Ciência e Natura, Santa Maria, v. 37 Ed. Especial PROFMAT, 2015, p. 452–462
Revista do Centro de Ciências Naturais e Exatas - UFSM
ISSN impressa: 0100-8307 ISSN on-line: 2179-460X

Uma Introdução às Curvas Elípticas com Aplicações para o Ensino Médio

An Introduction to Elliptic Curves with Application for Secondary Education

Joilma Silva Carneiro[1] e Kisnney Emiliano de Almeida[2]

[1,2] Universidade Estadual de Feira de Santana. BA, Brasil
joilma.carneiro@hotmail.com

Resumo

Este trabalho tem o objetivo de apresentar um material introdutório sobre as Curvas Elípticas, com algumas aplicações na forma de atividades para uso do professor de Ensino Médio. Curvas elípticas são curvas planas de grau 3 que podem ser equipadas com uma operação de grupo abeliano, definida geometricamente. Acreditamos que a apresentação do conceito de curvas elípticas, de uma maneira simplificada e intuitiva, pode ser muito enriquecedor para a formação dos alunos em várias sub-áreas da matemática.

Palavras-chave: *Curvas Elípticas, Ensino de Matemática, Curvas Planas.*

Abstract

This work aims to present an introductory text on Elliptic Curves, with some applications in form of activities for using of High school teachers. Elliptic Curves are plane curves of degree 3 that can be equipped with an operation of Abelian group geometrically defined. We believe the presentation of the concept of elliptic curves, in a simplified and intuitive way, may be very enlightening for the formations of students in several sub-areas of mathematics.

Keywords: *Elliptic Curves, Mathematics Teaching, Plane Curves.*

submissão: 2014-07-13 Aceito: 2014-12-02

1 Introdução

O estudo das curvas elípticas é uma área da Geometria Algébrica com aplicações em Teoria dos Números. Além disso, as curvas elípticas desempenharam uma papel fundamental na demonstração do último Teorema de Fermat. Neste artigo, nos limitamos aos aspectos mais elementares da Teoria de Curvas Elípticas e aplicações para o Ensino Médio.

Analisamos as curvas elípticas sob o ponto de vista da geometria algébrica clássica, ou seja, pensamos em uma curva elíptica como uma curva algébrica plana projetiva, *i.e.*, uma classe de equivalência de polinômios homogêneos não constantes $F \in \mathbb{R}[X,Y,Z]$, módulo a relação que identifica dois polinômios se um for múltiplo constante do outro. Sob essa ótica, o plano projetivo é o conjunto $P^2 := \frac{\mathbb{R}^3\setminus\{(0,0,0)\}}{\sim}$, onde a relação de equivalência $\sim$ é dada por $(x,y,z) \sim (tx,ty,tz)$ para todo $t > 0$. Denotamos um ponto de P^2, isto é, a classe de equivalência de um ponto não-nulo $(x,y,z) \in \mathbb{R}^3$, como sendo $(x : y : z)$. Os pontos do plano projetivo da forma $(x : y : 0)$ são chamados *pontos no infinito*. Existe uma correspondência natural entre curvas planas usuais (chamadas na geometria projetiva de "curvas afins") e curvas projetivas: Dada uma curva plana definida por uma equação polinomial $f(x,y) = 0$ de grau n, a mesma está associada à curva projetiva $F(X,Y,Z) = Z^n f(\frac{x}{z},\frac{y}{z})$. Reciprocamente, uma curva projetiva plana $F(X,Y,Z)$ está associada à curva afim $f(x,y) = F(X,Y,1)$. Embora esses conceitos sejam muito complexos para o ensino básico e não sejam necessários para as aplicações, fazem parte da fundamentação teórica de curvas elípticas. Para mais detalhes sobre o plano projetivo e curvas projetivas planas, *cf.* [3], [6] e [8] e [9].

É sabido que toda curva elíptica que possui pelo menos um ponto com coordenadas racionais pode ser escrita, após uma mudança de variáveis conveniente, na chamada Forma de Weierstrass, que simplifica muito os cálculos envolvidos. Nesse contexto, já definimos uma *curva elíptica sobre* $\mathbb{Q}$ em sua forma de Weierstrass, ou seja, como a curva definida por uma equação do tipo

$$y^2z = x^3 + axz^2 + bz^3,$$

com $a, b \in \mathbb{Q}$ e $\triangle = 4a^3 + 27b^2 \neq 0$. Mais detalhes sobre curvas elípticas e suas formas de Weierstrass, *cf.* [1], [6], [9], [10] e [11].

O estudo de curvas elípticas se torna mais interessante a partir de sua estrutura algébrica intrínseca. Dizemos que um conjunto não-vazio equipado com uma operação é um grupo abeliano se são satisfeitas as propriedades de comutatividade, associatividade, elemento neutro e elemento inverso. É possível definir geometricamente uma operação entre os pontos de uma curva elíptica qualquer de modo que a curva, equipada com essa operação, se constitui como um grupo abeliano. Essa propriedade permite o uso de técnicas de teoria de grupos para estudar curvas elípticas e traz grande destaque ao estudo dessas curvas dentro da Geometria Algébrica.

O problema de calcular pontos com coordenadas racionais sobre uma curva elíptica fascinou matemáticos desde a época dos gregos antigos, mas só em 1922 foi provado por Louis Mordell que é possível a construção de todos os pontos a partir de um número finito de secantes e tangentes - que consistem exatamente na aplicação sucessiva da operação de grupo. Em outras palavras, o famoso Teorema de Mordell garante que os pontos com coordenadas racionais de uma dada curva elíptica formam um (sub)grupo finitamente gerado, o que impulsionou as investigações sobre o assunto desde então.

Por mais que as definições formais e demonstrações sejam complexas, o conceito de curva elíptica, sua operação de grupo e sua visualização geométrica, bem como os cálculos envolvidos, são simples. Dessa forma, se torna possível uma introdução ao conceito de curvas elípticas no Ensino Médio, que dá oportunidade para que os alunos exercitem conteúdos como: plano cartesiano, polinômios, geometria plana, geometria analítica, interseção entre curvas, dentre outros. Além disso, o tópico atuaria como uma introdução à matemática abstrata, em particular ao conceito de estrutura algébrica, aspecto raro em nosso currículo do Ensino Médio.

Vale salientar que a maioria das figuras deste artigo e, consequentemente, das atividades que aplicaremos, foi construída com o auxílio do aplicativo Geogebra. Para informações sobre este aplicativo, *cf.* [4].

