UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Dissertação de Mestrado

UMA INTRODUÇÃO ÀS CURVAS ELÍPTICAS COM APLICAÇÕES PARA O ENSINO MÉDIO

Joilma Silva Carneiro

Orientador: Prof. Dr. Kisnney Emiliano de Almeida

Feira de Santana

Abril de 2014

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Departamento de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

UMA INTRODUÇÃO ÀS CURVAS ELÍPTICAS COM APLICAÇÕES PARA O ENSINO MÉDIO

Joilma Silva Carneiro

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT do Departamento de Ciências Exatas, UEFS, como requisito parcial para a obtenção do título de **Mestre**.

Orientador: Prof. Dr. Kisnney Emiliano de Almeida.

Feira de Santana

08 de Abril de 2014

Ficha Catalográfica – Biblioteca Central Julieta Carteado

Carneiro, Joilma Silva
C289i Uma introdução às curvas elípticas com aplicações para o ensino médio / Joilma Silva Carneiro. – Feira de Santana, 2014.
95 f. : il.

Orientador: Kisnney Emiliano de Almeida.

Mestrado (dissertação) – Universidade Estadual de Feira de Santana, Programa de Pós-Graduação em Matemática, 2014.

1. Matemática – Estudo e ensino. 2. Curvas elípticas. 3. Curvas algébricas. 4. Ensino médio. I. Almeida, Kisnney Emiliano de, orient. II. Universidade Estadual de Feira de Santana. III. Título.

CDU: 51.09

UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA
DEPARTAMENTO DE CIÊNCIAS EXATAS
Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

ATA DA SESSÃO PÚBLICA DE DEFESA DE DISSERTAÇÃO DA DISCENTE JOILMA SILVA CARNEIRO DO PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL DA UNIVERSIDADE ESTADUAL DE FEIRA DE SANTANA

Aos oito dias do mês de abril de dois mil e quatorze às 13:30 horas na Sala MT67, Módulo 6, UEFS , ocorreu a Sessão pública de defesa de dissertação apresentada sob o título **"Uma introdução às curvas elípticas com aplicações para o ensino médio"**, da discente **Joilma Silva Carneiro** , do Mestrado Profissional em Matemática em Rede Nacional - PROFMAT da Universidade Estadual de Feira de Santana, para obtenção do título de MESTRE. A Banca Examinadora foi composta pelos professores: Kisnney Emiliano de Almeida (Orientador, UEFS), Sérgio Mota Alves (UESC) e Maurício de Araujo Ferreira (UEFS). A sessão de defesa constou da apresentação do trabalho pela discente e das arguições dos examinadores.
Em seguida, a Banca Examinadora se reuniu em sessão secreta para julgamento final do trabalho e atribuiu o conceito: aprovado.
Sem mais a tratar, foi lavrada a presente ata, que segue assinada pelos membros da Banca Examinadora e pelo Coordenador Acadêmico Institucional do PROFMAT. Feira de Santana, 08 de abril de 2014.

Prof. Dr. Kisnney Emiliano de Almeida (UEFS)
Orientador

Prof. Dr. Sérgio Mota Alves (UESC)

Prof. Dr. Maurício de Araujo Ferreira (UEFS)

Visto do Coordenador:

Prof. Dr. Maurício de Araujo Ferreira
Coordenador do PROFMAT / UEFS

Agradecimentos

Escrever uma dissertação de Mestrado é uma experiência enriquecedora e de plena superação. A cada tentativa, nos modificamos, ao buscar respostas para nossas aflições de "pesquisador". Para aqueles que compartilham conosco desse momento, parece uma tarefa interminável e enigmática que só se torna realizável graças a muitas pessoas que participam, direta ou indiretamente, mesmo sem saber realmente o que e para que nos envolvemos nessa tarefa. Portanto, são para essas pessoas meus agradecimentos:

Primeiramente, a Deus, que permitiu que tudo acontecesse ao longo de minha vida e que é o maior de todos os mestres.

Aos meus pais, meu infinito agradecimento. Sempre acreditaram em minha capacidade e isto sempre me fortaleceu e me fez tentar fazer o melhor de mim. Muito obrigada pelo amor incondicional!

Obrigada aos meus familiares que, nos momentos da minha ausência dedicados aos estudos, sempre fizeram entender que o futuro é feito a partir da constante dedicação e determinação no presente.

Ao meu marido, Ildivan Cordeiro, companheiro, amigo e amor, que soube compreender minha opção pelos estudos desde de graduação e, como ninguém, sempre esteve disponível para me apoiar nos momentos difíceis e comemorar os momentos bons a cada etapa vencida, com sua importante frase: "é isso aí Ilma, você vai conseguir".

À minha pequena filha e grande tesouro da minha vida, Yasmim Carneiro da Silva, que soube entender com seu jeitinho e respeitar minha ausência em tantos momentos, mas sempre me incentivando: "Mamãe, tu tem que tirar dez".

À minha funcionária do lar, Nilzete Alves, pelo suporte nos afazeres domésticos e cuidados tão especiais à minha filha.

A todos os funcionários da Realeza, pelas palavras de incentivo, principalmente pré e pós

avaliações.

A todos os colegas e professores do Mestrado Profissional em Matemática pela amizade e excelente ambiente de estudo, resoluções de questões, troca e discursão de opiniões, em especial aos colegas Tenivam e Rosipléia e à colega de departamento, professora e amiga Fabíola. Valeu mesmo! A aprendizagem foi significativa.

À minha amiga Anatália, amiga de longas datas, uma das minhas inspirações na opção pelo magistério e que, neste curso, foi uma amiga sempre presente em todos os momentos, inclusive finais de semana e feriados. Nossa dedicação fez a diferença.

À Uefs, especialmente aos colegas de departamento e área que me incentivaram e permitiram a liberação para o mestrado.

Finalmente, ao professor Kisnney Emiliano de Almeida, pela disponibilidade manisfestada para orientar este trabalho, pela precisa ajuda na definição do objeto de estudo, pela exigência de método e rigor, pela atenciosa revisão crítica do texto, pelos profícuos comentários e indicações de algumas referêcias bibliográficas relevantes para a temática em análise. Professor Kisnney, obrigada por ter aceitado a orientação da minha dissertação e espero retribuir, com seriedade, a confiança em mim depositada.

Resumo

Este trabalho tem o objetivo de apresentar um material introdutório sobre as Curvas Elípticas e algumas aplicações para o Ensino Médio. Curvas elípticas são curvas planas de grau 3 que podem ser equipadas com uma operação de grupo abeliano, definida geometricamente. Por meio de uma abordagem simples, iniciamos com definições, propriedades, exemplos e gráficos de curvas algébricas planas, analisando a interseção entre duas curvas, para, em seguida, fazer um tratamento algébrico e geométrico dos pontos racionais pertencentes a uma curva elíptica, mostrando sua rica estrutura aritmética e algébrica. Ao final da dissertação, são propostas algumas atividades que podem ser aplicadas para alunos do Ensino Médio.

Palavras-chaves: curvas algébricas, ensino de matemática, curvas elípticas.

Abstract

This is a study on Elliptic Curves and its application in specific educacional context, namely, the High School. This work aims to present an introductory text on Elliptic Curves, as well as some of the theoretical currents that base them. Elliptic Curves are plane curves of degree 3 can be equipped with an operation of Abelian group defined geometrically. With a simple approach, we start the study with definitions, properties, examples and graphs of algebraic plane curves. Then, we analyze the intersection of two curves so that next we can make an algebraic and geometric treatment of rational points of an Elliptic Curve. Thus, we show its rich arithmetic and algebraic structure. At the end of the dissertation, we present some activities involving Elliptic Curves as a proposal to be developed with High School students.

Keywords: Algebraic Curves, teaching Mathematics, Elliptic Curves.

Sumário

Capítulo 1

Introdução

O estudo das curvas elípticas é uma área central de investigação em Teoria dos Números com aplicações em Criptografia e na rápida fatoração dos números inteiros. Além disso, as curvas elípticas desempenharam uma papel fundamental na demonstração do último Teorema de Fermat. Aqui, nos limitamos aos aspectos mais elementares da Teoria de Curvas Elípticas e aplicações para o Ensino Médio.

A Geometria Algébrica Clássica pode ser pensada como a junção entre a Geometria Projetiva e a Geometria Analítica, sendo a primeira um modelo bidimensional sem retas paralelas, *i.e.*, quaisquer duas retas se intersectam em um único ponto. Esse modelo projetivo é possível a partir do acréscimo de pontos no infinito. Trabalharemos com plano projetivo, *i.e.*, o plano cartesiano real usual adicionado de pontos no infinito. Enquanto na Geometria Analítica as curvas são representadas por equações polinomiais de duas variáveis, no modelo da Geometria Projetiva são usados polinômios homogêneos - ou seja, polinômios cujos monômios têm o mesmo grau - de três variáveis. Um resultado essencial para a geometria algébrica, que discutimos brevemente em nosso trabalho, é o célebre Teorema de Bezout, que essencialmente diz que o número de pontos de intersecção entre duas curvas (projetivas) é igual ao produto de seus graus, desde que consideradas multiplicidades e pontos no infinito.

Em nosso trabalho, 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 $F \in [X, Y, Z]$, módulo a relação que identifica dois tais polinômios F, G, se um for múltiplo constante do outro. É sabido que toda curva elíptica que possui pelo menos um ponto racional 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 $\triangle = 4a^3 + 27b^2 \neq 0$.

A propriedade fundamental que motiva o estudo de curvas elípticas é o fato de seus pontos, quando pensados em pontos do espaço projetivo, formarem uma estrutura de grupo abeliano, que pode ser definida geometricamente de uma maneira intuitiva, que construimos durante este trabalho. Uma curva elíptica, definida dessa maneira, possui um único ponto no infinito ($(0 : 1 : 0)$), que é definido exatamente como o elemento neutro de sua estrutura de grupo.

O problema de calcular pontos 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 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 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.

Quanto à estrutura do trabalho, dividimos em cinco capítulos. No segundo capítulo, descreveremos de forma resumida tópicos de polinômios para em seguida estudar as curvas definidas por equações polinomiais, discutindo conceitos, proposições, exemplos e gráficos. A seguir, faremos uma rápida discussão de geometria projetiva, definindo pontos no infinito, plano projetivo, curvas projetivas e interseção entre duas curvas, com o objetivo de enunciarmos o Teorema de Bezout. Terminaremos este capítulo mostrando como encontrar pontos racionais de uma cônica. Foram utilizadas, neste capítulo, as referências [3], [5], [7], [12] e [17] como apoio nos tópicos de Teoria dos Números e Álgebra.

No terceiro capítulo, definiremos uma curva elíptica e, usando o teorema de Bezout, construiremos uma operação de grupo sobre o conjunto de pontos racionais de uma curva elíptica. Apresentaremos um tratamento geométrico e algébrico para estes pontos e verificaremos as principais propriedades desta curva. Durante toda a discussão deste capítulo, utilizaremos fi-

guras para que possamos visualizar as curvas, interseções e seus pontos que foram construídas em sua maioria usando o aplicativo Geogebra. Neste capítulo, foram utilizadas as referências bibliográficas [2], [4], [6], [10], [15] e [16] para estruturar o estudo de curvas elípticas.

No quarto capítulo, proporemos algumas atividades com resolução que podem ser aplicadas no ensino médio e estão relacionadas com a abordagem desenvolvida nesta dissertação. Iniciaremos as atividades com um exemplo prático, para, na sequência, explorar atividades com as operações entre os pontos racionais pertences a uma curva elíptica, seguindo um tratamento algébrico e geométrico. Terminaremos com uma atividade que é uma aplicação de curvas elípticas contextualizada com a geometria plana, geometria analítica e trigonometria.

No quinto capítulo, apresentaremos algumas propostas de trabalhos futuros para que possamos aprofundar contéudos deste trabalho, principalmente do segundo e terceiro capítulos.

Capítulo 2

Introdução às Curvas Algébricas Planas

Neste capítulo, destacaremos alguns resultados de polinômios para, em seguida, fazer um estudo de curvas algébricas planas e projetivas, explorando vários exemplos e seus respectivos traços. Estudaremos a interseção entre duas curvas para, finalmente, enunciar e verificar a aplicabilidade do relevante Teorema de Bezout.

Seguiremos as abordagens feitas por [5] , [7] , [17] , [15] e [12].

2.1 Polinômios

Nesta seção, iremos listar alguns resultados de polinômios que precisaremos para este trabalho, em especial utilizando as referências [5] e [7].

Seja A um anel. Um símbolo x não pertencente ao anel A será chamado de uma indeterminada sobre A.

Definição 2.1.1. Um polinômio $f(x)$ com coeficientes em A é uma expressão formal do tipo

$$f(x) = a_0 + a_1x + \ldots + a_nx^n = \sum_{j=0}^{n} a_jx^j,$$

onde $n \in \mathbb{N} \cup \{0\}$, $a_j \in A$, para $0 \leq j \leq n$.

Para $0 \leq j \leq n$, os elementos a_j são chamados de coeficientes do polinômio $f(x)$, as parcelas a_jx^j, de termos e os termos a_jx^j tais que $a_j \neq 0$, de monômios de grau j do polinômio $f(x)$. O coeficiente a_0 é chamado de termo constante. O conjunto de polinômios com coeficientes em A é denotado por $A[x]$ e é um anel com as operações entre polinômios definidas de maneira usual. Para mais detalhes sobre polinômios, *cf.* [7].

Definição 2.1.2. Seja A um anel e seja $f(x) := a_0 + a_1x + ... + a_nx^n \in A[x]$ com $a_n \neq 0$. O coeficiente a_n se chama o coeficiente líder de $f(x)$. Quando o coeficiente líder for igual a 1, o polinômio é dito *mônico*.

Sejam A um anel e $A[x_1]$ o anel de polinômios com coeficientes em A na indeterminada x_1. Se x_2 é uma indeterminada sobre o anel $A[x_1]$, definimos

$$A[x_1, x_2] := (A[x_1])[x_2]$$

Procedendo indutivamente, definimos o anel de polinômios em n indeterminadas

$$A[x_1, x_2, ..., x_n] := (A[x_1, x_2, ..., x_{n-1}])[x_n].$$

O polinômio em n indeterminadas $f(x_1, ..., x_n) \in A[x_1, x_2, ..., x_n]$ pode ser escrito como

$$f(x_1, ..., x_n) = \sum_{0 \leq j_1 \leq s_1} a_{j_1,...j_n} x_1^{j_1} \dots x_n^{j_n}, \text{ onde } s_1 \dots s_n \in \mathbb{N} \cup \{0\}$$

e $a_{j_1,...j_n} \in A$.

Cada termo do tipo $a_{j_1,...j_n} x_1^{j_1} \dots x_n^{j_n}$ é chamado de *monômio* e seu grau é definido como $j_1 + \dots + j_n$, sempre que $a_{j_1,...j_n} \neq 0$.

Definimos o grau de um polinômio não nulo em n indeterminadas com coeficientes em A como sendo o maior dos graus dos seus monômios não nulos.

Seja f um polinômio, denotaremos por $\delta(f)$ o grau do polinômio.

O exemplo abaixo, de [7], ilustra.

Exemplo 2.1.3. São polinômios em $\mathbb{Q}[x_1, x_2, x_3]$

$f(x_1, x_2, x_3) = x_1x_2 - \frac{1}{4}x_1x_3 + x_2^2 - x_1^2$,

$h(x_1, x_2, x_3) = 2 + x_1x_3 - \frac{3}{4}x_1x_2x_3 + 4x_2^3 - 3x_1x_3x_2^3 + x_2^5 + \frac{1}{2}x_2^3x_3^3$.

Temos que $\delta(f) = 2$ e $\delta(h) = 6$.

Um polinômio não nulo é chamado *homogêneo* de grau d se todos os seus monômios não nulos têm grau d.

Em um polinômio não nulo em n indeterminadas, a soma dos seus monômios não nulos de grau d é um polinômio *homogêneo*, chamado de *componente homogênea* de grau d. Todo polinômio não nulo é a soma das suas *componentes homogêneas*.

No exemplo 2.1.3, $f(x_1, x_2, x_3)$ é um polinômio de grau 2 e as componentes homogêneas de $h(x_1, x_2, x_3)$ são:

componente homogênea de grau 0: 2;

componente homogênea de grau 2: x_1x_3

componente homogênea de grau 3:$-\frac{3}{4}x_1x_2x_3 + 4x_2^3$

componente homogênea de grau 5: $-3x_1x_3x_2^3 + x_2^5$

componente homogênea de grau 6: $\frac{1}{2}x_2^3x_3^3$

Proposição 2.1.4. *Sejam A um anel, $f(x) \neq 0 \in A[x]$ e $\alpha \in A$. Então $f(\alpha) = 0$ se e somente se existe um polinômio $t(x) \in A[x]$ tal que $f(x) = (x - \alpha)t(x)$.*

Demonstração. cf. [5](p. 63). □

Definição 2.1.5. Sejam A um anel, $f(x) \in A[x]$ e $\alpha \in A$, e um inteiro $n \geq 1$. Dizemos que α é uma *raiz* de $f(x)$ de multiplicidade n se $(x - \alpha)^n$ divide $f(x)$ mas $(x - \alpha)^{n+1}$ não divide $f(x)$.

Exemplo 2.1.6. Seja o polinômio $f(x) = x^3 - 4x^2 + 5x - 2$ em $\mathbb{R}[x]$, $\alpha = 1$ é raiz de $f(x)$ com multiplicidade 2, pois $f(x) = (x - 1)^2 \cdot (x - 2)$.

Exemplo 2.1.7. Seja o polinômio $f(x) = x^4 - 7x^3 + 15x^2 - 13x + 4$ $\mathbb{R}[x]$, $\alpha = 1$ é raiz de $f(x)$ com multiplicidade 3, pois $(x - 1)^3 \cdot (x - 4)$.

Proposição 2.1.8. *Seja A um domínio de integridade e seja $f(x)$ em $A[x]\backslash\{0\}$. Se $f(x)$ tem grau n, então f(x) tem, no máximo, n raízes em A.*

Demonstração. cf. [7](p. 130). □

Teorema 2.1.9 (Teorema Fundamental da Álgebra)**.** *Todo polinômio não constante com coeficientes complexos tem uma raiz complexa.*

Demonstração. cf. [7]. □

Definição 2.1.10. Dizemos que um corpo $\mathbb{K}$ é *algebricamente fechado* quando todo polinômio não constante com coeficientes em $\mathbb{K}$ tem uma raiz em $\mathbb{K}$. Portanto, o *Teorema Fundamental da Álgebra* nos diz que $\mathbb{C}$ é algebricamente fechado.

Proposição 2.1.11. *Sejam $\mathbb{K}$ um corpo algebricamente fechado e $f(x)$ em $\mathbb{K}[x]$, com $\delta(f(x)) = n \geq 1$. Então, existem $\beta_1, \ldots \beta_n \in \mathbb{K}$, não necessariamnete distintos, e $a \in \mathbb{K}\backslash\{0\}$ tais que*

$$f(x) = a(x - \beta_1) \ldots (x - \beta_n).$$

Demonstração. cf. [7]. □

Observação 2.1.12. A proposição 2.1.11 nos diz que, todo polinômio de grau $n \geq 1$ tem exatamente n raízes, contadas com as multiplicidades.

Como consequência da Observação 2.1.12, podemos reenunciar o *Teorema Fundamental da Álgebra* da seguinte forma:

Teorema 2.1.13. *Todo polinômio $f(x)$ com coeficientes complexos e grau $n \geq 1$, se escreve de uma única maneira, a menos da ordem dos fatores, como*

$$f(x) = a(x - \beta_1)^{r_1} \dots (x - \beta_s)^{r_s},$$

onde $a \in \mathbb{C}\backslash\{0\}$ é o coeficiente líder de $f(x)$, $\beta_1 \dots \beta_s$ são números distintos e $r_1, \dots, r_s$ são inteiros positivos tais que $r_1 + \dots + r_s = n$.

Demonstração. cf. [7] (p. 133). □

Exemplo 2.1.14. O polinômio $x^2 - 2 \in \mathbb{Q}[x]$ não tem raízes em $\mathbb{Q}$. Entretanto, $x^2 - 2 \in \mathbb{R}[x]$ tem duas raízes reais, $\sqrt{2}$ e $-\sqrt{2}$. O polinômio $x^2 + 1 \in \mathbb{Q}[x] \subset \mathbb{R}[x]$ não tem raízes reais, mas tem duas raízes em $\mathbb{C}$, i e $-i$.

Definição 2.1.15. Seja A um domínio de integridade. Dizemos que o polinômio não constante $f(x)$ é irredutível em $A[x]$(ou irredutível sobre A) se é impossível expressar $f(x)$ com produto $g(x) \cdot h(x)$ de dois polinômios $g(x)$ e $h(x)$ em $A[x]$ cujos graus são ambos maiores ou iguais a um.

Salientamos que utilizamos "irredutível sobre A", e não simplesmente "irredutível", pois não faz sentido dizer que um dado polinômio $f(x)$ é irredutível simplesmente. Para justificar isto, seja o polinômio $f(x) = x^2+1$ é irredutível sobre $\mathbb{R}$, mas não sobre $\mathbb{C}$, pois $x^2+1 = (x+i)(x-i)$.

Quando um polinômio não é irredutível, chamamos de redutível sobre A.

Portanto, um polinômio $f(x)$ é redutível sobre A se, e somente se, existem polinômios $g(x)$ e $h(x)$ em $A[x]$ tais que $f(x) = g(x) \cdot h(x)$, com $0 < \delta(g(x)) < \delta(f(x))$ e $0 < \delta(h(x)) < \delta(f(x))$.

Exemplo 2.1.16. Seja K um corpo qualquer. O polinômio $ax + b$, onde a, $b \in K$ e $a \neq 0$, é irredutível em K.

De fato, escrevendo $ax + b = f(x) \cdot g(x)$, com $f(x)$, $g(x) \in K[x]$ temos que ambos os fatores são não nulos e

$$1 = \delta(ax + b) = \delta(f(x)) + \delta(g(x)).$$

Logo, $\delta(f(x)) = 0$ e $\delta((g(x)) = 1$, ou $\delta(f(x)) = 1$ e $\delta(g(x)) = 0$. Então, $f(x)$ ou $g(x)$ é um polinômio constante não nulo.

Em particular, o polinômio mônico $x - \beta$, com $\beta \in F$, é irredutível em $K[x]$.

Exemplo 2.1.17. $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ em $\mathbb{R}[x]$, então $x^2 - 2$ não é irredutível em $\mathbb{R}[x]$. Entretanto, $x^2 - 2$ é irredutível em $\mathbb{Q}[x]$, pois tem grau 2 e não tem raiz em $\mathbb{Q}$.

Teorema 2.1.18. *Todo polinômio de grau maior ou igual a 1 em $K[x]$ pode ser fatorado em $K[x]$ como produto de polinômios irredutíveis. Esta fatoração é unica, a menos de ordem dos fatores e da multiplicação por constantes não nulas de K.*

Demonstração. cf. [7](p. 133). □

Definição 2.1.19. Os fatores irredutíveis de um polinômio dado são os polinômios irredutíveis que dividem o polinômio.

Os fatores irredutíveis tem um papel análogo ao de números primos.

Proposição 2.1.20. *Sejam f, g polinômios de duas variáveis com coeficientes em $\mathbb{R}$. Então $f(x,y) = 0$ e $g(x,y) = 0$ têm as mesmas soluções em $\mathbb{R}^2$ se e somente se os fatores irredutíveis são os mesmos.*

Demonstração. cf. [17](p.9). □

Exemplo 2.1.21. Os polinômios

$$f(x,y) = x^2 - y^2 = (x-y)(x+y), \quad g(x,y) = x^3 - xy^2 + x^2y - y^3 = (x-y)(x+y)^2$$

têm os mesmos fatores irredutíveis.

Exemplo 2.1.22. Os polinômios, $f(x,y) = x^2 - y^2 - 1$ e $g(x,y) = y^2 - x^3 + 16$ não têm os mesmos fatores irredutíveis. Para verificar este fato, observemos que as raízes do primeiro polinômio formam uma círcunferência em $\mathbb{R}^2$ e o segundo tem o seguinte traço:

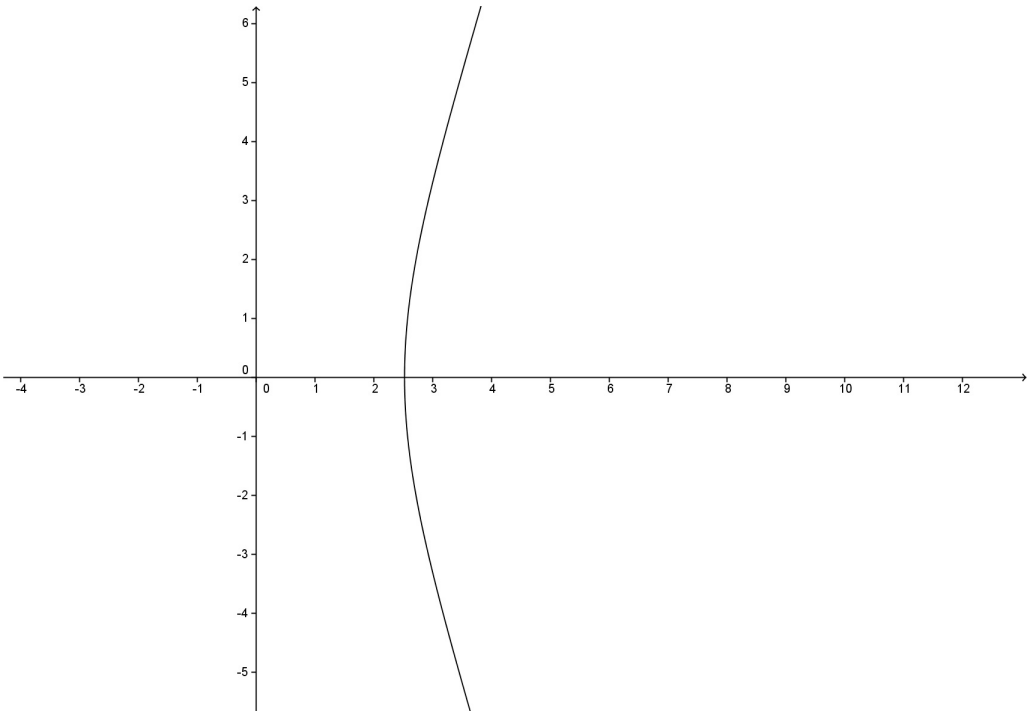


Figura 2.1: Traço

Definição 2.1.23. Dizemos que dois polinômios $f, g \in K[x, y]$ são equivalentes se satisfazem as condições da Proposição 2.1.20, ou seja, se possuem os mesmos fatores irredutíveis.

