



# Técnicas para resolução de equações Diofantinas lineares

Egídio Costa Filho 

Márcio Lúcio Rodrigues 

Orlando Eduardo da Silva Ferri 

## Resumo

Diferentes estratégias matemáticas podem ser utilizadas para resolver o mesmo problema e é salutar que o aluno experimente múltiplas técnicas de enfrentamento de situações-problema, entendendo assim que a matemática é dinâmica. Com base nessa premissa, este artigo traz um estudo de equações diofantinas lineares apresentando três estratégias de resolução, em que duas delas possuem em essência a teoria do maior divisor comum entre dois inteiros, e a outra trata basicamente de divisões sucessivas.

**Palavras-chave:** Equações Diofantinas Lineares; Máximo Divisor Comum; Divisões Sucessivas.

## Abstract

Different mathematical strategies can be used to solve the same problem and it is salutary that the student experiences multiple techniques for facing problem situations, thus understanding that mathematics is dynamic. Based on this premise, this paper brings a study of linear Diophantine equations presenting three resolution strategies, in which two of them have in essence the theory of the greatest common divisor between two integers and the other deals basically with successive divisions.

**Keywords:** Linear Diophantine Equations; Greatest Common Divisor; Successive Divisions.

## 1. Introdução

Abordar equações diofantinas lineares na educação básica proporciona uma excelente oportunidade para explorar estratégias diversificadas de aprendizagem envolvendo a resolução de situações-problemas, estimulando a autonomia e a criatividade do aluno. Oliveira (2006), [5], argumenta que muitos pesquisadores em educação matemática têm enfatizado que trabalhar a matemática discreta na educação básica contribui para uma formação mais sólida do aluno, onde é possível desenvolver ideias fundamentais tais como investigar, conjecturar, argumentar etc., pois os objetos examinados (números) são familiares aos estudantes.

Serão apresentadas três técnicas de resolução de equações diofantinas lineares como parte de estratégias diversificadas para a resolução de situações-problemas. Primeiramente, serão desenvolvidos

alguns conceitos teóricos relativos às equações diofantinas lineares, bem como a condição para que tais equações tenham solução no conjunto dos números inteiros.

O método de resolução 1, que é o método mais encontrado nos livros que abordam o assunto, como [1], [3] e [4], baseia-se no fato de que, a partir de qualquer solução particular encontrada, é possível escrever expressões matemáticas para obter outras soluções da equação. Para encontrar uma solução particular, será utilizado o algoritmo de Euclides.

O método de resolução 2 apresenta uma forma alternativa para encontrar uma solução particular de equações diofantinas lineares explorando de forma mais abrangente o algoritmo de Euclides; nesse método é discutido o que foi apresentado por Carneiro (1998), em [2].

Por fim, é apresentado o método 3 de resolução de equações diofantinas lineares, método esse que utiliza basicamente divisões sucessivas e manipulação matemática simples, consistindo em uma variação do método da pulverização utilizado por Euler em seu livro *Álgebra*, de 1970, [6].

Ao longo do texto, a partir de uma situação problema será exemplificada uma aplicação desses três métodos de resolução, assim o leitor poderá analisar as peculiaridades de cada método. Nas considerações finais, há uma seleção de problemas considerados interessantes pelos autores.

## 2. Equações Diofantinas Lineares

Uma equação diofantina linear de duas variáveis é uma equação do tipo

$$ax + by = c, \tag{1}$$

em que  $a$ ,  $b$  e  $c$  são números inteiros,  $x$  e  $y$  são incógnitas a serem determinadas no conjunto dos números inteiros, e os coeficientes  $a$  e  $b$  não são ambos nulos.

Segundo [3]:

*o primeiro a considerar problemas desse tipo, isto é, equações indeterminadas que eventualmente admitem soluções, foi Diophanto de Alexandria (em torno de 250 d.C.); porém, ele procurava soluções racionais. De qualquer forma, esse tipo de equações associa-se tradicionalmente ao seu nome e, por extensão, até hoje o adjetivo “diofantino” é usado para indicar problemas relativos a números inteiros. ([3], p97)*

Muitos problemas do cotidiano que podem ser modelados matematicamente pela equação (1) só fazem sentido para soluções inteiras. A equação  $6x + 8y = 14$  é um exemplo de equação diofantina, e de imediato é possível verificar que o par  $x_0 = 1$  e  $y_0 = 1$  é uma solução, pois substituindo os valores de  $x_0$  e  $y_0$  na equação, obtém-se:

$$6x + 8y = 6.1 + 8.1 = 6 + 8 = 14.$$

Já a equação  $6x + 8y = 15$  é um exemplo de equação diofantina que não possui solução. Sendo  $I = \{6x + 8y \mid x, y \in \mathbb{Z}\}$  o conjunto de todos os valores assumidos pelo primeiro membro dessa equação, nota-se que os valores do conjunto  $I$  são todos pares, portanto, nunca igual a 15, logo, a equação  $6x + 8y = 15$  não tem solução.

## 2.1. Condição para que a equação $ax + by = c$ possua solução inteira.

É útil de antemão saber identificar em que condição a equação (1) possui solução. Para enunciar e justificar tal condição, será utilizado o teorema de Bézout cuja demonstração será feita a partir do conceito de conjunto ideal.

**Definição 1.** Um conjunto não vazio  $J$  de números inteiros diz-se um ideal de  $\mathbb{Z}$  se:

- $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J$ ;
- $\alpha \in J, k \in \mathbb{Z} \Rightarrow \alpha k \in J$ .

E ainda, considerando  $J \neq 0$ . Seja  $m$  o menor inteiro positivo que pertence ao conjunto  $J$ , todos os elementos do conjunto  $J$  são múltiplos de  $m$ , ou seja,  $J = m\mathbb{Z}$ , a demonstração dessa afirmação pode ser encontrada em [3].

**Teorema 1. (Teorema de Bézout)** *Sejam  $a, b$  e  $d = \text{mdc}(a, b)$ . Então existem números inteiros  $s$  e  $t$  tais que  $d = sa + tb$*

*Demonstração.* Considere o conjunto  $J = \{xa + yb \mid x, y \in \mathbb{Z}\}$ . Veja que  $J$  é um ideal de  $\mathbb{Z}$ , pois pela definição (1), sendo  $\alpha$  e  $\beta$  elementos de  $J$ , com  $\alpha = x_1a + y_1b$  e  $\beta = x_2a + y_2b$ , e  $k \in \mathbb{Z}$ , tem-se:

- $\alpha + \beta = x_1a + y_1b + x_2a + y_2b = (x_1 + x_2)a + (y_1 + y_2)b \in J$ ;
- $k\alpha = k(x_1a + y_1b) = (kx_1)a + (ky_1)b \in J$ .

