$, também é uma solução da equação de Pell, menor que a solução mínima. Temos também que $x'x_n - y'y_nA \geq 0$, pois caso contrário $x'x_n - y'y_nA < 0 \iff \dfrac{x'}{y'}\dfrac{x_n}{y_n} < A$. Porém,

$$x_n^2 - y_n^2A = 1 \to \left(\frac{x_n}{y_n}\right)^2 = A + \frac{1}{y_n^2} > A \to \frac{x_n}{y_n} > \sqrt{A}$$

e analogamente $\frac{x^{'}}{y^{'}} > \sqrt{A}$, o que contradiz $\frac{x^{'}}{y^{'}}\frac{x_n}{y_n} < A$. Da mesma forma, $y^{'}x_n - x^{'}y_n \geq 0$, pois caso contrário,

$$\frac{x_n}{y_n} < \frac{x^{'}}{y^{'}} \to A + \frac{1}{y_n^2} = \left(\frac{x_n}{y_n}\right)^2 < \left(\frac{x^{'}}{y^{'}}\right)^2 = A + \frac{1}{y'^2} \to y^{'} < y_n \to x^{'} < x_n,$$

o que contradiz o fato de $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n \leq x^{'} + y^{'}\sqrt{A}$. Em resumo, temos que $(x^{'}x_n - y^{'}y_nA, y^{'}x_n - x^{'}y_n) \in \mathbb{N}^2$ é uma solução menor do que a solução mínima. Logo $x^{'}x_n - y^{'}y_nA = 1$ e $y^{'}x_n - x^{'}y_n = 0$, ou seja, $(x^{'} + y^{'}\sqrt{A})(x_1 - y_1\sqrt{A})^{-n} = 1 \iff x^{'} + y^{'}\sqrt{A} = x_n + y_n\sqrt{A}$, donde $(x^{'}, y^{'}) = (x_n, y_n)$, como queríamos.

Sendo assim, todas as soluções da equação $x^2 - Ay^2 = 1$, com x e y inteiros positivos podem ser enumerados por $(x_n, y_n), n \geq 0$ de modo que, para todo $n, x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$. □

Exemplo 5.8. Determinemos todas as soluções inteiras, positivas e não nulas da equação

$$x^2 - 2y^2 = 1.$$

Vimos que as soluções positivas dessa equação são da forma (x_n, y_n), onde x_n e y_n são os únicos inteiros para os quais $x_n + y_n\sqrt{2} = (x_1 + y_1\sqrt{2})^n$, sendo (x_1, y_1) a solução positiva, para a qual $x_1 + y_1\sqrt{2}$ é o menor possível.

É fácil notar que os pares $(x, y) = (1, 1), (1, 2), (2, 1), (2, 2), (2, 3)$ não são soluções da equação, sendo assim, é fácil nos convencermos de que $(x_1, y_1) = (3, 2)$. Desse modo, temos os pares (x_n, y_n) dados pela igualdade $x_n + y_n = (3 + 2\sqrt{2})^n$.

Nesse exemplo foi fácil encontrar uma solução mínima para a equação $x^2 - 2y^2 = 1$, para que a partir desta solução mínima possamos encontrar todas a outras. Porém, nem sempre é fácil encontrar uma solução mínima para uma equações de Pell, como no caso da equação $x^2 - 21y^2 = 1$. Devido a este fato, apresentamos a seguir um método mais eficiente, ao qual nos permite encontrar a solução mínima para uma equação de Pell.

5.3.2 Encontrando uma Solução para a Equação de Pell

Se $x^2 - Ay^2 = 1$, com x, y inteiros e positivos, então

$$x^2 - Ay^2 = (x - y\sqrt{A})(x + y\sqrt{A}) = 1.$$

Logo,

$$|x - y\sqrt{A}| = \frac{1}{x + y\sqrt{A}} < \frac{1}{y\sqrt{A}} < \frac{1}{y}. \tag{5.12}$$

Dividindo ambos os lados da desigualdade (5.12) por y, obtemos

$$\left|\frac{x}{y} - \sqrt{A}\right| < \frac{1}{y^2\sqrt{A}} < \frac{1}{y^2}.$$

Na verdade,

$$|x - y\sqrt{A}| < \frac{1}{y} < 1 \to x - y\sqrt{A} > -1 \to x > y\sqrt{A} - 1 \to x + y\sqrt{A} > 2y\sqrt{A} - 1 \geq 2y.$$

