

Frações Contínuas, Determinantes e Equações Diofantinas Lineares

Continued Fractions, Determinants and Linear Diophantine Equations

Delfim Dias Bonfim^{*1} e Gilmar Pires Novaes²

¹Colégio Dom Alano Marie Du Noday, TO, Brasil

²Universidade Federal do Tocantins, TO, Brasil

Resumo

O presente artigo se destina à apresentação de um método de resolução de equações diofantinas lineares, utilizando, para tal finalidade, os conceitos de frações contínuas e determinantes. Inicialmente, apresentamos a definição de fração contínua simples, sua interpretação geométrica e alguns teoremas fundamentais relacionados a esse conceito. Posteriormente, relacionamos as frações contínuas simples finitas com os determinantes. Finalmente, apresentamos a definição de equação diofantina linear e demonstramos o método para resolvê-la utilizando os conceitos anteriormente mencionados.

Palavras-chave: Frações contínuas, Determinantes, Equações diofantinas lineares.

Abstract

This article is intended to present a method for solving linear diophantine equations, using for this purpose, the concepts of continuous fractions and determinants. Initially we present the definition of simple continued fraction, geometric interpretation and some fundamental theorems related to this concept. Subsequently we relate the finite simple continued fractions with determinants. Finally we present the definition of linear Diophantine equation and we demonstrate the method to solve it using the concepts mentioned above.

Keywords: Continued Fractions, Determinants, Linear Diophantine Equations.

1 Introdução

Em geral, para resolver equações diofantinas lineares, utilizamos o algoritmo de Euclides de "trás para frente". Neste artigo, apresentaremos um método alternativo. Em outras palavras, mais precisamente, demonstraremos um método para resolução de equações diofantinas lineares utilizando frações contínuas e determinantes.

O primeiro resultado (Teorema 1) nos mostra a estreita relação entre as frações contínuas simples e finitas e os números racionais. O segundo resultado (Teorema 2) nos fornece as relações que nos permitem obter tanto o numerador quanto o denominador do i -ésimo convergente de uma dada fração, de forma recorrente, ou seja, a partir de condições iniciais e dos quocientes parciais da fração contínua. Apresentaremos (terceiro resultado - Teorema 3) a Fórmula do determinante, a qual, em particular, nos mostra que o máximo divisor comum de dois convergentes consecutivos é 1.

Alternativamente ao método recorrente descrito no Teorema 2, veremos que, usando determinantes, podemos obter o numerador e o denominador de um convergente conhecendo apenas os quocientes parciais, sem a necessidade dos convergentes precedentes.

A partir da definição de equação diofantina linear, demonstraremos um resultado (Proposição 1) que nos fornece condições necessárias e suficientes para que uma dada equação diofantina linear possua solução. Usando frações contínuas, mostraremos (Teorema 4) que, quando tais equações possuem solução, essas são infinitas.

Mostraremos, também, como obter soluções particulares, e, por consequência, as soluções gerais, de equações diofantinas lineares usando frações contínuas e determinantes, mostrando, assim, que esses conceitos estão intimamente relacionados.

2 Frações Contínuas

Inicialmente, definiremos fração contínua simples, sua representação geométrica associada e alguns resultados essenciais.

Definição 1. Uma fração contínua simples ou regular é uma expressão da forma

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}} \tag{1}$$

sendo a_2, a_3, \dots números inteiros positivos e a_1 um número inteiro qualquer. Os termos a_1, a_2, a_3, \dots são denominados quocientes parciais.

Podemos, ainda, denotar (1) por $[a_1, a_2, a_3, \dots]$ ou

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}$$

2.1 Interpretação geométrica da Definição 1

No caso particular em que a_1 é um número inteiro positivo, podemos fornecer uma interpretação geométrica da Definição 1 para a representação de um número por meio de frações contínuas. Para tal finalidade, consideremos

$$x = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}$$

Inicialmente, devemos construir um retângulo de dimensões $1 \times x$. Em seguida, construiremos quadrados "gulosos" dentro desse retângulo, isto é, sempre colocando o maior quadrado dentro do espaço ainda livre. Por exemplo, na Figura 1 a seguir, temos $a_1 = 1, a_2 = 2, a_3 = 2, \dots$, ou seja,