O Geogebra é um *software* gratuito de matemática dinâmica desenvolvido para o ensino e aprendizagem da matemática no vários níveis de ensino (do básico ao universitário), reunindo recursos de geometria, álgebra, tabelas, gráficos, probabilidade, estatística e cálculos simbólicos em um único ambiente. Este *software* é uma excelente ferramneta para criar ilustrações e gráficos. Além disso, não podemos deixar de destacar o quanto é importante aliar a tecnologia à realidade escolar, motivando e instrumentalizando o processo de construção do conhecimento matemático.

2 Curvas Elípticas

2.1 Um pouco de História

Neste artigo, faremos um estudo das Curvas Elípticas sobre o corpo dos números racionais utilizando um tratamento geométrico e algébrico para a compreensão das

operações com pontos pertencentes à curva. Seguiremos as abordagens feitas por [1], [6], [8] e [9].

O estudo de Curvas Elípticas surgiu a partir dos problemas da Teoria dos Números. A Teoria das Equações Diofantinas é uma corrente da Teoria Numérica que trata de soluções de equações polinomiais contidas nos números inteiros ou nos números racionais. Existem muitos problemas famosos em equações diofantinas. Um dos mais famosos problemas na história da Matemática e talvez um dos que mais inspirou o desenvolvimento de novas teorias é o chamado *Último Teorema de Fermat.*

Pierre Fermat, que tinha o costume de fazer anotações nas margens de sua cópia do livro de Diofanto, enunciou o teorema que afirma ser impossível encontrar inteiros positivos x, y, z tais que:

$$x^n + y^n = z^n \tag{1}$$

quando n é um inteiro maior do que 2.

Um outro exemplo é o problema da escrita de números inteiros ou racionais como a diferença entre um quadrado e um cubo, que equivale a procurar soluções inteiras ou racionais da equação

$$y^2 - x^3 = c. \tag{2}$$

Estudaremos, neste artigo, problemas com certas equações polinomiais de grau 3, chamadas *curvas elípticas*. Vale salientar que curvas elípticas não são elipses, uma vez que elipses são seções cônicas e seções cônicas são dadas por equações do segundo grau. Estas curvas denominam-se elípticas porque surgem no estudo de uma classe específica de funções complexas chamadas *funções elípticas*.

2.2 Caracterização de Curvas Elípticas

Definição 2.1. Uma *curva projetiva plana* definida por uma equação da forma

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{3}$$

com $a, b \in \mathbb{Q}$ e $\triangle = 4a^3 + 27b^2 \neq 0$ é denominada *curva elíptica* sobre $\mathbb{Q}$.

Observemos que a curva acima é união da curva afim de equação

$$y^2 = x^3 + ax + b \tag{4}$$

(considerando $z = 1$) a um único "ponto no infinito" $O = (0 : 1 : 0)$, interseção da curva projetiva acima com a "reta no infinito" $Z = 0$, pois escrevendo a equação (4) na forma projetiva, temos:

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Tomando $Z = 0$, temos o ponto $(0 : 1 : 0)$. Por este motivo, muitas vezes, ao fazermos as contas, trabalharemos com a equação afim (4), até porque no ensino médio precisamos trabalhar com curvas afins no plano.

Vejamos uma curva elíptica, por exemplo

$$y^2 = x^3 - x (Fig 1)$$

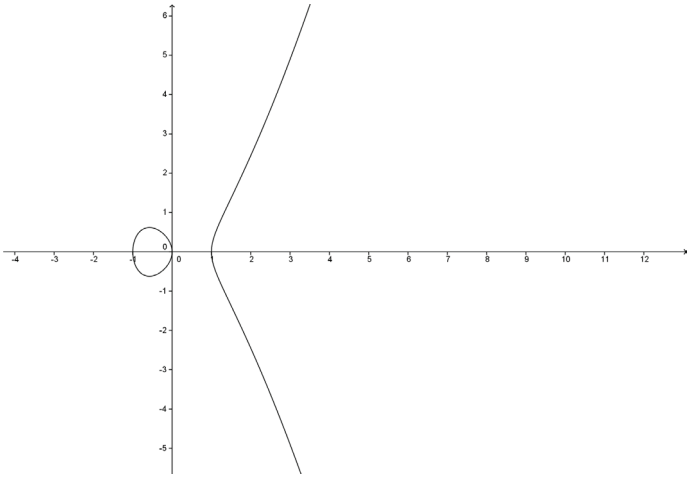

Figura 1: Uma curva elíptica

A condição do discriminante na definição de curva elíptica é importante para garantir que a curva seja *lisa*; *cf.* [3] e [9]. Curvas lisas são curvas que não contém *pontos singulares*, isto é, para as quais existe uma reta tangente bem definida em cada um dos pontos da curva.

Vejamos exemplos de algumas curvas de grau 3 abaixo que não são elípticas:

$$y^2 = x^3 + x^2, \quad \triangle = 0;$$

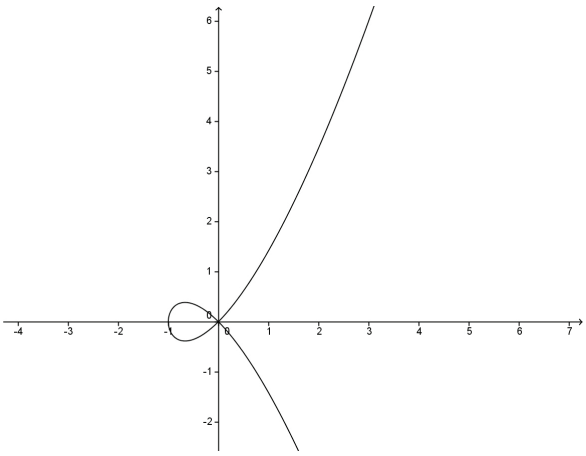

Figura 2: Uma curva com um ponto singular

$$y^2 = x^3, \quad \triangle = 0. (Fig.3)$$

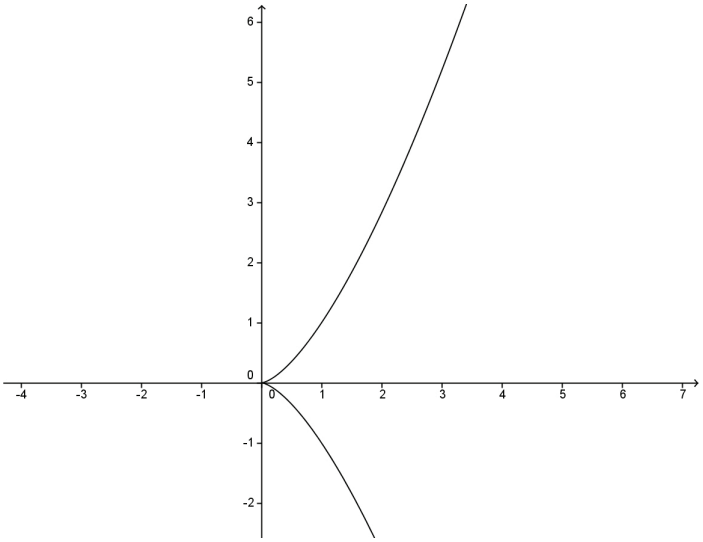

Figura 3: Uma curva com um ponto singular

Observação 2.2. É importante saber que as curvas elípticas que consideraremos em nossos exemplos estão na chamada *Forma Normal de Weierstrass*:

$$y^2 = x^3 + ax + b. \tag{5}$$

Toda curva elíptica com pelo menos um ponto com coordenadas racionais pode ser colocada nessa forma através de uma mudança conveniente de variáveis. Neste artigo, não faremos a prova desta transformação, basta consultar [7] e [9].

Veremos abaixo um exemplo da passagem da equação cúbica para a Forma Normal de Weierstrass:

Exemplo 2.3. Seja a cúbica de equação:

$$n^3 - n - m^2 - m = 0.$$

Fazendo a substituição de variável, $m = y - \frac{1}{2}$ e $n = x$, temos:

$$x^3 - x - \left(y - \frac{1}{2}\right)^2 - y + \frac{1}{2} = 0.$$

$$x^3 - x - \left(y^2 - y + \frac{1}{4}\right) - y + \frac{1}{2} = 0.$$

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

Temos assim, a forma de Weierstrass.

A proposição a seguir evidencia a coerência do modelo proposto pela Geometria Projetiva: todas as retas paralelas ao eixo vertical se encontram em um ponto no infinito, que poderia ser pensado com o ponto no horizonte vertical. Seria possível provar resultados semelhantes para cada uma das direções do plano - por exemplo, toda reta horizontal passa pelo ponto no infinito $(1:0:0)$. Evidenciamos esse resultado em particular porque ele será útil na sequência deste artigo.

Proposição 2.4. *Toda reta afim é vertical se, e somente, passa pelo ponto no infinito* $(0:1:0)$.

Demonstração. $\Longrightarrow$:
Se uma reta afim é vertical, temos que sua equação é da forma:

$$x = c.$$

Escrevendo na forma projetiva, temos:

$$X = cZ. \tag{6}$$

Agora, para verificar que toda reta vertical passa pelo ponto no infinito , basta substituir $(0:1:0)$ na equação (6).
$\Longleftarrow$:
Provaremos a volta usando a contrapositiva do enunciado. Considerando a reta afim não vertical

$$ax + by = c, \quad b \neq 0 \tag{7}$$

e escrevendo-a (7) na forma projetiva, temos a equação

$$aX + bY = cZ, \quad b \neq 0. \tag{8}$$

Substituindo o ponto no infinito $(0:1:0)$ na equação (8) chegamos a uma contradição, encontrando $b = 0$. □

2.3 A Geometria das Curvas Elípticas

Iniciaremos esta seção enunciando o teorema abaixo que será importante no decorrer deste artigo.

Teorema 2.5. ***(Teorema de Bezout)*** *Sejam C_1 e C_2 duas curvas projetivas planas sem componentes comuns, então o número de pontos na interseção $C_1 \cap C_2$, contados com a multiplicidade, é igual a $\delta(C_1) \cdot \delta(C_2)$.*

Demonstração. cf. [9]. □

Exemplo 2.6. Considere a reta afim

$$C_1 : x - y = 0,$$

e

$$C_2 : x^3 - y^2 = 0. \tag{9}$$

Analisaremos a interseção entre estas curvas afins.

Substituindo $y = x$ na equação (9), temos:

$$x^3 - x^2 = 0.$$
$$x^2(x-1) = 0.$$

$$x^2 = 0 \quad \text{ou} \quad x = 1.$$

Portanto, a solução da interseção entre as curvas é $(0,0)$, com multiplicidade 2, e $(1,1)$. Logo, $\#(C_1 \cap C_2) = 3$. As curvas C_1 e C_2 não têm componentes em comum, portanto é possível aplicar o Teorema de Bezout e assim

$$\#(C_1 \cap C_2) = \delta(C_1) \cdot \delta(C_2) = 1 \cdot .3 = 3$$

Observação 2.7. Quando estamos contando interseções, estamos considerando a multiplicidade.

Mais detalhes e exemplos do Teorema de Bezout, consultar [1].

Se temos dois pontos com coordenadas racionais sobre uma curva, então podemos geralmente encontrar o terceiro. Inicialmente, desenhamos a reta determinada por estes dois pontos; esta reta será uma reta com coeficientes racionais e se encontra com a cúbica em mais um ponto, pelo Teorema de Bezout (*cf.* [11]). Em seguida, para calcularmos as três interseções entre a reta com coeficientes racionais com uma cúbica com coeficientes racionais, teremos uma equação cúbica com coeficientes racionais. Se duas raízes forem racionais, então a terceira também será. Trabalharemos com alguns exemplos que nos permitirão encontrar algum tipo de *lei de composição*: Começaremos com dois pontos P e Q; em seguida, traçaremos a reta que passa por P e Q e denotaremos $P * Q$ como sendo o terceiro ponto da interseção da reta com a cúbica.

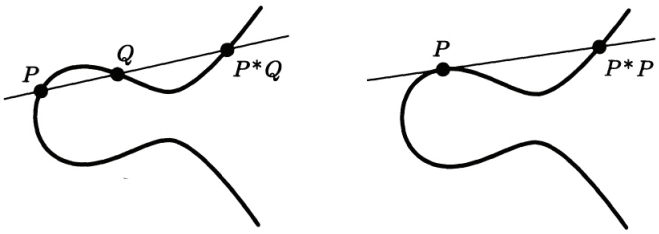

Figura 4: Composição de pontos em uma curva elíptica

Mesmo se só tivermos um ponto P com coordenadas racionais, podemos traçar a reta tangente à cúbica em P. Esta reta tangente intersecta a cúbica duas vezes em P (no sentido de multiplicidade) e, pelo Teorema de Bezout, esta reta intersecta a cúbica em um novo ponto. O mesmo argumento usado anteriormente mostra que este novo ponto de interseção é um ponto com coordenadas racionais. Então, podemos juntar esses novos pontos acima e encontrar mais pontos.

