INSTITUTO FEDERAL
DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
São Paulo

PROFMAT
Mestrado Profissional
em Matemática

A EQUAÇÃO DE PELL E O PROCESSO DE EXTRAÇÃO DE RAÍZES QUADRADAS

Felipe Marcos Pinto

Dissertação apresentada ao Programa de Pós-Graduação *Stricto Sensu* em Matemática em Rede Nacional, como parte dos requisitos para obtenção do título de Mestre em Matemática, orientada pelo Prof. Dr. Marco Aurélio Granero Santos e co-orientada pelo Prof. Me. Luciano Aparecido Magrini.

IFSP
São Paulo
2019

FELIPE MARCOS PINTO

A EQUAÇÃO DE PELL E O PROCESSO DE EXTRAÇÃO DE RAÍZES QUADRADAS

Dissertação de mestrado apresentada e aprovada em 30 de outubro de 2019 como requisito parcial para obtenção do título de Mestre em Matemática.

A banca examinadora foi composta pelos seguintes membros:

Prof. Dr. Marco Aurélio Granero Santos
IFSP – Câmpus São Paulo
Orientador e Presidente da Banca

Prof. Me. Luciano Aparecido Magrini
IFSP – Câmpus São Paulo
Co-orientador e Membro da Banca

Profa. Dra. Valéria Ostete Jannis Luchetta
IFSP – Câmpus São Paulo
Membro da Banca

Prof. Dr. Márcio Luis Lanfredi Viola
Universidade Federal de São Carlos
Membro da Banca

“Quando mais aumenta nosso conhecimento, mais evidente fica nossa ignorância”.

John F. Kennedy

AGRADECIMENTOS

Agradeço inicialmente ao meu orientador (Marco Granero), onde com certeza sem o seu apoio e críticas, não seria possível esse trabalho.

Agradeço também a minha mãe, por sempre apoiar e acreditar em mim.

Agradeço aos meus colegas do IF, tanto como aluno quanto professor, pela ajuda e conhecimentos fornecidos.

Por fim agradeço aos meus alunos, dos quais nem preciso citar nomes, para que saibam a força que deram ao acreditarem em mim.

RESUMO

Este trabalho tem por objetivo estudar a equação de Pell, o processo de resolução e sua aplicação no processo de obtenção de raízes quadradas. Além disso, esta dissertação apresenta conceitos de aritmética e matemática discreta que constituem ferramentas para determinar as soluções da equação de Pell através de frações contínuas. O trabalho também compara a eficiência da aproximação da raiz através da equação de Pell com métodos numéricos usuais, a saber: método da bissecção, método de Newton e método da secante. Por fim, o trabalho aponta possibilidades de desenvolvimento e aprimoramento dos conhecimentos aqui estudados para a Educação Básica.

Palavras-chaves: Equação de Pell; Aproximação de Raiz Quadrada; Métodos Numéricos; Frações Contínuas.

ABSTRACT

This work aims to study the Pell’s equation, the process of resolution and its application in the process of obtaining square roots. In addition, this dissertation presents concepts of arithmetic and discrete mathematic that constitute tools to determine the solutions of the Pell equation through continued fractions. The work also compares the efficiency of root approximation through the Pell equation with usual numerical methods: the bisection method, Newton-Raphson method and secant method. Finally, the work points possibilities of development and improvement of the knowledge studied for the Basic Education.

Keywords: Pell's equation; Square Root Approximation; Numerical methods; Continued Fractions.

LISTA DE FIGURAS

Pág.

LISTA DE QUADROS

Pág.

SUMÁRIO

Pág.

1 INTRODUÇÃO

Equações diofantinas talvez sejam um dos objetos de estudo mais antigos da Matemática. Como afirma Schroeder (2009), investigações históricas relatam que problemas desse tipo apareciam na forma de quebra-cabeças. Atualmente, as equações diofantinas desempenham um papel cada vez maior em aplicações modernas relacionadas ao cotidiano. Deus (2017), em seu texto, utiliza equações diofantinas no desenvolvimento do Sistema de Posicionamento Global (GPS).

No Ensino Superior, este tema também é utilizado para aprofundar outros tópicos, como o estudo de equações algébricas ou o estudo de congruências.

Historicamente, as equações diofantinas levam esse nome em homenagem a Diofanto de Alexandria (200-284), o primeiro a estudar equações dessa forma. Entretanto, como relatam Milies e Coelho (2013), Diofanto procurava soluções racionais. Mesmo assim usamos até hoje o termo “diofantino” para indicar problemas relativos a números inteiros.

Ainda segundo Millies e Coelho (2013), o correto seria associar esses problemas a Pierre de Fermat (1601-1665), pois foi o primeiro a estudar essas questões estritamente no conjunto dos números inteiros.

Fermat, em 1657, afirmou sem demonstrar que a equação:

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

apresentava infinitas soluções desde que A seja livre de quadrados[1]. Esta equação, em particular, ficou conhecida historicamente como equação de Pell, homenagem de Leonhard Euler (1707-1783) a John Pell (1611-1685). Entretanto, Weil (2013) relata que possivelmente Euler atribuiu erroneamente o trabalho desenvolvido por William Brouncker (1620-1684) nesse tipo de equação à Pell.

Na verdade, como explica Neto (2016), as equações atribuídas a Pell tem uma longa história. Séculos antes de Cristo, o matemático hindu Baudhayana (em torno de 800 a.C.) encontrou a fração $\frac{577}{408}$ para aproximar $\sqrt{2}$.

[1] Um inteiro é livre de quadrados quando todas as potências de seus divisores primos são iguais a 1.

Neto (2016) também comenta sobre estudos envolvendo as equações de Pell realizados por Brahmagupta (598-670) e Bhaskara II (1114-1185), tendo seu desenvolvimento realizado por Joseph-Louis Lagrange (1736-1685) séculos depois. De um modo geral, esses matemáticos utilizaram as equações de Pell em seus estudos, relacionando essas equações com a obtenção de raízes quadradas de números inteiros positivos.

Neste trabalho, temos como objetivo estudar as equações de Pell e sua aplicação para o processo de obtenção de raízes quadradas através de aproximações sucessivas entre suas soluções. Além disso, estes serão comparados com resultados obtidos a partir de métodos numéricos iterativos usualmente abordados no Ensino Superior. Por fim, destacamos algumas possibilidades de desenvolvimento do tema que podem ser utilizadas e aprofundadas na Educação Básica.

No Capítulo 2, apresentamos alguns conceitos que serão uteis para o estudo das equações de Pell e para sua resolução. Além disso, este capítulo aborda tópicos sobre divisibilidade, equações diofantinas lineares, recorrências e congruências, temas presentes no Ensino Superior, tratando também sobre frações contínuas.

O Capítulo 3 é dedicado exclusivamente a estabelecer as bases teóricas para a obtenção das soluções da equação de Pell e sua aplicação no processo de aproximação de raízes. No fim do capítulo faremos uma análise na precisão das soluções mostrando que, em apenas algumas iterações, conseguimos obter uma boa aproximação das raízes quadradas através da solução da equação de Pell.

O Capítulo 4 traz um comparativo do método utilizando as equações de Pell com métodos numéricos usuais de zeros de funções para a obtenção de raízes. Os métodos numéricos utilizados são os da Bissecção, de Newton e da Secante.

Nas Considerações Finais, concluiremos as análises levantadas nos Capítulos 3 e 4, apontando ideias para abordagens e aplicações no Ensino Básico.

2 CONCEITOS BÁSICOS

Ao estudarmos as equações diofantinas, diversos outros temas surgem de forma a auxiliar, não só no entendimento, mas também na resolução dessas equações. Sendo assim, para estudar e resolver as Equações de Pell faz-se necessário abordarmos outros temas, como divisibilidade, equações diofantinas lineares, congruências, recorrências e frações contínuas possibilitando, a partir de algumas definições, teoremas e proposições, construir o alicerce teórico que será utilizado para o próximo capítulo.

2.1. DIVISIBILIDADE

É inevitável falarmos sobre equações diofantinas sem nos referirmos à divisibilidade. Para que seja possível mostrarmos os resultados sobre a existência e métodos de obtenção de soluções de uma equação diofantina, e especificamente da equação de Pell, o conceito de divisibilidade se faz essencial, de modo que esta seção servirá para definir e demonstrar algumas propriedades referentes a este conceito.

Definição 2.1 (Conjunto limitado): Dado A um subconjunto de $\mathbb{Z}$, dizemos que A é limitado inferiormente se existe algum inteiro k tal que, para todo $a \in A$, temos $k \leq a$. Caso exista um elemento m, com $m \in A$, tal que para todo $a \in A$ temos $m \leq a$, o denominaremos como elemento mínimo de A e denotaremos por $m = min\, A$.

De forma análoga, define-se também conjunto limitado superiormente e elemento máximo de um conjunto onde, caso exista, representaremos por $max\, A$.

Axioma 2.1 (Propriedade Transitiva): Para todos inteiros a, b e c, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Axioma 2.2: Para todos inteiros a, b e c, se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

Axioma 2.3 (Princípio da Boa Ordem): Todo conjunto não vazio de inteiros não negativos possui um elemento mínimo.

Proposição 2.1: Dado a um inteiro tal que $0 \leq a \leq 1$. Então $a = 0$ ou $a = 1$.

Demonstração: Por absurdo, vamos supor que exista um inteiro a diferente de 0 e 1 que satisfaz $0 \leq a \leq 1$. Assim, o conjunto $A = \{a \in \mathbb{Z} \mid 0 < a < 1\}$ é não vazio e pelo Axioma 2.3 (Princípio da Boa Ordem), possui $m = min\, A$. Como $m \in A$, $m > 0$ e $m < 1$. Pelo Axioma 2.2, multiplicando por m ambas as desigualdades, obtemos $m^2 > 0$ e $m^2 < m$. Já pelo Axioma 2.1 (Propriedade Transitiva), como $m < 1$ e $m^2 < m$, temos $m^2 < 1$. Assim $m^2 \in A$, mas $m^2 < m = \min A$, uma contradição. ■

Com esse primeiro conjunto de definição, axiomas e proposição, podemos agora tratar sobre a divisão entre dois números inteiros.

Definição 2.2 (Divisibilidade): Dados dois números inteiros a e b, dizemos que b divide a (ou que a é divisível por b) se existe um inteiro c tal que $a = bc$. Podemos ainda falar que a é um múltiplo de b. Quando isso ocorrer, podemos usar a notação $b \mid a$; caso contrário, dizemos que b não divide a, isto é, $b \nmid a$.

Mesmo quando um número inteiro b, com b diferente de zero, não divide o inteiro a, ainda é possível fazer a divisão entre esses números, como veremos na Proposição 2.2 e no Teorema 2.1.

Proposição 2.2: Sejam a e b inteiros não negativos, com $b \neq 0$. Então existem q e r tais que $a = bq + r$ e $0 \leq r < b$.

Demonstração: Considere o seguinte conjunto:

$$X = \{a - bx \mid x \in \mathbb{Z}, a - bx \geq 0\}.$$

Note que para $x = 0$, temos $a - bx = a$ onde, por hipótese, temos $a \geq 0$. Logo $a \in X$ e X é um conjunto não vazio.

Pelo Axioma 2.1 (Princípio da Boa Ordem), existe $r = min\, X$ e como $r \in X$ e, é da forma $r = a - bq \geq 0$, para algum $q \in \mathbb{Z}$**.** Da proposição, falta mostrar que $r < b$.

Por absurdo, vamos supor que $r \geq b$.

Caso isso aconteça, teríamos,

$$a - b(q + 1) = a - bq - b = (a - bq) - b = r - b \geq 0.$$

E assim $a - b(q+1)$ também pertenceria a X. Mas

$$a - b(q+1) = r - b < r = min\, X$$

que resulta numa contradição. ■

Teorema 2.1 (Algoritmo da Divisão): Dados a e b inteiros, com $b \neq 0$, existem inteiros únicos q e r (denotamos como quociente q e resto r) de forma que $a = bq + r$, com $0 \leq r < |b|$.

Demonstração: Inicialmente mostraremos que podemos determinar q e r. Caso $b > 0$ e $a \geq 0$, o resultado está provado pela Proposição 2.2. Se $b > 0$ e $a < 0$, podemos ainda, pela Proposição 2.2, obter q' e r' de forma que:

$$|a| = bq' + r' \ e \ 0 \leq r' < b.$$

Onde, caso $r' = 0$, temos $-|a| = a = b(-q') + 0$, de onde $q = -q'$ e $r = 0$ verificam as condições do enunciado.

Porém, caso $r' > 0$, teremos:

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

Lembrando que $r' < b$, então $0 < b - r' < b$ e assim os números $q = -q' - 1$ e $r = b - r'$ satisfazem as condições do enunciado.

Com isso, precisamos mostrar que o teorema também vale quando $b < 0$. Utilizando a primeira parte dessa demonstração, qualquer que seja o valor de a, conseguimos determinar q' e r' de modo que

$$a = |b|q' + r' \ \text{ e } \ 0 \leq r' < |b|.$$

Se $b < 0$, temos $|b| = -b$ e com isso

$$a = |b|q' + r' = (-b)q' + r' = b(-q') + r'$$

de modo que os inteiros $q = -q'$ e $r = r'$ satisfazem as condições do enunciado.

Falta mostrar a unicidade. Suponha que existe $a = bq_1 + r_1 = bq_2 + r_2$ com q_1, q_2, r_1 e r_2 inteiros, $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$. Sem perda de generalidade, suponhamos $r_1 \leq r_2$, de onde $r_2 - r_1 \geq 0$. Reagrupando a igualdade $bq_1 + r_1 = bq_2 + r_2$, temos:

$$r_2 - r_1 = bq_1 - bq_2 = b(q_1 - q_2).$$

Lembrando que $r_2 - r_1 \geq 0$ e como de $r_2 < |b|$, temos que $r_2 - r_1 < |b|$, substituindo na expressão acima, obtemos:

$$0 \leq r_2 - r_1 = b(q_1 - q_2) < |b|.$$

E, aplicando módulo, resulta em

$$0 \leq |b||(q_1 - q_2)| < |b|.$$

Como $|b| > 0$, cancelando na expressão acima, temos $0 \leq |(q_1 - q_2)| < 1$, de onde, pela Proposição 2.1, resulta que $(q_1 - q_2) = 0$, ou seja, $q_1 = q_2$. Substituindo na expressão $bq_1 + r_1 = bq_2 + r_2$, teremos $bq_1 + r_1 = bq_1 + r_2$ onde, cancelando os termos iguais, resulta em $r_1 = r_2$. ■

Um conceito bastante útil quando trabalhamos com divisibilidade é o de divisor comum, no qual é definido por Milies e Coelho (2013) como sendo um inteiro c que divide simultaneamente a e b, ou seja, c divide a ($c|a$) e c divide b ($c|b$), onde a e b, são inteiros e ambos não nulos.

Podemos construir o conjunto $D(a,b)$, formado por todos os divisores positivos comuns de a e b. Esse conjunto é limitado superiormente, pois se a é diferente de zero, para todo elemento c pertencente ao conjunto $D(a,b)$, c é menor ou igual ao módulo de a. Consequentemente, $D(a,b)$ tem elemento máximo, resultando na próxima definição.

Definição 2.3 (Máximo Divisor Comum): Dados a e b inteiros, ambos não nulos, chamamos de máximo divisor comum de a e b o maior de seus divisores comuns, denotado por:

$$mdc(a,b) = \max D(a,b).$$

Para aprofundarmos a noção de máximo divisor comum, precisamos de um conceito matemático que é o de ideal.

Definição 2.4 (Ideal de $\mathbb{Z}$): Chamamos de um ideal de $\mathbb{Z}$ a um conjunto I não vazio de inteiros se:

a) $a, b \in I \Rightarrow a + b \in I$;
b) $a \in I, k \in \mathbb{Z} \Rightarrow ka \in I$.

Exemplo de um ideal é o próprio conjunto dos inteiros. Um exemplo mais interessante é o conjunto dos números pares, pois é fácil ver que a soma de números pares é par e o produto de um número par por qualquer número, também é par. Como contraexemplo, temos que o conjunto dos números ímpares não é um ideal, pois a soma de dois números ímpares não pertence a esse conjunto.

Exemplo 2.1: Mostrar que, dados dois números inteiros a e b, o conjunto $A = \{xa + yb;\ x, y\ \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.

