ReviSeM

Revista Sergipana de Matemática e Educação Matemática

https://doi.org/10.34179/revisem.v6i3.15046

SOLUÇÃO PARTICULAR DE EQUAÇÕES DIOFANTINAS LINEARES $ax + by = c$ VIA ABORDAGEM POR SUBSTITUIÇÃO PROGRESSIVA DO ALGORITMO DE EUCLIDES.

Luiz Augusto Richit
Universidade Federal do Rio Grande do Sul - UFRGS, *campus* Porto Alegre - RS
luizaugustorichit@gmail.com
Adriana Richit
Universidade Federal da Fronteira Sul - UFFS, *campus* Erechim - RS
adrianarichit@gmail.com
Andriceli Richit
Instituto Federal Catarinense - IFC, *campus* Concórdia - SC
andricelirichit@gmail.com

Resumo

Uma Equação Diofantina (ED) é uma equação algébrica de uma ou mais variáveis para a qual se inquerem soluções inteiras. EDs do tipo $ax + by = c$ com $a, b, c \in \mathbb{Z}$, são as Equações Diofantinas (EDs) mais estudadas em livros-texto de Aritmética. Para obtenção de soluções (x, y) nos inteiros de EDs deste tipo, são importantes os conceitos de divisibilidade, Algoritmo de Euclides e Máximo Divisor Comum (MDC). A estratégia comumente empregada e que compõe a maioria dos livros-texto sobre EDs consiste da aplicação sucessiva do Algoritmo de Euclides e escrita do $\text{mdc}(a, b)$ como uma combinação linear de a e b, fornecendo assim uma solução nos inteiros para a equação $ax + by = \text{mdc}\,(a, b)$. Neste texto apresentamos e discutimos alguns resultados preliminares para o estudo de EDs e detalhamos um desencadeamento operatório para calcular a solução particular de $ax + by = \text{mdc}(a, b)$, denominado *Abordagem por Substituição Progressiva* (ASP).

Palavras-chave: Abordagem por Substituição Progressiva, Equações Diofantinas Lineares, Algoritmo da Divisão de Euclides, Divisibilidade.

Abstract

A Linear Diophantine Equation (DE) is an algebraic equation of one or more variables for which integer solutions are needed. DEs of the kind of $ax + by = c$ with $a, b, c \in \mathbb{Z}$, are the most studied Diophantine Equations (DEs) in Arithmetic textbooks. To obtain solutions (x, y) in the integers of EDs of this type, the concepts of divisibility,

Euclid's Algorithm and Greatest Common Divisor (GCD) are importants. The usual strategy employed and that appears in the majority of textbooks on the DEs consists of successive applications of the Euclid's Algorithm and the writing of the $\gcd(a, b)$ as a linear combination of a and b, thus providing a solution in integers for $ax + by = \gcd(a, b)$ equation. In this text, we present and discuss some preliminary results for the study of DEs, and we detail an operative trigger to compute the particular solution of $ax + by = \gcd(a, b)$ called the *Forward Substitution Approach* (FSA).
Keywords: Forward Substitution Approach, Linear Diophantine Equations, Division Euclid's Algorithm, Divisibility.

1 Introdução

Equações do tipo $ax + by = c$ estabelecem a relação mais simples entre as funções matemáticas elementares. Uma abordagem possível é a sua resolução nos inteiros. Uma equação algébrica com uma ou mais incógnitas (i.e. $ax + by = c$; $a, b, c \in \mathbb{Z}$), para a qual se inspecionam soluções inteiras são chamadas *Equações Diofantinas* [4, 23]. Essas equações foram assim nomeadas em homenagem ao grego Diofanto, matemático que viveu em Alexandria por volta do ano 250 *a.c.* e que foi responsável pelo estudo de suas soluções [14]. Embora, originalmente, Diofanto preocupava-se com as soluções racionais de equações de valores indeterminados [23, 20], [14] aponta que Diofanto teve seu nome atribuído às equações, restrita aos inteiros, por suas contribuições profundas dentro do desenvolvimento da Matemática neste campo de estudo.

Uma Equação Diofantina (ED) pode não ter solução, ou ter um número finito ou infinito de soluções [8]. São exemplos, além de equações do tipo $ax + by = c$, as EDs $2x + 3y + z = 8$, $x^3 + y^3 = z^3$, $x^2 + y^2 = z^2$ e $x + y^2 + z^3 + w^4 = 5$. As equações do tipo $x^n + y^n = z^n$ são equações diofantinas famosas devido ao célebre Último Teorema de Fermat, que afirma que a equação não têm soluções inteiras simultâneas para x, y e z se $n > 2$ (n natural). A demonstração deste teorema foi finalizada em 1995 por Andrew Wiles com a colaboração de Richard Taylor [31]. Para $n = 2$, a relação de Fermat reduz-se à equação $x^2 + y^2 = z^2$, resultado conhecido por Teorema de Pitágoras/Gougu e que sabemos ter infinitas soluções, sendo exemplos as ternas pitagóricas $(3, 4, 5)$ e $(8, 15, 17)$.

No estudo de EDs destacam-se, em particular, as equações onde aparecem a soma de monômios de grau um (1) ou zero (0). Estas EDs, chamadas Lineares (EDLs), têm como exemplos as equações do tipo $ax + by = c$ que estudaremos neste texto. Elas podem aparecer em diversos contextos de ensino, embora o enfoque aritmético deste tipo de problema não seja em geral desenvolvido a nível escolar. Mesmo encontrando trabalhos sobre o ensino deste tipo de EDLs em nível de escola básica [21, 23, 19,

22, 28, 29, 32], tratam-se de tentativas de aproximação para o ensino do tópico, o que revela assim um caráter de excepcionalidade. De fato, o mais comum é o ensino da solução nos inteiros de $ax + by = c$ a nível universitário, em especial, em cursos de Matemática [18]. Apesar disso, também podem ser observados em trabalhos e pesquisas com abordagens específicas, cursos e programas de ensino de tópicos deste campo [24, 25] ou em competições olímpicas para alunos do ensino fundamental, como por exemplo, na Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP).

Exemplos de equações diofantinas são aquelas obtidas no balanceamento de equações químicas e determinação da fórmula molecular (seguindo a Lei de Lavoisier - [5]), podendo ser encontradas em [11]. Nesses casos, o balanceamento resulta na escrita de sistemas de EDLs. Algoritmos para verificação da solubilidade e a obtenção das soluções para sistemas de EDLs podem ser encontrados em [13] e [7]. Outros exemplos de problemas aplicados envolvendo EDLs do tipo $ax + by = c$ podem ser encontrados em [1, 2, 11, 12, 30, 33].

A resolução de EDLs comumente apresentada em livros-texto dá-se pela aplicação sucessiva do Algoritmo de Euclides [27], seguida de obtenção da solução particular escrita em função dos restos das divisões [10, 14] . Esta tarefa pode ser longa, dependendo dos números envolvidos [15], e inclui tanto produtos crescentes quanto uma atenção especial com sinais, aumentando a chance de erros operatórios. Diferentemente dos materiais didáticos que versam sobre a resolução nos inteiros de $ax + by = c$, partindo-se de cada uma das divisões pelo Algoritmo de Euclides, uma possibilidade não explorada relaciona-se a reformulação que envolve evidenciar os restos, substituí-los sucessivamente nas relações do Algoritmo de Euclides de onde se verifica um padrão operatório [15, 35]. À essa alternativa, denomina-se *Abordagem por Substituição Progressiva do Algoritmo de Euclides* [15].

Nosso objetivo com a apresentação deste texto é prover ao estudo de EDLs do tipo $ax + by = c$ uma janela para busca da solução particular diferenciada daquela comumente encontrada nos principais documentos de ensino do tópico. Para isso, organizamos o trabalho de forma a contemplar tanto aspectos detalhados do ponto de vista matemático, incluindo resultados preliminares importantes (Seção 2), como também exemplos que facilitem a compreensão das ideias envolvidas. Do mesmo modo, na Seção 3, é apresentado o resultado principal seguido de demonstração e adicionado de exemplos ilustrativos, envolvendo recursos algébricos e apresentação gráfica por esquemas.