Se temos quaisquer dois pontos com coordenadas racionais em uma cúbica definida sobre os racionais, digamos P e Q, então podemos traçar uma reta que une P a Q, obtendo o terceiro ponto que já denotamos por $P * Q$. Se considerarmos o conjunto de todos os pontos com coordenadas racionais sobre a cúbica, podemos dizer que o conjunto tem uma *lei de composição*. Podemos nos perguntar sobre a estrutura algébrica do conjunto com esta *lei de composição*: por exemplo, constitui um grupo? Todavia, para ser um grupo, precisamos ter um elemento neutro, o que não parece possível com essa definição.

No entanto, podemos definir uma operação de grupo com a seguinte regra:

Consideremos O um ponto com coordenadas racionais fixado na cúbica.

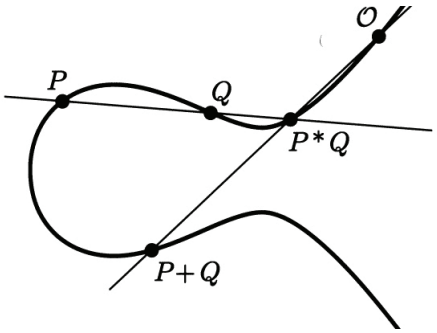

Figura 5: A lei do grupo em um curva elíptica

"Tome a reta que passa por P e Q, sendo $P * Q$ o terceiro ponto de interseção com a cúbica. A reta que passa por O e por $P * Q$ intersecta a cúbica em um novo ponto denotado por $P + Q$. Assim, por definição, $P + Q = O * (P * Q)$".

A operação do grupo é ilustrada na Figura 5, e o fato de que O atua como elemento neutro é ilustrado na figura a seguir.

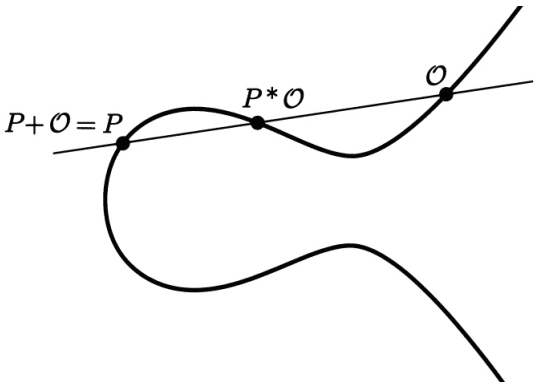

Figura 6: O é o elemento neutro

Teorema 2.8. *Seja C uma curva elíptica sobre um corpo $\mathbb{Q}$ com um ponto $O \in C(\mathbb{Q})$. Então, $C(\mathbb{Q})$ é um grupo abeliano com a operação + definida anteriormente. Em outras palavras, temos:*

1. Comutatividade: $P + Q = Q + P$ para quaisquer dois pontos com coordenadas racionais P e Q;

2. Elemento Neutro: $P + O = O + P$ para qualquer racional P;

3. Inverso: para qualquer ponto com coordenadas racionais P, existe um outro ponto com coordenadas racionais $-P$ tal que $P + (-P) = (-P) + P = O$;

4. Associatividade: $(P + Q) + R = P + (Q + R)$ para quaisquer três pontos com coordenadas racionais P, Q e R.

Temos assim uma estrutura algébrica muito rica, definida geometricamente de maneira intuitiva que nos permite fazer uma introdução à matemática abstrata, em particular ao conceito de estrutura algébrica, no

ensino médio. Nesse nível de ensino não precisamos demonstrar o teorema acima (a demonstração pode ser encontrada em [1] e [9]), mas nas atividades a serem apresentadas exemplificaremos que essas propriedades são satisfeitas.

2.4 Caracterização algébrica dos pontos em uma Curva Elíptica

Para uma curva elíptica na forma (5), uma escolha natural para o ponto O é o ponto $(0:1:0)$ que se encontra no infinito (em relação ao plano afim $z=1$). Podemos, então, afirmar que o conjunto de pontos da curva elíptica $\mathcal{C}$ é o conjunto de pares (x,y) satisfazendo $y^2 = x^3 + ax + b$ juntamente com o ponto no infinito O. A Figura 7 ilustra o processo de adição dos pontos P e Q sobre uma curva elíptica (na Forma Normal de Weierstrass), visto que a reta que passa por um ponto qualquer e o ponto O é uma reta vertical no plano afim, pela proposição 2.4.

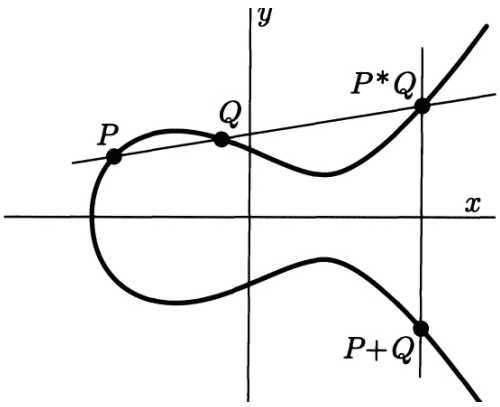

Figura 7: Adicionando pontos em uma curva elíptica

O inverso de Q, que denotaremos de $-Q$, é o ponto Q refletido através do eixo Ox na curva elíptica. Ou seja, se $Q=(x,y)$, teremos $-Q=(x,-y)$.

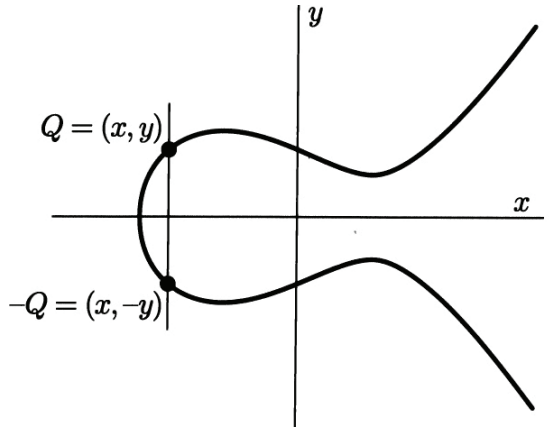

Figura 8: O inverso de um ponto na curva elíptica

Já vimos como calcular $P+Q$ geometricamente. Veremos, em seguida, o processo algébrico para adição de pontos de uma curva elíptica.