De fato, considerando $x_1a + y_1b$ e $x_2a + y_2b$, pertencentes a A, temos que $(x_1a + y_1b) + (x_2a + y_2b) = (x_1 + x_2)a + (y_1 + y_2)b \in A$. Da mesma forma, dado $k \in \mathbb{Z}$, temos que $k(x_1a + y_1b) = (kx_1)a + (ky_1)b \in A$. Além disso, como observado em Hefez (2016), caso a e b não sejam simultaneamente nulos, então A é não vazio pois $a^2 + b^2 = a \cdot a + b \cdot b \in A$. Pela Definição 2.4, temos que o conjunto A é um ideal de $\mathbb{Z}$.

Retomando o exemplo do conjunto dos números pares, esse conjunto nada mais é do que o conjunto dos múltiplos de 2. De forma análoga, podemos obter novos exemplos de ideais utilizando esse conceito de múltiplo.

Dado um inteiro c, indicaremos por $c\mathbb{Z}$ o conjunto $c\mathbb{Z} = \{cr | r \in \mathbb{Z}\}$, isto é, o conjunto de todos os múltiplos de c. Note que, dados $a, b \in c\mathbb{Z}$ existem x e y inteiros tais que $a = cx$ e $b = cy$. Temos assim que $a + b = cx + cy = c(x + y)$ pertence a $c\mathbb{Z}$. Da mesma forma, dado $k \in \mathbb{Z}$, temos que $ka = k(cx) = c(kx)$ também pertence a $c\mathbb{Z}$, satisfazendo a Definição 2.4 de ideal de $\mathbb{Z}$.

O Teorema 2.2 a seguir estabelece uma relação entre o conceito de ideal e o de máximo divisor comum:

Teorema 2.2: Sejam a, b inteiros, não ambos nulos e o ideal dado por $I = \{xa + yb;\ x, y\ \in \mathbb{Z}\}$. Se $d = min\, I \cap \mathbb{N}$, então d é o máximo divisor comum de a e b e $I = d\mathbb{Z}$.

Demonstração: Inicialmente, vamos mostrar que d é o máximo divisor comum de a e b. Para isso, considere um número c tal que c divide a e c divide b, logo c divide também os números da forma xa e yb e, consequentemente, a soma $xa + yb$. Sendo assim, c divide todos os números do conjunto I. Em particular, c divide d.

Considere agora, por absurdo, um número $f \in I$ tal que $d \nmid f$. Assim, pela divisão euclidiana, temos $f = dq + r$, com $0 < r < d$. Mas $f = xa + yb$ e $d = ma + nb$, para alguns x, y, m, n inteiros, e podemos reescrever o resto r da forma

$$\begin{aligned} r &= f - dq \\ &= (xa + yb) - (ma + nb)q \\ &= xa - qma + yb - qnb \\ &= (x - qm)a + (y - qn)b. \end{aligned}$$

E, portanto, $r \in I \cap \mathbb{N}$, contradição, pois $0 \leq r < d$ e $d = min\, I \cap \mathbb{N}$. Em particular, $d|a$ e $d|b$, logo d é o máximo divisor comum de a e b.

Falta mostrarmos que $I = d\mathbb{Z}$. Como todo elemento de I é divisível por d, segue que $I \subset d\mathbb{Z}$. Para a inclusão contrária, dado um elemento $g \in d\mathbb{Z}$, podemos escrever g como sendo $g = hd$, para algum h inteiro. Lembrando que, como $d \in I$ pode ser escrito como $d = ma + nb$ para algum m e n inteiros, temos então,

$$hd = h(ma + nb) = (hm)a + (hn)b.$$

E assim $hd \in I$. Logo, $d\mathbb{Z} \subset I$ e consequentemente, $d\mathbb{Z} = I$. ■

Com os resultados anteriores, conseguimos mostrar que, a partir de dois números inteiros, é possível escrever o máximo divisor comum como uma combinação entre eles, como mostra o teorema a seguir.

Teorema 2.3 (Teorema de Bézout): Dados a, b inteiros e $d = mdc(a, b)$, então existem inteiros r e s tais que $d = ra + sb$.

Demonstração: Considere o conjunto $I = \{xa + yb;\ x, y \in \mathbb{Z}\}$ e, utilizando o Teorema 2.2, temos que $I = d\mathbb{Z}$. Logo, $d = mdc(a, b)$ e $d \in I$ e, pela Definição 2.4, d pode ser escrito como $d = ra + sb$ para alguns r e s inteiros. ■

Com o Teorema de Bézout (Teorema 2.3) conseguimos também estabelecer uma condição para a existência de soluções de uma equação diofantina linear, como veremos na próxima seção.

Teorema 2.4 (Lema de Gauss): Dados a, b e c números inteiros. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração: Como, da hipótese $a|bc$, existe um inteiro e tal que $bc = ae$. Também da hipótese, como $mdc(a, b) = 1$, pelo Teorema 2.3 (Teorema de Bézout), existem r e s também inteiros tais que $ra + sb = 1$.

Multiplicando ambos os lados dessa última expressão por c, obtemos

$$rac + sbc = c$$

como $bc = ae$, substituindo na expressão acima, obtemos:

$$rac + sae = c \Rightarrow a(rc + se) = c$$

e como a divide o primeiro membro, temos que $a|c$. ■

Por fim, apresentamos o Algoritmo de Euclides, no qual abordaremos para trabalhar com frações contínuas.

Teorema 2.5 (Algoritmo de Euclides): Dados a e b inteiros com $b \neq 0$ e sejam q e r, respectivamente, o quociente e o resto da divisão de a por b. Então $D(a, b) = D(b, r)$. Temos ainda que $mdc(a, b) = mdc(b, r)$.

Demonstração: Pelo Teorema 2.1, podemos expressar a como sendo $a = bq + r$, com $0 \leq r < |b|$. Considere $x \in D(a, b)$, então $x|a$ e $x|b$. Sendo $r = a - bq$, temos então que $x|r$, pois $x \in D(a, b)$ e, portanto, $x \in D(b, r)$. Com isso, $D(a, b) \subset D(b, r)$.

Da mesma forma, dado $y \in D(b, r)$, então $y|b$ e $y|r$. Sendo $a = bq + r$, temos então que $y|a$ e, portanto, $y \in D(a, b)$. Com isso, $D(b, r) \subset D(a, b)$, resultando na igualdade

dos conjuntos. Consequentemente, como os conjuntos são iguais e possuem elemento máximo, segue que $mdc(a,b) = mdc(b,r)$. ■

Esse processo pode ser repetido, gerando assim divisões sucessivas:

$$a = bq_1 + r_1, \ \ 0 \leq r_1 < |b|$$
$$b = r_1q_2 + r_2, \ \ 0 \leq r_2 < r_1$$
$$r_1 = r_2q_3 + r_3, \ \ 0 \leq r_3 < r_2$$
$$\ldots$$
$$r_{n-2} = r_{n-1}q_n + r_n, \ \ 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_nq_{n+1}$$

Como o resto vai diminuindo em cada divisão, o processo se torna finito e alguma das divisões será exata. Suponhamos que isso aconteça pela primeira vez para r_{n-1}. Sendo assim, aplicando o Teorema 2.5, temos:

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots = mdc(r_{n-2},r_{n-1}) = mdc(r_{n-1},r_n)$$

e como r_n divide r_{n-1}, temos que $mdc(r_{n-1},r_n) = r_n$ e, portanto, $mdc(a,b) = r_n$.

2.2. EQUAÇÕES DIOFANTINAS LINEARES

Como explica Hefez (2016), vários problemas de aritmética recaem na resolução, em números inteiros, de equações da forma $ax + by = c$, com a, b e c inteiros e diferentes de zero. Essas equações são chamadas equações diofantinas lineares.

Embora seu estudo aprofundado se concentre no Ensino Superior, é possível encontrar abordagens no Ensino Básico, como por exemplo, os trabalhos desenvolvidos por Neto (2016), Deus (2017) e Maia (2018). No trabalho de Maia, o autor também destaca a influência desse assunto em competições olímpicas voltadas à Matemática.

Segundo Milies e Coelho (2013), além dos aspectos aritméticos envolvidos, podemos também resolver esse problema de forma geométrica, uma vez que equações do tipo $ax + by = c$, em que x e y são números reais, representam uma

reta no plano cartesiano. Neste caso, a resolução de uma equação diofantina linear pode ser reduzida a encontrar os pares ordenados (x, y) pertencentes à reta e que possuem coordenadas inteiras.

Destacamos que nem todas as equações diofantinas possuem solução, como exemplo a equação $4x + 6y = 7$. Para quaisquer inteiros x e y, o primeiro membro da equação sempre resultará num número par, enquanto o segundo é o número 7, um número ímpar. Logo, esta equação nunca é satisfeita.

Assim, dada a equação diofantina linear $ax + by = c$, o primeiro passo para a resolução dessa equação é estabelecer condições para a existência de soluções.

Proposição 2.3: Dados a, b e c inteiros e $d = mdc(a, b)$, a equação diofantina linear $ax + by = c$ tem soluções se e somente se $d|c$.

Demonstração: Considere o conjunto I formado por todos os valores que o primeiro membro pode assumir, isto é,

$$I = \{ax + by \mid x, y \in \mathbb{Z}\}.$$

O qual já vimos no Exemplo 2.1 se tratar de um ideal de $\mathbb{Z}$ e, pelo Teorema 2.2, $I = d\mathbb{Z}$. Como $c = ax + by$, a equação diofantina linear tem solução se e somente se $c \in I$, ou seja, $c = dk$ para algum k inteiro, e isso acontece se e somente se $d|c$. ■

A partir disso, precisamos encontrar um método para a resolução da equação diofantina linear.

Proposição 2.4: Considere a equação diofantina linear $ax + by = c$, onde $d = mdc\,(a, b)|c$. Considere também o teorema de Bézout, no qual podemos escrever $d = ra + sb$, com r, s inteiros. Dado essas informações, uma solução particular da equação diofantina é dada por

$$x_0 = r \cdot \frac{c}{d} \;\; e \;\; y_0 = s \cdot \frac{c}{d}$$

e toda outra solução será da forma:

$$\begin{aligned} x &= r\cdot\frac{c}{d}+\frac{b}{d}\cdot t \Rightarrow x = x_0+\frac{b}{d}\cdot t \\ y &= s\cdot\frac{c}{d}-\frac{a}{d}\cdot t \Rightarrow y = y_0-\frac{a}{d}\cdot t \end{aligned} \quad , t \in \mathbb{Z} \qquad (2.1)$$

Reciprocamente, para todo t inteiro, os valores x e y dados pela Equação (2.1) são soluções da equação diofantina $ax + by = c$.

Demonstração: Dado $d = ra + sb$, multiplicando ambos os membros por $\frac{c}{d}$, temos:

$$r\left(\frac{c}{d}\right)a + s\left(\frac{c}{d}\right)b = d\left(\frac{c}{d}\right) = c \Longrightarrow a\left(r\cdot\frac{c}{d}\right) + b\left(s\cdot\frac{c}{d}\right) = c.$$

Logo, considerando

$$x_0 = r\cdot\frac{c}{d} \;\; e \;\; y_0 = s\cdot\frac{c}{d}$$

temos que x_0 e y_0 é uma solução.

Falta mostrar que todo par de inteiros dados pela Equação (2.1) é solução e que toda solução é dessa forma. De fato, substituindo as expressões dadas pela Equação (2.1) na equação diofantina linear, obtemos:

$$a\left(x_0+\frac{b}{d}\cdot t\right) + b\left(y_0-\frac{a}{d}\cdot t\right) = ax_0 + \frac{ab}{d}\cdot t + by_0 - \frac{ab}{d}\cdot t = ax_0 + by_0 = c.$$

Considere agora (x_1, y_1) uma solução da equação diofantina linear. Como mostram Milies e Coelho (2013), basta provar que existe t inteiro tal que

$$x_1 = x_0 + \frac{b}{d}\cdot t \;\; e \;\; y_1 = y_0 - \frac{a}{d}\cdot t.$$

Como os pares (x_0, y_0) e (x_1, y_1) são soluções da equação diofantina $aX + bY = c$, temos

$$ax_1 + by_1 = ax_0 + by_0 \Rightarrow ax_1 - ax_0 = by_0 - by_1 \Rightarrow a(x_1 - x_0) = b(y_0 - y_1) \qquad (2.2)$$

Tomando $d = mdc(a, b)$, podemos reescrever $a = a'd$ e $b = b'd$, de onde:

$$a' = \frac{a}{d} \ \ e \ \ b' = \frac{b}{d}.$$

Note que d é o máximo divisor comum entre a e b. Sendo assim, os números dados por a' e b' não possuem divisores comuns entre si, resultando em:

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

Dividindo o resultado obtido na Equação (2.2) por d, obtemos:

$$\frac{a(x_1 - x_0)}{d} = \frac{b(y_0 - y_1)}{d} \Rightarrow a'(x_1 - x_0) = b'(y_0 - y_1)$$

como b' divide $b'(y_0 - y_1)$, temos que $b'|a'(x_1 - x_0)$. Porém, como $mdc(a', b') = 1$, do Teorema 2.4 (Lema de Gauss) vem que $b'|x_1 - x_0$, e, portanto existe t inteiro tal que $x_1 - x_0 = b't$. Reescrevendo:

$$x_1 - x_0 = b't \Rightarrow x_1 - x_0 = \frac{b}{d}t \Rightarrow x_1 = x_0 + \frac{b}{d}t.$$

Por fim, substituindo $x_1 - x_0 = b't$ na expressão $a'(x_1 - x_0) = b'(y_0 - y_1)$, temos:

$$a'(b't\ ) = b'(y_0 - y_1) \Rightarrow a't = y_0 - y_1 \Rightarrow \frac{a}{d}t = y_0 - y_1 \Rightarrow y_1 = y_0 - \frac{a}{d}t.$$

Assim, obtemos as mesmas expressões apresentadas na Equação (2.1) para as soluções da equação diofantina linear dada. ■

Sendo assim, resolver uma equação diofantina linear consiste em obter r e s de modo que tenhamos $d = ra + sb$. Milies e Coelho (2013), assim como Hefez (2016), resolvem as equações diofantinas lineares através do Algoritmo de Euclides, no qual como vimos, consiste em realizar a divisão entre os inteiros a e b e, a partir do quociente e restos obtidos, realizar divisões sucessivas entre o divisor e o novo quociente obtido. Como o resto está vinculado a ser menor do que o quociente (como visto no Teorema 2.1), e maior que zero, esse processo se torna finito na medida que os novos quocientes também vão decrescendo.

Nesse ponto escolhemos fazer uma abordagem que embora também trabalhe com a divisão euclidiana, segue uma linguagem familiar para os estudantes do

Ensino Básico. Neto (2016) denomina o processo como Método de Euler que consiste em, dada uma equação diofantina linear $ax + by = c$, isolar a variável que apresenta menor coeficiente para que possamos analisar a fração resultante e, assim, repetir o processo se necessário.

Método de Euler: Dado a equação diofantina $ax + by = c$, sem perda de generalidade, vamos supor $a > b$. Dessa forma, podemos a partir do menor coeficiente (b), reescrever a equação como:

$$ax + by = c \Longrightarrow y = \frac{c - ax}{b} = \frac{c}{b} - \frac{ax}{b}.$$

Considerando que a não seja divisível por b, pelo Teorema 2.1, podemos reescrever a como sendo $a = bq + r$, com $0 \leq r < b$. Substituindo na equação acima, obtemos:

$$y = \frac{c}{b} - \frac{ax}{b} = \frac{c}{b} - \frac{(bq + r)x}{b} = \frac{c}{b} - \frac{rx}{b} - \frac{bqx}{b} = \frac{c - rx}{b} - qx.$$

E, assim, por estarmos buscando soluções inteiras, para que a equação original tenha solução, temos que $b|(c - rx)$, ou em outras palavras, existe um número inteiro q tal que $bq = c - rx$ no qual, reagrupando, obtemos uma nova equação diofantina $rx + bq = c$, mas que apresenta um dos coeficientes, em módulo, menor do que o da equação original (pois $0 < r \leq b < a$). A partir dessa nova equação diofantina, podemos repetir o processo aplicado inicialmente.

Note que esse processo também trata de divisões sucessivas e, consequentemente, o processo é finito decorrente do resto de cada divisão ir se aproximando de zero. O método encerra quando temos uma divisão exata (nesse caso, uma expressão livre de frações) ou quando existe possibilidade de presumir uma solução particular da equação diofantina.

A diferença em apresentarmos o Método de Euler mostrado por Neto (2016) ao invés do método utilizando o Algoritmo de Euclides consiste na facilidade de se trabalhar com esse procedimento na Educação Básica, pois trabalha apenas com frações, polinômios e substituições.