2 Preliminares

2.1 Algoritmo da Divisão de Euclides e MDC

Para resolução nos inteiros de $ax + by = c$, são importantes alguns resultados preliminares relacionados à divisibilidade e aritmética de restos. Assim, baseando-se em [10], definimos e apresentamos os seguintes resultados:

Definição 2.1. *Sejam $a, b \in \mathbb{N}$. Dizemos que o número a divide o número b se, e somente se, existe $c \in \mathbb{N}$ tal que $b = a \cdot c$ e escrevemos $a \mid b$. A mesma definição pode ser estendida para $\mathbb{Z}$.*

Se a não divide b, escrevemos $a \nmid b$.

Definição 2.2. *(Máximo Divisor Comum - MDC) Seja $\mathrm{div}_{\mathbb{N}}(a)$ o conjunto de todos os divisores em $\mathbb{N}$ de a. Sejam $a, b \in \mathbb{N}$ não simultaneamente nulos. Seja $\mathrm{div}_{\mathbb{N}}(a, b) = \mathrm{div}_{\mathbb{N}}(a) \cap \mathrm{div}_{\mathbb{N}}(b)$, o maior elemento de $\mathrm{div}_{\mathbb{N}}(a, b)$ é chamado de máximo divisor comum entre a e b e é denotado por $\mathrm{mdc}(a, b)$.*

Teorema 2.3. *(Divisão Euclidiana) Sejam $n, d \in \mathbb{N}$ com $d \neq 0$. Então, existem e são únicos os números $q, r \in \mathbb{N}$ tais que $n = q \cdot d + r$, com $0 \leq r < d$.*

Demonstração: Ver [10] ou [6].

Proposição 2.4. *Seja $a, b, c, x, y \in \mathbb{Z}$, a não nulo. Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy)$.*

Demonstração: Ver [10].

Lema 2.5. *(Lema de Euclides) Sejam $a, b, n \in \mathbb{N}\backslash\{0\}$ tais que $an \leq b$. Então, $\mathrm{mdc}(a, b - na) = \mathrm{mdc}(a, b)$.*

Demonstração: Ver [10].

O Teorema 2.3 da Divisão Euclidiana, garante que existem e são únicos $q_1, r_1 \in \mathbb{N}$ tais que $b = a \cdot q_1 + r_1$ com $0 \leq r_1 < a$ ($a, b \in \mathbb{N} \setminus \{0\}$ e $a \leq b$) [6]. Este resultado, juntamente do resultado da Proposição 2.4 que garante que toda combinação linear de b e c é divisível por qualquer número a que divida b e c simultaneamente, é utilizado para Demonstração do Algoritmo de Euclides para o cálculo do MDC. Por fim, pelo Lema de Euclides (Lema 2.5), obtermos o resultado de que $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, b - a \cdot q_1) = \mathrm{mdc}(a, r_1)$. Se $r_1 = 0$, já temos o máximo divisor comum, pois $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, 0) = a$. Se $r_1 \neq 0$, aplicamos novamente o Algoritmo da Divisão (Teorema 2.3), dividindo a por r_1 e assim sucessivamente até que o resto seja zero.

A partir dos resultados básicos apresentados nesta seção com base em [10], iniciamos, na seção seguinte, a análise da solubilidade nos inteiros de $ax + by = c$. Ao final do texto, no Apêndice 5A, apresentamos também um código Matlab (versão R2018a) para cálculo do MDC entre dois números naturais não nulos.

2.2 Existência de solução inteira (x, y) da EDL $ax + by = c$

Diz-se que uma EDL do tipo $ax + by = c$ tem solução sempre que $\text{mdc}(a, b)|c$. Para sua demonstração, indicamos o resultado intermediário que estabelece que $\text{mdc}(a, b)$ pode ser escrito como uma combinação linear entre a e b. Esse resultado é conhecido como Teorema de Bézout, cujo enunciado é:

Teorema 2.6. *(Teorema de Bézout) Sejam $a, b \in \mathbb{Z}$ não simultaneamente nulos e $D = \text{mdc}(a, b)$. Então, existem $\alpha, \beta \in \mathbb{Z}$, tais que $D = \alpha a + \beta b$.*

Demonstração: Ver demonstração em [10]

Assim, o Teorema 2.6 confere o resultado requerido para demonstração da existência de solução inteira de uma EDL do tipo $ax + by = c$ aqui apresentada. Dessa forma, seguindo [10]:

Teorema 2.7. *Sejam $a, b, c \in \mathbb{Z}$, com a e b não ambos nulos e seja $D = \text{mdc}(a, b)$. Então, a equação $ax + by = c$ tem solução em $\mathbb{Z}$ se, e somente se, $D \mid c$.*

Demonstração: Ver demonstração em [10].

Como conclusão imediata, se $D = \text{mdc}(a, b) = 1$, toda equação $ax + by = c$ tem solução em $\mathbb{Z}$, pois qualquer que seja $c \in \mathbb{Z}$, $D \mid c$, já que $1 \mid c$. Adicionalmente, se a e b possuem sinais opostos, o número de soluções inteiras positivas é infinito, enquanto do contrário será finito [34]. Por fim, se $D \nmid c$, então a equação mencionada não possui solução inteira. Uma vez que $ax + by = c$ representa uma reta, disso resulta dizer que a reta não passa por quaisquer pontos de coordenadas simultamentente inteiras no reticulado $\mathbb{Z} \times \mathbb{Z}$ do plano cartesiano.

Além disso, podemos encontrar infinitas soluções por meio do termo geral de soluções inteiras da EDL, dado por [13, 14, 26]:

$$\begin{cases} x = x_0 + \frac{b}{D}t \\ y = y_0 - \frac{a}{D}t \end{cases}$$

sendo $t \in \mathbb{Z}$, e desde que seja conhecida ao menos uma solução (x_0, y_0) inteira. Esse resultado, que discutiremos na Seção 2.4, já era conhecido por Brahmagupta, enquanto

Diofanto ao estudar equações indeterminadas, preocupou-se em encontrar uma solução particular [9, 3]. Pelo Teorema 2.7, não se deduz que todas as soluções inteiras podem ser obtidas do termo geral (o que requer demonstração) e o que de fato ocorre. Tal resultado pode ser encontrado, por exemplo, nas referências [10, 14, 18].

2.3 Aplicação do Algoritmo de Euclides e solução particular por retrossubstituição

Para obter a solução particular da EDL $ax + by = c$, se $c = \text{mdc}\,(a, b)$, podemos aplicar o algoritmo de Euclides e escrever o $\text{mdc}\,(a, b)$ como uma combinação linear de a e b, isto é, $\text{mdc}\,(a, b) = \alpha a + \beta b$ (Teorema de Bézout 2.6). Para este caso, os valores de α e β obtidos são a solução particular desejada. Se, por outro lado, $\text{mdc}(a, b) \neq c$, como $\text{mdc}\,(a, b) \mid c$, então temos que $\exists k \in \mathbb{Z}$ tal que $k \cdot \text{mdc}\,(a, b) = c$. Assim, basta multiplicar $\text{mdc}\,(a, b) = \alpha a + \beta b$ por k, obtendo-se $k \cdot \alpha a + k \cdot \beta b = k \cdot \text{mdc}\,(a, b) = c$ de modo que a solução particular será $(x_0, y_0) = (k \cdot \alpha, k \cdot \beta)$.

Para ilustrar a aplicação do Lema de Euclides e a obtenção de uma solução particular para o caso da EDL $ax + bx = c$, utilizaremos alguns exemplos.