Ainda pela definição (1),  $J$  possui um menor inteiro positivo tal que todos os demais elementos de  $J$  são múltiplos desse elemento. Sendo  $m = sa + tb$  esse menor elemento, pode-se concluir que  $m$  pertence ao conjunto de divisores de  $a$  e  $b$ , ou seja,  $m \in D(a, b)$ , pois  $a \in J$ , (basta tomar  $s = 1$  e  $t = 0$ ) e  $b \in J$ , (basta tomar  $s = 0$  e  $t = 1$ ), veja:

$$\left. \begin{array}{l} a = 1a + 0b \\ b = 0a + 1b \end{array} \right\} a \text{ e } b \in J,$$

e como qualquer elemento de  $J$  é múltiplo de  $m$ ,  $m$  divide  $a$  e  $m$  divide  $b$ .

Seja  $d$  o máximo divisor comum de  $a$  e  $b$ ,  $d = \text{mdc}(a, b)$ , logo  $d \geq m$ . Dividindo ambos os lados da equação  $m = sa + tb$  por  $d$ , tem-se:

$$\frac{m}{d} = s\frac{a}{d} + t\frac{b}{d}. \quad (2)$$

Como o segundo membro da equação (2) é um número inteiro, o primeiro membro também é, portanto  $d$  divide  $m$ , logo  $d \leq m$ . Uma vez que  $d \geq m$  e  $d \leq m$ , conclui-se que  $m = d$  e fica demonstrado o teorema de Bézout.  $\square$

**Proposição 1.** *A equação diofantina (1) admite solução se, e somente se,  $\text{mdc}(a, b)$  divide  $c$*

*Demonstração.* Tomando por hipótese que  $x = x_0$  e  $y = y_0$  é uma solução da equação (1), ou seja,  $ax_0 + by_0 = c$ . Sendo,  $d$  o máximo divisor comum de  $a$  e  $b$ , existem números inteiros  $\alpha$  e  $\beta$  tais que  $a = \alpha d$  e  $b = \beta d$ , assim:

$$\begin{aligned}
 ax_0 + by_0 &= c \\
 (\alpha d)x_0 + (\beta d)y_0 &= c \\
 d(\alpha x_0 + \beta y_0) &= c.
 \end{aligned}$$

Fazendo  $\rho = \alpha x_0 + \beta y_0 \in \mathbb{Z}$ , tem-se  $d\rho = c$ , portanto,  $d = \text{mdc}(a, b)$  divide  $c$ .

Reciprocamente, se  $d = \text{mdc}(a, b)$  divide  $c$ , existe um inteiro  $\lambda$  tal que  $c = \lambda d$ . Além disso, pelo teorema (1), existem os inteiros  $s$  e  $t$  tais que  $d = sa + tb$ . Multiplicando essa última equação por  $\lambda$ , tem-se:

$$\begin{aligned}
 \lambda d &= \lambda sa + \lambda tb \\
 c &= a(\lambda s) + b(\lambda t).
 \end{aligned}$$

Desse modo,  $x = \lambda s$  e  $y = \lambda t$  é solução da equação (1). □

### 3. Método de resolução 1

Esse método de resolução baseia-se no fato de que, a partir de qualquer solução particular da equação (1), é possível escrever expressões para obter todas as suas soluções.

**Teorema 2.** *Seja o par ordenado  $x = x_0$  e  $y = y_0$  uma solução particular da equação diofantina linear (1), e  $d = \text{mdc}(a, b)$  que divide  $c$ , então todas as soluções da equação são do tipo:*

$$x = x_0 + \frac{b}{d}k \quad \text{e} \quad y = y_0 - \frac{a}{d}k,$$

com  $k$  variando no conjunto dos números inteiros.

*Demonstração.* Sendo o par  $x = x_0$  e  $y = y_0$  solução da equação, então:

$$\begin{aligned}
 ax + by &= ax_0 + by_0 \\
 ax - ax_0 &= by_0 - by \\
 a(x - x_0) &= b(y_0 - y).
 \end{aligned} \tag{3}$$

Como  $d$  divide  $a$  e  $d$  divide  $b$ , existem números inteiros  $a_1$  e  $b_1$ , tais que:

$$a = a_1 d \quad \text{e} \quad b = b_1 d.$$

Ocorre que  $a_1$  e  $b_1$  são primos entre si, pois escrevendo  $a_1 = \frac{a}{d}$  e  $b_1 = \frac{b}{d}$ , tem-se que:

$$\text{mdc}(a_1, b_1) = \text{mdc}\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\text{mdc}(a, b)}{d} = \frac{d}{d} = 1.$$

Substituindo  $a = a_1 d$  e  $b = b_1 d$  na equação (3) e dividindo ambos os lados por  $d$ :

$$a(x - x_0) = b(y_0 - y) \quad (4)$$

$$a_1 d(x - x_0) = b_1 d(y_0 - y)$$

$$a_1(x - x_0) = b_1(y_0 - y). \quad (5)$$

Como  $a_1$  e  $b_1$  são primos entre si, pela equação (5), conclui-se que  $b_1$  divide  $x - x_0$  e, portanto, existe um número inteiro  $k$  tal que  $x - x_0 = b_1 k$ . Substituindo  $b_1 = \frac{b}{d}$  nesta última expressão, tem-se que:

$$x - x_0 = \frac{b}{d}k \quad (6)$$

$$x = x_0 + \frac{b}{d}k. \quad (7)$$

E, finalmente, substituindo (6) em (4):

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

$$a \frac{b}{d}k = b(y_0 - y)$$

$$\frac{a}{d}k = y_0 - y$$

$$y = y_0 - \frac{a}{d}k. \quad (8)$$

De fato, sendo  $x = x_0$  e  $y = y_0$  solução particular da equação (1),  $x = x_0 + \frac{b}{d}k$  e  $y = y_0 - \frac{a}{d}k$ , com  $k \in \mathbb{Z}$ , é solução geral da equação (1), e isso pode ser verificado substituindo (7) e (8) no primeiro membro da equação (1), veja:

$$\begin{aligned}
 ax + by &= a \left( x_0 + \frac{b}{d}k \right) + b \left( y_0 - \frac{a}{d}k \right) \\
 &= ax_0 + a \frac{b}{d}k + by_0 - b \frac{a}{d}k \\
 &= ax_0 + by_0 \\
 &= c.
 \end{aligned}$$

□

**Problema 1.** Considere a seguinte situação hipotética: Uma empresa deseja investir exatamente de R\$ 100000,00 na compra de dois modelos distintos de celulares, sabe-se que os preços dos equipamentos são respectivamente R\$ 1300,00 e R\$ 480,00. Escreva as possibilidades de compras que essa empresa dispõe.