Para facilitar a compreensão do Método de Euler, ilustraremos o seu processo através dos Exemplos 2.2 e 2.3. Além disso, simplificaremos as frações obtidas sempre que isso for possível de forma a diminuir os cálculos.

Exemplo 2.2: Resolver a equação diofantina $172x + 20y = 1000$.

Inicialmente, pela Proposição 2.3, é preciso verificar se a equação dada possui solução ou não. Para obtermos o $mdc\,(172, 20)$, basta observar que, entre os divisores de 20, 4 é o maior deles que também divide 172. E, a partir disso, o máximo divisor comum entre os coeficientes 172 e 20 divide o termo independente 1000, o que garante a existência da solução. Assim

$$mdc\,(172, 20) = 4 \text{ e } 4|1000.$$

Como descrito pelo Método de Euler, identificadas as duas variáveis, isolaremos a que apresenta o menor dos coeficientes para que possamos analisar a fração resultante e assim repetir o processo se necessário. Neste caso, isolaremos a variável y, obtendo:

$$y = \frac{1000 - 172x}{20} = 50 - \frac{43x}{5} = 50 - 8x - \frac{3x}{5}.$$

As soluções serão inteiras caso x seja múltiplo de 5, ou seja, $5|3x$.

Da Proposição 2.4 e, tomando $x = 0$, temos a solução particular $x = 0$ e $y = 50$. Considerando a solução particular e que no caso do exemplo temos $a = 172$, $b = 20$, $c = 1000$ e $d = mdc\,(172, 20) = 4$, obtemos as soluções da forma:

$$\begin{matrix} x = 0 + \frac{20}{4} \cdot t \Longrightarrow x = 5t \\ y = 50 - \frac{172}{4} \cdot t \Rightarrow y = 50 - 43t \end{matrix} \quad , \quad t \in \mathbb{Z}.$$

Exemplo 2.3: Resolver a equação diofantina $172x + 20y = 996$.

De acordo com a Proposição 2.3, a equação possui solução, pois assim como no Exemplo 2.2, o $mdc\,(172, 20) = 4$ e 4 também divide 996.

Aplicando o Método de Euler, isolando y temos:

$$y = \frac{996 - 172x}{20} = \frac{980 - 160x}{20} + \frac{16 - 12x}{20} = 49 - 8x + \frac{4 - 3x}{5}$$

que resultará em um número inteiro se, e somente se, $5|(4 - 3x)$, ou seja, existe um inteiro p, de tal forma que:

$$5p = 4 - 3x \Rightarrow 3x + 5p = 4.$$

Repetindo o método aplicado inicialmente, iremos isolar x, obtendo:

$$x = \frac{4 - 5p}{3} = \frac{3 - 3p}{3} + \frac{1 - 2p}{3} = 1 - p + \frac{1 - 2p}{3}$$

no qual mais uma vez resultará em um número inteiro se $3|(1 - 2p)$. Assim, existe um inteiro q, de tal forma que:

$$3q = 1 - 2p \Rightarrow 2p + 3q = 1.$$

Como descrito no Método de Euler, podemos continuar o processo para reduzir cada vez mais as frações obtidas até obtermos uma simplificação que não envolva divisões. Pórem, pela última equação, é fácil perceber que $p = -1$ e $q = 1$ é uma solução particular da equação onde fazendo as devidas substituições, vem que:

$$x = \frac{4 - 5p}{3} = \frac{4 + 5}{3} = 3$$
$$y = \frac{996 - 172x}{20} = \frac{996 - 516}{20} = \frac{480}{20} = 24.$$

Que de fato é uma solução da equação diofantina linear dada, pois $172 \cdot 3 + 20 \cdot 24 = 996$. Além disso, a partir dessa solução particular, pela Proposição 2.4, temos as soluções gerais dadas por:

$$\begin{matrix} x = 3 + \frac{20}{4} \cdot t \Longrightarrow x = 3 + 5t \\ y = 24 - \frac{172}{4} \cdot t \Rightarrow y = 24 - 43t \end{matrix} \quad , \qquad t \in \mathbb{Z}.$$

Outros métodos também podem ser utilizados para resolver equações, como por exemplo, através do uso de congruências, onde observa-se que obter a solução de uma congruência é similar a obter as soluções inteiras de uma equação diofantina linear.

2.3. CONGRUÊNCIAS

Utilizando a definição dada por Hefez (2016) temos:

Definição 2.5 (Congruência): Dado m um número inteiro, dois números inteiros a e b são congruentes módulo m se os restos de sua divisão por m são iguais. Caso isso aconteça, podemos escrever:

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

Por exemplo, $13 \equiv 22\ (\mathrm{mod}\ 3)$, pois ao dividirmos 13 por 3 obtemos resto 1, assim como ao dividirmos 22 por 3. Caso a relação $a \equiv b\ (mod\ m)$ seja falsa, diremos que a e b não são congruentes, ou que são incongruentes módulo m.

Proposição 2.5: Dados a, b e m inteiros, com $m > 1$. Temos que $a \equiv b\ (mod\ m)$ se, e somente se, $m|(b - a)$.

Demonstração: Aplicando o Teorema 2.1 (Algoritmo da Divisão) para realizar as divisões de a e b por m, obtemos $a = mq_1 + r_1$, com $0 \leq r_1 < m$ e $b = mq_2 + r_2$, com $0 \leq r_2 < m$ e q_1 e q_2 números inteiros . Subtraindo as divisões, temos:

$$b - a = (mq_2 + r_2) - (mq_1 + r_1) = mq_2 - mq_1 + r_2 - r_1 = m(q_2 - q_1) + (r_2 - r_1).$$

Caso tenhamos $a \equiv b\ (mod\ m)$, pela definição dada por Hefez (2016), dois números inteiros a e b são congruentes módulo m se os restos de sua divisão por m são iguais, ou seja, $r_1 = r_2$. Consequentemente, $b - a = m(q_2 - q_1)$, de onde obtemos que $m|(b - a)$.

Reciprocamente, caso $m|(b - a)$, a expressão dada abaixo

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

só será verdadeira se $m|(r_2 - r_1)$. Porém, como $r_2 < m$ temos que $0 \leq |r_2 - r_1| < m$ de onde temos que $r_2 - r_1 = 0$ resultando em $r_1 = r_2$. ■

Estabelecer a congruência linear entre dois números é equivalente ao problema de determinar, se existir, valores inteiros x tais que:

$$ax \equiv b\ (mod\ m), \text{ com } a, b, m \in \mathbb{Z} \text{ e } m > 1. \qquad (2.3)$$

Proposição 2.6: Dados a, b e m inteiros, com $m > 1$, a congruência linear $ax \equiv b\ (mod\ m)$ possui solução se, e somente se, o $mdc\ (a,m)$ divide b.

Demonstração: Inicialmente, caso a congruência linear $ax \equiv b\ (mod\ m)$ possua uma solução x_0, temos pela Proposição 2.5 que $m|(ax_0 - b)$ ou, em outras palavras, existe y_0 inteiro tal que:

$$my_0 = ax_0 - b \Rightarrow ax_0 - my_0 = b.$$

E, portanto, a equação $ax_0 - my_0 = b$ possui solução. Como temos uma equação diofantina linear, provamos na Proposição 2.3 que a equação possui solução se $mdc\ (a,m)$ divide b.

Reciprocamente, caso $mdc\ (a,m)|b$, novamente pela Proposição 2.3, a equação $ax - my = b$ admite x_0 e y_0 como soluções. Dessa forma, temos

$$ax_0 - my_0 = b \Rightarrow ax_0 = my_0 + b.$$

De onde x_0 é solução da congruência $ax \equiv b\ (mod\ m)$. ■

Observe assim que, obter a solução da congruência $ax \equiv b\ (mod\ m)$ é similar a obter as soluções inteiras x e y da equação diofantina linear $ax - my = b$.

Estamos assim interessados em determinar todas as soluções da congruência $ax \equiv b\ (mod\ m)$. Note inicialmente que, caso x_0 seja uma das soluções dessa recorrência, então todo x tal que $x \equiv x_0\ (mod\ m)$ também será, pois

$$ax \equiv ax_0 \equiv b\ (mod\ m).$$

Embora isso gere infinitas soluções, iremos considerar como uma só, por serem congruentes entre si. Precisamos assim encontrar todas as soluções que, além de resolver a congruência dada, sejam incongruentes entre si (módulo m).

Teorema 2.6: Dados a, b e m inteiros, com $m > 1$. Se x_0 é uma solução da congruência $ax \equiv b\ (mod\ m)$, então

$$x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \dots, x_0 + (d-1)\frac{m}{d}$$

onde $d = mdc(a, m)$ representa um sistema completo de d soluções da congruência, duas a duas incongruentes (módulo m).

Demonstração: Precisamos mostrar que toda solução x da congruência linear $ax \equiv b\ (mod\ m)$ é congruente, módulo m, a expressão $x_0 + k\,\frac{m}{d}$ para algum k, com $0 \leq k < d$.

Assim, considerando x uma solução qualquer da congruência, temos

$$ax \equiv ax_0\ (mod\ m)$$

onde, pela Proposição 2.5, a equação possui solução, assim temos que $m|(ax - ax_0)$. Isso significa que, para algum inteiro l, temos $ml = ax - ax_0$. Como $d = mdc(a, m)$, podemos dividir ambos os membros por d, obtendo:

$$\frac{ml}{d} = \frac{ax - ax_0}{d} \Rightarrow \frac{m}{d}l = \frac{a}{d}(x - x_0). \tag{2.4}$$

Além disso, note que como d é o máximo divisor comum entre a e m, ao dividirmos ambos os valores por d, retiramos todos os divisores que são comuns entre os dois números, de modo que

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

Para facilitar os cálculos, como existe um inteiro a' tal que $a = a'd$, substituindo na Equação (2.4) obtemos:

$$\frac{m}{d}l = \frac{a}{d}(x - x_0) \Rightarrow \frac{m}{d}l = a'(x - x_0).$$

Como o número a' divide o segundo membro, ao dividirmos ambos os lados da equação por a', teremos que a' divide l, pois o máximo divisor comum entre $\frac{m}{d}$ e a' é igual a 1. Com isso,

$$\frac{m}{d} \cdot \frac{l}{a'} = x - x_0$$

onde, considerando $\frac{l}{a'} = n$, resulta em

$$\frac{m}{d} \cdot \frac{l}{a'} = x - x_0 \Rightarrow \frac{mn}{d} = x - x_{0.}$$

Fazendo a divisão de n por d, pelo Teorema 2.1 (Algoritmo da Divisão) existem inteiros q e k, com $0 \leq k < d$ de tal modo que $n = qd + k$. Substituindo na expressão acima, temos

$$\frac{mn}{d} = x - x_0 \Rightarrow \frac{m(qd+k)}{d} = x - x_0 \Rightarrow mq + k\frac{m}{d} = x - x_0$$

reagrupando, obtemos:

$$mq + k\frac{m}{d} = x - x_0 \Rightarrow x = x_0 + mq + k\frac{m}{d} \Rightarrow x \equiv x_0 + k\frac{m}{d}\ (mod\ m).$$

Reciprocamente, os números da forma $x_0 + k\ \frac{m}{d}$ são soluções da congruência linear $ax \equiv b\ (mod\ m)$. De fato, pois como d divide a e x_0 é uma solução, temos:

$$ax = a\left(x_0 + k\frac{m}{d}\right) = ax_0 + k\frac{a}{d}m \equiv ax_0 \equiv b\ (mod\ m).$$

Com isso, falta mostrar que os números da forma $x_0 + k\ \frac{m}{d}$ são incongruentes entre si. Para tanto, considere duas soluções distintas, $x_0 + i\ \frac{m}{d}$ e $x_0 + j\ \frac{m}{d}$, com $i \neq j$, $0 \leq i < d$ e $0 \leq j < d$. Por absurdo, supondo que essas soluções são congruentes entre si, temos:

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d}\ (mod\ m)$$

no qual, pela Proposição 2.5, temos que

$$m \left| \left(\left(x_0 + i\frac{m}{d}\right) - \left(x_0 + j\frac{m}{d}\right)\right) \Rightarrow m \right| \left(i\frac{m}{d} - j\frac{m}{d}\right)$$

e assim,

$$i\frac{m}{d} \equiv j\frac{m}{d}\ (mod\ m).$$

Como $0 \leq i < d$, multiplicando a desigualdade por $\frac{m}{d}$, obtemos que $0 \leq i\frac{m}{d} < m$. De forma similar, obtemos também que $0 \leq j\frac{m}{d} < m$. Note então que:

$$0 \leq i\frac{m}{d} < m \Rightarrow 0 \leq \left|i\frac{m}{d} - j\frac{m}{d}\right| < m$$

como já vimos que m divide $\left(i\frac{m}{d} - j\frac{m}{d}\right)$, segue que

$$i\frac{m}{d} = j\frac{m}{d} \Rightarrow i = j$$

contradição, pois por hipótese, $i \neq j$. ■

Exemplo 2.4: Resolver a congruência

$$2x \equiv 8\ (\mathrm{mod}\ 6).$$

Como 6 é múltiplo de 2, podemos observar que $mdc\ (2,6) = 2$. Pela Proposição 2.6, 2 divide 8, garantindo a existência da solução.

Nessa congruência, como $d = 2$, obtemos assim duas soluções incongruentes entre si módulo 6. Por inspeção, 1 é uma dessas soluções. Aplicando o Teorema 2.6, as duas soluções são dadas por

$$x_0 \text{ e } x_0 + \frac{m}{d}.$$

No qual, chamando $x_0 = 1$, encontramos como segunda solução $x_0 + \frac{m}{d} = 1 + 3 = 4$.

A partir dessas soluções, podemos encontrar outros valores que também são soluções da equação dada, mas que são congruentes aos dois valores encontrados.

Utilizando o mesmo exemplo, aplicando a Proposição 2.5, temos, para algum inteiro y, que $6y = 2x - 8$, resultando na equação diofantina linear $2x - 6y = 8$, da

qual, considerando a solução da congruência $x = 1$ obtemos $y = -1$, representando assim uma das soluções particulares da equação diofantina. Em outras palavras, podemos utilizar congruências para auxiliar na obtenção das soluções de uma equação diofantina.

Na próxima seção, serão abordados alguns tópicos sobre recorrência, de forma a auxiliar na resolução das Equações de Pell.

2.4. RECORRÊNCIAS

Quando trabalhamos com recorrências, é inevitável falarmos sobre sequências. Como define Neto (2016), uma sequência de números reais é uma função que faz uma bijeção entre os números naturais e os números reais, de tal forma que temos $a: \mathbb{N} \to \mathbb{R}$, ou seja, para cada n pertencente aos naturais associa-se um número a_n pertencente aos reais e denominado de enésimo termo da sequência.

Morgado e Carvalho (2015) argumentam que diversas sequências podem ser definidas por recorrência, isto é, recursivamente por intermédio de uma regra que permite obter qualquer termo em função dos termos antecessores.

Como exemplo de recorrência, temos a sequência F_n de Fibonacci (cujos termos são 1, 1, 2, 3, 5, 8, ...), na qual, a partir do 3º termo, cada termo é a soma dos dois imediatamente anteriores. Dessa forma, tendo para n natural e $n \geq 1$, podemos definir a sequência por $F_{n+2} = F_{n+1} + F_n$, com $F_1 = F_2 = 1$. Qualquer progressão aritmética ou geométrica também são exemplos de recorrências, pois os termos são definidos em função do primeiro termo e da razão da progressão.

Caso tivéssemos estabelecido outros termos iniciais da sequência F_n, não teríamos a sequência de Fibonacci e sim, uma outra sequência que tem a mesma regra de formação.

Dito isso, é fácil perceber que, para que a sequência fique perfeitamente determinada recursivamente, são necessárias informações referentes ao tipo de recorrência.

Uma recorrência na qual cada termo depende exclusivamente dos anteriores é dita homogênea. Caso contrário, a recorrência é dita não-homogênea.

Além disso, uma recorrência é dita de primeira ordem caso cada termo seja expresso diretamente em função do termo imediatamente anterior a ele. Estendendo a ideia, uma recorrência é dita de segunda ordem quando cada termo é obtido em função dos dois termos anteriores a ele.

Por fim, a recorrência é dita linear quando a relação entre cada termo da recorrência com os termos anteriores se dá de forma semelhante a uma função do primeiro grau.