A relação acima é uma *relação de equivalência*. Sejam f, g e h polinômios que possuem os mesmos fatores irredutíveis, temos:

- f é equivalente a f (Reflexividade);
- Se f é equivalente a g, então g é equivalente a f. (Simetria);
- Se f é equivalente a g e g é equivalente a h, então f é equivalente h (Transitividade).

2.2 Curvas Algébricas

Seria intuitivo definir uma curva algébrica plana como o lugar dos pontos do plano $\mathbb{R}^2$ cujas coordenadas cartesianas satisfazem uma equação do tipo

$$f(x, y) = 0,$$

onde f é um polinômio com coeficientes reais, não constante.

Exemplo 2.2.1. Círculo:

$$f = x^2 + y^2 - 1.$$

Círculo centrado em (0,0) e raio 1.

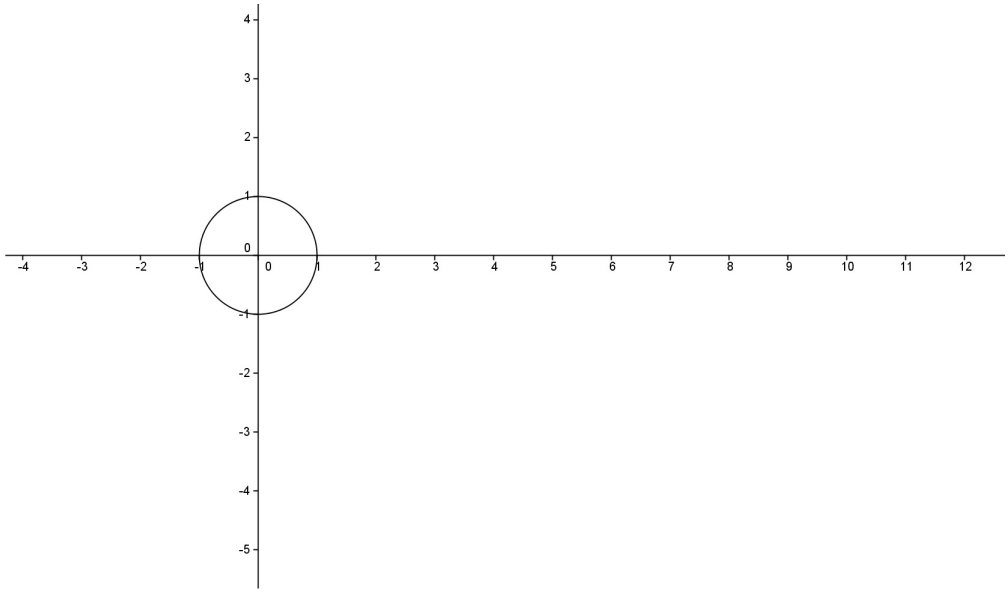


Figura 2.2: Círculo centrado em (0,0) e raio 1.

Exemplo 2.2.2. Parábola:

$$f = y - x^2.$$

Parábola de centro na origem e eixo focal em Oy.

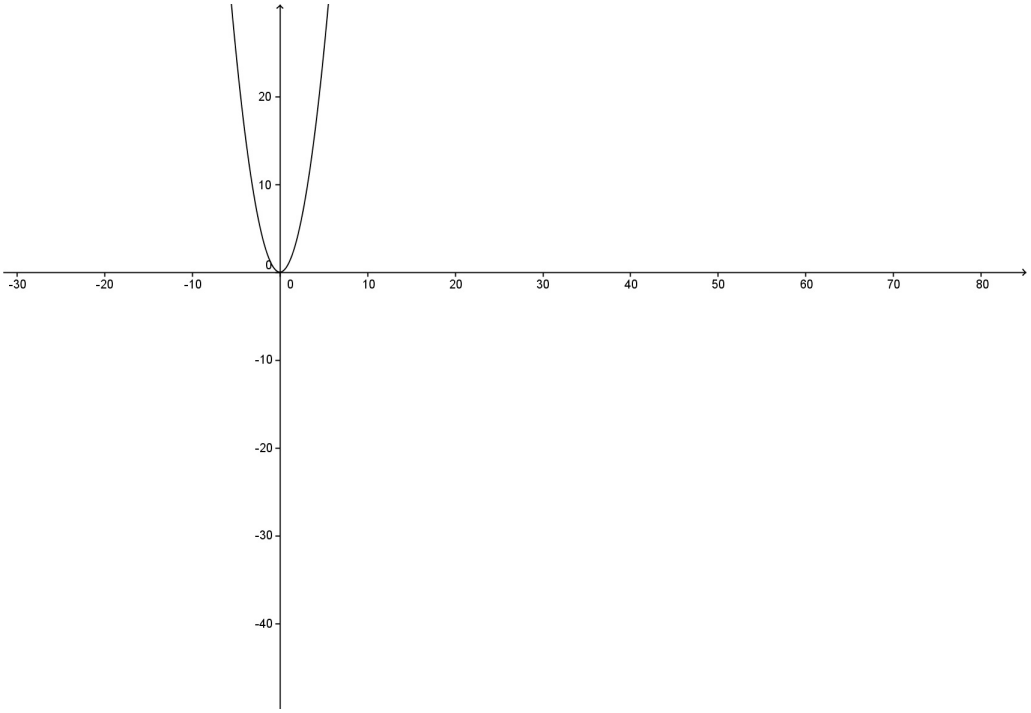


Figura 2.3: Parábola de centro na origem.

Exemplo 2.2.3. Elipse:

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

Elipse de centro em (0,0), eixo maior em Ox e eixo menor em Oy. Esta elipse possui semieixo maior igual a 2, semieixo menor igual a 1 e distância focal igual a $\sqrt{3}$.

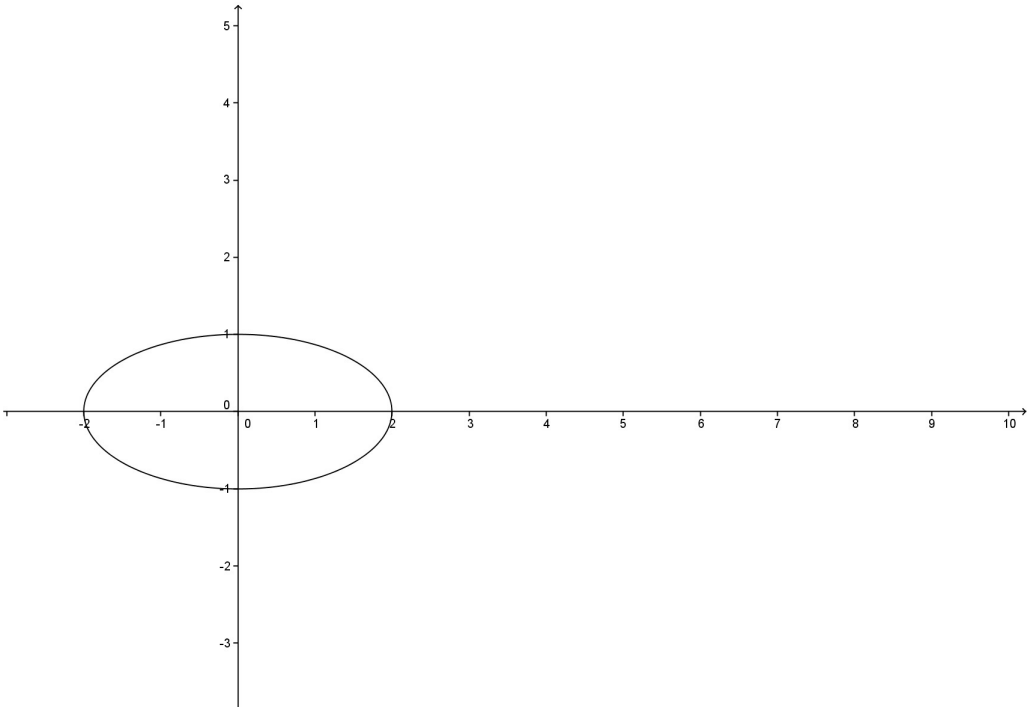


Figura 2.4: Elípse de centro na origem

Exemplo 2.2.4. A curva algébrica definida por

$$f = x^2 + y^2 + 1$$

é também uma curva degenerada e não possui nenhum ponto em $\mathbb{R}^2$.

Exemplo 2.2.5. A curva dada pela equação

$$f = y^2 - x^3 + x$$

possui o seguinte traço:

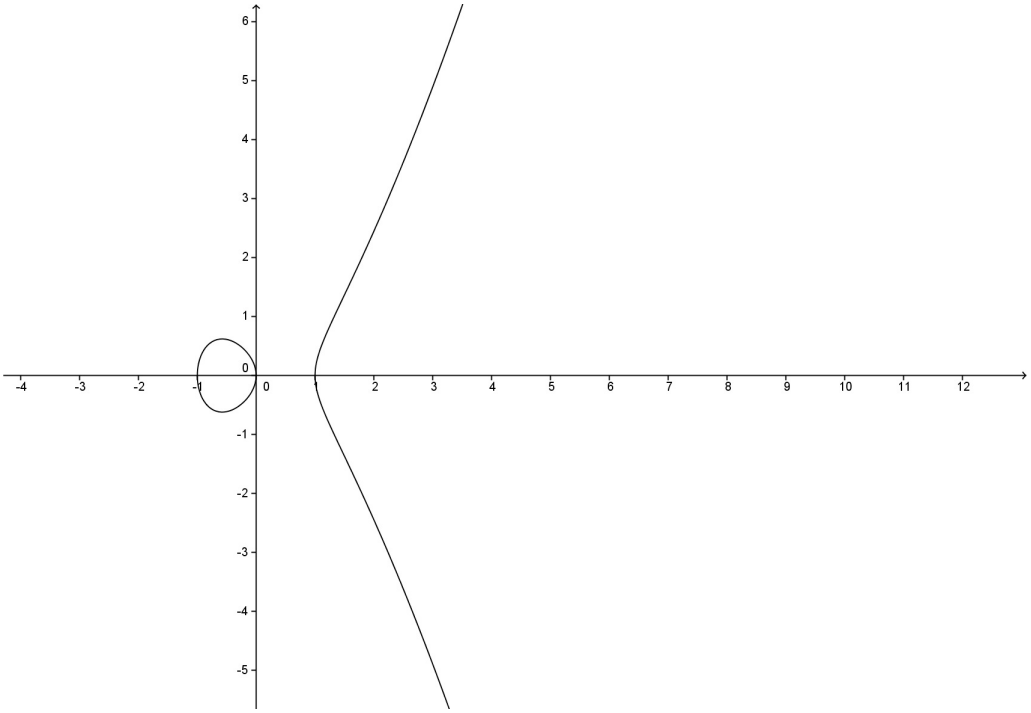


Figura 2.5: Equação de uma curva algébrica

Esta curva é um exemplo do que chamaremos de *curva elíptica*.

Exemplo 2.2.6. A curva definida por

$$f = x^2 + y^2$$

é uma curva degenerada, formada apenas pelo ponto $(0, 0)$.

Observação 2.2.7. A partir do exemplo anterior, nota-se que dois polinômios distintos podem ter as mesmas raízes. Por exemplo,

$$f = x^2 + y^2 \quad \text{e} \quad f = 2x^2 + y^2$$

definiriam a mesma curva degenerada.

Da mesma forma, os polinômios

$$f(x, y) = \frac{x^2}{4} - \frac{y^2}{2} - 1 \quad \text{e} \quad g(x, y) = x^2 - 2y^2 - 2.$$

também representariam a mesma curva. Como queremos diferenciar essas duas curvas, usaremos uma definição ligeiramente diferente da proposta no início da seção.

Definição 2.2.8. Dois polinômios de K, com K corpo, são ditos associados se $p(x) = \alpha q(x)$, para algum $\alpha \in K - \{0\}$.

Observe-se que a relação "$p(x)$ é associado a $q(x)$" é uma relação de equivalência.

Definição 2.2.9. Seja K um corpo. Uma *curva algébrica plana afim* sobre K(ou, mais abreviadamente, *curva*) é uma classe de equivalência de polinômios não constantes $f \in K[x, y]$ módulo a relação de equivalência da Definição 2.2.8. A *equação* de uma curva é qualquer um dos polinômios nessa classe. Uma curva é dita *irredutível* se admite uma equação que é um polinômio irredutível. Dizemos que uma curva está definida sobre o corpo K_0, subcorpo de K, se ela admitir uma equação com coeficientes em K_0. Usaremos apenas os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$.

Definição 2.2.10. Dizemos que o traço real de uma curva é o conjunto das soluções reais de qualquer uma de suas equações.

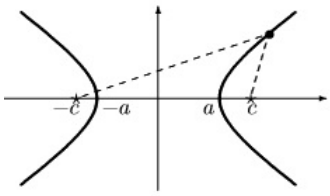
Dessa forma, as curvas da Observação 2.2.7 são curvas diferentes com o mesmo traço real.

O grau de uma curva f é o grau de sua equação e será denotado por $\delta(f)$(note-se que todas as equações de uma dada curva têm o mesmo grau). Curvas de grau 1, 2, 3,... são chamadas retas, cônicas, cúbicas.

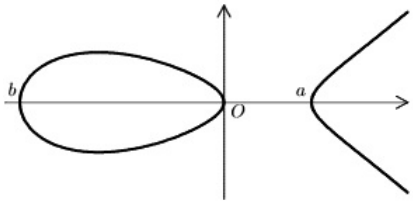
Definição 2.2.11. As componentes irredutíveis de uma curva f são as curvas definidas pelos fatores irredutíveis de f. A multiplicidade de uma componente p de f é o expoente com que o fator p ocorre na decomposição de f. Quando a multiplicidade de uma componente p é maior ou igual a 2, dizemos que p é componente múltipla de f.

Intuitivamente, as componentes irredutíveis de uma curva f são os "pedaços"que constituem f e que são também curvas. Precisamos ficar atentos para o fato de que uma curva pode ser irredutível mesmo sendo seu *traço real* formado por duas ou mais partes disjuntas. Confirmaremos este fato com os exemplos abaixo:

Exemplo 2.2.12. A hipérbole de equação $f = \frac{x^2}{a^2} - \frac{y^2}{b^2} - 1$ possui o seguinte traço:



Exemplo 2.2.13. A cúbica de equação: $y^2 = x(x - a)(x - b), (b < 0 < a)$, possui o seguinte traço:



A multiplicidade de uma componente p de f é o expoente com que o fator p ocorre na decomposição de f; quando ≥ 2, dizemos que p é componente múltipla de f.

2.3 Pontos no Infinito

Figura 2.6: Retas paralelas

Na Geometria Euclidiana, postula-se a existência de retas que não se intersectam. Isto ocorrendo, diz-se que elas são paralelas. Tal postulado contradiz a realidade que aprendemos visualmente.

Quando estamos numa longa estrada em linha reta, seus lados são assumidos paralelos. No entanto, a nossa intuição nos diz que elas concorrem num ponto de fuga. No ponto de fuga, as duas retas estão se intersectando.

Se existe uma outra estrada em linha reta, cruzando a primeira, ao olharmos na direção desta outra, veremos o mesmo fenômeno, mas agora o ponto de fuga é diferente.

Este fenômeno é comparável a uma fotografia ou por uma pintura, sugerindo que a Geometria Euclidiana é um modelo da realidade não tão próximo das nossas sensações quanto estamos acostumados a pensar.

Se acrescentarmos os pontos de fuga, isto é, se assumirmos que quaisquer duas retas se intersectam num único ponto, que tipo de espaço geométrico teremos? Um modelo de geometria bidimensional sem retas paralelas é chamado de Geometria Projetiva ou Geometria Elíptica Simples.

A Geometria Projetiva surgiu com a dificuldade que os artistas do Renascimento encontravam em dar aos quadros que pintavam uma forma real dos objetos, de modo que qualquer pessoa identificasse sem dificuldades o que estava longe e o que estava perto. Motivados pelo desafio, eles estudaram as leis que determinam a construção dessas projeções, criando a teoria fundamental da perspectiva geométrica, que depois foi expandida por um grupo de matemáticos franceses liderados por Gérard Desargues.

Gérard Desargues (1591-1661) foi arquiteto e engenheiro. Cem anos depois dos pintores renascentistas, o autor descobriu a perpectiva na matemática. Suas obras ficaram perdidas por cerca de 200 anos. Foi dele a ideia usual de acrecentar ao plano usual uma reta no infinito, constituindo um plano projetivo. Seu livro publicado em 1639 pretendia dar uma fundamentação

matemática aos métodos de perspectiva empregados pelos pintores e arquitetos. A concepção de Desargues do plano projetivo é, em essência, a que descreveremos a seguir.

2.3.1 O Plano Projetivo

Consideremos um plano afim mergulhado no espaço tridimensional como o plano π de equação $Z = 1$.

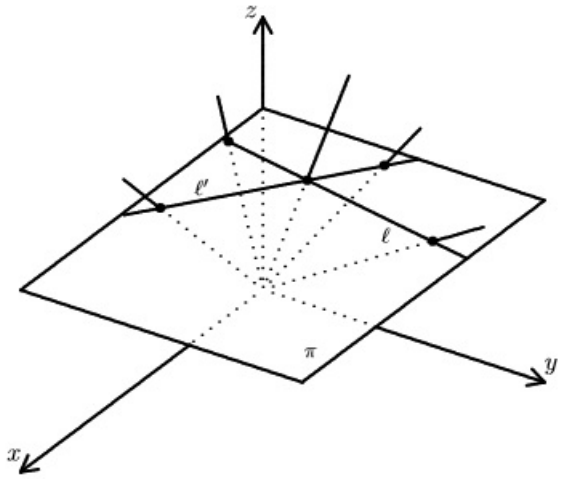


Figura 2.7: Plano Projetivo

Cada ponto do plano π determina uma reta passando pela origem e pelo dado ponto. Cada reta de π determina um plano passando pela origem. Se as retas l e l' que estão contidas em π se encontram, seu ponto de interseção dá lugar à reta de interseção dos dois planos associados a l, l'. Quando as retas l, l' estão contidas em π são paralelas, os planos que elas definem ainda se cruzam, desta feita ao longo de uma reta passando pela origem e contida no plano $Z = 0$.

Definição 2.3.1. O plano projetivo $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional passando pela origem.

O plano π se identifica com um subconjunto de $\mathbb{P}^2$ que ainda denotaremos por π. Os pontos de $\mathbb{P}^2 \backslash \pi$ são chamados de *pontos no infinito*.

Podemos dizer, assim, que o plano projetivo contém os pontos finitos e os pontos no infinito.

Iremos denotar 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, z são coordenadas homogênas do ponto (x, y, z) relativas à base canônica $\{(1, 0.0), (0, 1, 0), (0, 0, 1)\}$.

Por definição, temos que:

$(x : y : z) = (x' : y' : z')$ se, e somente se, existe constante $t \neq 0$ tal que $(x, y, z) = t(x', y', z')$.

Por exemplo, $(1 : 2 : 3) = (2 : 4 : 6)$ e $(1 : 0 : 0) = (t : 0 : 0)$, para qualquer $t \neq 0$.

Em geral, fixada uma base qualquer no espaço tridimensional, as coordenadas homogêneas do ponto $\neq 0$ relativas a essa base são chamadas homogêneas do ponto correspondente de $\mathbb{P}^2$. Coordenadas homogêneas de um ponto de $\mathbb{P}^2$(relativas a uma base prefixada) só estão bem definidas a menos de um fator escalar $\neq 0$.

O espaço $\mathbb{R}^2$ pode ser naturalmente identificado com o plano horizontal π: $z = 1$(paralelo ao plano xy) em $\mathbb{R}^3 \setminus (0,0,0)$. A identificação é simples:

$$\begin{aligned} \mathbb{R}^2 &\to \quad \pi \\ (x,y) &\mapsto (x,y,1). \end{aligned}$$

Agora, cada ponto $(x : y : 1) \in \pi \subset \mathbb{R}^3 \setminus (0,0,0)$ determina um único ponto em $\mathbb{P}^2$, qual seja, $(x : y : 1)$. Isso motiva a seguinte definição:

Definição 2.3.2. O conjunto

$$\mathbb{A}^2 := \{(x : y : 1) \in \mathbb{P}^2; (x,y,1) \in \mathbb{R}^3\}$$

é chamado de *plano euclidiano* ou *afim* e seus elementos de *pontos afins*. Dessa forma, *plano projetivo* se escreve como a união

$$\mathbb{P}^2 := \mathbb{A}^2 \cup \mathbb{P}^1,$$

onde os elementos de

$$\mathbb{P}^1 := \{(x : y : z) \in \mathbb{P}^2 \mid z = 0\}$$

são chamados de *pontos no infinito*.

2.3.2 Curvas Projetivas

Nesse capítulo, definiremos curvas projetivas planas, *i.e.*, curvas no plano projetivo. Para tanto, devemos destacar o fato de que um ponto no plano projetivo é uma classe de equivalência, logo possui vários representantes. Portanto, para a definição de uma curva plana projetiva ser consistente, é preciso que trabalhemos apenas com polinômios para os quais um representante de cada ponto do plano projetivo seja raiz se e somente se qualquer outro representante também o for. Tais polinômios são precisamente os *polinômios homogêneos*, conforme veremos a seguir.

Definição 2.3.3. Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes $F \in K[X,Y,Z]$, módulo a relação que identifica dois tais polinômios, F, G, se um for múltiplo constante do outro.

Note-se que a definição é consistente, pois, se F um polinômio homogêneo de grau d, a relação

$$F(tx,ty,tz) = t^d F(x,y,z)$$

mostra que a condição para que um ponto $(x : y : z)$ pertença ao traço de uma curva projetiva é independente das coordenadas homogêneas. Ainda, se F se anula em um ponto (x, y, z), ele se anula também em (tx, ty, tz).

Curvas de grau 1, 2 e 3 são, como antes, chamadas de *retas*, *cônicas* e *cúbicas*, respectivamente.

A reta $Z = 0$ é usualmente chamada de *reta no infinito*, em $\mathbb{P}^2$. Seu complemento $(Z \neq 0)$ é o plano $\mathbb{A}^2$, cujos pontos são ditos estarem a uma distância finita.

Definição 2.3.4. Seja $f = \sum_0^d f_i$, onde cada $f_i \in K[X, Y]$ é homogêneo de grau i, $f_d \neq 0$. A homogeneização de f é o polinômio de grau $d = g(f)$,

$$f^*(X, Y, Z) = \sum Z^{d-i} f_1(X, Y).$$

A curva projetiva definida pela homogeneização f^* é chamada de *fecho projetivo* da curva afim definida por f.

Definição 2.3.5. Seja $F \in K[X, Y, Z]$ um polinômio homogêneo não constante. As soluções da equação

$$F(X, Y, 1) = 0$$

são chamadas de *pontos a distância finita* da curva definida por F. O polinômio no primeiro membro desta equação é chamado de *desomogeneização* de F (com respeito à variável Z), denotado por $F*$. Note-se ainda que F_* é não constante, a menos que F seja igual a uma potência de Z.

No decorrer deste trabalho, identificaremos as curvas algébricas planas afins $f(x, y) = 0$ com os pontos a distância finita da curva projetiva $f^*(X, Y, Z) = 0$.

A partir do que construímos, vemos que existe uma correspondência natural entre curvas afins e curvas algébricas projetivas.

Proposição 2.3.6. *Seja K um corpo e $f \in K[X, Y]$ um polinômio. Então, a desomogeneização da homomogeneização de f é igual a f. Reciprocamente, se $F \in K[X, Y, Z]$ é um polinômio homogêneo, então a homogeneização da desomogeneização de F é igual a F.*

Exemplo 2.3.7. Quando nos referirmos à parábola $Y = X^2$, estaremos pensando na curva projetiva $ZY = X^2$.

Exemplo 2.3.8. Considere a curva plana afim $f(x, y) = y - x^2$. Homogeneizando a curva, obtemos $F(X, Y, Z) = ZY - X^2$, curva projetiva de grau 2. Desomogeneizando F, obtemos novamente f.

Exemplo 2.3.9. Considere a curva projetiva de grau 3

$$F(X, Y, Z) = X^3 - 3YZ^2 + XZ^2 - XYZ + 2Z^3.$$

Desomogeneizando F, obtemos:

$$f(x, y) = x^3 - 3y + x - xy + 2,$$

uma curva plana afim de grau 3. Homogeneizando f, obtemos novamente F.

Veremos alguns exemplos de como encontrar algebricamente os pontos no infinito de uma curva projetiva F, ou seja, os pontos de interseção da curva F com a reta projetiva $Z = 0$.

Exemplo 2.3.10. Considere a curva projetiva de grau 2

$$C : X^2 - Y^2 - Z^2 = 0.$$

Considerando $Z = 0$ em C temos,

$$(X + Y) \cdot (X - Y) = 0.$$

$$X = -Y.$$

ou

$$X = Y.$$

Assim, encontramos os pontos $(1 : 1 : 0)$ e $(1 : -1 : 0)$. Estes pontos correspondem respectivamente aos pontos no infinito $(1, 1)$ e $(1, -1)$ pertencentes a P^1 ou, equivalentemente, às direções $y = x$ e $y = -x$ em A^2. Fazendo a desomogeneização, a parte afim de C é a hipérbole:

$$x^2 - y^2 = 1.$$

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. 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 nos capítulos posteriores.