$$x = 1 + \frac{1}{2 + \frac{1}{2 + \dots}}$$

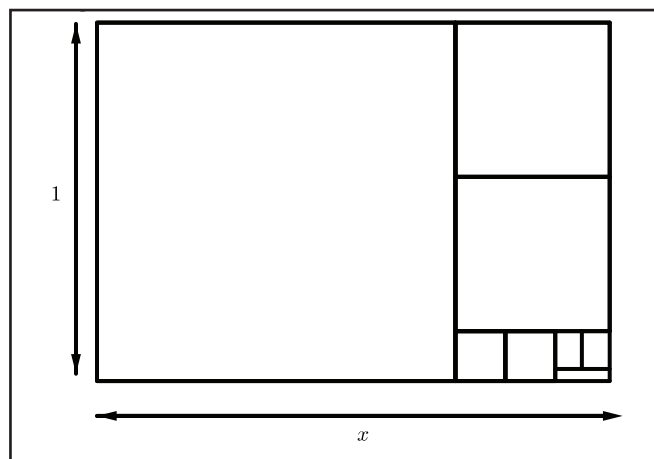


Figura 1 - interpretação geométrica de funções contínuas

Observamos, assim, que os quocientes parciais a_1, a_2, a_3, \dots representam a quantidade de quadrados de cada tamanho.

Caso a fração contínua simples seja finita, podemos escrever a expressão (1) como

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}$$

a qual denotaremos por $[a_1, a_2, a_3, \dots, a_n]$ ou

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_n}}}$$

Neste caso, podemos aplicar o mesmo processo de construção acima para um retângulo com dimensões $p \times q$ (com $p < q, p, q$ inteiros positivos).

O Teorema a seguir relaciona frações contínuas simples e finita aos números racionais. Omitiremos a demonstração desse resultado, a qual pode ser obtida em BONFIM (2014), MOORE (1964) e OLDS (1963).

Teorema 1. *Qualquer fração contínua simples e finita $[a_1, a_2, \dots, a_n]$ representa um número racional. Reciprocamente, qualquer número racional pode ser representado por uma fração contínua simples finita.*

Definição 2. *Denominamos convergente de ordem i da fração contínua $[a_1, a_2, \dots, a_n]$ o número*

$$c_i = \frac{p_i}{q_i} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots + \frac{1}{a_i}}}, \quad 1 \leq i \leq n.$$

O Teorema a seguir mostra como obter os numeradores e os denominadores do i -ésimo convergente de forma recorrente. Omitiremos a demonstração desse resultado, a qual pode ser obtida em BONFIM (2014), MOORE (1964) e OLDS (1963).

Teorema 2. *O numerador p_i e o denominador q_i do i -ésimo convergente $c_i = \frac{p_i}{q_i}$ da fração contínua $[a_1, a_2, a_3, \dots, a_n]$ satisfazem as equações*

$$\begin{cases} p_i &= a_i \cdot p_{i-1} + p_{i-2} \\ q_i &= a_i \cdot q_{i-1} + q_{i-2} \end{cases}, \quad i = 1, 2, 3, \dots, n,$$

com as condições iniciais

$$\begin{cases} p_{-1} &= 0 \\ q_{-1} &= 1 \end{cases} \quad e \quad \begin{cases} p_0 &= 1 \\ q_0 &= 0 \end{cases}.$$

3 Determinantes e as frações contínuas

Nesta seção, apresentaremos a relação existente entre as frações contínuas e os determinantes.

Teorema 3 (Fórmula do Determinante). *A relação*

$$\begin{vmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{vmatrix} = p_i \cdot q_{i-1} - p_{i-1} \cdot q_i = (-1)^i \quad (2)$$

é verdadeira para todo $i \geq 0$, sendo p_i e q_i o numerador e o denominador, respectivamente, do i -ésimo convergente (c_i).

Demonstração. Pode ser obtida em BONFIM (2014), MOORE (1964) e OLDS (1963).

Pelo Teorema 2 temos que os numeradores e os denominadores de um convergente são obtidos de forma recorrente, ou seja, usamos a representação do número em frações contínuas e as condições iniciais para obtermos os numeradores e denominadores dos convergentes subsequentes.

Inicialmente, vamos considerar a seguinte pergunta: Será possível obter o n -ésimo convergente de uma fração contínua, sem antes obter todos os convergentes precedentes àquela?

Veremos que a resposta a essa pergunta é afirmativa, bem como apresentaremos um modo diferente de resolver esse problema usando determinantes. Para esse propósito, necessitaremos apenas dos números inteiros a_1, a_2, \dots, a_n , obtidos da expansão de um dado número em forma de fração contínua.