Seja  $x$  a quantidade que será comprada do modelo de celular que custa R\$ 1300,00 e  $y$  a quantidade que será comprada do modelo de celular que custa R\$ 480,00. Para resolver esse problema precisam-se determinar as soluções da equação  $1300x + 480y = 100000$ . Simplificando essa equação, obtém-se a equação equivalente

$$65x + 24y = 5000. \quad (9)$$

Os coeficientes da equação (9) são 65 e 24; pelo Algoritmo de Euclides<sup>1</sup> é possível determinar o  $\text{mdc}(65, 24)$ . A tabela (1) sintetiza as divisões necessárias no Algoritmo de Euclides.

	Dividendo	Divisor	Quociente	Resto
1 <sup>a</sup> divisão	65	24	2	17
2 <sup>a</sup> divisão	24	17	1	7
3 <sup>a</sup> divisão	17	7	2	3
4 <sup>a</sup> divisão	7	3	2	1
5 <sup>a</sup> divisão	3	1	3	0

Tabela 1: Divisões sucessivas do Algoritmo de Euclides.

Observando a tabela (1), verifica-se que a última divisão com resto diferente de 0 foi a 4<sup>a</sup> divisão, assim, o resto da 4<sup>a</sup> divisão é o  $\text{mdc}$  procurado e, portanto,  $\text{mdc}(65, 24) = 1$ . Como o número 1 é divisor de qualquer número, segue pela proposição (1) que a equação (9) tem solução.

É comum apresentar essas divisões pelo diagrama ilustrado na tabela (2)

	2	1	2	2	3
65	24	17	7	3	(1)
	17	7	3	1	0

Tabela 2: Diagrama: Algoritmo de Euclides.

Pelo Teorema (1), dado que  $\text{mdc}(65, 24) = 1$ , existem números inteiros  $s$  e  $t$  tais que  $1 = 65s + 24t$ . Para encontrar os inteiros  $s$  e  $t$ , utilizam-se as equações geradas a partir das divisões sucessivas realizadas no Algoritmo de Euclides. Por exemplo, pela tabela (1) na 4<sup>a</sup> divisão, tem-se 7 dividido por 3, obtém-se quociente 2 e resto 1, logo  $1 = 7 - 2 \cdot 3$ . Com exceção da 5<sup>a</sup> divisão cujo resto é 0, obtém-se as seguintes equações:

$$1 = 7 - 2 \cdot 3 \quad \text{gerada pela 4<sup>a</sup> divisão} \quad (10)$$

$$3 = 17 - 2 \cdot 7 \quad \text{gerada pela 3<sup>a</sup> divisão} \quad (11)$$

$$7 = 24 - 1 \cdot 17 \quad \text{gerada pela 2<sup>a</sup> divisão} \quad (12)$$

$$17 = 65 - 2 \cdot 24 \quad \text{gerada pela 1<sup>a</sup> divisão} \quad (13)$$

Substituindo a equação (11) na equação (10):

<sup>1</sup>O leitor pode encontrar um estudo do Algoritmo de Euclides em [4, p. 53], ou em [3, p. 71].

$$\begin{aligned}
 1 &= 7 - 2.3 \\
 &= 7 - 2(17 - 2.7) \\
 &= 7 - 2.17 + 4.7 \\
 &= 5.7 - 2.17.
 \end{aligned} \tag{14}$$

Substituindo a equação (12) na equação (14):

$$\begin{aligned}
 1 &= 5.7 - 2.17 \\
 &= 5.(24 - 1.17) - 2.17 \\
 &= 5.24 - 5.17 - 2.17 \\
 &= 5.24 - 7.17.
 \end{aligned} \tag{15}$$

Substituindo a equação (13) na equação (15):

$$\begin{aligned}
 1 &= 5.24 - 7.17 \\
 &= 5.24 - 7(65 - 2.24) \\
 &= 5.24 - 7.65 + 14.24 \\
 &= 65(-7) + 24.(19).
 \end{aligned} \tag{16}$$

Pela equação (16), conclui-se que  $s = -7$  e  $t = 19$ , cuja existência já estava garantida pelo Teorema (1). Além disso, vale comentar que os valores de  $s$  e  $t$  não são únicos. Para obter uma solução particular da equação (9) do problema (1), basta multiplicar ambos os lados da equação (16) por 5000, assim:

$$\begin{aligned}
 65(-7) + 24(19) &= 1 \\
 65(-35000) + 24(95000) &= 5000.
 \end{aligned} \tag{17}$$

Pelo teorema (2), a solução geral da equação (9) pode ser dada por:

$$x = -35000 + 24k, \quad y = 95000 - 65k, \quad \text{com } (k \in \mathbb{Z}). \tag{18}$$

Como as soluções devem ser números inteiros e positivos, para que a variável  $x$  seja positiva,  $k > \frac{35000}{24}$ . Para que a variável  $y$  seja positiva,  $k < \frac{95000}{65}$ . Os únicos valores de  $k$  que satisfazem essas duas inequações são  $k_1 = 1459$ ,  $k_2 = 1460$  e  $k_3 = 1461$ . Assim:

Portanto, tem-se três soluções distintas para o problema (1):

- 16 celulares que custam R\$ 1300,00 cada e 165 celulares que custam R\$ 480,00 cada.
- 40 celulares que custam R\$ 1300,00 cada e 100 celulares que custam R\$ 480,00 cada.
- 64 celulares que custam R\$ 1300,00 cada e 35 celulares que custam R\$ 480,00 cada.

k	x	y
1459	16	165
1460	40	100
14601	64	35

Tabela 3: Soluções inteiras positivas.