Utilizando as definições acima estabelecidas, a sequência de Fibonacci é um exemplo de recorrência linear de segunda ordem homogênea. Recorrências desse tipo são da forma:

$$x_{n+2} + px_{n+1} + qx_n = 0, \text{ com } p, q \in \mathbb{R} \; e \; q \neq 0. \tag{2.5}$$

Segundo Morgado e Carvalho (2015), a cada recorrência estabelecida pela Equação (2.5) é possível associar uma equação do segundo grau $t^2 + pt + q = 0$, denominada equação característica, cujas raízes são utilizadas para a obtenção de suas soluções, conforme as Proposições 2.7 e 2.8.

Proposição 2.7: Seja a recorrência $x_{n+2} + px_{n+1} + qx_n = 0$, com p, q reais e $q \neq 0$, na qual podemos associar a equação característica $t^2 + pt + q = 0$. Dados t_1 e t_2 raízes da equação $t^2 + pt + q = 0$, então para quaisquer valores c_1 e c_2, $a_n = c_1 t_1^n + c_2 t_2^n$ é solução da recorrência $x_{n+2} + px_{n+1} + qx_n = 0$.

Demonstração: Suponhamos que t_1 e t_2 são raízes da equação $t^2 + pt + q = 0$. Desse modo, temos ${t_1}^2 + pt_1 + q = 0$ e ${t_2}^2 + pt_2 + q = 0$. Sendo $a_n = c_1 t_1^n + c_2 t_2^n$, ao substituir a_n na recorrência $x_{n+2} + px_{n+1} + qx_n$, obtemos:

$$(c_1 t_1^{n+2} + c_2 t_2^{n+2}) + p(c_1 t_1^{n+1} + c_2 t_2^{n+1}) + q(c_1 t_1^n + c_2 t_2^n)$$

no qual, reagrupando, temos:

$$c_1 t_1^n t_1^2 + c_2 t_2^n t_2^2 + pc_1 t_1^n t_1 + pc_2 t_2^n t_2 + qc_1 t_1^n + qc_2 t_2^n =$$
$$c_1 t_1^n (t_1^2 + pt_1 + q) + c_2 t_2^n (t_2^2 + pt_2 + q) = c_1 t_1^n 0 + c_2 t_2^n 0 = 0.$$

Portanto, a_n é solução da recorrência. ■

Caso tenhamos raízes distintas para a equação característica, segue a Proposição 2.8.

Proposição 2.8: Seja a recorrência $x_{n+2} + px_{n+1} + qx_n = 0$, com p, q reais e $q \neq 0$, na qual podemos associar a equação característica $t^2 + pt + q = 0$. Dados t_1 e t_2 raízes de $t^2 + pt + q = 0$, com $t_1 \neq t_2$, então todas as soluções da recorrência $x_{n+2} + px_{n+1} + qx_n = 0$ são da forma $a_n = c_1 t_1^n + c_2 t_2^n$, com c_1 e c_2 constantes reais.

Demonstração: Note que, por definição da recorrência $x_{n+2} + px_{n+1} + qx_n = 0$, temos $q \neq 0$, o que implica em $t_1 \neq 0$ e $t_2 \neq 0$, pois caso contrário teríamos para a equação característica

$$t^2 + pt + q = 0^2 + p \cdot 0 + q = 0 \Longrightarrow q = 0,$$

o que seria uma contradição.

Considere y_n uma solução qualquer de $x_{n+2} + px_{n+1} + qx_n = 0$. Inicialmente, vamos considerar que y_n seja da forma $a_n = c_1 t_1^n + c_2 t_2^n$, na qual, como vimos na Proposição 2.7, trata-se de uma solução da recorrência dada. Assim, de modo a encontrar as constantes c_1 e c_2, resolveremos o sistema de equações:

$$\begin{cases} y_1 = c_1 t_1 + c_2 t_2 \\ y_2 = c_1 t_1^2 + c_2 t_2^2 \end{cases}$$

Isolando c_1 na primeira equação do sistema, obtemos:

$$c_1 = \frac{y_1 - c_2 t_2}{t_1} \tag{2.6}$$

no qual, ao substituirmos na segunda equação, resulta em:

$$y_2 = \left(\frac{y_1 - c_2 t_2}{t_1}\right) t_1^2 + c_2 t_2^2 = (y_1 - c_2 t_2) t_1 + c_2 t_2^2$$
$$= t_1 y_1 - c_2 t_2 t_1 + c_2 t_2^2 = c_2(t_2^2 - t_2 t_1) + t_1 y_1.$$

Assim, isolando c_2, temos:

$$c_2(t_2^2 - t_2 t_1) + t_1 y_1 = y_2 \Rightarrow c_2 = \frac{y_2 - t_1 y_1}{t_2^2 - t_2 t_1} \Rightarrow c_2 = \frac{y_2 - t_1 y_1}{t_2(t_2 - t_1)}.$$

Para encontrar c_1, basta substituir o valor encontrado de c_2 na Equação (2.6):

$$c_1 = \frac{y_1 - c_2 t_2}{t_1} = \frac{y_1 - \left(\frac{y_2 - t_1 y_1}{t_2(t_2 - t_1)}\right) t_2}{t_1} = \frac{y_1 - \frac{y_2 - t_1 y_1}{(t_2 - t_1)}}{t_1}$$
$$= \frac{\frac{y_1(t_2 - t_1) - y_2 + t_1 y_1}{(t_2 - t_1)}}{t_1} = \frac{y_1 t_2 - y_1 t_1 - y_2 + t_1 y_1}{t_1(t_2 - t_1)} = \frac{y_1 t_2 - y_2}{t_1(t_2 - t_1)}.$$

Com o sistema resolvido, temos então as constantes c_1 e c_2 dadas por:

$$c_1 = \frac{y_1 t_2 - y_2}{t_1(t_2 - t_1)} \quad \text{e} \quad c_2 = \frac{y_2 - t_1 y_1}{t_2(t_2 - t_1)}.$$

Assim, basta mostrarmos que $y_n = c_1 t_1^n + c_2 t_2^n$ para todo n natural. Para isso considere a sequência $z_n = y_n - c_1 t_1^n - c_2 t_2^n$. Vamos mostrar que $z_n = 0$ para todo natural n. Substituindo essa sequência na expressão $x_{n+2} + p x_{n+1} + q x_n$ temos:

$$z_{n+2} + p z_{n+1} + q z_n = (y_{n+2} + p y_{n+1} + q y_n) - c_1 t_1^n (t_1^2 + p t_1 + q) - c_2 t_2^n (t_2^2 + p t_2 + q).$$

Por hipótese, $(y_{n+2} + p y_{n+1} + q y_n) = 0$ e pela Proposição 2.7, $t_1^2 + p t_1 + q = 0$ e $t_2^2 + p t_2 + q = 0$. Logo,

$$z_{n+2} + p z_{n+1} + q z_n = (0) - c_1 t_1^n (0) - c_2 t_2^n (0) = 0$$

além disso, como $y_1 = c_1 t_1 + c_2 t_2$ e $y_2 = c_1 t_1^2 + c_2 t_2^2$, temos:

$$z_1 = y_1 - c_1 t_1 - c_2 t_2 = c_1 t_1 + c_2 t_2 - c_1 t_1 - c_2 t_2 = 0$$
$$z_2 = y_2 - c_1 t_1^2 - c_2 t_2^2 = c_1 t_1^2 + c_2 t_2^2 - c_1 t_1^2 - c_2 t_2^2 = 0$$

e, dado que $z_{n+2} + p z_{n+1} + q z_n = 0$, então $z_n = 0$ para todo n natural. Isso só é possível caso $y_n = c_1 t_1^n + c_2 t_2^n$, como queríamos demonstrar. ■

Veremos como essas proposições se aplicam em um exemplo.

Exemplo 2.5: Determinar as soluções da recorrência $x_{n+2} + 5x_{n+1} + 6x_n = 0$.

A recorrência dada tem equação característica $t^2 + 5t + 6 = 0$, cujas raízes são -2 e -3. Utilizando as Proposições 2.7 e 2.8, as soluções da recorrência são as sequências da forma $a_n = c_1(-2)^n + c_2(-3)^n$, com c_1 e c_2 constantes arbitrárias.

Nesse exemplo, como não foram fornecidas condições iniciais para a sequência, não é possível encontrar os valores reais para c_1 e c_2.

2.5. FRAÇÕES CONTÍNUAS

Moreira (2011) explica que podemos utilizar a representação decimal para escrevermos números, sendo esses racionais ou não, através de frações contínuas.

Definição 2.6 (Frações Contínuas): Chamamos de fração contínua a expressão na forma:

$$c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{c_4 + \cfrac{1}{\ldots + \cfrac{1}{c_n}}}}}}$$

A qual será denotada por $[c_0, c_1, c_2, c_3, c_4, \ldots, c_n]$, cujos números $c_0, c_1, c_2, c_3, c_4, \ldots, c_n$ são denominados de quocientes parciais.

Sousa (2017) descreve dois métodos para a obtenção da fração contínua, um para representação de números racionais e outro para a representação de números irracionais.

Obtenção da fração contínua de um número racional: Dado um número racional $\frac{d_0}{d_1}$, com d_0 e d_1 primos entre si e, d_1 positivo, pelo Teorema 2.1 (Algoritmo da Divisão), conseguimos obter o quociente c_0 e o resto d_2, inteiros e com $0 \leq d_2 < d_1$. E assim, com o Teorema 2.5 (Algoritmo de Euclides), podemos repetir esse processo, realizando as divisões sucessivas e obtendo:

$$d_0 = d_1 c_0 + d_2, \;\; 0 \leq d_2 < d_1$$
$$d_1 = d_2 c_1 + d_3, \;\; 0 \leq d_3 < d_2$$
$$d_2 = d_3 c_2 + d_4, \;\; 0 \leq d_4 < d_3$$
$$\ldots$$
$$d_{n-1} = d_n c_{n-1} + d_{n+1}, \;\; 0 \leq d_{n+1} < d_n$$

$$d_n = d_{n+1}c_n.$$

Denominando $e_i = \frac{d_i}{d_{i+1}}$, com $0 \leq i \leq n$, note que:

$$d_i = d_{i+1}c_i + d_{i+2} \Rightarrow \frac{d_i}{d_{i+1}} = c_i + \frac{d_{i+2}}{d_{i+1}} \Rightarrow e_i = c_i + \frac{1}{e_{i+1}}, 0 \leq i \leq n-1$$

$$d_n = d_{n+1}c_n \Rightarrow \frac{d_n}{d_{n+1}} = c_n \Rightarrow e_n = c_n.$$

Assim, para $i = 0$ e $i = 1$, temos:

$$e_0 = c_0 + \frac{1}{e_1}$$

$$e_1 = c_1 + \frac{1}{e_2}$$

onde, substituindo a segunda equação na primeira, resulta em:

$$e_0 = c_0 + \frac{1}{c_1 + \frac{1}{e_2}}$$

no qual, repetindo sucessivas vezes esse processo, iremos obter:

$$e_0 = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{c_4 + \cfrac{1}{\ldots + \cfrac{1}{c_n}}}}}}$$

E por fim, lembrando que $e_i = \frac{d_i}{d_{i+1}}$, temos assim que $e_0 = \frac{d_0}{d_1}$, se tratando do número racional dado inicialmente. Com isso,

$$\frac{d_0}{d_1} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{c_4 + \cfrac{1}{\ldots + \cfrac{1}{c_n}}}}}}$$

Em outras palavras, através das divisões sucessivas e do Teorema 2.5 (Algoritmo de Euclides) podemos representar um número racional através da expansão em frações contínuas.

Exemplo 2.6: Escrever o número racional $\frac{67}{23}$ através de uma fração contínua.

Tomando inicialmente as divisões sucessivas para os inteiros 67 e 23:

$$67 = 2 \cdot \mathbf{23} + 21$$
$$23 = 1 \cdot \mathbf{21} + 2$$
$$21 = 10 \cdot \mathbf{2} + 1$$
$$2 = 2 \cdot \mathbf{1}$$

E assim, temos os valores em negrito de $c_0, c_1, c_2, e\ c_3$. Note que a fração também pode ser expressa da seguinte forma:

$$\frac{67}{23} = 2 + \frac{21}{23} = 2 + \frac{1}{\frac{23}{21}} = 2 + \frac{1}{1 + \frac{2}{21}} = 2 + \frac{1}{1 + \frac{1}{\frac{21}{2}}} = 2 + \frac{1}{1 + \frac{1}{10 + \frac{1}{2}}}$$

À última igualdade, chamamos de fração contínua referente ao número racional $\frac{67}{23}$ e a notação usada é $[2, 1, 10, 2]$.

Veremos como representar um número irracional por aproximações sucessivas de números racionais.

Obtenção da fração contínua de um número irracional: Dado o número irracional positivo α, considere $c_0 = \lfloor \alpha \rfloor$ como o maior inteiro menor do que α. Assim:

$$\alpha = c_0 + \frac{1}{d_0}$$

onde $\frac{1}{d_0}$ representa a diferença entre o número irracional α e $\lfloor \alpha \rfloor$ e assim $0 < \frac{1}{d_0} < 1$. Isolando d_0, temos:

$$d_0 = \frac{1}{\alpha - c_0}.$$

Como α é irracional, $\alpha - c_0$ também o será e consequentemente, d_0 também é irracional. Além disso, como $\frac{1}{d_0} < 1$, temos $d_0 > 1$, permitindo repetir o processo. Reescrevendo d_0 e tomando $c_1 = \lfloor d_0 \rfloor$ como o maior inteiro menor do que d_0, temos:

$$d_0 = c_1 + \frac{1}{d_1}.$$

Sendo $\frac{1}{d_1}$ a diferença entre o número irracional d_0 e $\lfloor d_0 \rfloor$, temos $0 < \frac{1}{d_1} < 1$. Assim, da mesma forma que d_0, teremos que d_1 também é irracional e maior que 1.

Seguindo este processo, é fácil perceber que cada elemento c_i é maior ou igual a 1 e cada elemento d_i é um irracional maior do que 1, permitindo repetir este método quantas vezes for necessário.

Continuando este processo, temos:

$$\alpha = c_0 + \frac{1}{d_0}$$

$$d_0 = c_1 + \frac{1}{d_1}$$

$$d_1 = c_2 + \frac{1}{d_2}$$

...

$$d_n = c_{n+1} + \frac{1}{d_{n+1}}.$$

Utilizando cada valor obtido de d_i na expressão dada por d_{i-1}, obtemos:

$$\alpha = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{c_4 + (\dots)}}}}$$

Conforme a Definição 2.6, denotaremos por $\alpha = [c_0, c_1, c_2, c_3, c_4, \dots]$. O processo se estende indefinidamente ou até que se observe a repetição dos quocientes, caracterizando um período. Nesse caso, chamamos essa representação de fração contínua periódica e colocamos uma barra sobre a parte do número que se repete, chamada de período da fração contínua. Supondo $c_1, c_2, c_3, \dots, c_k$ o período de α, podemos denotar como $\alpha = [c_0, \overline{c_1, c_2, c_{3,} \dots, c_k}]$.

Exemplo 2.7: Obter a expansão de $\sqrt{7}$.

Note que $c_0 = \lfloor\sqrt{7}\rfloor = 2$. Aplicando o método acima descrito, temos:

$$c_0 = \lfloor\sqrt{7}\rfloor = 2$$

$$d_0 = \frac{1}{\sqrt{7}-2} = \frac{\sqrt{7}+2}{3}$$

$$c_1 = \left\lfloor\frac{\sqrt{7}+2}{3}\right\rfloor = 1$$

$$d_1 = \frac{1}{\left(\frac{\sqrt{7}+2}{3}\right)-1} = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2}$$

$$c_2 = \left\lfloor\frac{\sqrt{7}+1}{2}\right\rfloor = 1$$

$$d_2 = \frac{1}{\left(\frac{\sqrt{7}+1}{2}\right)-1} = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3}$$

$$c_3 = \left\lfloor\frac{\sqrt{7}+1}{3}\right\rfloor = 1$$

$$d_3 = \frac{1}{\left(\frac{\sqrt{7}+1}{3}\right)-1} = \frac{3}{\sqrt{7}-2} = \sqrt{7}+2$$

$$c_4 = \lfloor\sqrt{7}+2\rfloor = 4$$

$$d_4 = \frac{1}{(\sqrt{7}+2)-4} = \frac{\sqrt{7}+2}{3}$$

Note que $d_4 = d_0$ e, consequentemente, $c_5 = c_1$, $c_6 = c_2$ e assim por diante.

