Universidade Federal de Goiás
Regional de Jataí
Unidade Acadêmica Especial de Ciências
Exatas e Tecnologia
Programa de Mestrado Profissional em
Matemática em Rede Nacional

Curvas Elípticas

Lucas Silva de Oliveira

Jataí

2017

sistema de bibliotecas ufg

UFG

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÃO ELETRONICA DE TESES E DISSERTAÇÕES NA BIBLIOTECA DIGITAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio da Biblioteca Digital de Teses e Dissertações (BDTD/UFG), regulamentada pela Resolução CEPEC nº 832/2007, sem ressarcimento dos direitos autorais, de acordo com a Lei nº 9610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou *download*, a título de divulgação da produção científica brasileira, a partir desta data.

1. Identificação do material bibliográfico: [X] Dissertação [ ]Tese

2. Identificação do Trabalho:

Nome completo do Autor: **Lucas Silva de Oliveira**

Titulo do trabalho: **Curvas Elípticas**

3. Informações de acesso ao documento:

Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

Havendo concordância com a disponibilização eletrônica, torna-se imprescindível o envio do(s) arquivo(s) em formato digital PDF oda tese ou dissertação.

Lucas Silva de Oliveira
Assinatura do(a) autor(a)

Ciente e de acordo:

Adriana Araujo Cintra
Assinatura do(a) orientador(a)

Data: 06 / 12 / 2017

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. A extensão deste prazo suscita justificativa junto à coordenação do curso. Os dados do documento não serão disponibilizados durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;
- Submissão de artigo em revista científica;
- Publicação como capítulo de livro;
- Publicação da dissertação/tese em livro.

[2] A assinatura deve ser escaneada

Lucas Silva de Oliveira

Curvas Elípticas

Trabalho de Conclusão de Curso apresentado aUnidade Acadêmica Especial de Ciências Exatas e Tecnologia da Universidade Federal de Goiás - Regional de Jataí, como parte dos requisitos para obtenção do grau de Mestre Profissional em Matemática.
Área de Concentração: Mestrado Profissional em Matemática
Orientador: Prof. Dra. Adriana de Araujo Cintra

Jataí

2017

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Oliveira, Lucas Silva de
Curvas Elípticas [manuscrito] / Lucas Silva de Oliveira. - 2017.
65 f.: il.

Orientador: Profa. Dra. Dra Adriana Araújo Cintra.
Dissertação (Mestrado) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Exatas e Tecnológicas, Jataí, PROFMAT- Programa de Pós-graduação em Matemática em Rede Nacional - Sociedade Brasileira de Matemática (RJ), Jataí, 2017.
Bibliografia.
Inclui lista de figuras.

1. Curvas Elípticas. 2. Álgebra. 3. Geometria. I. Cintra, Dra Adriana Araújo, orient. II. Título.

CDU 51

Universidade Federal de Goiás-UFG REGIONAL JATAÍ
Mestrado profissional em Matemática em Rede Nacional - PROFMAT/UFG
Regional Jataí – Caixa Postal 03 – CEP: 75,804-020 – Jataí-GO.
Fones: (64) 3606-8213 **www.jatai.ufg.br/matematica**

Ata da reunião da Banca Examinadora da Defesa de Trabalho de Conclusão de Curso do aluno Lucas Silva de Oliveira – Aos seis dias do mês de dezembro do ano de dois mil e dezessete (06/12/2017), às 14:00 horas, reuniram-se os componentes da Banca Examinadora, Profa. Dra. Adriana Araújo Cintra - Orientadora, Prof. Dr. Benedito Leandro Neto e Prof. Dr. Tharsis Souza Silva, sob a presidência da primeira, e em sessão pública realizada no Auditório da Pós Graduação da Universidade Federal de Goiás - Regional Jataí, procederem a avaliação da defesa intitulada: **"Curvas Eliptícas",** em nível de Mestrado, área de concentração Matemática do Ensino Básico, do Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Federal de Goiás, polo Jataí. A sessão foi aberta pelo Presidente da Banca, Profa. Dra. Adriana Araújo Cintra, que fez a apresentação formal dos membros da banca. A seguir, a palavra foi concedida ao autor da Dissertação que, em 40 minutos, procedeu a apresentação de seu trabalho. Terminada a apresentação, cada membro da banca arguiu o examinando, tendo-se adotado o sistema de diálogo sequencial. Terminada a fase de arguição, procedeu-se a avaliação da defesa. Tendo em vista o que consta na Resolução nº. 1403/2016 do Conselho de Ensino, Pesquisa, Extensão e Cultura (CEPEC), que regulamenta os Programas de Pós-Graduação da UFG e procedidas as correções recomendadas, o trabalho de conclusão foi **APROVADO** por unanimidade, considerando-se integralmente cumprido este requisito para fins de obtenção do título de **MESTRE EM MATEMÁTICA**, na área de concentração Matemática do Ensino Básico pela Universidade Federal de Goiás. A conclusão do curso dar-se-á quando da entrega na Secretaria da Coordenação de Matemática da Regional Jataí da versão definitiva do trabalho, com as devidas correções supervisionadas e aprovadas pelo orientador. Cumpridas as formalidades de pauta, às 16:00 horas a presidência da mesa encerrou a sessão e para constar, eu, José Alfredo Cespi de Oliveira, Secretário da Coordenação Geral de Pós-Graduação da Regional Jataí - UFG, lavrei a presente ata que, depois de lida e aprovada, é assinada pelos membros da Banca Examinadora em quatro vias de igual teor.

Adriana Araújo Cintra

Profa. Dra. Adriana Araújo Cintra - CPF 705.549.431-15
Profmat (Pólo Jataí)-UFG
Presidente da Banca

Benedito Leandro Neto

Prof. Dr. Benedito Leandro Neto – CPF 734.276.081-15
Profmat (Pólo Jataí)-UFG
Membro interno

Tharsis Souza Silva

Prof. Dr. Tharsis Souza Silva – CPF 016.547.161-11
IFG- Campus Anápolis
Membro externo

Lucas Silva de Oliveira graduou-se em Matemática pela Universidade Estadual de Goiás no ano de 2008. Mestrando em Matemática pela Universidade Federal de Goiás - Regional de Jataí no ano de 2017.

Dedicar esse trabalho a algumas poucas pessoas seria injusto devido a quantidade de pessoas envolvidas no mesmo mas tenho que citar primeiramente a Deus que tem guiado a minha mão desde o primeiro dia nesse mestrado desde o dia da minha aprovação no Exame de admissão, passando por cada prova e no Exame de qualificação, a Prof Adriana de Araujo Cintra, que aceitou de prontidão encarrar essa ultima e árdua empreitada desse trabalho.

Agradecimentos

Agradecimentos especiais são direcionados ao IMPA, a Universidade Federal de Goiás e ao corpo docente da núcleo de Mestrado Profissional em Matemática (ProfMat) da Jataí que contribuíram e que ainda contribuirão para a evolução do Matemática em todos os níveis.

"Peçam, e lhes será dado; busquem, e encontrarão; batam, e a porta lhes será aberta. Pois todo o que pede, recebe; o que busca, encontra; e àquele que bate, a porta será aberta."

(Bíblia Sagrada, Mateus 7: 7,8)

Resumo

Este trabalho se faz através de uma breve explanação a respeito de curvas elípticas trazendo conceitos simples sobre sua álgebra e geometria.

Na parte geométrica, caracterizamos uma curva elíptica com enfoque em um tipo especifico: as que estão na forma de Weierstrass. Trazemos também o Teorema de Bézout, que nos mostra não só quantos pontos em comum duas curvas elípticas podem ter, mas quaisquer classe de equivalência de polinômios, podendo ser interação entre retas, cônicas, cubicas...

Na parte algébrica, voltada a demonstrar como os pontos se relacionam entre si e algumas formas de operações que podemos fazer com eles. Trazendo a demonstração de que o conjunto de pontos racionais de uma curva elíptica C formam um grupo abeliano. E ainda formas de se encontrar outros pontos dentro das curvas elípticas a partir de um ou dois pontos a ela pertencentes.

Palavras-chave: Curvas Elípticas. Geometria. Álgebra.

Abstract

This work is done through a brief explanation about elliptic curves bringing simple concepts about their algebra and geometry.

In the geometric part,we characterize an elliptical curve with focus on a specific type: that are in the form of Weierstrass. We also draw the Bezout Theorem, which shows us not only how many points in common two elliptic curves can have, but any class of equivalence of polynomials, which can be interaction with straight lines, conic, cubic ...

In the algebraic part, we demonstrate with the points are related to each other and some forms operations we can do with them. Bringing the proof that the set of rational points of an elliptic curve C form an abelian group. And still ways to find other points within the elliptical curves from one or two points to it.

Keywords: Elliptic Curves. Geometry. Algebra.

Lista de Figuras

Sumário

Capítulo 1

Introdução

A matemática se faz bela pelo poder de inter-relação que suas áreas conseguem ter. Podendo se relacionar, por exemplo, a Álgebra com a Aritmética ou a Geometria com Álgebra. Esse trabalho é uma prova disso, um trabalho que pelo nome deveria se encaixar dentro da Geometria mas que se entrelaça também dentro da Álgebra.

Este trabalho sobre curvas algébricas trás de inicio uma breve explanação sobre os conceitos básicos necessários de Álgebra e Geometria antes de nos deleitarmos com o conceito de curvas elípticas. Na seção de álgebra, trazemos o conceito de corpo e algumas de suas propriedades, apresentados por (HEFEZ, 2013) e (LIMA, 2012), além dos conceitos de matrizes e determinantes esplanadas por (BOLDRINI et al., 1980). Na seção de Geometria, usamos as definições de curvas algébricas e plano projetivo introduzidos por (VAINSENCHER, 1979) .

No segundo capítulo, definimos o que é uma curva elíptica, abordando uma de suas formas mais interessante; a forma de Weierstrass. Mostramos algumas de suas propriedades dentro de sua geometria e álgebra abordados por (CASTILLO, 2016) e (VAINSENCHER, 1979). Apresentamos também o Teorema de Bezout (NIVEN; ZUCKERMAN; MONTGOMERY, 2008), além do Teorema de Poincaré (SALEHYAN, 2015), que nos diz como os pontos de uma curva elíptica pode formar um grupo abeliano (SOUZA, 2012) e as implicações disso. Além de demonstrar como podemos determinar pontos dentro dessas curvas elípticas usando um ou dois pontos já conhecidos.

No último capítulo, vimos algumas aplicações de (CARNEIRO, 2014) voltadas para os alunos do ensino médio; o que parece ser um exagero tendo em vista que alguns conceitos exigem um grau de conhecimento mais elevado, mas que também não impede

de ser abordado nesta fase do estudo; dando exemplo pratico que pode ser usado no dia a dia e mostrando exemplos mais voltados apenas para cálculos, mas que integram com conhecimentos do cotidiano dos alunos.

O material do nosso estudo se torna ainda mais interessante devido a esse motivo que ao mesmo tempo que tem conceitos que podem facilmente ser abordados por alunos que tenham um conceito básico sobre plotagem de gráficos até conhecimento mais aprofundados de geometria projetiva e aritmética.

Vale ressaltar que todos gráficos contidos nesse trabalho foram gerados utilizando o programa GeoGebra, ferramenta bastante interessante no ensino da matemática em todos os níveis.

Capítulo 2

Fundamentos de Matemática

O estudo das curvas elípticas é uma área da Geometria Algébrica com aplicações em Teoria dos Números, ela auxiliou na resolução de um dos grandes problemas da Matemática, o Último Teorema de Fermat. Fermat ficou muito conhecido por fazer pequenas anotações as margens do livro de Diofanto. O Último Teorema de Fermat diz que seria impossível encontrar inteiros positivos x, y e z tais que $x^n + y^n = z^n$ para todo $n > 2$.

Antes de darmos inicio a estudo das curvas elípticas, e entender porque ela auxiliou a explicar o Último Teorema de Fermat, precisamos ressaltar alguns tópicos que tem grande relevância não só para a compreensão das curvas elípticas. Daremos enfoque aqui em alguns breves tópicos que se mostram de conhecimento geral das classes iniciais de um curso de matemática e que fundamentam bem todo o estudo da matemática.

2.1 Álgebra

Definição 2.1. *Em um conjunto não vazio A se pudermos definir duas operações denotadas por $+$ (adição) e $\cdot$ (multiplicação) satisfazendo as seguintes propriedades para quaisquer a, b, $c \in A$*

- ***Associatividade na adição:*** $a + (b + c) = (a + b) + c$;
- ***Comutatividade:*** $a + b = b + a$;

- *Existe uma elemento em A, denotado por 0, que é denominado de elemento neutro da adição, que satisfaz a relação $a + 0 = 0 + a = a$, $\forall a \in A$;*
- *Existe uma elemento em A, denotado por $(-a)$, que é denominado de elemento oposto da adição, que satisfaz a relação $a + (-a) = (-a) + a = 0$, $\forall a \in A$;*
- ***Distributividade:*** $(a + b) \cdot c = a \cdot c + b \cdot c$;
- ***Associatividade na multiplicação:*** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Se o conjunto A apresenta todas as propriedades para uma única operação, ou adição ou multiplicação, dizemos que o conjunto A é um grupo.

Se conjunto A apresenta essas propriedades dizemos que o conjunto A é um anel.

Se o conjunto A, além dessas propriedades, também apresentar um elemento em A, denotado por 1, que é denominado de elemento neutro da multiplicação, tal que $a \cdot 1 = 1 \cdot a = a$, dizemos que A é um anel com unidade.

Se o conjunto A cumprir a propriedade $a \cdot b = b \cdot a$, dizemos que o conjunto A é um anel comutativo com unidade.

E ainda, se existe em A um elemento, denotado por a^{-1}, para qualquer $a \neq 0$, é chamado de elemento oposto da multiplicação, tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1$, dizemos que A é um corpo.

2.1.1 Polinômios

Definição 2.2. *Sejam K um corpo, $\{a_0, a_1, a_2, \cdots, a_n\} \in K$ e $n \in \mathbb{N}$. Dizemos que $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x^1 + a_0 x^0$ é um polinômio.*

Determinamos o grau de um polinômio pelo termo que apresenta maior índice cujo coeficiente seja diferente de 0 (zero) e descrevemos $\deg p = n$ para $a_n \neq 0$ ou $\delta(p) = n$.

Podemos dar nomes específicos para os polinômios de acordo com a quantidade de termos que eles apresentam. Para polinômios com apenas um termo damos o nome de monômios, um exemplo clássico seria x, ou y, ou z^n entre outros. Para polinômios com dois termos podemos definir como binômios, com três termos trinômios.

Dados dois polinômios $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x^1 + a_0 x^0$ e $q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_2 x^2 + b_1 x^1 + b_0 x^0$, eles são ditos iguais se $n = m$ e $a_i = b_i$ para todo $i \in \{0, 1, \cdots, n\}$.

Agora que já vimos algumas definições básicas de polinômios, veremos como podemos realizar algumas operações entre eles.

Operações com Polinômios

Dados dois polinômios $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0$ e $q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x^1 + b_0x^0$, com $p(x)$ e $q(x) \neq 0$ e $n \geq m$ definimos:

Adição $p(x)+q(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x^1 + a_0x^0 + b_m x^m + b_{m-1}x^{m-1} + \cdots + b_2x^2 + b_1x^1 + b_0x^0 = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + a_1x^1 + c_0x^0$, onde $c_i = a_i + b_i$ e $0 \leq i \leq n$.

Exemplo 1. $(ax^3 + bx + c) + (dx^2 + ex + f) = ax^3 + dx^2 + (b + e)x + (c + f)$.