Proposição 2.3.11. *Toda reta afim é vertical se, e somente, passa pelo ponto no infinito* $(0 : 1 : 0)$.

Demonstração. Se a reta afim é vertical, temos

$$x = c \tag{2.3.1}$$

Escrevendo na forma projetiva:

$$X = cZ \tag{2.3.2}$$

Agora, para verificar que toda reta vertical passa pelo ponto no infinito , basta substituir $(0 : 1 : 0)$ na equação (2.3.13). Considerando a reta afim não vertical:

$$ax + by = c, b \neq 0 \tag{2.3.3}$$

Escrevendo-a (2.3.3) na forma projetiva:

$$aX + bY = cZ, b \neq 0 \tag{2.3.4}$$

Substituindo o ponto no infinito $(0 : 1 : 0)$ na equação (2.3.4) chegamos a uma contradição, encontrando $b = 0$. □

Exemplo 2.3.12. Considere a curva plana dada por

$$f(x, y) = y - x^2,$$

uma parábola. Vamos encontrar os pontos no infinito de f, ou seja, de sua curva projetiva correspondente. Inicialmente, vamos homogeneizar a curva, encontrando, assim, a curva projetiva de grau 2

$$F(X, Y, Z) = ZY - X^2.$$

Para determinar os pontos no infinito, tomamos $Z = 0$. Logo, temos $X^2 = 0$ e, desta forma, os pontos no infinito são:

$$\{(0, Y, 0) \,|\, Y \neq 0\} = (0 : 1 : 0).$$

Quando encontramos os pontos no infinito de curva, estamos encontrando a interseção da curva com a reta projetiva $Z = 0$. O grau 2 da última equação nos motiva a definir o conceito de multiplicidade a seguir.

A noção de multiplicidade é muito importante na Teoria de Curvas Algébricas. Historicamente, descende do simples fato de que todo polinômio de grau n com uma varíavel admite exatamente n raízes, contadas com as devidas multiplicidades, como foi visto no Teorema 2.1.13. Isto significa, intuitivamente, atribuir um peso que indica quantas raízes coincidem com o mesmo valor. Tal moção dá um sentido preciso à ideia de uma curva passar um certo número de vezes por um mesmo ponto.

Seja f uma curva e seja l uma reta de equação $Y = aX + b$. Os pontos de $f \cap l$ podem ser obtidos eliminando Y e resolvendo a equação

$$f_l(X) := f(X, aX + b) = 0.$$

Eis as possibilidades:

- (1)$f_l(X)$ é identicamente nulo, caso em que l é uma componente de f;
- (2)$f_l(X)$ é uma constante $\neq 0$, quando $f \cap l = \varnothing$
- (3)$f_l(X)$ é um polinômio não constante, decompondo-se na forma

$$f_l(X) = c\prod_{i=1}^{r}(X - x_i)^{m_i},$$

onde c é uma constante e os x_i são as abscissas(duas a duas distintas) dos pontos de interseção. Procede-se de maneira evidente quando l é da forma $X = cY + d$

Definição 2.3.13. *A multiplicidade ou índice de interseção* de l, f no ponto P é dada por

$$(l, f)_P = \begin{cases} 0 & \text{se } P \notin l \cap f \\ \infty & \text{se } P \in l \subset f \\ m_i & \text{se } P = (x_i, ax_i + b) \end{cases}$$

como no caso (3) acima. Se $l \subseteq f$, chamamos o inteiro

$$m_\infty : d^o f - \sum_{i=1}^{r} m_i$$

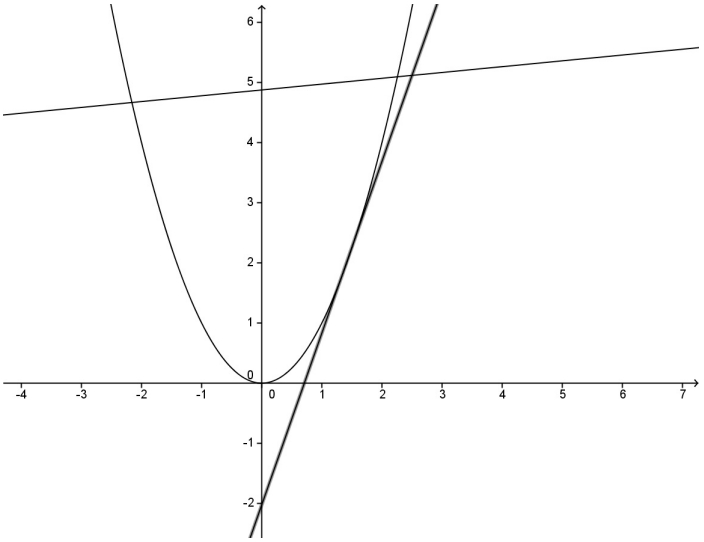
de multiplicidade de interseção de l, f no ponto impróprio ou ponto de l no infinito.

Exemplo 2.3.14. Sejam

$$f = Y - X^2$$

$$l = Y - (aX + b).$$

Se $a^2 + 4b \neq 0$, temos dois pontos de interseção distintos. Se $a^2 + 4b = 0$, temos um só, com multiplicidade 2.



2.3.3 Interseção entre Curvas Projetivas

Para calcular os pontos que estejam na interseção de uma curva C_1 com uma curva C_2, basta resolver o sistema de equações simultâneas(o que nem sempre é uma tarefa fácil).

Uma questão importante a ser analisada é: Quantos pontos de interseção há entre duas curvas? Veremos que a resposta para essa pergunta remete ao grau das curvas.

Analisaremos alguns exemplos com foco no grau das curvas. Primeiramente, citaremos exemplos com *curvas afins*.

Exemplo 2.3.15. Considere as curvas:

$$C_1 : x + y + 1 = 0 \tag{2.3.5}$$

$$C_2 : x^2 + y^2 = 1 \tag{2.3.6}$$

Quantos pontos tem $\#(C_1 \cap C_2)$?

Escrevendo a equação (2.3.5) $y = -x - 1$ e substituindo na equação (2.3.6), teremos uma equação em x, $x^2 + (-x - 1)^2 = 1$. Assim, temos $x = 0$ ou $x = -1$. Para cada valor de x, encontramos y e, consequentemente, os pares $(0, -1)$ e $(-1, 0)$ satisfazem ambas equações (2.3.5) e (2.3.6). Logo, $\#(C_1 \cap C_2) = 2$.

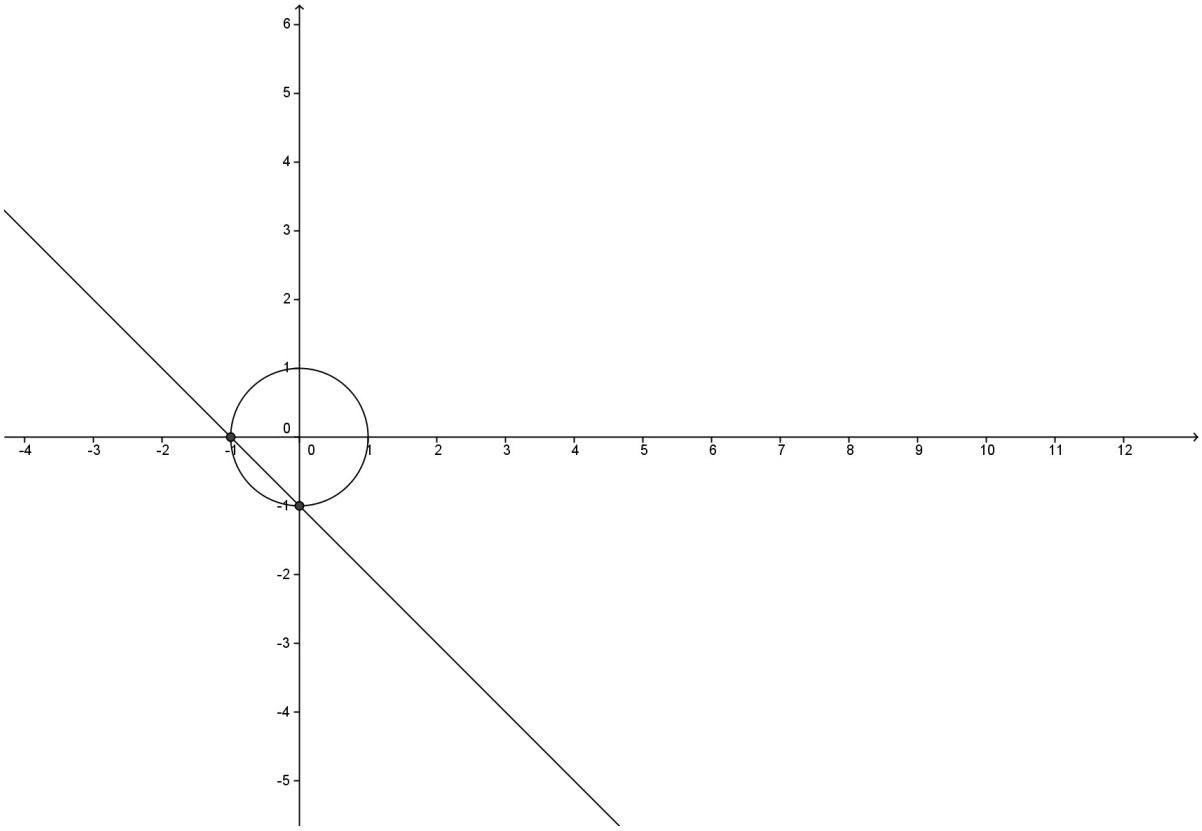


Figura 2.8: Interseção entre reta e curva

Exemplo 2.3.16. Considere as curvas afins

$$C_1 : x + y = 0 \quad \text{e} \quad C_2 : x^2 + y^2 = 1.$$

Quantos são os pontos de $C_1 \cap C_2$?

A primeira curva é a reta $y = -x$, ou melhor, o traço de C_1 é formado por pontos da forma $(x - x)$, com $x \in \mathbb{R}$. Se substituirmos $y = -x$ na equação $x^2 + y^2 = 1$, teremos: $x^2 + (-x)^2 = 1$. Assim, $x = \pm\frac{\sqrt{2}}{2}$. Substituindo esses valores na primeira equação, temos $y = \mp\frac{\sqrt{2}}{2}$.. Consequentemente , os pares $(\frac{\sqrt{2}}{2}, \frac{-\sqrt{2}}{2})$ e $(\frac{-\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$ satisfazem ambas equações. Logo, $\#(C_1 \cap C_2) = 2$.

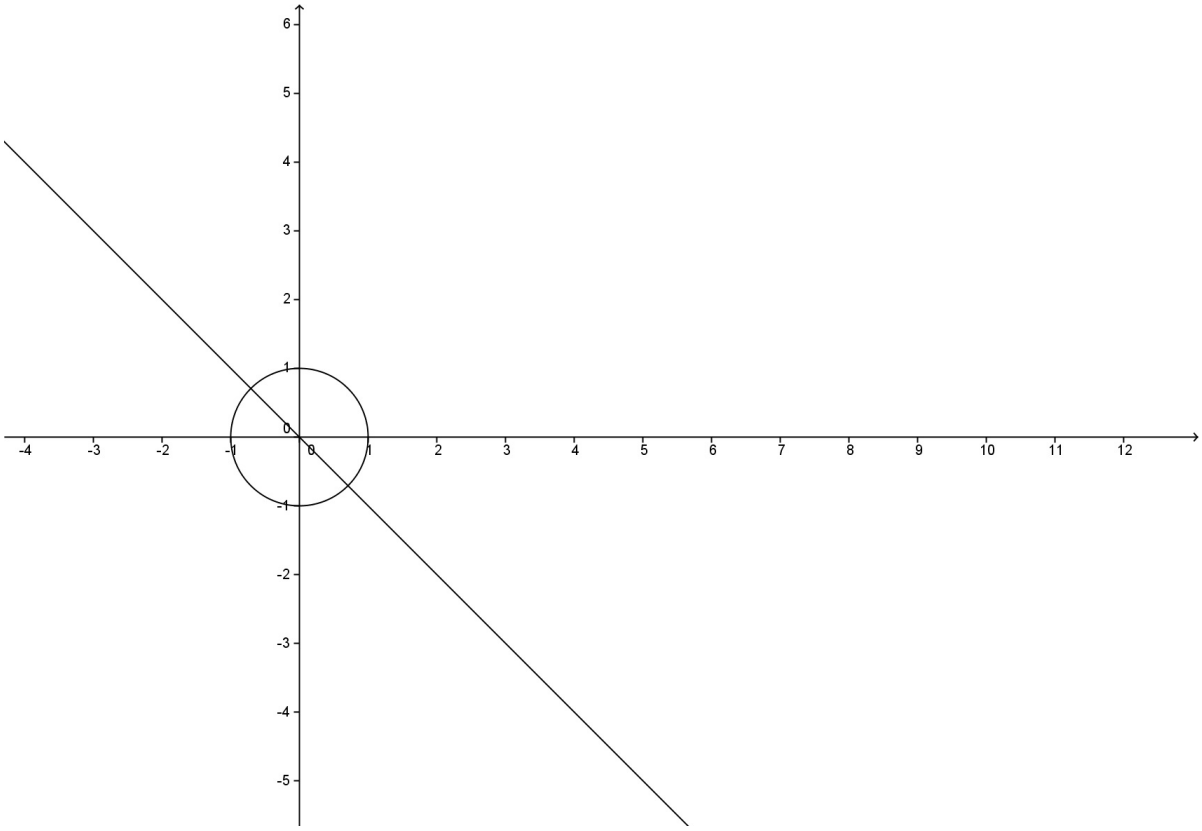


Figura 2.9: Interseção entre reta e curva

Exemplo 2.3.17. Considere a reta afim

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

e

$$C_2 : x^3 - y^2 = 0. \tag{2.3.7}$$

Analisaremos a interseção entre estas curvas afins.

Substituindo $y = x$ na equação (2.3.7), 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, $\#(C_1 \cap C_2) = 3$.

Observação 2.3.18. Quando estamos contando interseções, estamos considerando a multiplicidade.

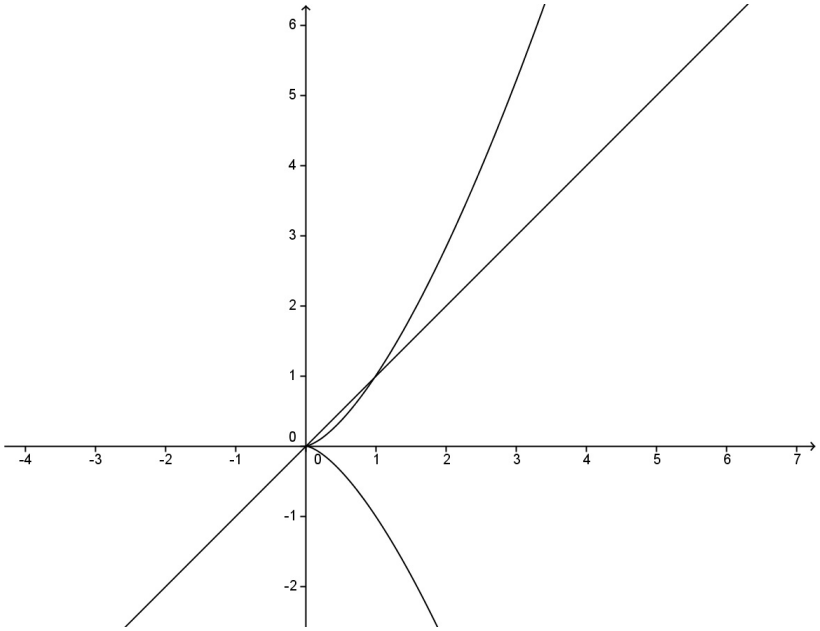


Figura 2.10: Interseção entre reta e cúbica

Exemplo 2.3.19. Sejam

$$C_1 : x + 1 = 0$$

e

$$C_2 : x^2 - y = 0$$

A primeira curva é uma reta afim vertical $x = \dot{-}1$ e a segunda uma parábola afim com eixo focal em Oy. Quantos são os pontos de $C_1 \cap C_2$?
Substituindo $x = -1$ na segunda equação, temos: $1 - y = 0$ e, assim, $y = 1$. Portanto, encontraremos apenas o ponto $(-1, 1)$.

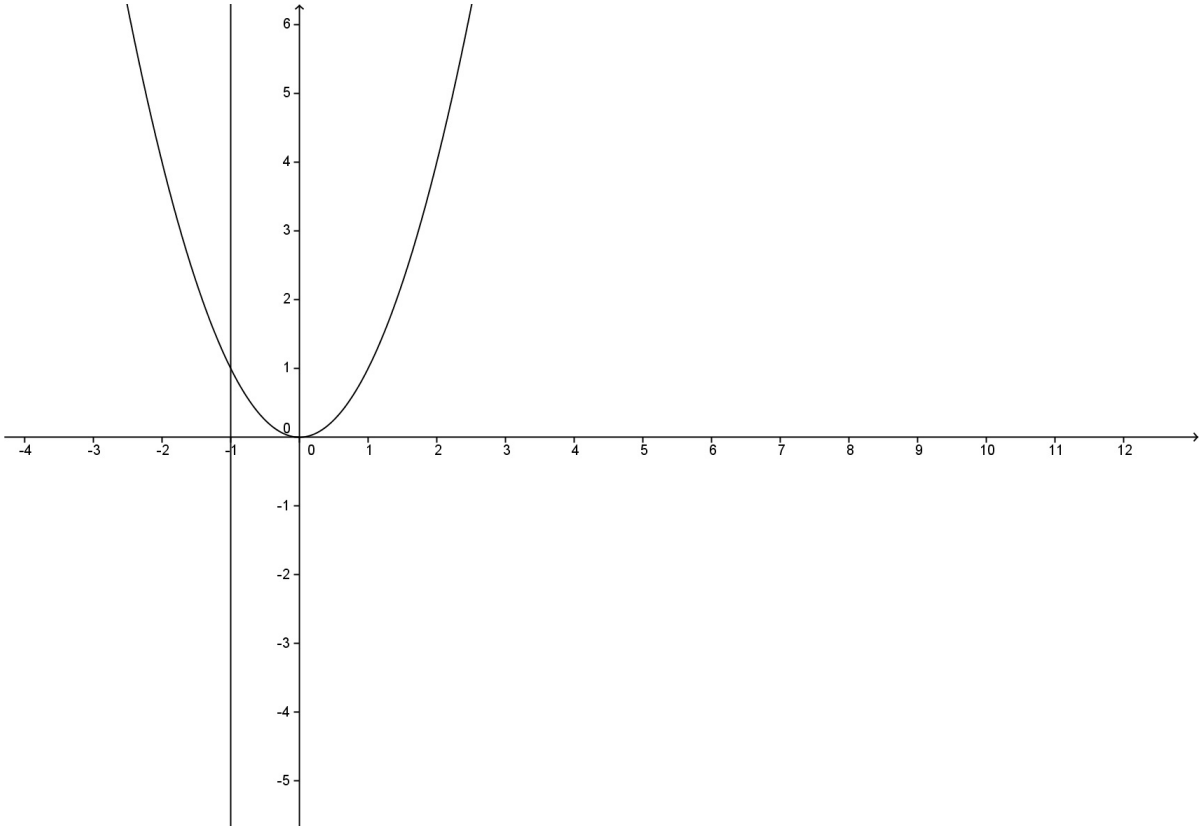


Figura 2.11: Interseção entre reta e cônica

Exemplo 2.3.20. Considere as curvas afins:

$$C_1 : x^2 - 2xy = 1 \tag{2.3.8}$$

$$C_2 : x - 2y = 0. \tag{2.3.9}$$

Substituindo $x = 2y$ na (2.3.8), encontraremos: $0 = 1$. Não há interseções em $\mathbb{R}^2$.

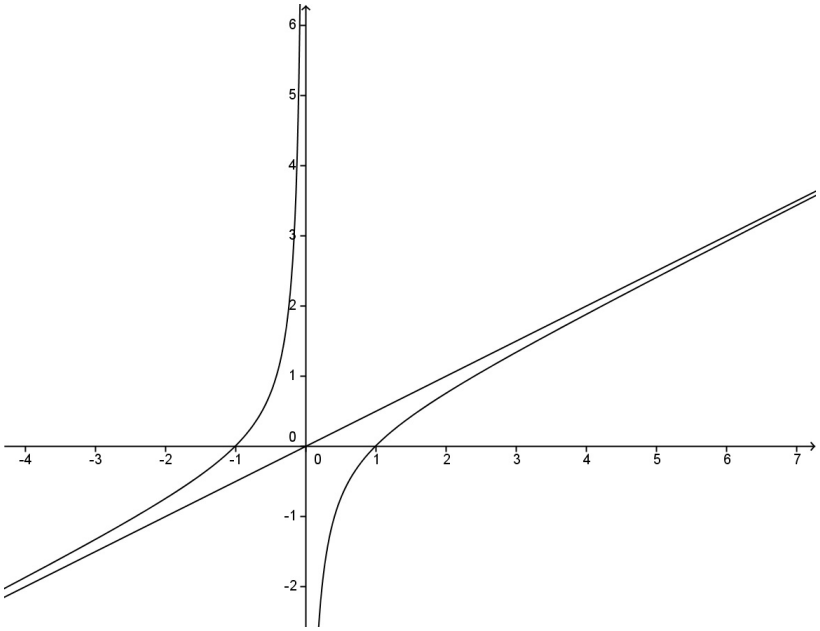


Figura 2.12: Interseção entre reta e cônica

Definição 2.3.21. A curva C_1 é componente da curva C_2 quando o polinômio C_1 faz parte da fatoração do polinômio C_2. Ou seja, a interseção é formada por infinitos pontos.

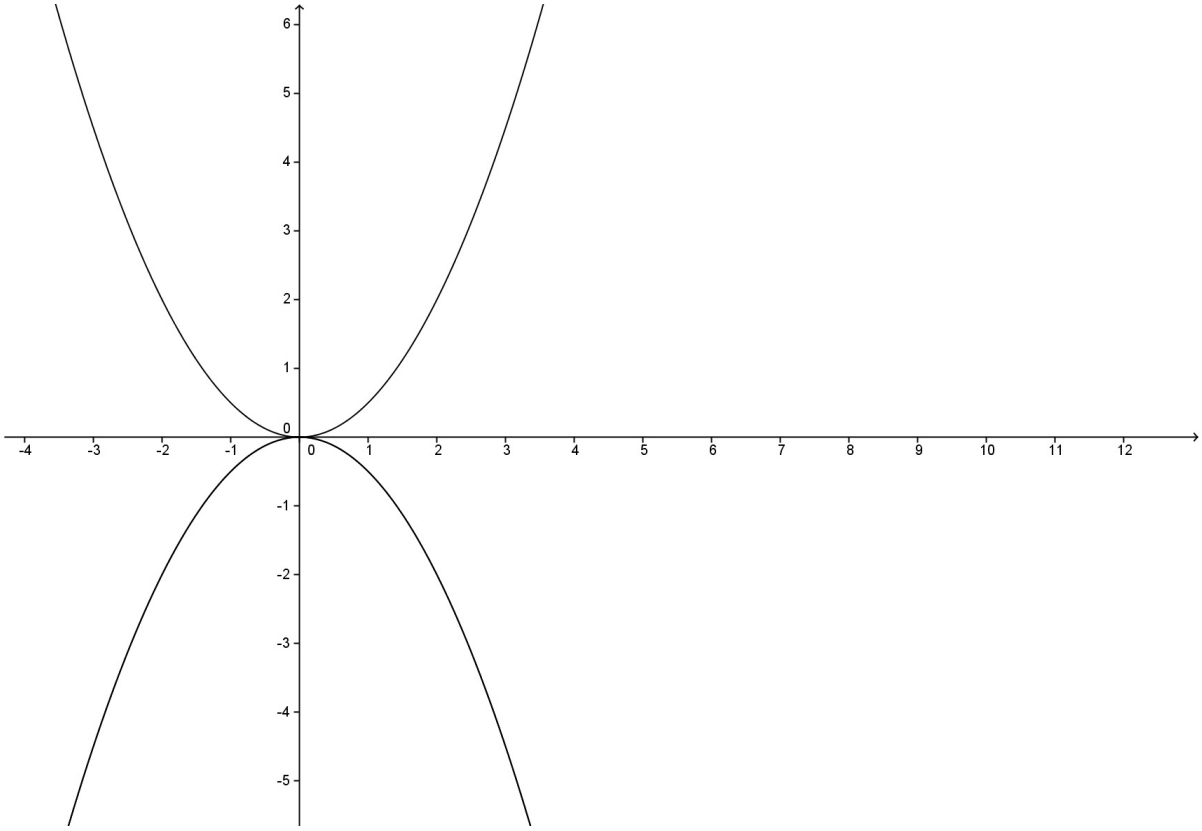
Exemplo 2.3.22. Os exemplos acima podem nos fazer pensar que sempre teremos um número finito de pontos de interseção entre curvas. No entanto, isto nem sempre ocorre. Por exemplo, considere as curvas

$$C_1 : 4y^2 - x^4 = 0$$

e

$$C_2 : 2xy - x^3 = 0,$$

a primeira de grau 4 e a segunda de grau 3, satisfazem a Definição 2.3.21 e, portanto, a interseção é formada por infinitos pontos. Visualizemos:



Faremos agora exemplos com *curvas projetivas*:

Exemplo 2.3.23. Considere as curvas do 2.3.20, em que não há interseções em $\mathbb{R}^2$. Faremos a homegeneização destas curvas, obtendo assim:

$$C_1' : X^2 - 2XY = Z^2 \tag{2.3.10}$$

$$C_2' : X - 2Y = 0. \tag{2.3.11}$$

Substituindo $X = 2Y$ na equação (2.3.10) temos, $Z^2 = 0$.

Agora, temos interseção não vazia, o ponto $(2 : 1 : 0)$, com multiplicidade 2.