Exemplo 2.8. *Encontrar uma solução particular, nos inteiros, das seguintes equações:*
a) $12x + 105y = 3$
b) $4x + 27y = 7$.

a) Cálculo do $\text{mdc}(12, 105)$:

$$\begin{aligned} 105 &= 12 \cdot 8 + 9 \\ 12 &= 9 \cdot 1 + \underline{3} \\ 9 &= 3 \cdot 3 + 0 \\ &\Downarrow \\ \underline{3} &= \text{mdc}(12, 105) \end{aligned}$$

$\text{mdc}\,(12, 105) = 3$ e $3 \mid 3$, portanto a equação possui solução em $\mathbb{Z}$.
Solução particular:

$$\begin{aligned} 3 &= 12 - 9 \cdot 1 \\ 3 &= 12 - (9) \cdot 1 \\ 3 &= 12 - (105 - 12 \cdot 8) \cdot 1 \\ 3 &= -105 + 9 \cdot 12 \\ 3 &= 12 \cdot (9) + (-1) \cdot 105 \end{aligned}$$

E assim, obtemos a solução particular $(x_0, y_0) = (9, -1)$.
b) Cálculo do mdc$(4, 27)$:

$$\begin{aligned} 27 &= 4 \cdot 6 + 3 \\ 4 &= 3 \cdot 1 + \underline{1} \\ 3 &= 1 \cdot 3 + 0 \\ &\Downarrow \\ \underline{1} &= \text{mdc}(4, 27) \end{aligned}$$

mdc $(4, 27) = 1$ e $1 \mid 7$, portanto a equação possui solução em $\mathbb{Z}$.
Solução particular:

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ 1 &= 4 - (3) \cdot 1 \\ 1 &= 4 - (27 - 4 \cdot 6) \cdot 1 \\ 1 &= -27 + 4 \cdot 7 \\ 1 &= 4 \cdot (7) + (-1) \cdot 27 \\ &\Downarrow \times 7 \\ 7 &= 4 \cdot (49) + (-7) \cdot 27 \end{aligned}$$

E assim obtemos a solução particular $(x_0, y_0) = (49, -7)$.

2.4 Solução Geral de uma EDL $ax + by = c$

Como mencionado anteriormente, a partir da solução particular, podemos obter o termo geral de soluções inteiras da EDL $ax + by = c$. Este resultado pode ser resumido no teorema seguinte [10]:

Teorema 2.9. *Se D divide c, sendo $D = \text{mdc}(a, b)$, e se o par de inteiros (x_0, y_0) é uma solução particular da Equação Diofantina Linear $ax + by = c$, então são soluções desta equação os pares (x, y) tais que: $x = x_0 + \frac{b}{D}t$ e $y = y_0 - \frac{a}{D}t$, com $t \in \mathbb{Z}$.*

Uma versão mais forte do Teorema 2.9 afirma que todas as soluções inteiras são dadas por $x = x_0 + \frac{b}{D}t$ e $y = y_0 - \frac{a}{D}t$. Este resultado pode ser encontrado em [10] e [14], por exemplo.

Outra estratégia para obtenção da solução geral pode ser feita por inspeção e equivale à parametrização da equação da reta $ax + by = c$. Neste caso, a parametrização é

dada por: $a\,(x - x_p) + b\,(y - y_p) = 0$, onde $ax_p + by_p = c$. Esse novo problema consiste em encontrar dois números $x_p, y_p \in \mathbb{Z}$, por inspeção, que somados resultem em c, mas um seja divisível por a e o outro por b. Essa reformulação, que embora trate-se do mesmo problema inicial, é ainda interessante. Estes números podem ser exatamente aqueles obtidos pela determinação da solução particular. Esta estratégia é uma maneira de se obter a expressão da solução geral sem recorrer à memorização da lei do termo geral do Teorema 2.9. Para isto, basta que se tome (x_p, y_p) como a solução particular:

$$\begin{aligned} ax + by &= c \\ ax + by &= ax_0 + by_0 \\ a\,(x - x_0) + b\,(y - y_0) &= 0 \\ a\,(x - x_p) + b\,(y - y_p) &= 0 \\ a\,(x - x_p) &= b\,(y_p - y) \\ \frac{(x - x_p)}{b} &= \frac{(y_p - y)}{a} \end{aligned}$$

Seja t a constante da igualdade, podemos escrever:

$$\frac{(x - x_0)}{b} = \frac{(y_0 - y)}{a} = t \quad \Rightarrow \begin{cases} \frac{(x-x_0)}{b} = t & \Rightarrow x = x_0 + bt \\ \frac{(y_0-y)}{a} = t & \Rightarrow y = y_0 - at \end{cases}$$

Em muitos casos é consideravelmente fácil obter uma solução por meio de inspeção. Consideremos um exemplo.

Exemplo 2.10. *Encontrar o termo geral de soluções inteiras de* $2x + 3y = 17$. *Como* $17 = 2 + 15 = 2 \times 1 + 3 \times 5$, *podemos reescrever:*

$$\begin{aligned} 2x + 3y &= 17 \\ 2x + 3y - 17 &= 0 \\ 2x - 2 + 3y - 15 &= 0 \\ 2(x - 1) + 3(y - 5) &= 0 \\ 2(x - 1) &= 3(5 - y) \end{aligned}$$

O que indica que $2(x-1) = 3(5-y) \iff \frac{(x-1)}{3} = \frac{(5-y)}{2}$. Seja t a constante da igualdade, podemos escrever:

$$\frac{(x-1)}{3} = \frac{(5-y)}{2} = t \quad \Rightarrow \begin{cases} \frac{(x-1)}{3} = t & \Rightarrow x = 1+3t \\ \frac{(5-y)}{2} = t & \Rightarrow y = 5-2t \end{cases}$$

Note que essa estratégia é simples desde que seja fácil encontrar ax_p e by_p tal que $ax_p+by_p = c$. Apesar disso, a partir da solução particular obtida por meio do Algoritmo de Euclides, podemos realizar o mesmo procedimento dispensando a tarefa de inspeção que, por ocasião dos valores dos coeficientes a, b e c, pode ser menos evidente.

3 Resultado principal

Nesta seção, apresentamos a *Abordagem por Substituição Progressiva* de forma ilustrada, a seguir demonstramos esse resultado e exemplificamos sua aplicação.

3.1 Abordagem por Substituição Progressiva para obtenção da solução particular da EDL $ax + by = c$

A *Abordagem por Substituição Progressiva* apresenta-se como uma técnica alternativa à abordagem comumente empregada para escrever uma solução particular da EDL $ax + by = c$. Assim, desde que $ax + by = c$ possua solução, o Algoritmo de Euclides para o cálculo de $\text{mdc}(a, b)$ ainda precisa ser aplicado [15, 35]. Em contrapartida, com essa técnica, elimina-se a necessidade das sucessivas substituições conforme abordagem empregada em livros-texto. Além disso, reduz-se a atenção adicional necessária nas operações com sinais e o evidenciamento de restos deixa de ser uma fonte de erros [15, 35].

Inicialmente, consideremos a aplicação do Lema de Euclides para o cálculo do MDC entre a e b. Denotemos por r_i e q_i o resto e o quociente das seguintes divisões sucessivas pela aplicação da Divisão Euclidiana [35]:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \\ b &= r_1 \cdot q_2 + r_2 \\ r_1 &= r_2 \cdot q_3 + r_3 \\ r_2 &= r_3 \cdot q_4 + r_4 \\ &\vdots \ddots \vdots \\ r_{n-1} &= r_n \cdot q_{n+1} + r_{n+1} \\ r_n &= r_{n+1} \cdot q_n + 0 \end{aligned} \tag{3.1}$$

Dessa forma, considerando-se o resultado das sucessivas divisões pelo Lema de Euclides (conforme Seção 2.1) e empregando-se a mesma notação que a precedente, podemos expressar genericamente os restos da divisão do seguinte modo [15]:

$$\begin{aligned} r_1 &= 1a - q_1 b \\ r_2 &= b - r_1 q_2 = b - (a - q_1 b)\, q_2 = -q_2 a + (1 + q_1 q_2)\, b \\ r_3 &= r_1 - r_2 q_3 = (a - b q_1) - q_3 \left[-a q_2 + (1 + q_1 q_2)\, b\right] = (1 + q_2 q_3)\, a - \left[q_1 + q_3\,(1 + q_1 q_2)\right] b \\ r_4 &= r_2 - r_3 q_4 = \text{-}a q_2 + (1 + q_1 q_2)\, b - q_4 \left[a\,(1 + q_2 q_3) - (q_1 + q_3\,(1 + q_1 q_2))\, b\right] = \\ &= -\left[q_2 + q_4\,(1 + q_2 q_3)\right] a + \left[(1 + q_1 q_2) + q_4\,(q_1 + q_3\,(1 + q_1 q_2))\right] b \\ &\ldots \end{aligned} \tag{3.2}$$

Avaliando-se os coeficientes de a e b em cada linha, encontramos um padrão alternado do sinal e um padrão operatório para o cálculo destes coeficientes. Seguindo a apresentação dada por [15], podemos organizar o desencadeamento operatório para o coeficiente de b e o de a, que nesta formulação envolve apenas os quocientes da Divisão Euclidiana de cada linha, excetuando-se a que resulta em resto zero. Nas Fig.s 1 e 2, semelhante ao apresentado por [15], é exposto o cálculo de y (Fig. 1) e o cálculo de x (Fig. 2), soluções inteiras da EDL $ax + by = \text{mdc}(a, b)$.