De fato, se $A \geq 3, y \geq 1$, segue que

$$2y\sqrt{A} - 2y \geq (2\sqrt{3} - 2)y > 1,$$

e, se $A = 2, y \geq 2$, segue que

$$2y\sqrt{A} - 2y \geq (2\sqrt{2} - 2)y \geq 2(2\sqrt{2} - 2) > 1.$$

Portanto,

$$|x - y\sqrt{A}| = \frac{1}{x + y\sqrt{A}} < \frac{1}{2y},$$

que ao dividirmos tudo por y, obtemos

$$\left|\frac{x}{y} - \sqrt{A}\right| < \frac{1}{2y^2},$$

e, pelo Teorema 5.5, $\frac{x}{y}$ é uma reduzida $\frac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$.

Agora, consideramos a fração contínua de $\sqrt{A} + \lfloor\sqrt{A}\rfloor = [a_0; a_1, a_2, ...]$ (a qual difere da fração contínua de $\sqrt{A}$ apenas pelo primeiro termo $a_0 = 2\lfloor\sqrt{A}\rfloor$, que na fração contínua de $\sqrt{A}$ é igual a $\lfloor\sqrt{A}\rfloor = \frac{a_0}{2}$). O que queremos mostrar é que a fração contínua $\sqrt{A} + \lfloor\sqrt{A}\rfloor$ é puramente periódica, ou seja, ela já é periódica a partir do primeiro termo a_0 e quando termina esse período, teremos uma solução para a Equação de Pell. Para tal, mostramos que existem duas sequências de inteiros positivos b_i e c_i, com $i \geq 0$ tal que

$$0 < \frac{\sqrt{A} - c_i}{b_i} < 1$$

e

$$\alpha_i = \frac{\sqrt{A} + c_i}{b_i} = [a_i; a_{i+1}, a_{i+2}, \cdots] \tag{5.13}$$

para todo $i \geq 0$. Definimos $b_0 = 1$ e $c_0 = \lfloor\sqrt{A}\rfloor \geq 1$. Notemos que, para $i = 0$

$$0 < \sqrt{A} - \lfloor\sqrt{A}\rfloor = \frac{\sqrt{A} - c_0}{b_0} < 1.$$

Em geral, definimos recursivamente $c_{i+1} = a_i b_i - c_i$ e $b_{1+i} = \frac{A - c_{i+1}^2}{b_1}$.

Vamos agora mostrar, por indução, que b_i e c_i são inteiros com $b_i \neq 0$ e tais que $b_i \mid A - c_{i+1}^2$ para todo i. Para isso, vejamos que por definição de fração contínua

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i} = \frac{1}{\frac{c_i + \sqrt{A}}{b_i} - a_i} = \frac{b_i}{c_i - a_i b_i + \sqrt{A}}. \tag{5.14}$$

Multiplicando a equação (5.14) por $\sqrt{A}+a_ib_i-c_i$, temos

$$\frac{b_i(\sqrt{A}+a_ib_i-c_i)}{A-(a_ib_i-c_i)^2}=\frac{\sqrt{A}+c_{i+1}}{b_{i+1}}.$$

Suponhamos agora, que a_i, b_i e c_i sejam inteiros. Vejamos que,
$c_1=a_0b_0-c_0=2\lfloor\sqrt{A}\rfloor-\lfloor\sqrt{A}\rfloor=\lfloor\sqrt{A}\rfloor=c_0\geq 1$ e $b_1=\dfrac{A-c_i^2}{b_0}=\dfrac{A-\lfloor\sqrt{A}\rfloor^2}{1}>0$.
Então, se $i\geq 1$, $b_i=\dfrac{A-c_i^2}{b_{i-1}}\in\mathbb{Z}$, donde $A-c_i^2=b_ib_{i-1}\Rightarrow b_i\mid A-c_i^2$. Logo,

$$b_{i+1}=\frac{A-c_{i+1}^2}{bi}=\frac{A-(a_ib_i-c_i)^2}{b_i}.$$

Temos então, que $A-(a_ib_i-c_i)^2\equiv A-(-c_i)^2=A-c_i^2\equiv 0\ (mod\ b_i)$. Portanto $b_{i+1}=\dfrac{(A-c_{i+1}^2)}{b_i}$ será um inteiro não nulo tal que $b_{i+1}\mid A-c_{i+1}^2$.