Exemplo 2.3.24. Sejam

$$C_1 : X + Z = 0 \tag{2.3.12}$$

$$C_2 : X^2 - YZ = 0 \tag{2.3.13}$$

curvas projetivas, sendo a primeira de grau 1 e a segunda de grau 2. Calculemos a interseção entre estas curvas. Na equação (2.3.13) trocando $X = -Z$, temos $Z^2 - YZ = 0$ e, assim, $Z = 0$ ou $Z = Y$.

Logo, $C_1 \cap C_2$ consiste de dois pontos: $(-1 : 1 : 1)$ e $(0 : 1 : 0)$. É importante lembrar que: $(-1 : 1 : 1) = t(-1 : 1 : 1)$ com $t \neq 0$, representam o mesmo ponto e o ponto $(0 : 0 : 0)$ não pertence à interseção.

Temos, assim, $\#(C_1 \cap C_2) = 2$.

Exemplo 2.3.25. Considere agora as curvas afins,

$$C_1 : x + y = 2 \tag{2.3.14}$$

$$C_2 : x^2 + y^2 = 2 \tag{2.3.15}$$

Substituindo $y = -x + 2$ na equação (2.3.15),temos:

$$x^2 + (2 - x)^2 = 2.$$

$$x^2 + 4 - 4x + x^2 = 2.$$

$$2x^2 - 4x + 2 = 0.$$

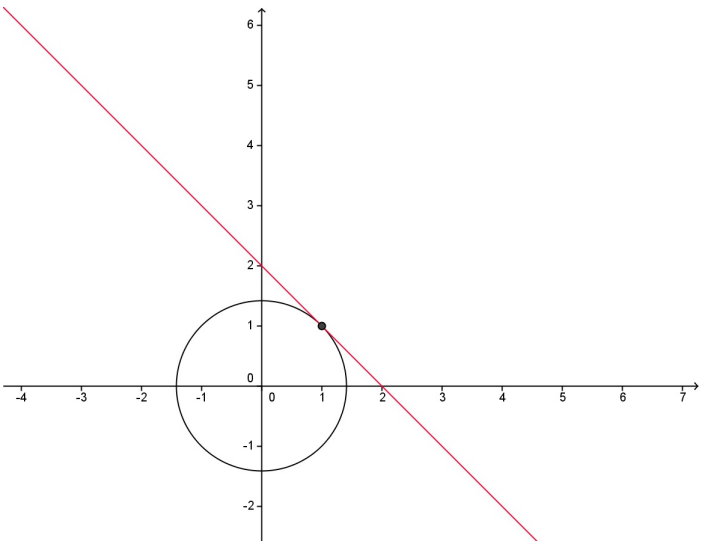
$$2(x - 1)^2 = 0.$$

$$x = 1.$$

$\therefore$ raiz com multiplicidade 2.

Temos, assim, $\#(C_1 \cap C_2) = 2$.

Geometricamente, visualizamos que a curva C_1 é uma reta tangente ao círculo C_2 no ponto $(1, 1)$.



Considerando agora a geometria projetiva e homogeneizando as curvas, obtemos:

$$C_1 : X + Y = 2Z \tag{2.3.16}$$

$$C_2 : X^2 + Y^2 = 2Z^2 \tag{2.3.17}$$

A equação (2.3.16) pode ser escrita da seguinte forma:

$$X = 2Z - Y.$$

Substituindo na equação (2.3.17), temos:

$$(2Z - Y)^2 + Y^2 = 2Z^2.$$

$$4Z^2 - 4ZY + Y^2 + Y^2 = 2Z^2.$$

$$Z^2 - 2ZY + Y^2 = 0.$$

$$(Y - Z)^2 = 0.$$

$$(Y - Z)(Y + Z) = 0.$$

$$Y = Z.$$

ou

$$Y = -Z.$$

Substituindo $Y = Z$ na equação (2.3.16), temos o ponto $t(1 : 1 : 1)$ com $t \neq 0$. Substituindo $Y = -Z$, temos o ponto $t(3 : -1 : 1)$ com $t \neq 0$. Logo, temos dois pontos de interseção.

Exemplo 2.3.26. Sejam

$$C_1 : x + y + 1 = 0$$

e

$$C_2 : 2x^2 + xy - y^2 + 4x + y + 2 = 0,$$

sendo a curva C_1 uma reta e a curva C_2 uma hipérbole degenerada, ou melhor, a união de duas retas (*cf.* [9]):

$$C_2 : 2x^2 + xy - y^2 + 4x + y + 2 = (x + y + 1) \cdot (2x - y + 2).$$

Portanto, C_2 é a união de duas curvas e uma delas é C_1. Neste caso, a curva $C_1 \subset C_2$, a curva C_2 não é um polinômio irredútivel. Como em 2.3.22 a curva C_1 é uma componente da curva C_2. Logo, a interseção entre elas não é um conjunto finito de pontos.

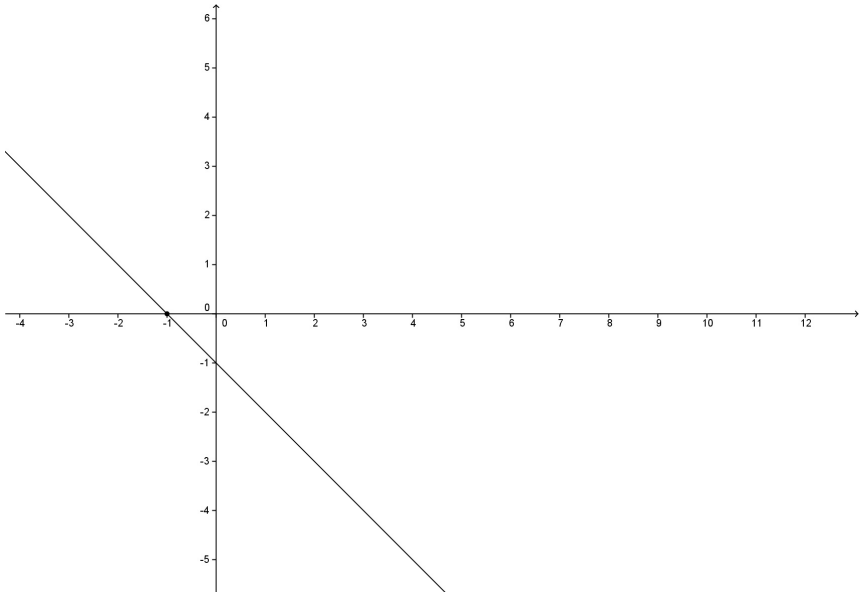


Figura 2.13: Interseção entre reta e cônica

Após esta sequência de exemplos de interseção entre curvas, percebemos que, em alguns deles, a quantidade de pontos da interseção foi exatamente igual ao produto dos graus das curvas; em outros isto não acontece. O teorema que veremos a seguir esclarece como podemos contar os pontos de interseção entre duas curvas no plano.

Etienne Bezout (1730-1783) escreveu uma obra monumental em seis volumes que cobria toda a matemática conhecida na época (basicamente Cálculo, Equações Diferenciais e Geometrias). O Teorema de Bezout versa sobre a contagem de pontos em comum entre duas curvas no plano, desde que essa quantidade de pontos da interseção seja um número finito. Historicamente, pode ser considerado o primeiro teorema da Geometria Algébrica.

Maclaurim (1720), a partir de generalizações de trabalhos de Newton, enunciou o teorema sem, no entanto, prová-lo. Em 1770, Etienne Bezout desenvolveu a área chamada Teoria da Eliminação e provou o teorema que leva seu nome.

Lema 2.3.27. *Sejam F e G curvas planas projetivas. Então, $F \cap G$ é finita se e só se F, G não admitirem componente em comum.*

Demonstração. cf. [17] □

Teorema 2.3.28. *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. [15].

□

No exemplo 2.3.24, as curvas projetivas

$$C_1 : X + Z = 0.$$

$$C_2 : X^2 - YZ = 0.$$

não têm componentes em comum, portanto é possível aplicar o Teorema de Bezout e assim

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

No exemplo 2.3.25, as curvas projetivas

$$C_1 : X + Y = 2Z$$

$$C_2 : X^2 + Y^2 = 2Z^2$$

também não têm componentes em comum. Aplicando Bezout, temos:

$$\#(C_1 \cap C_2) = \delta(C_1) \cdot \delta(C_2),$$

lembrando que, neste caso, o ponto foi raiz com multiplicidade 2.

Nos exemplos 2.3.22 e 2.3.26, não podemos aplicar o Teorema de Bezout, pois uma curva é componente da outra.

Exemplo 2.3.29. Considere as curvas:

$$C_1 : X + Y + Z = 0,$$

$$C_2 : X^3 + Y^3 = 3XYZ.$$

Como são curvas projetivas sem componetes em comum, temos que:

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

Exemplo 2.3.30. Observando o exemplo 2.3.19, percebemos que o Teorema de Bezout não valeria se não contasse com os pontos no infinito. Neste exemplo $\#(C_1 \cap C_2) = 1$ e o outro ponto que está faltando é exatamente o ponto no infinito.

Para confirmar este fato, basta homogeneizar as curvas e calcular a interseção.

Homogeneizando, temos as curvas:

$$X + Z = 0 \tag{2.3.18}$$

e

$$X^2 - YZ = 0. \tag{2.3.19}$$

Substituindo (2.3.18) na (2.3.19) encontramos:

$$Z^2 - YZ = 0.$$

$$Z(Z - Y) = 0.$$

Assim temos os pontos de interseção: $(O : 1 : 0)$ (ponto no infinito) e $t(-1 : 1 : 1)$ com $t \neq 0$.

2.4 Pontos Racionais em Cônicas

Nesta seção faremos um breve estudo de como encontrar os pontos racionais de uma cônica.

Inicialmente, vejamos algumas definições.

Definição 2.4.1. Um ponto do plano cartesiano $\mathbb{R}^2$ é dito *racional* se ambas as suas coordenadas são números racionais.

Definição 2.4.2. Uma reta afim é racional se sua equação pode ser escrita com coeficientes racionais, isto é:

$$ax + by + c = 0$$

com a,b,c, racionais.

A equação geral de uma cônica afim é dada por:

$$ax^2 + bxy + cz^2 + dx + ey + f = 0. \tag{2.4.1}$$

Definição 2.4.3. Uma cônica é racional se a equação (2.4.1) é escrita com números racionais.

A interseção entre duas retas racionais é um ponto racional.

Exemplo 2.4.4. Sejam as retas afins racionais:

$$2x - y = 1 \tag{2.4.2}$$

$$x + 3y = 4. \tag{2.4.3}$$

Na equação (2.4.2), temos $2x - 1 = y$ e, substituindo na equação (2.4.3), encontramos o ponto racional $(1, 1)$.

Uma questão a ser analisada é: a interseção entre uma reta racional e uma cônica racional é formada por pontos racionais? Geralmente, não. Para encontrar as coordenadas destes pontos de interseção, poderemos utilizar a Geometria Analítica, encontrando uma equação quadrática para a coordenada x da interseção. Se a cônica e a reta forem racionais, a equação quadrática terá coeficientes racionais. Então, os pontos de interseção serão racionais se, e somente se, as raízes da equação quadrática forem racionais.

Exemplo 2.4.5. Considere a reta afim e a cônica afim racionais:

$$r : x - 2y + 2 = 0 \tag{2.4.4}$$

$$C : x^2 + 4y^2 - 4x - 8y + 4 = 0. \tag{2.4.5}$$

Calcularemos $r \cap C$.

Substituindo $x = 2y - 2$ na equação (2.4.7), temos:

$$(2y-2)^2 + 4y^2 - 4 \cdot (2y-2) - 8y + 4 = 0.$$

$$8y^2 - 16y + 16 = 0.$$

$$y^2 - 2y + 2 = 0.$$

Portanto, a interseção entre a reta racional e a cônica racional será constituída de pontos racionais se, e somente, as raízes da equação quadrática forem racionais. Como $\triangle = 2^2 - 4 \cdot 1 \cdot 2 = -4 < 0$, não temos raízes reais e, cosequentemente, não há pontos racionais.

Exemplo 2.4.6. Considere a reta afim e a cônica afim racionais:

$$r : x + 2y - 3 = 0 \tag{2.4.6}$$

$$C : x^2 + 4y^2 - 6x - 16y + 17 = 0. \tag{2.4.7}$$

Calcularemos $r \cap C$.

Substituindo $x = 2y - 2$ na equação (2.4.7), temos:

$$(3-2y)^2 + 4y^2 - 6 \cdot (3-2y) - 16y + 17 = 0.$$

$$8y^2 - 16y + 8 = 0.$$

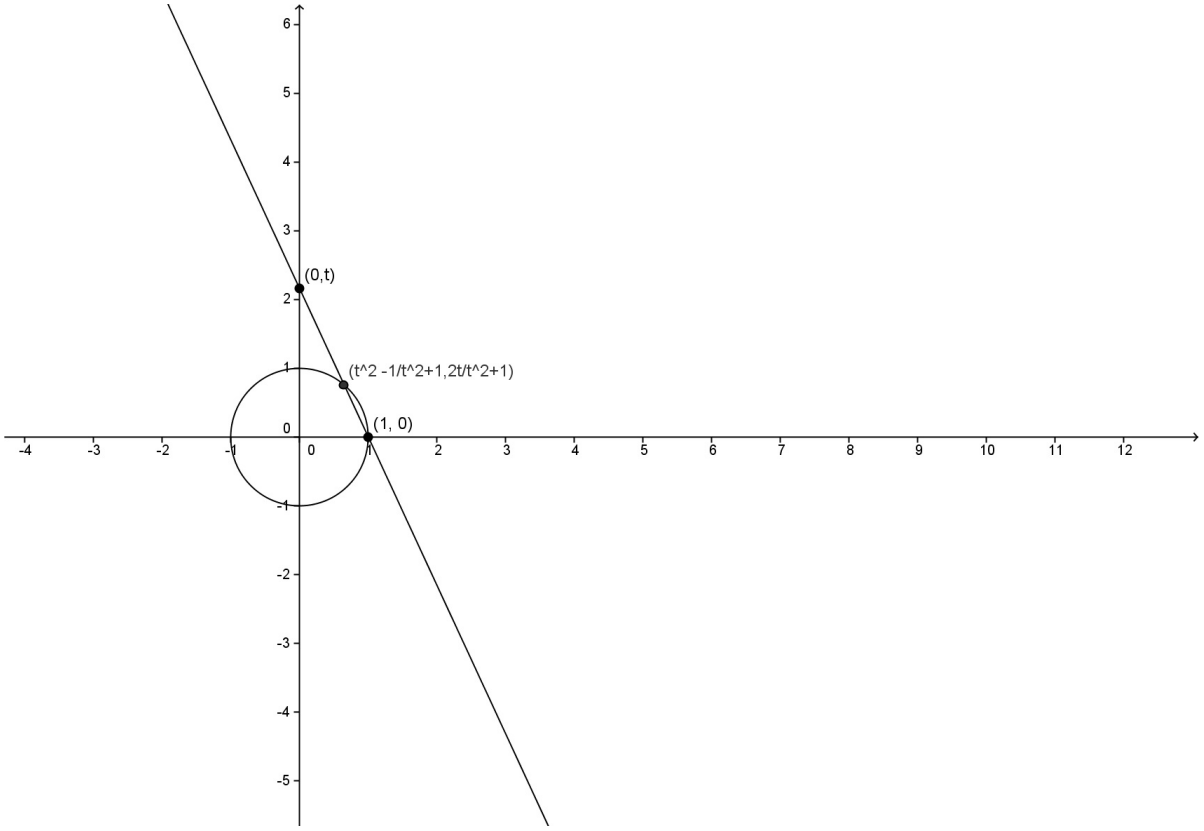
$$y^2 - 2y + 1 = 0.$$

Como $\triangle = 2^2 - 4 \cdot 1 \cdot 1 = 0$, teremos pontos racionais para a interseção entre a reta racional e a cônica racional.

Em seguida analisaremos o Teorema 2.4.7 e exemplo 2.4.8 de [10] que mostram como encontrar todos os pontos racionais de uma cônica quando conhecemos um deles.

Teorema 2.4.7. *Os pontos racionais (x, y) da circunferência de equação $x^2 + y^2 = 1$ são $(x, y) = (1, 0)$ e todos os pontos da forma $(x, y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$ com $t \in \mathbb{Q}$.*

Demonstração. Considere a reta passando pelos pontos $(1, 0)$ e $(0, t)$ com $t \in \mathbb{Q}$, ou seja, a reta de equação $y = -t(x - 1)$. Esta reta intercepta a circunferência em dois pontos: $(1, 0)$ e $\left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$, como mostra a figura:



Agora observe que $(0,t) \longmapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$ estabelece uma bijeção entre os pontos racionais do eixo y e os pontos racionais P da circunferência $x^2+y^2=1$, menos o ponto $(1,0)$. De fato, é claro que se $t \in \mathbb{Q}$ então $(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1})$ é um ponto racional da circunferência. Reciprocamente, dado um ponto $P \neq (1,0)$ da circunferência, temos que a reta que une P a $(1,0)$ admite uma equação com coeficentes racionais, logo intercepta o eixo y em um ponto $(0,t)$ com $t \in \mathbb{Q}$. Isto completa a demonstração. □

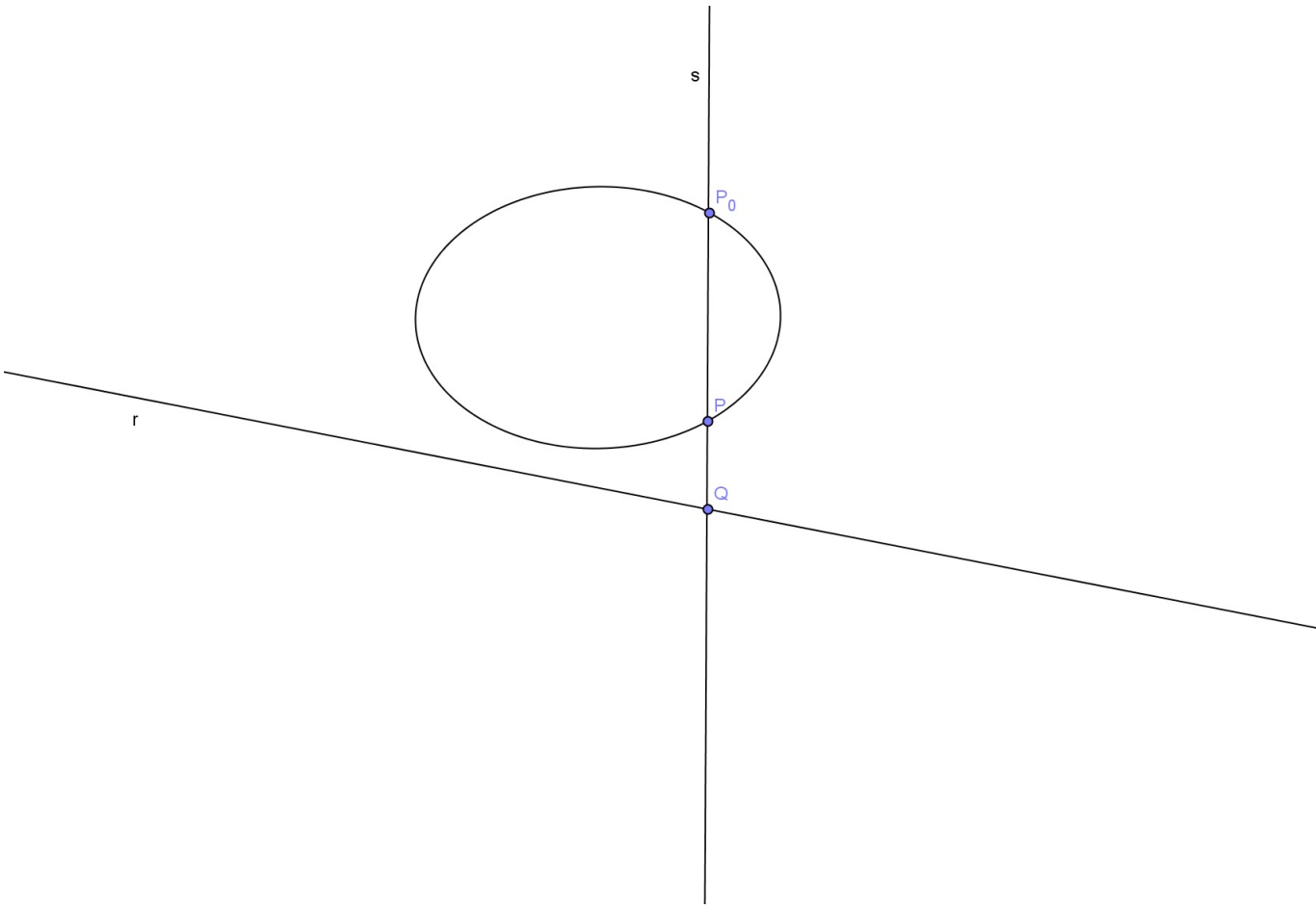
Assim, substituindo $t = \frac{m}{n}$ com $m,n \in \mathbb{Z}$ e $\text{mdc}(m,n) = 1$ obtemos as soluções racionais $\left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$, que correspondem às ternas pitagóricas $(m^2-n^2, 2mn, m^2+n^2)$.

Exemplo 2.4.8. Encontre todos os pontos racionais da elipse.

$$\frac{x^2}{5/2} + \frac{y^2}{5/3} = 1.$$

Solução: Incialmente, é fácil encontrar um destes pontos racionais, digamos $(x,y) = (1,1)$. Para encontrar os demais, começamos traçando uma reta r de coeficientes racionais paralela à reta tangente à elipse no ponto $P_0 = (1,1)$. Derivando a equação da elipse em relação a x, obtemos $\frac{2x}{5/2} + \frac{2yy'}{5/3} = 0$ e, assim, $y' = -\frac{2}{3}$ para $(x,y) = (1,1)$. Portanto, podemos tomar, por exemplo, a reta r de equação $y = -\frac{2}{3}x - 2$. Agora, para um ponto $P \neq P_0$ da elipse, seja s a reta que liga P a $P_0 = (1,1)$; como esta reta não é paralela a r, temos que r e s determinam um

ponto Q, como na figura a seguir:



Mostraremos que a associação $P \longleftrightarrow Q$ define uma bijeção entre os pontos racionais da elipse, excetuando o ponto P_0, e os pontos racionais da reta r.

Em primeiro lugar, se P é um ponto racional da elipse então a equação da reta s, que liga dois pontos racionais P e P_0, possui coeficientes racionais. Logo, Q será um ponto racional, sendo a interseção de duas retas r e s cujas equações têm coeficientes racionais. Reciprocamente, suponhamos que $Q = (a, b)$ é um ponto racional de r. Então a equação da reta s, determinada pelos pontos racionais P_0 e Q, terá coeficientes racionais, a interseção $P \neq P_0$ de s com a elipse será um ponto racional, já que, isolando y na equação de s e substituindo na equação da elipse, obtemos uma equação quadrática com coeficientes racionais.

$$\frac{2}{5}x^2 + \frac{3}{5}\left(1 + \frac{b-1}{a-1}(x-1)\right)^2 - 1 = 0$$

Entretanto, a abscissa de $x = 1$ de P_0 é uma das raízes. Logo, a outra raiz(que é abscissa de P) é racional também pelas relações de Girard. Como P pertence à reta s cuja equação tem coeficientes racionais, a ordenada de P também será racional, ou seja, P será um ponto racional.

Após algumas contas, obtemos a seguinte fórmula para P em função de $Q = (a, b)$:

$$P = \left(\frac{10a^2 + 90a + 21}{10a^2 + 24a + 87}, \frac{10a^2 - 20a - 111}{10a^2 + 24a + 87}. \right)$$

Assim, os pontos racionais P da elipse são obtidos fazendo a percorrer todos os racionais $a \in \mathbb{Q}$ juntamente com $a = \infty$, i.e., o limite para $a \longrightarrow \infty$ na expressão acima, que fornece o ponto inicial $P_0 = (1, 1)$, que corresponde ao "ponto no infinito" de r, interseção de r com a reta s tangente à elipse no ponto P_0 (plano projetivo).

De uma forma geral, se conhecemos um ponto racional da cônica, podemos encontrar todos os outros pontos racionais usando um procedimento análogo aos usados no Teorema 2.4.7 e no exemplo 2.4.8. Este processo é chamado de *Princípio geométrico das cônicas* e será descrito de maneira geral a seguir.

Observação 2.4.9. *Princípio Geométrico das Cônicas*

Suponhamos que tenhamos um ponto O racional da cônica. Desenhamos uma reta racional e projetamos a cônica para a reta a partir deste ponto. Pelo Teorema de Bezout, sabemos que reta encontra a cônica em dois pontos. Portanto, para cada ponto P da cônica, temos um ponto Q na reta e, reciprocamente, para cada Q na reta, juntando-se ao ponto O temos um ponto P sobre a cônica (Observe-se a figura 2.20). Temos uma correspondência biunívoca entre os pontos da cônica e os pontos da reta. Note-se que se o ponto P sobre a cônica tem coordenadas racionais, então o ponto Q na reta será racional. Reciprocamente, se Q é racional, então, como O foi assumido como racional, a reta determinada por P e Q encontra a cônica em dois pontos, um dos quais é racional. Então, o outro ponto é racional também. Os pontos racionais em retas são facilmente descritos em termos de valores racionais de algum parâmetro.

Capítulo 3

Curvas Elípticas

Neste capítulo, 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 [10], [12] e [15].

3.1 Contexto Histórico

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 :

$$x^n + y^n = z^n \tag{3.1.1}$$

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

$$y^2 - x^3 = c. \tag{3.1.2}$$

Em 1621, *Bachet* descobriu uma proposição chamada *Fórmula da Duplicação de Bachet* que afirmava: *Se* (x, y) *é uma solução para a equação* (3.1.2) *com* x *e* y *racionais, então*

$\left(\frac{x^4-8cx}{4y^2}, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$ *também é uma solução para* (3.1.2) *com números racionais.(para um maior detalhamento cf. a introdução de [15])*

Estudaremos, neste trabalho, 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*.