Os valores finais de x e y são a solução particular, enquanto os intermediários são necessários apenas para sua obtenção e determinam os seus sinais. Em resumo, podemos computar uma solução particular da EDL $ax + by = \text{mdc}(a, b)$ por meio da seguinte recorrência [15]:

$$P = \begin{cases} x_i = x_{i-2} + q_i \cdot x_{i-1}, & \text{para } 1 < i < n,\ x_0 = 0 \text{ e } x_1 = 1, \\ y_i = y_{i-2} + q_i \cdot y_{i-1}, & \text{para } 1 < i < n,\ y_0 = 1 \text{ e } y_1 = q_1. \end{cases} \tag{3.3}$$

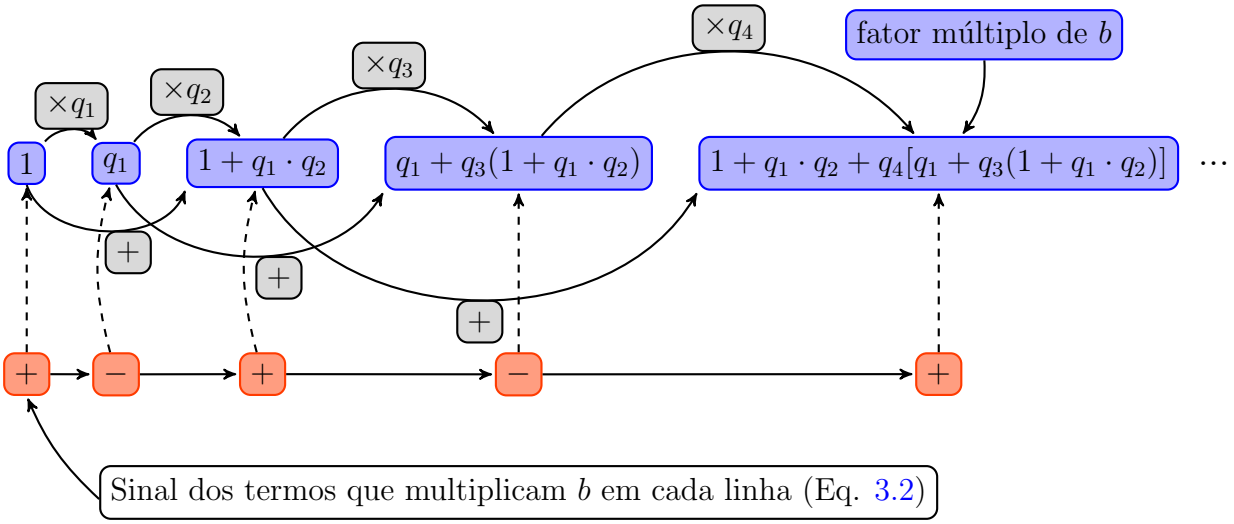

Figura 1: Representação esquemática do cálculo de y da solução particular da EDL $ax + by = \text{mdc}\,(a, b)$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5.

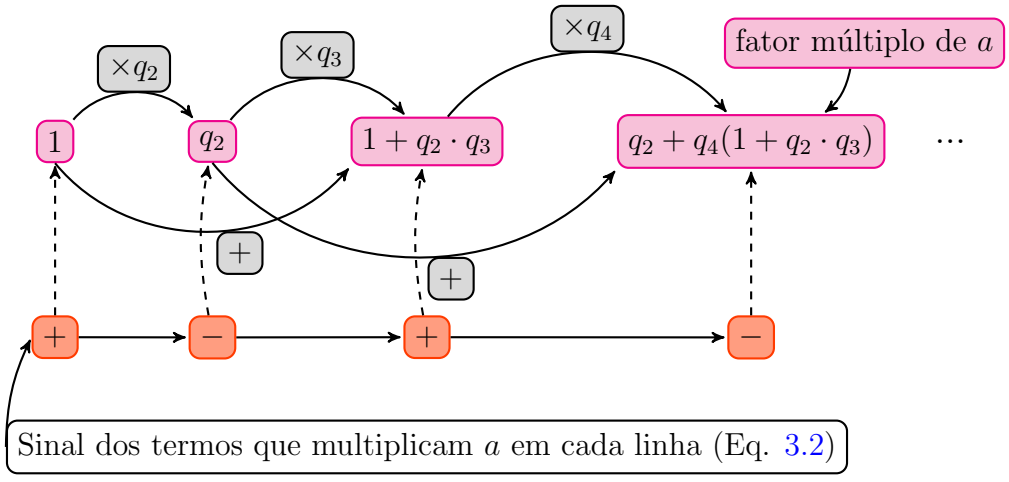

Figura 2: Representação esquemática do cálculo de x da solução particular da EDL $ax + by = \text{mdc}\,(a, b)$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5.

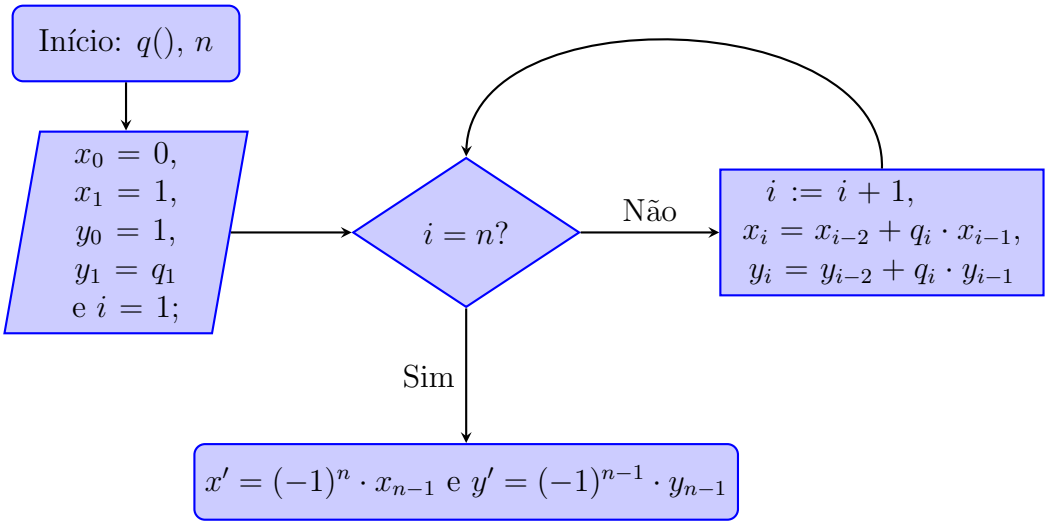

Figura 3: Fluxograma mostrando esquema para computação da solução particular da EDL $ax + by = \text{mdc}(a, b)$ a partir dos quocientes ($q\,()$) obtidos através do cálculo do $\text{mdc}(a, b)$ pelo Lema de Euclides 2.5.

Se tormarmos $x' := (-1)^n\, x_{n-1}$ e $y' := (-1)^{n-1}\, y_{n-1}$, temos que (x', y') são soluções de $ax + by = c = \text{mdc}\,(a, b)$ [15] . Para os casos em que $c = k \cdot \text{mdc}\,(a, b)$ basta que multipliquemos a solução pelo inteiro k e assim dispomos de uma ferramenta adicional para computar uma solução inteira particular da equação. Na Fig. 3 é apresentado um fluxograma padrão para o cálculo de x_i e y_i seguindo a recorrência apresentada por [15]. Em acréscimo, no Apêndice 6B, um código para computação da solução particular via ASP é provido.