Desta forma, temos

$$\frac{\sqrt{A}+c_i}{b_i}=a_i+\frac{\sqrt{A}-c_{i+1}}{b_i}=a_i+\frac{b_{i+1}}{\sqrt{A}+c_{i+1}}=a_i+\frac{1}{\dfrac{\sqrt{A}+c_{i+1}}{b_{i+1}}},$$

de modo que (5.13) será válida para todo i. Agora, vamos mostrar que b_i e c_i são positivos. Para isto, provamos por indução que $b_i>0$ e $0<c_i<\sqrt{A}$, o que é verdadeiro para $i=0$ pois $c_0=\lfloor\sqrt{A}\rfloor$, e A não é quadrado perfeito. Além disso, pela definição de a_i temos

$$a_i<\frac{\sqrt{A}+c_i}{b_i}=[a_i;a_{i+1},a_{i+2},\cdots]<a_{i+1},$$

donde obtemos $a_ib_i<\sqrt{A}+c_i<a_ib_i+b_i$ (já que $b_i>0$ por hipótese de indução) e portanto,

$$c_{i+1}=a_ib_i-c_i<\sqrt{A}<a_ib_i-c_i=c_{i+1}+b_i$$

e assim $c_{i+1}<\sqrt{A}$, o que implica $b_{i+1}=\dfrac{A-c_{i+1}^2}{b_i}>0$. Agora suponhamos por absurdo que $c_{i+1}\leq 0$. Neste caso, teríamos $b_i>\sqrt{A}-c_{i+1}\geq\sqrt{A}$, mas como $\sqrt{A}>c_i$ por hipótese de indução, teríamos $b_i>c_i$ donde $c_{i+1}=a_ib_i-c_i\geq b_i-c_i>\sqrt{A}-c_i>0$, o que é uma contradição. Portanto $c_{i+1}>0$, completando a indução.

Finalmente, temos

$$\frac{\sqrt{A}-c_{i+1}}{b_{i+1}}=\frac{\sqrt{A}-c_{i+1}}{\dfrac{A-c_{i+1}^2}{b_i}}=\frac{b_i}{\sqrt{A}+c_{i+1}}$$

$$=\frac{b_i}{\sqrt{A}+a_ib_i-c_i}=\frac{1}{a_i+\dfrac{\sqrt{A}-c_i}{b_i}}\in(0,1),\qquad(5.15)$$

pois, $a_i \geq 1$ e $\dfrac{\sqrt{A}-c_i}{b_i} > 0$.

Como $0 < c_i < \sqrt{A}$ e $b_i \mid A - c_i^2$, temos que as sequências $\{c_i\}$ e $\{b_i\}$ só assumem um número finito de valores. Além disso, podemos recuperar os valores de b_i e c_i a partir dos valores de b_{i+1} e c_{i+1}, para todo $i \geq 0$. De fato, pois, dados b_{i+1} e c_{i+1}, temos que $c_{i+1} = a_i b_i - c_i \Rightarrow c_i = a_i b_i - c_{i+1}$ e $b_{i+1} = \dfrac{A - c_{i+1}^2}{b_i} \Rightarrow b_i = \dfrac{A - c_{i+1}^2}{b_{i+1}}$, sendo assim, por (5.15) temos que

$$\frac{\sqrt{A}-c_{i+1}}{b_{i+1}} = \frac{1}{a_i + \dfrac{\sqrt{A}-c_i}{b_i}} \to a_i + \frac{\sqrt{A}-c_i}{b_i} = \frac{b_{i+1}}{\sqrt{A}-c_{i+1}}.$$

Como $0 < \dfrac{\sqrt{A}-c_i}{b_i} < 1$, temos

$$a_i = \left\lfloor a_i + \frac{\sqrt{A}-c_i}{b_i} \right\rfloor = \left\lfloor \frac{b_{i+1}}{\sqrt{A}-c_{i+1}} \right\rfloor = \left\lfloor \frac{\sqrt{A}+c_{i+1}}{b_i} \right\rfloor.$$

Portanto estas sequências, assim como a fração contínua $\sqrt{A} + \lfloor \sqrt{A} \rfloor = [a_0; a_1, a_2, \cdots]$, são periódicas puras, digamos de período $k \geq 1$. Em particular se $b_k = b_0 = 1, c_k = a_0$ e $\alpha_k = \dfrac{\sqrt{A}+c_k}{b_k} = \alpha_0$, então $a_{n+k} = a_n, \forall n \geq 0$.