Na definição a seguir, usamos as terminologias função n -linear e alternada. A primeira significa que a função é linear em cada uma das suas n variáveis. A segunda, por sua vez, significa que a função é antissimétrica.

Definição 3. *O determinante de uma matriz quadrada A de ordem n , denotado por $\det(A)$, é a única função (escalar) f que possui as seguintes propriedades:*

- f é n -linear e alternada nas linhas da matriz A .
- $f(I_n) = 1$, em que I_n denota a matriz identidade de ordem n .

Para o cálculo concreto do determinante de uma matriz quadrada A de ordem n , podemos usar o conhecido desenvolvimento de Laplace, como segue: escolhemos convenientemente uma coluna j de A , de modo que

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{ij}),$$

sendo A_{ij} a matriz obtida de A por supressão da sua i -ésima linha e sua j -ésima coluna. De modo análogo, podemos, alternativamente, escolher convenientemente uma linha i de A , tal que

$$\det(A) = \sum_{i=1}^n (-1)^{i+j} \cdot a_{ij} \cdot \det(A_{ij}).$$

Inicialmente, para os nossos propósitos, vamos obter o numerador p_i do i -ésimo convergente. Primeiramente, analisaremos os cinco primeiros, os quais, conforme o Teorema 2, satisfazem as equações

$$\begin{cases} a_1 \cdot p_0 + p_{-1} &= p_1 \\ a_2 \cdot p_1 + p_0 &= p_2 \\ a_3 \cdot p_2 + p_1 &= p_3 \\ a_4 \cdot p_3 + p_2 &= p_4 \\ a_5 \cdot p_4 + p_3 &= p_5 \end{cases} \quad (3)$$

Podemos reescrever a expressão (3) da seguinte maneira

$$\begin{cases} p_{-1} + a_1 \cdot p_0 - p_1 &= 0 \\ p_0 + a_2 \cdot p_1 - p_2 &= 0 \\ p_1 + a_3 \cdot p_2 - p_3 &= 0 \\ p_2 + a_4 \cdot p_3 - p_4 &= 0 \\ p_3 + a_5 \cdot p_4 - p_5 &= 0 \end{cases} \quad (4)$$

De acordo com o Teorema 2 temos que $p_{-1} = 0$ e $p_0 = 1$. Substituindo essas informações na expressão (4), resulta que

$$\begin{cases} p_1 = a_1 \\ a_2 \cdot p_1 - p_2 = -1 \\ p_1 + a_3 \cdot p_2 - p_3 = 0 \\ p_2 + a_4 \cdot p_3 - p_4 = 0 \\ p_3 - a_5 \cdot p_4 - p_5 = 0 \end{cases} \quad (5)$$

Dessa forma, temos cinco equações lineares nas cinco incógnitas p_1, p_2, p_3, p_4 e p_5 . Isso significa que podemos resolver o sistema acima para obter o valor de qualquer uma dessas incógnitas, que, em verdade, são os numeradores dos convergentes c_1, c_2, c_3, c_4 e c_5 , respectivamente. Vamos concentrar nossa atenção na obtenção da incógnita p_5 , a qual será dada por

$$p_5 = \frac{\begin{vmatrix} -1 & 0 & 0 & 0 & -a_1 \\ a_2 & -1 & 0 & 0 & -1 \\ 1 & a_3 & -1 & 0 & 0 \\ 0 & 1 & a_4 & -1 & 0 \\ 0 & 0 & 1 & a_5 & 0 \end{vmatrix}}{\begin{vmatrix} -1 & 0 & 0 & 0 & 0 \\ a_2 & -1 & 0 & 0 & 0 \\ 1 & a_3 & -1 & 0 & 0 \\ 0 & 1 & a_4 & -1 & 0 \\ 0 & 0 & 1 & a_5 & -1 \end{vmatrix}} \quad (6)$$

Analisando o denominador da expressão acima, observamos claramente que seu resultado será $(-1)^5$, e, de maneira mais geral, para p_n , será $(-1)^n$, pois se trata de uma matriz diagonal inferior, cujo determinante é o produto dos elementos de sua diagonal.