Logo, o número $\sqrt{7}$ pode ser expresso por:

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots] = [2, \overline{1, 1, 1, 4}].$$

Nesse exemplo, como demonstram Martinez *et al* (2013), é possível perceber que mesmo o número sendo um irracional, ele admite uma representação periódica envolvendo frações contínuas.

3 EQUAÇÕES DE PELL

Estendendo a noção de equação diofantina, Neto (2016) detalha que uma equação diofantina se trata de uma equação polinomial

$$p(x_1, x_2, \dots, x_n) = 0$$

com n incógnitas e coeficientes inteiros no qual se buscam soluções que também são inteiras.

Em particular, Souza (2017) define as equações diofantinas quadráticas como equações algébricas em que o maior grau do expoente de cada variável envolvida é igual a dois e as soluções sejam números inteiros. Um dos exemplos mais conhecidos e trabalhados de uma equação diofantina quadrática é a busca de ternas pitagóricas, uma terna de números naturais (x, y, z) que satisfaz a relação:

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

Observe que esta equação também é conhecida por Teorema de Pitágoras, onde temos a associação dessa relação com os catetos e a hipotenusa de um triângulo retângulo. Alguns exemplos de ternas pitagóricas (x, y, z) são $(3, 4, 5)$ e $(5, 12, 13)$.

A equação de Pell se trata de um caso particular das equações diofantinas quadráticas definidas por:

$$x^2 - Ay^2 = m$$

desde que A seja um número inteiro positivo e não seja um quadrado perfeito.

Em particular, como o foco do trabalho é estudar aproximações para raízes quadradas, iremos estudar as equações do tipo:

$$x^2 - Ay^2 = 1. \tag{3.1}$$

Como destacam Martinez *et al* (2013), pode surgir o questionamento da existência de uma teoria mais geral que possibilite não só estudar as equações de Pell como também das equações diofantinas quadráticas. Ainda segundo os autores, este é essencialmente o décimo problema de Hilbert, no qual pergunta ser

possível determinar um processo que determine as soluções inteiras de uma equação diofantina qualquer. Neste caso, considera-se que o problema foi resolvido por Martin Davis, Yuri Matiyasevich, Hilary Putnam e Julia Robinson, ao terem demonstrado não existir um algoritmo capaz de estimar se uma equação diofantina qualquer admite soluções inteiras. Dessa forma, estudamos situações e condições particulares, como as da Equação de Pell.

Como afirma Weiss (2007), Joseph-Louis Lagrange (1736-1813), em 1766, mostrou que a Equação (3.1) apresenta um número infinito de soluções inteiras. Porém, caso A fosse um quadrado perfeito, teríamos uma fatoração que envolveria números inteiros, possuindo, assim, um número limitado de soluções.

Exemplo 3.1: Resolver a equação $x^2 - 25y^2 = 1$.

Note que:

$$x^2 - 25y^2 = (x - 5y)(x + 5y) = 1.$$

Como queremos obter x e y inteiros, então as expressões $x - 5y$ e $x + 5y$ também representam números inteiros, e isso só é possível nos casos abaixo:

$$\begin{cases} x - 5y = 1 \\ x + 5y = 1 \end{cases} \text{ ou } \begin{cases} x - 5y = -1 \\ x + 5y = -1 \end{cases}$$

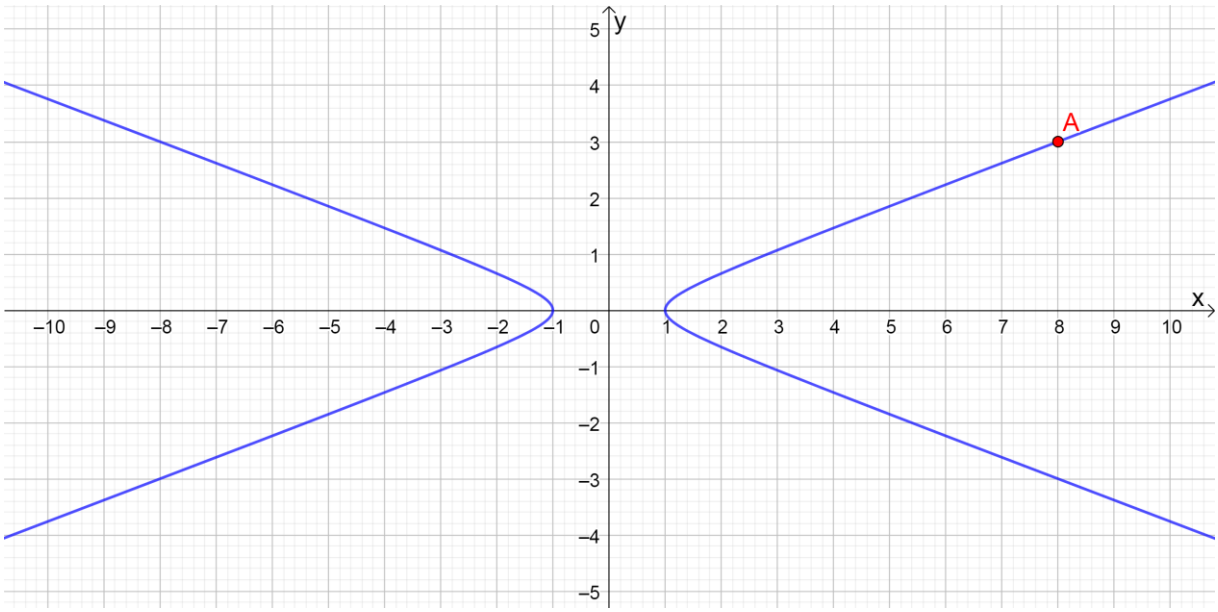
cujas soluções são $(1, 0)$ e $(-1, 0)$.

Embora a equação possua soluções, como A é um quadrado perfeito, não temos uma Equação de Pell.

Voltando às equações de Pell, geometricamente esse tipo de equação polinomial pode ser representado no plano cartesiano, em $\mathbb{R}^2$, através de uma hipérbole, conforme podemos observar no gráfico da equação $x^2 - 7y^2 = 1$ da Figura 3.1, obtida com o auxílio do *software* GeoGebra.

Porém, como a Equação de Pell busca soluções inteiras, estamos interessados em obter somente pontos no gráfico que possuem coordenadas inteiras.

Figura 3.1 - Ramos da hipérbole $x^2 - 7y^2 = 1$.



Fonte: Próprio autor.

Na Figura 3.1, as soluções da Equação de Pell são os pares ordenados (x, y), com x e y inteiros, que pertencem à hipérbole. Note que podemos buscar as soluções utilizando a representação da equação no gráfico. Ao analisar a hipérbole, encontramos o ponto de coordenadas inteiras $(8, 3)$, que de fato é solução da equação, pois $8^2 - 7 \cdot 3^2 = 1$.

Generalizando, as equações quadráticas com duas incógnitas podem ser expressas pela equação:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \qquad (3.2)$$

nas quais, como afirmam Delgado, Frensel e Crissaff (2017), são representadas geometricamente por cônicas.

Andreescu e Andrica (2002) detalham que a curva representada pela equação (3.2) pode ser classificada em função do discriminante $\Delta = b^2 - 4ac$, de modo que ela será uma hipérbole, parábola ou elipse (ou nos seus casos degenerados), caso o discriminante seja positivo, nulo ou negativo, respectivamente.

No nosso estudo, os casos mais interessantes são quando $\Delta > 0$, ou seja, hipérboles descritas por equações que podem ser reduzidas à equação de Pell através de uma mudança de variáveis envolvendo fatoração. Por exemplo, a equação quadrática:

$$6x^2 - 14xy + 7y^2 + 1 = 0 \tag{3.3}$$

pode ser fatorada por:

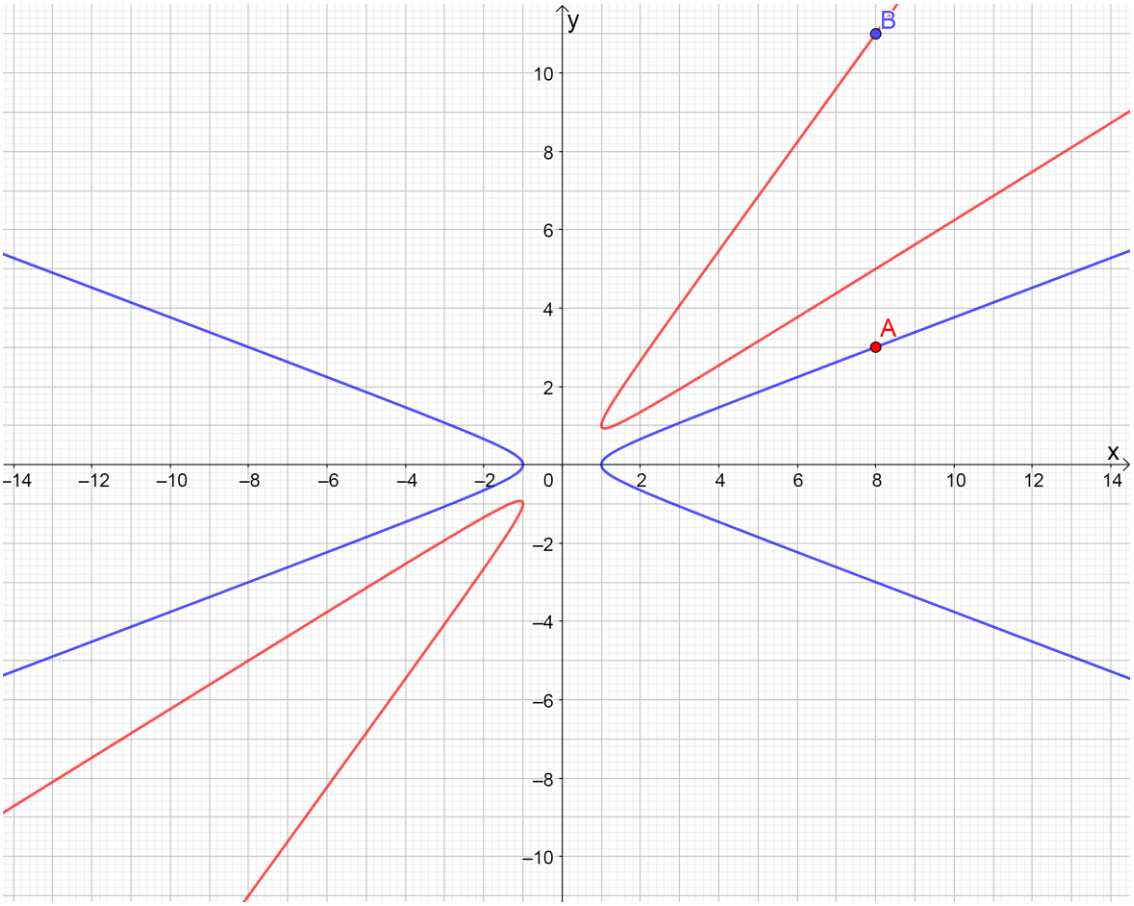
$$-6x^2 + 14xy - 7y^2 - 1 = 0$$
$$x^2 - 7x^2 + 14xy - 7y^2 = 1$$
$$x^2 - 7(y - x)^2 = 1.$$

De modo a ter uma equação polinomial que pode ser interpretada como a equação de Pell, utilizamos as substituições $X = x$ e $Y = y - x$, obtendo:

$$X^2 - 7Y^2 = 1.$$

Na Figura 3.2 temos a representação da equação $6x^2 - 14xy + 7y^2 + 1 = 0$, curva em vermelho e, em azul a transformação da equação (3.3) na equação $X^2 - 7Y^2 = 1$, ambas com domínios reais.

Figura 3.2 - Equação (3.3), em vermelho, e sua equivalente
na forma da equação de Pell, em azul.



Fonte: Próprio autor

É possível observar a alteração das soluções inteiras da equação (3.3) devido as substituições realizadas. No exemplo, o ponto original $B = (8, 11)$ foi transladado para o ponto $A = (8, 3)$ da equação de Pell.

Note que devido as substituições realizadas, o valor de X se mantém enquanto o valor de Y passa a ser a diferença entre as variáveis originais.

3.1. RESOLVENDO A EQUAÇÃO DE PELL

Dada a equação $x^2 - Ay^2 = 1$, em que A é um número inteiro positivo e desde que não seja um quadrado perfeito, o par ordenado $(1, 0)$ é chamado de solução trivial, pois toda equação de Pell da forma $x^2 - Ay^2 = 1$ apresenta $(1, 0)$ como solução.

Neste contexto, embora estejamos interessados apenas em inteiros positivos devido às aproximações racionais das raízes quadradas, cabe ressaltar que caso (x, y) seja solução da equação $x^2 - Ay^2 = 1$, como trabalhamos com x^2 e y^2, números sempre positivos, então os pares $(x, -y)$, $(-x, y)$, $(-x, -y)$ também são soluções da equação de Pell.

Segundo Andreescu e Andrica (2002), além da solução trivial, a equação de Pell $x^2 - Ay^2 = 1$ possui infinitas outras soluções, cuja solução geral será dada por:

$$\begin{aligned} x_{n+1} &= x_1 x_n + A y_1 y_n \\ y_{n+1} &= y_1 x_n + x_1 y_n \end{aligned} \tag{3.4}$$

onde (x_1, y_1) é uma solução fundamental (ou minimal), ou seja, uma solução mínima diferente de $(1, 0)$.

Precisamos assim, além de verificar que as soluções serão dadas por essas recorrências, obter um método para encontrar a solução minimal, pois, a partir dessa, conseguimos aplicar a recorrência (3.4) para obter as demais soluções.

Para provarmos que a solução geral será dada pela Equação (3.4), utilizaremos a proposição dada por Pereira (2014), onde consiste em encontrar uma segunda recorrência que também satisfaz a equação de Pell.

Proposição 3.1: Dada a equação de Pell $x^2 - Ay^2 = 1$, na qual a solução é dada pelo par ordenado (x_n, y_n) e satisfaz a Equação (3.4):

$$\begin{aligned} x_{n+1} &= x_1 x_n + A y_1 y_n \\ y_{n+1} &= y_1 x_n + x_1 y_n \end{aligned}$$

em que (x_1, y_1) é a solução minimal da equação dada. Então, para todo n inteiro positivo, o par ordenado (x_n, y_n) satisfaz as recorrências dadas por:

$$x_n = 2x_1 \cdot x_{n-1} - x_{n-2}$$
$$y_n = 2x_1 \cdot y_{n-1} - y_{n-2}$$

Demonstração: Inicialmente, note que dados os pares (x_1, y_1) e (x_n, y_n), temos:

$$x_{n+1} = x_1x_n + Ay_1y_n \Rightarrow Ay_1y_n = x_{n+1} - x_1x_n.$$

Observe também que dados (x_1, y_1) e (x_{n+1}, y_{n+1}) temos:

$$x_{n+2} = x_1 \cdot x_{n+1} + Ay_1 \cdot y_{n+1}.$$

Substituindo $y_{n+1} = y_1x_n + x_1y_n$, na equação acima temos:

$$x_{n+2} = x_1 \cdot x_{n+1} + Ay_1(y_1x_n + y_nx_1) = x_1 \cdot x_{n+1} + A{y_1}^2x_n + x_1(Ay_1y_n).$$

Considerando $Ay_1y_n = x_{n+1} - x_1x_n$, temos:

$$\begin{aligned} x_{n+2} &= x_1 \cdot x_{n+1} + A{y_1}^2x_n + x_1(x_{n+1} - x_1x_n) \\ &= x_1 \cdot x_{n+1} + A{y_1}^2x_n + x_1 \cdot x_{n+1} - (x_1)^2x_n \\ &= 2x_1 \cdot x_{n+1} - ((x_1)^2 - A(y_1)^2)x_n. \end{aligned}$$

E como (x_1, y_1) é solução da equação de Pell, $(x_1)^2 - A(y_1)^2 = 1$. Assim,

$$x_{n+2} = 2x_1 \cdot x_{n+1} - x_n.$$

Além disso, temos também:

$$y_{n+2} = y_1 \cdot x_{n+1} + x_1 \cdot y_{n+1}.$$

E dado $x_{n+1} = x_1x_n + Ay_1y_n$, substituindo obtemos:

$$y_{n+2} = y_1(x_1x_n + Ay_1y_n) + x_1 \cdot y_{n+1} = x_1(y_1x_n) + A{y_1}^2y_n + x_1 \cdot y_{n+1}.$$

Como pela hipótese, temos $y_{n+1} = y_1x_n + x_1y_n$, logo $y_1x_n = y_{n+1} - x_1y_n$. Assim, substituindo na expressão acima, temos:

$$\begin{aligned} y_{n+2} &= x_1(y_{n+1} - x_1y_n) + A{y_1}^2y_n + x_1 \cdot y_{n+1} \\ &= x_1 \cdot y_{n+1} - (x_1)^2y_n + A{y_1}^2y_n + x_1 \cdot y_{n+1} \\ &= 2x_1 \cdot y_{n+1} - ((x_1)^2 - A(y_1)^2)y_n. \end{aligned}$$

Onde, novamente temos $(x_1)^2 - A(y_1)^2 = 1$, resultando em:

$$y_{n+2} = 2x_1 \cdot y_{n+1} - y_n.$$

■

Mostraremos agora que os elementos dessas novas recorrências são de fato soluções da equação de Pell.