Exemplo 2. $(x^3 + 2x^2 + 3) + (3x^2 + 4x - 1) = x^3 + 5x^2 + 4x + 2$.

Multiplicação $p(x).q(x) = (a_n x^n + \cdots + a_1x^1 + a_0x^0) \,.\, (b_m x^m + \cdots + b_1x^1 + b_0x^0) =$

$a_0b_0x^0 + (a_1b_0 + a_0b_1)x^1 + (a_2b_0 + a_1b_1 + a_0b_2)x_2 + \cdots + a_nb_mx^{n+m} = c_nx^n + c_{n-1}x^{n-1} + \cdots + c_2x^2 + a_1x^1 + c_0x^0$, onde $c_k = \sum a_ib_j$ com $0 \leq k \leq (m + n)$ e $i + j = k$.

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

Exemplo 4. $(x^3 + 2x^2 + 3).(3x^2 + 4x - 1) = 3x^5 + 10.x^4 + 7x^3 + 7x^2 + 12x - 3$.

A relação entre os graus do polinômios $p(x)$ e $q(x)$ e suas soma e produto são dadas por $\deg(p + q) \leq \max\{\deg p, \deg q\}$ e $\deg\{p.q\} = \deg p + \deg q$ respectivamente.

É fácil verificar que $K[x]$, corpo K ao qual o elemento x pertence, munido dessas operações forma um anel, cujos zero e unidade são 0 e 1. Além disso $\{a.x^0 | a \in K\}$ forma um corpo isomorfo a K, então podemos considerar $K \subset K[x]$.

Até nesse momento só foram apresentados polinômios com uma única variável, apesar de que, eles se mostrem em graus diferentes mais ainda sim uma única variável. Vale ressaltar que existem polinômios com um, duas ou mais variáveis.

Para polinômios com duas ou mais variáveis vale a seguinte definição:

Definição 2.3. *Um polinômio é dito homogêneo se todos os seus monômios com coeficientes não-nulos tem o mesmo grau total, ou seja, a soma do grau de suas variáveis é o mesmo.*

Exemplo 5. *Dado o polinômio* $y^2.z = a.x^3 + b.x.z^2 + c.z^3$ *podemos verificar que ele é homogêneo uma vez que se dividirmos este polinômios em monômios temos* $y^2.z$, $a.x^3$, $b.x.z^2$ *e* $c.z^3$. *Assim desprezando os coeficientes temos:*

- $y^2.z$, *o graus de* y *e* z *são respectivamente* 2 *e* 1, *logo somando os dois temos* 3.
- x^3, *o grau de* x *é* 3.
- $x.z^2$, *o graus de* x *e* z *são respectivamente* 1 *e* 2, *logo somando os dois temos* 3.
- z^3, *o grau de* z *é* 3.

ou seja, todos tem graus iguais a 3

Para maiores informação sobre alguns conceitos mais abrangente de álgebra recomenda-se a leitura dos livros (LIMA, 2012) e (HEFEZ, 2013).

2.2 Álgebra Linear

Sejam K um corpo, o conjunto

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = y_1, \\ \vdots + \vdots + \cdots + \vdots = \vdots, \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = y_m \end{cases}$$

de equações lineares de coeficientes $a_{ij} \in K$, com $i = \{1, 2, \cdots, m\}$ e $j = \{1, 2, \cdots, n\}$, com $y_1, y_2, \cdots, y_m \in K$ e $x_1, x_2, \cdots, x_n$ são incógnitas. Partindo dessa informação desejamos resolver este sistema de equações lineares.

No caso em que $y_1 = y_2 = \cdots = y_m = 0$ dizemos que o sistema é homogêneo.

Exemplo 6. *Um exemplo simples de sistema linear é:*

$$\begin{cases} 3x + 2y = 0, \\ x - 2y = 0. \end{cases}$$

Dois sistemas são ditos equivalentes se, e somente se, tem o mesmo número de variáveis e as mesmas soluções.

Em um sistema linear, a fim de encontrar uma solução satisfatória, podemos realizar algumas operações a fim de determinar os valores das variáveis. Algumas destas operações podem ser:

- Multiplicação de um equação por escalar.
- Substituição de uma equação devido a soma/subtração com outra.
- Rearranjo das equações.

Estes sistemas lineares podem ser reescritos como sendo matriz para maiores informações a esse respeito ver (BOLDRINI et al., 1980) e (LIMA, 2012).

2.2.1 Matrizes

Definição 2.4. *(LIMA, 2012) Sejam m, $n \in \mathbb{N}$. Uma matriz $m \times n$ é uma lista de números reais a_{ij}, com índices duplos, onde $1 \leq i \leq m$ e $1 \leq j \leq n$. Costuma-se representar a matriz S com um quadro numérico com m linhas e n colunas, no qual o elemento a_{ij} situa-se no cruzamento da i-ésima linha com a j-ésima coluna. Notação:*

$$S = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} = (a_{ij})_{m \times n}.$$

Operação com matrizes

I **Soma entre matrizes:** Seja $A = (a_{ij})_{m \times n}$ e $B = (b_{ij})_{mxn}$, a soma $A + B$ é uma matriz $C = (c_{ij})$, tal que $c_{ij} = a_{ij} + b_{ij}$. Vale salientar que as matrizes A e B tem que ter o mesmo número de linhas e de colunas para que tal operação seja possível.

II **Multiplicação de matriz por escalar** Seja $A = (a_{ij})_{m \times n}$ e $\lambda \in \mathbb{R}$, o produto de λ por A será a matriz B tal que todo $b_{ij} = \lambda a_{ij}$.

III **Multiplicação entre matrizes** Seja $A = (a_{ij})_{m\times n}$ e $B = (b_{ij})_{n\times m}$, então definimos o produto $A.B$ como sendo $C = (c_{ij})$ tal que:

$$c_{ij} = a_{i1}.b_{1j} + a_{i2}.b_{2j} + \cdots + a_{i(n-1)}.b_{(n-1)j} + a_{in}.b_{nj} = \sum_{e=1}^{n} a_{ie}b_{ej}.$$

Vale lembrar também que para realizar esse tipo de operação entre matrizes é necessário que o número de colunas de A seja o número de linhas de B.

Fizemos operações entre escalares e matrizes e entre matrizes, mas será que existem algo que se possa calcular só como a matriz sem necessitar de outros artifícios?

Determinante

Elon, em seu livro (LIMA, 2012), diz que o determinante surgiu inicialmente nas fórmulas que exprimem a solução de um sistema determinado de n equações lineares a n incógnitas. Posteriormente, ele foi identificado como área de um paralelogramo ou o volume de um paralelogramo e depois, de forma definitiva como função multilinear alternada do qual todas as outras se deduzem.

De maneira bem simplicista definiremos o determinante de uma matriz quadrada com sendo um escalar que a define. A forma de determinar o valor desse escalar depende da quantidade de linhas/colunas que a matriz apresenta.

No caso de uma matriz de ordem 1, ou seja, com apenas uma linha e uma coluna o seu determinante é o próprio número que a representa, ou seja,

$$M = |a_{11}| \longrightarrow \det(M) = a_{11}.$$

Exemplo 7. $M_1 = |2| \longrightarrow \det(M_1) = 2$

No caso de matriz de ordem 2, o determinante pode ser expresso através da soma do produto de seus elementos da seguinte forma,

$$M = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \longrightarrow \det(M) = a_{11}.a_{22} - a_{12}.a_{21}.$$

Exemplo 8. $M_2 = \begin{vmatrix} 12 & 9 \\ 7 & 5 \end{vmatrix} \longrightarrow \det(M_2) = 12.5 - 9.7 = -3$

Nos casos de matriz de ordem 3, utilizamos que o $\det(M)$ será:

$$M = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \longrightarrow$$

$$\det(M) = a_{11}.a_{22}.a_{33} + a_{12}.a_{23}.a_{31} + a_{13}.a_{21}.a_{32} - a_{11}.a_{23}.a_{32} - a_{12}.a_{21}.a_{33} - a_{13}.a_{22}.a_{31}.$$

Exemplo 9.

$$M = \begin{vmatrix} -1 & 0 & 4 \\ 2 & 0 & 0 \\ -1 & 1 & -1 \end{vmatrix}$$

$$\det(M) = (-1).(0).(-1) + 0.0.(-1) + 4.2.1 - (-1).0.1 - 0.2.(-1) - 4.0.(-1) = 8$$

Boldrini em (BOLDRINI et al., 1980), reescreve o determinante de uma matriz de ordem 3 em função do determinante de ordem 2 da seguinte forma:

$$\det(M) = a_{11}.a_{22}.a_{33} - a_{11}.a_{23}.a_{32} + a_{12}.a_{23}.a_{31} - a_{12}.a_{21}.a_{33} + a_{13}.a_{21}.a_{32} - a_{13}.a_{22}.a_{31}.$$

Reescrevendo temos que:

$$\det(M) = a_{11}.[a_{22}.a_{33} - a_{23}.a_{32}] - a_{12}.[-a_{23}.a_{31} + a_{21}.a_{33}] + a_{13}.[a_{21}.a_{32} - a_{22}.a_{31}],$$

onde podemos observar que:

- $[a_{22}.a_{33} - a_{23}.a_{32}] = \det(A_{11})$
- $[a_{21}.a_{33} - a_{23}.a_{31}] = \det(A_{12})$
- $[a_{21}.a_{32} - a_{22}.a_{31}] = \det(A_{13})$

e assim teríamos:

$$\det(M) = a_{11}.\det(A_{11}) - a_{12}.\det(A_{12}) + a_{13}.\det(A_{13}).$$

logo

$$\det(M) = (-1)^{1+1}a_{11}.\det(A_{11}) + (-1)^{1+2}a_{12}.\det(A_{12}) + (-1)^{1+3}a_{13}.\det(A_{13}).$$

Portanto

$$\det(M) = \sum_{j=1}^{n} a_{1j}.(-1)^{1+j}.\det(A_{1j})$$

Esse método ficou conhecido como **desenvolvimento de Laplace** e nos permite calcular o determinante de matrizes de ordem 3 ou maiores (realizando as devidas alterações/expansões). Existem outros métodos bem interessantes para se calcular o determinante de matrizes de ordem superior a 3, mas que não serão abordados aqui. Caso o leitor se interesse pelo conteúdo sugerimos leitura de bons livros de Álgebra Linear como o do (BOLDRINI et al., 1980) para iniciantes e do (LIMA, 2012) para um nível de conhecimento mais avançado.

2.3 Geometria

O dicionário define geometria (do grego antigo, $\gamma\epsilon\omega\mu\epsilon\tau\rho\iota\alpha$) como sendo a parte da matemática que estuda o espaço e as figuras que o ocupam. Partindo disso, nessa seção veremos algumas definições a respeitos de alguns curvas e seus comportamento dentro de um espaço tridimensional.

Definição 2.5. *Uma curva algébrica é o lugar geométrico dos pontos cujas coordenadas cartesianas satisfazem uma equação do tipo $f(X, Y) = 0$, onde f é um polinômio não constante.*

Exemplo 10. *A função $f(x) = x^2 + y^2 - r^2$ tem como curva algébrica plana o círculo de centro na origem e raio r.*

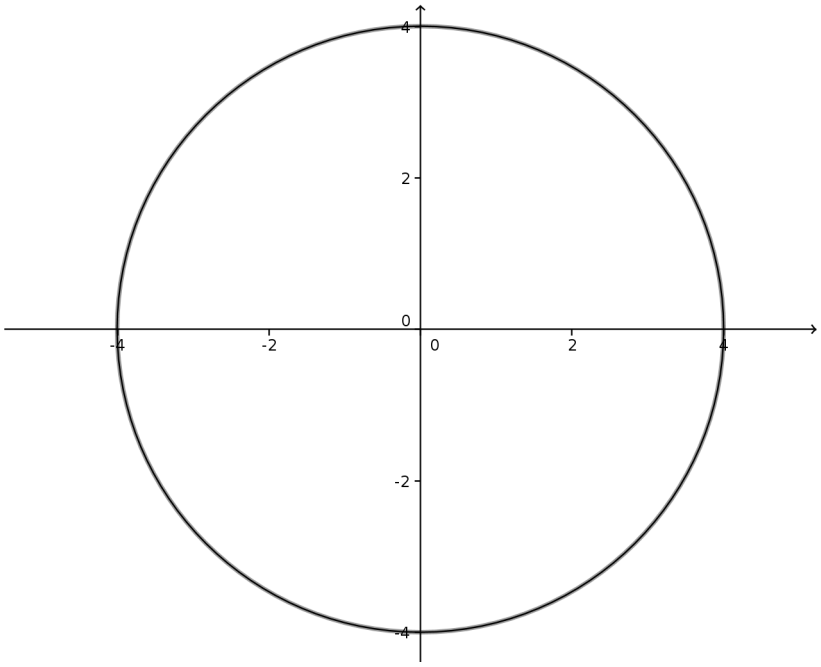


Figura 2.1: $f(x) = x^2 + y^2 - 4$ - Círculo

Exemplo 11. *A função* $f(x) = y - x^2$ *que tem como curva algébrica plana a parábola.*

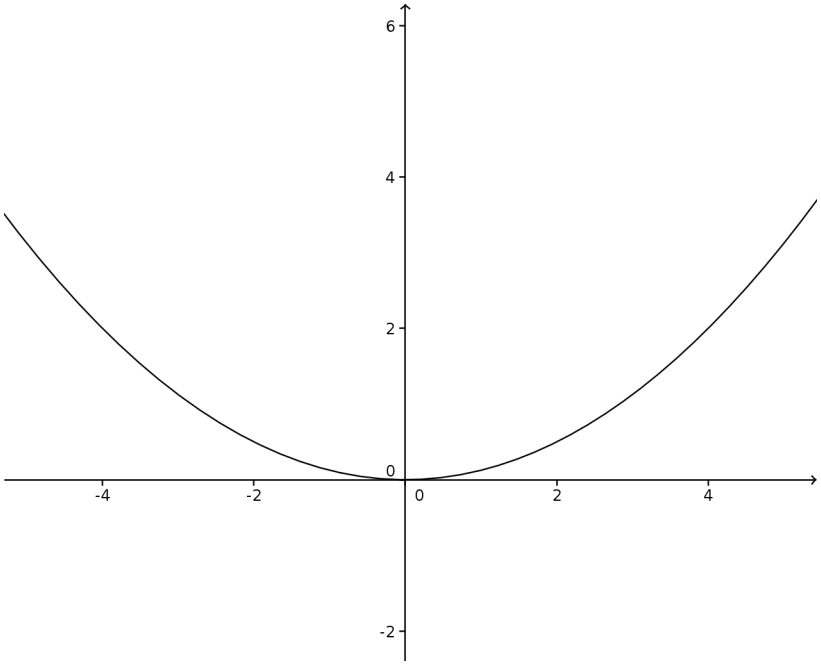


Figura 2.2: $f(x) = y - x^2$ - Parábola

Exemplo 12. *Seja a função* $f(x) = x^2 + y^2$. *É fácil ver que a* f *admite uma única solução em* $\mathbb{R}$ *com* $V(f) = (0, 0)$, *onde* $V(f)$ *é o conjunto das soluções da função* f.