O próximo passo será permutar a última coluna do numerador com a sua primeira, o que requer um total de $4 = 5 - 1$ (ou $n - 1$) permutações, lembrando que, ao permutar duas colunas (ou inversão de sinais de uma coluna), seu determinante (em valor absoluto) não se altera. Assim, necessitamos realizar $5 = (5 - 1) + 1$ alterações de sinais, sendo as quatro primeiras devido à troca de colunas, acrescida de uma inversão de sinais da coluna mencionada. Geralmente, precisamos de $n = (n - 1) + 1$ alterações de sinais. Realizar as $n = (n - 1) + 1$ alterações de sinais do numerador corresponde a executar essas modificações e multiplicar o resultado por $(-1)^n$. Observando que o denominador é $(-1)^n$, temos que esses valores se simplificam, independentemente de n ser par ou ímpar. Por consequência, a expressão (6) se resume a

$$p_5 = \begin{vmatrix} a_1 & -1 & 0 & 0 & 0 \\ 1 & a_2 & -1 & 0 & 0 \\ 0 & 1 & a_3 & -1 & 0 \\ 0 & 0 & 1 & a_4 & -1 \\ 0 & 0 & 0 & 1 & a_5 \end{vmatrix} \quad (7)$$

Isso significa que, para o cálculo de p_5 , necessitamos apenas dos termos a_1, a_2, a_3, a_4 e a_5 , decorrentes da expansão em fração contínua do número dado.

Para obter o denominador q_i do i -ésimo convergente, que ocorre no Teorema 2, procedemos de maneira análoga. A única alteração consiste nas condições iniciais, em que $q_{-1} = 1$ e $q_0 = 0$. Assim, obtemos a seguinte expressão para o denominador q_5 , ou seja,

$$q_5 = \begin{vmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & a_2 & -1 & 0 & 0 \\ 0 & 1 & a_3 & -1 & 0 \\ 0 & 0 & 1 & a_4 & -1 \\ 0 & 0 & 0 & 1 & a_5 \end{vmatrix} \quad (8)$$

$$q_5 = \begin{vmatrix} a_2 & -1 & 0 & 0 \\ 1 & a_3 & -1 & 0 \\ 0 & 1 & a_4 & -1 \\ 0 & 0 & 1 & a_5 \end{vmatrix}$$

Portanto, a partir das expressões (7) e (8), obtemos o convergente $c_5 = \frac{p_5}{q_5}$, sem a necessidade dos convergentes precedentes.

Por um raciocínio análogo podemos obter o convergente c_n , conhecendo apenas os quocientes parciais $[a_1, a_2, \dots, a_n]$, isto é,

$$c_n = \frac{p_n}{q_n} = \frac{\begin{vmatrix} a_1 & -1 & 0 & 0 & 0 \\ 1 & a_2 & -1 & 0 & 0 \\ 0 & 1 & \ddots & -1 & 0 \\ 0 & 0 & 1 & a_{n-1} & -1 \\ 0 & 0 & 0 & 1 & a_n \end{vmatrix}}{\begin{vmatrix} a_2 & -1 & 0 & 0 \\ 1 & \ddots & -1 & 0 \\ 0 & 1 & a_{n-1} & -1 \\ 0 & 0 & 1 & a_n \end{vmatrix}}$$

No exemplo a seguir, ilustramos o uso de determinantes, conforme apresentamos anteriormente.

Exemplo 1. Usando determinantes (sem usar os convergentes precedentes), obteremos o quarto convergente da fração contínua correspondente ao número $\frac{225}{157}$.

Pelo algoritmo de Euclides, obtemos

$$\begin{aligned} 225 &= 1 \cdot 157 + 68 \\ 157 &= 2 \cdot 68 + 21 \\ 68 &= 3 \cdot 21 + 5 \\ 21 &= 4 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Assim,

$$\begin{aligned} \frac{225}{157} &= 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{5}}}} \\ &= [1, 2, 3, 4, 5] = [a_1, a_2, a_3, a_4, a_5]. \end{aligned}$$

Para fixar ideias, adaptaremos as expressões (7) e (8) para o caso em que $n = 4$. Ou seja,

$$\begin{aligned} c_4 &= \frac{p_4}{q_4} = \frac{\begin{vmatrix} a_1 & -1 & 0 & 0 \\ 1 & a_2 & -1 & 0 \\ 0 & 1 & a_3 & -1 \\ 0 & 0 & 1 & a_4 \end{vmatrix}}{\begin{vmatrix} a_2 & -1 & 0 \\ 1 & a_3 & -1 \\ 0 & 1 & a_4 \end{vmatrix}} \\ c_4 &= \frac{\begin{vmatrix} 1 & -1 & 0 & 0 \\ 1 & 2 & -1 & 0 \\ 0 & 1 & 3 & -1 \\ 0 & 0 & 1 & 4 \end{vmatrix}}{\begin{vmatrix} 2 & -1 & 0 \\ 1 & 3 & -1 \\ 0 & 1 & 4 \end{vmatrix}} \\ c_4 &= \frac{43}{30}. \end{aligned}$$

Observemos que, para obtermos o convergente desejado, devemos calcular os determinantes presentes no numerador (de ordem 4) e no denominador (de ordem 3), que resultam em aplicações relacionadas a esse conceito.