Vejamos que, como $a_0 = 2\lfloor \sqrt{A} \rfloor$, temos que a representação de $\sqrt{A}$ em fração contínua é $\left[\dfrac{a_0}{2}; a_1, a_2, \cdots\right]$. Logo, para $i \geq 1$, denotando por $\dfrac{p_i}{q_i}$ a i-ésima convergente desta fração contínua, temos pelo Corolário 5.1,

$$\sqrt{A} = \frac{\alpha_{i+1}p_i + p_{i-1}}{\alpha_{i+1}q_i + q_{i-1}} = \frac{\dfrac{\sqrt{A}+c_{i+1}}{b_{i+1}}p_i + p_{i-1}}{\dfrac{\sqrt{A}+c_{i+1}}{b_{i+1}}q_i + q_{i-1}},$$

e portanto, ao desenvolvermos a igualdade acima, e portanto obtemos

$$Aq_i + c_{i+1}\sqrt{A}q_i + \sqrt{A}b_{i+1}q_{i-1} = \sqrt{A}p_i + c_{i+1}p_i + b_{i+1}p_{i-1}.$$

Na qual podemos separar a parte racional da parte irracional, obtemos as equações

$$Aq_i = c_{i+1}p_i + b_{i+1}p_{i-1} \text{ e } p_i = c_{i+1}q_i + b_{i+1}q_{i-1}.$$

Isolando c_{i+1} nas equações anteriores e as igualando obtemos

$$\begin{aligned}
&\frac{Aq_i - b_{i+1}p_{i-1}}{p_i} = \frac{p_i - b_{i+1}q_{i-1}}{q_i} \\
&\iff Aq_i^2 - b_{i+1}p_{i-1}q_i = p_i^2 - b_{i+1}q_{i-1}p_1 \\
&\iff p_i^2 - Aq_i^2 = b_{i+1}(p_iq_{i-1} - p_{i-1}q_i),
\end{aligned}$$

sendo que, pelo Lema 5.1, $p_iq_{i-1} - p_{i-1}q_i = (-1)^{i+1}$. Logo,

$$p_i^2 - Aq_i^2 = (-1)^{i+1}b_{i+1},$$

donde obtemos uma solução da equação $x^2 - Ay^2 = (-1)^{i+1}b_{i+1}$. Se k é o período então $b_k = b_0 = 1$. Daí $p_{k-1}^2 - Aq_{k-1}^2 = (-1)^{k-2}$ e portanto, a equação $x^2 - Ay^2 = -1$ tem solução se k é ímpar, enquanto que, se $b_{2k} = b_k = b_0 = 1$ então $p_{2k-1}^2 - Aq_{2k-1}^2 = (-1)^{2k-2} = 1$, ou seja, a equação $x^2 - Ay^2 = 1$ sempre tem solução.

Por outro lado, se x e y são inteiros positivos tais que $x^2 - Ay^2 = \pm 1$, vimos que $\dfrac{x}{y}$ é uma reduzida $\dfrac{p_n}{q_n}$ da fração contínua de $\sqrt{A}$. Como $p_n^2 - Aq_n^2 = (-1)^{n+1}b_{n+1}$, segue que $b_{n+1} = 1$, mas como $0 < \sqrt{A} - c_{n+1} = \dfrac{\sqrt{A} - c_{n+1}}{b_{n+1}} < 1$, segue que $c_{n+1} = \lfloor \sqrt{A} \rfloor$, donde $[a_{n+1}, a_{n+2}, a_{n+3}, \ldots] = \dfrac{\sqrt{A} + c_{n+1}}{b_{n+1}} = \sqrt{A} + \lfloor \sqrt{A} \rfloor$, e portanto $n+1$ é necessariamente múltiplo de período k.