O estudo das Equações Diofantinas, em particular da Teoria das Curvas Elípticas tem aplicações. As curvas elípticas têm sido utilizadas para lançar luz sobre alguns problemas importantes, relacionados à criptografia, reticulados, a problemas de empacotamento da esfera e à rápida fatoração de números inteiros.

3.2 Caracterização de Curvas Elípticas

Definição 3.2.1. Uma *curva projetiva plana* definida por uma equação da forma

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{3.2.1}$$

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

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

$$y^2 = x^3 + ax + b \tag{3.2.2}$$

(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 (3.2.2) 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 (3.2.2).

Vejamos uma curva elíptica, por exemplo $y^2 = x^3 - x$. Note-se que, na figura a seguir, as duas pontas do ramo da direita se encontram na direção do "ponto do infinito" $O = (0 : 1 : 0)$, que é o ponto de interseção da "reta no infinito" com qualquer reta vertical $x - cz = 0$. Em outras palavras, O é o ponto de concorrência de todas as retas verticais, pois toda reta vertical passa pelo ponto no infinito, *cf.* Proposição 2.3.11.

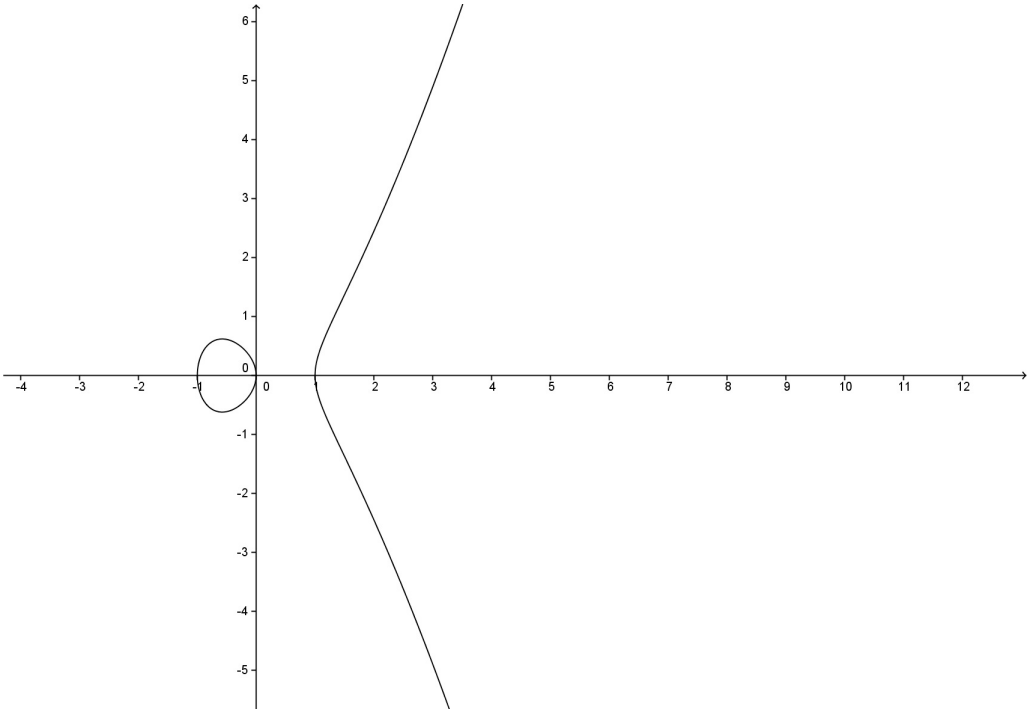


Figura 3.1: Uma curva elíptica

A condição do discriminante na definição de curva elíptica é importante para garantir que a curva seja *lisa*; *cf.* [6] e [15]. 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.

Mais detalhadamente, uma equação $f(x, y) = 0$ define uma curva lisa exatamente quando não há pontos na curva em que ambas derivadas parciais de f se anulem simultaneamente, ou seja, quando não houver soluções comuns das equações:

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

Como estamos trabalhando com a curva elíptica da forma $y^2 = g(x)$ com $g(x)$ um polinômio de grau 3, podemos decidir quando podem haver pontos singulares e mesmo que tipo de pontos singulares eles são. Se pusermos $f(x, y) = y^2 - g(x)$, teremos:

$$\frac{\partial f}{\partial x}(x, y) = -g'(x)$$

e

$$\frac{\partial f}{\partial y}(x, y) = 2y$$

e a condição para um ponto ser "mal comportado" passa a ser:

$$y^2 = g(x), \quad g'(x) = 0, \quad 2y = 0,$$

que se reduz a $y = g(x) = g'(x) = 0$. Daí, um ponto será "ruim" exatamente quando sua ordenada y é zero e sua abcissa x é uma raiz dupla do polinômio $g(x)$. Todavia, como $g(x)$ é de grau 3, há apenas três possibilidades:

- $g(x)$ não tem raízes múltiplas e a equação define uma curva elíptica;
- $g(x)$ tem uma raiz dupla;
- $g(x)$ tem uma raiz tripla.

Veremos exemplos para cada caso:
Para o primeiro caso, seja a curva: $y^2 = x^3 + x$ com $\triangle = 4a^3 + 27b^2 = 4 \cdot 1^3 + 27 \cdot 0 = 4 \neq 0$.

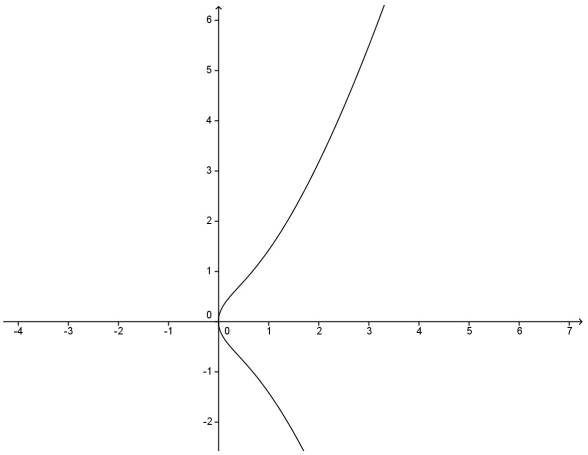


Figura 3.2: Uma curva sem pontos singulares

Considere a curva: $y^2 = x^3 + x^2$, $\triangle = 0$

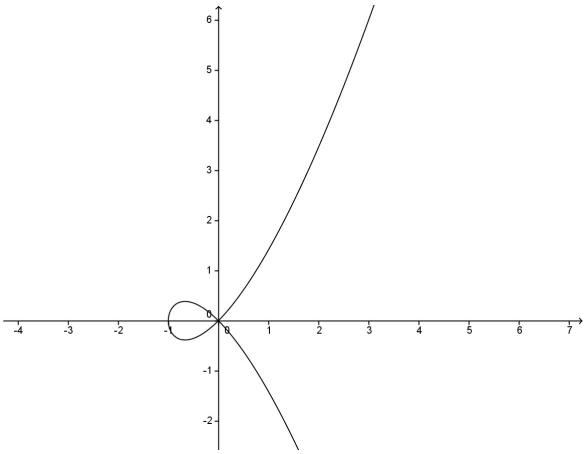


Figura 3.3: Uma curva com um ponto singular

Finalmente, considere a curva: $y^2 = x^3$, também com $\triangle = 0$.

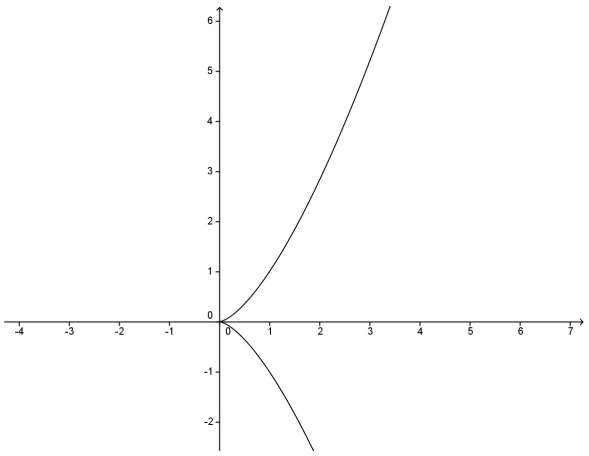


Figura 3.4: Uma curva com um ponto singular

Quando há pontos "ruins", o que acontece é que ou duas das ráizes de $g(x)$ coincidem, ou as três coincidem. No traço da curva $y^2 = x^3 + x^2$ temos um "nó", a curva tem duas retas tangentes diferentes ($x = 0$ é raiz dupla), enquanto no traço da curva $y^2 = x^3$ as três raízes coincidem, caso em que temos uma singularidade cuspidal. Para mais detalhes sobre pontos singulares e curvas lisas, *cf.* [6] e [15].

Observação 3.2.2. É importante saber que as curvas elípticas que consideraremos estão na chamada *Forma Normal de Weierstrass*. Toda curva elíptica com pelo menos um ponto racional pode ser colocada nessa forma através de uma mudança conveniente de variáveis. Neste trabalho, não faremos a prova desta transformação, basta consultar [15].

Equação na forma de Weierstrass:

$$x^3 + ax + b = 0. \tag{3.2.3}$$

3.2.1 A Geometria das Curvas Elípticas

Consideremos o famoso exemplo do último Teorema de Fermat para expoente três:

$$x^3 + y^3 = 1, \tag{3.2.4}$$

ou, na forma homogênea,

$$X^3 + Y^3 = Z^3. \tag{3.2.5}$$

Para encontrar soluções racionais para a equação (3.2.4), encontraremos as soluções inteiras da equação (3.2.5); este é o primeiro caso não trivial do último teorema de Fermat. Não podemos usar o princípio geométrico que funciona tão bem para cônicas, como foi visto na Observação

2.4.9, porque, pelo Teorema de Bezout, uma reta geralmente encontra uma cúbica em três pontos. Ou seja, se temos um ponto racional, não podemos projetar a cúbica sobre uma reta porque cada ponto sobre a reta seria, em seguida, correspondente a dois pontos sobre a curva.

No entanto, podemos utilizar propriedades geométricas. Se temos dois pontos racionais sobre uma curva, então podemos geralmente encontrar o terceiro. Inicialmente, desenhamos a reta determinada por estes dois pontos; esta reta será uma reta racional e se encontra com a cúbica em mais um ponto, pelo Teorema 2.3.28. Em seguida, para calcularmos as três interseções entre a reta racional com uma cúbica racional, 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.

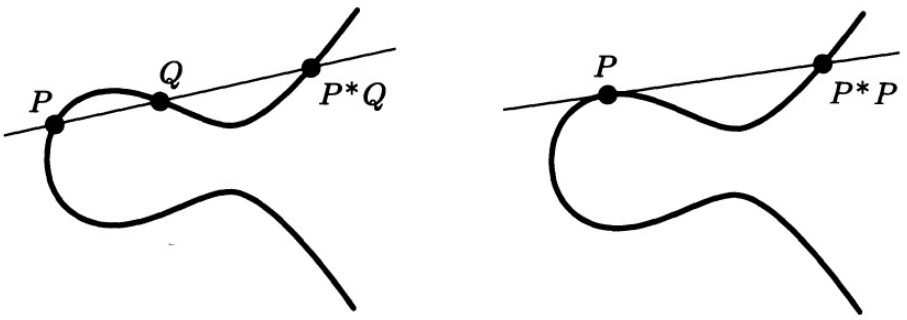


Figura 3.5: Composição de pontos em uma curva elíptica

Mesmo se só tivermos um ponto P racional, 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 racional. Então, podemos juntar esses novos pontos acima e encontrar mais pontos. Essa é a ideia por trás do Teorema de Mordell, um importante resultado da área.

Teorema 3.2.3. Teorema de Mordell. *Se $\mathcal{C}$ é uma curva cúbica racional plana não-singular , então existe um conjunto finito de pontos racionais que gera todos os pontos pertencentes à curva.*

Se temos quaisquer dois pontos 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 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:

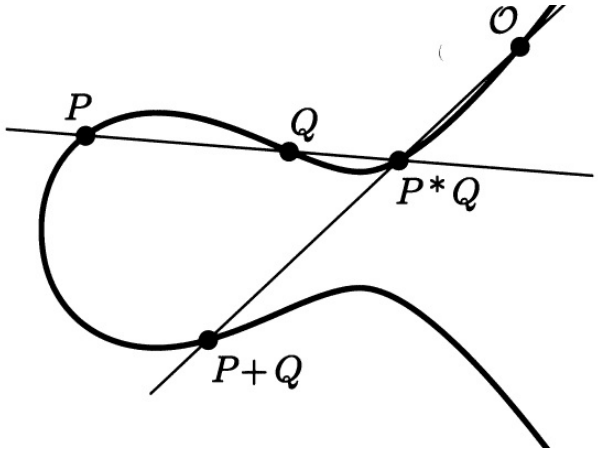


Figura 3.6: A lei do grupo em um curva elíptica

"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 acima, e o fato de que O atua como elemento neutro é na figura a seguir.

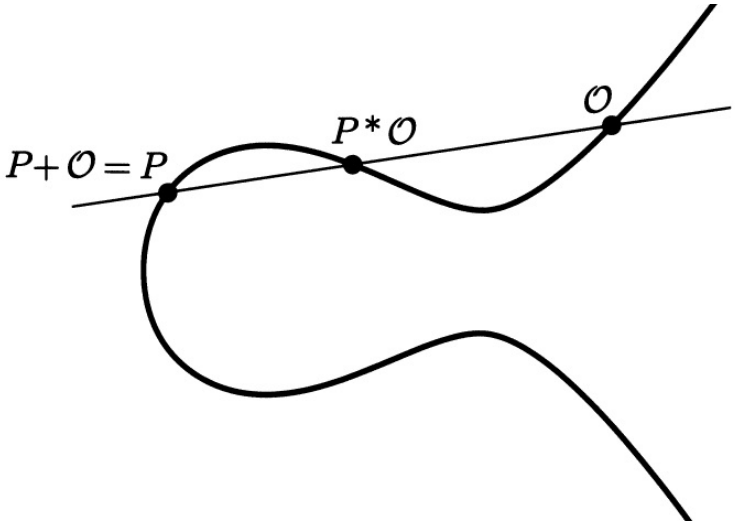


Figura 3.7: O é o elemento neutro

Teorema 3.2.4. *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 racionais P e Q;

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

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

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

Demonstração. Essa operação é comutativa, isto é, $P + Q = Q + P$, pois $P * Q = Q * P$. Provemos que $P + O = P$. Seja l a reta que passa por P e O. Pelo Teorema de Bezout, existe um terceiro ponto $P * O$ na interseção $C \cap l$. A (única) reta que passa por O e por $P * O$ é a própria reta l e o terceiro ponto de interseção é o ponto P, isto é $P + O = P$.

Assim, O é o elemento neutro da lei de grupo.

Procuremos o inverso $-Q$ de um ponto Q. Seja l a reta tangente à cúbica 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, $O * S = O$. Assim, $Q + (-Q) = O$

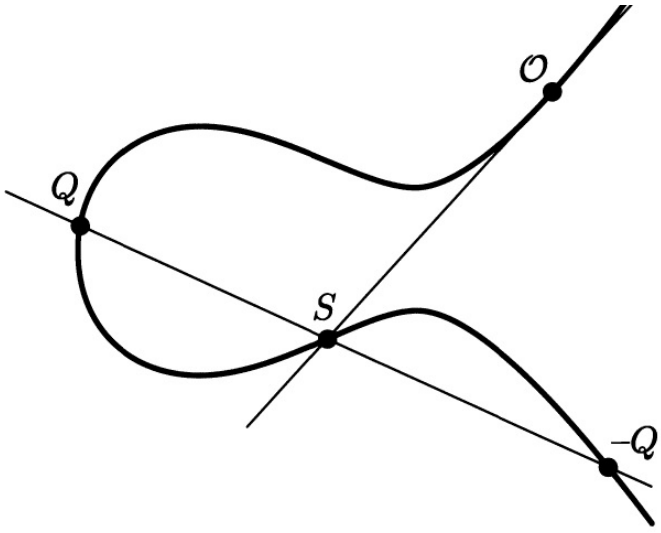


Figura 3.8: O inverso de um ponto

Finalmente, provemos a associatividade de +. Sejam P, Q e R três pontos sobre a curva C. Provar que $(P + Q) * R = P * (Q + R)$ é suficiente para provar que $(P + Q) + R = P + (Q + R)$. Seja l_1 a reta que passa por P e Q e $P * Q$. Seja r_1 a reta que passa por O, $P * Q$ e $P + Q$. Seja l_2 a reta que passa por $P + Q$, R e $(P + Q) * R$. Seja r_2 a reta que passa por Q, R e $Q * R$. Seja l_3 a reta que passa por O, $Q * R$ e $Q + R$. Finalmente, seja r_3 a reta que passa por P, $Q + R$

e $P * (Q + R)$. Na figura, r_1, r_2, r_3 estão desenhadas por um traço contínuo e as retas l_1, l_2, l_3 por um traço pontilhado. 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 $Q + R$.

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

Assim, $C \cap C_l$ e $C \cap C_r$ posuem 8 pontos em comum. Agora, pela Proposição 3.2.5 o nono ponto de interseção deve ser o mesmo. Ou seja, $(P + Q) * R = P * (Q + R)$.

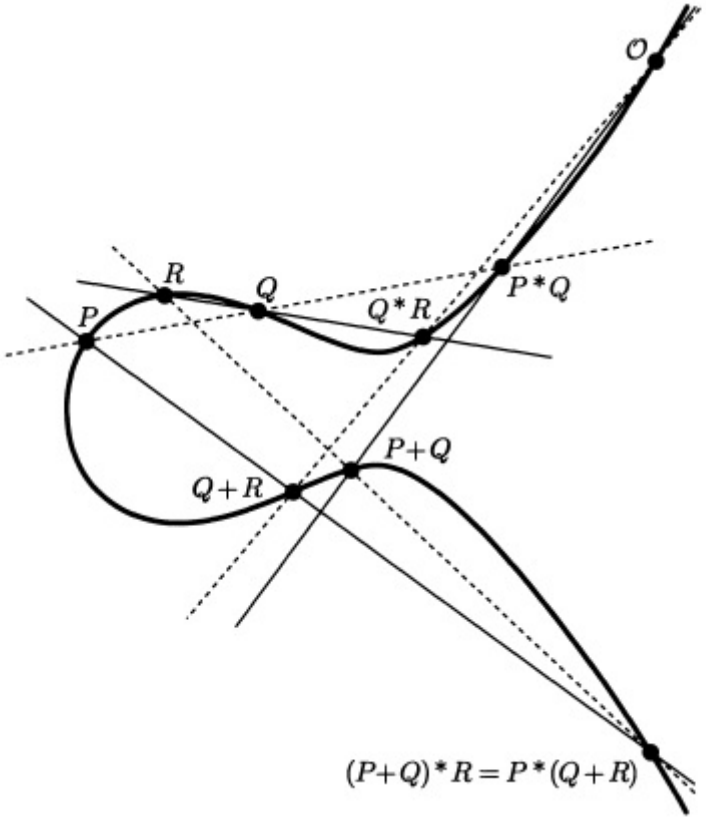


Figura 3.9: Verificação de que a lei é associativa

□

Proposição 3.2.5. *Se duas curvas cúbicas em* $\mathbb{P}^2$ *se intersectam em exatamente nove pontos, então toda curva cúbica que passa por oito desses nove pontos, também passará pelo nono ponto.*

Demonstração. cf. [15](p.16) □

Observação 3.2.6. O Teorema de Mordell mostra que o grupo dos pontos racionais de uma curva elíptica é um grupo finitamente gerado.

3.2.2 Caracterização algébrica dos pontos em uma Curva Elíptica

Seja $\mathcal{C}$ a curva elíptica definida pela equação $YZ^2 = X^3 + aXZ^2 + bZ^3$. Substituindo $Z = 0$ nesta equação, obtemos $X^3 = 0$, ou seja, $(0 : 1 : 0)$ possui multiplicidade 3 na interseção $\mathcal{C} \cap z = 0$. Essa é precisamente a definição de um ponto de inflexão em geometria algébrica. De fato, pode ser provado que esse é o único ponto de inflexão da curva *cf.* [15].

Assim, para uma curva elíptica na forma de Weierstrass, 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 abaixo ilustra o processo de adição dos pontos P e Q sobre uma curva elíptica, visto que a reta que passa por um ponto qualquer e o ponto O é uma reta vertical no plano afim.

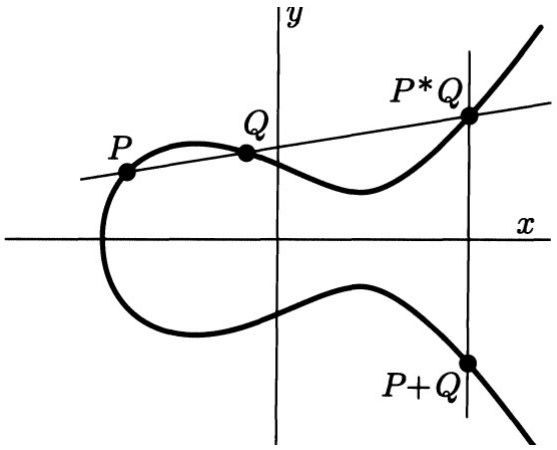


Figura 3.10: Adicionando pontos em uma curva elíptica

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 $-Q = (x, -y)$.

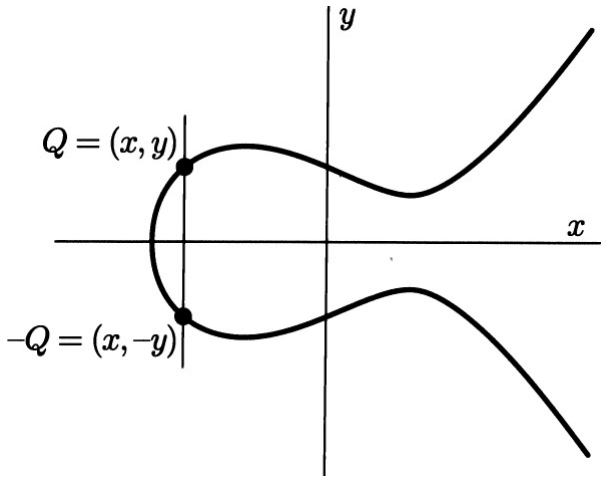


Figura 3.11: O inverso de um ponto na curva elíptica

Observação 3.2.7. Para verificarmos esta possibilidade, suponha que adicionemos Q ao ponto que afirmamos ser $-Q$. A reta através de Q e $-Q$ é vertical, de modo que o terceiro ponto de interseção é o ponto O. Tracemos a tangente a O. Esta reta é a reta no infinito, que possui interseção tripla em O. Logo, $O * O = O$. Isso mostra que $Q + (-Q) = O$, então $-Q$ é o inverso de Q. Esta fórmula não se aplica ao caso $Q = O$, mas obviamente $-O = O$.

Observação 3.2.8. A reta que traçamos para obter a operação de grupo em uma curva elíptica é vertical e a reta vertical passa pelo ponto no infinito $(0 : 1 : 0)$, *cf.* proposição 2.3.11.

Observação 3.2.9. *Lei da Corda Tangente.* Notemos que $P*Q = -(P+Q)$, logo $P+Q+P*Q = O$. Assim, podemos dizer que três pontos têm soma zero se, e somente se, eles estão alinhados.

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

Considere os pontos $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 * P_2 = (x_3, y_3)$, $P_1 + P_2 = (x_3, -y_3)$.

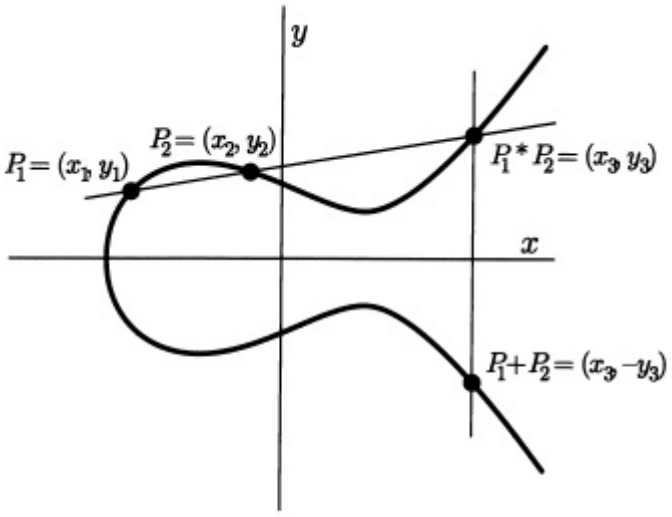


Figura 3.12: A lei da adição

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

$$y = \lambda x + v, \tag{3.2.6}$$

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), pois não passa pelo ponto no infinito, como foi visto na Proposição 2.3.11. Para obtermos este terceiro ponto de interseção, substituiremos (3.2.6) na equação (3.2.2):

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

$$\lambda^2 x^2 + 2\lambda x v + v^2 = x^3 + ax + b$$

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

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.

Assim, obtemos:

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

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 3.2.10. 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 $\mathbb{R}^2$.

Aplicaremos as fórmulas para adicionar pontos pertecentes a curvas elípticas em alguns exemplos abaixo (*cf.* [15]).

Exemplo 3.2.11. Seja a curva elíptica:

$$y^2 = x^3 + 17$$

e os seguintes dois pontos, pertencentes à mesma: $P_1 = (-1, 4)$ e $P_2 = (2, 5)$. Calcularemos $P_1 + P_2$.

Como vimos, iremos primeiramente encontrar a reta que passa por esses dois pontos. Temos que

$$y = \lambda x + v.$$

Determinando λ:

$$\lambda = \frac{5-4}{2-(-1)} = \frac{1}{3}.$$

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

Após encontrado o valor de λ e v, percebemos que a reta é não vertical e, observando a equação na forma de Weierstrass e comparando com a equação dada: $y^2 = x^3 + 17$, podemos finalmente determinar $P_1 + P_2$ utilizando as fórmulas para o valor de x_3 e y_3.