Proposição 3.2: Sejam (x_1, y_1) a solução minimal da equação $x^2 - Ay^2 = 1$ e a solução trivial $(1,0)$. Dados as sequências definidas por $a_n = 2x_1 \cdot a_{n-1} - a_{n-2}$ e $b_n = 2x_1 \cdot b_{n-1} - b_{n-2}$, com $n \geq 2$, e $(a_0, b_0) = (1, 0)$ e $(a_1, b_1) = (x_1, y_1)$, então o par ordenado (a_n, b_n) é solução da equação de Pell para todo número natural.

Demonstração: As sequências $a_n = 2x_1 \cdot a_{n-1} - a_{n-2}$ e $b_n = 2x_1 \cdot b_{n-1} - b_{n-2}$ têm equação característica dada por $t^2 - 2x_1 \cdot t + 1 = 0$, na qual resolvendo, obtemos:

$$\Delta = 4(x_1)^2 - 4$$
$$t = \frac{2x_1 \pm 2\sqrt{(x_1)^2 - 1}}{2}$$

cujas raízes são dadas por $t_1 = x_1 + \sqrt{(x_1)^2 - 1}$ e $t_2 = x_1 - \sqrt{(x_1)^2 - 1}$.

Como (x_1, y_1) é a solução minimal da equação, então ${x_1}^2 - A{y_1}^2 = 1$. Rearranjando, temos ${x_1}^2 - 1 = A{y_1}^2$.

Reescrevendo as raízes t_1 e t_2, obtemos $t_1 = x_1 + y_1\sqrt{A}$ e $t_2 = x_1 - y_1\sqrt{A}$.

Pela Proposição 2.7, temos que as soluções da recorrência são $a_n = c_1 \cdot t_1^n + c_2 \cdot t_2^n$ e $b_n = c_3 \cdot t_1^n + c_4 \cdot t_2^n$.

Lembrando que $(a_0, b_0) = (1, 0)$ e $(a_1, b_1) = (x_1, y_1)$, temos para c_1 e c_2 o sistema:

$$\begin{cases} c_1 + c_2 = 1 \\ c_1\left(x_1 + y_1\sqrt{A}\right) + c_2\left(x_1 - y_1\sqrt{A}\right) = x_1 \end{cases}.$$

Desenvolvendo a segunda informação desse sistema, temos:

$$c_1x_1 + c_1y_1\sqrt{A} + c_2x_1 - c_2y_1\sqrt{A} = x_1 \Rightarrow$$
$$(c_1 + c_2)x_1 + \left(c_1y_1\sqrt{A} - c_2y_1\sqrt{A}\right) = x_1.$$

Onde, através da igualdade de polinômios, resulta em $c_1 y_1\sqrt{A} - c_2 y_1\sqrt{A} = 0$, resultando em $c_1 = c_2$. Retornando ao sistema, obtemos $c_1 = c_2 = \frac{1}{2}$, fazendo que a solução da recorrência seja escrita como:

$$a_n = \frac{1}{2}\left[\left(x_1 + y_1\sqrt{A}\right)^n + \left(x_1 - y_1\sqrt{A}\right)^n\right] \tag{3.5}$$

Da mesma forma, temos para c_3 e c_4 o sistema:

$$\begin{cases} c_3 + c_4 = 0 \\ c_3\left(x_1 + y_1\sqrt{A}\right) + c_4\left(x_1 - y_1\sqrt{A}\right) = y_1 \end{cases}.$$

Onde, repetindo o processo realizado no primeiro sistema, iremos desenvolver a segunda informação desse sistema:

$$\begin{aligned} &c_3 x_1 + c_3 y_1\sqrt{A} + c_4 x_1 - c_4 y_1\sqrt{A} = y_1 \Rightarrow \\ &(c_3 + c_4)x_1 + \left(c_3\sqrt{A} - c_4\sqrt{A}\right)y_1 = y_1 . \end{aligned}$$

Onde, através da igualdade de polinômios, resulta em $c_3\sqrt{A} - c_4\sqrt{A} = 1$. Lembrando que $c_3 + c_4 = 0$, logo $c_3 = -c_4$, resultando em:

$$c_3\sqrt{A} - c_4\sqrt{A} = 1 \Rightarrow 2c_3\sqrt{A} = 1$$

Do qual obtemos $c_3 = \frac{1}{2\sqrt{A}}$ e $c_4 = -\frac{1}{2\sqrt{A}}$. Assim, a solução da recorrência é dada por:

$$b_n = \frac{1}{2\sqrt{A}}\left[\left(x_1 + y_1\sqrt{A}\right)^n - \left(x_1 - y_1\sqrt{A}\right)^n\right] \tag{3.6}$$

Falta agora mostrar que o par ordenado (a_n, b_n) é solução da equação de Pell para todo n natural.

Através de (3.5) e (3.6), obtemos:

$$\begin{cases} 2a_n = \left(x_1 + y_1\sqrt{A}\right)^n + \left(x_1 - y_1\sqrt{A}\right)^n \\ 2b_n\sqrt{A} = \left(x_1 + y_1\sqrt{A}\right)^n - \left(x_1 - y_1\sqrt{A}\right)^n \end{cases} \tag{3.7}$$

Montaremos um novo sistema, no qual a primeira informação será obtida pela soma das informações do sistema dado em (3.7) e a segunda informação será resultado da subtração das informações do sistema (3.7). Assim:

$$\begin{cases} 2a_n + 2b_n\sqrt{A} = 2\left(x_1 + y_1\sqrt{A}\right)^n \\ 2a_n - 2b_n\sqrt{A} = 2\left(x_1 - y_1\sqrt{A}\right)^n \end{cases}$$

Ao dividirmos ambas as expressões por 2 e multiplicarmos entre si, obtemos:

$$\left(a_n + b_n\sqrt{A}\right)\left(a_n - b_n\sqrt{A}\right) = \left(x_1 + y_1\sqrt{A}\right)^n\left(x_1 - y_1\sqrt{A}\right)^n \Rightarrow$$
$$\Rightarrow (a_n)^2 - A(b_n)^2 = [(x_1)^2 - A(y_1)^2]^n = 1$$

sendo isso que queríamos demonstrar. ■

Deste modo, caso a equação possua a solução minimal e satisfaça as restrições estabelecidas para o valor de A, a equação possuirá infinitas soluções. A proposição também fornece uma fórmula para obter essas soluções, dadas pelas equações (3.5) e (3.6).

Portanto, para resolver a equação de Pell basta obter a solução minimal.

O método para a obtenção da solução minimal utiliza as ideias contidas nos trabalhos de Neto (2016) e Moreira (2011).

3.1.1. OBTENÇÃO DA SOLUÇÃO MINIMAL

Considere o número irracional $\sqrt{A}$ cuja expansão é dada pela fração contínua:

$$\sqrt{A} = c_0 + \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{c_3 + \cfrac{1}{c_4 + (\dots)}}}}$$

ou seja, $\sqrt{A} = [c_0, c_1, c_2, c_3, c_4, \dots]$, na qual $c_0 = \lfloor\sqrt{A}\rfloor$ e $c_1, c_2, c_3, c_4, \dots$ é uma sequência de números positivos inteiros. Sendo $c_1, c_2, c_3, \dots, c_k$ o período de $\sqrt{A}$, a solução minimal da equação de Pell $x^2 - Ay^2 = 1$ será dada por:

$$(x_1, y_1) = \begin{cases} (r_{k-1}, s_{k-1}), & \text{se } k \text{ é par} \\ (r_{2k-1}, s_{2k-1}), & \text{se } k \text{ é ímpar} \end{cases} \tag{3.8}$$

em que:

$$\frac{r_k}{s_k} = [c_0, c_1, c_2, c_3, \dots, c_k]$$

sendo r_k e s_k primos entre si.

Veremos como esse método se aplica num exemplo.

Exemplo 3.2: Resolver a equação de Pell $x^2 - 7y^2 = 1$.

O primeiro passo consiste em obter a solução minimal da equação dada. Como visto no Exemplo 2.7, o número $\sqrt{7}$ pode ser expresso por:

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots] = [2, \overline{1, 1, 1, 4}]$$

cujo período é $k = 4$. Utilizando (3.8), temos $(r_{k-1}, s_{k-1}) = (r_3, s_3)$, sendo possível calcular a fração:

$$\frac{r_3}{s_3} = [c_0, c_1, c_2, c_3] = [2, 1, 1, 1] = 2 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1}}} = \frac{8}{3}\ .$$

E como $(r_{k-1}, s_{k-1}) = (x_1, y_1)$, a solução minimal é dada pelo ponto $(8, 3)$. De fato, temos $8^2 - 7 \cdot 9 = 1$. Além disso, pelas fórmulas dadas em (3.5) e (3.6), temos:

$$a_n = \frac{1}{2}\left[\left(x_1 + y_1\sqrt{A}\right)^n + \left(x_1 - y_1\sqrt{A}\right)^n\right] = \frac{1}{2}\left[\left(8 + 3\sqrt{7}\right)^n + \left(8 - 3\sqrt{7}\right)^n\right]$$

$$b_n = \frac{1}{2\sqrt{A}}\left[\left(x_1 + y_1\sqrt{A}\right)^n - \left(x_1 - y_1\sqrt{A}\right)^n\right] = \frac{1}{2\sqrt{7}}\left[\left(8 + 3\sqrt{7}\right)^n - \left(8 - 3\sqrt{7}\right)^n\right]$$

Podemos também utilizar as fórmulas de recorrência dadas em (3.4):

$$x_{n+1} = x_1 x_n + A y_1 y_n = 8x_n + 21y_n$$

$$y_{n+1} = y_1 x_n + x_1 y_n = 3x_n + 8y_n$$

Ao variar o valor de n, encontramos as soluções $(x_2, y_2) = (127, 48)$, $(x_3, y_3) = (2024, 765)$ e assim por diante.

Uma outra demonstração deste método, originalmente atribuída a Lagrange, utiliza os conceitos de recorrência, frações contínuas e congruências e, caso o leitor tenha interesse de saber o passo a passo dessa demonstração, recomendamos a leitura dos livros de Andreescu e Andrica (2002) e Martinez *et al* (2013).

3.2. A EQUAÇÃO DE PELL E A APROXIMAÇÃO DE RAÍZES QUADRADAS

Como vimos na Introdução, historicamente as equações de Pell foram utilizadas como uma forma de obter aproximações de raízes irracionais. Baudhayana, citado na introdução desse texto, não foi o único a tratar desse problema. Neto (2016) relata que Theon de Smyrna (70-135) aproximou o valor de $\sqrt{2}$ através das soluções inteiras da equação $x^2 - 2y^2 = 1$.

Ainda segundo Neto (2016), no século VII, Brahmagupta encontrou a solução $(1151, 120)$ para a equação $x^2 - 92y^2 = 1$, obtendo assim uma aproximação para $\sqrt{92}$. Bhaskara II, no século XII, encontrou a menor solução da equação $x^2 - 61y^2 = 1$, que é $(1766319049, 226153980)$.

Como é possível perceber, a tentativa em obter aproximações racionais de números irracionais a partir das equações na forma $x^2 - Ay^2 = 1$ tem motivado matemáticos ao longo de séculos.

Andreescu e Andrica (2002) relatam que as soluções da equação de Pell apresentadas em (3.5) e (3.6) podem ser usadas na aproximação das raízes quadradas de números inteiros positivos que não são quadrados perfeitos.

De fato, dado (x_n, y_n) uma solução não trivial da equação $x^2 - Ay^2 = 1$, temos:

$$x_n^2 - Ay_n^2 = 1 \Rightarrow (x_n - y_n\sqrt{A})(x_n + y_n\sqrt{A}) = 1 \Rightarrow x_n - y_n\sqrt{A} = \frac{1}{x_n + y_n\sqrt{A}} .$$

E assim, como $y_n \neq 0$, dividindo a última equação por y_n resulta em:

$$\frac{x_n}{y_n} - \sqrt{A} = \frac{1}{y_n\left(x_n + y_n\sqrt{A}\right)} .$$

De onde, temos:

$$\frac{1}{y_n\left(x_n + y_n\sqrt{A}\right)} < \frac{1}{y_n^2\sqrt{A}} < \frac{1}{y_n^2}.$$

E assim,

$$\frac{x_n}{y_n} - \sqrt{A} < \frac{1}{y_n^2}. \tag{3.9}$$

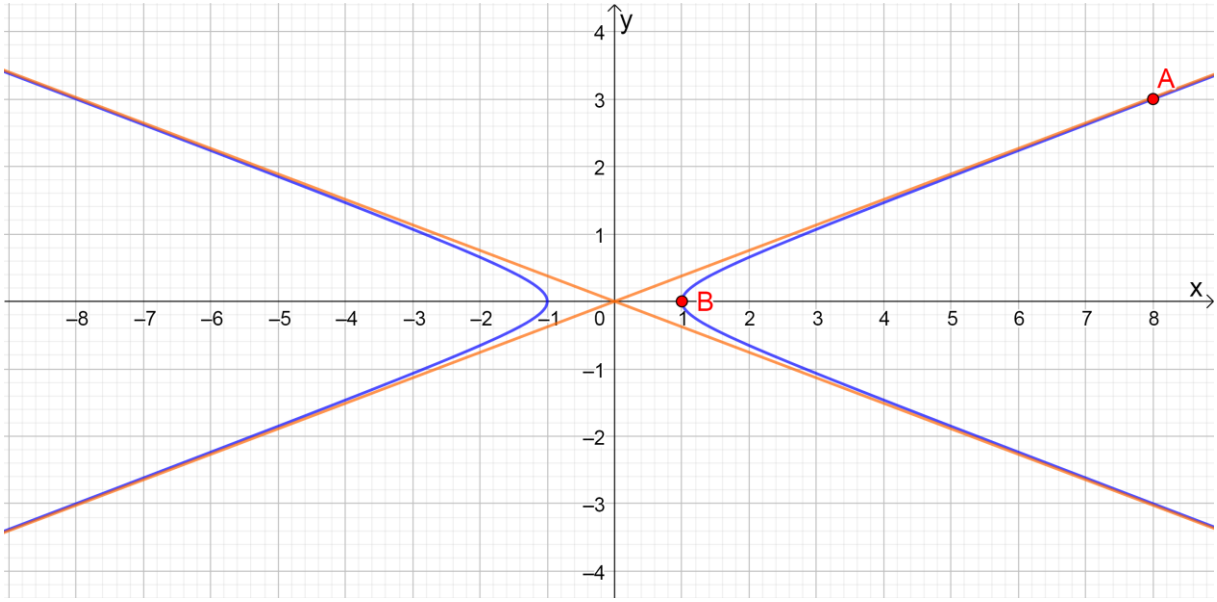
Isso mostra que, na medida que aumenta o valor de y_n, temos $\frac{1}{y_n^2}$ se aproximando de zero, de onde, por (3.9), temos $\frac{x_n}{y_n} - \sqrt{A}$ também se aproximando de zero. Assim, a fração $\frac{x_n}{y_n}$ aproxima o valor de $\sqrt{A}$ com um erro da ordem de $\frac{1}{y_n^2}$.

Retomando o Exemplo 3.2, a solução minimal da equação $x^2 - 7y^2 = 1$ é $(8, 3)$. Para efeito de comparação, considere $\sqrt{7} \cong 2{,}64575131$, enquanto que $\frac{8}{3} \cong 2{,}66666667$. Essa aproximação possui um erro percentual de $0{,}76\%$.

Entretanto, ao aplicar as equações dadas em (3.4), obtemos outras soluções dadas a partir da solução minimal. A terceira solução $(x_3, y_3) = (2024, 765)$ aproxima $\sqrt{7}$ pela fração $\frac{2024}{765} \cong 2{,}64575163$, no qual comparado com o valor esperado possui um erro percentual de $0{,}000012\%$, apresentando uma precisão de 6 casas decimais.

