

# Implementações aritméticas

Evilson Vieira

## Resumo

Neste trabalho apresentamos uma implementação para execução manual do algoritmo estendido das divisões sucessivas de Euclides para a obtenção de soluções de equações diofantinas lineares de duas variáveis e, em particular, para o cálculo do inverso multiplicativo modular. Também apresentamos uma implementação para o cálculo manual da solução de um sistema de restos.

**Palavras-chave:** implementações aritméticas; inverso modular; sistema de restos.

## Abstract

In this work we present an implementation for manual execution of the extended algorithm of the successive divisions of Euclid to obtain solutions of linear equations of two variables and, in particular, for the calculation of the modular multiplicative inverse. We also present an implementation for the manual calculation of the solution of a system of remainders.

**Keywords:** arithmetic implementations; modular inverse; system of remainders.

## 1. Introdução

Quando efetuamos cálculos manuais sempre estamos executando alguns algoritmos previamente estudados, comprovados e documentados por matemáticos ao redor do mundo. Para executarmos tais algoritmos é necessário que usemos uma implementação desses algoritmos. Chamamos de implementação uma diagramação intuitiva associada a um algoritmo, que registra, de forma organizada, os passos do algoritmo e seus valores parciais. Uma boa implementação é aquela que além de tornar possível a execução do algoritmo:

- ◇ faz com que essa execução seja rápida;
- ◇ evita cálculos desnecessários;
- ◇ evita repetições desnecessárias de termos;
- ◇ facilita a detecção de erros de cálculo;

Como exemplo citamos uma implementação bem conhecida do cálculo do mdc (máximo divisor comum) de dois números inteiros positivos em que dispomos os valores parciais das divisões sucessivas de Euclides em uma estrutura matricial com três linhas conforme ilustramos a seguir:

**Problema 1.** Dados os inteiros positivos  $m, n$ , encontrar  $\text{mdc}(m, n)$ .

**Solução:** Convenientemente tomamos  $m \geq n$ . Usamos o algoritmo das divisões sucessivas de Euclides, registrando os quocientes e restos parciais na estrutura matricial abaixo:

$$\begin{array}{c|c|c|c|c|c} & q_2 & q_3 & \cdots & q_{k-1} & q_k \\ \hline d_1 & d_2 & d_3 & \cdots & d_{k-1} & d_k \\ \hline r_1 & r_2 & r_3 & \cdots & (0) & \end{array}$$

Colocamos  $d_1 = m$  e  $d_2 = n$  e, para cada  $j = 1, 2, 3, \dots, k$ , fazemos, recursivamente:

$$\boxed{d_j = d_{j+1} \cdot q_{j+1} + r_j} \text{ e } \boxed{d_{j+2} = r_j}$$

ou seja, dividimos  $d_j$  por  $d_{j+1}$  e anotamos o quociente  $q_{j+1}$  na primeira linha e o resto  $r_j$  na terceira linha e, depois disso, copiamos o resto obtido para a segunda linha. Repetimos esse procedimento até obtermos um resto zero. Então, o último termo da segunda linha é o valor procurado, ou seja,

$$d_k = \text{mdc}(d_1, d_2).$$

**Exemplo:** Para  $m = 487$  e  $n = 305$  temos:

$$\begin{array}{c|c} & 1 \\ \hline 487 & 305 \\ \hline 182 & \end{array}$$

Pois  $487 = 305 \cdot 1 + 182$ ;

$$\begin{array}{c|c|c} & 1 & 1 \\ \hline 487 & 305 & 182 \\ \hline 182 & 123 & \end{array}$$

Pois  $305 = 182 \cdot 1 + 123$ ;  
(note que 182 foi copiado da terceira para a segunda linha)

Continuamos até obter um resto zero:

$$\begin{array}{c|c|c|c|c|c|c|c} & 1 & 1 & 1 & 2 & 11 & 1 & 4 \\ \hline 487 & 305 & 182 & 123 & 59 & 5 & 4 & (1) \\ \hline 182 & 123 & 59 & 5 & 4 & 1 & 0 & \end{array}$$

E concluímos que  $\text{mdc}(487, 305) = 1$ .

Essa implementação aritmética é bem popular e ilustra o quanto é interessante ter uma diagramação organizada das etapas parciais de um algoritmo.

## 2. Resolvendo equações diofantinas lineares com duas variáveis

Nesta seção, o foco é resolver equações da forma

$$mx + ny = c, \tag{1}$$

onde  $m, n \in \mathbb{Z}$ , e queremos encontrar todos os pares de inteiros  $(x, y)$  que sejam soluções desta equação. É bem conhecido (veja [1] ou [2]) que, para essa equação ter solução, basta que  $\text{mdc}(m, n) \mid c$ . Consideraremos que tal afirmação é válida aqui em nosso problema.

Suponhamos que conheçamos duas soluções distintas da equação (1), digamos  $(x_0, y_0)$  e  $(x_1, y_1)$ , nesse caso temos:

$$\begin{cases} mx_0 + ny_0 = c \\ mx_1 + ny_1 = c. \end{cases}$$

Subtraindo-se os membros esquerdo e direito dessas duas equações, obtemos:

$$m(x_1 - x_0) + n(y_1 - y_0) = 0.$$

Portanto, o par de inteiros  $(x_1 - x_0, y_1 - y_0)$  é solução da equação diofantina linear

$$mx + ny = 0. \quad (2)$$

Seja  $d = \text{mdc}(m, n)$ . Escrevamos  $m = dm_1$  e  $n = dn_1$ , dessa forma,  $\text{mdc}(m_1, n_1) = 1$ . Assim, (2) torna-se

$$\begin{cases} ny = -mx \\ dn_1y = -dm_1x \\ n_1y = -m_1x. \end{cases} \quad (3)$$

Seja  $(x, y)$  uma solução de (3). Como  $\text{mdc}(m_1, n_1) = 1$ , concluímos que  $n_1 \mid x$ , então podemos escrever  $x = n_1t$ , para algum inteiro  $t$ . Substituído-se essa igualdade em (3), temos

$$\begin{cases} n_1y = -m_1n_1t \\ y = -m_1t. \end{cases} \quad (4)$$

Então, as soluções de (2) são os pares da forma  $(x, y) = (n_1t, -m_1t)$ , ou seja,  $(x, y) = \left(\frac{n}{d}t, -\frac{m}{d}t\right)$ , onde  $t$  percorre todos os números inteiros. De acordo com tais resultados, se  $(x_0, y_0)$  é uma solução particular de (1) então, o conjunto de todas as soluções de (1) é dado por

$$\left\{ \left( x_0 + \frac{n}{\text{mdc}(m, n)}t, y_0 - \frac{m}{\text{mdc}(m, n)}t \right); t \in \mathbb{Z} \right\}.$$

**Exemplo:**  $(3, 4)$  é uma solução particular da equação  $5x - 3y = 3$ . Portanto o conjunto solução dessa equação é  $\{(3 + 3t, 4 + 5t); t \in \mathbb{Z}\}$ .

Dessa forma, resolver uma equação diofantina linear de duas variáveis reduz-se à determinação de uma solução particular  $(x_0, y_0)$ .

Na verdade, basta que saibamos resolver o Problema 2 abaixo:

**Problema 2.** Dados os inteiros positivos  $m, n$ , encontrar inteiros  $r$  e  $s$  tais que

$$r \cdot m + s \cdot n = d, \quad (5)$$

onde  $d = \text{mdc}(m, n)$ .

De fato, considere a equação (1), onde  $d \mid c$ , se tivermos uma solução  $(r, s)$  do Problema 2, então o par  $\left(\frac{c}{d}r, \frac{c}{d}s\right)$  é uma solução de (1), pois:

$$\frac{c}{d}rm + \frac{c}{d}sn = \frac{c}{d}(rm + sn) = \frac{c}{d}d = c.$$

É bem conhecido que o Problema 2 sempre tem solução (veja Teorema de Bachet-Bézout em [3]). Esta solução é obtida executando-se o algoritmo estendido das divisões sucessivas de Euclides. Na seção seguinte propomos uma implementação para a execução deste algoritmo.

### 3. Implementação do Algoritmo Estendido de Euclides

Nosso foco agora é propor uma implementação para resolver o Problema 2. Primeiramente propomos enxugar a implementação do cálculo do mdc mencionado na Introdução. Note que a terceira linha pode ser ignorada devido ao fato de que todos os seus termos são copiados para a segunda linha. Podemos, então, deixar a implementação apenas com as duas primeiras linhas:

$$\begin{array}{c|c|c|c|c|c|c} & q_2 & q_3 & \cdots & q_{k-1} & q_k & \\ \hline d_1 & d_2 & d_3 & \cdots & d_{k-1} & (d_k) & 0 \end{array}$$

Onde  $d_1 = m$  e  $d_2 = n$  e para cada  $j = 1, 2, 3, \dots, k$ , fazemos, recursivamente:

$$d_j = d_{j+1} \cdot q_{j+1} + d_{j+2} \tag{6}$$

até que o último termo da segunda linha seja zero. Então o penúltimo termo da segunda linha é o valor procurado, ou seja,

$$d_k = \text{mdc}(d_1, d_2)$$

**Exemplo:** Para  $m = 487$  e  $n = 305$  temos:

$$\begin{array}{c|c|c} 1 & & \\ \hline 487 & 305 & 182 \end{array} \quad \begin{array}{c|c|c|c} 1 & 1 & & \\ \hline 487 & 305 & 182 & 123 \end{array} \quad \begin{array}{c|c|c|c|c|c|c|c|c} 1 & 1 & 1 & 2 & 11 & 1 & 4 & & \\ \hline 487 & 305 & 182 & 123 & 59 & 5 & 4 & (1) & 0 \end{array}$$

E concluímos que  $\text{mdc}(487, 305) = 1$ .

Note que, nos casos em que  $\text{mdc}(m, n) = 1$ , podemos encerrar a etapa das divisões sucessivas no momento em que obtivermos o primeiro resto igual a 1, pois já sabemos que o próximo resto será zero.