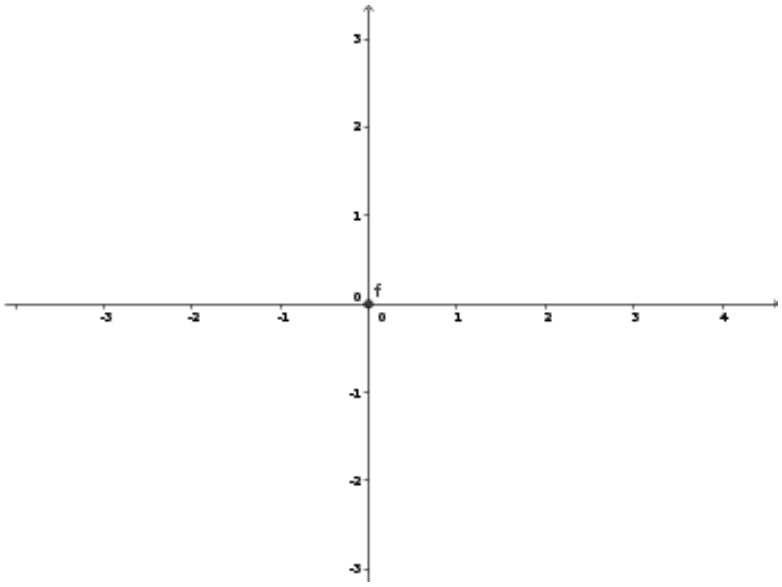


Figura 2.3: $f(x) = x^2 + y^2$

Exemplo 13. *A função* $f(x) = x^2 + y^2 + 1$ *não admite solução. Logo* $V(f) = \varnothing$.

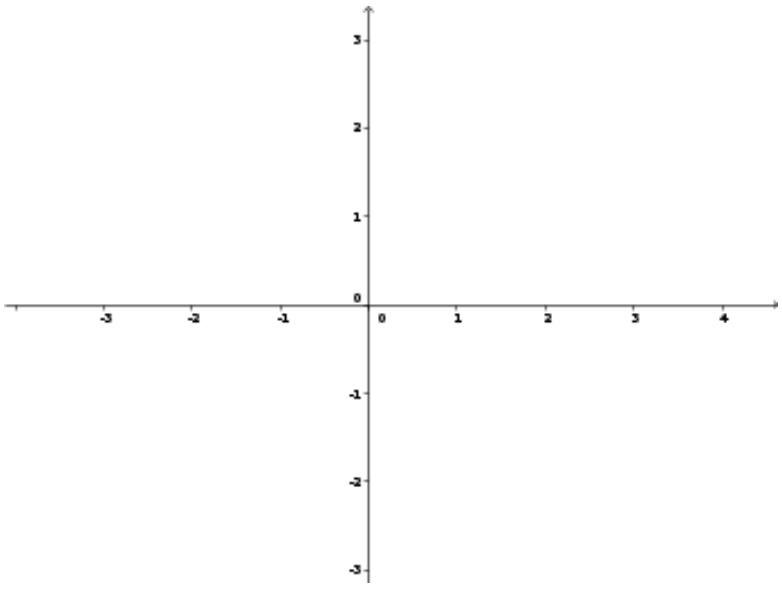


Figura 2.4: $f(x) = x^2 + y^2 + 1$

Observação: 1. *: Vale notar que se admitirmos soluções no conjunto dos números complexos vemos que os exemplos 12 e 13 passam a ter infinitas soluções.*

Definição 2.6. *(VAINSENCHER, 1979) Uma curva algébrica plana afim é uma classe de equivalência de polinômios não constante $f \in K[X,Y]$, onde K é um corpo que contém X e Y, módulo a relação que identifica dois tais polinômios se um é múltiplo do outro por uma constante diferente de 0. Nesse caso, a equação de uma curva é qualquer dos polinômios nessa classe.*

Dizemos que uma curva está definida sobre um corpo K_0, subcorpo de K, se ela admite uma equação com coeficientes em K_0.

O traço de uma curva é o conjunto das soluções da equação.

O grau de uma curva f é dado pelo grau de sua equação e deve ser denotado por δf.

Curvas de grau $1, 2, 3, ...$ são denominadas retas, cônicas, cúbicas, ...

Exemplo 14. *A curva $C_1 : y = m.x + d$ tem grau 1, cujo traço é uma reta. Vale ressaltar também que esta é a equação geral da reta, onde m é o coeficiente angular e d é o coeficiente linear.*

Exemplo 15. *A curva $C_2 : y = x^2$ tem como variável de maior grau a variável x e que tem grau 2 e que por definição é uma cônica, denominada parábola.*

Exemplo 16. *A curva $C_3 : x^2 = y^3 + y$ tem como variável de maior grau a variável y e que tem grau 3.*

2.3.1 Plano Projetivo

Considere um plano α, mergulhado no espaço tridimensional, de equação $z = a$ com $a \neq 0$. Por cada ponto de α podemos desenhar uma reta r que passa pela origem.

Uma reta s contida no plano α define um plano que contém a origem. Dados duas retas s e s' contidas no plano α, se as duas retas forem paralelas no plano α, os planos que elas definem se interceptam em uma reta contida no plano xy que passa pela origem. Se as duas retas forem concorrente elas se interceptam em um único ponto que define uma reta que passa pela origem.

Definição 2.7. *Plano projetivo, a que denotaremos por $\mathbb{P}^2$, é o conjunto de todas as retas que cruzam o espaço tridimensional e que passam pela origem.*

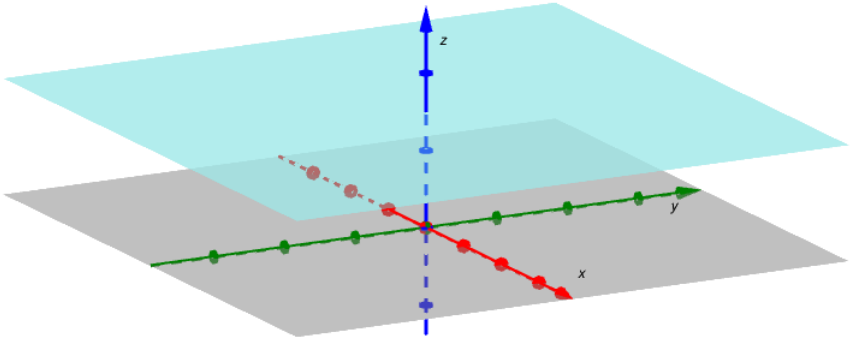


Figura 2.5: Plano $z = a \neq 0$

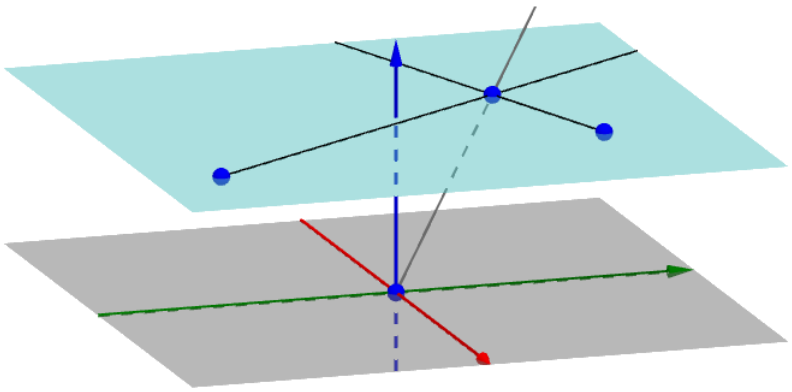


Figura 2.6: Retas concorrentes no plano $z = a$

Agora podemos verificar que todos pontos de α formam um subconjunto de pontos de $\mathbb{P}^2$. Assim sendo os pontos do subconjunto $\mathbb{P}^2 - \alpha$ denotaremos por ***pontos no infinito.***

Denotamos por $(x : y : z)$ o ponto de $\mathbb{P}^2$ que representa a reta ligando a origem O a um ponto $(x, y, z) \neq 0$. Dizemos que x, y e z são coordenadas homogêneas do ponto $(x : y : z)$ relativas à base canônica $\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$.

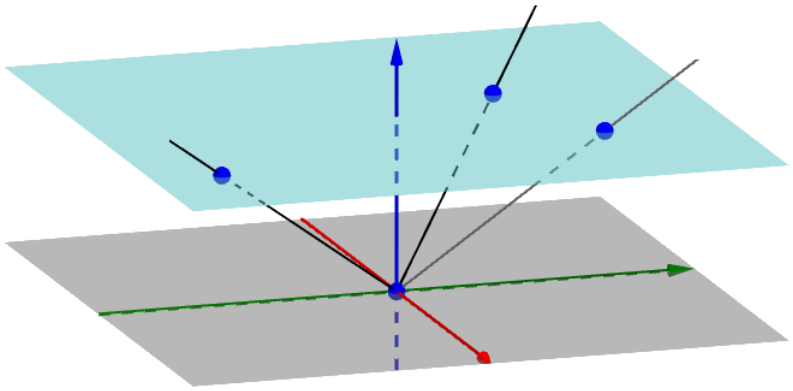


Figura 2.7: Projeção dos pontos do plano z sobre a origem

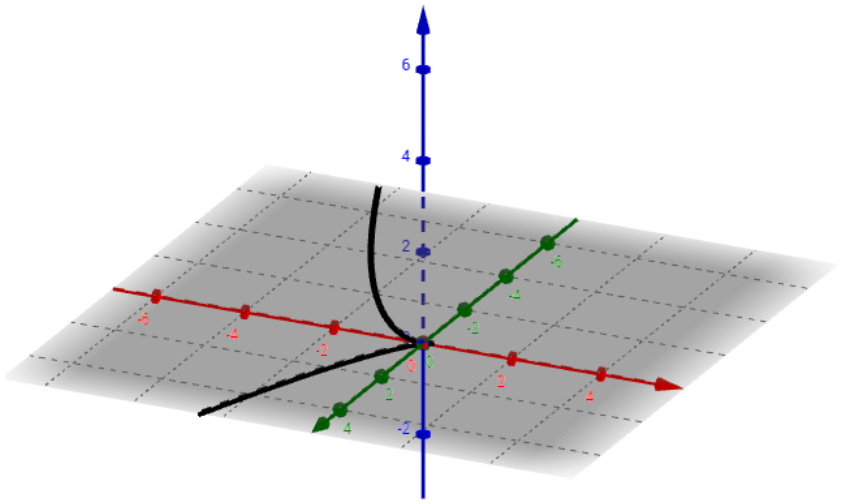
Capítulo 3

Curvas Elípticas

Antes de definirmos curvas elípticas, vamos determinar o que são curvas projetivas planas, uma vez que curva elíptica é um caso especifico.

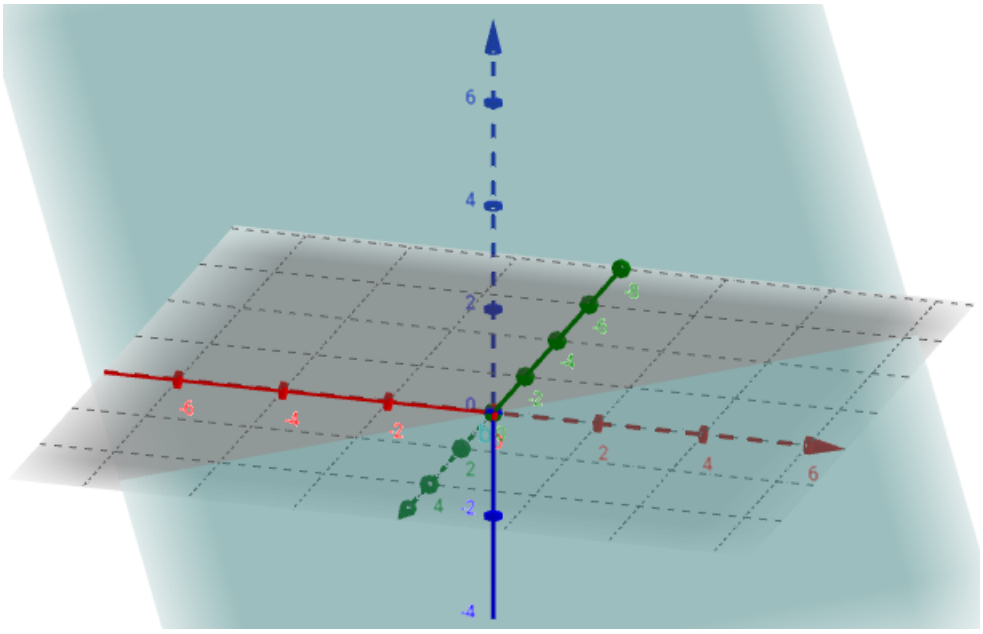
Definição 3.1. *(VAINSENCHER, 1979) Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos* [1] *não constantes,* $f \in k[X, Y, Z]$.

Exemplo 17. $x^3 + y^2.z + x.y.z = 0$.



Exemplo 18. $x + y + z = c$.

[1] polinômios em que os monômios com coeficiente não nulos tem o mesmo grau



Vale ressaltar que a convenções adotadas na seção 2.3 podem aqui serem utilizadas, realizando as devidas mudanças necessárias.

Um caso específico das curvas projetivas planas são as curvas elípticas. Existem várias formas de se definir as curva elíptica. Trabalharemos com a seguinte definição.

Definição 3.2. *Uma curva projetiva plana definida pela equação*

$$y^2.z = x^3 + a.x.z^2 + b.z^3, \tag{3.1}$$

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

E ainda tomando $z = 1$ podemos reescreve-la na forma:

$$y^2 = x^3 + a.x + b, \tag{3.2}$$

que é denominada curva elíptica sobre $\mathbb{Q}$ na forma de Weierstrass.

Os exemplos abaixo representam algumas curvas elípticas e algumas curva não elíptica em R^2

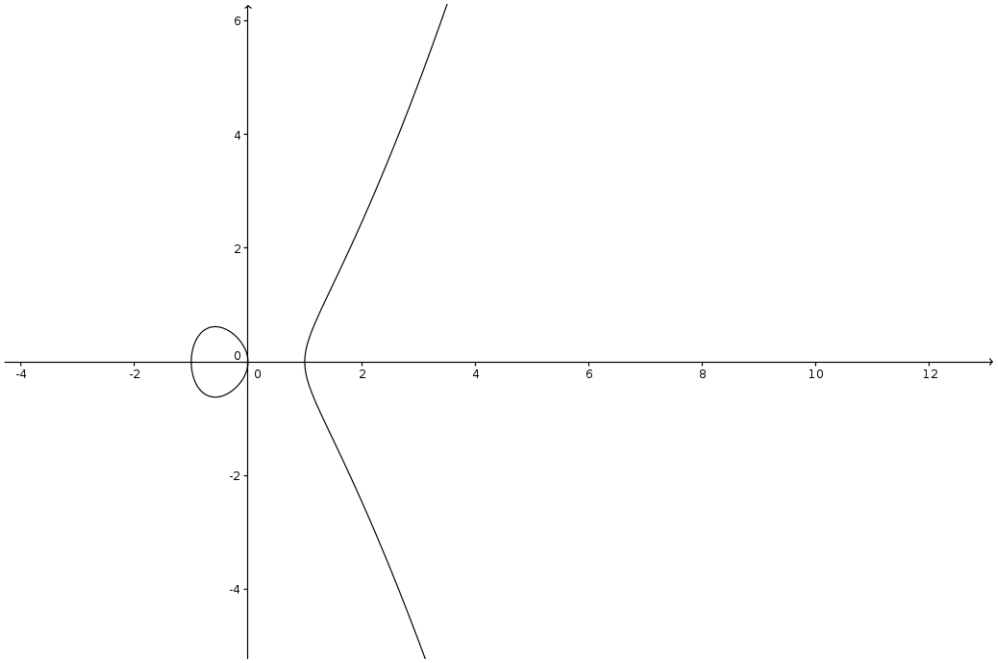


Figura 3.1: Curva $y^2 = x^3 - x$

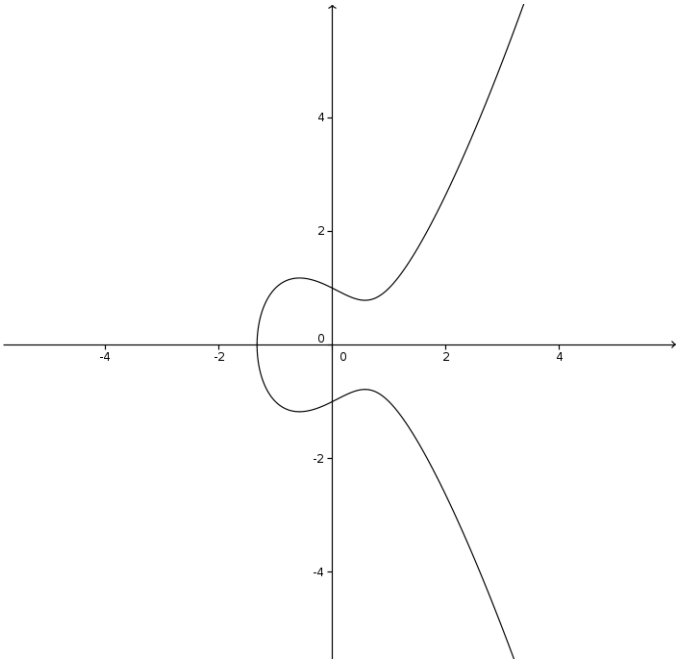


Figura 3.2: Curva $y^2 = x^3 + x + 1$

Na figura 3.1, temos a função $y^2 = x^3 - x$, nesse caso temos $a = 1$ e $b = 0$, logo o discriminante é $\Delta = 4.(1)^3 + 27.0 = 4 \neq 0$ e na figura 3.2, temos a função $y^2 = x^3 - x + 1$ de discriminante é $\Delta = 4(-1)^3 + 27.1 = 23 \neq 0$ ambas curvas elípticas.