#### 4. Método de resolução 2

Agora será resolvida a equação (9) do Problema 1 usando o Algoritmo de Euclides e o Teorema 1 expondo passo a passo o procedimento de um dispositivo prático para determinar os valores de  $s$  e  $t$  a partir do maior divisor comum de dois números inteiros, apresentado por [2]:

**1º Passo:** *Primeiramente, preenche-se a coluna “n” de acordo com o número da linha. Em seguida, preenche-se a coluna “q” com os quocientes obtidos no algoritmo de Euclides, tabela (1), desprezando-se o último, que corresponde ao resto zero (no caso, o quociente igual a 3) na ordem contrária ao de seu aparecimento no algoritmo, e deixando-se em branco a primeira linha.*

n	q	s,t
1		
2	2	
3	2	
4	1	
5	2	

**2º Passo:** *Na coluna “s,t”, coloca-se o número 1 na primeira linha (é sempre 1 mesmo), e na segunda linha repete-se o valor do quociente da linha 2.*

n	q	s,t
1		1
2	2	2
3	2	
4	1	
5	2	

**3º Passo:** *Agora, a partir da terceira linha, cada valor seguinte da coluna “s,t” vai sendo obtido de acordo com a lei de formação:*

Conforme o esquema abaixo:

$$|(s, t)_n| = q_n \cdot |(s, t)_{n-1}| + |(s, t)_{n-2}|, \quad \text{para } n \leq 3.$$

O penúltimo valor da coluna “s,t” é o valor de  $|s|$  e o último valor da coluna “s,t” é o valor de  $|t|$ . Pela tabela (4), conclui-se que  $|s| = 7$  e  $|t| = 19$ . Para decidir sobre os sinais, aplica-se a seguinte regra: se o número de quocientes aproveitados (ou seja, o número de linhas preenchidas na coluna “q”) for ímpar, então  $s$  é positivo e  $t$  negativo; se o número de quocientes aproveitados for par,



<b>n</b>	<b>q</b>	<b>s,t</b>
1		<b>1</b>
2	2	<b>2</b>
3	2	$2 \times 2 + 1 = \mathbf{5}$
4	1	$1 \times 5 + 2 = \mathbf{7}$
5	2	$2 \times 7 + 5 = \mathbf{19}$

Tabela 4: Dispositivo prático para determinar os valores de s e t a partir do  $\text{mdc}(65, 24)$ .

ocorrerá o contrário, então s é negativo e t é positivo. Como no problema foram aproveitados quatro quocientes, segue que  $s = -7$  e  $t = 19$ .

Na maioria dos livros o processo envolve uma combinação linear dos valores a e b dados. Esse processo, que usa a expressão literal, é um tanto trabalhoso quando comparado ao dispositivo apresentado.

Dessa forma, obtém-se através do dispositivo acima, a equação (16):

$$65 \cdot (-7) + 24 \cdot (19) = 1.$$

A partir daqui segue a solução dada anteriormente.

#### 4.1. Dedução do dispositivo prático

Supondo  $|a| > |b| > 0$ , com  $a, b \in \mathbb{Z}$ , aplica-se o Algoritmo de Euclides:

<b>Quocientes</b>	$q_n$	$q_{n-1}$	$q_{n-2}$	$q_{n-3}$	$\dots$	$q_2$	$q_1$	$q_0$
<b>a</b>	<b>b</b>	$r_1$	$r_2$	$r_3$	$\dots$	$r_{n-2}$	$r_{n-1}$	<b><math>(r_n)</math></b>
<b>Restos</b>	$r_1$	$r_2$	$r_3$	$r_4$	$\dots$	$r_{n-1}$	$r_n$	<b>0</b>

obtendo as equações abaixo:

$$\begin{aligned}
 a &= q_n \cdot b + r_1 \\
 b &= q_{n-1} \cdot r_1 + r_2 \\
 r_1 &= q_{n-2} \cdot r_2 + r_3 \\
 r_2 &= q_{n-3} \cdot r_3 + r_4 \\
 &\vdots \\
 r_{n-3} &= q_2 \cdot r_{n-2} + r_{n-1} \\
 r_{n-2} &= q_1 \cdot r_{n-1} + r_n \\
 r_{n-1} &= q_0 \cdot r_n,
 \end{aligned}$$

de modo que  $r_n = \text{mdc}(a, b)$ .

Isolando os restos das equações obtidas pelo Algoritmo de Euclides, segue:

$$\begin{aligned}
 r_1 &= a - q_n \cdot b \\
 r_2 &= b - q_{n-1} \cdot r_1 \\
 r_3 &= r_1 - q_{n-2} \cdot r_2 \\
 r_4 &= r_2 - q_{n-3} \cdot r_3 \\
 &\vdots \\
 r_{n-1} &= r_{n-3} - q_2 \cdot r_{n-2} \\
 r_n &= r_{n-2} - q_1 \cdot r_{n-1}.
 \end{aligned}$$

Substituindo a primeira das equações, no caso  $r_1$ , na segunda equação referente ao  $r_2$ , obtém-se:

$$\begin{aligned}
 r_2 &= b - q_{n-1} \cdot (a - q_n \cdot b) \\
 r_2 &= b - q_{n-1} \cdot a + q_n \cdot q_{n-1} \cdot b \\
 \mathbf{r_2} &= \mathbf{a \cdot (-q_{n-1}) + b \cdot (1 + q_n \cdot q_{n-1})}.
 \end{aligned} \tag{19}$$

Note que  $r_2$  foi escrito como combinação linear de  $a$  e  $b$ .

Continuando o processo, substituindo  $r_1$  e o novo valor obtido de  $r_2$  em  $r_3$ , segue:

$$\begin{aligned}
 r_3 &= (a - q_n \cdot b) - q_{n-2} \cdot [a \cdot (-q_{n-1}) + b \cdot (1 + q_n \cdot q_{n-1})] \\
 r_3 &= a - q_n \cdot b + q_{n-1} \cdot q_{n-2} \cdot a - b \cdot (q_{n-2} + q_n \cdot q_{n-1} \cdot q_{n-2}) \\
 \mathbf{r_3} &= \mathbf{a \cdot (1 + q_{n-1} \cdot q_{n-2}) - b \cdot (q_n + q_{n-2} + q_n \cdot q_{n-1} \cdot q_{n-2})},
 \end{aligned}$$

que também nos dá  $r_3$  como combinação linear de  $a$  e  $b$ . O processo continua para os demais restos  $r_4, r_5, \dots, r_{n-1}$  até obter  $r_n = a \cdot s + b \cdot t$ . O que importa aqui é entender que os valores  $s$  e  $t$  que formam a combinação linear com  $a$  e  $b$  (vide Teorema de Bézout) dependem apenas dos quocientes  $q_n, q_{n-1}, q_{n-2}, \dots, q_2, q_1$ .