4 Equações Diofantinas lineares

A resolução de vários problemas em Matemática conduzem a equações cujas soluções devem ser números inteiros (possivelmente positivos). Como exemplo típico, citamos um proposto por Euler:

Exemplo 2. (Euler) De quantas maneiras podemos comprar selos de 7 e 11 reais, se dispomos de 100 reais?

Iniciamos esta seção com a seguinte definição:

Definição 4. Uma equação da forma

$$ax + by = c \quad \text{ou} \quad ax - by = c,$$

sendo a, b e c números inteiros não nulos, é denominada equação diofantina linear.

Tais equações receberam este nome em homenagem ao matemático grego Diofanto de Alexandria, que viveu aproximadamente no século III d.C.

Definição 5. Uma solução particular arbitrária da equação diofantina linear $ax + by = c$ (respectivamente, $ax - by = c$) é um par ordenado (x_0, y_0) de números inteiros tal que $ax_0 + by_0 = c$ (respectivamente $ax_0 - by_0 = c$).

O resultado que segue nos fornece uma condição necessária e suficiente para que uma equação diofantina linear possua solução.

Proposição 1. Sejam a e b inteiros positivos tais que $d = \text{mdc}(a, b)$. A equação $ax + by = c$ admite soluções inteiras se e somente se d divide c .

Demonstração. Suponhamos que a equação $ax + by = c$ admita solução x_0 e y_0 . Como d divide a e b , segue que d divide $c = ax_0 + by_0$. Reciprocamente, se d divide c , então existe um número inteiro k tal que $c = kd$. Por outro lado, pelo Teorema de Bachet-Bézout¹, existem inteiros n e m de modo que $d = an + bm$. Multiplicando por k essa última equação, obtemos $c = kd = a(kn) + b(km)$. Logo, a equação $ax + by = c$ admite pelo menos uma solução, a saber, $x = kn$ e $y = km$. □

Exemplo 3. A equação diofantina linear $3x + 9y = 4$ não possui solução. De fato, basta observar que $\text{mdc}(3, 9) = 3$ não divide 4.

Se $ax + by = c$ possui solução, é imediato verificar que essa equação é equivalente à $a_1x + b_1y = c_1$, em que $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ e $c_1 = \frac{c}{d}$ tal que $\text{mdc}(a_1, b_1) = 1$. Assim, podemos nos concentrar apenas em $ax + by = c$, tais que $d = \text{mdc}(a, b) = 1$.

Teorema 4. Se a e b são números inteiros positivos, tais que $d = \text{mdc}(a, b) = 1$, então a equação

$$ax - by = 1 \tag{9}$$

possui infinitas soluções inteiras.

Demonstração. Pelo Teorema 1, podemos representar o número racional $\frac{a}{b}$ como uma fração contínua simples e finita

$$\frac{a}{b} = [a_1, a_2, \dots, a_n]. \tag{10}$$

Os dois últimos convergentes $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ e $c_n = \frac{p_n}{q_n} = \frac{a}{b}$ constituem o meio adequado para a solução da equação $ax - by = 1$, pois eles satisfazem as relações do Teorema 3, ou seja,

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

e, substituindo $p_n = a$ e $q_n = b$, obtemos

$$a \cdot q_{n-1} - b \cdot p_{n-1} = (-1)^n. \tag{11}$$

¹O Teorema de Bachet-Bézout afirma que: se $d = \text{mdc}(a, b)$, então existem números inteiros n e m tais que $d = an + bm$.

Se n é par, segue que $x_0 = q_{n-1}$ e $y_0 = p_{n-1}$ é uma *solução particular* da equação $ax - by = 1$.