3.2 Validade da Abordagem Progressiva por recorrência

Suponha, por hipótese, que podemos calcular os valores dos coeficientes de a e b em cada linha da Eq. 3.2 através da Eq. 3.3, isto é:

$$P = \begin{cases} x_i = x_{i-2} + q_i \cdot x_{i-1}, & \text{para } 1 < i < n,\ x_0 = 0 \text{ e } x_1 = 1, \\ y_i = y_{i-2} + q_i \cdot y_{i-1}, & \text{para } 1 < i < n,\ y_0 = 1 \text{ e } y_1 = q_1. \end{cases}$$

Para o qual o sinal de cada x_i e y_i é dado por $(-1)^{i+1}$ e $(-1)^i$ respectivamente, até que se obtenha $x' = (-1)^{i+1}\, x_i$ e $y' = (-1)^i\, y_i$, com $i = n - 1$, solução particular da EDL. Vamos provar por indução que a recorrência é verdadeira e que, consequentemente, (x', y') é uma solução particular da EDL.

Demonstração:
Base de Indução:
Para $i = 2$*:*
Temos por hipótese que $x_2 = x_0 + q_2 \cdot x_1 = 0 + q_2 \cdot 1 = q_2$ *na Eq. 3.3, com* $x_2' = x_2 (-1)^{2+1} = -q_2$*. Pela Eq. 3.2 temos que* $x_2' = -q_2$ *como requerido.*
Temos por hipótese que $y_2 = y_0 + q_2 \cdot y_1 = 1 + q_2 \cdot q_1 = 1 + q_2 \cdot q_1$ *na Eq. 3.3, com* $y_2' = y_2 (-1)^2 = 1 + q_2 \cdot q_1$*. Pela Eq. 3.2 temos que* $y_2' = 1 + q_1 \cdot q_2$*, o que mostra que Eq. 3.3 é válida para* $i = 2$*.*
Passagem de Indução: Por hipótese, suponha que a propriedade é válida para todo $i < n-1$ *(Indução forte).Vamos calcular* x_{i+1} *e* y_{i+1} *a partir da equação* $r_{i+1} = r_{i-1} - r_i \cdot q_{i+1}$ *(isolando o resto euclidiano* r_{i+1} *pela Eq. 3.1).*
Primeiro, temos em cada linha da Eq. 3.2, o *resto escrito como uma combinação linear de* a *e* b*. Empregando a hipótese da Eq. 3.3 (incluindo o sinal), podemos escrever os restos como:* $r_i = a \cdot (-1)^{i+1} x_i + b \cdot (-1)^i y_i$ *e* $r_{i-1} = a \cdot (-1)^i x_{i-1} + b \cdot (-1)^{i-1} y_{i-1}$*. Substituindo-se em* $r_{i+1} = r_{i-1} - r_i \cdot q_i$*, encontramos:*

$$
\begin{aligned}
r_{i+1} &= r_{i-1} - r_i \cdot q_{i+1} \\
r_{i+1} &= a \cdot (-1)^i x_{i-1} + b \cdot (-1)^{i-1} y_{i-1} - \left[a \cdot (-1)^{i+1} x_i + b \cdot (-1)^i y_i\right] q_{i+1} \\
r_{i+1} &= a \left[(-1)^i x_{i-1} - (-1)^{i+1} x_i q_{i+1}\right] + b \cdot \left[(-1)^{i-1} y_{i-1} + (-1)(-1)^i y_i q_{i+1}\right] \\
r_{i+1} &= a \left[(-1)^i x_{i-1} + \frac{1}{(-1)^1}(-1)^{i+1} x_i q_{i+1}\right] + b \cdot \left[(-1)^{i-1} y_{i-1} + \frac{1}{(-1)^1}(-1)^i y_i q_{i+1}\right] \\
r_{i+1} &= a \left[(-1)^i x_{i-1} + (-1)^{-1}(-1)^{i+1} x_i q_{i+1}\right] + b \cdot \left[(-1)^{i-1} y_{i-1} + (-1)^{-1}(-1)^i y_i q_{i+1}\right] \\
r_{i+1} &= a \left[(-1)^i x_{i-1} + (-1)^i x_i q_{i+1}\right] + b \cdot \left[(-1)^{i-1} y_{i-1} + (-1)^{i-1} y_i q_{i+1}\right] \\
r_{i+1} &= a \cdot (-1)^i \left[x_{i-1} + x_i q_{i+1}\right] + b \cdot (-1)^{i-1} \left[y_{i-1} + y_i q_{i+1}\right] \\
r_{i+1} &= a \cdot (-1)^{i+2-2} \left[x_{i-1} + x_i q_{i+1}\right] + b \cdot (-1)^{i-1+2-2} \left[y_{i-1} + y_i q_{i+1}\right] \\
r_{i+1} &= a \cdot (-1)^{i+2} \cdot 1 \left[x_{i-1} + x_i q_{i+1}\right] + b \cdot (-1)^{i-1+2} \cdot 1 \left[y_{i-1} + y_i q_{i+1}\right] \\
r_{i+1} &= a \cdot \underbrace{(-1)^{i+2}}_{sinal} \left[\underbrace{x_{i-1} + x_i q_{i+1}}_{x_{i+1}}\right] + b \cdot \underbrace{(-1)^{i+1}}_{sinal} \left[\underbrace{y_{i-1} + y_i q_{i+1}}_{y_{i+1}}\right]
\end{aligned}
$$

Isso mostra que para o algoritmo de Euclides com n *divisões, para* $1 < i < i+1 < n$*,* $i \in P(i) \Rightarrow i + 1 \in P(i)$*, o que finaliza a demonstração.*

c.q.d.

Esse resultado mostra que, para a aplicação do algoritmo de Euclides com n divisões, a recorrência definida para o cálculo de x' e y' é sempre válida, pois partindo-se da hipótese de que ocorridas i substituições sucessivas é possível calcular a $(i+1)$-ésima substituição subsequente (e portanto calcular cada r_i da Eq. 3.2 como combinação linear de a e b) por meio da recorrência dada. Assim, uma aplicação de cálculo pelo Algoritmo de Euclides com n divisões, tendo a n-ésima linha resto zero, x_i e y_i são dados pela recorrência da Equação 3.3 e consequentemente, para a última linha com resto diferente de zero (linha $n-1$ na Equação 3.1) os coeficientes x' e y' para Equação 3.2 são a solução particular da EDL $ax+by = \text{mdc}\,(a,b) = \text{mdc}\,(r_{n+1},0) = r_{n+1}$ (veja na Equação 3.1, última linha antes que o resto seja zero, que $\text{mdc}(a,b) = r_{n+1}$).

3.3 Solução Particular de uma EDL $ax+by=c$ por meio da Abordagem por Substituição Progressiva.

A *Abordagem por Substituição Progressiva*, conforme alternativa apresentada por [15] e [35], consiste em um desencadeamento operatório sobre os valores dos quocientes obtidos da aplicação sucessiva do Algoritmo de Euclides. Assim, com base na Seção 3.1, apresentamos dois exemplos da aplicação do resultado para obter a solução particular de uma EDL $ax+by=c$.