Após executada esta primeira parte do algoritmo, adicionamos uma nova linha à estrutura inicial, com elementos  $a_j$ :

$$\begin{array}{c|c|c|c|c|c|c} & q_2 & q_3 & \cdots & q_{k-1} & q_k & \\ \hline d_1 & d_2 & d_3 & \cdots & d_{k-1} & (d_k) & 0 \\ \hline a_1 & a_2 & a_3 & \cdots & a_{k-1} & a_k & \end{array}$$

de forma que, para cada posição  $j$  tenhamos:

$$a_j \cdot d_{j+1} + a_{j+1} \cdot d_j = d_k \tag{7}$$

$$\begin{array}{c|c|c|c|c|c|c} \cdots & q_j & q_{j+1} & \cdots & q_k & & \\ \hline \cdots & d_j & d_{j+1} & \cdots & (d_k) & & 0 \\ \hline \cdots & a_j & a_{j+1} & \cdots & a_k & & \end{array}$$

As setas duplas cruzadas indicam os pares de inteiros a serem multiplicados, de forma que a soma desses produtos seja  $d_k$ . Observe que, substituindo  $d_{j+1}$  na equação (7) usando (6), obtemos uma expressão para  $a_{j-1}$  que depende, apenas, de  $q_j$ ,  $a_j$  e  $a_{j+1}$ :

$$\begin{aligned} a_j \cdot (d_{j-1} - d_j \cdot q_j) + a_{j+1} \cdot d_j &= d_k \\ a_j \cdot d_{j-1} - a_j \cdot d_j \cdot q_j + a_{j+1} \cdot d_j &= d_k \\ \underbrace{(a_{j+1} - q_j \cdot a_j)}_{a_{j-1}} \cdot d_j + a_j \cdot d_{j-1} &= d_k \end{aligned} \tag{8}$$

$$\begin{array}{c|c|c|c|c} \cdots & q_{j-1} & q_j & q_{j+1} & \cdots \\ \cdots & d_{j-1} & d_j & d_{j+1} & \cdots \\ \cdots & a_{j-1} & a_j & a_{j+1} & \cdots \end{array}$$

Ou seja, cada termo da terceira linha pode ser obtido a partir dos dois termos posteriores, então a terceira linha precisa ser preenchida da direita para a esquerda. Observemos que os candidatos mais simples para as duas últimas posições,  $a_k$  e  $a_{k-1}$ , para que satisfaçam a equação (7), são  $a_k = 0$  e  $a_{k-1} = 1$ . Portanto, podemos iniciar o preenchimento da terceira linha começando com 0 e 1:

$$\begin{array}{c|c|c|c|c|c|c} & q_2 & q_3 & \cdots & q_{k-1} & q_k & \\ \hline d_1 & d_2 & d_3 & \cdots & d_{k-1} & (d_k) & 0 \\ \hline & & & & 1 & 0 & \end{array}$$

Veja que:

$$1 \cdot d_k + 0 \cdot d_{k-1} = d_k$$

Terminamos o preenchimento usando a recorrência obtida na equação (8):

$$a_{j-1} = a_{j+1} - q_j \cdot a_j.$$

No final da recorrência obteremos os valores  $a_1$  e  $a_2$  que satisfazem à equação

$$a_1 \cdot d_2 + a_2 \cdot d_1 = d_k$$

que era nosso objetivo.

**Exemplo:** Para  $m = 487$  e  $n = 305$ , a implementação fica da seguinte forma:

$$\begin{array}{c|c|c|c|c|c|c|c|c} & 1 & 1 & 1 & 2 & 11 & 1 & 4 & \\ \hline 487 & 305 & 182 & 123 & 59 & 5 & 4 & (1) & 0 \\ \hline 99 & -62 & 37 & -25 & 12 & -1 & 1 & 0 & \end{array}$$

E temos os valores  $r = -62$  e  $s = 99$ , que satisfazem à equação que queríamos:

$$(-62) \cdot 487 + 99 \cdot 305 = 1$$

### 3.1. O inverso multiplicativo modular

Quando  $\text{mdc}(m, n) = 1$ , os valores  $r$  e  $s$  obtidos podem ser interpretados como inverso multiplicativo de  $m$  módulo  $n$  e inverso multiplicativo  $n$  módulo  $m$ , respectivamente. De fato, se tivermos:

$$r \cdot m + s \cdot n = 1$$

Então:

$$\boxed{r \cdot m \equiv 1 \pmod{n}} \text{ e } \boxed{s \cdot n \equiv 1 \pmod{m}}$$

Denotaremos por  $m_{(n)}^{-1}$  o inverso multiplicativo de  $m$  módulo  $n$ .

No nosso exemplo temos  $487_{(305)}^{-1} = -62$  e  $305_{(487)}^{-1} = 99$ . A seguir fazemos uso de um problema para ilustrar a aplicação do dispositivo:

**Problema 3.** Qual o menor inteiro positivo cujo produto com 305 deixa resto 43 quando dividido por 487?

**Solução:**

$$\begin{aligned} 305x &\equiv 43 && (\text{mod } 487) \\ \underbrace{(305_{(487)}^{-1} \cdot 305)}_{\equiv 1} x &\equiv 305_{(487)}^{-1} \cdot 43 && (\text{mod } 487) \\ x &\equiv 99 \cdot 43 && (\text{mod } 487) \\ x &\equiv 361 && (\text{mod } 487). \end{aligned}$$

#### 4. Resolvendo um sistema de restos

Nosso problema agora é resolver o sistema de restos:

$$\begin{cases} x \equiv a_1 & (\text{mod } m_1) \\ x \equiv a_2 & (\text{mod } m_2) \\ x \equiv a_3 & (\text{mod } m_3) \\ \vdots & \vdots \\ x \equiv a_k & (\text{mod } m_k), \end{cases} \quad (9)$$

onde  $\text{mdc}(m_i, m_j) = 1$ , para  $i \neq j$ .

É bem conhecido (veja Teorema Chinês do Resto em [1], [2] ou [3]) que esse sistema tem solução, e que essa solução é dada por:

$$x \equiv M_1 b_1 + M_2 b_2 + M_3 b_3 + \dots + M_k b_k \pmod{M}, \quad (10)$$

onde

$$\begin{cases} M = m_1 m_2 m_3 \dots m_k \\ M_j = \frac{M}{m_j}, \quad j \in \{1, 2, 3, \dots, k\} \\ M_j b_j \equiv a_j \pmod{m_j}, \quad j \in \{1, 2, 3, \dots, k\}. \end{cases}$$

O valor de  $M$  e os valores  $\{M_1, M_2, M_3, \dots, M_k\}$  são obtidos sem dificuldade. Para obter os valores  $\{b_1, b_2, b_3, \dots, b_k\}$ , fazemos:

$$\begin{aligned} M_j b_j &\equiv a_j && (\text{mod } m_j) \\ \underbrace{(M_{j(m_j)}^{-1} M_j)}_{\equiv 1} b_j &\equiv M_{j(m_j)}^{-1} a_j && (\text{mod } m_j) \\ b_j &\equiv M_{j(m_j)}^{-1} a_j && (\text{mod } m_j), \end{aligned} \quad (11)$$

onde  $M_{j(m_j)}^{-1}$  pode ser calculado da seguinte forma:

$$\begin{aligned}
 M_{j(m_j)}^{-1} &\equiv \left( \prod_{i \neq j} m_i \right)_{(m_j)}^{-1} \pmod{m_j} \\
 &\equiv \prod_{i \neq j} m_i^{-1} \pmod{m_j}.
 \end{aligned} \tag{12}$$

E, assim, temos a solução do sistema (9).

#### 4.1. A implementação do algoritmo

Apresentamos, agora, a implementação proposta para o cálculo da solução do sistema (9).

Primeiramente, ordenamos as equações do sistema de forma que  $m_1 > m_2 > m_3 > \dots > m_k$  e montamos uma tabela com os termos  $c_{(i,j)} = m_i^{-1} \pmod{m_j}$ , para  $i \neq j$ .

	$c_{(1,2)}$	$c_{(1,3)}$	...	$c_{(1,k)}$
$c_{(2,1)}$		$c_{(2,3)}$	...	$c_{(2,k)}$
$c_{(3,1)}$	$c_{(3,2)}$		...	$c_{(3,k)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$	$c_{(k,2)}$	$c_{(k,3)}$	...	

Note que deixamos vazias as células  $c_{(j,j)}$ , ou seja, as células da diagonal.

Executando-se a implementação do cálculo do inverso multiplicativo modular para os pares  $(m_1, m_2)$ ,  $(m_1, m_3)$ , ...,  $(m_1, m_k)$ , obtemos a primeira coluna e primeira linha da tabela, conforme ilustrado abaixo:

	$c_{(1,2)}$	$c_{(1,3)}$	...	$c_{(1,k)}$
$c_{(2,1)}$			...	
$c_{(3,1)}$			...	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$			...	

	#	...
$m_1$	$m_2$	...
$c_{(2,1)}$	$c_{(1,2)}$	...

	#	...
$m_1$	$m_3$	...
$c_{(3,1)}$	$c_{(1,3)}$	...

	#	...
$m_1$	$m_k$	...
$c_{(k,1)}$	$c_{(1,k)}$	...

Executando-se a implementação do cálculo do inverso multiplicativo modular para os pares  $(m_2, m_3)$ ,  $(m_2, m_4)$ , ...,  $(m_2, m_k)$ , completamos a segunda coluna e segunda linha da tabela. E assim por diante (os símbolos “#” representam valores que aparecem na implementação mas que não serão úteis na montagem da tabela).

Feito isso, preenchemos as células vazias com os termos  $\{a_1, a_2, a_3, \dots, a_k\}$  do sistema de restos, de forma que o termo  $a_j$  ocupe a célula  $(j, j)$ . Por fim, acrescentamos uma linha extra à tabela onde colocaremos os valores  $\{b_1, b_2, b_3, \dots, b_k\}$ .