Exemplo 5.9. Vamos encontrar uma solução para a equação $x^2 - 19y^2 = 1$.

Vimos que $c_{i+1} = a_ib_i - c_i, b_{i+1} = \dfrac{A - c_{i+1}}{b_i}$ e $a_i = \left\lfloor \dfrac{\sqrt{A} + c_i}{b_i} \right\rfloor$. Sendo assim, vamos encontrar a fração contínua de $\sqrt{19} + \lfloor \sqrt{19} \rfloor$. Para tal, tomamos $i \geq 0$. Logo,

- Tomando $i = 0$, temos $a_0 = 2\lfloor \sqrt{19} \rfloor = 8, c_0 = \lfloor \sqrt{19} \rfloor = 4$ e $b_0 = 1$.
- Para $i = 1$, temos

  $$c_1 = a_0b_0 - c_0 = 2\lfloor \sqrt{19} \rfloor - \lfloor \sqrt{19} \rfloor = 4$$

  e

  $$b_1 = \frac{A - c_1^2}{b_0} = \frac{19 - 4^2}{1} = 19 - 16 = 3.$$

  Consequentemente

  $$a_1 = \left\lfloor \frac{\sqrt{19} + 4}{3} \right\rfloor = 2.$$

- Para $i = 2$, obtemos
  $c_2 = a_1b_1 - c_1 = 2 \cdot 3 - 4 = 2$ e $b_2 = \dfrac{A - c_2^2}{b_1} = \dfrac{19 - 2^2}{3} = 5.$
  Desta forma,

  $$a_2 = \left\lfloor \frac{\sqrt{19} + 2}{5} \right\rfloor = 1.$$

- Para $i = 3$, temos $c_3 = a_2b_2 - c_2 = 1 \cdot 5 - 2 = 3$ e $b_3 = \dfrac{A - c_3^2}{b_2} = \dfrac{19 - 3^2}{5} = 2.$
  Sendo assim,

  $$a_3 = \left\lfloor \frac{\sqrt{19} + 3}{2} \right\rfloor = 3.$$

- Para $i = 4$, temos $c_4 = a_3b_3 - c_3 = 3 \cdot 2 - 3 = 3$ e $b_4 = \dfrac{A - c_4^2}{b_3} = \dfrac{19 - 3^2}{2} = 5$. Consequentemente
$$a_4 = \left\lfloor \frac{\sqrt{19} + 3}{5} \right\rfloor = 1.$$

- Para $i = 5$, temos $c_5 = a_4b_4 - c_4 = 1 \cdot 5 - 3 = 2$ e $b_5 = \dfrac{A - c_5^2}{b_4} = \dfrac{19 - 2^2}{5} = 3$. Donde obtemos
$$a_5 = \left\lfloor \frac{\sqrt{19} + 2}{3} \right\rfloor = 1.$$

- Para $i = 6$, temos $c_6 = a_5b_5 - c_5 = 2 \cdot 3 - 2 = 4$ e $b_5 = \dfrac{A - c_5^2}{b_4} = \dfrac{19 - 4^2}{3} = 1$. E portanto,
$$a_6 = \left\lfloor \frac{\sqrt{19} + 4}{1} \right\rfloor = 8.$$

Observe que $i_6 = i_0$, ou seja, $a_6 = a_0, b_6 = b_0, c_6 = c_0$. Com isso concluímos que

$$4 + \sqrt{19} = [\overline{8; 2, 1, 3, 1, 2}] \text{ e } \sqrt{19} = [4; \overline{2, 1, 3, 1, 2, 8}].$$

Vimos que a equação $x^2 - Ay^2 = 1$, tem como solução $\dfrac{x}{y}$ que é uma reduzida $\dfrac{p_i}{q_i}$ da fração contínua de $\sqrt{A}$. Como $\sqrt{A} = \sqrt{19}$, segue que

$$\frac{p_5}{q_5} = 4 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2}}}}} = \frac{170}{39}.$$

Com isso, segue que $x = 170$ e $y = 39$ é solução da equação $x^2 + 19y^2 = 1$, pois $170^2 + 19 \cdot 39^2 = 1$. O que nos leva a concluir que também é a solução mínima da equação do exemplo.