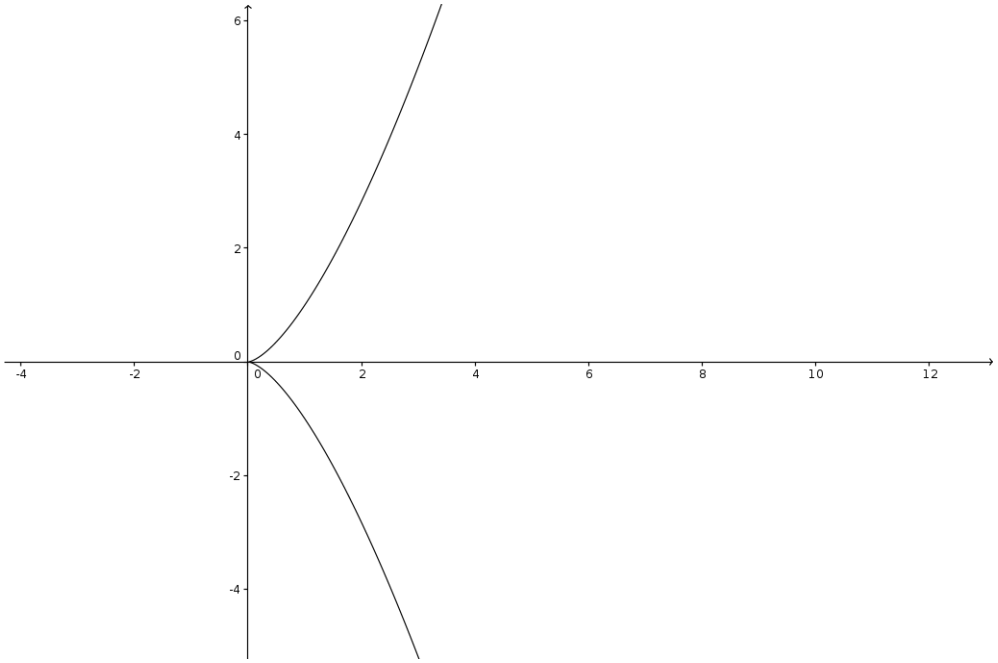


Figura 3.3: Curva $y^2 = x^3$

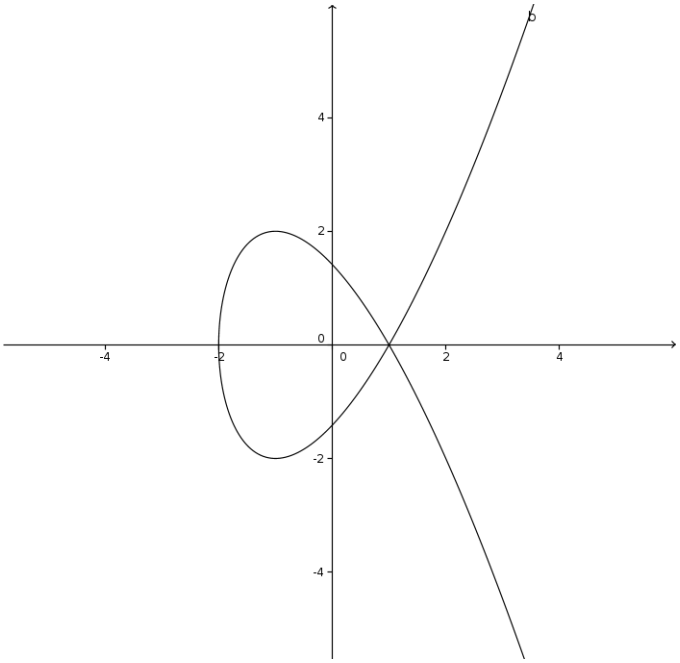


Figura 3.4: Curva $y^2 = x^3 - 3x + 2$

A figura 3.3, temos a função $y^2 = x^3$, por ela vemos que os coeficientes a e b são 0 (zeros) e o discriminante é $\Delta = 0$. Já na figura 3.4, o discriminante é $\Delta = 4.(-3)^3 + 27.(2)^2 = 0$, por esse motivo ambas não são consideradas curvas elípticas.

A importância de que o discriminante Δ seja diferente de 0 (zero) é para garantir que a curva elíptica seja uma curva lisa.

Definição 3.3 (Curva Lisa)**.** *Dizemos que uma curva é lisa quando a mesma não apresenta pontos de singularidade*[2]*, ou seja, para qualquer ponto da curva existe uma reta tangente bem definida.*

No desenrolar desse trabalho vale ressaltar que somente serão abordadas curvas na forma de Weierstrass, o que facilitara a nossa abordagem uma vez que toda curva que apresente no mínimo um ponto racional pode ser reescrita nessa forma através de uma mudança de variáveis convenientes. Para maiores informações sobre essas mudanças de variaveis ver bons livros de cálculo.

3.1 Geometria

Definimos anteriormente uma curva elíptica e sua forma normal de Weierstrass. Mas como determinar pontos dessa curva? É possível determinar um novo ponto a partir de outro já pré-determinado ou precisaria ter pelo menos dois, ou três? E como podemos defini-los?

Primeiro vamos verificar se existe intersecção entre duas curvas quaisquer e se quando elas se interseccionam quantos pontos em comum elas apresentam.

Teorema 3.1 (Teorema de Bézout)**.** *Sejam C_1 e C_2 duas curvas projetivas planas sem componentes comuns, ou seja, não existe um divisor comum para as duas curvas. Então o número de pontos na intersecção $C_1 \cap C_2$, contando com a multiplicidade, é igual ao produto do grau de seus polinômios, ou seja,*

$$\sharp(C_1 \cap C_2) = \delta(C_1).\delta(C_2).$$

Demonstração: *Ver (NIVEN; ZUCKERMAN; MONTGOMERY, 2008)*

[2]Dado um ponto $P = (x, y)$ da uma curva, ele se diz singular se

$$\frac{\partial f(P)}{x} = \frac{\partial f(P)}{y} = 0,$$

ou seja, tem suas derivadas parciais nulas.

Principais pontos da demonstração: *Como já foi visto no capítulo anterior tendo dois polinômios é possível gerar uma matriz com seus coeficientes, logo dadas C_1 e C_2 curvas algébricas de graus m e n, é possível montar tal matriz específica com seus coeficientes em z, isto é, as potências de x e y também aparecem na matriz. O determinante dessa matriz gerada; como, por definição, elas não apresentam componentes em comum, é um polinômio nas variáveis x e y. Demonstra-se que este polinômio é identicamente igual a zero ou uma forma de grau $m.n$*[3]*.*

Com este fato, pode-se demonstrar que duas curvas C_1 e C_2 sem componentes comuns de graus m e n respectivamente se intersectam em um número finito de pontos, em particular elas se intersectam no máximo em $m.n$ pontos distintos.[4]

O número de interseção $I(P, C_1, C_2)$ de um ponto $P = (x_0 : y_0 : z_0)$ é definido como a multiplicidade de (x_0, y_0) como raiz do resultante $R(x, y)$ após feitos os ajustes necessários. Se P não é ponto de interseção então $I(P, C_1, C_2) = 0$ e se P pertente a uma componente comum de C_1 e C_2 então $I(P, C_1, C_2) = \infty$.

A demonstração do Teorema de Bézout se conclui com, uma vez que a soma das multiplicidades das raízes de $R(x, y)$ é exatamente $m.n$, pois este é o grau de $R(x, y)$. A parte final é simples, se C_1 e C_2 não se encontrassem em nenhum ponto, teríamos $m.n = 0$, o que é claramente um absurdo.

Exemplo 19. *Considerando as curvas afins $C_1 : x - y = 0$ e $C_2 : x^3 - y^2 = 0$.*

As curvas C_1 e C_2 não tem componentes em comum, portanto é possível aplicar o Teorema de Bézout e assim:

$$\sharp(C_1 \cap C_2) = \delta(C_1).\delta(C_2) = 1.3 = 3$$

Vamos verificar fazendo os cálculos

[3]Em caso de duvidas a respeito desse assunto, ver (BOLDRINI et al., 1980), ou qualquer outro bom livro de Álgebra Linear

[4]Para maiores esclarecimentos sobre essa conclusão favor consultar (NIVEN; ZUCKERMAN; MONTGOMERY, 2008)

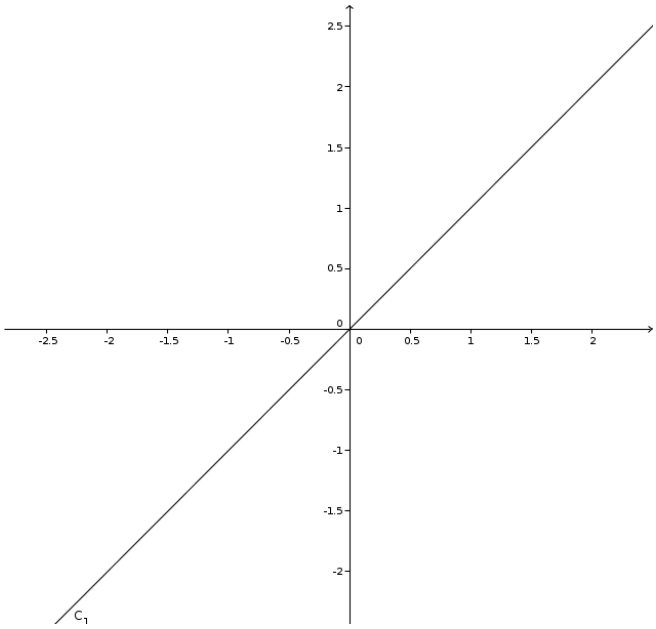


Figura 3.5: Curva C_1

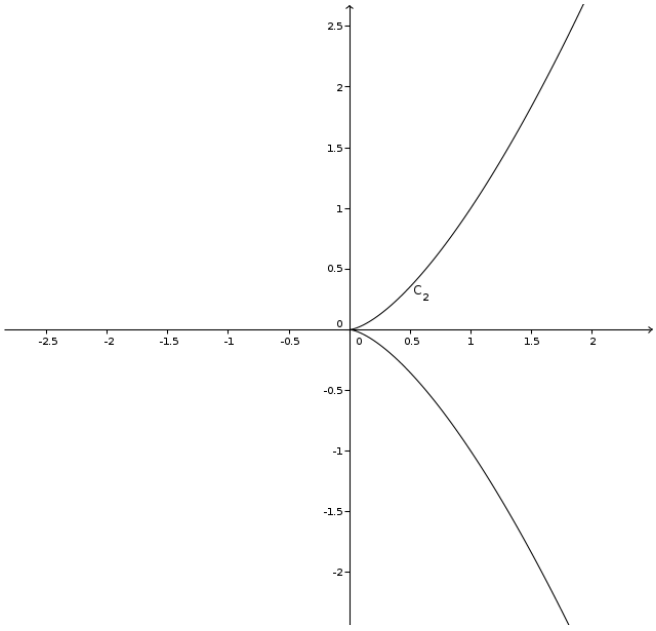


Figura 3.6: Curva C_2

Analisando a intersecção das curvas e substituindo C_1 em C_2 temos:

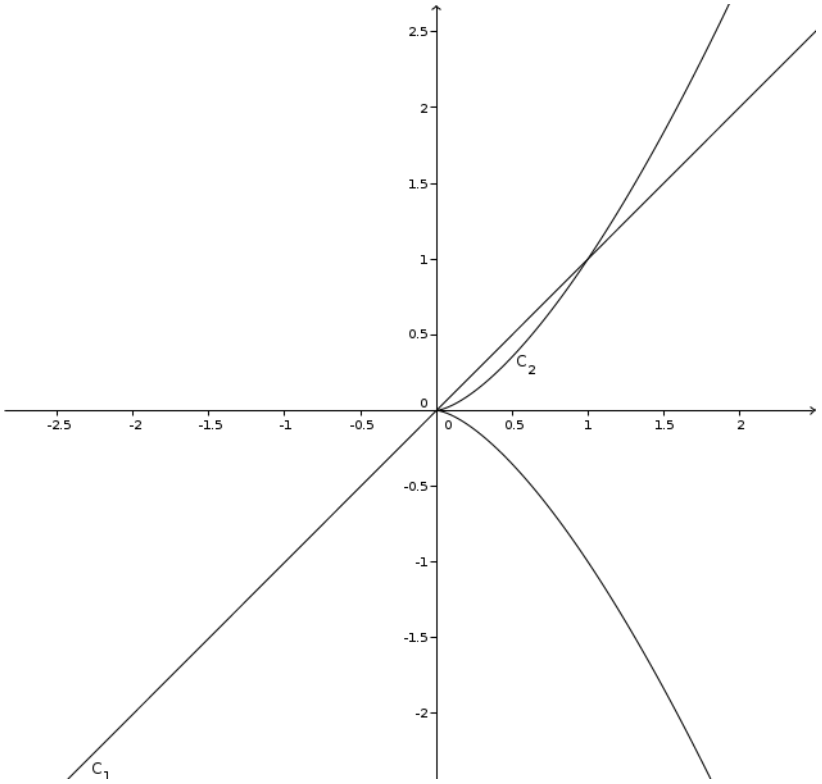


Figura 3.7: $C_1 \cap C_2$

$$C_1 : x = y.$$

$$C_2 : x^3 - x^2 = 0.$$

Então

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

Logo

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

Assim podemos concluir que os pontos de intersecção são $(0,0)$ *com multiplicidade* 2 *e* $(1,1)$. *Logo* $\sharp(C_1 \cap C_2) = 3$.

Portanto a partir desse exemplo podemos verificar que entre uma curva elíptica e uma reta qualquer existem até 3 pontos em comum se levarmos em consideração que nenhum desses pontos tem multiplicidade, isso pode ser verificado pelo Teorema de Bézout, uma vez que tratamos as curvas elípticas na forma de Weierstrass $C : y^2 =$

$x^3 + ax + b$ e a reta qualquer $r : y = m.x + d$, podemos ver que $\sharp C \cap r = \delta(C).\delta(r) = 3.1 = 3$. Logo concluímos que podemos conseguir até 3 pontos.