$a_1$	$c_{(1,2)}$	$c_{(1,3)}$	$\dots$	$c_{(1,k)}$
$c_{(2,1)}$	$a_2$	$c_{(2,3)}$	$\dots$	$c_{(2,k)}$
$c_{(3,1)}$	$c_{(3,2)}$	$a_3$	$\dots$	$c_{(3,k)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$	$c_{(k,2)}$	$c_{(k,3)}$	$\dots$	$a_k$
$b_1$	$b_2$	$b_3$	$\dots$	$b_k$

Das equações (11) e (12) concluímos que cada  $b_j$  é o produto de todos os elementos da coluna  $j$  da tabela, módulo  $m_j$ , ou seja:

$$\begin{cases} b_1 \equiv a_1 c_{(2,1)} c_{(3,1)} \dots c_{(k,1)} & (\text{mod } m_1) \\ b_2 \equiv c_{(1,2)} a_2 c_{(3,2)} \dots c_{(k,2)} & (\text{mod } m_2) \\ b_3 \equiv c_{(1,3)} c_{(2,3)} a_3 \dots c_{(k,3)} & (\text{mod } m_3) \\ \vdots & \vdots \\ b_k \equiv c_{(1,k)} c_{(2,k)} c_{(3,k)} \dots a_k & (\text{mod } m_k). \end{cases}$$

E, finalmente, podemos escrever a solução:

$$x \equiv M_1 b_1 + M_2 b_2 + M_3 b_3 + \dots + M_k b_k \pmod{M}. \quad (13)$$

Em geral, buscamos a menor solução não negativa do sistema, ou seja, queremos que  $0 \leq x < M$ . Para isso, basta escolher os  $b_j$ s, convenientemente, de forma que:

$$\begin{aligned} 0 &\leq M_1 b_1 + M_2 b_2 + M_3 b_3 + \dots + M_k b_k < M \\ 0 &\leq \frac{M_1 b_1}{M} + \frac{M_2 b_2}{M} + \frac{M_3 b_3}{M} + \dots + \frac{M_k b_k}{M} < 1 \\ 0 &\leq \frac{b_1}{m_1} + \frac{b_2}{m_2} + \frac{b_3}{m_3} + \dots + \frac{b_k}{m_k} < 1. \end{aligned}$$

Cabe observar que escolha dos  $b_j$  s dessa forma não é única.

Para fins de organização, é interessante escrever a solução (13) como:

$$x \equiv [b_1 m_2 m_3 \dots m_k] + [m_1 b_2 m_3 \dots m_k] + [m_1 m_2 b_3 \dots m_k] + \dots + [m_1 m_2 m_3 \dots b_k] \pmod{M}.$$

ou seja, a  $j$ -ésima parcela é obtida substituindo-se  $m_j$  por  $b_j$ .

## 4.2. Um exemplo ilustrativo

Vamos resolver o sistema de restos: 
$$\begin{cases} x \equiv 7 & (\text{mod } 17) \\ x \equiv 12 & (\text{mod } 15) \\ x \equiv 4 & (\text{mod } 11) \\ x \equiv 5 & (\text{mod } 7) \end{cases}$$



	1	7		
17	15	2	1	
8	-7	1	0	

	1	1	1	
17	11	6	5	1
-3	2	-1	1	0

	2	2	
17	7	3	1
5	-2	1	0

	1	2	1	
15	11	4	3	1
-4	3	-1	1	0

	2	
15	7	1
-2	1	0

	1	1	1	
11	7	4	3	1
-3	2	-1	1	0

Preenchemos a diagonal da matriz com os valores fornecidos no problema.

7	-7	2	-2
8	12	3	1
-3	-4	4	2
5	-2	-3	5

Substituiremos o 12 por  $-3$  na segunda coluna, visto que é módulo 15. Usar valores o mais próximos de zero quanto pudermos pode simplificar os cálculos. Os valores obtidos na implementação do inverso multiplicativo modular já estão o mais próximo de zero possível. Agora calculamos os valores  $\{b_1, b_2, b_3, b_4\}$  colocando-os na linha extra da matriz. Cada  $b_j$  é o produto dos termos da coluna  $j$  módulo  $m_j$ .

$$\begin{cases} b_1 \equiv 7 \cdot 8 \cdot (-3) \cdot 5 \equiv -7 \pmod{17} \\ b_2 \equiv (-7) \cdot (-3) \cdot (-4) \cdot (-2) \equiv 3 \pmod{15} \\ b_3 \equiv 2 \cdot 3 \cdot 4 \cdot (-3) \equiv 5 \pmod{11} \\ b_4 \equiv (-2) \cdot 1 \cdot 2 \cdot 5 \equiv 1 \pmod{7} \end{cases}$$

7	-7	2	-2
8	-3	3	1
-3	-4	4	2
5	-2	-3	5
-7	3	5	1

E então temos a solução:

$$x \equiv [(-7) \cdot 15 \cdot 11 \cdot 7] + [17 \cdot 3 \cdot 11 \cdot 7] + [17 \cdot 15 \cdot 5 \cdot 7] + [17 \cdot 15 \cdot 11 \cdot 1] \pmod{17 \cdot 15 \cdot 11 \cdot 7}$$

$$x \equiv 7572 \pmod{19635}$$

Note que

$$\frac{-7}{17} + \frac{3}{15} + \frac{5}{11} + \frac{1}{7} > \frac{3}{15} + \frac{1}{7} > 0$$

$$\frac{-7}{17} + \frac{3}{15} + \frac{5}{11} + \frac{1}{7} < \frac{5}{11} + \frac{1}{7} < \frac{1}{2} + \frac{1}{2} = 1$$

Note, também, que poderíamos ter escolhido  $b_1 = 10$  e  $b_3 = -6$ , pois  $0 < \frac{10}{17} + \frac{3}{15} + \frac{-6}{11} + \frac{1}{7} < 1$ .

Para fugir dessa desigualdade podemos escolher os  $b_j$  s o mais próximos de zero que pudermos. Mas, ocasionalmente, será necessário somar algum múltiplo de  $M$  (positivo ou negativo) ao resultado final para obtermos a menor solução não negativa.

Observe que todas as etapas intermediárias ficam bem diagramadas e organizadas favorecendo uma menor possibilidade de erro. E se houver erros, a diagramação facilita sua detecção.

## Referências

- [1] Hefez, Abramo. *Curso de Álgebra*, vol. 1. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1993.
- [2] Hefez, Abramo. *Elementos de Aritmética*. 2<sup>a</sup> ed. Rio de Janeiro-RJ: Sociedade Brasileira de Matemática, 2006.
- [3] Martinez, Fabio Brochero; et alli. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2010.

Evilson Vieira  
Universidade Federal de Sergipe - UFS  
<[evilson@ufs.br](mailto:evilson@ufs.br)>

Recebido: 2017

# O uso do *GeoGebra* no ensino de elipse nas aulas de matemática da Educação Básica

Gracino Rodrigues

Elisabete de Oliveira

## Resumo

O presente estudo discute a utilização do *GeoGebra*, um *software* de Matemática e multiplataforma. Parte-se do princípio que esse *software* oferece aos alunos uma metodologia de ensino interativa para aprender os conceitos matemáticos, considerando a necessidade de introduzir recursos tecnológicos no Ensino da Matemática na Educação Básica. Essa discussão enfoca a proposição de uma sequência didática para o uso do referido *software* sobre elipse nas turmas de Ensino Médio. Nesse sentido, mostram-se algumas definições e propriedades matemáticas encontradas na elipse, identificando seus elementos principais. Dessa forma é criada uma conexão entre Geometria e Álgebra usando uma perspectiva metodológica de ensino que vai além do “quadro e giz”, buscando uma construção geométrica que parte da abstração a concretude dos conceitos. Os resultados corroboram a defesa de que o *GeoGebra* se configura em uma metodologia inovadora e interativa para o ensino da área em foco.

**Palavras-chave:** Elipse; *GeoGebra*; Ensino da Matemática

## Abstract

The present study discusses the use of GeoGebra, a mathematical and multiplatform software. It is assumed that this software offers students an interactive teaching methodology to learn mathematical concepts, considering the need to introduce technological resources in Mathematics Teaching in Basic Education. This discussion focuses on the proposition of a didactic sequence for the use of said software on ellipse in the classes of High School. In this sense, some definitions and mathematical properties are found in the ellipse, identifying its main elements. In this way, a connection between Geometry and Algebra is created using a methodological perspective of teaching that goes beyond the “chalkboard”, seeking a geometric construction that starts from abstraction to the concreteness of concepts. The results corroborate the defense that GeoGebra configures itself in an innovative and interactive methodology for the teaching of the area in focus.

**Keywords:** Ellipse; GeoGebra; Mathematics Teaching

## 1. Introdução

No presente trabalho compreende-se o estudo da elipse, tendo em vista a relação Geometria e Álgebra, assim como, quando necessário, substituição de características de difícil compreensão

de uma, por características mais simples da outra; ou seja, procura-se explorar o que existe de mais avançado da Geometria Analítica ([6]). Para tanto, com o intuito de facilitar o estudo do conteúdo abordado, propõe-se a utilização de uma ferramenta tecnológica, um programa de geometria dinâmica, o *software GeoGebra* [3]<sup>1</sup>, que nos permite fazer representações algébricas e geométricas de um mesmo objeto.

No Ensino de Geometria Analítica existem instrumentos que são usados para realizar as construções geométricas como retas e circunferências. Como exemplos desses instrumentos, mencionamos a régua e o compasso, bem como o papel milimetrado, que também facilitam tais construções. No entanto, a elipse, considerada seção do cone duplo, tem um gráfico de difícil construção- existem alguns artifícios que ajudam, usando a régua e o cordão, mas comprometem a precisão e dificultam seu uso em sala de aula. Dessa forma, faz-se necessário introduzir uma ferramenta que facilite a construção geométrica de elipses.

Historicamente, a curva cônica elipse é um objeto de estudo discutido desde a Antiguidade. Sua descoberta é atribuída ao matemático Menaecmus (380 - 320 a.C. aproximadamente), e mais tarde estudada e aprimorada pelo geômetra grego Aristeu (370 - 300 a.C.) e pelo astrônomo e matemático grego Apolônio de Perga (262 - 190 a.C.). O filósofo e matemático francês René Descartes foi quem lançou as primeiras ideias a respeito da solução de problemas geométricos utilizando recursos algébricos, mas foi Pierre de Fermat quem representou os lugares geométricos estudados por Apolônio na forma de equações algébricas ([2]). Devido à necessidade de introduzir ferramentas tecnológicas no Ensino da Matemática na Educação Básica, utilizaremos na aplicação da pesquisa deste estudo um programa de geometria dinâmica, o *GeoGebra*, que é um *software* livre, multiplataforma e disponível em português. O *GeoGebra* foi criado por Markus Hohenwarter e reúne os recursos necessários para o desenvolvimento da pesquisa<sup>2</sup>.

Diante do exposto, o objetivo desse estudo é elaborar uma sequência didática para interessados no uso do *GeoGebra* como ferramenta metodológica do processo ensino-aprendizagem de Matemática na Educação Básica, especificamente, no terceiro ano do Ensino Médio. A proposição da sequência didática tem como foco a resolução de problemas envolvendo a curva cônica elipse, utilizando o *software GeoGebra* para identificar e relacionar elipses com suas equações algébricas.