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

$$x_3 = \left(\frac{1}{3}\right)^2 - (-1) - 2.$$

$$x_3 = -\frac{8}{9}.$$

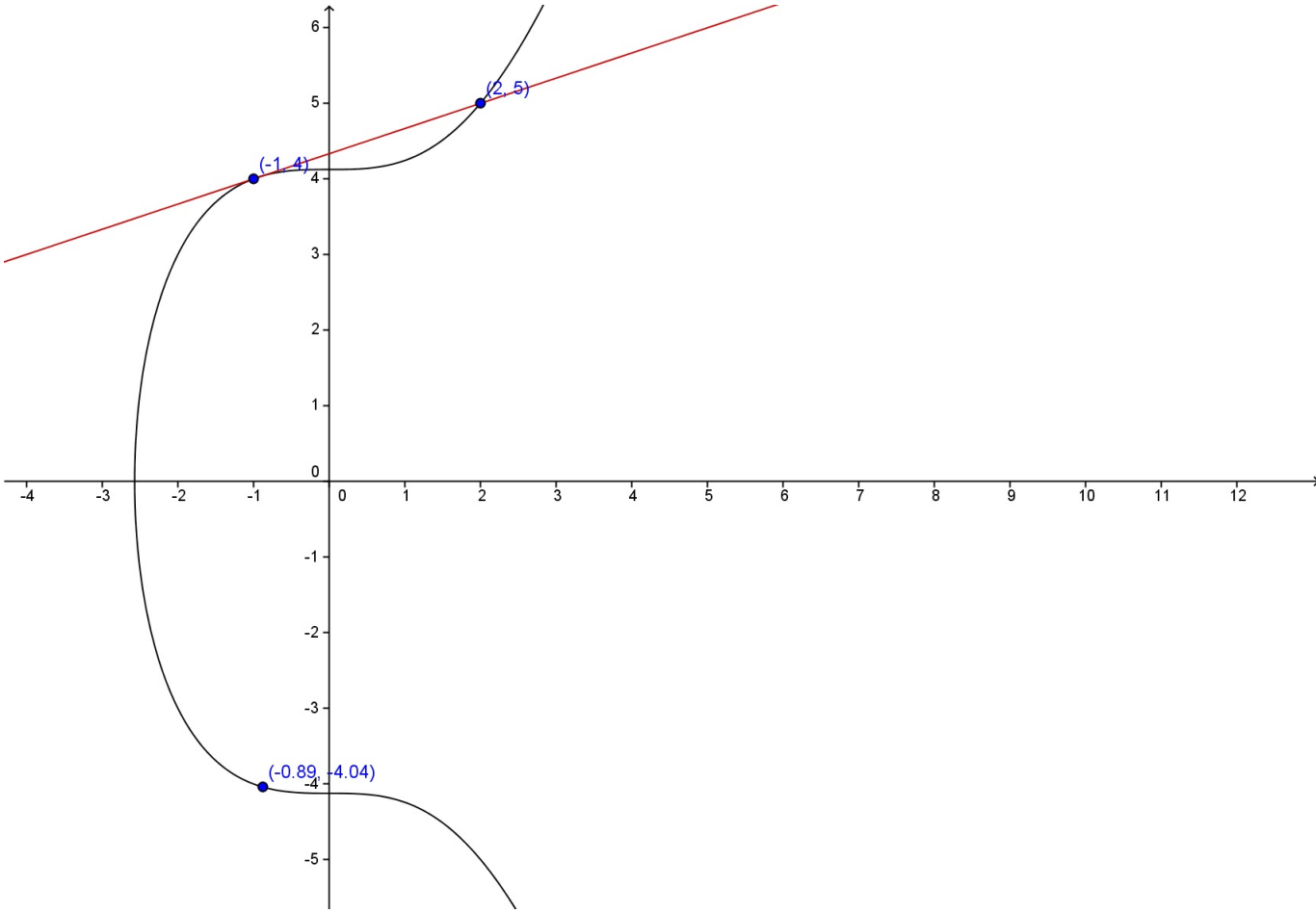
e como y_3 é dado por: $y_3 = \lambda x_3 + v$, temos que:

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

Isto é:

$P_1 + P_2 = P_3 = (x_3, -y_3) = \left(-\frac{8}{9}, -\frac{109}{27}\right)$.

Visualizemos o traço da curva com os pontos $P_1 = (-1, 4)$, $P_2 = (2, 5)$, $P_1 + P_2 = \left(-\frac{8}{9}, -\frac{109}{27}\right)$.



Observação 3.2.12. No traço da curva acima, não está representado o ponto $P_1 * P_2 = \left(-\frac{8}{9}, \frac{109}{27}\right)$. por está muito próximo de $(-1, 4)$. No entanto, basta ficarmos atentos para o fato de $P_1 * P_2 = (x_3, y_3)$

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

$$y^2 = x^3 + 17$$

como $y^2 = f(x)$ e usando diferenciação, temos que:

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

Assim, temos a fórmula para calcular λ quando os pontos coincidirem, ou seja, para obter o dobro de um ponto (na operação do grupo em questão).

Exemplo 3.2.13. Considere a mesma curva elíptica do exemplo 3.2.11 e o ponto $(-1, 4) \in C(\mathbb{Q})$. Calcularemos o dobro de P_1, ou seja, $P_1 + P_1$. Primeiramente, calcularemos λ; como os pontos coincidem, utilizaremos a fórmula da diferenciação.

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y} = \frac{3x^2}{2y} = \frac{3(-1)^2}{2 \cdot 4} = \frac{3}{8}.$$

Agora, precisamos do valor de v. Como a equação da reta tangente é dada por $y = \lambda x + v$, substituindo o ponto $(-1, 4)$, temos que:

$$4 = -\frac{3}{8} \cdot 4 + v.$$

Assim, $v = \frac{35}{8}$ e, então, a reta tangente a C que passa por P_1 é dada por:

$$y = \frac{3}{8}x + \frac{35}{8}.$$

Podemos determinar x_3 e y_3;

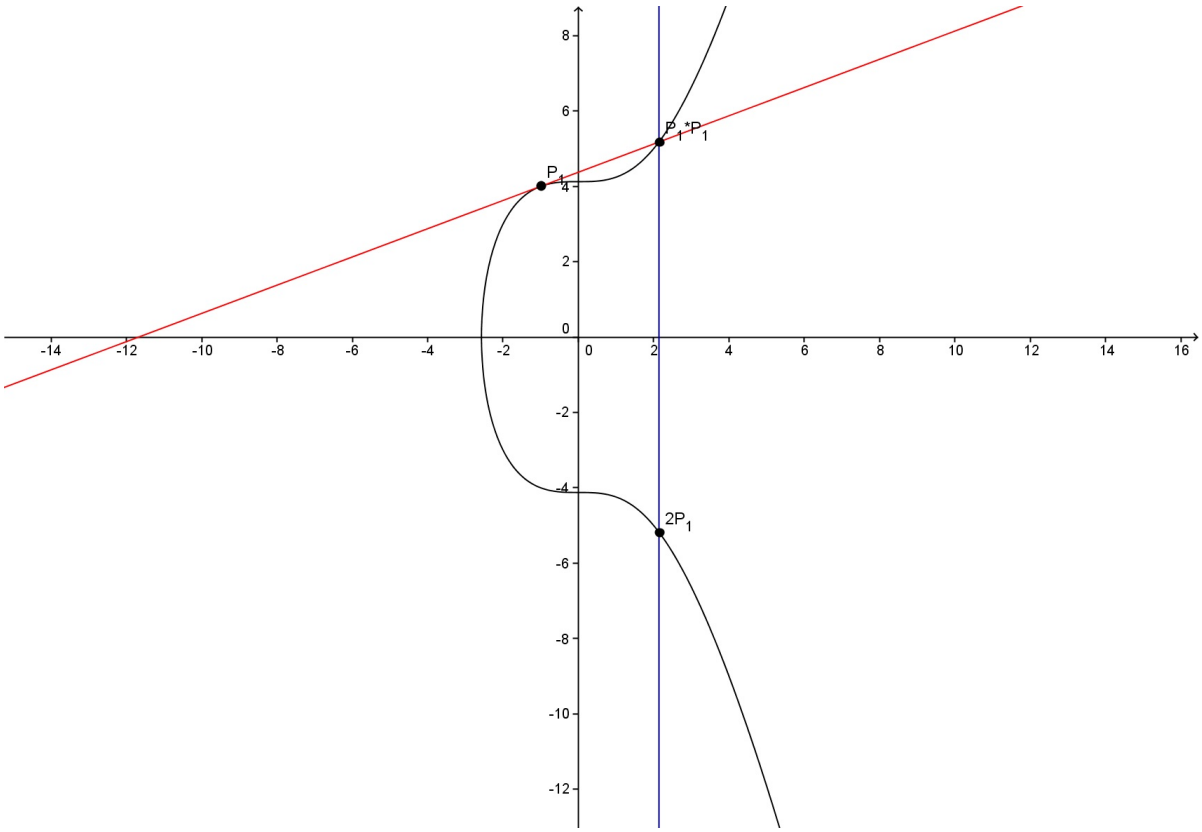
$$x_3 = \lambda^2 - x_1 - x_2$$

$$x_3 = \left(\frac{3}{8}\right)^2 - (-1) - (-1) = \frac{137}{64}$$

$$y_3 = \lambda x_3 + v = \frac{3}{8} \cdot \frac{137}{64} + \frac{35}{8} = \frac{2651}{512}.$$

Assim, $(-1, 4) + (-1, 4) = 2 \cdot (-1, 4) = (x_3, -y_3) = \left(\frac{137}{64}, -\frac{2651}{512}\right)$.

Visualizando no traço da curva, os pontos $P_1 = (-1, 4)$, $P_1 * P_1 = \left(\frac{137}{64}, \frac{2651}{512}\right)$ e $2P_1 = \left(\frac{137}{64}, -\frac{2651}{512}\right)$:



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:

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

Estas são as fórmulas para adição de pontos sobre uma cúbica quando a cúbica está na forma de Weierstrass. Temos a seguinte regra: Sejam P_1 e P_2 sobre uma curva elíptica $\mathcal{C}$ na forma de Weierstrass, o ponto $P_3 = P_1 + P_2$ é obtido traçando-se um reta r que passa por P_1 e P_2. A reta r intersecta o traço da curva $\mathcal{C}$ em um terceiro ponto denotado $-P_3$. O sinal negativo significa que o ponto $-P_3$ é o reflexo do ponto desejado P_3 em relação ao eixo Ox. Note-se que o ponto $-P_3$ está a mesma distância que P_3 em relação ao eixo Ox, pois o traço da curva $\mathcal{C}$ é simétrico em relação a tal eixo. Então, se $-P_3$ tem coordenadas (x_3, y_3), o ponto P_3 terá coordenadas $(x_3, -y_3)$. Observemos que quando $P_1 = P_2$ a reta r tangencia $\mathcal{C}$ nesse ponto e encontra $\mathcal{C}$ em apenas dois pontos: $P_1 = P_2$ e $-P_3$. O ponto P_3 é obtido da mesma forma através da reflexão de $-P_3$ no eixo Ox.

Aplicando a regra da soma descrita, em que resulta a adição P_1 e $-P_1$ pertencente a uma mesma reta vertical? A resposta é o ponto no infinito O. Temos que: Se traçarmos a reta ligando P_1 e $-P_1$, tal reta parece não encontrar a curva elíptica novamente, ou seja, a reta r encontra a curva no infinito. Então, temos que $P_3 = P_1 + (-P_1) = O$, como foi visto na observação 3.2.7.

O cálculo da soma de pontos em uma curva elíptica é descrito pelo algoritmo a seguir.

Algoritmo. Algoritmo de soma de pontos de uma curva elíptica.

1: Se $P_1 = O$, então $P_1 + P_2 = P_2$.

2: Senão, se $P_2 = O$, então $P_1 + P_2 = P_1$.

3: Senão, escreva $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$.

4: Se $x_1 = x_2$ e $y_1 = -y_2$, então $P_1 + P_2 = O$.

5: Senão, faça

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{se } P_1 \neq P_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{se } P_1 = P_2 \end{cases}$$

6: Compute $x_3 = \lambda^2 - x_1 - x_2$.

7: Compute $y_3 = \lambda(x_1 - x_3) - y_1$.

Saída: $P_1 + P_2 = (x_3, y_3)$.

3.2.3 Pontos de ordem finita

Definição 3.2.14. 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.

É interessante encontrar pontos P de ordem finita em uma curva elíptica, especialmente para curvas definidas sobre $\mathbb{Q}$.

Exemplo 3.2.15. Encontrar a ordem de $P = (2, 3)$ em $y^2 = x^3 + 1$ sobre os racionais.

Aplicaremos as fórmulas: $x_3 = \lambda^2 - x_1 - x_2$, $y_1 = \lambda x_1 + v$,$y_3 = x_3 + v$ e $\lambda = \frac{f'(x)}{2y}$. Encontramos inicialmente $2P$: $P + P$

$$\lambda = \frac{f'(x)}{2y} = \frac{3x^2}{2y} = \frac{3 \cdot 2^2}{2 \cdot 3} = 2.$$

$$x_3 = 4 - 2 - 2 = 0.$$

$$v = y_1 - \lambda x_1 = 3 - 2 \cdot 2 = -1.$$

$$y_3 = -1.$$

Portanto, $P + P = 2P = (0, 1)$.

Calculando $2P + P$.

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = 1.$$

$$x_3 = 1 - 0 - 2 = -1.$$

$$y_3 = -1 + 1 = 0.$$

Portanto $3P = (-1, 0)$.

Calculando $4P = 3P + P$, aplicando as fórmulas de maneira análoga, encontramos $4P = (0, -1)$.

Daí, temos $4P = -2P$ ou ainda $6P = O$, concluindo, assim, que P tem ordem 6.

Para mais detalhes sobre pontos de ordem finita, *cf.* [15].

Capítulo 4

Aplicações de Curvas Elípticas para o Ensino Médio

Neste capítulo, veremos algumas aplicações de Curvas Elípticas para o Ensino Médio, utilizando a teoria dos capítulos II e III e buscando uma linguagem mais direcionada a este nível de ensino.

As Curvas Elípticas são curvas planas cujas equações são polinômios com duas variáveis de grau 3 que possuem uma estrutura aritmética muito rica: seus pontos, juntamente com a operação binária definida no capítulo 3, 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 e secantes e interseção com a curva. As fórmulas para calcular a soma de dois pontos pertecentes a uma curva elíptica que foi obtida no cápítulo III podem ser aplicadas no Ensino Médio, uma vez que os pré-requesitos para dedução destas também se encontram no Ensino Médio.

Veremos nas atividades com curvas elípticas que podemos explorar contéudos do Ensino Médio: plano cartesiano, polinômios, geometria plana, geometria analítica, interseção de reta e cúbica, teoria dos números (números racionais), além de servir como introdução à ideia de operações abstratas em estruturas algébricas.

Vale salientar que a maioria das figuras deste trabalho e, consequentemente, das atividades que aplicaremos foi construída com o auxílio do aplicativo Geogebra.

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. Em seguida, veremos as atividades com aplicações de curvas elípticas.

4.1 Atividade I

Esta atividade é 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. Por indução finita, temos que:

$$1^2 + 2^2 + 3^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6}. \tag{4.1.1}$$

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

$$y^2 = \frac{x(x+1)(2x+1)}{6}. \tag{4.1.2}$$

A equação (4.1.2) 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 $y^2 = \frac{x(x+1(2x+1)}{6}$, obtendo-se:

$$x^2 = \frac{x(x+1(2x+1)}{6}, \tag{4.1.3}$$

cujo desenvolvimento resulta na igualdade.

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0. \tag{4.1.4}$$

A equação (4.1.4) 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 (4.1.4)), 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 (4.1.2) , 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 $(\frac{1}{2}, -\frac{1}{2})$ 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 (4.1.2). 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:

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

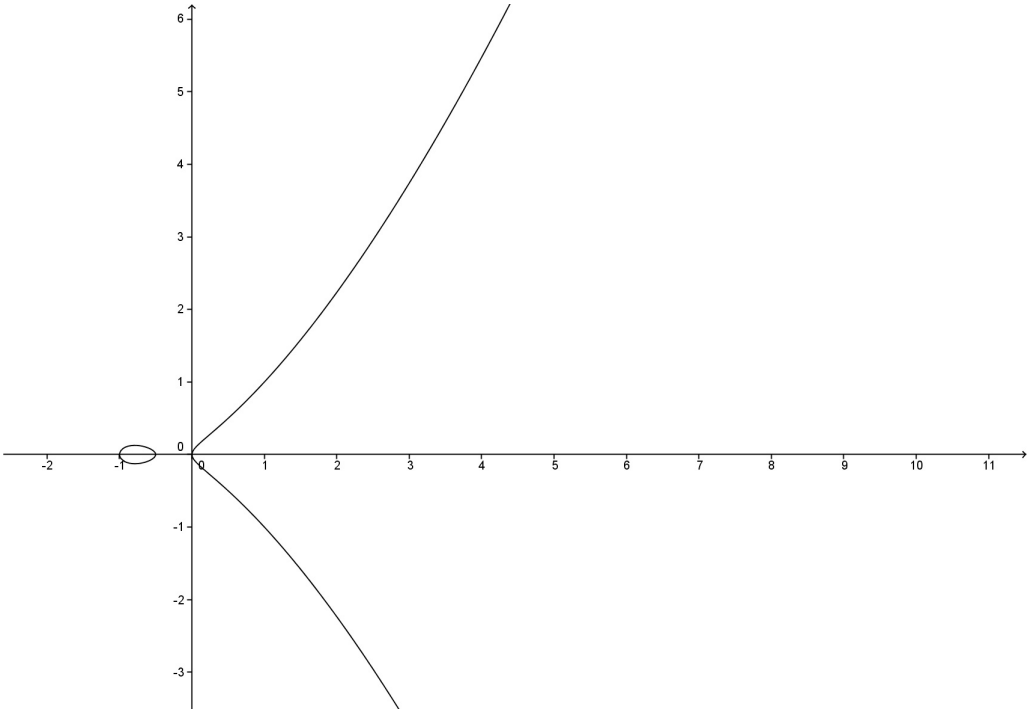


Figura 4.1: Traço da Curva Elíptica

Observação 4.1.1. Podemos comprovar pelo traço da curva, a simetria em relação ao eixo Ox, ou seja, dado um ponto (x, y) pertencente ao traço, o ponto $(x, -y)$ também pertence.

4.2 Atividade II

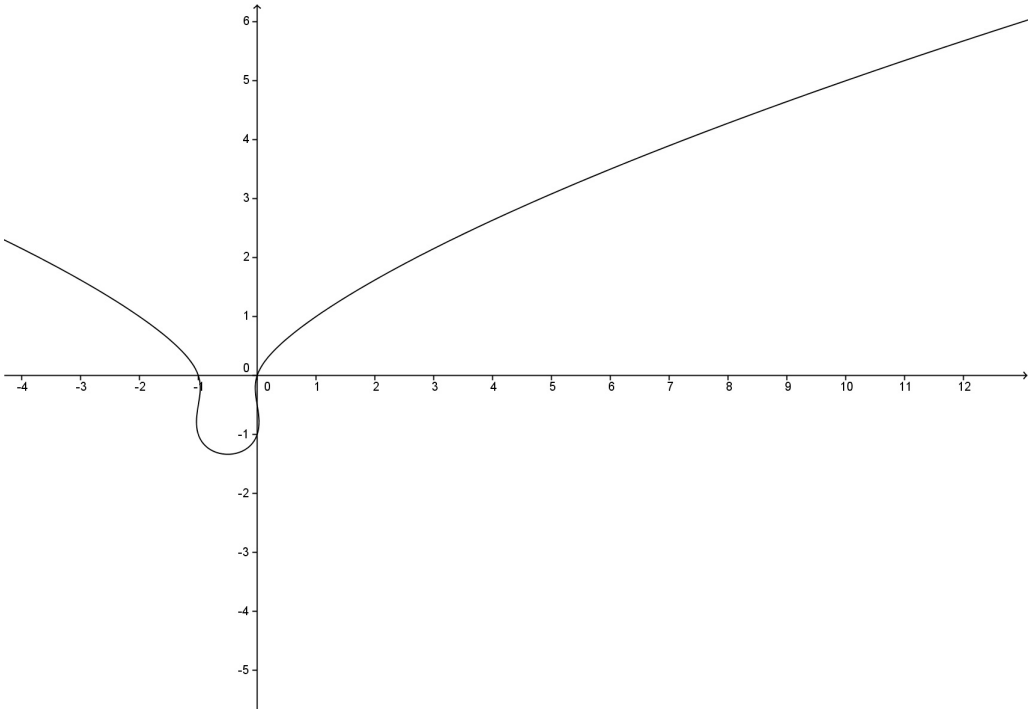
Podemos citar ainda exemplos de problemas da *Teoria Elementar dos Números* que expressam curvas elípticas.

O professor do Ensino Médio pode falar um pouco da história dos problemas elementares dos números, em seguida expressá-los na linguagem matemática, mostrar que representam curvas elípticas, justificando com as definições vistas no capítulos II e III, construindo o traço para visualização das curvas, sua simetria e escolher pontos pertencentes às curvas, fazendo um processo análogo ao exposto na Atividade I.

Exemplo 4.2.1. *Encontrar todos os pares dos números naturais x e y tais que a soma dos primeiros x números naturais é igual à soma dos quadrados dos primeiros y números naturais.*

Escrevendo este problema na linguagem algébrica, temos:

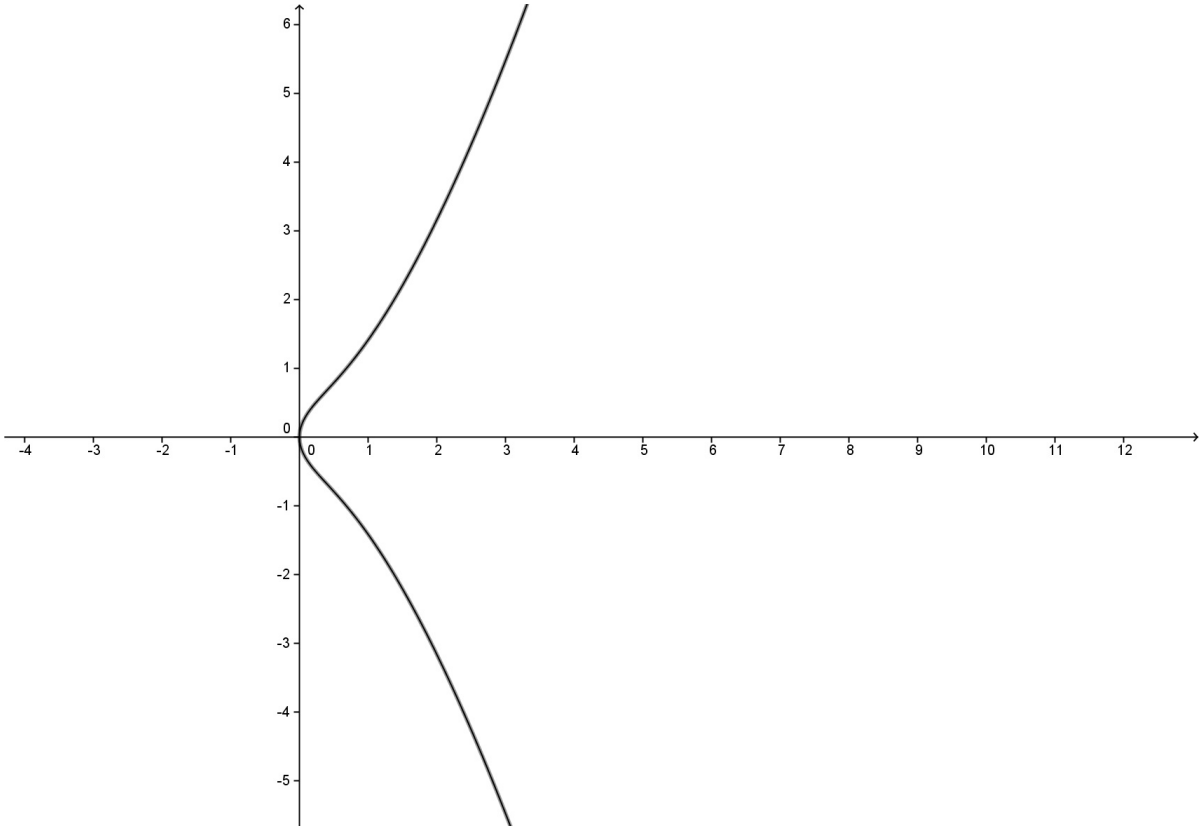
$$\frac{x(x+1)}{2} = \frac{y(y+1)(2y+1)}{6}.$$
$$3x(x+1) = y(y+1)(2y+1).$$



Exemplo 4.2.2. *Quando é que a soma de um número racional e o cubo desse mesmo número racional é o quadrado de um número racional?*

Na linguagem algébrica:

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



Exemplo 4.2.3. *Mostrar que a equação*

$$x^3 + y^3 = z^3$$

não tem soluções (de números) naturais (Último Teorema de Fermat) para expoentes três.

Notemos que não podemos construir o traço de $x^3 + y^3 = z^3$ no plano. Portanto, trabalharemos com algumas transformações.

Considerando x, y e $z \in \mathbb{Z}_+^*$. $(x : y : z)$ é solução de $x^3 + y^3 = z^3 \iff (\frac{x}{z} : \frac{y}{z} : 1)$ é solução de $x^3 + y^3 = z^3$, pois $x^3 + y^3 = z^3 \iff (\frac{x}{z})^3 + (\frac{y}{z})^3 = 1$

$\therefore (\frac{x}{z}, \frac{y}{z})$ é solução de $x^3 + y^3 = 1$ com $\frac{x}{z}$, $\frac{y}{z} \in \mathbb{Q}_+^*$

Em seguida, construiremos o traço da curva com o problema reescrito: *Mostrar que a equação*

$$x^3 + y^3 = 1$$

não tem soluções (de números) racionais positivos.