Podemos determinar um novo ponto dentro de curva elíptica usando dois métodos:

I) Com um ponto $P \in C$ podemos desenhar a reta tangente a C em P e determinar um novo o ponto de interseção da reta com a curva.

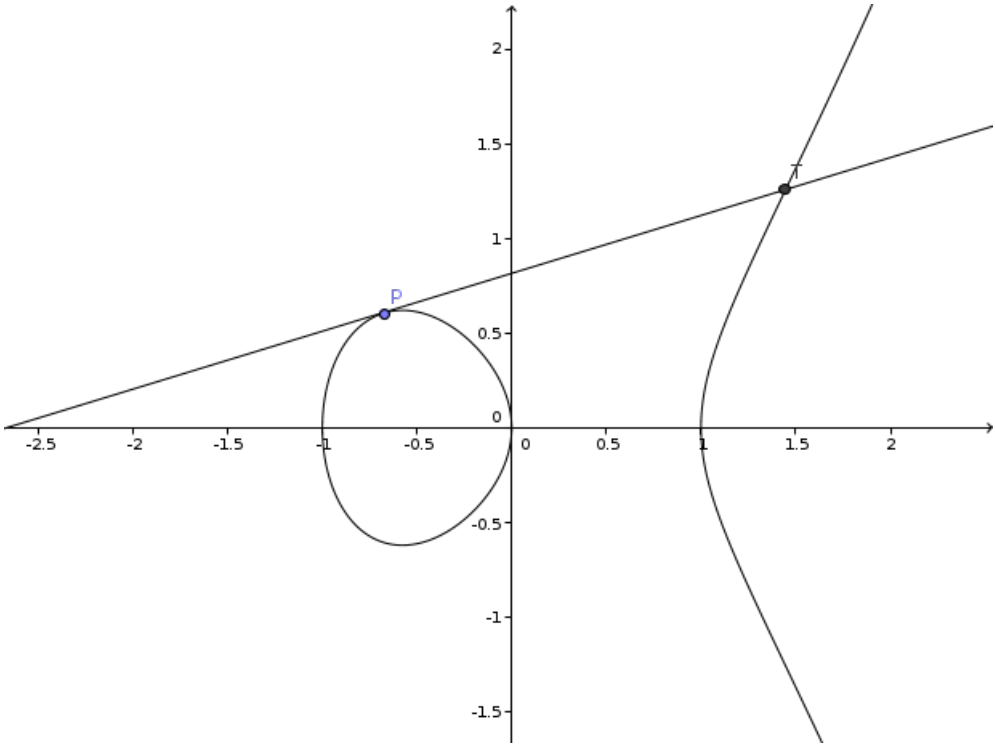


Figura 3.8: Ponto gerado pela tangente

II) A outra forma de conseguir um novo ponto racional da curva elíptica seria tomando dois pontos com coordenadas racionais P e Q da curva elíptica C e uma reta r definida também por esses dois pontos temos então que a interseção da curva e da reta nos apresenta mais um ponto que daremos o nome de $P * Q$.

Como os pontos P e Q são pontos com coordenadas racionais logo podemos concluir que $P * Q$ também será.

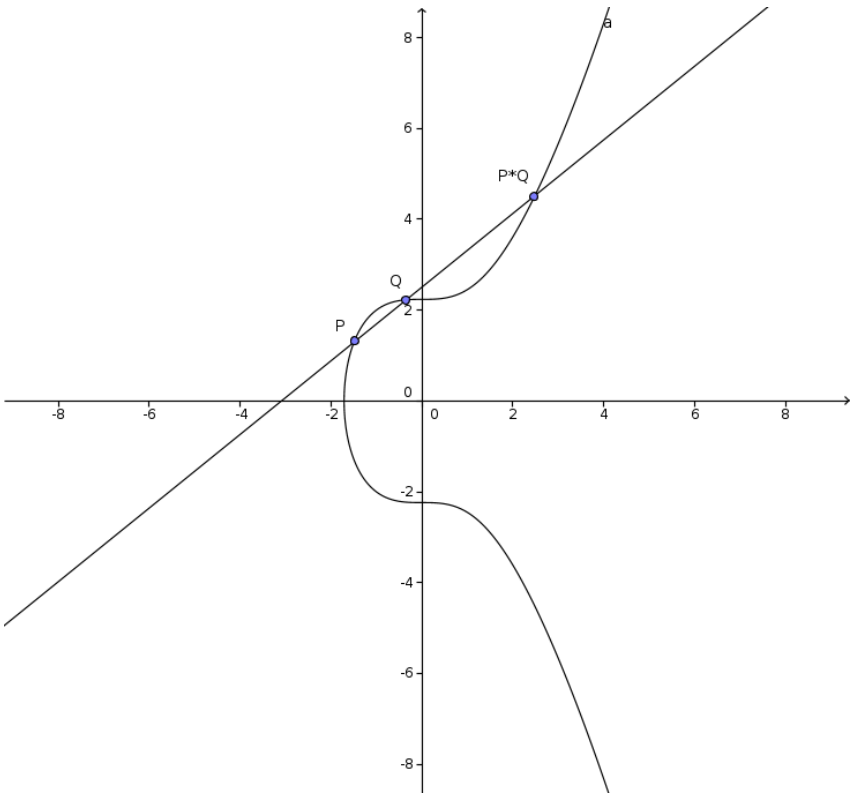


Figura 3.9: Ponto $P * Q$ gerado por P e Q

3.2 Álgebra

Assim em posse dessa operação vamos ver algumas de suas propriedades com pontos de C:

- $P * Q = Q * P$; a demonstração disso é de forma direta uma vez que essa propriedade se origina da definição
- $(P * Q) * Q = P$; novamente a demonstração vem da definição
- $((P * Q) * R) * S = P * (Q * R) * S$; a demonstração dessa propriedade não é usual tendo em vista da necessidade do Teorema dos nove pontos, encontrado em (SILVERMAN; TATE, 1992)

Se consideramos o conjunto de todos pontos com coordenadas racionais definidos na curva C podemos dizer que o conjunto apresenta um lei de composição. Para definirmos esse conjunto como um grupo há a necessidade de um elemento neutro.

Mas antes, vamos definir o que é $P + Q$. Tomemos $O, P, Q \in C$, definimos $P * Q$ sendo a intersecção da reta que contém P e Q com a curva C e $P + Q$ sendo a intersecção da reta que contém $P * Q$ e O com a curva C.

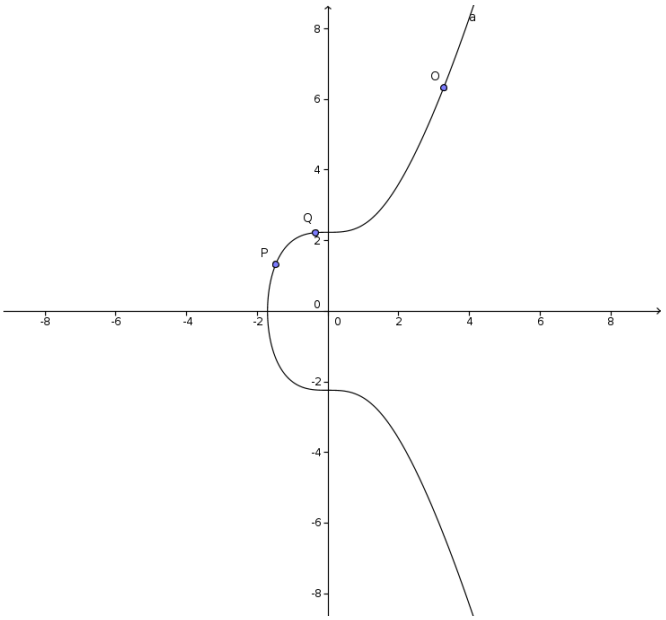


Figura 3.10: Ponto P, Q e O

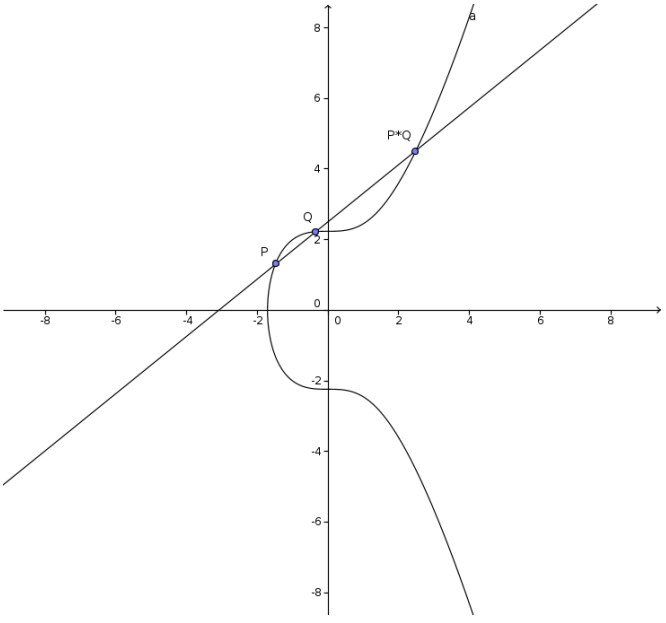


Figura 3.11: Ponto P, Q e P*Q

Assim definimos $P + Q = O * (P * Q)$.

Vamos mostrar que O é o elemento neutro, isto é, $P + O = P$. Seja l a reta que passa por P e O. Pelo Teorema de Bézout, existe um terceiro ponto $P * O$ na interseção $C \cap l$. Observe que a reta que passa por O e por $P * O$ é a própria reta l e o terceiro ponto de interseção é o ponto P, ou seja, $P + O = P$.

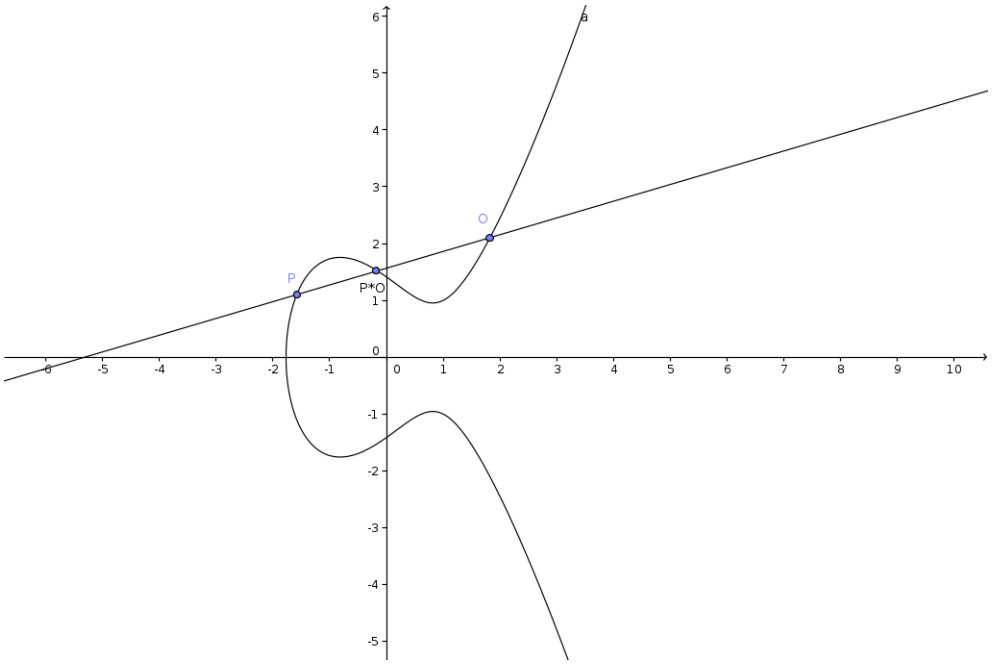


Figura 3.12: $P + O = P$

Assim nessa operação de grupo o ponto O atua como elemento neutro.

Teorema 3.2. *(SOUZA, 2012) Seja C uma curva elíptica sobre um corpo $\mathbb{Q}$ com um ponto $O \in C(\mathbb{Q})$, onde $C(\mathbb{Q})$ é o conjunto dos pontos racionais da curva C. Então, $C(\mathbb{Q})$ é um grupo abeliano com a operação $+$ definida anteriormente.*

Demonstração: Além das propriedades já mencionadas anteriormente para demonstrarmos que uma curva elíptica é uma grupo abeliano só falta determinarmos a existência do elemento inverso e da associatividade da operação pois a comutatividade é obvia.

Achemos de inicio o elemento inverso $-Q$ de um ponto Q. Seja l a reta tangente à cubica no ponto O, e seja S o terceiro ponto de interseção de C e l.

Seja r a reta que passa por Q e S. Então $-Q$ será o terceiro ponto de interseção de C e r. Pois a reta que passa por Q e $-Q$ é a reta r, logo $Q * (-Q) = S$. A reta que passa por O e S é a reta l, que é tangente a C no ponto O, isto é, $O * S = O$. Portanto $Q + (-Q) = O$.

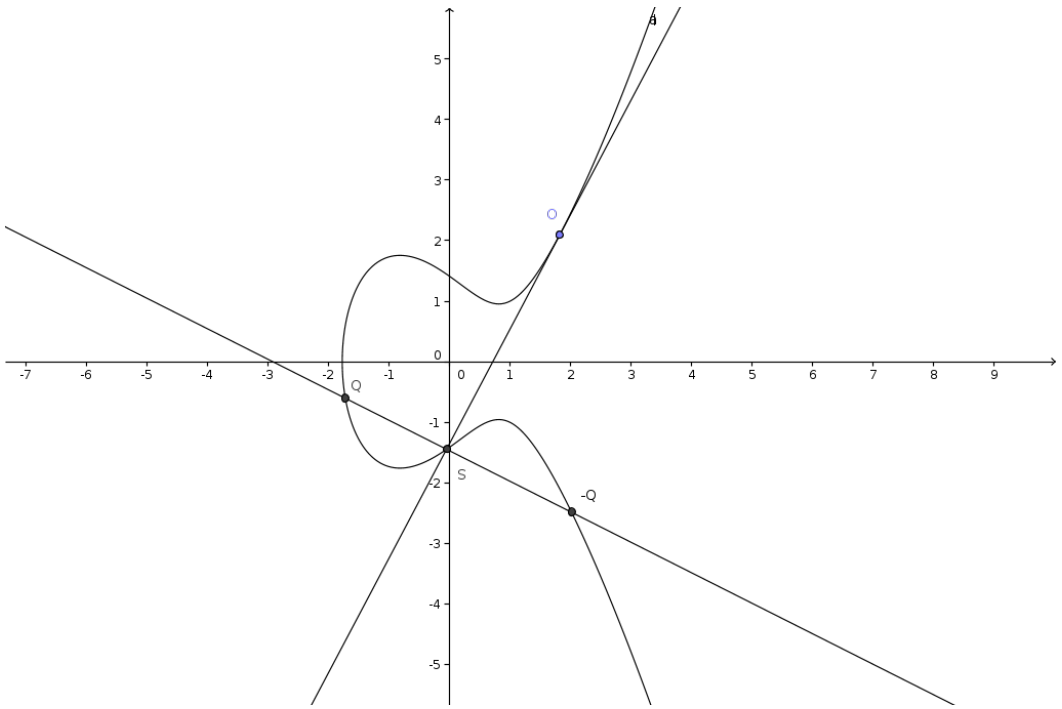


Figura 3.13: Q e $-Q$

Vamos provar a associatividade desta operação. Sejam P, Q, R três pontos sobre a curva C. Provar que $(P + Q) * R = P * (Q + R)$ é suficiente para demonstrar que $(P + Q) + R = P + (Q + R)$:

- l_1 a reta que passa por P, Q e $P * Q$.
- r_1 a reta que passa por O, $P * Q$ e $P + Q$.
- l_2 a reta que passa por R, $P + Q$ e $R * (P + Q)$.
- r_2 a reta que passa por Q, R e $Q * R$.
- l_3 a reta que passa por O, $Q * R$ e $Q + R$.
- r_3 a reta que passa por P, $Q + R$ e $P * (Q + R)$.