Se n é ímpar, temos que $(-1)^n = -1$. Neste caso, podemos modificar o último termo a_n da expansão da fração contínua obtida em (10), substituindo

$$\begin{cases} \frac{1}{a_n} & \text{por} & \frac{1}{a_n - 1 + \frac{1}{1}}, & \text{se} & a_n > 1 \\ \frac{1}{a_{n-1} + \frac{1}{a_n}} & \text{por} & \frac{1}{a_{n-1} + 1}, & \text{se} & a_n = 1 \end{cases}.$$

Em outras palavras, se a expressão (10) possui um número ímpar de quocientes parciais, podemos transformá-la em outra com um número par, ao considerarmos

$$\begin{cases} [a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_n - 1, 1], & \text{se } a_n > 1 \\ [a_1, a_2, \dots, a_n] = [a_1, a_2, \dots, a_{n-1} + 1], & \text{se } a_n = 1 \end{cases}.$$

Uma vez que obtivemos a solução particular (x_0, y_0) da equação (9), decorre facilmente a sua *solução geral*. Para isso, consideremos (x, y) outra solução de (9). Logo,

$$ax - by = ax_0 - by_0 = 1.$$

Daí resulta que

$$a(x - x_0) = b(y - y_0). \tag{12}$$

Como $\text{mdc}(a,b) = 1$, segue que b divide $x - x_0$. Logo, existe um número inteiro t tal que

$$x - x_0 = bt \text{ se e somente se } x = x_0 + bt. \tag{13}$$

Substituindo (13) em (12), obtemos

$$b(at) = b(y - y_0).$$

Logo,

$$y - y_0 = at \text{ se e somente se } y = y_0 + at. \tag{14}$$

Portanto, qualquer solução (x, y) da equação $ax - by = 1$ é da forma

$$\begin{cases} x = x_0 + bt \\ y = y_0 + at \end{cases}, \quad t \in \mathbb{Z}. \tag{15}$$

Por outro lado, se (x_0, y_0) é uma solução particular de $ax - by = 1$, as relações dadas em (15) satisfazem a equação dada. De fato,

$$\begin{aligned} ax - by &= a(x_0 + bt) - b(y_0 + at) \\ &= a(x_0 - by_0) + abt - abt \\ &= a(x_0 - by_0) = 1. \end{aligned}$$

□

Portanto, as soluções dadas, conforme (15), são denominadas de *solução geral* da equação $ax - by = 1$.

Exemplo 4. Obteremos as soluções gerais das equações $13x - 17y = 1$ e $13x - 17y = -1$.

Usando o algoritmo de Euclides, obtemos

$$\begin{aligned} 17 &= 1 \cdot 13 + 4 \\ 13 &= 3 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

e, com isso, $\frac{13}{17} = [0, 1, 3, 4]$. Ou seja, existe um número par de quocientes parciais. Devemos calcular o convergente c_3 , o qual satisfaz

$$c_3 = \frac{p_3}{q_3} = \frac{\begin{vmatrix} a_1 & -1 & 0 \\ 1 & a_2 & -1 \\ 0 & 1 & a_3 \end{vmatrix}}{\begin{vmatrix} a_2 & -1 \\ 1 & a_3 \end{vmatrix}} = \frac{\begin{vmatrix} 0 & -1 & 0 \\ 1 & 1 & -1 \\ 0 & 1 & 3 \end{vmatrix}}{\begin{vmatrix} 1 & -1 \\ 1 & 3 \end{vmatrix}} = \frac{3}{4}.$$

Segue que $(x_0, y_0) = (4, 3)$ é uma solução particular da equação $13x - 17y = 1$, pois $13(4) - 17(3) = 1$. Portanto, sua solução geral é dada por

$$\begin{cases} x = 4 + 17t \\ y = 3 + 13t \end{cases}, \quad t \in \mathbb{Z}.$$

Multiplicando $13(4) - 17(3) = 1$ por (-1) , obtemos $13(-4) - 17(-3) = -1$. Logo, $(x_1, y_1) = (-4, -3)$ é uma solução particular da equação $13x - 17y = -1$. Portanto, sua solução geral é da forma

$$\begin{cases} x = -4 + 17t \\ y = -3 + 13t \end{cases}, \quad t \in \mathbb{Z}.$$

Estudaremos, agora, as soluções das equações $ax - by = c$ e $ax + by = c$, tais que $\text{mdc}(a,b) = 1$. Tendo aprendido como resolver a equação $ax - by = 1$, as soluções dessas equações decorrem sem dificuldade, como segue.

- **1º caso:** Consideremos a equação $ax - by = c$, tal que $\text{mdc}(a,b) = 1$.