O *GeoGebra* é um *software* como amplo reconhecimento, dentre os programas de geometria dinâmica. Esse reconhecimento não é por acaso, deve-se a eficiência e à facilidade de utilização do programa. É um *software* gratuito desenvolvido para o ensino-aprendizagem da Matemática nos vários níveis de ensino, do básico ao ensino superior. O programa *GeoGebra*, como a maioria dos *softwares*, passa por atualizações contínuas e novas versões são disponibilizadas com regularidade, além de ser multiplataforma. O *GeoGebra* pode ser usado simplesmente como uma ferramenta de situações-problema, para elaborar material de exposição ou disponibilizando a todos a oportunidade de experimentar as percepções extraordinárias que a matemática torna possível.

Este estudo encontra-se organizado da seguinte forma: *a priori* a elipse será definida e apresentados seus principais elementos, esses conceitos são fundamentados no aporte teórico referenciados no trabalho; *a posteriori* será apresentado o *software GeoGebra* com o objetivo de identificar e esboçar a curva cônica elipse, representada geométrica e algebricamente. Além disso, serão apre-

<sup>1</sup>Este *software* pode ser obtido em <<https://www.geogebra.org/>>. O presente estudo não tem por objetivo explicar as instruções para *download*, instalação e o uso detalhado do aplicativo. Essas informações podem ser obtidas do endereço mencionado nesta nota.

<sup>2</sup>Conforme explicitado em <<https://www.geogebra.im.uff.mat.br/>>. [4]

sentados alguns problemas matemáticos visando a aplicação dos conceitos estudados, bem como suas resoluções utilizando o *GeoGebra*.

Após a exposição dos principais conceitos relacionados à elipse, também serão analisados os fatos ocorridos na aplicação em sala de aula, através da utilização da sequência didática construída a partir do material desenvolvido anteriormente. As atividades realizadas pelos alunos, propostas pela sequência, produziram os dados que revelaram a reação dos alunos com a introdução do programa de geometria dinâmica nas aulas. Esses dados, bem como os demais resultados dessa investigação, serão apontados nas considerações finais deste estudo.

## 2. Elipse

A Elipse é uma curva plana, mas tem sua origem como seção do cone duplo, ou melhor: é uma superfície cônica seccionada por um plano que não passa pelo vértice, não é paralelo à reta geratriz e não é paralelo ao eixo da superfície (Figura 1). O estudo da elipse ganhou maior importância quando o astrônomo alemão Johannes Kepler (1571-1630) afirmou que todos os planetas do sistema solar descrevem uma órbita elíptica, o que ficou conhecido como a primeira lei de Kepler ([2]).

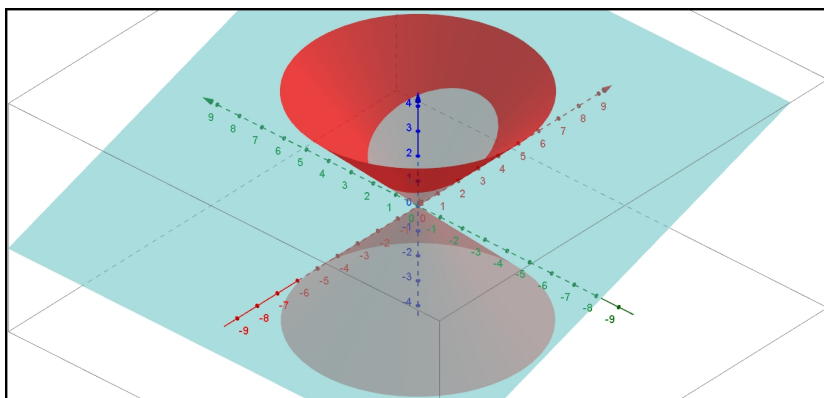


Figura 1: Elipse com Seção do Cone Duplo.

**Definição:** Sejam  $F_1$  e  $F_2$  dois pontos pertencentes a um plano  $\pi$ , o **lugar geométrico dos pontos**  $P$  pertencentes a  $\pi$ , onde a soma das distâncias de  $P$  a  $F_1$  e  $P$  a  $F_2$  é igual a uma constante  $r$ , com  $r$  maior que a distância entre  $F_1$  e  $F_2$ , é chamado de **elipse  $\mathcal{E}$  de focos  $F_1$  e  $F_2$** , ou seja,

$$\mathcal{E} = \{P | d(P, F_1) + d(P, F_2) = r\}. \quad (1)$$

## 3. Elementos da elipse

Pela definição temos  $d(P, F_1) + d(P, F_2) = r$ ; sem perda de generalidade, vamos escrever  $d(F_1, F_2) = 2c$  e  $r = 2a$ , onde  $a$  e  $c$  são constantes reais, com  $a > c \geq 0$ . Em uma elipse temos alguns elementos que podemos destacar, são eles:

- Os pontos  $F_1$  e  $F_2$  são chamados de **focos**;
- A **distância focal** é a distância  $2c$  entre os pontos  $F_1$  e  $F_2$ ;
- A reta  $t$  que contém os pontos  $F_1$  e  $F_2$  é chamada de **reta focal**;
- O ponto médio  $C$  do segmento  $F_1F_2$  é o **centro da elipse**  $\mathcal{E}$ ;
- A reta  $t'$  perpendicular à reta  $t$  que passa pelo centro  $C$  é chamada de **reta não focal**;
- As interseções das retas  $t$  e  $t'$  com a elipse  $\mathcal{E}$  são os pontos  $A_1$ ,  $A_2$ ,  $B_1$  e  $B_2$ , chamados de **vértice** da elipse;
- As cordas  $A_1A_2$  e  $B_1B_2$  são, respectivamente, o **eixo maior** e o **eixo menor** da elipse;
- A razão  $e = \frac{c}{a}$  é a **excentricidade** elipse;
- Os números  $a$ ,  $b$ , e  $c$  são, respectivamente, a distância entre os vértices  $A_1$  e  $A_2$  ao centro  $C$ , a distância entre os vértices  $B_1$  e  $B_2$  ao centro  $C$ , com  $b = \sqrt{a^2 - c^2}$ , e a distância dos focos  $F_1$  e  $F_2$  ao centro  $C$ .

#### 4. Sugestão de aula expositiva

Diante do exposto sobre os conceitos que envolvem a definição e os elementos da Elipse, de forma pontual, bem como a partir dos esclarecimentos sobre a introdução do uso do *GeoGebra*, abordasse a seguir a discussão e aplicação desses conceitos na compreensão de alguns problemas e suas respectivas resoluções

##### 4.1. Equação polinomial da elipse

Nesse momento, para simplificar nossos cálculos, vamos escolher uma elipse centrada na origem do sistema de coordenadas, ou seja, com  $C = (0, 0)$ , e reta focal coincidente com o eixo  $OX$ . Um ponto  $P$  pertence à elipse  $\mathcal{E}$  se, e somente se,

$$d(P, F_1) + d(P, F_2) = 2a \quad (2)$$

como  $A_1 = (a, 0)$ ,  $A_2 = (-a, 0)$ ,  $B_1 = (0, b)$ ,  $B_2 = (0, -b)$ ,  $F_1 = (c, 0)$  e  $F_2 = (-c, 0)$ , temos

$$\sqrt{(x-c)^2 + (y-0)^2} + \sqrt{(x+c)^2 + (y-0)^2} = 2a \quad (3)$$

$$\sqrt{x^2 + y^2 + 2cx + c^2} = 2a - \sqrt{x^2 + y^2 - 2cx + c^2} \quad (4)$$

elevando os dois lados da igualdade ao quadrado,

$$x^2 + y^2 - 2cx + c^2 = 4a^2 - 4a\sqrt{x^2 + y^2 - 2cx + c^2} + x^2 + y^2 - 2cx + c^2 \quad (5)$$

$$4a\sqrt{x^2 + y^2 - 2cx + c^2} = 4a^2 - 4cx \quad (6)$$

$$a\sqrt{x^2 + y^2 - 2cx + c^2} = a^2 - cx \quad (7)$$

elevando ao quadrado mais uma vez,

$$a^2(x^2 + y^2 - 2cx + c^2) = a^4 + c^2x^2 - 2a^2cx \quad (8)$$

logo,

$$(a^2 - c^2)x^2 + a^2y^2 = a^2(a^2 - c^2) \quad (9)$$

mas

$$b^2 = (a^2 - c^2), \quad (10)$$

substituindo equação (10) em equação (9),

$$b^2x^2 + a^2y^2 = a^2b^2 \quad (11)$$

dividindo todos os membros da equação (11) por  $ab$  encontramos

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1, \quad (12)$$

que é a equação da elipse centrada na origem do sistema de eixos cartesiano com reta focal paralela ao eixo  $OX$ .

Para a elipse centrada na origem e com reta focal coincidente com o eixo  $OY$ , temos  $A_1 = (0, a)$ ,  $A_2 = (0, -a)$ ,  $B_1 = (b, 0)$ ,  $B_2 = (-b, 0)$ ,  $F_1 = (0, c)$  e  $F_2 = (0, -c)$ ; refazendo os cálculos de modo análogo ao caso anterior, podemos verificar que a equação da elipse é:

$$\frac{x^2}{b^2} + \frac{y^2}{a^2} = 1, \quad (13)$$

## 4.2. Esboço da elipse com o uso do *GeoGebra*

Nosso objetivo é determinar o conjunto de pontos  $P(x, y)$  no plano, usando a definição de elipse e admitindo um caso particular, com  $F_1 = (3, 0)$ ,  $F_2 = (-3, 0)$  e  $r = 10$ , então  $\mathcal{E} = \{P \in \mathbb{R}^2 \mid d(P, F_1) + d(P, F_2) = 10\}$ .

Para que sejam satisfeitas as condições dadas pela definição, faremos uma parametrização. Temos  $P = (t, \frac{\sqrt{400-16t^2}}{5})$  e  $P' = (t, -\frac{\sqrt{400-16t^2}}{5})$ ; com  $-5 \leq t \leq 5$ , o ponto  $P'$  é simétrico ao ponto  $P$  em relação à reta que contém os pontos  $F_1$  e  $F_2$ , portanto o ponto  $P'$  tem a mesma propriedade de  $P$  ([2]). Dessa forma o uso do *GeoGebra* apresentará os seguintes passos:

**PASSO 1.** Para apresentação de forma clara da demonstração geométrica da definição de elipse, construa os segmentos  $a = F_1P$  e  $b = F_2P$ . Usando o recurso *Planilha* pode-se construir uma

tabela que mostra de forma interativa as distâncias  $d(F_1, P)$  e  $d(F_2, P)$ , que são, respectivamente, as medidas dos segmentos  $a$  e  $b$ . A soma  $d(F_1, P) + d(F_2, P)$  também pode ser observado na tabela. No menu *Exibir* selecione a opção *Planilha* e digite as distâncias com seus respectivos valores (Figura 2).