Considere agora as cúbicas C_l definida pela união de l_1, l_2 e l_3 e C_r definida pela união $r_1 \cup r_2 \cup r_3$. Observe que C e C_l se intersectam nos pontos P, Q, $P * Q$, $P + Q$, R, $(P + Q) * R$, O, $Q * R$ e $Q + R$.

Observe também que C e C_r se intersectam nos pontos O, $P * Q$, $P + Q$, Q, R, $Q * R$, $Q + R$, P e $P * (Q + R)$.

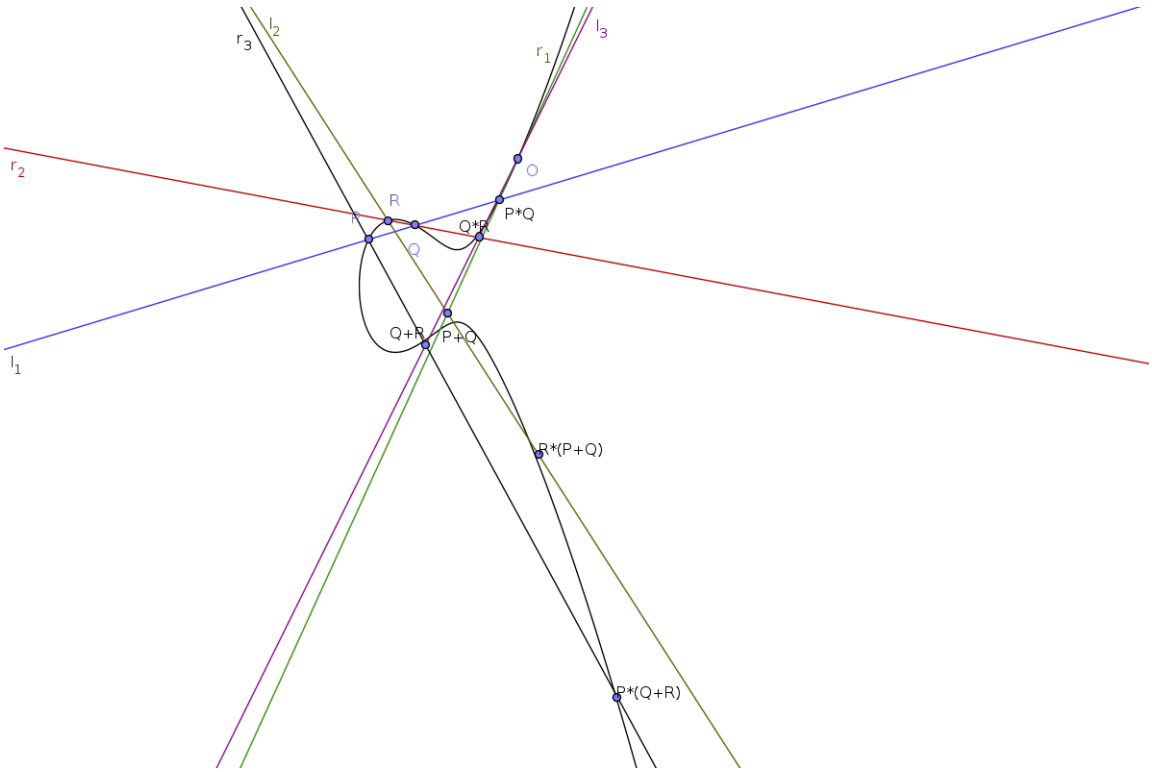


Figura 3.14: Conjunto das retas

Assim $C \cap C_l$ e $C \cap C_r$ possuem 8 pontos em comum. Agora, pela proposição a seguir o nono ponto de interseção deve ser o mesmo. Ou seja $(P+Q)*R = P*(Q+R)$.

Proposição 3.1. [5] *Se duas curvas cúbicas em K se intersectam em exatamente nove pontos, então toda curva cúbica que passa por oito desses nove pontos, também passará pelo nono ponto.*

Demonstração: *Ver em (MILNE, 2006).*

A partir disso alguns pontos são interessante de se notar.

Teorema 3.3. ***(Poincaré)*** *(SALEHYAN, 2015) Sejam C uma cúbica irredutível. O seu ponto no infinito, $P \in S_C$, onde S_C é o grupo abeliano formado com os pontos de C. Denote por $+'$ a operação definida em S_C tomando P' como o ponto fixo. Então $A +' B = A + B - P'$, para todo $A, B \in S_C$. Em particular a aplicação*

$$A \mapsto^{\Phi} A - P'$$

[5] Proposição extraída de (MILNE, 2006)

define um isomorfismo entre $(S_C, +')$ *e* $(S_C, +)$.

Demonstração: A igualdade é obtida usando a propriedade de elemento inverso do grupo:

$$\begin{aligned} A + B - P' &= (((A * B) * P) * (-P')) * P \\ &= (A * B) * ((P * P) * (-P')) \\ &= (A * B) * ((-P') * (P * P)) \\ &= (A * B) * P' \\ &= A +' B. \end{aligned}$$

Claramente Φ e uma bijeção. Utilizando a igualdade entre as operações:

$$\begin{aligned} \Phi(A +' B) &= \Phi(A + B - P') \\ &= A + B - P' - P' \\ &= A - P' + B - P' \\ &= \Phi(A) + \Phi(B). \end{aligned}$$

Tomando o ponto no infinito como o ponto fixo obteremos algumas vantagens, por exemplo fica mais simples determinar o inverso de um ponto. Nesse caso $O*O = O$, portanto $-P = P * O$.

Proposição 3.2. *(SALEHYAN, 2015) Tome o ponto no infinito,* O*, como o ponto fixo. Sejam* P*,* Q*,* $R \in S_C$*. Então* $P + Q + R = O$*, se, e somente se,* P, Q, R *são colineares.*

De fato,

$$\begin{aligned} P+Q+R=O &\iff P+Q=-R \\ &\iff (P*Q)*O=R*O \\ &\iff ((P*Q)*O)*O=(R*O)*O \\ &\iff P*(-(Q*O))=-(-R) \\ &\iff P*Q=R. \end{aligned}$$

3.3 Caracterização algébrica dos pontos

Sejam uma curva elíptica, na forma de Weierstrass, e um ponto $O = (0 : 1 : 0)$ no infinito. Vamos definir um método para determinar pontos racionais na curva elíptica.

3.3.1 Dois pontos da curva elíptica

Como já foi relatado e provado pelo Teorema de Bézout, dados dois pontos $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ da curva C podemos definir um terceiro ponto sobre a curva ao qual denotaremos por $P * Q = (x_3, y_3)$. Ao reflexo deste ponto pelo eixo Ox daremos o nome de $P + Q = (x_3, -y_3)$. Agora vamos tentar determinar os valores de x_3 e y_3.

Primeiro, a equação da reta[6] que passa por P e Q em função do coeficiente angular, é dada por:

$$y = m.x + d, \tag{3.3}$$

onde nesse caso $m = \dfrac{y_2 - y_1}{x_2 - x_1}$ e $d = y_2 - m.x_2 = y_1 - m.x_1$.

Substituindo os valores de (3.3) em (3.2) temos que:

$$y^2 = (mx + d)^2 = x^3 + ax + b.$$

Reescrevendo temos que

[6]Para mais informações ver (SILVA, 1985)

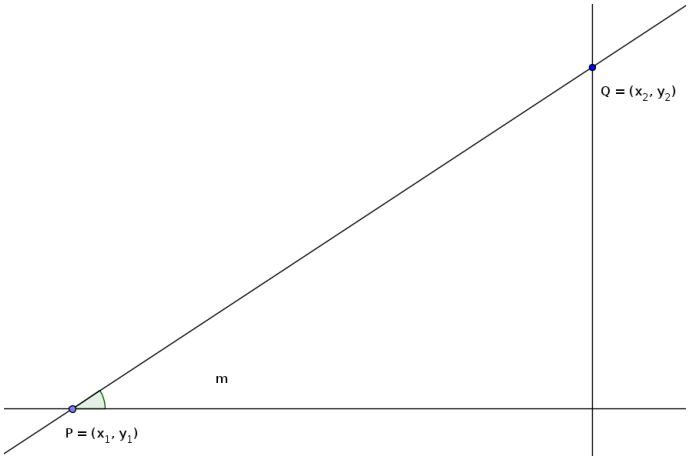


Figura 3.15: Coeficiente angular

$$m^2x^2 + 2mxd + d^2 = x^3 + ax + b,$$

logo

$$x^3 - m^2.x^2 + (a - 2md).x + (b - d^2) = 0.$$

Como já determinamos por definição que duas raízes são racionais isso implica que a terceira raiz também será. Portanto

$$(x - x_1)(x - x_2)(x - x_3) =$$

$$x^3 - (x_1 + x_2 + x_3).x^2 + (x_1.x_2 + x_1.x_3 + x_2.x_3).x + ((-1)(x_1.x_2.x_3)),$$

logo comparando

$$x^3 - m^2.x^2 + (a - 2md).x + (b - d^2) =$$

$$x^3 - (x_1 + x_2 + x_3).x^2 + (x_1.x_2 + x_1.x_3 + x_2.x_3).x + ((-1)(x_1.x_2.x_3)).$$

Assim temos as seguintes igualdades

$$\begin{cases} m^2 = (x_1 + x_2 + x_3), \\ a - 2md = (x_1.x_2 + x_1.x_3 + x_2.x_3), \\ b - d^2 = ((-1)(x_1.x_2.x_3). \end{cases}$$

O que nos interessa é somente a primeira. Isolando x_3 obtemos:

$$m^2 - x_1 - x_2 = x_3.$$

Assim ficamos com seguinte para determinarmos o valor de $P * Q$ e $P + Q$:

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

Exemplo 20. *Seja a curva elíptica* $y^2 = x^3 + 17$ *e os dois pontos pertencentes a ela* $P_1 = (-1, 4)$ *e* $P_2 = (2, 5)$*. Calculemos* $P_1 + P_2$*.*

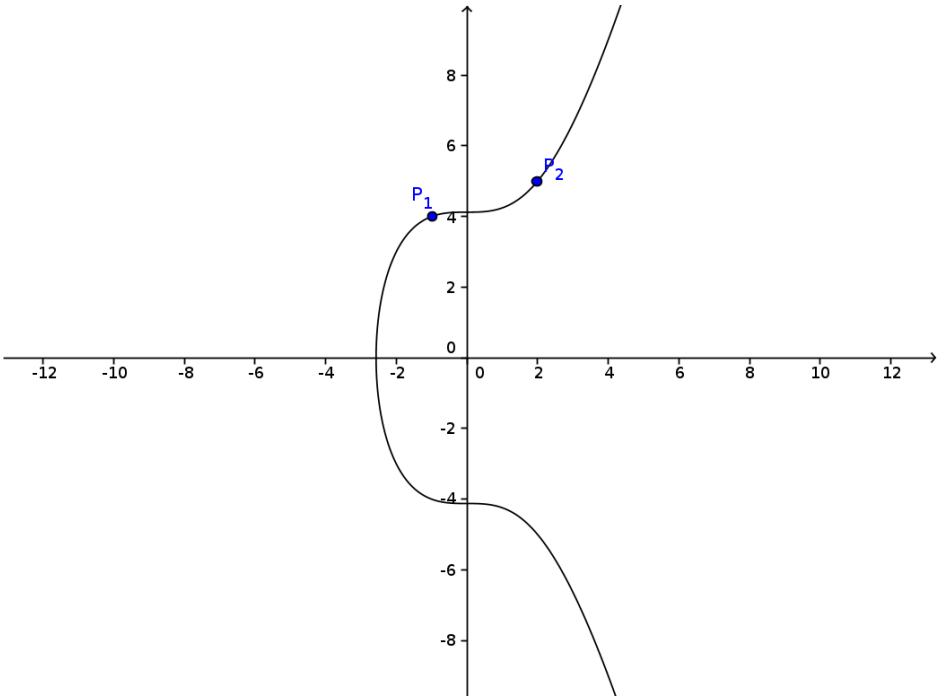


Figura 3.16: $y^2 = x^3 + 17$

Primeiramente, vamos determinar a reta que passa por P_1 *e* P_2 *e que por consequência gera* $P_1 * P_2$ *para isso vamos determinar* m*. Assim*

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - 4}{2 - (-1)} = \frac{1}{3}.$$

Em posse de m*, vamos determinar o valor de* d*. Logo,*

$$y = m.x + d \iff 5 = \frac{1}{3}2 + d \iff d = 5 - \frac{2}{3} = \frac{13}{3}.$$

Assim a equação da reta é

$$y = \frac{1}{3}x + \frac{13}{3}.$$

Em posse disso vamos determinar o valor de $P_1 * P_2$*:*

$$x_3 = m^2 - x_1 - x_2 \iff x_3 = \frac{1}{3} - (-1) - 2 = -\frac{8}{9}.$$

e

$$y_3 = m.x_3 + d \iff y_3 = \frac{1}{3}.\left(-\frac{8}{9}\right) + \frac{13}{3} = \frac{109}{27}.$$

Como vimos anteriormente temos que $P_1 + P_2 = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$.

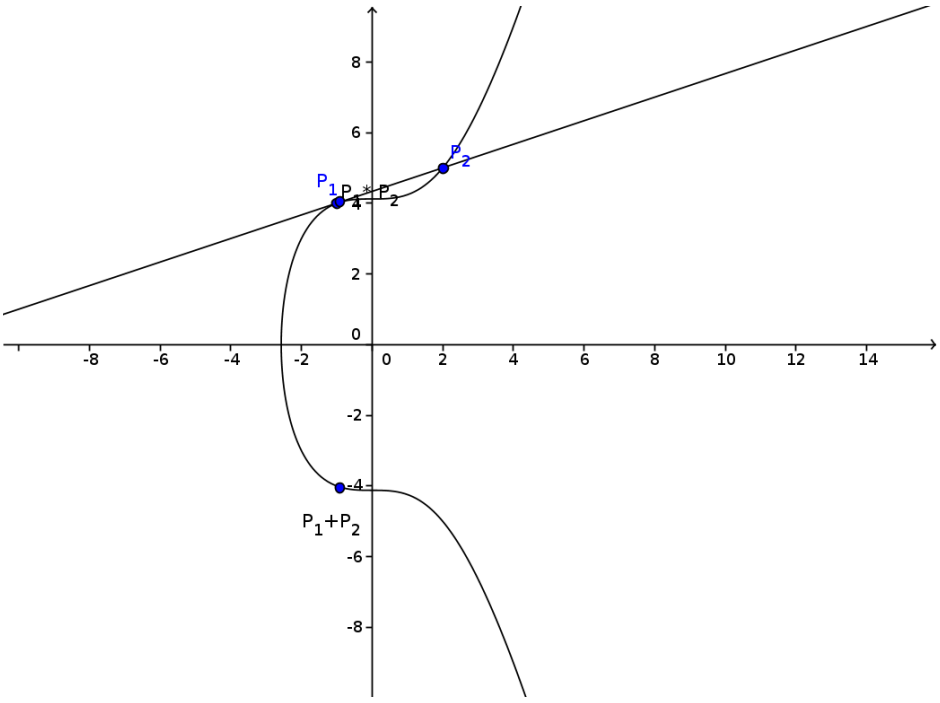


Figura 3.17: Ponto $P_1 + P_2$

3.3.2 Reta tangente

Na seção anterior vimos como determinar um terceiro ponto racional de uma curva elíptica a partir de outros dois pontos racionais quaisquer da curva. Mas e se tivéssemos apenas um ponto P racional dessa mesma curva? A resposta dessa questão está na reta tangente à curva nesse determinado ponto P, ou seja, consideraremos m como sendo:

$$m = \frac{dy}{dx} = \frac{f'(x)}{2y}. \tag{3.4}$$

Analisando a equação antiga temos:

$$x_3 = m^2 - x_1 - x_2.$$

Como $x_1 = x_2$ temos que:

$$x_3 = m^2 - 2.x_1.$$

Substituindo também o novo valor de m temos que

$$x_3 = \left(\frac{f'(x)}{2y}\right)^2 - 2x. \tag{3.5}$$

Abriremos aqui um parenteses para desenvolver melhor a equação 3.5 com o uso da 3.1. Assim

$$y^2 = f(x) = x^3 + ax + b$$

Diferenciando-a encontramos

$$f'(x) = 3x^2 + a$$

Aplicando em 3.5 temos

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

logo

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

assim

$$x_3 = \left(\frac{9x^4 + 6ax^2 + a^2}{4y^2}\right) - 2x.$$

Substituindo y^2 na equação temos:

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

Portanto,

$$x_3 = \left(\frac{9x^4 + 6ax^2 + a^2}{4x^3 + 4ax + 4b}\right) - 2x$$

Reescrevendo temos que

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

Logo

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

Assim

$$x_3 = \left(\frac{9x^4 + 6ax^2 + a^2 - 8x^4 - 8ax^2 - 8xb}{(4x^3 + 4ax + 4b)}\right)$$

Concluímos que

$$x_3 = \frac{x^4 - 2ax^2 - 8xb + a^2}{(4x^3 + 4ax + 4b)}; \tag{3.6}$$

depende apenas do ponto P e da curva.