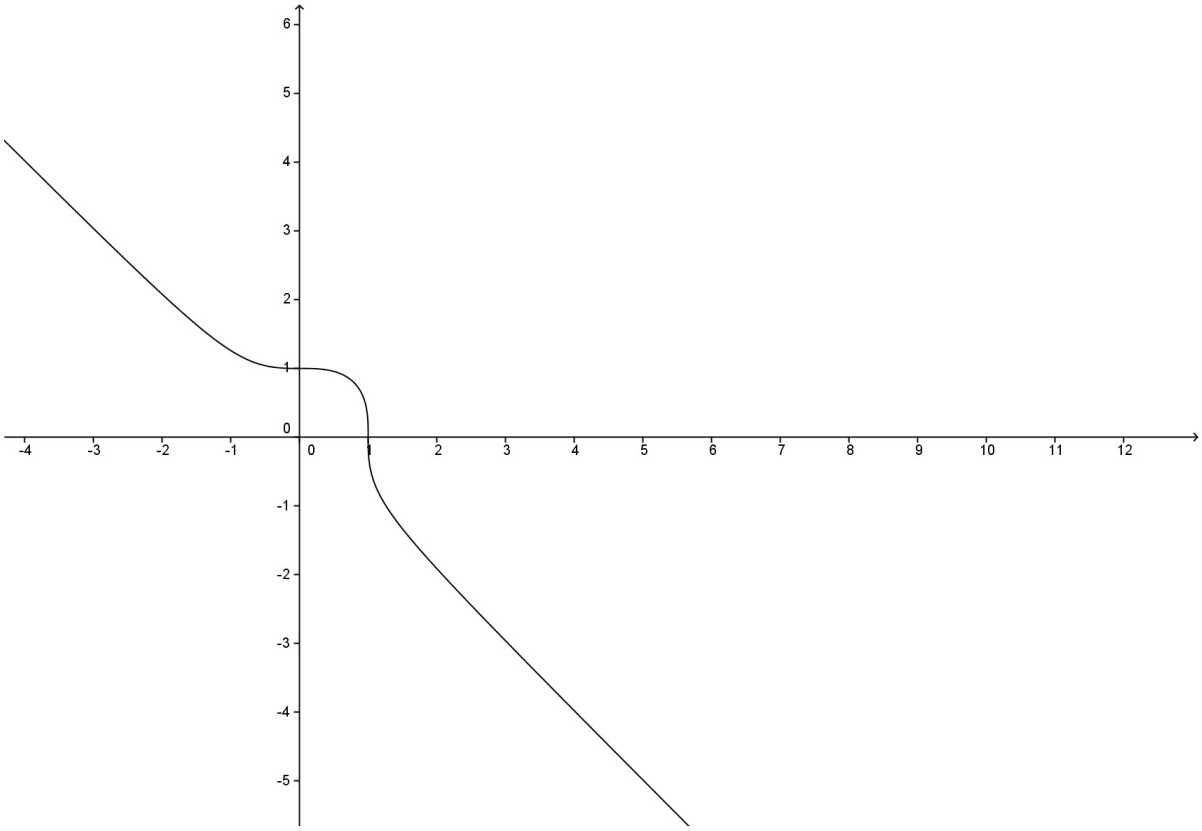


Figura 4.2: Traço de $x^3 + y^3 = 1$

4.3 Atividade III

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, incluindo o caso mais sutil que é somar pontos coincidentes (em que o professor poderá explorar a ideia intuitiva de limite) e ainda visualizar no traço da curva a operação de grupo da curva. É uma atividade também aplicável no Ensino Superior. 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 algumas propriedades que utilizaremos.

Considere a curva

$$y^2 = x^3 - 36x, \tag{4.3.1}$$

uma curva algébrica plana de grau 3 chamada de *cúbica*, em especial *elíptica*, pois atende à forma da equação (3.2.1).

Sejam $P = (-3, 9)$ e $Q = (-2, 8)$ pontos pertencentes a esta cúbica. Vamos deteminar $P+Q$.

Como a curva (4.3.1) está na forma (3.2.3) vista no Capítulo III, 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:

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

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

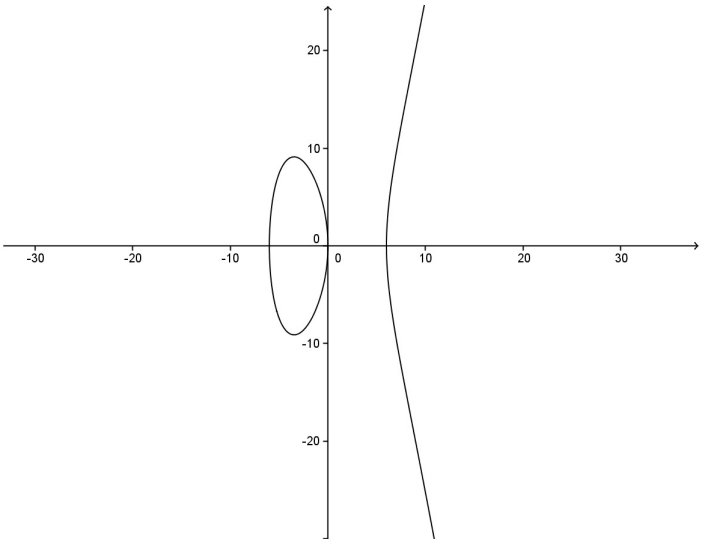
Temos $P + Q = -P * Q = (x_3, -y_3)$.

$P + Q = (6, 0)$.

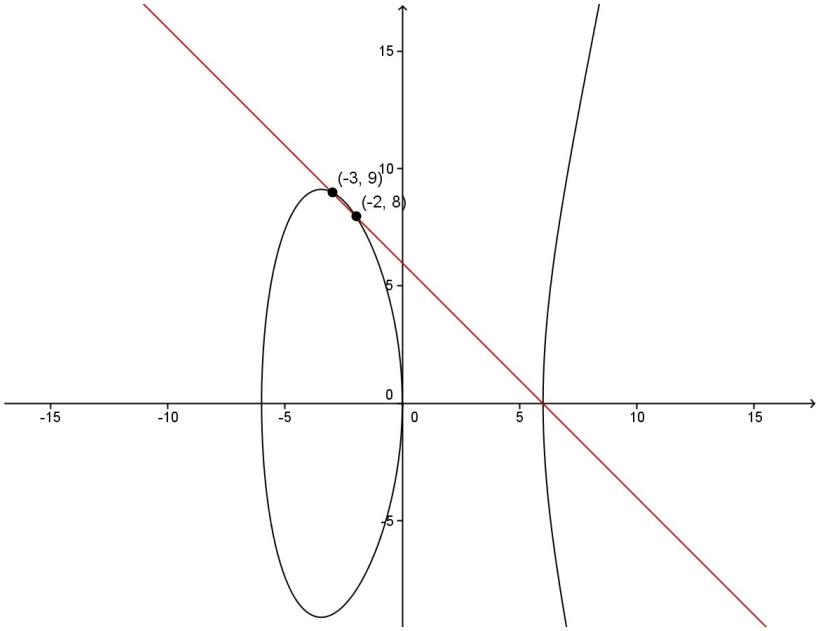
Poderíamos ainda calcular $P + (-Q)$, uma vez que $(-Q)$ é o oposto de Q.

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, incialmente construimos o 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 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.

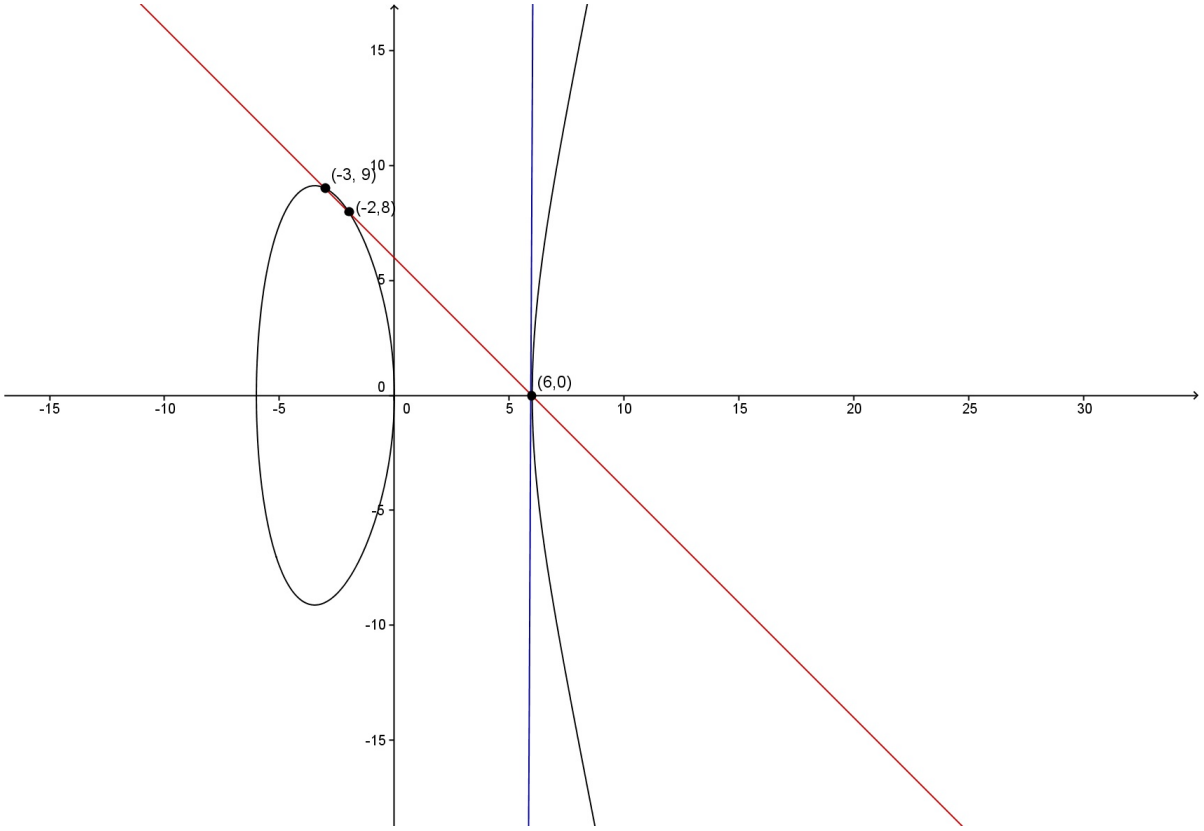


Figura 4.3: Soma de pontos

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 $y^2 = x^3 - 36x$ (já sabemos pelo Teorema de Bezout 2.3.28 que uma reta encontra uma cúbica em geralmente 3 pontos). Substituindo $y = -x + 6$ na equação (4.3.1), temos:

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

$$36 - 12x + x^2 = x^3 - 36x.$$

$$-x^3 + x^2 + 24x + 36 = 0.$$

$$x^3 - x^2 - 24x - 36 = 0. \tag{4.3.2}$$

Como a equação (4.3.2) 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:

$$-(a+b+c) = -1.$$

$$a+b+c = 1.$$

$$-3 - 2 + x = 1.$$

$$x = 6.$$

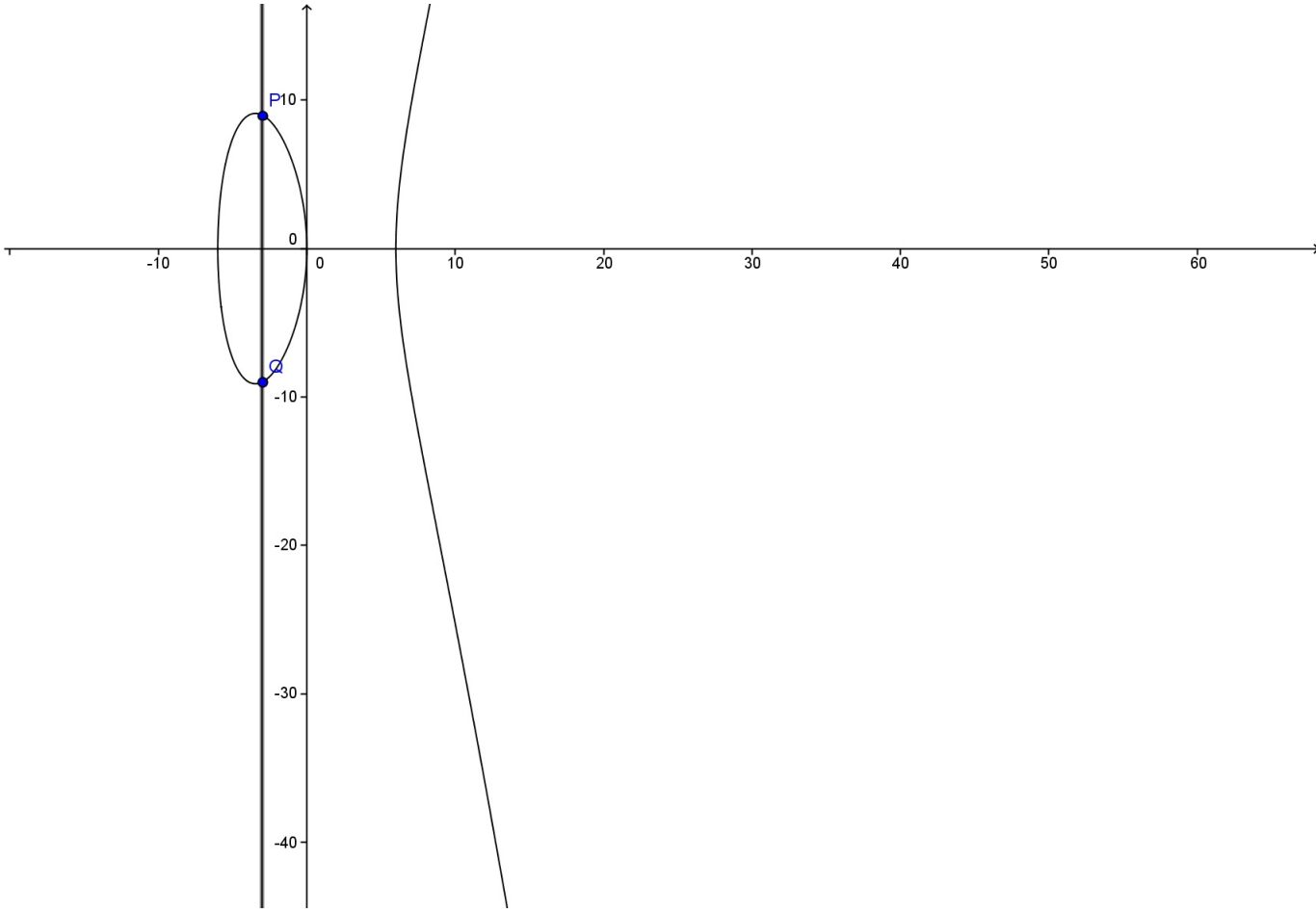
Substituindo na equação da reta o valor de $x = 6$, temos que $y = -6 + 6 = 0$ ou ainda $y^2 = 6^3 - 36 \cdot 6 = 216 - 216 = 0$. Assim, encontramos uma nova solução a partir de duas soluções dadas, a solução $(6, 0)$, que também pertence à curva elíptica

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

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: $y^2 = x^3 - 36x$ e a reta determinada por esses pontos.



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 2.3.11, 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 $(P + Q) + R = P + (Q + R)$.

Os pontos racionais pertencentes a uma curva elíptica satisfazem as seguintes propriedades:

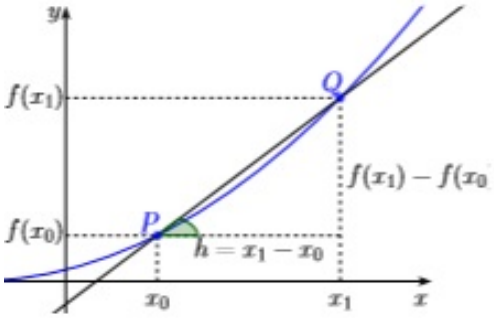
- comutatividade
- existência de elemento neutro
- existência de elemento oposto
- associatividade

Finalmente, calcularemos $P + P = 2P$. Utilizaremos a fórmula:

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}. \tag{4.3.3}$$

Todavia, não podemos calcular o limite de $f(x)$ diretamente no Ensino Médio. Antes de utilizar a fórmula (4.3.3), veremos a ideia intuitiva da definição de limite. Veremos abaixo como determinar $f'(x)$:

Seja $f(x)$ uma função e seja $x = x_0$ um ponto do seu domínio. Seja $x_1 = x_0 + h$. Observemos o gráfico de uma função $f(x)$, onde traçamos a reta secante que passa pelos pontos $P = (x_0, f(x_0))$ e $Q = (x_1, f(x_1))$.

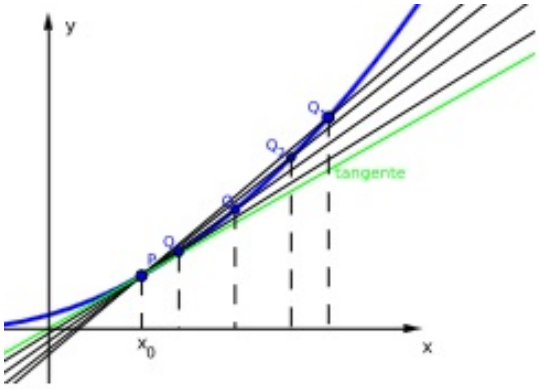


O coeficente angular ou inclinação da reta secante à curva passando pelos pontos $P = (x_0, f(x_0))$ e $Q = (x_1, f(x_1))$ é dado por:

$$\frac{f(x_1) - f(x_0)}{x_1 - x_0} = \frac{f(x_0 + h) - f(x_0)}{h}$$

Tomando h cada vez mais próximo de zero, obtemos retas secantes que cortam a curva em dois pontos P e Q_i cada vez mais próximos. Observemos a figura a seguir.

Intuitivamente, percebemos que, quando $x_0 + h$ se aproxima de x_0, os pontos $f(x_0 + h)$ e $f(x_0)$, onde a secante corta a curva, ficam cada vez mais próximos e, assim, estas curvas secantes se aproximam cada vez mais da tangente em x_0.



Quando h se aproxima de zero, se o quociente

$$\frac{f(x_0+h)-f(x_0)}{h},$$

que representa o coefiente angular da reta secante que passa por $(x_0, f(x_0))$ e $(x_0+h, f(x_0+h))$, se aproxima de um determinado valor, esse, intuitivamente, deverá ser o coeficiente angular da reta tangente.

Assim, como estamos calculando a adição de pontos coincidentes e se tratando de uma atividade direcionada ao Ensino Médio, usaremos a ideia de aproximação para o cálculo de λ, coeficiente angular da reta tangente.

Calculemos o quociente abaixo:

$$\frac{f(x+h)-f(x)}{h} \tag{4.3.4}$$

com h bem próximo de zero.

Com $f(x) = x^3 - 36x$, temos que a fórmula (4.3.4) segue:

$$\frac{(x+h)^3-36(x+h)-(x^3-36x)}{h}.$$

$$\frac{x^3+3x^2h+3xh^2+h^3-36x-36h-x^3+36x}{h}.$$

$$\frac{3x^2h+3xh^2+h^3-36h}{h}.$$

$$\frac{h(3x^2+3xh+h^2-36)}{h}.$$

e, como estamos considerando h bem próximos de zero, temos:

$$3x^2 + 3xh + h^2 - 36.$$

se aproxima de

$$3x^2 - 36.$$

quando h se aproxima de zero.

Assim, o valor de λ na fórmula (4.3.3) será:

$$\lambda = \frac{3x^2 - 36}{2y}. \tag{4.3.5}$$

Substituindo $P = (-3, 9)$ em (4.3.5), encontramos

$$\lambda = \frac{3 \cdot (-3)^2 - 36}{2 \cdot 9} = \frac{-9}{18} = -\frac{1}{2}.$$

Assim,

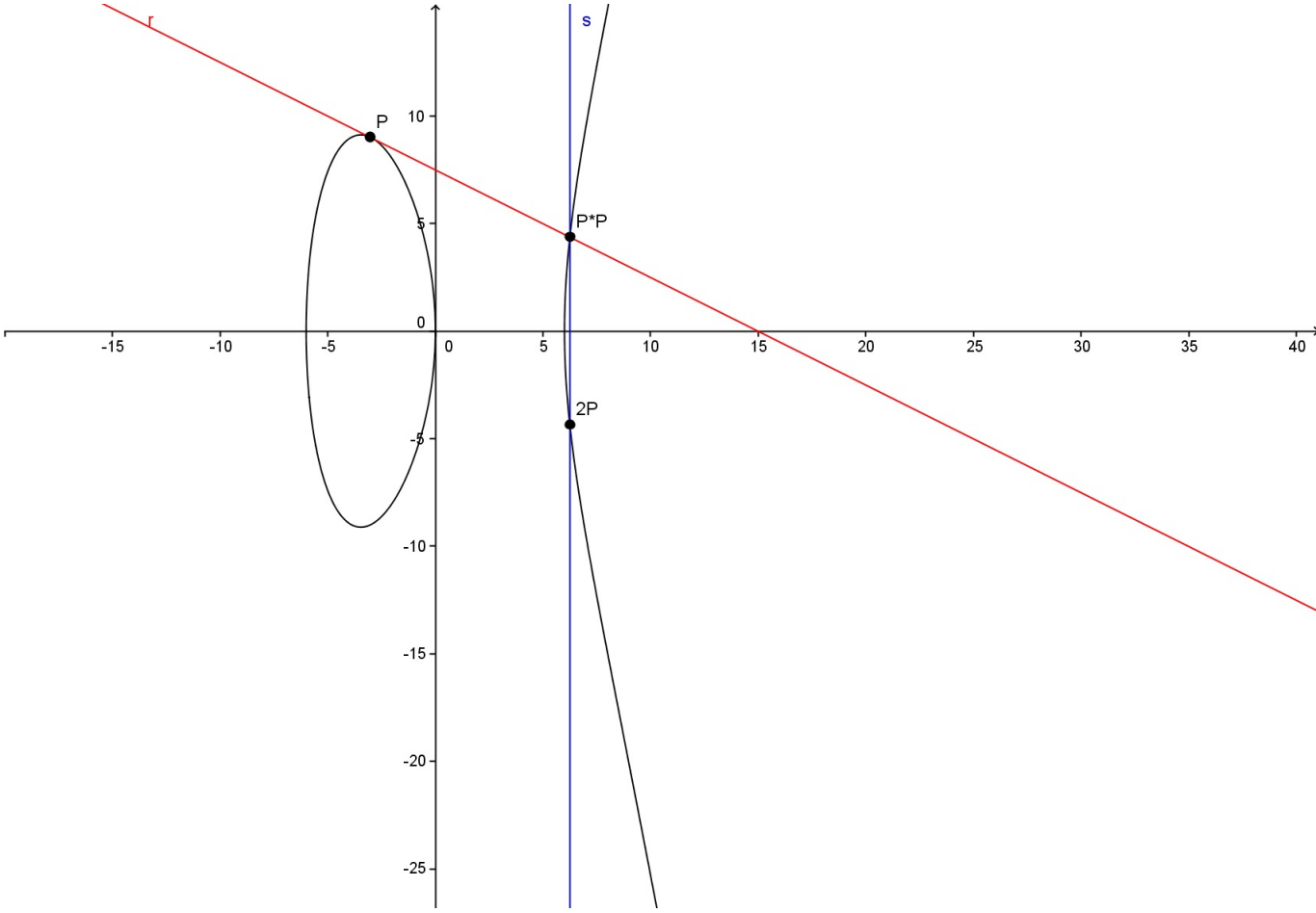
$$x_3 = \left(-\frac{1}{2}\right)^2 + 3 + 3 = \frac{25}{4}.$$

$$v = y_1 - \lambda x_1 = 9 + \frac{1}{2} \cdot (-3) = \frac{15}{2}.$$

$$y_3 = \lambda x_3 + v = -\frac{1}{2} \cdot \frac{25}{4} + \frac{15}{2} = -\frac{25}{8} + \frac{15}{2} = \frac{35}{8}.$$

Logo, $P + P = 2P = (x_3, -y_3) = \left(\frac{25}{4}, -\frac{35}{8}\right)$.

Visualizemos o ponto $P = (3, 9)$, $P * P = \left(\frac{25}{4}, \frac{35}{8}\right)$ e $2P = \left(\frac{25}{4}, -\frac{35}{8}\right)$ e as retas r tangente em P e a reta vertical s:



De forma análoga, poderíamos ainda encontrar $4P$ fazendo $2P + 2P$.

Observação 4.3.1. Caso esta atividade estivesse direcionada ao Ensino Superior, a diferença seria apenas que poderíamos fazer menos detalhes na parte da resolução referente aos pontos coincidentes porque limites e derivadas já fazem parte do currículo de Ensino Superior.

4.4 Atividade IV

Esta atividade é um exercício proposto do livro [10] (p. 407) das OBM 2001. Por se tratar de uma questão das Olímpiadas de Matemática, compreendemos que pode ser aplicado por professores no Ensino Médio. É um exercício que permite trabalhar a adição com pontos pertencentes a uma curva elíptica e também a multiplicação de um escalar por um ponto, bem como explorar a ideia de pontos de ordem finita. Há como trabalharmos com as propriedades(comutatividade, associatividade e principalmente a existência de elemento neutro).

Considere o ponto racional $P = (3, 8)$ na curva elíptica:

$$y^2 = x^3 - 43x + 166. \tag{4.4.1}$$

Calcule $2001P$.

Queremos calcular $\underbrace{P + P + \ldots + P}_{2001 \text{ vezes}}$.

Calculemos inicialmente $P + P$.