Considere os pontos:

$$P_1 = (x_1,y_1), \quad P_2 = (x_2,y_2),$$

$$P_1 * P_2 = (x_3,y_3), \quad P_1 + P_2 = (x_3, -y_3).$$

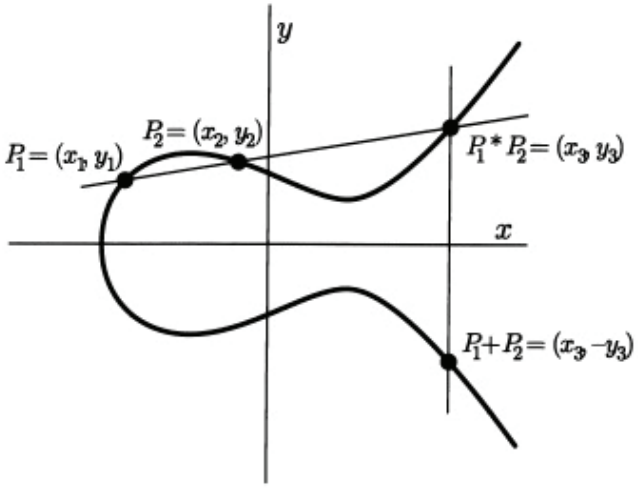

Figura 9: A lei da adição

Assumiremos que (x_1,y_1) e (x_2,y_2) são dados e queremos calcular (x_3,y_3). Primeiro, observemos que a reta que passa por (x_1,y_1) e (x_2,y_2) tem equação

$$y = \lambda x + v, \tag{10}$$

onde $\lambda = \frac{y_2-y_1}{x_2-x_1}$ e $v = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Pelo Teorema de Bezout, a reta não vertical geralmente corta a cúbica nos pontos (x_1,y_1), (x_2,y_2) e (x_3,y_3). Para obtermos este terceiro ponto de interseção, substituiremos (10) na equação (4):

$$y^2 = (\lambda x - v)^2 = x^3 + ax + b$$
$$\lambda^2 x^2 + 2\lambda x v + v^2 = x^3 + ax + b$$
$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + (b - v^2) = 0,$$

que também é uma equação com coeficientes racionais. Como duas de suas raízes são racionais x_1 e x_2, a terceira raíz x_3 será racional pelas relações entre coeficientes e raízes de um polinômio.

$$x^3 - \lambda^2 x^2 + (a - 2\lambda v)x + (b - v^2) =$$
$$x^3 + (-x_1 - x_2 - x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1x_2x_3.$$

Igualando os coeficientes do termo x^2 em ambos os lados, temos:

$$-\lambda^2 = -x_1 - x_2 - x_3.$$

Ou seja,

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{e} \quad y_3 = \lambda x_3 + v.$$

Portanto, estas são as fórmulas para calcular a soma $P_1 + P_2 = (x_3, -y_3)$.

Observação 2.9. Precisamos ficar atentos para o fato de que, quando adicionamos pontos pertencentes a uma curva elíptica, deve-se proceder de forma diferente da usual para adicionar vetores no $\mathbb{R}^2$. Esse é um fato muito interessante para o ensino médio, uma vez que não se costuma trabalhar neste nível com operações não usuais.

As fórmulas anteriores envolvem o ângulo de inclinação da reta que passa pelos dois pontos da cúbica (λ). E se os pontos coincidirem? Ou seja, supondo que $P_0 = (x_0,y_0)$, como encontrar $P_0 + P_0$? Para isso, precisamos encontrar a reta tangente à curva que passa por P_0. Como $x_1 = x_2$ e $y_1 = y_2$, não podemos usar a mesma fórmula para (λ). Porém, considerando a equação da curva elíptica dada por $y^2 = f(x)$ e usando a diferenciação, temos que:

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}.$$

Vale ressaltar que podemos ter uma fórmula explícita para $2P$ em termos das coordenadas de $P = (x,y)$. Para isso, devemos substituir $\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$ nas fórmulas apresentadas anteriormente:

$$x_3 = \lambda^2 - x_1 - x_2.$$

Como estamos considerando o caso de os pontos coincidirem, então $x_1 = x_2$ e $y_1 = y_2$. Portanto, podemos escrever:

$$x_3 = \lambda^2 - x_1 - x_1 = x_3 = \lambda^2 - 2x.$$

Substituindo o valor de λ,

$$x_3 = \left(\frac{f'(x)}{2y}\right)^2 - 2x.$$

$$x_3 = \left(\frac{(3x^2 + a)^2}{4y^2}\right) - 2x.$$

$$x_3 = \frac{9x^4 + 6x^2a + a^2}{4x^3 + 4ax + 4b} - 2x.$$

$$x_3 = \frac{x^4 - 2ax^2 - 8bx + a^2}{4x^3 + 4ax + 4b}.$$

Esta fórmula que é utilizada para calcular a coordenada x de $2P$ é também chamada de *fórmula de duplicação do ponto*. Para a coordenada y, temos:

$$y_3 = \frac{f'(x)}{2y}x_3 + v.$$

Mais detalhes, *cf.* [1], [2] e [9].

Um outro conceito interessante, vindo da teoria de grupos, que enuciaremos abaixo e o utilizaremos na atividades seguintes é o de ordem de ponto.

Definição 2.10. A ordem n de um ponto P em uma curva elíptica é o menor inteiro positivo tal que $nP = O$, sendo que tal n não precisa necessariamente existir.

A seguir, apresentaremos atividades com aplicações de Curvas Elípticas nas quais exploraremos os conceitos e propriedades discutidos nas seções anteriores, buscando uma linguagem mais direcionada ao Ensino Médio.

3 Atividades

As Curvas Elípticas são curvas planas cujas equações são polinômios com duas variáveis de grau 3 que possuem uma estrutura algébrica muito rica: seus pontos, juntamente com a operação binária, formam um grupo abeliano. Todavia, no nível básico não precisamos definir o que é um grupo, podemos apenas falar das propriedades que são satisfeitas para esse conjunto de pontos de forma que os alunos percebam que curvas elípticas têm uma estrutura bastante interessante. Podemos explorar também a operação, que é definida de maneira geométrica, usando retas tangentes, secantes e suas interseções com a curva. As fórmulas para calcular a soma de dois pontos pertecentes a uma curva elíptica que foram obtidas na seção 2.4 podem ser aplicadas no Ensino Médio, uma vez que os pré-requisitos para dedução destas também se encontram no Ensino Médio.

3.1 Atividade I

Para esta atividade, seguiremos as abordagens feitas por [1] e [5]. É uma atividade interessante para ser aplicada no Ensino Médio, uma vez que podemos explorar algumas propriedades das Curvas Elípticas em um exemplo prático. O professor do Ensino Médio pode usar esta atividade com alunos que tenham estudado Geometria Plana, Analítica e polinômios e, assim, poderia explorar os conceitos de: grau de um polinômio, raízes do polinômio, números que são quadrados perfeitos, reta secante, interseção entre curvas, simetria , dentre outros que veremos com a resolução.