Agora, para a coordenada y continua valendo a regra antiga, mas com as devidas alterações, trocando m por $\frac{f'(x)}{2y}$ ficando com:

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

Estas são as fórmulas aplicadas para determinar novos pontos racionais através

da adição de pontos dentro das curvas elípticas na forma de Weierstrass.

Capítulo 4

Aplicações

Existem diversas aplicações para os estudos que se desenvolvem nas curvas elípticas que podem ser usadas no ensino médio ou em estudos mais avançados. Mostraremos alguns casos bem interessante que podem ser usados como curiosidade para alunos tanto do ensino médio quanto da graduação para ver as varias metodologias que podem ser abordada para a resolução desses problemas.

4.1 Piramide de base quadrada

[1] 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 nível, nove no terceiro e assim por diante. Uma questão que pode ser levantada é: será possível desmanchar esta pirâmide e reagrupar estas bolas de maneira que formem um quadrado?

Vamos determinar quantas balas tem a pirâmide dependendo do nível.

- $n = 1$, temos 1 bala

[1] Exemplo extraído de (CARNEIRO, 2014)

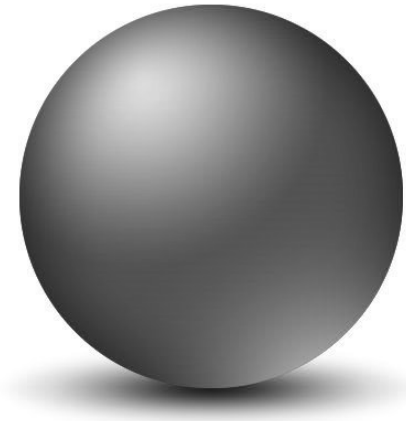


Figura 4.1: Pirâmide formada com apenas uma esfera - Imagem extraída e adaptada do site

- $n = 2$, temos $1 + 2^2 = 5$ balas

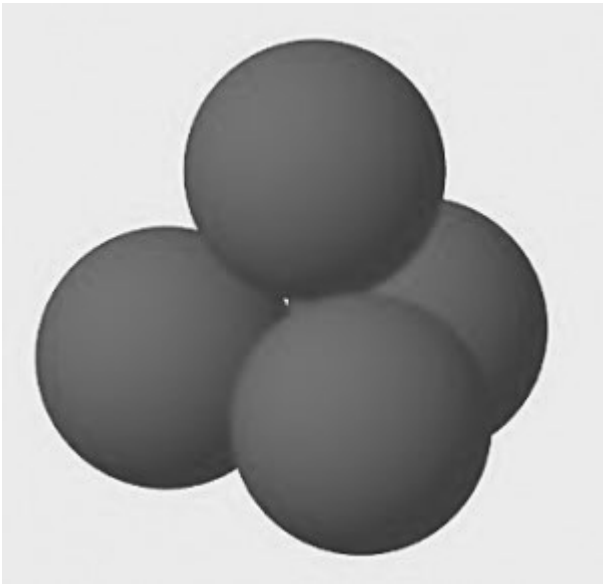


Figura 4.2: Pirâmide formada com cinco esferas - Imagem extraída e adaptada do site

- $n = 3$, temos $1 + 2^2 + 3^2 = 14$ balas

Por analogia, vemos que a quantidade de bolas de um nível é dado somando o número do nível elevado ao quadrado com a quantidade de bolas do nível anterior. Seguindo o raciocínio a quantidade de bolas do nível x será

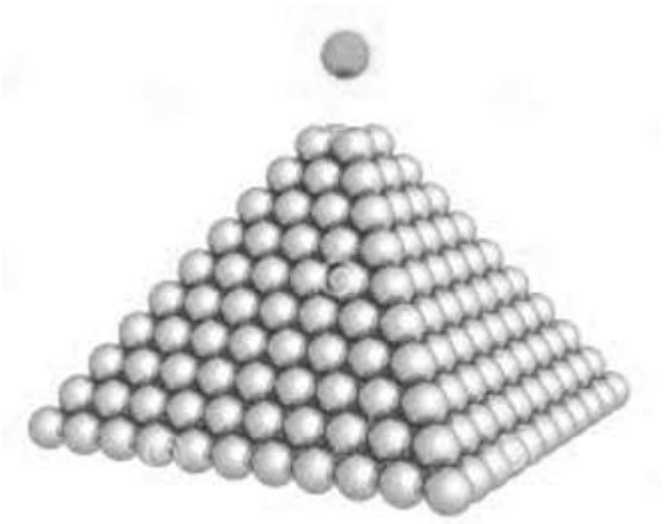


Figura 4.3: Piramide de esferas - Imagem extraida e adaptada do site

$$1 + 2^2 + \cdots + (x-1)^2 + x^2, \tag{4.1}$$

É de fácil compreensão que essa soma 4.1 pode ser reescrita como:

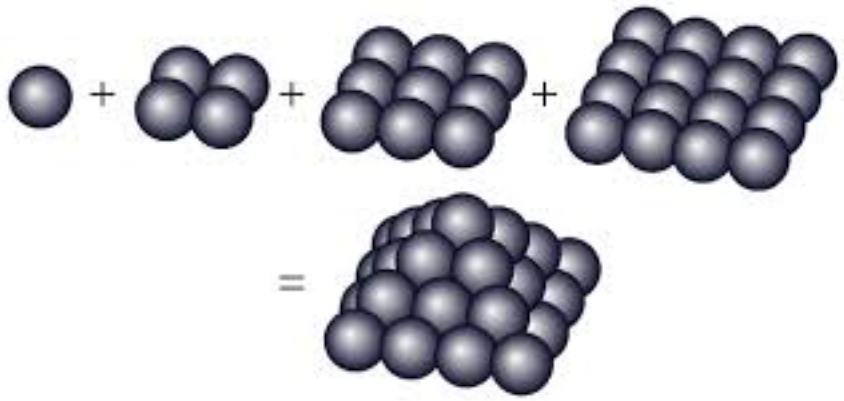


Figura 4.4: Organização da piramide - Imagem extraída e adaptada do site

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

Sabendo o número de balas tem a forma de um quadrado temos que:

$$\frac{x(x+1)(2x+1)}{6} = y^2. \tag{4.2}$$

A equação (4.2) 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 (4.2), obtendo-se:

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

Desenvolvendo os cálculos

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0. \tag{4.3}$$

A equação (4.3) é um polinômio de terceiro grau. Logo, é possível 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

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

O coeficiente de x^3 é 1 (conforme acontece na equação (4.3)), 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 4.2, 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 $\left(\frac{1}{2}, -\frac{1}{2}\right)$ 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

4.2. Podemos repetir o processo usando agora os pontos $\left(\frac{1}{2}, -\frac{1}{2}\right)$ e $(1, 1)$, desta vez, encontra-se $x = 24$ e $y = 70$, o que representa:

$$1 + 2^2 + \cdots + 24^2 = 70^2$$

encontrando assim uma solução para o problema.

4.2 Calculo de um ponto da curva

Considere a curva $C : y^2 = x^3 - 36.x$ e sejam $P = (-3, 9)$ e $Q = (-2, 8)$ pontos da curva C. Vamos determinar $P + Q$.

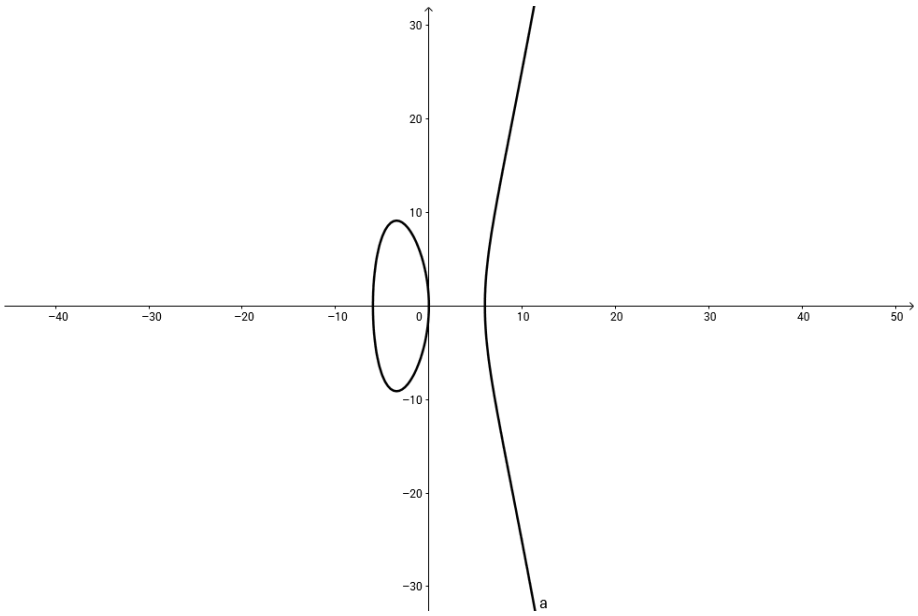


Figura 4.5: $C : y^2 = x^3 - 36x$

Solução: Como vimos anteriormente $P + Q = -(P * Q) = (x_3, -y_3)$ assim para calcularmos o valor de $P + Q$ precisamos determinar o valor de $P * Q$.

Usando os conhecimento adquiridos em 3.3.1 vamos determinar m e d.

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8 - 9}{-2 - (-3)} = -1$$

Agora em posse do m vamos calcular o d:

$$d = y_1 - m.x_1 = 9 - (-1).(-3) = 6$$

Agora vamos calcular $P * Q$

$$x_3 = m^2 - x_1 - x_2 = (-1)^2 - (-3) - (-2) = 6$$

$$y_3 = m.x_3 + d = (-1).6 + 6 = 0$$

Assim $P * Q = (6, 0)$ sabendo disso podemos concluir que $P + Q = (6, 0)$

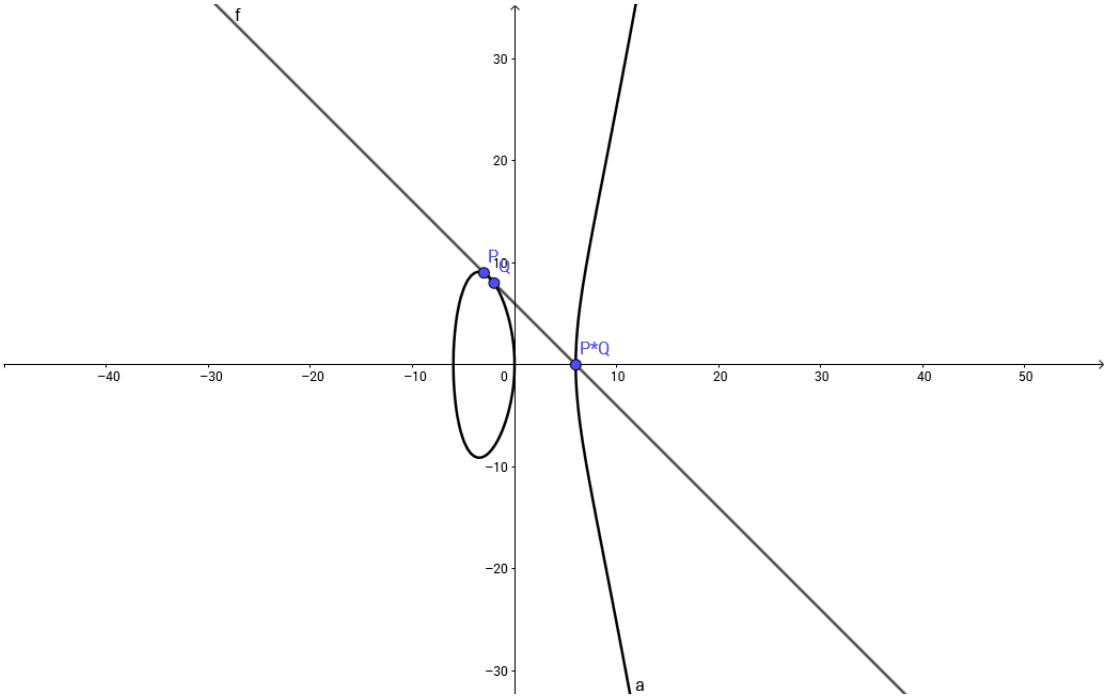


Figura 4.6: Ponto $P * Q = P + Q$

4.3 Calculo de 2P

Seja a curva eliptica $C : y^2 = x^3 + 17$ e o ponto $P = (-1, 4) \in C(\mathbb{Q})$. Calculemos $2.P$

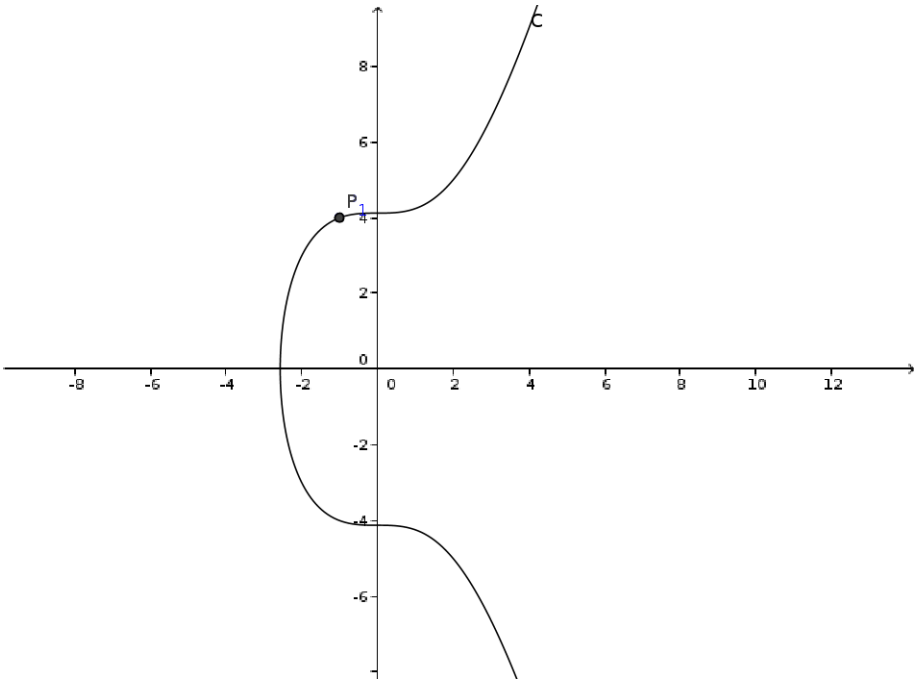


Figura 4.7: Curva C e o ponto P

Como só temos um único ponto P da curva C então teremos que usar os conceitos apresentados na seção 3.3.2. Assim sendo primeiro vamos determinar o valor de m para isso usaremos a equação 3.4.