Em [2] é apresentada a tabela a seguir em que é possível analisar os valores que  $s$  e  $t$  assumem a cada novo quociente

$n$	$q_n$	$s_n$	$t_n$
1	$q_1$	1	$-q_1$
2	$q_2$	$-q_1$	$q_2 \cdot q_1 + 1$
3	$q_3$	$q_2 \cdot q_1 + 1$	$-q_3 \cdot (q_2 \cdot q_1 + 1) - q_1$
4	$q_4$	$-q_3 \cdot (q_2 \cdot q_1 + 1) - q_1$	$-q_4 \cdot [-q_3 \cdot (q_2 \cdot q_1 + 1) - q_1] + (q_2 \cdot q_1 + 1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Tabela 5: Dedução do dispositivo prático. Fonte:[2].

Observe que a tabela mostra-nos uma lei de formação dada por uma recorrência para  $n > 1$ :

$$\begin{cases} s_n &= t_{n-1} \\ t_n &= -q_n \cdot t_{n-1} + s_{n-1} \end{cases}, \tag{20}$$

com  $s_1 = 1$  e  $t_1 = -q_1$ .

Voltando no Problema 1 e ainda analisando o Algoritmo de Euclides, de acordo com a equação (1) bem como a Tabela (4), observe que:

$$\text{mdc}(65, 24) = \text{mdc}(24, 17) = \text{mdc}(17, 7) = \text{mdc}(7, 3) = 1.$$

Sendo assim,

$$\begin{aligned} \text{mdc}(7, 3) &= 7 \cdot (1) + 3 \cdot (-2) \\ \text{mdc}(17, 7) &= 17 \cdot (-2) + 7 \cdot (5) \\ \text{mdc}(24, 17) &= 24 \cdot (5) + 17 \cdot (-7) \\ \text{mdc}(65, 24) &= 65 \cdot (-7) + 24 \cdot (19). \end{aligned}$$

em que os valores realçados podem ser obtidos conforme a Tabela (5):

$n$	$q_n$	$s_n$	$t_n$
1	2	1	-2
2	2	-2	$-2 \cdot (-2) + 1 = 5$
3	1	5	$-1 \cdot (5) - 2 = -7$
4	2	-7	$-2 \cdot (-7) + 5 = 19$

### 5. Método de resolução 3

O método que será apresentado agora consiste basicamente na busca de soluções inteiras da equação (1) utilizando apenas divisões e manipulações matemáticas simples. Segundo [6], a utilização de divisões sucessivas para encontrar soluções inteiras de equações diofantinas lineares são variações do método da pulverização utilizado por Euler em seu livro *Álgebra*, de 1970.

Inicia-se o processo de resolução isolando na equação diofantina (1) a variável cujo coeficiente em valor absoluto é menor. Supondo  $|a| < |b|$ , isola-se a variável  $x$  para obter uma expressão para  $x$  em função de  $y$

$$\begin{aligned} ax + by &= c \\ x &= \frac{c - by}{a}. \end{aligned} \tag{21}$$

Se  $\frac{c - by}{a}$  for um número inteiro para todo  $y \in \mathbb{Z}$ , então  $x$  também será e, desta forma, a solução geral da equação (1) pode ser dada em função do parâmetro  $y$  por  $x = \frac{c - by}{a}$ , com  $y \in \mathbb{Z}$ .

Caso contrário, buscam-se soluções inteiras realizando algumas manipulações matemáticas. Como  $|a| < |b|$  na equação (21), para seguir o processo de resolução, há três casos a considerar de acordo com os possíveis valores do termo  $c$ , que são:  $|c| > |a|$ ,  $|c| = |a|$  e  $|c| < |a|$ .

### 5.1. Caso I, $|c| > |a|$

Caso  $|c| > |a|$  na equação (21), substitui-se  $c$  nessa equação por  $c_1 + c_2$  com a condição de  $c_1$  ser múltiplo de  $a$  e  $|c_2| < |a|$ , substitua também  $b$  por  $b_1 + b_2$ , com a condição de  $b_1$  ser múltiplo de  $a$  e  $|b_2| < |a|$ . A expressão resultante é:

$$\begin{aligned}
 x &= \frac{c - by}{a} \\
 &= \frac{(c_1 + c_2) - (b_1 + b_2)y}{a} \\
 &= \frac{c_1 - b_1y}{a} + \frac{c_2 - b_2y}{a}.
 \end{aligned} \tag{22}$$

Analisando a equação (22),  $\frac{c_1 - b_1y}{a} \in \mathbb{Z}$  para todo  $y \in \mathbb{Z}$ , já que  $c_1$  e  $b_1$  são múltiplos de  $a$ . Então, para que  $x$  seja sempre um número inteiro,  $c_2 - b_2y$  deve ser divisível por  $a$ , ou seja, deve existir um número  $u \in \mathbb{Z}$  tal que  $c_2 - b_2y = au$ . Escrevendo  $y$  em função de  $u$ :

$$\begin{aligned}
 c_2 - b_2y &= au \\
 y &= \frac{c_2 - au}{b_2}.
 \end{aligned} \tag{23}$$

Na equação (23), se  $c_2$  e  $a$  forem múltiplos de  $b_2$ ,  $y$  será um número inteiro para todo  $u \in \mathbb{Z}$ , e a equação (23) será uma expressão para  $y$  da solução geral de (1). Para obter uma expressão para  $x$  da solução geral, basta substituir a equação (23) na equação (21), conclui-se que a solução geral da equação (1), neste caso em função do parâmetro  $u$ , é dada por:

$$x = \frac{cb_2 - bc_2 + abu}{ab_2} \quad \text{e} \quad y = \frac{c_2 - au}{b_2}, \quad \text{com } u \in \mathbb{Z}.$$

Caso  $y$  na equação (23) não seja um número inteiro para todo  $u \in \mathbb{Z}$ , continua-se o processo das divisões sucessivas reescrevendo os termos do numerador da equação a fim de obter duas parcelas nas seguintes condições: uma das parcelas é divisível pelo denominador da fração, e a outra parcela é sempre formada por números tão menores quanto for possível expressar em valores absolutos. Dessa forma, o processo pode se repetir de maneira mais simples nessa segunda parcela, já que ela é composta por números menores em valores absolutos.

Continuando o processo das divisões sucessivas, na equação (23), sabe-se que  $|a| > |b_2|$ : quanto ao valor de  $c_2$ , há 3 situações que precisam ser consideradas:  $|c_2| > |b_2|$ ,  $|c_2| = |b_2|$  e  $|c_2| < |b_2|$ . A seguir, será analisada cada uma das três situações.