Exemplo 3.1. *Encontrar a solução inteira particular de*
a) $286x+60y=2$
b) $35x-97y=5$

a) Cálculo de $D = \text{mdc}(286,60)$:

$$\begin{aligned} 286 &= 60\cdot(4)+46\\ 60 &= 46\cdot(1)+14\\ 46 &= 14\cdot(3)+4\\ 14 &= 4\cdot(3)+\underline{2}\\ 4 &= 2\cdot(2)+0\\ &\Downarrow\\ \underline{2} &= \text{mdc}(286,60) \end{aligned}$$

Como $\text{mdc}\,(286,60) = 2$ e $2 \mid 2$, portanto a EDL possui solução em $\mathbb{Z}$. Os valores dos quocientes das divisões sucessivas foram destacados entre parênteses em face de que são estes os valores necessários para o cálculo da solução particular pela abordagem apresentada na Seção 3.1. Assim, com $q = \{4,1,3,3\}$ e utilizando-se do mesmo esquema

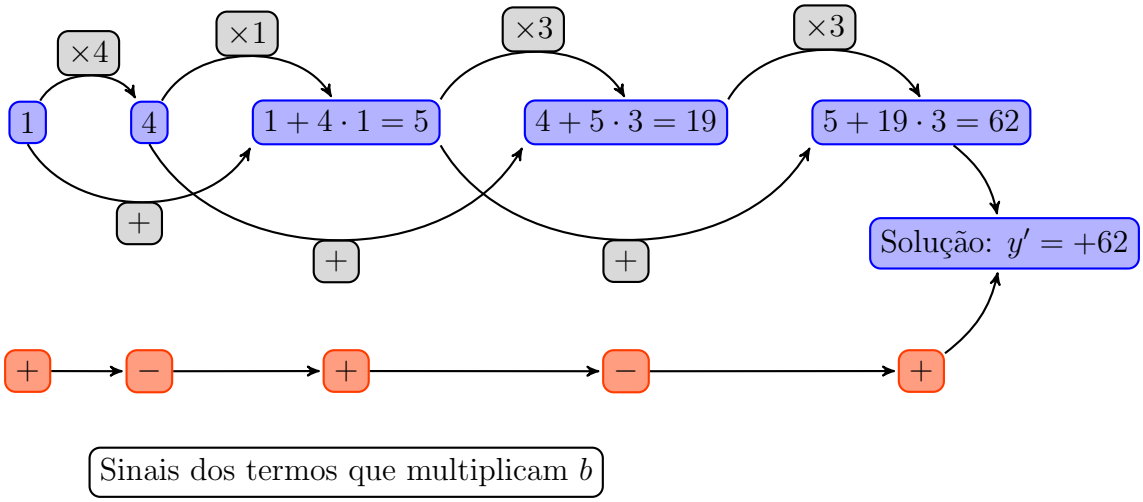

Figura 4: Modelo esquemático para o cálculo de y' da solução particular da EDL $286x + 60y = 2$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5.

das Fig.s 1 e 2, apresentaremos o cálculo da solução particular nas Fig.s 4 (cálculo de y') e 5 (cálculo de x').

Assim, obtemos a solução particular $(x', y') = (-13, 62)$. Pelo resultado do Teorema 2.9, temos como termo geral de soluções: $x = x_0 + \frac{b}{D}t = -13 + \frac{60}{2}t = -13 + 30t$ *e* $y = 62 - \frac{286}{2}t = 62 - 143t$ com $t \in \mathbb{Z}$.

b) Façamos a seguinte mudança de variável: $z = -y$. A nova EDL será: $35x + 97z = 5$. Cálculo de $D = \text{mdc}(97, 35)$:

$$\begin{aligned} 97 &= 35 \cdot (2) + 27 \\ 35 &= 27 \cdot (1) + 8 \\ 27 &= 8 \cdot (3) + 3 \\ 8 &= 3 \cdot (2) + 2 \\ 3 &= 2 \cdot (1) + \underline{1} \\ 2 &= 1 \cdot (2) + 0 \\ &\Downarrow \\ \underline{1} &= \text{mdc}(35, 97) \end{aligned} \tag{3.4}$$

Como $\text{mdc}\,(97, 35) = 1$ e $1 \mid 5$, a EDL possui solução em $\mathbb{Z}$. Do mesmo modo que para o item a), temos os seguintes quocientes: $q = \{2, 1, 3, 2, 1\}$. Calculemos a solução particular x' e z' (Fig.s 6 e 7).

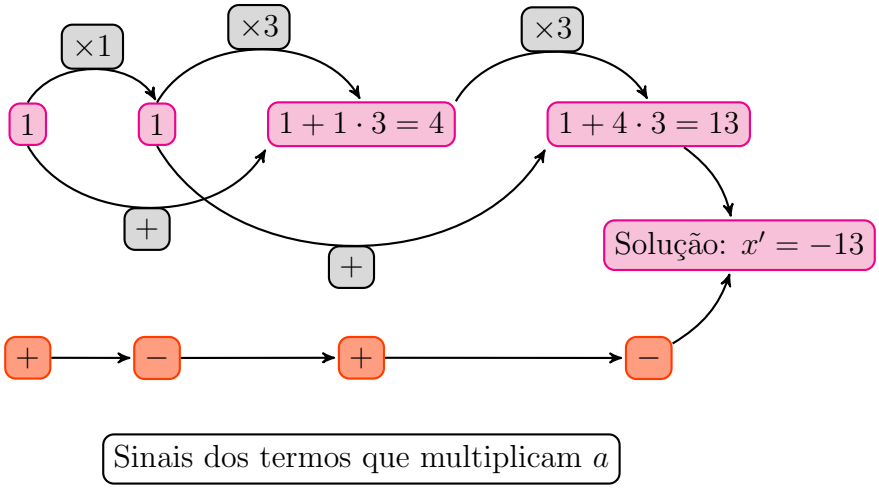

Figura 5: Modelo esquemático para o cálculo de x' da solução particular da EDL $286x + 60y = 2$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5.

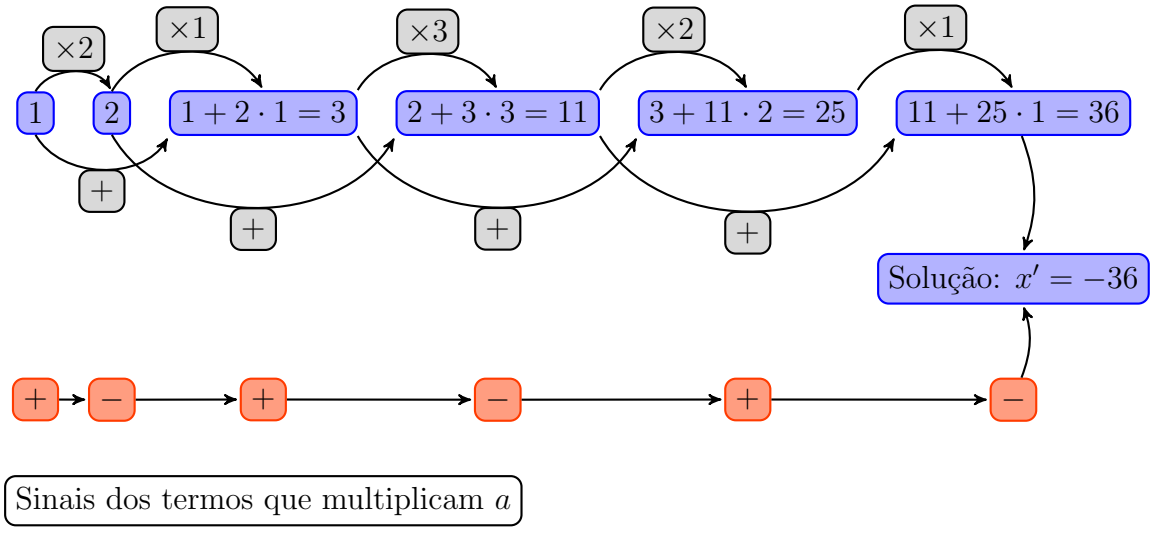

Figura 6: Modelo esquemático para o cálculo de x' da solução particular da EDL $35x + 97z = 1$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5.