Exemplo 5.10. Mostramos que existem infinitos pares (x, y) de números naturais tais que

$$x^2 - 3x - 3y^2 - y + 1 = 0. \tag{5.16}$$

Inicialmente iremos reduzir alguns termos da equação (5.16), através do complemento de quadrados, para que possam aparecer quadrados perfeitos na equação e ela fique parecida com a equação de Pell. Sendo assim,

$$2x^2 - 3x - 3y^2 - y + 1 = 0 \quad \to 2\left(x - \frac{3}{4}\right)^2 - 3\left(y + \frac{1}{6}\right)^2 - \frac{1}{24} = 0$$

$$\to 3(4x - 3)^2 - 2(6y + 1)^2 = 1.$$

Tomando $u = 4x - 3$ e $v = 6y + 1$, o problema inicial se transforma em encontrar infinitas soluções da equação

$$3u^2 - 2v^2 = 1 \text{ com } u \equiv 1 \ (mod\ 4) \text{ e } v \equiv 1 \ (mod\ 6).$$

Fatorando $3u^2 - 2v^2 = 1$, temos

$$3u^2 - 2v^2 = (u\sqrt{3} + v\sqrt{2})(u\sqrt{3} - v\sqrt{2}) = 1. \tag{5.17}$$

Consideremos agora, a equação de Pell auxiliar $a^2 - 6b^2 = 1$. Vejamos que, na equação (5.17) podemos substituir $(u\sqrt{3} - v\sqrt{2})$ por $a^2 - 6b^2$, pois, $(u\sqrt{3} - v\sqrt{2}) = 1 = a^2 - 6b^2$. Sendo assim,

$$(u\sqrt{3} + v\sqrt{2})(a + b\sqrt{6}) = (au + 2bv)\sqrt{3} + (av + 3bu)\sqrt{2},$$

onde calculando a norma, vamos obter

$$\begin{aligned} 3(au + 2bv)^2 - 2(av + 3bu)^2 &= 3(a^2u^2 + 4b^2v^2) - 2(a^2v^2 + 9b^2u^2) \\ &= (3u^2 - 2v^2)(a^2 - 6b^2) = 3u^2 - 2v^2. \end{aligned}$$

A ideia aqui é que, para conseguirmos infinitas soluções para a equação $3u^2 - 2v^2 = 1$, basta multiplicar pela equação auxiliar $a^2 - 6b^2 = 1$, que possui infinitas soluções. Porém, devemos encontrar infinitas soluções para a equação $3u^2 - 2v^2 = 1$, de tal forma que as congruências $u \equiv 1 \ (mod\ 4)$ e $v \equiv 1 \ (mod\ 6)$ sejam mantidas. Encontramos então, uma solução para a equação $a^2 - 6b^2 = 1$, de modo que $a \equiv 1 \ (mod\ 4)$ e b seja par, dessa forma, $au + 2bv \equiv u \ (mod\ 4)$ e $av + 3bv \equiv v \ (mod\ 6)$.

Analisando as soluções da equação $a^2 - 6b^2 = 1$, vemos facilmente que sua solução mínima é o par ordenado $(a_1, b_1) = (5, 2)$ e pela Proposição 5.6, segue que, $a_1 + b_1\sqrt{6} = 5 + 2\sqrt{6}$. Logo, todas as soluções de $a^2 - 6b^2 = 1$, são dadas por

$$a_n + b_n\sqrt{6} = (5 + 2\sqrt{6})^n.$$

Agora só nos resta mostrar que existem infinitos pares (a_n, b_n) tais que $a_n \equiv 1 \ (mod\ 4)$ e $b_n \equiv 1 \ (mod\ 6)$. Vejamos que,

i) $a_0 = 1, a_1 = 5$, e segue que $a_{n+2} = 10a_{n+1} - a_n$. Veja que $a_n \ (mod\ 4) = 1, 1, 1, 1, \ldots$ e $a_n \ (mod\ 3) = 1, 2, 1, 2, 1, 2, \cdots$. Sempre que n par, teremos $a_n \equiv 1 \ (mod\ 12)$;

ii) $b_0 = 0, b_1 = 2$, e segue que $b_{n+2} = b_{n+1} - b_n$. Vejamos que, b_n sempre é par, $\forall n \in \mathbb{N}$.