- **(Situação 1:)** Sendo  $|c_2| > |b_2|$  na equação (23), realizam-se duas substituições:  $c_2$  por  $c_3 + c_4$ , com a condição de  $c_3$  ser múltiplo de  $b_2$  e  $|c_4| < |b_2|$  e  $a$  por  $a_1 + a_2$  com a condição de  $a_1$  ser múltiplo de  $b_2$  e  $|a_2| < |b_2|$ , assim:

$$\begin{aligned}
 y &= \frac{c_2 - au}{b_2} \\
 &= \frac{(c_3 + c_4) - (a_1 + a_2)u}{b_2} \\
 &= \frac{c_3 - a_1u}{b_2} + \frac{c_4 - a_2u}{b_2}.
 \end{aligned} \tag{24}$$

Pela equação (24),  $\frac{c_3 - a_1u}{b_2} \in \mathbb{Z}$  para todo  $u \in \mathbb{Z}$ , já que  $c_3$  e  $a_1$  são múltiplos de  $b_2$ . Para que  $y$  seja sempre um número inteiro,  $c_4 - a_2u$  deve ser divisível por  $b_2$ , ou seja, deve existir um número  $v \in \mathbb{Z}$  tal que  $c_4 - a_2u = b_2v$ . Escrevendo  $u$  em função de  $v$ :

$$\begin{aligned}
 c_4 - a_2u &= b_2v \\
 u &= \frac{c_4 - b_2v}{a_2}.
 \end{aligned} \tag{25}$$

Na equação (25), se  $c_4$  e  $b_2$  forem múltiplos de  $a_2$ ,  $u$  será um número inteiro para todo  $v \in \mathbb{Z}$ . Dessa forma, substituindo a equação (25) na equação (23) obtém-se uma expressão para  $y$  da solução geral da equação (1). Para obter-se uma expressão da solução geral para  $x$ , basta substituir essa expressão geral de  $y$  na equação (21). Vale notar que a solução geral neste caso fica em função do parâmetro  $v \in \mathbb{Z}$ .

Caso  $u$  na equação (25) não seja um número inteiro para todo  $v \in \mathbb{Z}$ , continua-se o processo das divisões sucessivas.

- **(Situação 2:)** Sendo  $|c_2| = |b_2|$  na equação (23), realiza-se a substituição  $a$  por  $a_1 + a_2$  com a condição de  $a_1$  ser múltiplo de  $b_2$  e  $|a_2| < |b_2|$ , assim:

$$\begin{aligned}
 y &= \frac{c_2 - au}{b_2} \\
 &= \frac{c_2 - (a_1 + a_2)u}{b_2} \\
 &= \frac{c_2 - a_1u}{b_2} - \frac{a_2u}{b_2}.
 \end{aligned} \tag{26}$$

Pela equação (26),  $\frac{c_2 - a_1u}{b_2} \in \mathbb{Z}$  para todo  $u \in \mathbb{Z}$ , já que  $c_2$  e  $a_1$  são múltiplos de  $b_2$ . Para que  $y$  seja sempre um número inteiro,  $-a_2u$  deve ser divisível por  $b_2$ , ou seja, deve existir um número  $v \in \mathbb{Z}$  tal que  $-a_2u = b_2v$ . Escrevendo  $u$  em função de  $v$ :

$$\begin{aligned}
 -a_2u &= b_2v \\
 u &= \frac{-b_2v}{a_2}.
 \end{aligned} \tag{27}$$

Sendo  $b_2$  múltiplo de  $a_2$ ,  $u$  será um número inteiro para todo  $v \in \mathbb{Z}$ . Substituindo a equação (27) na equação (23) obtém-se uma expressão para  $y$  da solução geral da equação (1). Para

obter-se uma expressão da solução geral para  $x$ , basta substituir essa expressão geral de  $y$  na equação (21). Vale notar que a solução geral nesse caso fica em função do parâmetro  $v \in \mathbb{Z}$ .

Caso  $u$  na equação (27) não seja um número inteiro para todo  $v \in \mathbb{Z}$ , substitui  $b_2$  por  $b_3 + b_4$  na equação (27) com a condição de  $b_3$  ser múltiplo de  $a_2$  e  $|b_4| < |a_2|$  e continua o processo das divisões sucessivas.

- **(Situação 3:)** Sendo  $|c_2| < |b_2|$  na (23), realiza-se a substituição  $a$  por  $a_1 + a_2$  com a condição de  $a_1$  ser múltiplo de  $b_2$  e  $|a_2| < |b_2|$ , assim:

$$\begin{aligned}
 y &= \frac{c_2 - au}{b_2} \\
 &= \frac{c_2 - (a_1 + a_2)u}{b_2} \\
 &= \frac{-a_1u}{b_2} + \frac{c_2 - a_2u}{b_2}.
 \end{aligned} \tag{28}$$

Pela equação (28),  $\frac{-a_1u}{b_2} \in \mathbb{Z}$  para todo  $u \in \mathbb{Z}$ , já que  $a_1$  é múltiplo de  $b_2$ . Para que  $y$  seja sempre um número inteiro,  $c_2 - a_2u$  deve ser divisível por  $b_2$ , ou seja, deve existir um número  $v \in \mathbb{Z}$  tal que  $c_2 - a_2u = b_2v$ . Escrevendo  $u$  em função de  $v$ :

$$\begin{aligned}
 c_2 - a_2u &= b_2v \\
 u &= \frac{c_2 - b_2v}{a_2}.
 \end{aligned} \tag{29}$$

Sendo  $c_2$  e  $b_2$  múltiplo de  $a_2$ ,  $u$  será um número inteiro para todo  $v \in \mathbb{Z}$ . Substituindo a equação (29) na equação (23) obtém-se uma expressão para  $y$  da solução geral da equação (1). Para obter-se uma expressão da solução geral para  $x$ , basta substituir essa expressão geral de  $y$  na equação (21). Vale notar que a solução geral neste caso fica em função do parâmetro  $v \in \mathbb{Z}$ .

Caso  $u$  na equação (29) não seja um número inteiro para todo  $v \in \mathbb{Z}$ , continua-se o processo das divisões sucessivas.