Utilizaremos o processo aplicado no exemplo anterior para adicionarmos dois pontos coincidentes:

$$\lambda = \frac{3x^2 - 43}{2y} \tag{4.4.2}$$

Substituindo as coordenadas de P na equação (4.4.2), temos:

$$\lambda = \frac{3 \cdot 3^2 - 43}{2 \cdot 8}.$$

$$\lambda = -\frac{16}{16} = -1.$$

Como $x_3 = \lambda^2 - x_1 - x_2$, $v = y_1 - \lambda x_1$ e $y_3 = \lambda x_3 + v$.

$$x_3 = (-1)^2 - 3 - 3 = -5.$$

$$v = 8 + 1 \cdot 3 = 11.$$

$$y_3 = (-1) \cdot (-5) + 11 = 16.$$

Segue que $P + P = (x_3, -y_3) = (-5, -16)$.

Calculemos $3P$. Como vale a comutatividade, podemos calcular $2P + P$ ou $P + 2P$.

Utilizando a opção $2P + P$: $(-5, -16) + (3, 8)$.

Como os pontos não são iguais, $\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8+16}{3+5} = 3$

$$x_3 = 3^2 + 5 - 3 = 11.$$

$$v = -16 - 3 \cdot (-5) = -1.$$

$$y_3 = 3 \cdot 11 - 1 = 32.$$

Assim, $3P = (11, -32)$.

Calculemos $4P = P + 3P$.

$(3, 8) + (11, -32)$.

$$\lambda = \frac{-32 - 8}{11 - 3} = -5.$$

$$v = 8 + 5 \cdot 3 = 23.$$

$$x_3 = 25 - 11 - 3 = 11.$$

$$y_3 = (-5) \cdot 11 + 23 = -32.$$

Logo, $4P = (11, 32)$.

Assim, encontramos que $4P = -3P$, somando $3P$ a ambos os membros, temos $4P+3P = O$, ou seja, $7P$ é o elemento neutro.

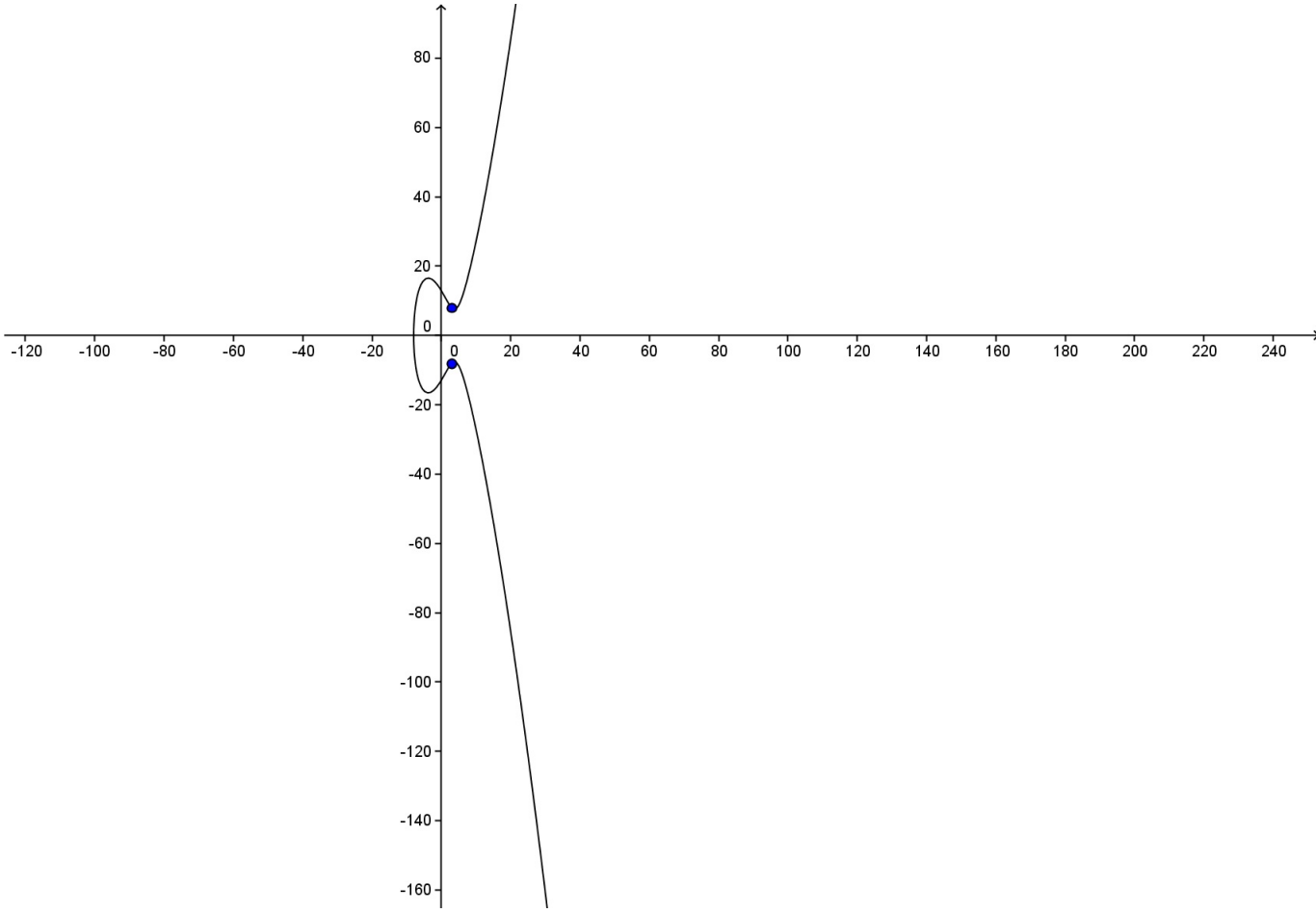
Queremos calcular o valor de $2001P$.

$2001P = 285 \cdot 7P + 6P = 285 \cdot O + 6P = 6P$

Somando $-P$ a ambos membros da equação: $7P = O$, segue-se que $6P = -P$.

Portanto $2001P = -P = (3, -8)$.

Faremos a seguir o traço da curva, localizando os pontos $P = (3, 8)$ e seu oposto $(3, -8) = 2001$, apenas para visualizar estes pontos.



Observação 4.4.1. Para o professor criar outras atividades semelhantes, é preciso encontrar novos pontos de ordem finita (*cf.* seção 3.2.3).

Ainda neste atividade, o professor poderia desenvolver geometricamente (com o auxílio do *software* Geogebra) a adição dos pontos utilizados nesta questão e conferir os resultados com álgebra utilizada.

4.5 Atividade V

Esta atividade é baseada em [13]. Como se trata de um artigo do Projeto Klein, é notável que apresente tópico relevante da Matemática que se conecte a conhecimentos matemáticos de nível médio, motivando com exemplos ou problemas estimulantes que interessam ao professor do Ensino Médio. A história deste artigo mostra a unidade notável da Matemática, começando pela forma como se apresenta na escola e terminando na investigação.

Trata-se de uma atividade em que o professor pode discutir e verificar propriedades da geometria plana, trigonometria, curvas no plano e em especial a procura de pontos na curva elíptica. Além disso, assim como as demais atividades, com a utilização do Geogebra, o professor pode explorar as particularidades dos pontos na curva, retas secantes, retas tangentes e interseção entre as curvas de forma dinâmica.

A atividade inicia-se com um questionamento que é foco de discussão entre professores e alunos do Ensino Médio:

Dois triângulos com lados iguais são necessariamente congruentes. Contudo, se tiverem o mesmo perímetro, não são necessariamente congruentes. E se tiverem a mesma área e o mesmo perímetro?

A resposta a este questionamento é: não são necessariamente congruentes.

Considere os dois triângulos abaixo:

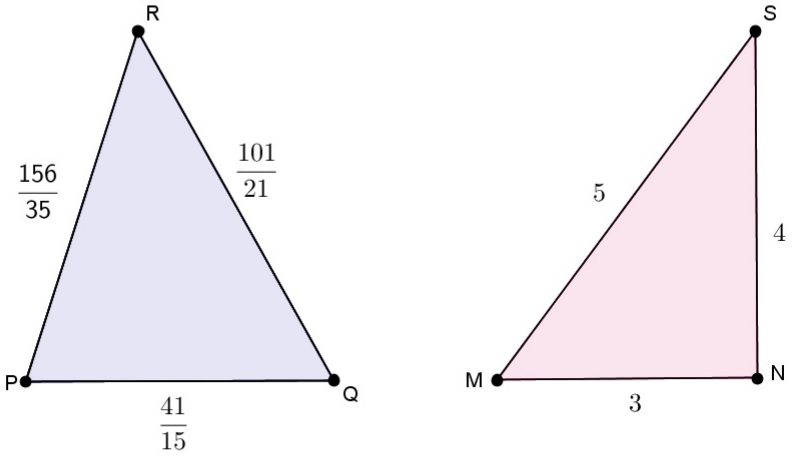


Figura 4.4: Dois triângulos não congruentes com a mesma área e o mesmo perímetro

O triângulo cujos lados medem 3, 4 e 5 tem a mesma área e o mesmo perímetro que o triângulo cujos lados medem $\frac{41}{15}$, $\frac{101}{21}$ e $\frac{156}{35}$. De fato, o perímetro vale:

$$\frac{41}{15}+\frac{101}{21}+\frac{156}{35}=\frac{287+505+468}{105}=\frac{1260}{105}=12=3+4+5.$$

Quanto a área, temos:

O triângulo de lados 3, 4 e 5, tem área $\frac{1}{2}\cdot 4\cdot 3=6$. Já para o triângulo de lados $\frac{41}{15}$, $\frac{101}{21}$ e $\frac{156}{35}$, usaremos a Fórmula de Herão para calcular a área. Sendo a, b e c os lados do triângulo.

$$A=\sqrt{s\cdot(s-a)\cdot(s-b)\cdot(s-c)}$$

onde $s=\frac{1}{2}(a+b+c)$ é o semiperímetro do triângulo. Assim,

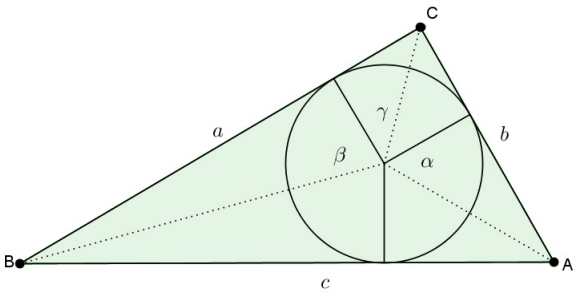
$$A=\sqrt{6\cdot(6-\frac{41}{15})\cdot(6-\frac{101}{21})\cdot(6-\frac{156}{35})}=6.$$

Portanto, exibimos um contraexemplo que justifica que triângulos que possuem a mesma área e o mesmo perímetro não são necessariamente congruentes.

Como o professor poderia encontrar outros contraexemplos como este? O segredo, segundo o autor do artigo, consiste em representar de forma apropriada o conjunto de todos os triângulos. No entanto, há várias formas de representar este conjunto; por exemplo, podemos representar o conjunto dos triângulos como um subconjunto dos ternos $(a, b, c) \in \mathbb{R}^3$ que correspondem às medidas dos três lados do triângulo, com algumas restrições, pois nem todos os termos de $\mathbb{R}^3$ corresponderão a triângulos, por exemplo, todas as coordenadas devem ser positivas.

Consideremos as coordenadas no espaço dos triângulos usando ângulos ao invés de de lados. De fato, qualquer triângulo tem uma circunferência inscrita e existe uma relação interessante entre o raio r desta cicunferência, a área A do triângulo e o semiperímetro s, respectivamente:

$$A = r \cdot s. \tag{4.5.1}$$



A equação (4.5.1) nos informa que, se dois triângulos têm a mesma área e o mesmo perímetro, então o raio das circunferências inscritas também é o mesmo. Portanto, quando estivermos à procura de dois triângulos com a mesma área e o mesmo perímetro, poderemos encontrá-los no conjunto de todos os triângulos circunscritos a uma dada circunferência fixa. Todavia, ao invés de comprimentos de lados para parametrizar este conjunto, utilizaremos os ângulos formados pelos três raios da circunferência, tal como a figura acima. Esta parametrização será bastante

interessante, pois nos permitirá encontrar dentro deste conjunto *curvas* que correspondem a uma família de triângulos com os mesmos valores de A e s. É fundamental ressaltar que estamos procurando criar outros contraexemplos como o que justificaram a negação do questionamento.

Vamos então expressar s em termos dos ângulos α, β e γ, e do raio r da circunferência inscrita. Os raios e os segmentos que ligam os vértices do triângulo original ao centro da circunferência dividem o triângulo original em seis triângulos retângulos. Como os segmentos de reta que unem os vértices ao centro bissectam os ângulos do triângulo original, estes triângulos dividem-se em três pares de triângulos congruentes. Considerando o comprimento da base de cada par e adicionando, temos:

$$\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}=\frac{\frac{a}{2}+\frac{b}{2}+\frac{c}{2}}{r}.$$

$$r\cdot\left(\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}\right)=\frac{a}{2}+\frac{b}{2}+\frac{c}{2}.$$

$$s=r\cdot\left(\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}\right). \tag{4.5.2}$$

Combinando as equações (4.5.1) e (4.5.2), resulta que, se a área A e o semiperímetro s são constantes, então também é constante a soma das seguintes tangentes:

$$r\cdot\left(\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}\right)=\frac{A}{r}.$$

$$\left(\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}\right)=\frac{A}{r^2}. \tag{4.5.3}$$

Pela (4.5.1), o valor de $r=\frac{A}{s}$, substituindo na equação (4.5.3), obtemos:

$$\operatorname{tg}\frac{\alpha}{2}+\operatorname{tg}\frac{\beta}{2}+\operatorname{tg}\frac{\gamma}{2}=\frac{s^2}{A}. \tag{4.5.4}$$

Agora, faremos uma transformação muito interessante, que é transformar a equação (4.5.4) numa equação que define uma *curva* no plano.

Considere $x=\operatorname{tg}\frac{\alpha}{2}$, $y=\operatorname{tg}\frac{\beta}{2}$ e $z=\operatorname{tg}\frac{\gamma}{2}$. Como, $\alpha+\beta+\gamma=2\pi$, temos:

$$\frac{\gamma}{2}=\pi-\frac{\alpha}{2}-\frac{\beta}{2},$$

logo,

$$z=\operatorname{tg}\frac{\gamma}{2}=\operatorname{tg}\left(\pi-\frac{\alpha}{2}-\frac{\beta}{2}\right)=-\operatorname{tg}\left(\frac{\alpha}{2}+\frac{\beta}{2}\right)=-\frac{x-y}{1-xy}.$$

Assim, se k for a constante $\frac{s^2}{A}$, a equação (4.5.4) pode ser reescrita da seguinte forma:

$$x+y-\frac{x-y}{1-xy}=k.$$

$$x-x^2y+y-xy^2-x-y=k-kxy.$$

com $xy \neq 1$

$$-x^2y - xy^2 = k - kxy.$$

$$x^2y + xy^2 - kxy = -k. \tag{4.5.5}$$

Qualquer triângulo com aréa A e semiperímetro s determina um ponto nesta curva e cada ponto desta curva numa determinada região do plano corresponde a um triângulo. A região corresponde a ângulos que de fato fazem sentido na figura, nomeadamente a ângulos que satisfazem $\alpha + \beta + \gamma = 2\pi$ e $0 < \alpha, \beta, \gamma < \pi$, que corresponde à região definida por $x > 0$, $y > 0$ e $xy > 1$ (uma vez que $x > 0$).

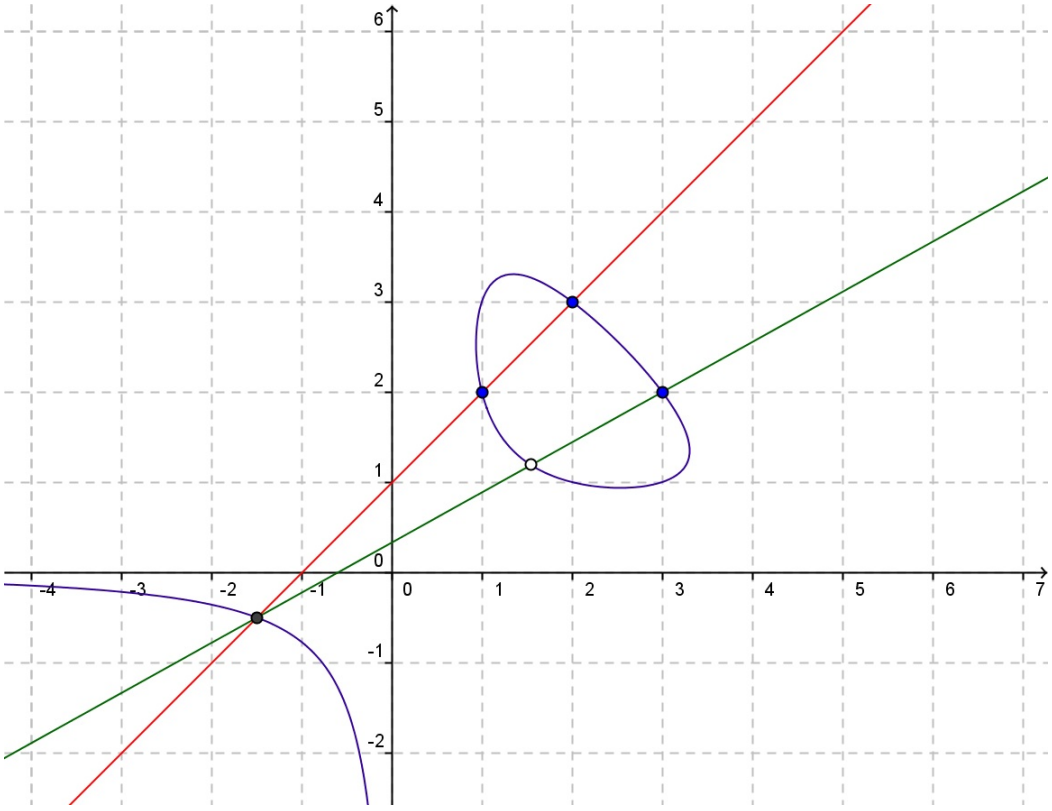


Figura 4.5: A curva dos triângulos.

A figura acima representa esta curva para $k = 6$, o valor que corresponde ao triângulo com lados 3, 4 e 5. Qualquer ponto na parte desta curva que se situa no primeiro quadrante corresponde a um triângulo cujos lados são $a = x + y$, $b = y + z$ e $c = z + x$. Em particular, os pontos $(1, 2)$, $(2, 1)$, $(2, 3)$, $(3, 2)$, $(1, 3)$, $(3, 1)$ correspondem todos ao triângulo com lados 3, 4 e 5, com os lados tomados por ordem diferente.

Como a curva representada pela equação (4.5.5) é definida por uma equação do terceiro grau, em particular uma curva eliptica, conhecemos alguns métodos para encontrar pontos nesta curva. Como a (4.5.5) não está na forma de Weierstrass, não podemos utilizar as fórmulas, então utilizaremos o método da secante, o mesmo da Atividade I. Dois pontos na curva determinam uma

secante que corta a curva num outro ponto; já conhecemos seis pontos na curva, portanto existem várias possibilidades pra determinarmos secantes e, conhecendo mais pontos, temos ainda mais possibilidades. Na verdade, a curva contém infinitos pontos com coordenadas racionais. Interessam aqui especificamente aqueles pontos no primeiro quadrante.

A seguir, utilizaremos o procedimento da secante.

Consideremos os pontos na curva: $\left(-\frac{3}{2}, -\frac{1}{2}\right)$ e $(3, 2)$. A reta determinada por estes dois pontos é:

$$y = \frac{5}{9}x + \frac{1}{3}. \tag{4.5.6}$$

Substituindo a equação (4.5.6) na curva:

$$x^2y + xy^2 - 6xy = -6$$

$$x^2 \cdot \left(\frac{5}{9}x + \frac{1}{3}\right) + x \cdot \left(\frac{5}{9}x + \frac{1}{3}\right)^2 - 6 \cdot x \cdot \left(\frac{5}{9}x + \frac{1}{3}\right) = -6.$$

$$\frac{5}{9}x^3 + \frac{1}{3}x^2 + x \cdot \left(\frac{25}{81}x^2 + \frac{10}{27}x + \frac{1}{9}\right) - \frac{30}{9}x^2 - \frac{6}{3}x = -6.$$

$$\frac{5}{9}x^3 + \frac{1}{3}x^2 + \frac{25}{81}x^3 + \frac{10}{27}x^2 + \frac{1}{9}x - \frac{30}{9}x^2 - \frac{6}{3}x = -6.$$

$$\frac{15x^3 + 27x^2 + 25x^3 + 30x^2 + 9x - 270x^2 - 162x}{81} = -\frac{486}{81}.$$

$$70x^3 - 213x^2 - 153x + 486 = 0.$$

$$(70x^2 - 3x - 162) \cdot (x - 3) = 0.$$

$$x = 3.$$

ou

$$70x^2 - 3x - 162 = 0.$$

$$\triangle = 45369.$$

$$x = \frac{3 \pm 213}{140}.$$

$$x = \frac{216}{140} = \frac{54}{35}.$$

ou

$$x = -\frac{210}{140}.$$

o último valor não nos interessa. Com $x = \frac{54}{35}$, substituimos na equação (4.5.6) e encontamos $y = \frac{25}{21}$.

Assim, somos conduzidos ao ponto $\left(\frac{54}{35}, \frac{25}{21}\right)$, que corresponde ao triângulo de lados:

$$a = \frac{54}{35} + \frac{25}{21} = \frac{287}{105} = \frac{41}{15}.$$

$$b = y + z$$

Todavia, $x + y + z = 6$.

$$\frac{54}{35} + \frac{25}{21} + z = 6.$$
$$\frac{162 + 125}{105} + z = 6.$$
$$z = -\frac{287}{105} + 6 = \frac{343}{105}.$$

Assim,

$$b = y + z = \frac{25}{21} + \frac{343}{105} = \frac{125 + 343}{105} = \frac{156}{35}.$$
$$c = z + x = \frac{343}{105} + \frac{54}{35} = \frac{343 + 162}{105} = \frac{505}{105} = \frac{101}{21}.$$

Observação 4.5.1. O método da secante funciona em qualquer cúbica no plano, em especial nas curvas elípticas.

Capítulo 5

Conclusão

Esse trabalho teve como foco principal uma introdução a Teoria das Curvas Elípticas. Para tanto, realizamos um estudo das curvas algébricas planas afins e projetivas.

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.

Do ponto de vista teórico-metodológico, foi possível efetuar um estudo cuidadoso do comportamento das curvas elípticas abordando as definições e as propriedades a ela inerentes. Mesmo considerando apenas a parte introdutória desta teoria, mostramos a rica estrutura aritmética dos pontos racionais pertencentes as estas curvas, verificando suas propriedades algebricamente e geometricamente.

Foi enriquecedor também, neste trabalho, buscar, a partir da teoria desenvolvida, aplicações para o Ensino Médio. Assim, desenvolvemos atividades com curvas elípticas em conexão com contéudos do ensino medio, tais como: plano cartesiano, interseção entre curvas, geometria plana, geometria analítica, trigonometria, entre outros. Utilizamos o *software* gratuito Geogebra para a construção da maioria das figuras para uma melhor compreensão das atividades.

Eventualmente, o desenvolvimento na íntegra de Curvas Elípticas é algo que requer um tratamento muito mais aprofundado do que foi dado neste trabalho, inclusive um estudo mais amplo da Geometria Projetiva.

5.1 Trabalhos Futuros

- Inicialmente, o segundo capítulo deste trabalho pode contribuir para um mini-curso de Geometria Projetiva;
- Pode-se desenvolver atividades tais como as propostas no capítulo IV, porém direcionadas

ao Ensino Superior(por exemplo: aplicações para cursos de Estruturas Algébricas, Cálculo e Teoria dos Números);

- Desenvolver atividades com Curvas Elípticas e aplicações na Computação;
- Aplicar o software *Geogebra* no tratamento geométrico das operações com pontos racionais de uma Curva Elíptica;
- Realizar um estudo mais aprofundado de Curvas Projetivas;
- Desenvolver a prova do Teorema de L. Mordell e A. Weil mostrando que o grupo dos pontos racionais de uma curva elíptica é um grupo abeliano finitamente gerado.

Referências Bibliográficas

[1] BOYER, Carl B. *História da Matemática*. Traduzido por Elza F. Gomide. São Paulo: Blucher,1996.

[2] BRANDT, Silva Tereza, Carla Montorfano. *O software Geogebra como Alternativa no ensino da geometria em um mini curso para professores*. Disponível em: http://www.diaadiaeducacao.pr.gov.br. Acesso em: 02. fev. 2014.

[3] DOMINGUES, Hygino H. e IEZZI, Gelson. *Álgebra Moderna*. São Paulo: Atual, 1982.

[4] 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.

[5] GARCIA, Arnaldo; LEQUAIN, Yves. *Elementos de Álgebra*. Rio de Janeiro: Impa, 2008.

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

[7] HEFEZ, Abramo. *Polinômios e Equações Algébricas*. Rio de Janeiro: SBM, 2012 (Coleção Profmat; 4).

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

[9] LIMA, Elon Lages. *Geometria Analítica e Álgebra Linear*. Rio de Janeiro: Impa, 2001 (Coleção Matemática Universitária).

[10] 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).

[11] NETO, Aref Antar *et al. Introdução ao Cálculo Diferencial e Integral*. Fortaleza: Ed. Vestseller, 2011 (Noções de Matemática; v.8).

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

[13] RALHA, Elfrida. *Os Triângulos de Herão e as curvas elípticas*. Disponível em: ⟨http://www.kleinproject.org/⟩ . Acesso em: 03. jan. 2014.

[14] RIBEMBOIM, Paulo. *Funções, Limites e Continuidade*. 1 ed. Rio de Janeiro: SBM, 2012 (Coleção Textos Universitários; 12).

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

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

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