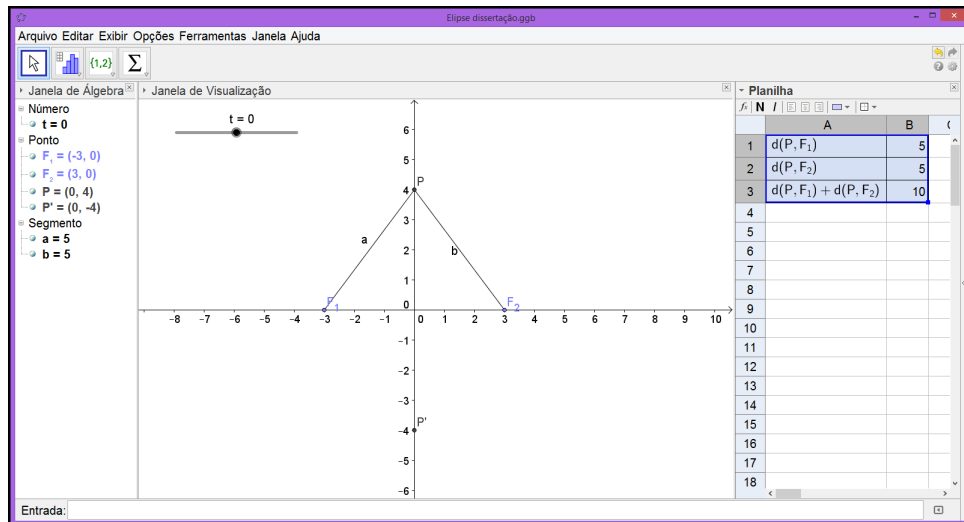


Figura 2: Usando recurso planilha.

**PASSO 2.** Selecione a tabela e clique sobre a parte selecionada com o botão direito do *mouse*, clique com o esquerdo em Criar e depois em Tabela (Figura 3); a tabela ficará visível na *Janela de Álgebra*.



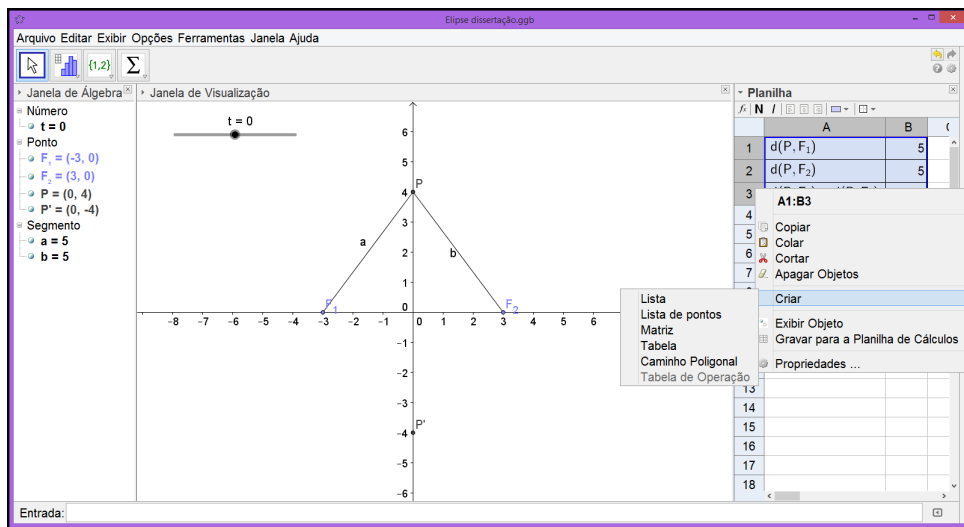


Figura 3: Tabela de dado

**PASSO 3.** Com objetivo de mostrar a construção da elipse, usando a definição  $\mathcal{E} = \{P \in \mathbb{R}^2 | d(P, F_1) + d(P, F_2) = 10\}$ , onde  $P$  depende apenas do parâmetro  $t$ , fazemos o parâmetro  $t$  variar mostrando, na tabela, que para as diferentes posições do ponto  $P$  as distâncias  $d(P, F_1)$  e  $d(P, F_2)$  variam, mas a soma das mesmas permanece constante (Figura 4).

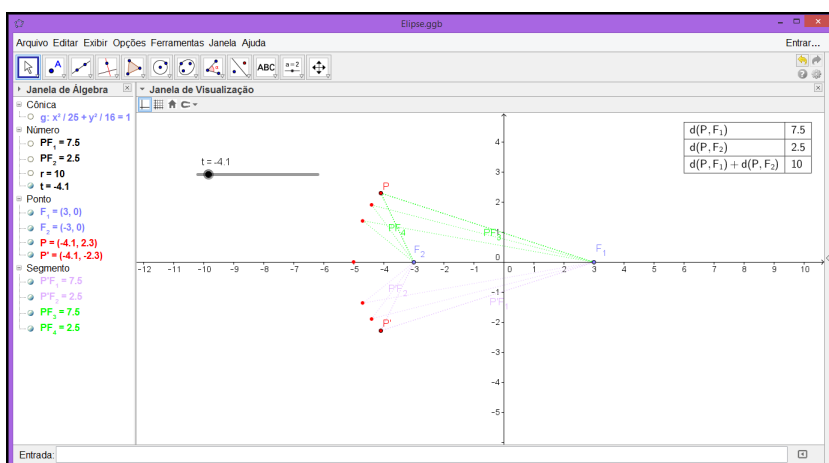


Figura 4: Conjunto de pontos 1.

**PASSO 4.** Com a variação de  $t$  podemos observar que a soma das distâncias de  $P$  aos focos  $F_1$  e  $F_2$  permanece constante, podemos visualizar esse processo a seguir (Figura 5).

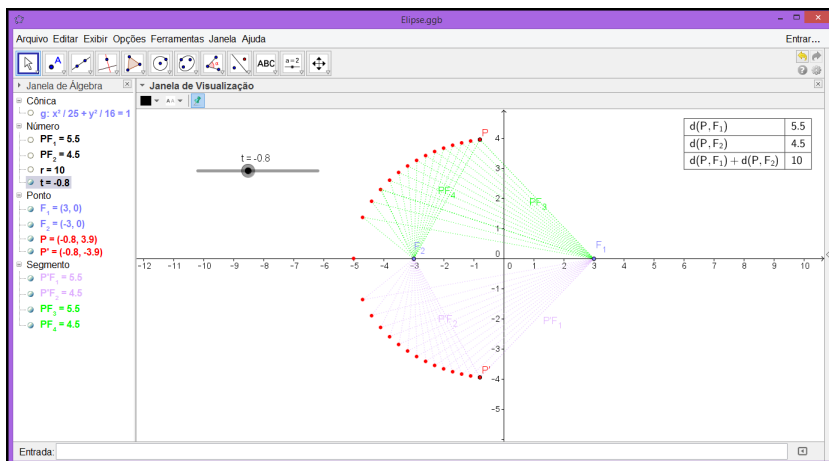


Figura 5: Conjunto de pontos 2.

PASSO 5. Para  $t$  próximo de 5 (Figura 6).

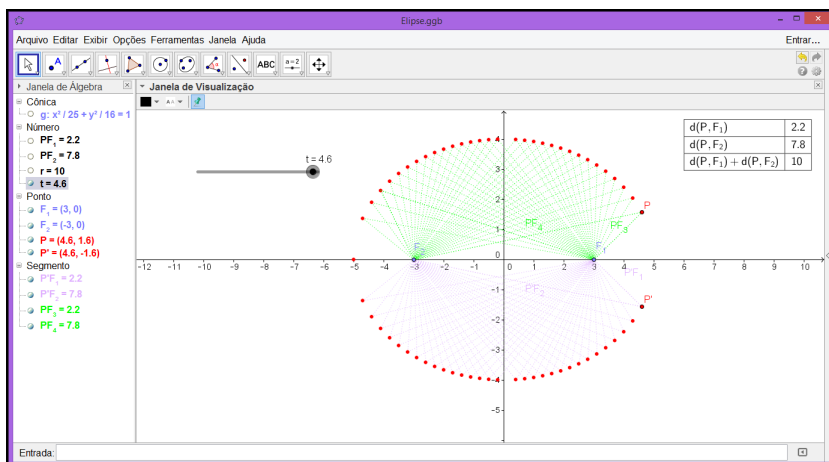


Figura 6: Conjunto de pontos 3.

PASSO 6. O lugar geométrico dos pontos  $P$  é a elipse  $\mathcal{E} : \frac{x^2}{25} + \frac{y^2}{16} = 1$  (Figura 7).

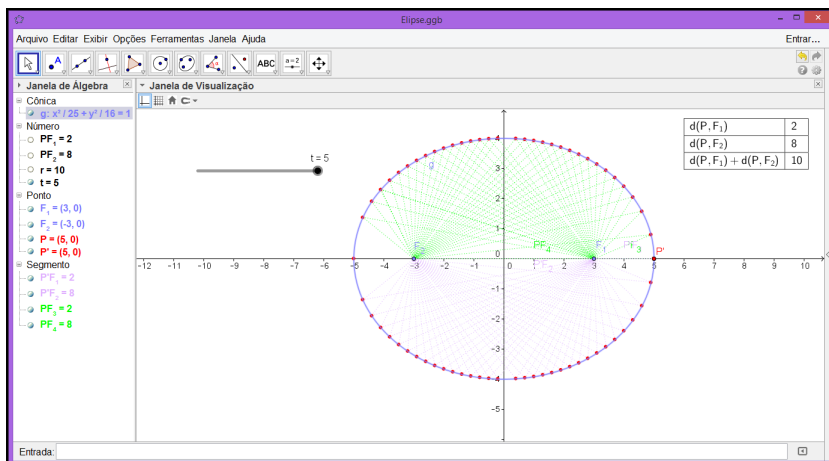


Figura 7: Elipse  $\mathcal{E}$ .

Destaca-se que, utilizando o *GeoGebra* pode-se substituir um recurso há muito utilizado no ensino da Elipse, o uso de cordão fixado em dois pregos (Focos) para mostrar sua definição.