Sendo assim, concluímos que $(\sqrt{3} + \sqrt{2})(5 + 2\sqrt{6})^n$ vai ser uma solução da equação $3u^2 - 2v^2 = 1$ e automaticamente fica provado que existem infinitos pares (x, y) de números naturais com $2x^2 - 3x - 3y^2 - y + 1 = 0$. Ainda assim, fizemos uma breve verificação de $(\sqrt{3} + \sqrt{2})(5 + 2\sqrt{6})^n$ para $n = 2$. Logo,

$$(\sqrt{3} + \sqrt{2})(5 + 2\sqrt{6})^n = (\sqrt{3} + \sqrt{2})(49 + 20\sqrt{6}) = 89\sqrt{3} + 109\sqrt{2},$$

que por sua vez, $89 \equiv 1 \ (mod\ 4)$ e $109 \equiv 1 \ (mod\ 6)$. Substituindo 89 e 109 na equação $3u^2 - 2v^2 = 1$, segue que $3 \cdot 89^2 - 2 \cdot 109^2 = 23.763 - 23.762 = 1$, e portanto a condição é verificada.

6 Conclusão

Neste trabalho apresentamos métodos que nos possibilitam encontrar as infinitas soluções de uma equação diofantina linear que contenha n variáveis. Sendo assim, foi feito um estudo sobre algumas propriedades aritméticas relativas a números inteiros, como a divisibilidade, o algoritmo de Euclides, a identidade de Bézout, o teorema fundamental da aritmética, congruência, entre outros. A partir daí foram sugeridos caminhos para a resolução de equações diofantinas lineares com duas variáveis, três variáveis, n variáveis e também para as equações diofantinas quadráticas, com soluções no conjunto dos inteiros. Mostramos ainda, que é possível a aplicação desses tipos de equações em situações do nosso cotidiano.

Analisando o contexto histórico a respeito de Diofanto, é possível reparar que ele fez grandes contribuições para o desenvolvimento da álgebra, pois foi pioneiro no desenvolvimento da notação algébrica. Algumas operações eram representadas por suas abreviações. A partir de suas contribuições, a linguagem algébrica evoluiu ao que conhecemos hoje, em que são usados apenas símbolos de forma organizada e estruturada para representa-lá.

Referências

[1] BERNSTEIN, L. *The Linear Diophantine Equation in n Variables and Its Application to Generalized Fibonacci Numbers*. Syracuse, New York, 2009.

[2] BOYER, C. B. *História da Matemática*. 2. ed. São Paulo, SP: EDGARD BLUCHERLTDA, 2001.

[3] CAMPOS, G. D. M. *Equações Diofantinas Lineares*. Dissertação (Mestrado Profissional em Matemática) - Universidade Federal de Mato Grosso. Cuiabá, MT, 2013

[4] DOMINGUES, H. H. *Fundamentos de Aritmética*. 1. ed. São Paulo: Atual Editora LTDA, 1991.

[5] EVES, H. *Introdução à História da Matemática*. 1. ed. Campinas, SP: EDITORA UNICAMP, 2007.

[6] FAUVEL, J.; GRAY, J. *The History of Mathematics: A Reader*. 1. ed. London: THE MACMILLAN EDUCATION LTD, 1987.

[7] FILHO, E. A. *Teoria Elementar dos Números*. 1. ed. São Paulo: Nobel,1981.

[8] HEATH,S. T. *A History of Greek Mathematics*. 1. ed. New York: Dover Publication, 1981.

[9] HEFEZ, A. *Curso de Álgebra*. 2. ed. Rio de Janeiro: IMPA, 1997.

[10] MARTINEZ, F. B. et al. *Teoria dos Números: Um Passeio com Primos e outros Números Familiares pelo Mundo Inteiro*. 2. ed. Rio de Janeiro: IMPA, 2013.

[11] SANTOS, J. P. O. *Introdução à Teoria dos Números*. 3. ed. Rio de Janeiro: IMPA, 2007.

[12] SAMPAIO, J. C. V.; CAETANO, P. A. S. *Introdução à Teoria dos Números: Um Curso Breve*. 1. ed. São Carlos, SP: EdUFSCar, 2008.