Uma certa quantidade de balas de canhão pode ser agrupada de maneira que forme uma pirâmide cuja base seja um

quadrado. Por exemplo, pode-se ter uma bola no primeiro nível (topo), quatro no segundo nivel, nove no terceiro e assim por diante. Uma questão que pode ser lenvantada é: será posssível desmanchar esta pirâmide e reagrupar estas bolas de maneira que formem um quadrado? Caso a pirâmide tenha quatro níveis, ter-se-á $1+4+9+16=30$. Logo, com esta quantidade de bolas, não é possível formar um quadrado, pois 30 não é um quadrado perfeito. Da mesma forma, se tivéssemos cinco níveis: $1+4+9+16+25=55$. Teríamos, assim, que 55 também não é um quadrado perfeito. Seguindo esse raciocínio, temos que:

$$1^2+2^2+3^2+\ldots+x^2=\frac{x(x+1)(2x+1)}{6}. \qquad (11)$$

Como desejamos que a quantidade total de bolas forme um quadrado, precisamos encontrar y inteiro tal que:

$$y^2=\frac{x(x+1)(2x+1)}{6}. \qquad (12)$$

A equação (12) representa o que chamamos de uma *curva elíptica*. Sua solução pode ser obtida através do método diofantino, que consiste em encontrar as novas soluções a partir de soluções já conhecidas. Nesse caso, identificam-se duas soluções que correspondem aos casos triviais: Para $x=0$, temos $y=0$ e, assim, (0,0) (uma pirâmide sem nenhuma bola) e (1,1) (uma pirâmide composta por somente uma bola). Com esses dois pontos, podemos encontrar a equação da reta definida por esses pontos, que é: $y=x$. Estudaremos agora a interseção entre essa reta e a curva que pode ser obtida substituindo $y=x$ na equação $y^2=\frac{x(x+1(2x+1)}{6}$, obtendo-se:

$$x^2=\frac{x(x+1(2x+1)}{6},$$

cujo desenvolvimento resulta na igualdade

$$x^3-\frac{3}{2}x^2+\frac{1}{2}x=0. \qquad (13)$$

A equação (13) é um polinômio de terceiro grau. Logo, é possivel expressá-la sob a forma fatorada $(x-a)(x-b)(x-c)$, desde que as raízes a, b e c sejam conhecidas. O desenvolvimento da forma fatorada mostra que

$$(x-a)(x-b)(x-c)= x^3-(a+b+c)x^2+(ab+ac+bc)x-abc,$$

indicando que quando o coeficiente de x^3 é 1 (conforme acontece na equação (13)), o valor de $-(a+b+c)$, ou seja, o simétrico da soma das raízes do polinômio, corresponde ao valor do coeficiente de x^2. Aplicando essa propriedade ao caso em estudo, tem-se:

$$0+1+x=\frac{3}{2}\Longrightarrow x=\frac{1}{2}.$$

Substituindo $x=\frac{1}{2}$ na equação (12) , temos $y=\pm\frac{1}{2}$. Como os valores encontrados não correspondem a números inteiros, não podemos considerá-los soluções válidas para o problema. No entanto, como $(\frac{1}{2},-\frac{1}{2})$ também é um ponto da curva, pois esta curva é simétrica em relação ao eixo Ox, para verificar essa simetria, basta tomar um ponto da forma $(x,-y)$ e observar que ele também pertence à curva de equação (12). Podemos repetir o processo usando agora os pontos $(\frac{1}{2},-\frac{1}{2})$ e (1,1), desta vez, encontra-se $x=24$ e $y=70$, o que representa:

$$1^2+2^2+3^2+4^2+5^2+\ldots+24^2=70^2,$$

encontrando assim uma solução para o problema. O traço da curva foi construído no Geogebra.

Visualizemos o traço:

$$y^2=\frac{x(x+1)(2x+1)}{6}.$$

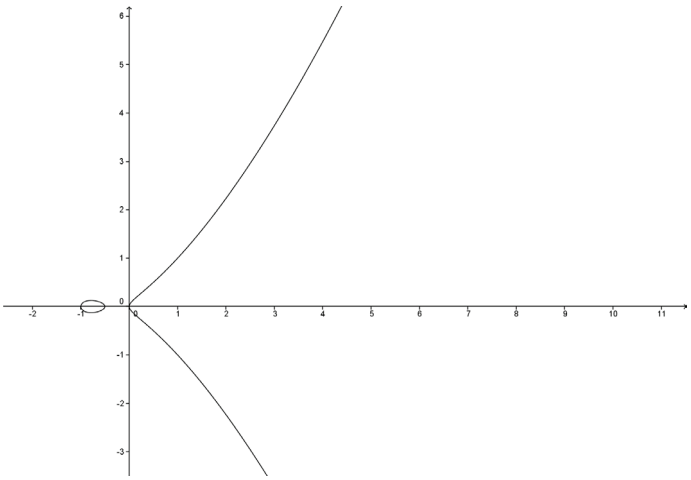

Figura 10: Traço da Curva Elíptica

3.2 Atividade II

Esta atividade será interessante aplicar no Ensino Médio porque escolhemos uma curva elíptica e faremos um estudo bem detalhado de sua equação, pontos pertecentes a ela, operações com seus pontos e ainda visualizar no traço da curva a operação de grupo da curva. Vale destacar que esta atividade seria uma excelente introdução à ideia de estrutura algébrica, mostrando outras operações que os alunos não conhecem, entre elementos pouco usuais. Além disso, essa atividade pode ser desenvolvida com mais detalhes no Ensino Superior ou em turmas avançadas, pois os recursos do Cálculo, tais como Limite e Derivadas são importantes para o cálculo da adição de pontos coincidentes. Não faremos neste

artigo a adição de pontos coincidentes, mas, caso o leitor queira consultar, em [1] há mais detalhes aprofundados desta atividade. Considere a curva

$$y^2 = x^3 - 36x, \tag{14}$$

uma curva algébrica plana de grau 3 chamada de *cúbica*, em especial *elíptica*, pois atende à forma da equação (3).

Sejam $P = (-3,9)$ e $Q = (-2,8)$ pontos pertencentes a esta cúbica. Vamos deteminar $P + Q$. Como a curva (14) está na forma (5), podemos aplicar as fórmulas:

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda x_3 + v.$$

Onde λ é o coeficiente angular da reta deteminada pelos pontos P e Q. Portanto, $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-9}{-2+3} = -1$

$v = y_1 - \lambda x_1 = 9 + 1 \cdot (-3) = 6$.