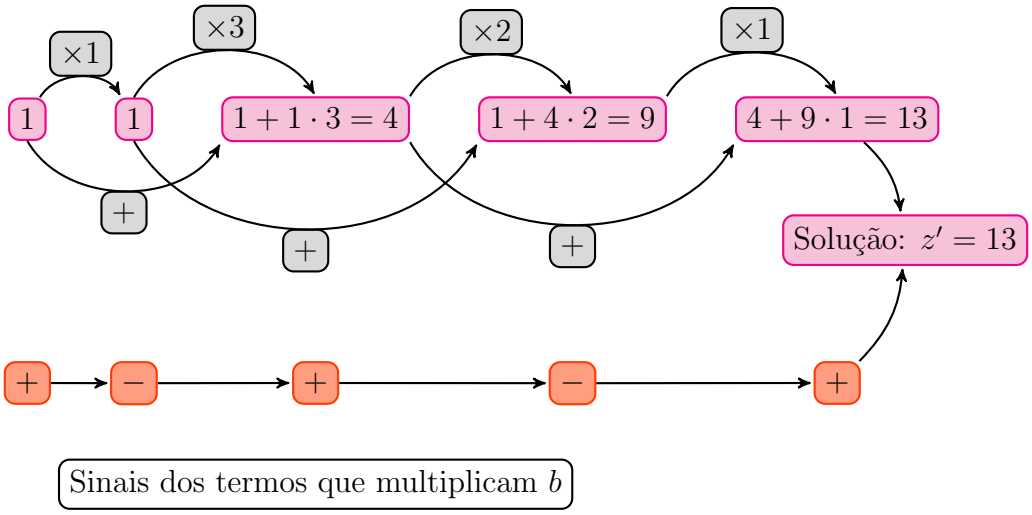

Figura 7: Modelo esquemático para o cálculo de z' da solução particular da EDL $35x + 97z = 1$ a partir dos valores dos quocientes obtidos da aplicação repetida do Lema de Euclides 2.5 .

Assim, obtemos a solução $(x', z') = (-36, 13)$ para $35x + 97z = 1$. A solução de $35x - 97y = 1$ para $z = -y$, é dada por $(x', y') = (x', -z') = (-36, -13)$. Por fim, como a equação original é $35x - 97y = 5$, basta que a multipliquemos por 5, isto é: $35 \cdot (-36) - 97 \cdot (-13) = 1 \overset{\times 5}{\Rightarrow} 35 \cdot (-180) - 97 \cdot (-65) = 5$. Assim, temos por solução particular de $35x - 97y = 5$, o par $(x', y') = (-180, -65)$.

Outros exemplos envolvendo a obtenção de solução particular de EDLs do tipo $ax + by = c$ podem ser encontrados em [16] e [17].

4 Considerações finais

Uma vez que a maioria dos livros-texto empregados no estudo de EDLs do tipo $ax + by = c$ apresentam uma abordagem única para obtenção da solução particular, percebe-se que um aprimoramento relevante para o ensino do tópico é incluir apresentações alternativas. Neste trabalho, com base em [15] e [35], detalhamos e discutimos uma alternativa para obtenção da solução particular para esse grupo de Equações Diofantinas: a *Abordagem por Substituição Progressiva* do Algoritmo de Euclides. A ref. [35] menciona que a abordagem tradicionalmente empregada é uma metodologia 'as cegas' até que se obtenha a relação final, onde aparecem os coeficientes inteiros desejados de a e b. Assim, a *Abordagem por Substituição Progressiva*, que pode ser de-

senhada exclusivamente a partir dos quocientes da Divisão Euclidiana, oferece algumas vantagens [15]. Um argumento atrativo refere-se a maior facilidade de computação, manual ou para programas de algoritmo [15]. Neste sentido, [35] menciona a vantagem da abordagem na escrita de programas computacionais, pois requer menor alocação de memória e permite uma implementação mais simplificada comparativamente à abordagem tradicional. Dessa forma, provemos no Apêndice 6B uma implementação em Matlab do algoritmo de cálculo da solução particular via *Abordagem por Substituição Progressiva*.

Por outro lado, o emprego da estratégia pressupõe que se tenham avaliado e compreendido as razões das operações requeridas para o cálculo da solução particular. Assim, a proposta aqui discutida mostra-se como um complemento, pois acresce ao estudo de EDLs uma nova abordagem para o cálculo da solução particular.

Agradecimentos

Os autores agradecem aos revisores anônimos pelas contribuições para aprimoramento da versão final do manuscrito. Os autores agradecem igualmente ao editor-chefe pela possibilidade de prover as correções e realizar nova submissão e ao CNPq pelo apoio financeiro (Processo: 305476/2020-3).

Referências

[1] Alves, Lucinda F. Aplicações de equações Diofantinas e um passeio pelo último teorema de Fermat. (Dissertação de Mestrado). Universidade Federal de Goiás. (2017). http://repositorio.bc.ufg.br/tede/handle/tede/8104.

[2] Borges, Fábio V. A. Equações diofantinas lineares em duas incógnitas e suas aplicações. (Dissertação de Mestrado). Universidade Federal de Goiás. (2013). http://repositorio.bc.ufg.br/tede/handle/tede/3124.

[3] Boyer, Carl B.; Merzbach, Uta C. História da matemática. Editora Blucher. (2019).

[4] Campbell, Stephen R.; Zazkis, Rina. Toward number theory as a conceptual field. *In*: Campbell, Stephen R.; Zazkis, Rina. (org.). Learning and Teaching Number Theory: Research in Cognition and Instruction. Boston: Ablex Publishing. **2** (2002), 1-14.

[5] Chang, Raymond. Química geral. AMGH Editora. (2009).

[6] Carrer, Janete J.; Doering, Luisa R.; Rippol, Cydara C. A divisão Euclidiana e seu resto desde os anos iniciais. III Simpósio Nacional do Professor de Matemática. (2018).

[7] Chou, Tsu-Wu J.; Collins, George E. Algorithms for the solution of systems of linear Diophantine equations. SIAM Journal on computing. **11** (2000), no. 4, 687-708. https://doi.org/10.1137/0211057.

[8] Courant, Richard; Robbins, Herbert. Che cos' è la matematica?: introduzione elementare ai suoi concetti e metodi. Bollati Boringhieri. (1971).

[9] Dickson, Leonard E. History of the theory of numbers: Diophantine Analysis. Courier Corporation. (2013).

[10] Domingues, Hygino H. Fundamentos de aritmética. Editora da UFSC. (2009).

[11] Duarte, José R. Equações diofantinas associadas a funções aritméticas. (Dissertação de Mestrado). Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP-SP). (2020). http://hdl.handle.net/11449/194411.

[12] Freitas, Carlos W. A. Equações diofantinas. (Dissertação de Mestrado). Universidade Federal do Ceará. (2015). http://www.repositorio.ufc.br/handle/riufc/12990.

[13] Gilbert, Willliam J.; Pathria, Anu. Linear diophantine equations. Preprint. (1990). http://www.math.uwaterloo.ca/~wgilbert/Research/GilbertPathria.pdf.

[14] Hefez, Abramo. Elementos de aritmética. Sociedade Brasileira de Matemática. (2006).

[15] Man, Yiu-Kwong. A forward approach for solving linear Diophantine equation.International Journal of Mathematical Education in Science and Technology. **51** (2020), no. 8, 1284-1288. https://doi.org/10.1080/0020739X.2020.1745915.

[16] Man, Yiu-Kwong. A top-down approach for solving linear Diophantine equation. In:Lecture Notes in Engineering and Computer Science: Proceedings of the World Congress on Engineering 2019. (2019). 3-5. http://www.iaeng.org/publication/WCE2019/WCE2019_pp11-13.pdf.

[17] Man, Yiu-Kwong. A Simple Approach for Solving Linear Diophantine Equation in Two Variables. In: Transactions on Engineering Technologies. Springer, Singapore. (2021), 83-87. https://doi.org/10.1007/978-981-15-8273-8_7.

[18] Oliveira, Sérgio A. Uma exploração didática das equações diofantinas lineares de duas e três incógnitas com estudantes de curso de licenciatura em matemática. (Dissertação de Mestrado). Pontifícia Universidade Católica de Minas Gerais. http://www.biblioteca.pucminas.br/teses/EnCiMat_OliveiraSA_1.pdf.

[19] Pommer, Wagner M. Equações diofantinas lineares: um tema articulador de estratégias no ensino básico. Revista Caderno Pedagógico. **9** (2012a), no. 1, 137-154. http://www.meep.univates.br/revistas/index.php/cadped/article/view/851.

[20] Pommer, Wagner M. Equações diofantinas lineares: um viés histórico para introduzir estratégias de resoluação em problemas de indeterminação linear. (2012b). https://www.ufsm.br/app/uploads/sites/534/2020/03/CC_Pommer_Wagner.pdf.