Como

$$f(x) = x^3 + 17 \longrightarrow f'(x) = 3x^2.$$

Assim

$$m = \frac{3x^2}{2y}.$$

Logo

$$m = \frac{3.(-1)^2}{2.4} = \frac{3}{8}.$$

Agora vamos calcular d da equação tal que temos que

$$d = 4 - \left(\frac{3}{8}\right).(-1) = \frac{35}{8}$$

Portanto da equação da reta tangente a C no ponto P é $y = \frac{3}{8}.x + \frac{35}{8}$.

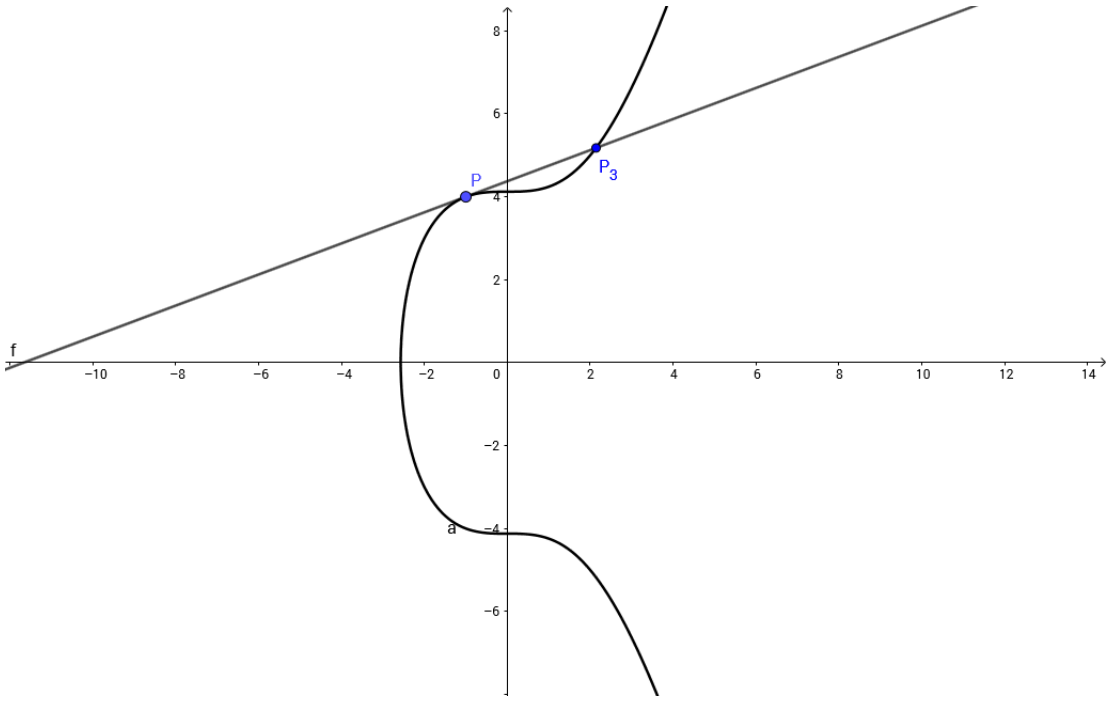


Figura 4.8: Reta tangente a curva C no ponto P

Agora determinaremos o outro ponto de intersecção da reta tangente com a curva C no $P_3 = (x_3, y_3)$. Primeiro vamos calcular x_3. Temos que na curva C os valores de $a = 0$ e $b = 17$ substituindo na equação 3.6 encontramos:

$$x_3 = \frac{(-1)^4 - 2.0.(-1)^2 - 8.(-1).17 + 0^2}{4(-1)^3 + 4.0.(-1) + 4.(17)} = \frac{137}{64}.$$

Em posse de x_3, vamos determinar o valor de y_3

$$y_3 = \frac{3}{8}.x_3 + \frac{35}{8}.$$

Logo

$$y_3 = \frac{3}{8}.\frac{137}{64} + \frac{35}{8} = \frac{2651}{512}.$$

Agora com x_3 e y_3 é fácil determinar o valor de $2.P$ como sendo $(x_3, -y_3)$ logo:

$$2.P = \left(\frac{137}{64}, -\frac{2651}{512}\right).$$

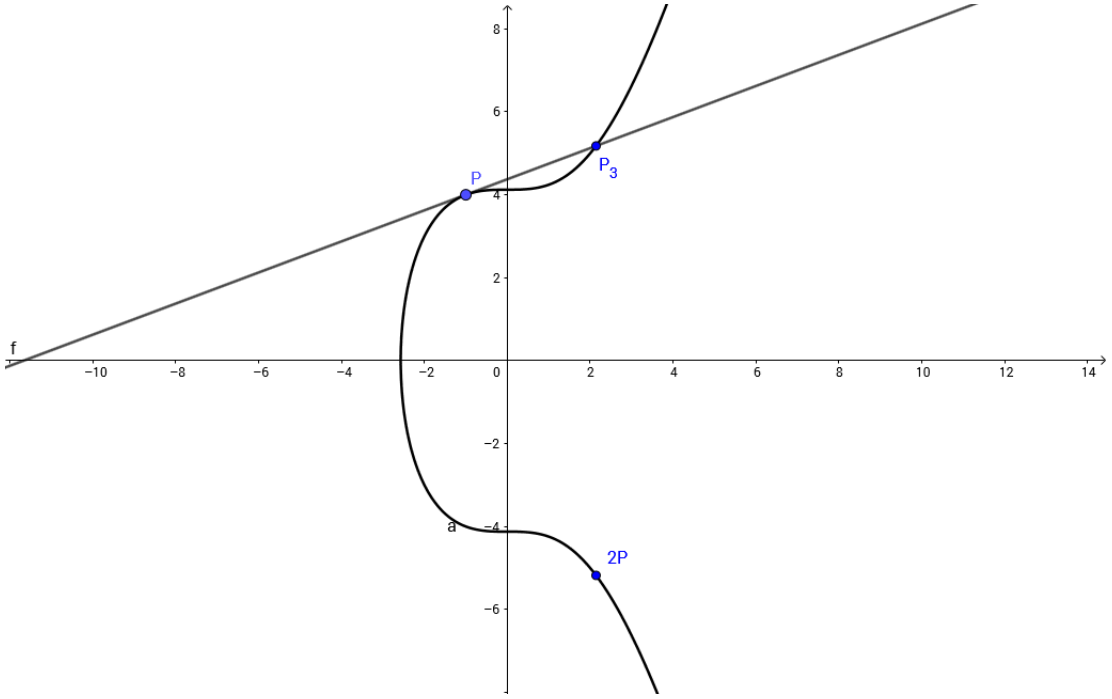


Figura 4.9: Ponto $2P$

4.4 A curva de Fermat

[2] A curva de Fermat é a curva C dada por $U^3 + V^3 = 1$. Recebeu este nome porque sua forma homogênea é $U^3 + V^3 = W^3$, de onde se segue que o último Teorema de Fermat para exponente 3 equivale a que $C(\mathbb{Q}) = \{(0, 1, 1), (1, 0, 1), (1, -1, 0)\}$.

A curva de Fermat não tem pontos singulares, ou seja, as derivadas de sua equação homogênea não se anulam em nenhum ponto de C.

De fato,seja $f(U, V, W) = U^3 + V^3 - W^3$. Calculando as derivadas parciais temos:

$$f_U = 3U^2, \quad f_V = 3V^2, \quad \text{e} \quad f_W = 3W^2.$$

Logo podemos concluir que f_U, f_V, f_W não zeram em C.

Ela apresenta três pontos no infinito, $[1, -\omega i, 0]$, onde ω é uma raiz cúbica da unidade. Podemos considerar C como curva elíptica sobre $\mathbb{Q}$ tomando $O = [1, -1, 0]$.

Vejamos como encontrar a equação na forma de Weierstrass para a curva C.

[2]Exemplo extraído de (CASTILLO, 2016)

Vamos considerar a curva C dada por

$$U^3 + V^3 = a.W^3,$$

onde $a \in K/\{0\}$. Suponhamos que K um corpo perfeito e que não tenha característica 3, para maiores informações sobre isso verificar (HERSTEIN, 2006).

Vemos que C também é uma curva elíptica com $O = \{1, -1, 0\}$. Se K contém uma raiz cubica então C é isomórfica sobre K a curva de Fermat (basta fazer $W' = \sqrt[3]{a}W$). Em geral, C é isomorfa sobre $\overline{K}$, com $\overline{K}$ sendo fecho algébrico de K, a curva de curva de Fermat, mas não necessariamente sobre K.

Agora vamos determinar a reta tangente a C. Como as derivadas no ponto O são

$$f_U(O) = 3, \quad f_V(O) = 3 \quad \text{e} \quad f_W(O) = 0.$$

e a equação da reta tangente é

$$f_U(O)(U - 1) + f_V(O)(V + 1) + f_W(O)(W - 0) = 0.$$

Substituindo temos que:

$$3.(U - 1) + 3(V + 1) + 0(W - 0) = 0.$$

Então $U + V = 0$.

Portanto a reta tangente a C no ponto O é a reta $U + V = 0$. Logo buscamos a transformação projetiva $[U, V, W] \mapsto [X, Y, Z]$ com correspondência entre O e $(0, 1, 0)$ e que as retas $U + V = 0$ e $Z = 0$. Para garantirmos a condição que as retas $U + V = 0$ e $Z = 0$ basta fazermos $Z = U + V$ e para garantir a correspondência entre O e $(0, 1, 0)$ basta que façamos $X = W$. Assim

$$(X, Y, Z) = (W, V - U, V + U).$$

e a inversa é

$$(U, V, W) = \left(\frac{Z - Y}{2}, \frac{Z + Y}{2}, X\right).$$

Vamos substituir os valores em $U^3 + V^3 = aW^3$. Logo,

$$\left(\frac{Z-Y}{2}\right)^3 + \left(\frac{Z+Y}{2}\right)^3 = aX^3.$$

Logo,

$$(Z-Y)^3 + (Z+Y)^3 = a8X^3.$$

Desenvolvendo os cubos temos que:

$$Z^3 - 3Z^2Y + 3ZY^2 - Y^3 + Z^3 + 3Z^2Y + 3ZY^2 + Y^3 = a8X^3.$$

Logo

$$2Z^3 + 6ZY^2 = a8X^3.$$

Portanto,

$$Z^3 + 3ZY^2 = 4aX^3.$$

Fazendo $Z = 1$ obtemos que

$$1 + 3Y^2 = 4.a.X^3.$$

Assim a equação se transforma em

$$3Y^2 = 4.a.X^3 - 1.$$

Para ficar na forma de Weierstrass temos que multiplicar $2^4.3^3.a^2$, assim

$$3Y^2.2^4.3^3.a^2 = 4.a.X^3.2^4.3^3.a^2 - 2^4.3^3.a^2,$$

Logo

$$Y^2.4^2.9^2.a^2 = X^3.4^3.3^3.a^3 - 2^4.3^3.a^2.$$

Reorganizando fica

$$(4.9.a.Y)^2 = (4.3.a.X)^3 - 16.27.a^2.$$

Trocando $X' = 12.a.X$ e $Y' = 4.9.a.Y$ obtemos a equação

$$(Y')^2 = (X')^3 - 432a^2.$$

As componentes da transformação que construímos é isomórfica as curvas dadas por pelo isormofismo:

$$U = \frac{36a - Y}{6X} \qquad e \qquad V = \frac{36a + Y}{6X}.$$

Pois se substituindo as componentes da transformação temos em $a = U^3 + Y^3$ obtemos que

$$a = \left(\frac{36a - Y}{6X}\right)^3 + \left(\frac{36a + Y}{6X}\right)^3$$

Assim

$$a = \frac{(36a - Y)^3 + (36a + Y)^3}{(6X)^3}.$$

Logo

$$6^3.X^3.a = (36a - Y)^3 + (36a + Y)^3.$$

Portanto

$$6^3.X^3.a = 36^3.a^3 - 3.36^2.a^2.Y + 3.36.a.Y^2 - Y^3 + 36^3.a^3 + 3.36^2.a^2.Y + 3.36.a.Y^2 + Y^3.$$

Então

$$6^3.X^3.a = 2.6^6.a^3 + 6^3.a.Y^2.$$

Logo,

$$X^3 = 2.6^3.a^2 + Y^2.$$

Reescrevendo temos que

$$Y^2 = X^3 - 432a^2.$$

Em um caso particular, a curva de Fermat é isomórfica (sobre $\mathbb{Q}$) a curva dada por $y^2 = x^3 - 432$ e seus pontos triviais são $(12, 36)$, $(12, -36)$ e O.

Referências Bibliográficas

BOLDRINI, J. L. et al. *Álgebra linear*. [S.l.]: Harper & Row, 1980.

CARNEIRO, J. S. *Uma introdução às curvas elípticas com aplicações para o ensino médio*. Tese (Doutorado) — Dissertação-Mestrado Profissional em Matemática. Universidade Estadual de Feira de Santana, Feira de Santana, 2014.

CASTILLO, C. I. Curvas elípticas. *Acessado no site https://www.uv.es/ivorra/Libros/Elipticas.pdf em outubro de 2017.*, 2016.

HEFEZ, A. *Curso de álgebra*. [S.l.]: Impa, 2013.

HERSTEIN, I. N. *Topics in algebra*. [S.l.]: John Wiley & Sons, 2006.

LIMA, E. L. *Algebra Linear*. 8a edição. ed. [S.l.]: IMPA, Rio de Janeiro, 2012.

MANASSAH, J. T. *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction*. 1. ed. [S.l.]: Cambridge University Press, 1999. ISBN 9780849310805,0849310806.

MILNE, J. *Elliptic Curves*. [S.l.]: BookSurge Publishers, 2006. 238+viii p. ISBN 1-4196-5257-5.

NIVEN, I.; ZUCKERMAN, H. S.; MONTGOMERY, H. L. *An introduction to the theory of numbers*. [S.l.]: John Wiley & Sons, 2008.

SALEHYAN, P. *Introdução às Curvas Elípticas e Aplicações*. [S.l.]: Instituto de Matemática Pura e Aplicada, 2015.

SILVA, V. GL dos REIS e da. *Geometría analítica*. [S.l.]: LTC, 1985.

SILVERMAN, J. H.; TATE, J. T. *Rational points on elliptic curves*. [S.l.]: Springer, 1992. v. 9.

SOUZA, A. O. *Pontos Racionais em Curvas Elípticas. 2012. 62 p.* Tese (Doutorado) — Dissertação (Mestrado em Matemática). Faculdade de Matemática, Universidade Federal de Uberlândia, Uberlândia, 2012.

VAINSENCHER, I. *Introdução às curvas algébricas planas*. [S.l.]: Instituto de Matemática Pura e Aplicada, 1979.