## 5.2. Caso II, $|c| = |a|$

Caso  $|c| = |a|$  na equação (21), substitui  $b$  nessa mesma equação por  $b_1 + b_2$  com a condição de  $b_1$  ser múltiplo de  $a$  e  $|b_2| < |a|$ . A expressão resultante será:

$$\begin{aligned}
 x &= \frac{c - by}{a} \\
 &= \frac{c - (b_1 + b_2)y}{a} \\
 &= \frac{c - b_1y}{a} + \frac{-b_2y}{a}.
 \end{aligned} \tag{30}$$

Pela equação (30),  $\frac{c - b_1 y}{a} \in \mathbb{Z}$  para todo  $y \in \mathbb{Z}$ , já que  $c$  e  $b_1$  são múltiplos de  $a$ . Para que  $x$  seja sempre um número inteiro,  $-b_2 y$  deve ser divisível por  $a$ , ou seja, deve existir um número  $u \in \mathbb{Z}$  tal que  $-b_2 y = au$ . Escrevendo  $y$  em função de  $u$ :

$$\begin{aligned} -b_2 y &= au \\ y &= \frac{-au}{b_2}. \end{aligned} \quad (31)$$

Na equação (31), se  $a$  for múltiplo de  $b_2$ ,  $y$  será um número inteiro para todo  $u \in \mathbb{Z}$  e a equação (31) é uma expressão para  $y$  da solução geral de (1). Para obter-se uma expressão para  $x$  da solução geral, basta substituir a equação (31) na equação (21), e conclui-se que a solução geral da equação (1), neste caso em função do parâmetro  $u$ , é dada por:

$$x = \frac{b_2 c + abu}{ab_2} \quad \text{e} \quad y = \frac{-au}{b_2}, \quad \text{com } u \in \mathbb{Z}.$$

Caso  $y$  na equação (31) não seja um número inteiro para todo  $u \in \mathbb{Z}$ , continua-se o processo das divisões sucessivas.

### 5.3. Caso III, $|c| < |a|$

Caso  $|c| < |a|$  na equação (21), substitui  $b$  nessa mesma equação por  $b_1 + b_2$  com a condição de  $b_1$  ser múltiplo de  $a$  e  $|b_2| < |a|$ . A expressão resultante será:

$$\begin{aligned} x &= \frac{c - by}{a} \\ &= \frac{c - (b_1 + b_2)y}{a} \\ &= \frac{-b_1 y}{a} + \frac{c - b_2 y}{a}. \end{aligned} \quad (32)$$

Pela equação (32),  $\frac{-b_1 y}{a} \in \mathbb{Z}$  para todo  $y \in \mathbb{Z}$ , já que  $-b_1$  é múltiplo de  $a$ . Para que  $x$  seja sempre um número inteiro,  $c - b_2 y$  deve ser divisível por  $a$ , ou seja, deve existir um número  $u \in \mathbb{Z}$  tal que  $c - b_2 y = au$ . Escrevendo  $y$  em função de  $u$ :

$$\begin{aligned} c - b_2 y &= au \\ y &= \frac{c - au}{b_2}. \end{aligned} \quad (33)$$

Na equação (33), se  $c - a$  forem múltiplos de  $b_2$ ,  $y$  será um número inteiro para todo  $u \in \mathbb{Z}$  e a equação (33) é uma expressão para  $y$  da solução geral de (1). Para obter-se uma expressão para  $x$  da solução geral, basta substituir a equação (33) na equação (21), conclui-se que a solução geral da equação (1), neste caso em função do parâmetro  $u$ , é dada por:

$$x = \frac{b_2c - bc + abu}{ab_2} \quad \text{e} \quad y = \frac{c - au}{b_2}, \quad \text{com } u \in \mathbb{Z}.$$

Caso  $y$  na equação (33) não seja um número inteiro para todo  $u \in \mathbb{Z}$ , continua-se o processo das divisões sucessivas.

Basicamente, o método das divisões sucessivas vai se repetindo até encontrar um parâmetro no conjunto dos números inteiros, garantindo que as incógnitas pertençam ao conjunto dos números inteiros. Esse processo é finito, já que se trabalha com números cada vez menores em valores absolutos. Agora, esse método será utilizado para resolver o problema (1).

#### 5.4. Resolução do problema 1

No problema (1) foi obtida a equação (9):  $65x + 24y = 5000$ . Como o coeficiente do  $y$  é menor que o coeficiente do  $x$ , escreve-se o  $y$  em função de  $x$ , substitui 5000 por  $4992 + 8$  e 65 por  $48 + 17$ :

$$\begin{aligned} 65x + 24y &= 5000 \\ 24y &= 5000 - 65x \\ y &= \frac{5000 - 65x}{24} \end{aligned} \tag{34}$$

$$\begin{aligned} &= \frac{(4992 + 8) - (48 + 17)x}{24} \\ &= \frac{4992 - 48x}{24} + \frac{8 - 17x}{24}. \end{aligned} \tag{35}$$

Analisando a equação (35),  $\frac{4992 - 48x}{24} \in \mathbb{Z}$  para todo  $x \in \mathbb{Z}$ . Para que  $y$  seja sempre um número inteiro,  $8 - 17x$  deve ser divisível por 24, ou seja, deve existir um número  $u \in \mathbb{Z}$  tal que  $8 - 17x = 24u$ . Escrevendo  $x$  em função de  $u$ :

$$\begin{aligned} 8 - 17x &= 24u \\ x &= \frac{8 - 24u}{17}. \end{aligned} \tag{36}$$

Na equação (36), note que  $\frac{8 - 24u}{17} \notin \mathbb{Z}$  para todo  $u \in \mathbb{Z}$ , então substitui 24 por  $17 + 7$  para continuar o processo de divisões sucessivas:

$$\begin{aligned} x &= \frac{8 - 24u}{17} \\ &= \frac{8 - (17 + 7)u}{17} \\ &= \frac{-17u}{17} + \frac{8 - 7u}{17}. \end{aligned} \tag{37}$$



Pela equação (37),  $\frac{-17u}{17} \in \mathbb{Z}$  para todo  $u \in \mathbb{Z}$ . Para que  $x$  seja sempre um número inteiro,  $8 - 7u$  deve ser divisível por 17, ou seja, deve existir um  $v \in \mathbb{Z}$  tal que  $8 - 7u = 17v$ . Escrevendo  $u$  em função de  $v$ :

$$\begin{aligned} 8 - 7u &= 17v \\ u &= \frac{8 - 17v}{7}. \end{aligned} \quad (38)$$

Na equação (38), note que  $\frac{8 - 17v}{7} \notin \mathbb{Z}$  para todo  $v \in \mathbb{Z}$ , então substituí 8 por  $7 + 1$  e 17 por  $14 + 3$  para continuar o processo das divisões sucessivas:

$$\begin{aligned} u &= \frac{8 - 17v}{7} \\ &= \frac{(7 + 1) - (14 + 3)v}{7} \\ &= \frac{7 - 14v}{7} + \frac{1 - 3v}{7}. \end{aligned} \quad (39)$$