[21] Pommer, Wagner M. Transição Aritmética&Álgebra: Contribuições da temática das Equações Diofantinas Lineares. PONTE. **11** (2005).

[22] Pommer, Wagner M. A Engenharia Didática em sala de aula: Elementos básicos e uma ilustração envolvendo as Equações Diofantinas Lineares. São Paulo. (2013).

[23] Pommer, Wagner M. Equações diofantinas lineares: um desafio motivador para alunos do ensino médio. (Dissertação de Mestrado). Pontifícia Universidade Católica de São Paulo. (2008). https://tede2.pucsp.br/handle/handle/11292.

[24] Richit, Luiz A.; Pasa, Bárbara C. O programa de iniciação científica da obmep e apredizagem em aritmética: uma perspectiva a partir da teoria dos registros semióticos. V Seminário de Pesquisa e Extensão. **5** (2015).

[25] Richit, Luiz A.; Pasa, Bárbara. C.; Moretti, Méricles T. Ensino e aprendizagem de aritmética: reflexões com base na teoria dos registros de representação semiótica. XII Encontro Nacional de Educação Matemática. (2016).

[26] Rosen, Kenneth H. Elementary number theory. London: Pearson Education. (2011).

[27] Savóis, Josias N. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. (Dissertação de Mestrado). Universidade Federal do Rio Grande (FURG-RS). (2014). http://repositorio.furg.br/handle/1/6641.

[28] Silva, Adriano V. Uso das equações diofantinas lineares no ensino fundamental. (Dissertação de Mestrado). Universidade Federal de Alagoas (UFAL-AL). (2013). http://www.repositorio.ufal.br/handle/riufal/2431.

[29] Silva, Diego A.; Brito, Arnaldo S.; De Sousa, Valdirene G. Equações Diofantinas Lineares: um estudo com estudantes do 1o ano do Ensino Médio. REMAT: Revista Eletrônica da Matemática. **6** (2020), no. 2, e2009-e2009. https://doi.org/10.35819/remat2020v6i2id3839.

[30] Silva, Rivanildo G. Congruência e equações diofantinas: Algumas aplicações. (Dissertação de Mestrado). Universidade Estadual da Paraíba, Campo Grande.(2018). http://tede.bc.uepb.edu.br/jspui/handle/tede/3221.

[31] Singh, Simon. *O último teorema de Fermat*. 1999.

[32] Sousa, Elvis M. R. Equações diofantinas lineares: uma abordagem para o ensino médio utilizando jogo matemático. (Dissertação de Mestrado). Universidade Federal Rural do Semi-Árido (UFERSA). (2019). http://repositorio.ufersa.edu.br/handle/prefix/5395.

[33] Souza, Romario S. Equações diofantinas lineares, quadráticas e aplicações. (Dissertação de Mestrado). Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP-SP). (2017). http://hdl.handle.net/11449/149949.

[34] Stark, Harold M. An introduction to number theory. Cambridge, MA: Mit Press. (1978).

[35] Stevens, Gary E. Forward and backward with Euclid. The Two-Year College Mathematics Journal. **12** (1981), no 5, 302-306. http://www.jstor.org/stable/3027301.

5 Apêndice A: Código para o cálculo do MDC

Produzido pelos autores, escrito em Matlab versão 2018Ra.

```
function [mdc]=MDC(a0,b0)
% Lembre-se de que 'a' e 'b' devem pertencer aos naturais e a e b não nulos
a=abs(a0);
```

```
b=abs(b0);
aux=1;

if (a<b)
    A=b;
    B=a;
else
    A=a;
    B=b;
end

if (a==b)
    mdc=a;
    r=0;
else
    r=a+b;
end


% Aplicacao recorrente do Algoritmo de Euclides da Divisao
while (r~=0)

    while (r>=B)
        r=A-B*aux;
        aux=aux+1;
        if (r~=0)
            mdc=r;
        end
    end
    A=B;
    B=r;
    aux=1;
end

 fprintf('\nmdc(%d,%d)=%d.\n',a0,b0,mdc);
 fprintf('\ngcd(%d,%d)=%d.\n',a0,b0,mdc);

```

```
end
```

6 Apêndice B: Código para o cálculo da solução particular da EDL via Abordagem Progressiva

Produzido pelos autores, escrito em Matlab versão 2018Ra.
Observar que se a e b são múltiplos entre si, mesmo a equação $ax+by=c$ sendo solúvel, a solução não pode ser computada pela *Abordagem por Substituição Progressiva*. Como o método emprega os quocientes das divisões em que o resto é diferente de zero, no caso de a e b mútiplos, não havendo nenhuma linha das divisões euclidianas com resto diferente de zero (i.e, decorre diretamente que $a = bk + 0$ ou $b = at + 0$, com $t, k \in \mathbb{Z}$), a abordagem aqui detalhada não pode ser empregada.

```
function  ASP(a,b,c)
% Encontra a solução particular de ax+by=c com a,b,c INTEIROS
% Calcular o MDC(a,b)
a0=abs(a);
b0=abs(b);

if (a0<b0)
    A=b0;
    B=a0;
    Aux=b0;
    Baux=a0;
else
    A=a0;
    B=b0;
    Aux=a0;
    Baux=b0;
end
r=a0;

% Aplicacao recorrente do Algoritmo de Euclides da Divisao
while (r~=0)
    aux=0;
    while (r>=B)
        r=A-B*aux;
```

```
25          aux=aux+1;
26          if (r~=0)
27              mdc=r;
28          end
29      end
30      A=B;
31      B=r;
32  end
33
34  fprintf('\nMDC(%d,%d) = %d\n',a,b,mdc);
35
36
37  if (rem(Aux,Baux)==0)
38      if (rem(abs(c),mdc)~=0)
39      fprintf('\nComo %d não divide %d a equação não tem solução
            nos inteiros.\n', mdc,c);
40      else
41      fprintf('\nOs valores de a=%d e b=%d são múltiplos entre
            si. ASP não roda essa circunstância. \nConsidere
            verificar se a equação pode ser simplificada.\n', a,b);
42      end
43  else
44
45  % Resolver a EDL ax+by=c
46  if rem(c, mdc)==0
47  fprintf('\nComo %d divide %d a equação tem solução nos
      inteiros.\n', mdc,c);
48
49  %Algoritmo para determinar os quocientes
50  j=1; q=0;
51
52      if(a0>=b0)
53          a1=a0;
54          b1=b0;
55      else
56          a1=b0;
57          b1=a0;
58      end
```

```
    r=b1;
    while (r~=0)
     r=rem(a1,b1);
     if (j==1)
          q=(a1-r)/b1;
     elseif (r==0)
     else
     q=[q,(a1-r)/b1];
     end
     j=j+1;
     a1=b1;
     b1=r;
    end

n=length(q);
%Algoritmo para computar a solução particular via ASP

x=zeros(1,n+2);
x(2)=1;
y=zeros(1,n+2);
y(1)=0;
y(2)=0;
y(3)=1;

for i=1:n
     x(i+2)=x(i)+q(i)*x(i+1);
end
for i=2:n
     y(i+2)=y(i)+q(i)*y(i+1);
end

fi=c/mdc;
X=x(n+2)*(-1)^(n+2);
X=X*fi;
Y=y(n+2)*(-1)^(n+1);
Y=Y*fi;

if (a0>b0)
```

```
97      Y=Y*(a/a0);
98      X=X*(b/b0);
99  fprintf('\nA solução particular via ASP é (x,y)=(%d,%d).\n',Y,
        X);
100 elseif(a0==b0)
101     X=c/a;
102     Y=0;
103 fprintf('\nA solução particular é (x,y)=(%d,%d).\n',X,0);
104 else
105     Y=Y*(b/b0);
106     X=X*(a/a0);
107 fprintf('\nA solução particular via ASP é (x,y)=(%d,%d).\n',X,
        Y);
108 end
109
110 else
111 fprintf('\nComo %d não divide %d, então a equação não tem
        solução nos inteiros. \n',mdc,c);
112 end
113 end
114 end
```