### 4.3. Resolução de problema

Quanto à resolução de problema, utilizaremos como exemplo: Determine a equação da família de elipse com centro  $(2, 3)$ , reta focal paralela ao eixo  $OX$  e excentricidade  $\frac{1}{2}$ . Os passos para solução apresentam-se conforme seguem:

**PASSO 1.** Com a janela do *GeoGebra* aberta digite o ponto  $C = (2, 3)$  no campo *Entrada*, e, depois, com a finalidade de materializar as coordenadas, teclae *Enter* (Figura 8).

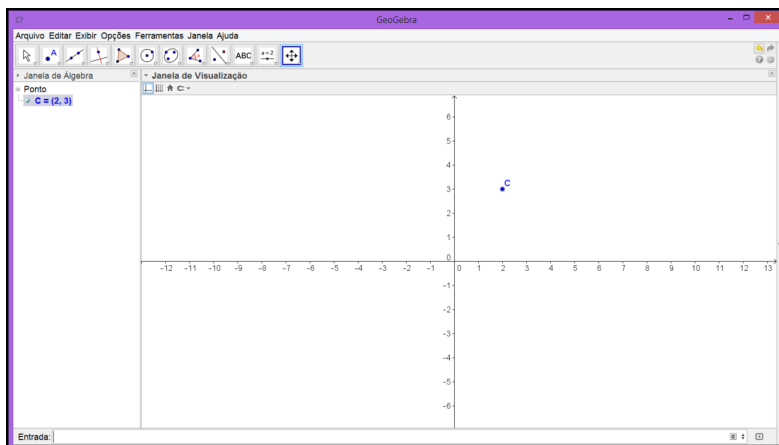


Figura 8: Centro da Elipse.

**PASSO 2.** Selecione o ícone *Reta Paralela*, depois com o botão direito do *mouse* clique no ponto *C* e sobre o eixo *x* (Figura 9).

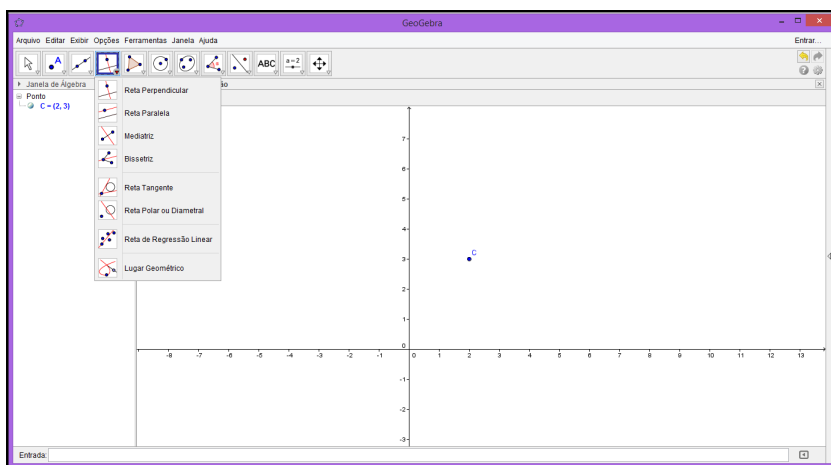


Figura 9: Reta Focal.

**PASSO 3.** A excentricidade  $E = \frac{c}{a} = \frac{1}{2}$ , fazendo  $c = t$ , temos  $a = 2t$ , onde  $t$  é um número real maior que zero. Precisamos criar um parâmetro. Com o botão direito do *mouse* clique no ícone *Controle Deslizante* e depois em qualquer lugar do campo *Janela de Visualização* (Figura 10).

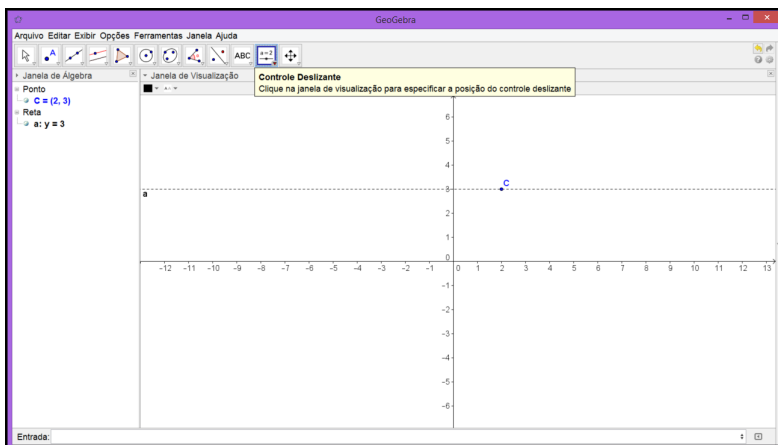


Figura 10: Parâmetro  $t$ .

**PASSO 4.** Na janela menor determine o nome e o intervalo e clique em *Aplicar* (Figura 11).

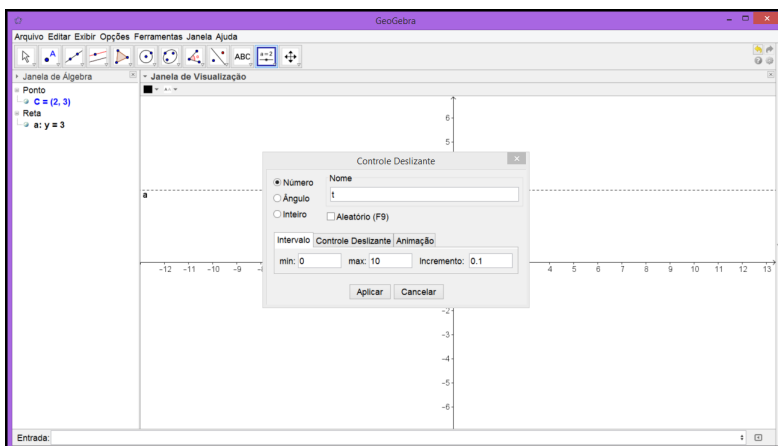


Figura 11: Controle Deslizante.

**PASSO 5.** Os focos  $F_1$  e  $F_2$  e os vértices  $A_1$  e  $A_2$  dependem do parâmetro  $t$ . Digite no campo *Entrada* os pontos  $F_1 = (2 - t, 3)$ ,  $F_2 = (2 + t, 3)$ ,  $A_1 = (2 - 2t, 3)$  e  $A_2 = (2 + 2t, 3)$ , um a um, teclando *Enter* posteriormente (Figura 12).

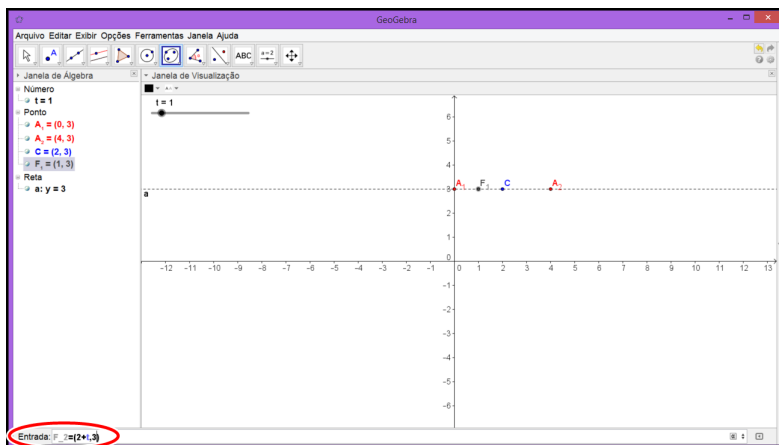


Figura 12: Foco da Elipse.

**PASSO 6.** Com o botão esquerdo do *mouse* selecione o ícone *Elipse*, depois clique sobre  $F_1$ ,  $F_2$  e em  $A_1$  ou  $A_2$ , nessa ordem. Temos a elipse de focos  $F_1$  e  $F_2$  (Figura 13).

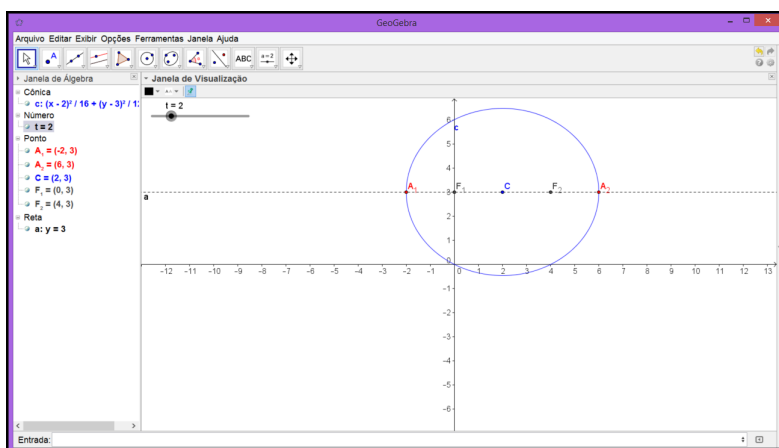


Figura 13: Elipse.

**PASSO 7.** Fazendo o parâmetro  $t$  variar, temos uma família de elipses (Figura 14).

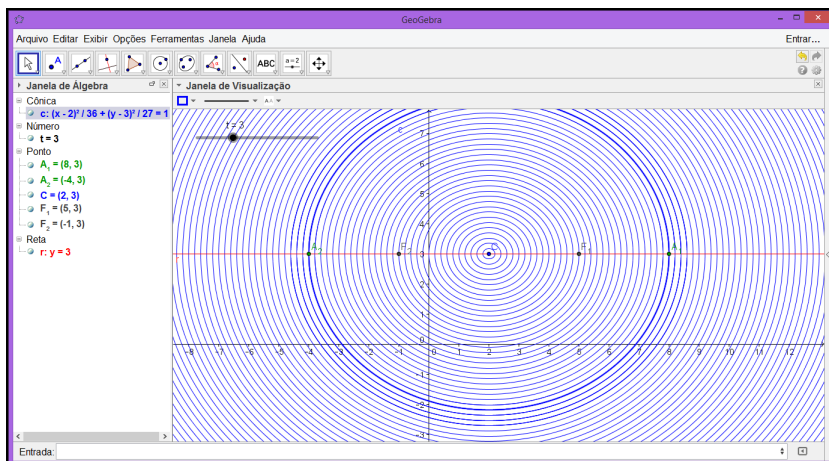


Figura 14: Família de Elipse.