Dada uma solução particular (x_0, y_0) de $ax - by = 1$, de modo que

$$ax_0 - by_0 = 1,$$

multiplicando ambos os membros dessa equação por c , obtemos

$$a(cx_0) - b(cy_0) = c. \tag{16}$$

Logo, (cx_0, cy_0) é uma solução particular de $ax - by = c$. Portanto, sua solução geral é dada por

$$\begin{cases} x = cx_0 + bt \\ y = cy_0 + at \end{cases}, \quad t \in \mathbb{Z}. \tag{17}$$

- **2º caso:** Consideremos a equação $ax + by = c$, tal que $\text{mdc}(a,b) = 1$.

Inicialmente, é necessário conhecer uma solução particular de $ax + by = 1$. Para isso, devemos obter a expansão em fração contínua de $\frac{a}{b}$ com um número par de convergentes, dos quais $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$, $c_n = \frac{p_n}{q_n} = \frac{a}{b}$ satisfazem

$$aq_{n-1} - b(p_{n-1}) = 1$$

ou, equivalentemente,

$$aq_{n-1} + b(-p_{n-1}) = 1, \quad (18)$$

mostrando, portanto, que $x_0 = q_{n-1}$ e $y_0 = -(p_{n-1})$ é uma solução particular de $ax + by = 1$.

Observamos que

$$\begin{aligned} ax + by = c \cdot 1 &= c \cdot [a \cdot q_{n-1} + b \cdot (-p_{n-1})], \text{ ou seja,} \\ a(x - c \cdot q_{n-1}) &= b(-y - c \cdot p_{n-1}) \end{aligned} \quad (19)$$

Como $\text{mdc}(a,b) = 1$, segue que b divide $(x - c \cdot q_{n-1})$. Logo, existe um número inteiro t , tal que

$$x - c \cdot q_{n-1} = bt \text{ se e somente se } x = c \cdot q_{n-1} + bt. \quad (20)$$

De (20) em (19), temos

$$b(at) = b(-y - c \cdot p_{n-1}).$$

Assim,

$$-y - c \cdot p_{n-1} = at \iff y = c \cdot (-p_{n-1}) - at. \quad (21)$$

Por outro lado, para qualquer número $t \in \mathbb{Z}$, uma substituição direta utilizando (18), (20) e (21), nos fornece

$$\begin{aligned} ax + by &= a(c \cdot q_{n-1} + bt) + b(-at - c \cdot p_{n-1}) \\ &= a \cdot c \cdot q_{n-1} + abt - abt + b \cdot c \cdot (-p_{n-1}) \\ &= c \cdot [a \cdot q_{n-1} + b \cdot (-p_{n-1})] = c \cdot 1 = c. \end{aligned}$$

Portanto, a solução geral da equação $ax + by = c$ tem a forma

$$\begin{cases} x = c \cdot q_{n-1} + bt \\ y = c \cdot (-p_{n-1}) - at \end{cases}, \quad t \in \mathbb{Z}. \quad (22)$$

Exemplo 5. Obteremos as soluções gerais das equações $205x - 93y = 5$ e $205x - 93y = -5$.

Usando o algoritmo de Euclides, obtemos

$$\begin{aligned} 205 &= 2 \cdot 93 + 19 \\ 93 &= 4 \cdot 19 + 17 \\ 19 &= 1 \cdot 17 + 2 \\ 17 &= 8 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Assim, $\frac{205}{93} = [2, 4, 1, 8, 2]$, que, por sua vez, tem um número ímpar de convergentes. Com isso, devemos

transformá-la em uma outra equivalente, com um número par de quocientes parciais. Como $a_n = a_5 = 2 > 1$, consequentemente $\frac{205}{93} = [2, 4, 1, 8, 2] = [2, 4, 1, 8, 1, 1]$.

$$\begin{aligned} c_5 &= \frac{p_5}{q_5} = \frac{\begin{vmatrix} a_1 & -1 & 0 & 0 & 0 \\ 1 & a_2 & -1 & 0 & 0 \\ 0 & 1 & a_3 & -1 & 0 \\ 0 & 0 & 1 & a_4 & -1 \\ 0 & 0 & 0 & 1 & a_5 \end{vmatrix}}{\begin{vmatrix} a_2 & -1 & 0 & 0 \\ 1 & a_3 & -1 & 0 \\ 0 & 1 & a_4 & -1 \\ 0 & 0 & 1 & a_5 \end{vmatrix}} \\ &= \frac{\begin{vmatrix} 2 & -1 & 0 & 0 & 0 \\ 1 & 4 & -1 & 0 & 0 \\ 0 & 1 & 1 & -1 & 0 \\ 0 & 0 & 1 & 8 & -1 \\ 0 & 0 & 0 & 1 & 1 \end{vmatrix}}{\begin{vmatrix} 4 & -1 & 0 & 0 \\ 1 & 1 & -1 & 0 \\ 0 & 1 & 8 & -1 \\ 0 & 0 & 1 & 1 \end{vmatrix}} \\ c_5 &= \frac{49}{108}. \end{aligned}$$