Agora faremos a análise geométrica da equação $x^2 - 7y^2 = 1$. Na Figura 3.3 são mostradas as soluções inteiras positivas $A = (8, 3)$ e $B = (1, 0)$, pertencentes à hipérbole dada por $x^2 - 7y^2 = 1$, e também suas assíntotas, representadas pelas retas $x \pm y\sqrt{7} = 0$.

Figura 3.3 - Gráfico da hipérbole $x^2 - 7y^2 = 1$ e de suas assíntotas.



Fonte: Próprio autor.

Neste ponto vale ressaltar que o coeficiente angular das assíntotas são equivalentes ao valor exato de $\sqrt{7}$ e, conforme os valores de n crescem, o quociente $\frac{x_n}{y_n}$ tende ao valor de $\sqrt{A}$ na equação $x^2 - 7y^2 = 1$, o que corrobora com o fato da precisão da aproximação melhorar com o aumento do valor de y_n.

Exemplo 3.3: Considere agora a equação $x^2 - 61y^2 = 1$, que apresenta solução minimal dada por $(1766319049, 226153980)$, cuja primeira solução possui um valor cujo erro absoluto é da ordem de 10^{-18}, apresentando uma excelente aproximação para $\sqrt{61}$.

Entretanto, pelos valores de x e y serem grandes, pode-se perceber, neste caso, que a dificuldade em se aproximar a $\sqrt{61}$ é devido ao trabalho que se leva para calcular a solução minimal através de frações contínuas. Nesse sentido, Andreescu e Andrica (2002) construíram uma tabela apresentando as soluções minimais da equação de Pell $x^2 - Ay^2 = 1$ para os valores de A variando de 2 a 103.

O Quadro 3.1 apresenta uma versão resumida dessa tabela, contendo apenas números primos para o valor de A (excluindo aqueles que são quadrados perfeitos) entre 2 e 103.

Quadro 3.1 - Soluções minimais para primos entre $2 \leq A \leq 103$.

A	x_n	y_n	A	x_n	y_n	A	x_n	y_n
2	3	2	*29*	9801	1820	*67*	48842	5967
3	2	1	*31*	1520	273	*71*	3480	413
5	9	4	*37*	73	12	*73*	2281249	267000
7	8	3	*41*	2049	320	*79*	80	9
11	10	3	*43*	3482	531	*83*	82	9
13	649	189	*47*	48	7	*89*	500001	53000
17	33	8	*53*	66249	9100	*97*	62809633	6377352
19	170	39	*59*	530	69	*101*	201	20
23	24	5	*61*	1766319049	226153980	*103*	227528	22419

Fonte: Adaptado de Andreescu e Andrica (2002).

Nesse ponto, é interessante fazer uma observação referente aos dados contidos no Quadro 3.1, na qual buscamos representar apenas os números primos entre 2 e 103, pois é possível obter qualquer outro resultado a partir dos contidos na tabela, uma vez que, obter a aproximação da $\sqrt{AB}$ através da equação $x^2 - ABy^2 = 1$ pode ser feita através das equações de Pell $x^2 - Ay^2 = 1$ e $x^2 - By^2 = 1$, que fornecerá as aproximações de $\sqrt{A}$ e $\sqrt{B}$, e depois bastando calcular $\sqrt{A} \cdot \sqrt{B}$.

Entretanto, caso não tenhamos acesso ou conhecimento da solução minimal, realizar este procedimento não necessariamente resultará em obter a solução mais rapidamente, já que a fração contínua obtida para a solução é diretamente relacionada com os números envolvidos na solução minimal. Por exemplo, caso estivéssemos interessados em resolver diretamente a equação $x^2 - 35y^2 = 1$, cuja solução minimal é $(6, 1)$, o processo é mais rápido do que resolver separadamente as equações $x^2 - 5y^2 = 1$ e $x^2 - 7y^2 = 1$, cuja soluções minimais são dadas respectivamente por $(9, 4)$ e $(8, 3)$.

Retomando às soluções minimais constantes no Quadro 3.1, através do *software* MATLAB (ver Anexo) foi implementada numericamente a Equação (3.4), permitindo calcular as iterações (x_n, y_n) da equação de Pell $x^2 - Ay^2 = 1$, de forma a obter uma aproximação para $\sqrt{A}$ com uma precisão de 9 casas decimais. Os resultados são mostrados no Quadro 3.2.

Quadro 3.2 - Número n de iterações para a aproximação de $\sqrt{A}$ com precisão de 9 casas decimais.

A	*Iterações necessárias*	*A*	*Iterações necessárias*	*A*	*Iterações necessárias*
2	7	*29*	2	*67*	2
3	9	*31*	2	*71*	2
5	4	*37*	3	*73*	1
7	5	*41*	2	*79*	3
11	4	*43*	2	*83*	3
13	2	*47*	3	*89*	1
17	3	*53*	1	*97*	1
19	3	*59*	2	*101*	2
23	4	*61*	1	*103*	1

Fonte: próprio autor.

Os valores do Quadro 3.2 indicam que são necessárias poucas iterações para se obter uma aproximação para $\sqrt{A}$, ilustrando o que foi discutido na Equação (3.9) sobre a influência dos valores de y_n (presente no Quadro 3.1) para o cálculo do erro.

Porém, como obter valores muito grandes para x e y pode ser trabalhoso sem a utilização do Quadro 3.1, o próximo capítulo faz um estudo numérico das soluções desta equação com três métodos de zeros de funções, a saber: o Método da Bissecção, o Método de Newton e o Método da Secante. Esses métodos serão aplicados para criar um comparativo entre o número de iterações necessários por cada um desses métodos numéricos com os da Equação de Pell, mostrados no Quadro 3.2.

4 APROXIMAÇÃO DE RAÍZES POR MÉTODOS NUMÉRICOS

Existem diferentes métodos para obtenção da raiz quadrada de um número estudados na Educação Básica e também no Ensino Superior. Na Educação Básica este tema é tratado basicamente por estimativas através de quadrados de números decimais cujo resultado seja próximo do valor desejado. No Ensino Superior, a aproximação de raízes quadradas, ou de outras ordens, são comumente trabalhadas em disciplinas sobre cálculo numérico, e estudadas via métodos de zeros de funções. Entretanto estes métodos envolvem conceitos não comumente abordados no Ensino Básico.

De um modo geral, um método de zero de função consiste em resolver a equação $f(x) = 0$, ou seja, determinar os valores de x onde sua imagem, através da função contínua f, seja nula.

Veremos um pouco mais sobre os principais métodos para obtenção de zeros de funções, em específico, os métodos de Newton, da secante e da bissecção. Para esta seção, utilizamos os conceitos definidos por Burden e Faires (2013).

4.1. MÉTODO DA BISSECÇÃO

O método da bissecção, cujo nome significa dividir, baseia-se no Teorema do Valor Intermediário, que iremos enunciar sem demonstrar. Caso o leitor tenha interesse em sua demonstração, recomendamos a leitura de Neto (2015).

Teorema 4.1 (Teorema do Valor Intermediário): Dado uma função contínua f definida em um intervalo fechado $[a, b]$ com $f(a)$ e $f(b)$ de sinais opostos, então existe um número p em $]a, b[$ tal que $f(p) = 0$.

Dado uma função f que satisfaz o Teorema 4.1, o método consiste em realizar repetidas divisões a partir do intervalo inicial $[a, b]$, reduzindo cada novo intervalo na metade do tamanho do intervalo anterior e identificando a cada passo qual desses intervalos contém o número p.

Para o processo, considere $a_1 = a$, $b_1 = b$ e p_1 o ponto médio de $[a, b]$, no caso:

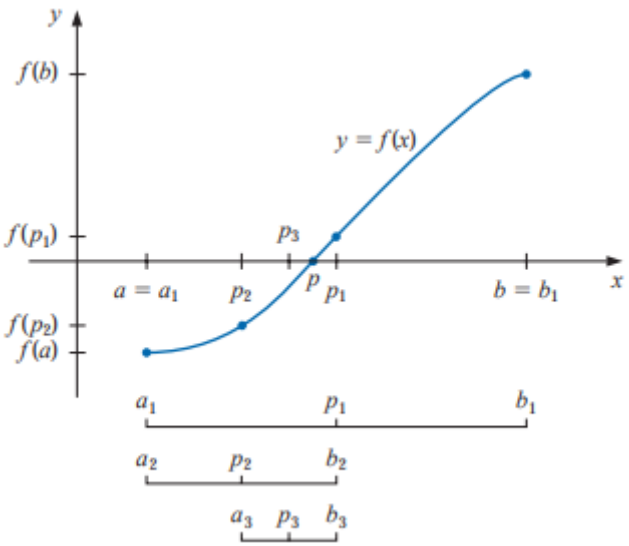
$$p_1 = \frac{a_1 + b_1}{2}$$

Caso $f(p_1) = 0$, o problema está resolvido, caso contrário, observamos se $f(p_1)$ tem o mesmo sinal de $f(a_1)$ ou de $f(b_1)$.

Se, por exemplo, $f(p_1)$ e $f(a_1)$ têm o mesmo sinal, então p pertence ao intervalo $[p_1, b_1]$. A partir disso renomeamos os extremos do intervalo para obter $[a_2, b_2]$, definimos p_2 como o ponto médio de $[a_2, b_2]$ e repetimos esse método. Porém, caso $f(p_1)$ e $f(b_1)$ tenham o mesmo sinal, então p pertence ao intervalo $[a_1, p_1]$, a partir do qual o processo é análogo ao descrito para $p \in [p_1, b_1]$.

A Figura 4.1 ilustra a aplicabilidade do método e a sucessão de subdivisões do intervalo que contém o valor p, tal que $f(p) = 0$.

Figura 4.1 - Método da bissecção.



Fonte: Burden e Faires (2013).

4.2. MÉTODO DE NEWTON

O método de Newton, também conhecido como método de Newton-Raphson, é considerado por Burden e Faires (2013) como um dos métodos mais conhecidos para a solução de um problema de zero de função.

Antes de descrevermos o método, faz-se necessário definirmos os polinômios de Taylor, cuja demonstração pode ser encontrada em Neto (2015).

Teorema 4.2 (Teorema de Taylor): Considere uma função f contínua em um intervalo $[a, b]$ e que possua derivada de ordem n também contínua em $[a, b]$. Considere ainda que $f^{(n+1)}$ exista em $[a, b]$ e que $x_0 \in [a, b]$. Para todo $x \in [a, b]$, então existe um número $\xi(p)$ entre x_0 e x tal que

$$f(x) = P_n(x) + R_n(x)$$

onde $P_n(x)$ é chamado de polinômio de Taylor de grau n de f em x_0 e é dado por

$$P_n(x) = f(x_0) + f'(x_0)(x - x_0) + f"(x_0)\frac{(x - x_0)^2}{2!} + \cdots + f^{(n)}(x_0)\frac{(x - x_0)^n}{n!}$$

e $R_n(x)$ é o resto relativo a $P_n(x)$, sendo igual a

$$R_n(x) = f^{(n+1)}\big(\xi(p)\big)\frac{(x - x_0)^{n+1}}{(n+1)!}.$$

Com isso definido, podemos voltar ao método de Newton.

Considere uma função contínua f definida em um intervalo fechado $[a, b]$, que possui derivadas de primeira e segunda ordem, f' e $f"$, também contínuas em $[a, b]$. Seja $p_0 \in [a, b]$, onde p_0 é um valor inicial para a aproximação da raiz p da função f, de modo que $f'(p_0) \neq 0$ e $|p - p_0|$ é um valor suficientemente pequeno.

Sendo $x = p$, ao escrever a função $f(x)$ em função de p_0 através do polinômio de Taylor de grau 1, obtemos:

$$f(p) = f(p_0) + (p - p_0)f'(p_0) + \frac{(p - p_0)^2}{2}f''\big(\xi(p)\big)$$

com $\xi(p)$ entre p e p_0 e resto dado por $R_1(x) = \frac{(p-p_0)^2}{2} f''\big(\xi(p)\big)$.

Considerando $f(p) = 0$ temos:

$$0 = f(p_0) + (p - p_0)f'(p_0) + \frac{(p - p_0)^2}{2} f''\big(\xi(p)\big).$$

Dado que $|p - p_0|$ é suficientemente pequeno, presume-se que $(p - p_0)^2$ será ainda menor, resultando em:

$$0 \approx f(p_0) + (p - p_0)f'(p_0).$$

Como $f'(p_0) \neq 0$, podemos reescrever a equação acima como:

$$\begin{aligned} 0 &\approx f(p_0) + pf'(p_0) - p_0 f'(p_0) \\ 0 &\approx \frac{f(p_0)}{f'(p_0)} + \frac{pf'(p_0)}{f'(p_0)} - \frac{p_0 f'(p_0)}{f'(p_0)} \\ 0 &\approx \frac{f(p_0)}{f'(p_0)} + p - p_0 \end{aligned}$$

e assim,

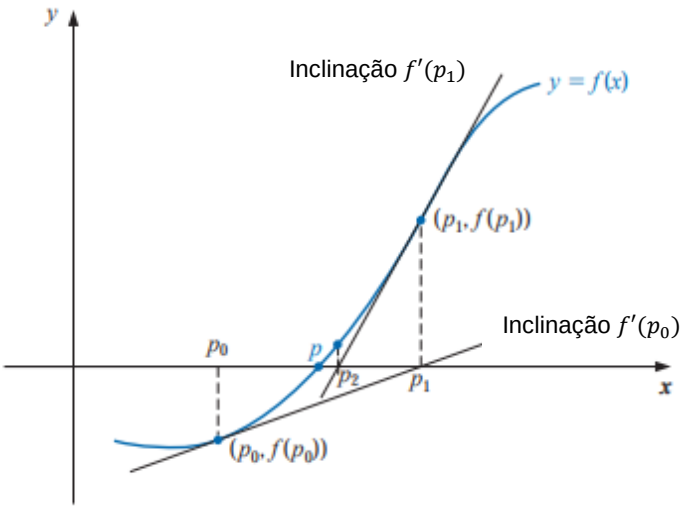
$$p \approx p_0 - \frac{f(p_0)}{f'(p_0)} = p_1.$$

Ao obtermos p_1, podemos reaplicar o procedimento, gerando uma sequência $\{p_n\}$ de aproximações dadas por:

$$p_n = p_{n-1} - \frac{f(p_{n-1})}{f'(p_{n-1})}, \text{com } f'(p_{n-1}) \neq 0 \qquad (4.1)$$

Graficamente, esse processo se resume em obter aproximações através de tangentes sucessivas. Iniciando com o valor inicial $(p_0, f(p_0))$, a aproximação p_1 será a intersecção da reta tangente ao gráfico de f em $x = p_0$ com o eixo das abscissas. Continuando o método, a aproximação p_2 será a intersecção da reta tangente ao gráfico de f em $(p_1, f(p_1))$ com o eixo x, e assim por diante. Na Figura 4.2 temos a ilustração desse método.

Figura 4.2 - Método de Newton.



Fonte: Burden e Faires (2013).

Burden e Faires (2013) ressaltam que, embora considerem esse método numérico como um dos mais eficientes para a determinação da raiz p de uma função f, isso depende de uma boa aproximação inicial, pois o método utiliza como hipótese que o termo $(p - p_0)^2$, em comparação com $|p - p_0|$, seja tão pequeno que pode ser desprezado. Caso isso não aconteça, temos a possibilidade da aproximação não convergir, ou seja, não encontrar a raiz do polinômio.

4.3. MÉTODO DA SECANTE

O método de Newton, de acordo com Burden e Faires (2013), embora necessite de um número menor de iterações para alcançar o valor esperado do que outros métodos numéricos, necessita do valor da derivada de f para cada aproximação, o que resulta em mais cálculos do que apenas calcular $f(x)$ em um valor específico. Uma alternativa para isso é o método da secante que, como o nome sugere, utiliza a reta secante para aproximar o cálculo da derivada.