Assim, temos:

$$x_3 = (-1)^2 + 3 + 2 = 6.$$

$$y_3 = -1 \cdot 6 + 6 = 0.$$

Temos $P + Q = -(P * Q) = (x_3, -y_3)$, o que implica $P + Q = (6,0)$. Poderíamos ainda calcular $P + (-Q)$, uma vez que $(-Q)$ é o oposto de Q.

Portanto, encontramos $P + Q$ algebricamente através das fórmulas apresentadas. O professor poderia ainda fazer uma atividade paralela, mostrando aos alunos como encontrar esses pontos geometricamente e comparar com os resultados algébricos da maneira indicada a seguir: Utilizando o Geogebra, inicialmente construimos o traço da curva:

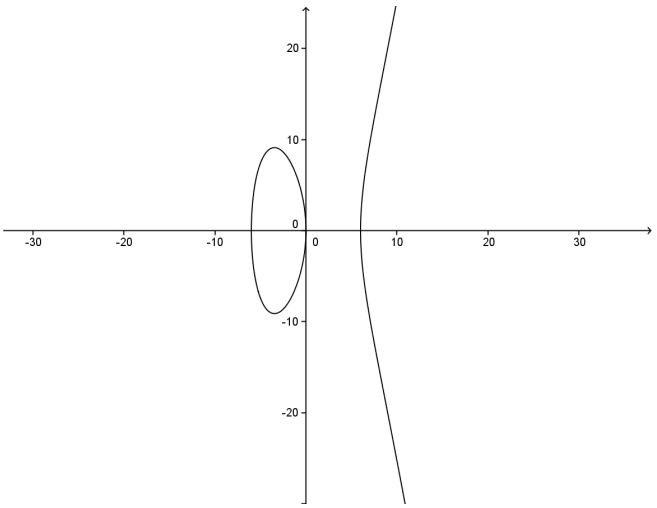

Figura 11: Traço da curva

Representando os pontos $(-3,9)$ e $(-2,8)$ e traçando uma reta definida por esses pontos, temos:

A reta intersecta a curva no ponto $P * Q = (6,0)$. Utilizando o Geogebra, é simples encontrar esta opção

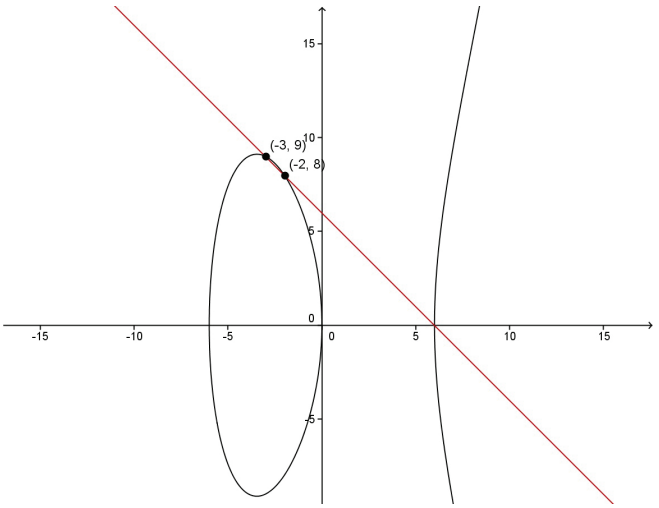

Figura 12: Representação dos pontos

de interseção entre reta e curva. Agora, traçamos uma reta vertical passando pelo ponto $P * Q$ e esta só encontra a curva em $(6,0)$, que é exatamente $P + Q$, confirmando o que já sabiámos por definição, que

$$P + Q = O * P * Q = -P * Q.$$

Vejamos o traço a seguir com os pontos P, Q, $P * Q$, $P + Q$ e as retas:

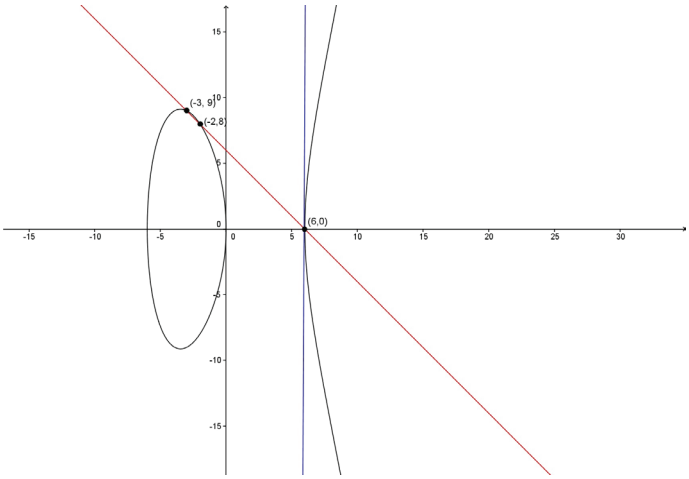

Figura 13: Soma de pontos

Agora, utilizaremos o processo aplicado no *exemplo prático* da Atividade I que consiste em encontrar novas soluções a partir de soluções já conhecidas. Neste caso, temos as soluções $(-3,9)$ e $(-2,8)$. Como a reta que contém esses pontos é definida por $y = -x + 6$, precisamos encontrar a interseção entre a reta e a curva $y^2 = x^3 - 36x$. Substituindo $y = -x + 6$ na equação (14), temos:

$$(-x + 6)^2 = x^3 - 36x.$$

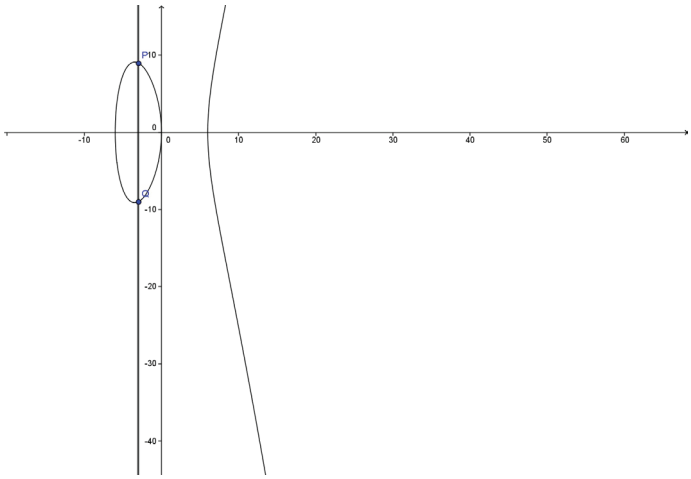

Figura 14: Traço da curva $y^2 = x^3 - 36x$

$$36 - 12x + x^2 = x^3 - 36x.$$
$$-x^3 + x^2 + 24x + 36 = 0.$$
$$x^3 - x^2 - 24x - 36 = 0. \quad (15)$$