Segue que $x_0 = q_5 = 49$ e $y_0 = p_5 = 108$ são soluções da equação $205x - 93y = 1$. Com isso, obtemos $205(245) - 93(540) = 5$. Logo, $(5x_0, 5y_0) = (245, 540)$ é uma solução particular da equação $205x - 93y = 5$. Portanto, sua solução geral é

$$\begin{cases} x = 245 + 93t \\ y = 540 + 205t \end{cases}, \quad t \in \mathbb{Z}.$$

Analogamente, $(-5x_0, -5y_0) = (-245, -540)$ é uma solução particular da equação $205x - 93y = -5$. Consequentemente, sua solução geral é

$$\begin{cases} x = -245 + 93t \\ y = -540 + 205t \end{cases}, \quad t \in \mathbb{Z}.$$

A seguir, resolveremos o Exemplo 2, devido a Euler, com o qual iniciamos a seção.

Exemplo 6. Dispondo-se de 100 reais, quais são as quantias que se podem gastar para comprar alimentos que custam 11 reais e 7 reais?

Sabendo que uma quantia (k_1) é múltipla de 11 e outra (k_2) é múltipla de 7, podemos escrever $k_1 = 11x$ e $k_2 = 7y$, em que x e y são números inteiros positivos. Assim, a solução do problema consiste em resolver a equação

$$11x + 7y = 100. \quad (23)$$

Utilizando o algoritmo de Euclides, obtemos $\frac{11}{7} = [1, 1, 1, 3] = [a_1, a_2, a_3, a_4]$. Como $n = 4$, segue

que $x_0 = q_{n-1} = q_3$ e $y_0 = p_{n-1} = p_3$ são soluções da equação $11x + 7(-y) = 1$. Usando determinantes, obtemos

$$c_3 = \frac{p_3}{q_3} = \frac{\begin{vmatrix} a_1 & -1 & 0 \\ 1 & a_2 & -1 \\ 0 & 1 & a_3 \end{vmatrix}}{\begin{vmatrix} a_2 & -1 \\ 1 & a_3 \end{vmatrix}} = \frac{\begin{vmatrix} 1 & -1 & 0 \\ 1 & 1 & -1 \\ 0 & 1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix}} = \frac{3}{2}.$$

Logo, $(x_0, y_0) = (2, 3)$. Segue de (22) que

$$\begin{cases} x = 200 + 7t \\ y = -300 - 11t \end{cases} \quad (24)$$

é solução geral da equação $11x + 7y = 100$. A natureza peculiar do problema exige que os números x e y sejam positivos, ou seja,

$$\begin{cases} x = 200 + 7t > 0 \\ y = -300 - 11t > 0 \end{cases}.$$

Daí, $t = -28$, uma vez que $t \in \mathbb{Z}$. Substituindo esse valor de t em (24), obtemos

$$\begin{cases} x = 200 + 7t = 200 + 7(-28) = 4 \\ y = -300 - 11t = -300 - 11(-28) = 8 \end{cases}.$$

Logo, $k_1 = 11x = 44$ e $k_2 = 7y = 56$. Portanto, podem ser gastos 44 reais comprando alimentos que custam 11, e 56 reais com os que custam 7.

5 Conclusões

Procuramos, no decorrer deste artigo, apresentar um método alternativo para a resolução de equações diofantinas lineares, usando frações contínuas e determinantes.

Entendemos que esse método, para valores em que a expansão em frações contínuas não seja muito extensa, torna-se bem mais interessante do que aquele tradicionalmente abordado, o qual se baseia no algoritmo de Euclides, de "trás para frente".

De outro modo, acreditamos que, em última análise, o método mencionado acima está respaldado pelos seus caracteres de cunho didático, educativo e informativo.

Referências

- BONFIM, D. D. (2014). *Frações contínuas com aplicações*. UFT.
- MOORE, C. G. (1964). *An introduction to continued fractions*. The National Council of Teachers of Mathematics.
- OLDS, C. D. (1963). *Continued fractions*. Handom House The L. W. Singer Company.