Pela equação (39),  $\frac{7 - 14v}{7} \in \mathbb{Z}$  para que  $u \in \mathbb{Z}$ . Para que  $u$  seja sempre um número inteiro,  $1 - 3v$  deve ser divisível por 7, ou seja, deve existir um  $w \in \mathbb{Z}$  tal que  $1 - 3v = 7w$ . Escrevendo  $v$  em função de  $w$ :

$$\begin{aligned} 1 - 3v &= 7w \\ v &= \frac{1 - 7w}{3}. \end{aligned} \quad (40)$$

Na equação (40), note que  $\frac{1 - 7w}{3} \notin \mathbb{Z}$  para todo  $w \in \mathbb{Z}$ , então substituí 7 por  $6 + 1$  para continuar o processo das divisões sucessivas:

$$\begin{aligned} v &= \frac{1 - 7w}{3} \\ &= \frac{1 - (6 + 1)w}{3} \\ &= \frac{6w}{3} + \frac{1 - w}{3}. \end{aligned} \quad (41)$$

Pela equação (41),  $\frac{6w}{3} \in \mathbb{Z}$  para todo  $v \in \mathbb{Z}$ . Para que  $v$  seja sempre um número inteiro,  $1 - w$  deve ser divisível por 3, ou seja, deve existir um  $k \in \mathbb{Z}$  tal que  $1 - w = 3k$ . Escrevendo  $w$  em função de  $k$ :

$$\begin{aligned} 1 - w &= 3k \\ w &= 1 - 3k. \end{aligned} \quad (42)$$

Na equação (42),  $w \in \mathbb{Z}$  para todo  $k \in \mathbb{Z}$ , e o processo de divisões sucessivas encerra-se. Agora será encontrada uma expressão que fornece o valor das incógnitas  $x$  e  $y$  e obtendo-se uma solução geral para a equação (9). Essa será uma solução paramétrica em função do parâmetro inteiro  $k$ , para tanto, serão feitas algumas substituições nas equações obtidas.

Substituindo a equação (42) na equação (40) obtém-se  $v$  em função do parâmetro  $k$ :

$$\begin{aligned}
 v &= \frac{1 - 7w}{3} \\
 &= \frac{1 - 7(1 - 3k)}{3} \\
 &= -2 + 7k.
 \end{aligned} \tag{43}$$

Substituindo a equação (43) na equação (38) obtém-se  $u$  em função do parâmetro  $k$ :

$$u = \frac{8 - 17v}{7} \tag{44}$$

$$\begin{aligned}
 &= \frac{8 - 17(-2 + 7k)}{7} \\
 &= 6 - 17k.
 \end{aligned} \tag{45}$$

Substituindo a equação (45) na equação (36) obtém-se  $x$  em função do parâmetro  $k$ :

$$\begin{aligned}
 x &= \frac{8 - 24u}{17} \\
 &= \frac{8 - 24(6 - 17k)}{17} \\
 &= -8 + 24k.
 \end{aligned} \tag{46}$$

E, finalmente, substituindo a equação (46) na equação (34) obtém-se  $y$  em função do parâmetro  $k$ :

$$\begin{aligned}
 y &= \frac{5000 - 65x}{24} \\
 &= \frac{5000 - 65(-8 + 24k)}{24} \\
 &= 230 - 65k.
 \end{aligned} \tag{47}$$

Portanto, uma solução geral da equação (9) pode ser dada por:

$$x = -8 + 24k, \quad e \quad y = 230 - 65k, \quad \text{com } k \in \mathbb{Z}. \tag{48}$$

Como as quantidades de celulares devem ser inteiras e positivas, para que variável  $x$  seja positiva,  $k > \frac{8}{24}$ ; para que a variável  $y$  seja positiva,  $k < \frac{230}{65}$ . Os únicos valores inteiros de  $k$  que satisfazem

k	x	y
1	16	165
2	40	100
3	64	35

Tabela 6: Soluções inteiras positivas.

essas duas inequações são  $k_1 = 1$ ,  $k_2 = 2$  e  $k_3 = 3$ . Na tabela (6) são apresentadas as soluções inteiras positivas obtidas através desses parâmetros  $k$ .

Vale comentar que as soluções gerais apresentadas no método 1 pela equação(18) e no método 3 pela equação (48) são dadas por expressões matemáticas diferentes, porém, representam a mesma solução; esse fato pode ser verificado pelas tabelas (3) e (6).

## 6. Considerações finais

Neste trabalho foram apresentados três métodos simples que são utilizados nas aulas preparatórias para olimpíadas com alunos de cursos técnicos integrados ao ensino médio do Instituto Federal de São Paulo - Câmpus Registro, além de jovens participantes do PIC da Obmep oriundos da região do Vale do Ribeira. Espera-se que ele possa contribuir com o aprimoramento do estudo e ensino de equações diofantinas lineares entre professores e alunos do ensino básico e ensino superior.

## Referências

- [1] ALENCAR FILHO, Edgard de. *Teoria Elementar dos números*. 2<sup>a</sup> edição. São Paulo: Nobel, 1984.
- [2] CARNEIRO, João Paulo Q. “Dispositivo prático para expressar o mdc de dois números como combinação linear deles”. In: *Revista do Professor de Matemática* nº 37. São Paulo: SBM, 1998. Disponível em: <https://rpm.org.br/cdrpm/37/6.htm>. Acesso em: 05 de junho de 2020
- [3] COELHO, S.P.; MILIES, F.C.P. *NÚMEROS: Uma Introdução à Matemática*. São Paulo-SP: SBM, Editora da Universidade de São Paulo, 1997.
- [4] HEFEZ, A. *Elementos de Aritmética*. Rio de Janeiro-RJ: SBM, 2011.
- [5] OLIVEIRA, S.B. *As Equações Diofantinas Lineares e o livro didático de Matemática para o Ensino Médio*. 2006. Dissertação Mestrado Acadêmico em Educação Matemática, Pontifícia Universidade Católica de São Paulo, São Paulo.
- [6] PATERLINI, R.R. *Aritmética dos Números inteiros*. São Carlos-SP: UFSCAR,2017.

Egídio Costa Filho  
Instituto Federal de São Paulo - Câmpus Registro  
<[egidiocosta@ifsp.edu.br](mailto:egidiocosta@ifsp.edu.br)>

Márcio Lúcio Rodrigues  
Instituto Federal de São Paulo - Câmpus Registro  
<[marcio.rodrigues@ifsp.edu.br](mailto:marcio.rodrigues@ifsp.edu.br)>

Orlando Eduardo da Silva Ferri  
Instituto Federal de São Paulo - Câmpus Registro  
<[orlandoferri@ifsp.edu.br](mailto:orlandoferri@ifsp.edu.br)>

Recebido: 08/06/2020  
Publicado: 13/01/2022