Como a equação (15) é um polinômio de terceiro grau, é possível expressá-lo na forma fatorada $(x-a)(x-b)(x-c)$, desde que as raízes a, b e c sejam conhecidas. De forma análoga ao exemplo prático, temos:

$$-(a+b+c) = -1.$$
$$a+b+c = 1.$$
$$-3-2+x = 1.$$
$$x = 6.$$

Substituindo na equação da reta o valor de $x = 6$, temos que $y = -6+6 = 0$ ou ainda $y^2 = 6^3 - 36 \cdot 6 = 216 - 216 = 0$. Assim, encontramos uma nova solução a partir de duas soluções dadas, a solução $(6,0)$, que também pertence à curva elíptica

$$y^2 = x^3 - 36x.$$

Ainda em relação a esta curva elíptica, sabemos que é simétrica em relação ao eixo Ox, pois, dado um ponto (x,y), o ponto $(x,-y)$ também pertence à curva. Temos, assim, que os pontos $P = (-3,9)$ e $-P = (-3,-9)$ pertencem à curva.

Calculemos $P + (-P)$. Se utizarmos a fórmula para λ, teremos: $\lambda = \frac{-9-9}{-3+3} = \frac{-18}{0}$. Logo, não podemos aplicar esta fórmula pois gera uma indeterminação. A reta determinada pelos pontos $(-3,9)$ e $(-3,-9)$ é uma reta vertical, $x = -3$.

Façamos agora uma análise geométrica. Visualizemos os pontos $(-3,9)$ e $(-3,-9)$ no traço da curva: $y^2 = x^3 - 36x$ (Fig. 14) e a reta determinada por esses pontos.

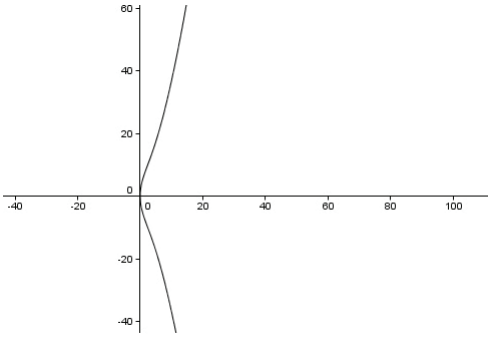

Figura 15: Traço da curva $y^2 = x^3 + 36x$

Pelo traço da curva, a reta intersecta a curva em dois pontos, mas pelo Teorema de Bezout sabemos que a reta intersecta a curva em três pontos, ou melhor, este terceiro ponto está no infinito. Como foi visto na Proposição 2.4, a reta vertical sempre passa pelo ponto no infinito, justificando, assim, que $P + (-P) = O$. Podemos, ainda, verificar que, se somarmos $Q + P$, encontraremos o mesmo resultado de $P + Q$ e, chamando a soma de $P + Q$ de R, temos que $(P + Q) + R = P + (Q + R)$.

Ainda nesta atividade, poderíamos analisar a curva elíptica com sinal trocado para o coeficiente a(considerando a forma Normal), uma vez que o coeficiente b é nulo. Assim, teríamos a curva (Fig. 15):

$$y^2 = x^3 + 36x$$

Podemos escolher pontos pertencentes a esta curva elíptica (Fig. 15), por exemplo, $P = \left(\frac{2523}{100}, \frac{1303}{10}\right)$ e $Q = \left(\frac{44}{50}, \frac{-1579}{50}\right)$ e fazer o processo análogo ao feito com a curva $y^2 = x^3 - 36x$.

De fato, foi possível constatar que as curvas elípticas constituem um tema muito interessante para as investigações futuras e podemos considerá-las como uma fonte muito rica em informações que faz conexões com ou maioria, senão todas as áreas da Matemática.

Aplicar curvas elípticas ao Ensino Médio é bastante interessante pois além de explorarmos conteúdos trabalhados neste nível de ensino podemos incentivar os alunos a uma matemática abstrata(operações não usuais) e mostrar a rica estrutura algébrica dos pontos pertencentes às curvas elípticas com a visualização dos traços destas curvas utilizando o Geogebra.

4 Referências

Referências

[1] CARNEIRO, Joilma Silva. *Uma introdução às curvas elípticas com aplicações para o ensino médio*. 2014. 95 p.

Dissertação - Mestrado Profissional em Matemática. Universidade Estadual de Feira de Santana, Feira de Santana, 2014.

[2] FLOSE, Vânia B. S. *Criptografia e Curvas Elípticas*. 2011. 55 p. Dissertação (Mestrado Profissional em Matemática). Instituto de Geociências e Ciências Exatas, Universidade estadual Paulista Júlio de Mesquita Filho, Rio Claro, 2011.

[3] GOUVÊA, Fernando Q. *Uma Demonstração Maravilhosa*. Matemática Universitária. n. 19, p. 16-43, dez, 1995.

[4] Instituto Geogebra no Rio de Janeiro. Disponível em: `http://www.geogebra.im-uff.mat.br` . Acesso em: 01 fev.2014.

[5] MARQUES, Leonardo G. *Curvas Elípticas: Aplicações Criptográficas*. 2007. 94 p. Monografia. Universidade Federal de Góias, Campus Catalão. 2007.

[6] MARTINEZ, Fábio Brochero *et al. Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 3. ed. Rio de Janeiro: Impa, 2013 (Projeto Euclides).

[7] MIRANDA, Luís Adriano Borges. *Introdução ao Estudo de Curvas Elípticas*. 2006. 46 p. TCC. ISE, 2006.

[8] PLACIDO, Andrade e Abdêgano Barros. *Introdução à Geometria Projetiva*. Rio de Janeiro: SBM, 2010 (Coleção Textos Universitários).

[9] SILVERMAN, J.H; TATE, J. *Rational Points on Elliptic Curvas*. Springer-Verdag, 1994.

[10] SOUZA, Aldenice O. *Pontos Racionais em Curvas Elípticas*. 2012. 62 p. Dissertação (Mestrado em Matemática). Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, 2012.

[11] VAINSENCHER, Israel. *Introdução às Curvas Algébricas Planas*. Rio de Janeiro: Impa, 2005 (Coleção Matemática Universitária).