Podemos concluir que a equação é da forma

$$\frac{(x - 2)^2}{4t^2} + \frac{(y - 3)^2}{3t^2} = 1.$$

## 5. Estudo da elipse a partir da sequência didática

Em uma perspectiva histórica, o Ensino da Matemática insere-se no escopo das abordagens tradicionais da Educação. Nessas abordagens a ênfase do ensino da área é dada à aquisição de conteúdos através da memorização e fixação, em detrimento das possibilidades metodológicas para a apropriação dos conhecimentos matemáticos. Essa realidade, ainda muito presente nas Escolas da Educação Básica, vem contribuindo para consequências negativas desse ensino, sobretudo no que diz respeito ao processo de transposição da concretude à abstração de conceitos matemáticos ([5]).

Nesse sentido, faz-se necessário a discussão sobre as possibilidades metodológicas para esse ensino que trate, especificamente, da questão abordada neste estudo: como os conceitos da Elipse podem ser apropriados pelos alunos da Educação Básica, através do uso do *GeoGebra*? Desta forma, sugerimos nas discussões que seguem a proposição de uma sequência didática para o estudo da elipse com o uso do *software*, e que apresenta os seguintes objetivos específicos:

- Reconhecer Elipse como seção da superfície do cone duplo;
- Obter, por meio de definição, a equação da Elipse;
- Identificar na Elipse os focos, a distância focal, os eixos, o centro e os vértices;
- Inserir a matemática no cotidiano do aluno, mostrando sua presença em várias situações de forma clara e objetiva;
- Trabalhar as construções geométricas com o uso do *GeoGebra*;

- Relacionar os aspectos algébricos com os geométricos;
- Inserir um *software* de geometria dinâmica como ferramenta ao processo de ensino-aprendizagem.

O alcance desses objetivos foi observado durante todo o desenvolvimento da sequência didática e será analisado, neste texto, na discussão sobre a avaliação dos alunos a respeito do uso do *software*, logo após ser explicitada a elaboração e o contexto de aplicação da sequência didática.

### 5.1. Contexto de elaboração e aplicação da sequência didática

As sequências didáticas são perspectivas de encadeamento e articulação de um conjunto de atividades que buscam o ensino de um determinado conteúdo. Através das sequências podemos acompanhar as diferentes formas de resolução das atividades que se realizam e, principalmente, pelo sentido que adquirem quando uma sequência orientada para a realização de determinados objetivos do conteúdo.

No caso deste estudo, o conteúdo em foco, a Elipse, foi apresentado aos estudantes considerando a necessidade de apropriação dos seus conceitos de forma inovadora e eficaz, inibindo, dessa forma, as experiências tradicionais suscetíveis à desmotivação e dificuldades de aprendizagem desses sujeitos, sobretudo ao entendimento de conceitos abstratos que fundamentam o conteúdo. A pesquisa foi aplicada no Instituto Federal de Alagoas-IFAL, *campus* Palmeira dos Índios, no mês de março de 2015. A sequência didática foi realizada em uma turma de terceiro ano do curso de Eletrotécnica - em tese, todos os alunos já tendo conhecimento prévio de geometria analítica. Para uso das atividades realizadas pelos alunos, foram solicitadas autorizações aos pais, através do Termo de Consentimento Livre e Esclarecido.

A análise dos dados produzidos pela pesquisa foi realizada através de observações durante a aula expositiva, na aplicação das atividades, das atividades respondidas pelos alunos e dos comentários feitos por eles. A turma é formada por dez alunos que compareceram a todos os encontros propostos. Para garantir o anonimato dos sujeitos da pesquisa, os alunos serão identificados apenas por códigos A1, A2, ... A10.

Utilizando os estudos desenvolvidos no decorrer dessa pesquisa sobre Elipse e o material didático utilizado da turma, Livro Didático ([1]) - LD adotado pelo Instituto para o terceiro ano do ensino técnico integrado, foi elaborada uma sequência didática com duração de quatro horas e dez minutos de forma presencial e uma hora e quarenta minutos a distância. As aulas foram realizadas no laboratório de informática do *campus*.

O primeiro encontro corresponde a duas aulas de cinquenta minutos. Nesse encontro foi realizada uma exposição do conteúdo seguindo as orientações do LD adotado, apresentando as demonstrações algébricas das equações reduzidas da Elipse, bem como a solução analítica de problemas. Assim sendo, nesse encontro, a sequência didática foi desenvolvida através de uma aula expositiva, tendo o professor como transmissor do conteúdo, utilizando o quadro branco e pincel para sistematizar a exposição. Durante o desenvolvimento da aula havia abertura para perguntas e considerações dos alunos.

No segundo encontro, com duração de uma hora e quarenta minutos, e partindo dos estudos anteriores com o uso do *software GeoGebra*, foi realizada a exposição do conteúdo Elipse. Essa exposição pode ser acompanhada pelos alunos através da projeção do *software* e utilização de todos



os passos já elencados quando da discussão, nesse texto, sobre o uso do *GeoGebra*. No decorrer desse momento da sequência, professor e alunos foram revisitando as orientações sobre o uso das ferramentas necessárias ao desenvolvimento das atividades propostas.

A última aula presencial teve duração de cinquenta minutos. Nessa aula os alunos foram convidados a resolver uma questão do LD utilizando o *software* e com a orientação do professor. A atividade realizada pelos alunos pode ser apresentada da seguinte forma:

1. Esboce o gráfico da elipse em cada um dos casos.

(a)  $\frac{(x - 9)^2}{25} + \frac{(y - 6)^2}{9} = 1;$

(b)  $\frac{(x + 4)^2}{16} + \frac{y^2}{9} = 1;$

(c)  $\frac{x^2}{16} + \frac{y^2}{36} = 1;$

Quanto à solução da atividade, a maioria dos alunos encontrou os vértices e os focos através de manipulações algébricas e em seguida usaram a ferramenta Elipse dados Focos e um de seus Pontos, assim como pode-se observar na janela Protocolo de Construção (Figura 15).

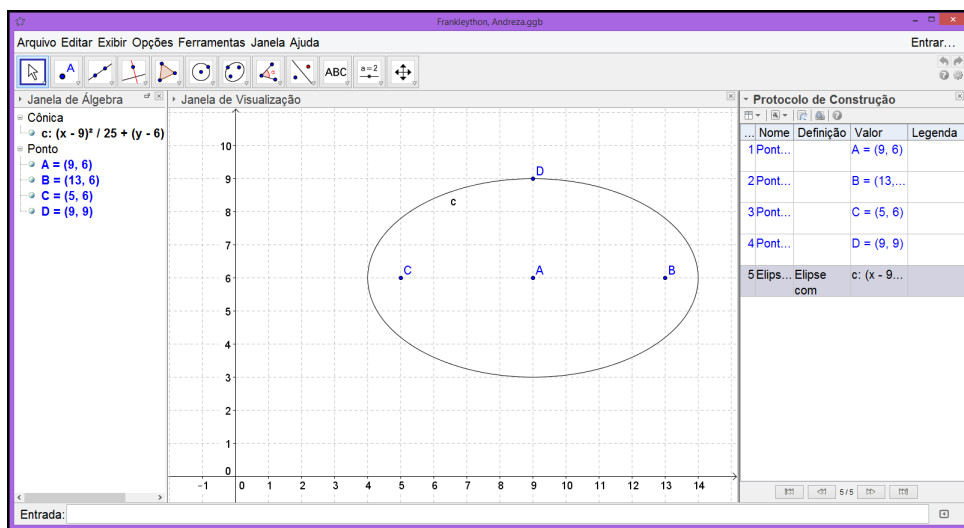


Figura 15: Solução 1.

Apenas um aluno, que já tinha conhecimento prévio sobre o uso do *GeoGebra*, resolveu a questão digitando as equações das elipses diretamente no campo Entrada (Figura 16)

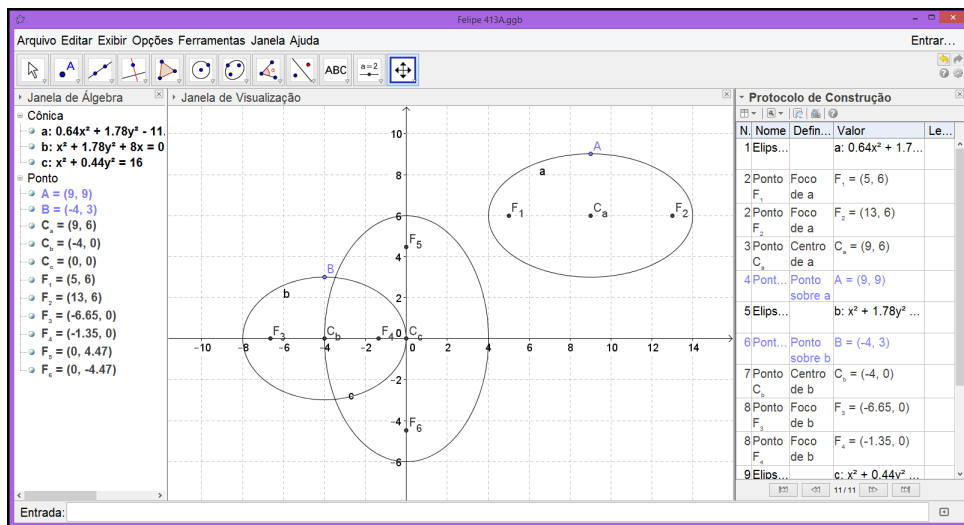


Figura 16: Solução 2.

O último momento da sequência ocorreu através de atividades a distância. Essas atividades consistiram em resolver duas situações problema, com o uso do *GeoGebra*, envolvendo o estudo das seções cônicas acompanhado de um breve comentário sobre o uso do *software* como ferramenta de ensino, baseando-se nos encontros anteriores. As soluções das atividades foram encaminhadas para o *e-mail* do professor.

## 5.2. Avaliação dos alunos sobre o uso do *GeoGebra*

Conforme foi explicitado durante a descrição da sequência didática, o último momento com os alunos foi destinado à avaliação da experiência com o uso do *GeoGebra* para o ensino da Elipse. Essa avaliação foi realizada a partir do registro dos comentários dos alunos. Tais comentários serão reproduzidos na íntegra, entretanto, não haverá identificação dos discentes, usaremos aqui apenas códigos, A1, A2, ..., A10.