Lembrando que a derivada de f, calculada no ponto p_{n-1} é dada por:

$$f'(p_{n-1}) = \lim_{x \to p_{n-1}} \frac{f(x) - f(p_{n-1})}{x - p_{n-1}}.$$

Considere a aproximação p_{n-2} para o valor de x. Assim,

$$\lim_{x \to p_{n-1}} \frac{f(x) - f(p_{n-1})}{x - p_{n-1}} \approx \frac{f(p_{n-2}) - f(p_{n-1})}{p_{n-2} - p_{n-1}} = \frac{f(p_{n-1}) - f(p_{n-2})}{p_{n-1} - p_{n-2}}$$

e consequentemente,

$$f'(p_{n-1}) \approx \frac{f(p_{n-1}) - f(p_{n-2})}{p_{n-1} - p_{n-2}}.$$

Substituindo esse resultado em (4.1), obtemos

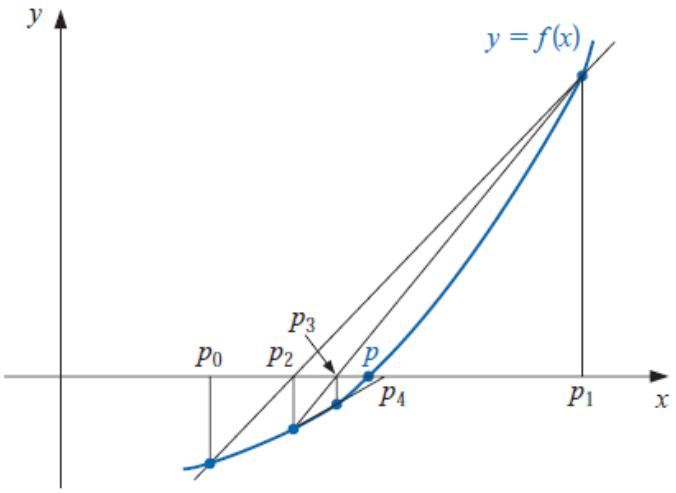
$$p_n = p_{n-1} - \frac{f(p_{n-1})}{f'(p_{n-1})}$$

$$p_n = p_{n-1} - \frac{f(p_{n-1})(p_{n-1} - p_{n-2})}{f(p_{n-1}) - f(p_{n-2})}.$$

Gerando assim a sequência de aproximações para $f(x) = 0$.

Graficamente, a partir de duas aproximações iniciais p_0 e p_1, obtemos a intersecção da reta secante à função f, calculada através dos pontos $(p_0, f(p_0))$ e $(p_1, f(p_1))$, com o eixo x, obtendo assim o valor p_2. Repetindo o procedimento a partir das aproximações p_1 e p_2 e da reta secante que passa agora pelos pontos $(p_1, f(p_1))$ e $(p_2, f(p_2))$, obtemos a intersecção desta reta com o eixo x para encontrar o valor p_3. Este processo é repetido até que o valor de $f(p_n)$ seja suficientemente próximo à 0 ou que um número máximo de iterações tenha sido feita. Esse método está ilustrado na Figura 4.3.

Figura 4.3 - Método da secante.



Fonte: Burden e Faires (2013).

4.4. APLICAÇÃO DOS MÉTODOS E ANÁLISE DOS RESULTADOS

Partindo da função $f(x) = x^2 - A$ e, considerando $f(x) = 0$, obtemos a equação $x^2 - A = 0$, a qual foi implementada numericamente nos três métodos de zeros de funções vistos anteriormente e será utilizada para aproximar o valor de $\sqrt{A}$.

Como condição inicial dos métodos numéricos utilizamos a solução trivial, $x = 1$, e, quando necessário, a solução minimal da equação de Pell, conforme Quadro 3.1.

Os métodos implementados foram analisados segundo o número de iterações de modo que o erro obtido em duas aproximações sucessivas fosse menor do que 10^{-9} e os resultados para os 27 primeiros números primos encontram-se no Quadro 4.1.

Quadro 4.1 - Número de iterações por método.

A	Bissecção	Newton	Secante	Pell
2	30	5	7	7
3	29	6	6	9
5	31	6	6	4
7	31	6	8	5
11	31	7	9	4
13	37	7	11	2
17	32	7	10	3
19	35	7	11	2
23	32	7	10	3
29	40	7	12	2
31	37	7	12	2
37	33	8	11	3
41	38	8	12	2
43	38	8	12	2
47	32	8	10	3
53	43	8	12	1
59	36	8	12	2
61	57	8	13	1
67	42	8	13	2
71	38	8	13	2
73	47	8	13	1
79	33	8	11	3
83	33	8	11	3
89	45	8	13	1
97	52	8	13	1
101	34	8	12	2
103	44	8	13	1

Fonte: Próprio Autor

Observando os resultados do Quadro 4.1, nota-se que o método da bissecção apresenta o maior número de iterações necessárias para se alcançar a precisão estipulada, corroborando com os resultados obtidos na bibliografia, Ruggiero e Lopes (2009) e Burden e Faires (2013).

O método da secante apresentou resultados, em número de iterações, melhores do que o método da bissecção e, não muito diferentes do que o método de Newton que apresentou, para todos os valores considerados de A, o menor número de iterações entre os métodos numéricos para obtenção de zeros de função.

Ainda pelo Quadro 4.1 nota-se que o uso de (3.4) para resolver a equação de Pell $x^2 - Ay^2 = 1$ e, assim, aproximar $\sqrt{A}$ por racionais, apresentou resultados comparáveis ao método de Newton para valores de A menores do que 10 e melhores para valores de A superiores a 10. Pode-se concluir também, para a maior parte dos valores considerados de A, que a solução minimal da equação de Pell representa uma boa aproximação para o valor de $\sqrt{A}$.

Os algoritmos utilizados na implementação dos métodos numéricos de zeros de função encontram-se no Anexo e foram implementados através do *software* MATLAB.

5 CONSIDERAÇÕES FINAIS

Neste trabalho, abordamos a equação de Pell e o processo de extração de raízes. Naturalmente, aspectos teóricos relacionados a esse assunto envolvem conceitos não usualmente utilizados no Ensino Básico. Já os aspectos práticos, tanto de obtenção da solução, da visualização gráfica ou de extração de raízes, são temas de fácil acesso ao estudante da Educação Básica.

Como exemplo, podemos citar o estudo de uma hipérbole envolvendo as equações de Pell, relacionando essas equações com a representação da curva e de suas assíntotas. Essa abordagem, além de enriquecer os conhecimentos dos alunos, pode contribuir para uma melhor compreensão do tema de cônicas. Como visto na Figura 3.3, a equação de Pell remete ao estudo de uma hipérbole em $\mathbb{R}^2$, cujos ramos se aproximam das assíntotas dadas pelas equações $x + y\sqrt{A} = 0$ e $x - y\sqrt{A} = 0$, o que reforça a ideia de que, na medida em que aumentamos o valor de y, melhor é a aproximação de $\sqrt{A}$.

Vale ressaltar que, embora partindo da solução minimal seja simples obter as demais soluções, uma parte importante do processo consiste em obter essa solução inicial. Livros, como o de Andreescu e Andrica (2002), explicam e descrevem o método de obtenção da solução, mas acabam utilizando tabelas para buscar esses valores. Porém, como um dos objetivos do nosso trabalho foi estudar aspectos das equações de Pell que podem ser voltados à Educação Básica, um desses tópicos, aprofundados na Seção 2.5, são as frações contínuas.

Frações contínuas, embora não façam parte do currículo básico, são de simples aplicação. A partir das frações contínuas é possível ensinar conceitos sobre divisões sucessivas (Exemplo 2.6) ou mostrar a representação de um número irracional por meio de frações (Exemplo 2.7). Ainda, relacionando com as equações de Pell, conseguimos obter aproximações iniciais para o valor de um número irracional $\sqrt{A}$ (Exemplo 3.2).

Relembrando a observação feita na Seção 3.2, obter a aproximação da $\sqrt{AB}$ através da equação $x^2 - ABy^2 = 1$ pode ser feita através das equações de Pell $x^2 - Ay^2 = 1$ e $x^2 - By^2 = 1$, pois fornecerá as aproximações de $\sqrt{A}$ e $\sqrt{B}$ e basta

calcular $\sqrt{A} \cdot \sqrt{B}$. Entretanto, caso não tenhamos acesso ou conhecimento da solução minimal, realizar este procedimento não, necessariamente, resultará em obter a solução mais rapidamente, já que a fração contínua obtida para a solução é relacionada com os números envolvidos na solução minimal.

Ao compararmos com os métodos iterativos da bissecção, secante e de Newton, foi possível perceber que, para os valores considerados de A, o método utilizando as equações de Pell converge para o valor esperado em menos iterações. Lembrando que o nosso trabalho é referente às equações de Pell no qual buscamos soluções exclusivamente inteiras, a comparação com os métodos iterativos serve apenas como uma análise da precisão que as soluções da equação de Pell possuem para a obtenção da aproximação racional.

Dos três métodos numéricos utilizados na comparação, embora o Método de Newton seja o que converge mais rapidamente, os conceitos envolvidos em sua formulação acabam por restringir sua aplicação na Educação Básica, por envolver, principalmente o cálculo de derivadas, tema este abordado somente no Ensino Superior. Assim, as equações de Pell $x^2 - Ay^2 = 1$, através das fórmulas vistas na Seção 3.2 e no Exemplo 3.2, também se tornam um meio de calcular zeros de funções, desde que devidamente adaptados para resultar algo em torno de $\sqrt{A}$.

Por fim, o trabalho buscou fornecer ferramentas que possibilitem aplicações desses temas em diversos momentos do estudante no Ensino Básico nos quais, caso aprofundados, permitem ampliar os conhecimentos desses alunos. Entretanto, cabe ressaltar que o tema já aparece em competições olímpicas e de conhecimentos relacionados à Matemática, normalmente debatendo e discutindo meios de obter soluções não só de equações de Pell como também de equações diofantinas de um modo geral.

Além do que já foi mencionado, as ideias para trabalhos futuros incluem estudar e aprofundar as variações das equações de Pell, como as do tipo $x^2 - Ay^2 = m$, de forma a buscar possibilidades de aplicações para a Educação Básica, trabalhando inclusive no desenvolvimento de atividades específicas que tenham como tema central a equação de Pell e, a partir dela, desenvolver os conceitos de frações contínuas, recorrência, hipérbole, assíntotas, entre outros.

REFERÊNCIAS

ANDREESCU, T.; ANDRICA, D. **An Introduction to Diophantine Equations.** Zalau: GIL, 2002.

BURDEN, R. L.; FAIRES, J. D. **Análise Numérica.** Tradução da 8º edição. São Paulo: Cengage Learning, 2008.

DELGADO, J. J.; FRENSEL, K. R.; CRISSAFF, L. S. **Geometria Analítica.** 2ª edição. Rio de Janeiro: SBM, 2017.

DEUS, N. S. P. **Equações Diofantinas Lineares e o GPS: Nova Conexão Curricular.** 2017. Dissertação (Mestrado em Matemática) – PROFMAT, Instituto de Matemática, Universidade Federal da Bahia, 2017.

HEFEZ, A. **Aritmética.** 2ª edição. Rio de Janeiro: SBM, 2016.

MAIA, L. F. **Equações Diofantinas.** 2018. Dissertação (Mestrado em Matemática) – PROFMAT, Instituto de Ciências Exatas e Naturais, Universidade Federal do Pará, 2018.

MARTINEZ, F. E. B., MOREIRA, C. G. T. A., SALDANHA, N. C. e TENGAN, E. **Teoria dos Números: Um passeio com primos e outros números familiares pelo mundo inteiro.** Rio de Janeiro: IMPA, 2013.

MILIES, C. P.; COELHO, S. P. **Números: Uma Introdução à Matemática.** 3ª edição. São Paulo: Edusp, 2013.

MOREIRA, C. G. T. A. **Frações Contínuas, Representações de Números e Aproximações Diofantinas.** 1º Colóquio da Região Sudeste. Rio de Janeiro: IMPA, 2011.

MORGADO, A. C.; CARVALHO, P. C. P. **Matemática Discreta.** 2ª edição. Rio de Janeiro: SBM, 2015.

NETO, A. C. M. **Fundamentos de Cálculo.** 1ª edição. Rio de Janeiro: SBM, 2015.

NETO, A. S. **Convite às Equações Diofantinas: Uma abordagem para a Educação Básica.** 2016. Dissertação (Mestrado em Matemática) – PROFMAT, Universidade Federal de Roraima, 2016.

OLIVEIRA, S. B. **As equações Diofantinas Lineares e o Livro Didático de Matemática para o Ensino Médio.** 2006. Dissertação (Mestrado em Educação Matemática) – PUC, 2006.

PEREIRA, M. V. **Recorrências – Problemas e Aplicações**. 2014. Dissertação (Mestrado em Matemática) – PROFMAT, Instituto de Ciências Exatas, Universidade de Brasília, 2014.

RUGGIERO, M. A. G.; LOPES, V. L. R. **Cálculo Numérico: aspectos teóricos e computacionais.** 2ª edição. São Paulo: Pearson Makron Books, 2009.

SCHROEDER, M. R. **Number Theory in Science and Communication.** 5ª edição. Springer, 2009.

SOUSA, C. M. de. **Aritmética, Frações Contínuas e Aplicações à Música.** 2017. Dissertação (Mestrado em Matemática) – PROFMAT, Departamento de Matemática, Universidade Federal de Rondônia, 2017.

SOUZA, R. S. **Equações Diofantinas Lineares, Quadráticas e Aplicações.** 2017. Dissertação (Mestrado em Matemática) – Instituto de Geociência e Ciências Exatas, Universidade Estadual Paulista, 2017.

WEIL, André. **Number Theory: An approach through history from Hammurapi to Legendre.** New York: Birkhäuser, 2007.

ANEXO – CÓDIGOS UTILIZADOS NO MATLAB

Nas linhas a seguir, temos o código utilizado para comparação dos valores dos Quadros 3.2 e 4.1, referentes a obtenção de aproximações de raízes quadradas utilizando a equação de Pell e os métodos da bissecção, de Newton e da secante.

```
function [Resultados] = Metodos_raizes(precisao)
%% Variáveis gerais
load Dados.mat; % Tabela 3
indiceraiz = length(Dados);
Resultados = zeros(20,5,indiceraiz);

for contador=1:indiceraiz
    D = Dados(contador,1);
    hh=find(Dados(:,1)==D);
    fun=@(x) x.^2-D;
    dfun=@(x) 2.*x;
    imax = 100;          %Número máximo de iterações

    %% Método da Bissecção
    i=1;     %Contador para estimar o número de iterações
    a = 1;               %Chute Inicial x0
    b = Dados(hh,2);     %Chute Inicial x1
    mk = (a+b)/2;        %Primeira previsão para a RAIZ
    Resultados(1,1,contador)=i;
    Resultados(1,2,contador)=mk;
    er=precisao+1;  % Para entrar no loop while
        while (er>precisao)
            xk=mk;
            fa=fun(a);
            fm=fun(mk);
            if fa.*fm < 0
                b=mk;
            elseif fa.*fm > 0
                a=mk;
            else
                break
            end
            i=i+1;
            mk=(a+b)/2;
            Resultados(i,1,contador)=i;
            Resultados(i,2,contador)=mk;
            er=abs((mk-xk)/mk);
        end

    %% Método de Newton-Raphson
    err = 100;
    j=0;     %Contador para estimar o número de iterações
```

```
    xold = 1;           %Chute Inicial
    Resultados(1,3,contador)=xold;
    while (err > precisao && j <= imax)
        j = j + 1;
        f = fun(xold);
        df = dfun(xold);
        xnew = xold - f/df;
        if (j > 1)
            err = abs(xnew - xold);
        end
        xold = xnew;
        Resultados(j,3,contador)=xold;
    end

    %% Método da Secante
    err = 100;
    k=0;
    a = 1;              %Chute Inicial x0
    Resultados(1,4,contador)=1;
    b = Dados(hh,2);    %Chute Inicial x1
    while (err > precisao && k <= imax)
        k = k + 1;
        c =(a*fun(b)-b*fun(a))/(fun(b)-fun(a));
        if (k > 1)
            err = abs(c - b); %abs((c - b)/c)
        end
        a=b; b=c;
        Resultados(k,4,contador)=c;
    end

    %% Equação de Pell
    xk=zeros(20,2);
    xk(1,1)=Dados(hh,2);
    xk(1,2)=Dados(hh,3);
    raiz=zeros(20,1);
    raiz(1)=xk(1,1)/xk(1,2);

    i=1;
    err = 100;
    while (err > precisao && i <= imax)
        xk(i+1,1)=xk(1,1)*xk(i,1)+D*xk(1,2)*xk(i,2);
        xk(i+1,2)=xk(1,2)*xk(i,1)+xk(1,1)*xk(i,2);
        raiz(i+1)=xk(i+1,1)/xk(i+1,2);
        err = abs(raiz(i+1)-raiz(i));
        i=i+1;
    end
    Resultados(1:length(raiz),5,contador)=raiz;

end
```