Através da análise dos comentários é possível observar que os alunos compreenderam o conteúdo proposto a partir do uso do *software*. Os comentários de A1 e A4 apresentam-se carregados das discussões e explicações realizadas na turma, além do entendimento de como funciona o *software* para o estudo sobre Elipse. Esse entendimento permitirá que os alunos utilizem o *GeoGebra* mesmo que não estejam na escola, em momento de aula. Podem, dessa forma, continuar estudando em espaços não escolares, favorecendo o fortalecimento do hábito de estudo e, conseqüentemente, a aprendizagem do conteúdo, conforme seguem os comentários:

*Foi uma aula gratificante, pois podemos aprender um assunto que é bem explorado em diversos setores: Seções Cônicas e com o uso do aplicativo do GeoGebra um*

programa que permite realizar construções geométricas com a utilização de pontos, retas, segmentos de reta, polígonos etc., assim como permite inserir funções e alterar todos esses objetos dinamicamente, após a construção estar finalizada. Equações e coordenadas também podem ser diretamente inseridas. Portanto, o GeoGebra é capaz de lidar com variáveis para números, pontos, vetores, derivar e integrar funções, e ainda oferecer comandos para se encontrar raízes e pontos extremos de uma função. Com isso, o programa reúne as ferramentas tradicionais de geometria com outras mais adequadas à álgebra e ao cálculo. Aprendemos ainda como construir uma elipse no aplicativo e por meio do professor Gracino, aprendemos a chegar à equação reduzida da elipse e a partir dela ir para diversos setores da área. (A1)

A seguinte aula nos trouxe um amplo conhecimento do software utilizado para a obtenção dos gráficos de uma elipse com precisão. Esta aula nos mostrou que o software utilizado, GeoGebra, facilita a obtenção do gráfico com exatidão, coisa que não seria obtida em uma aula teórica, pois os gráficos não sairiam com dimensões corretas. Com o uso do software GeoGebra, as aulas se tornam mais dinâmicas, práticas e mais compreensível por parte do aluno. (A4)

Os comentários de A3, A5, A7 e A10 revelam o anseio dos alunos em vivenciar experiências de ensino-aprendizagem que rompam com as metodologias tradicionais que norteiam as aulas de matemática na Educação Básica. Não se trata de supervalorizar as metodologias inovadoras do ensino em detrimento da contribuição das abordagens tradicionais, mas da assunção do papel do professor, como sujeito mediador do processo de ensino-aprendizagem, que percebe a fragilidade de determinadas proposições metodológicas e que, a partir dessa percepção, propõe possibilidades para a consolidação desse processo. Tal reflexão pode ser identificada nos comentários que seguem:

O GeoGebra é um excelente programa para o ensino aprendizagem, pois, além de fazer cálculos matemáticos de álgebra e geometria, possibilita a construção de gráficos. Com o GeoGebra também é possível inserir equações e coordenadas diretamente nos gráficos. A aula ministrada foi sobre cônicas, e, como o assunto envolve muitos gráficos, o GeoGebra pôde ser mais aproveitado. Foram feitos gráficos de elipses, parábolas e aprendemos a obter pontos notáveis, como os focos da elipse. **Utilizando o programa, a aula torna-se mais dinâmica em relação às aulas tradicionais, pois promove uma maior interação entre os alunos e o professor e mostra uma matemática mais aproximada do cotidiano.** (A3)(grifo nosso)

As aulas no laboratório, chamam mais atenção dos alunos. Elas são atrativas, e como é um método novo de ensino, os alunos tendem a prestar mais atenção na hora da explicação, e com isso o rendimento do aluno será melhor. (A5)

*A aula no laboratório proporcionou para nós, alunos, o contato direto com um programa que, a princípio, não tínhamos um conhecimento aprofundado sobre tal ou nunca tivemos oportunidade de manusear. **A aula se tornou algo atrativo, pelo simples fato do professor ter utilizado uma metodologia diferenciada da que vivenciamos cotidianamente.** O uso do GeoGebra despertou o interesse por tal conteúdo, assim como o “facilitamento” da construção de gráficos das mais diversas formas e a realização dos cálculos de álgebra. (A7)(grifo nosso)*

*A aula no laboratório com o professor Gracino foi de extrema importância, pois a partir dela tivemos um conhecimento importante para o aprendizado da matemática, **tornando a aula mais atrativa e dinâmica.** Aprendemos algumas coisas no que diz respeito ao GeoGebra e suas funções. A aula serviu também para que fizéssemos exercícios para a utilização do GeoGebra a nosso favor, pois o uso do programa nos permite provar o que foi calculado, além da melhor visualização. (A10)(grifo nosso)*

Os comentários de A2, A6 e A8, comprovam a defesa de que a abstração de conceitos matemáticos pode ser apreendida pelos alunos com maior facilidade a partir de um instrumento que transponha essa abstração à concretude. É comum, entre os alunos da Educação Básica, a máxima “é muito difícil aprender matemática”. Entretanto essa afirmação está relacionada muito mais à metodologia e instrumentos aplicados a esse ensino do que à complexidade dos conteúdos da área. Acredita-se que as explicações e demonstrações de conceitos realizados apenas através de aulas expositivas e estudo de livros didáticos, distanciam a reflexão dos alunos sobre o conteúdo, ficando a compreensão desses apenas no campo das ideias.

O *GeoGebra* é um instrumento que permite (re) construir os conceitos pelos próprios alunos. Essa (re) construção é realizada por etapas e acompanhadas *pari passo* pelo professor mediador. Os alunos são protagonistas dessa construção e, dessa forma, os conceitos deixam de ser apenas transmitidos, e passam a ser (re) construídos pelo sujeito aprendente. Essa defesa pode ser constatada nos comentários que seguem:

*Eu participei de uma aula diferente com o professor [...], abordando seções cônicas. **No começo da aula, quando as fórmulas foram demonstradas apenas com relações matemáticas, ficou um pouco confuso de se entender. Porém, ao desenhar e explicar pelo GeoGebra, tudo ficou mais claro e fácil.** (A2)(grifo nosso)*

*A aula no laboratório para o estudo desse assunto em questão é excelente, **pois com o uso do programa permite provar o que foi calculado e a melhor visualização.** A aula no laboratório com isso se torna um grande instrumento adicional no aprendizado da matemática (A6)(grifo nosso)*

*O software GeoGebra se mostrou, didaticamente, simples de ser utilizado. Facilitando, assim, a compreensão de gráficos que muitas vezes se tornam difíceis de serem reproduzidos no quadro de modo a atender a necessidade de entendimento do aluno. A utilização do programa torna a aula, além de melhor compreendida, mais dinâmica e prende a atenção dos alunos pela curiosidade de ver o programa em funcionamento. Vale ressaltar que continua sendo necessária a utilização do quadro para explicar a parte dos cálculos referentes ao assunto em questão para que o aluno não seja prejudicado quando necessário fazer cálculos matemáticos. (A8)(grifo nosso)*

Diante do exposto, considera-se que oportunizar a fala dos alunos sobre a experiência proposta possibilitou, para além da constatação das defesas teóricas sobre o uso do *GeoGebra*, também a compreensão de que as dificuldades de aprendizagem dos alunos sobre os conceitos matemáticos não estão centradas na incapacidade desses sujeitos em aprender, mas na fragilidade da proposição metodológica para essas aulas.

## 6. Considerações finais

A utilização de um programa de geometria dinâmica, no caso desse estudo o *GeoGebra*, otimiza o tempo disposto à exposição do conteúdo Elipse, de modo que facilita a obtenção de gráficos, além de proporcionar uma construção com exatidão que, muitas vezes, torna-se difícil de serem reproduzidas utilizando apenas quadro e giz.

Outro fator a ser observado é o dinamismo que ganha a aula em relação às aulas tradicionais, pois as construções geométricas feitas pelo *GeoGebra* preservam suas propriedades mesmo após serem manipuladas, permitindo distinguir elementos variantes e invariantes de uma figura geométrica, bem como sua relação com as equações algébricas. Vale ressaltar que o uso de um programa de geometria dinâmica não exclui as demonstrações analíticas; a utilização de quadro e giz é necessária para a exposição da parte algébrica.

O *GeoGebra* também se mostrou eficaz na resolução de exercícios, pois o uso do programa permite provar o que foi calculado analiticamente. Em atividades a distância o professor pode usar a janela *Protocolo de Construção*, que pode ser acessada no menu *Exibir*, para verificar a ordem dos passos dados pelos alunos, ou seja, os procedimentos podem ser revistos tanto pelo aluno quanto pelo professor, essa função de grande importância para a correção dos exercícios, para orientações futuras e para acompanhamento das aulas a distância. Com o *GeoGebra* o aluno aprende fazendo, ou melhor, construindo.

Dessa forma, considera-se que os objetivos do trabalho foram alcançados, sobretudo no que diz respeito ao desenvolvimento de metodologias utilizando a ferramenta tecnológica da informática, em particular o *software* de geometria dinâmica, que podem ser usados como material orientador para professores da Educação Básica.

Atualmente, na maioria das escolas públicas, existem recursos tecnológicos disponíveis para serem usados em sala de aula com a intenção de facilitar o processo de ensino-aprendizagem. No entanto, esses recursos ainda são pouco utilizados, haja vista as dificuldades de aplicação técnica e operacional. Espera-se, desta forma, que este estudo possa contribuir para reverter tal realidade, oferecendo dados produzidos e analisados de uma experiência de pesquisa sobre a aplicação do uso de um *software* em aulas do Ensino da Matemática.

## Referências

- [1] Dante, Luiz R. *Matemática: contexto e aplicação*. Volume 3, 2ª ed. São Paulo: Ática, 2013.
- [2] Delgado, Jorge; Frensel, Katia; Crissaff, Lhaylla. *Geometria Analítica*. Rio de Janeiro: SBM, 2013.
- [3] GeoGebra, Disponível em: <<https://www.geogebra.org/>>.
- [4] Instituto GeoGebra, Disponível em:<<https://www.geogebra.im.uff.mat.br>>.
- [5] Muniz Neto, Antônio C. *Geometria*. Rio de Janeiro: SBM, 2013.
- [6] Vainsencher, Israel. *Curvas Algébricas Planas*. Rio de Janeiro: IMPA, 2005.

Gracino Rodrigues  
Instituto Federal de Alagoas  
<[gracino.rodrigues@gmail.com](mailto:gracino.rodrigues@gmail.com)>

Elisabete de Oliveira  
Instituto Federal de Alagoas  
<[elisabete.ifal@gmail.com](mailto:elisabete.ifal@gmail.com)>

Recebido: 2017