NATHÁLIA MORAES DE OLIVEIRA

Curvas elípticas e o caso $n = 4$ da conjectura de Euler

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2014

NATHÁLIA MORAES DE OLIVEIRA

Curvas elípticas e o caso $n = 4$ da conjectura de Euler

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para obtenção do título de **MESTRE EM MATEMÁTICA.**

Área de Concentração: Matemática.
Linha de Pesquisa: Geometria Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2014

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da UFU , MG, Brasil

O48c 2014

Oliveira, Nathália Moraes de, 1986-
Curvas elípticas e o casa *n = 4* da conjectura de Euler / Nathália Moraes de Oliveira. - 2014.
65 f. : il.

Orientador: Victor Gonzalo Lopez Neumann.

Dissertação (mestrado) – Universidade Federal de Uberlândia, Programa de Pós-Graduação em Matemática.
Inclui bibliografia.

1. Matemática - Teses. 2. Curvas elípticas - Teses. 3. Números de Euler - Teses. I. Neumann, Victor Gonzalo Lopez. II. Universidade Federal de Uberlândia. Programa de Pós-Graduação em Matemática. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 152
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNA: Nathália Moraes de Oliveira.

NÚMERO DE MATRÍCULA: 11212MAT011.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Curvas elípticas e o caso $n = 4$ da conjectura de Euler.

ORIENTADOR: Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi APROVADA em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 21 de fevereiro de 2014, às 14h, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Victor Gonzalo Lopez Neumann UFU - Universidade Federal de Uberlândia	
Prof. Dr. Herivelto Martins Borges Filho USP - Universidade de São Paulo - São Carlos	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 21 de fevereiro de 2014.

Dedicatória

À minha família.

Agradecimentos

Agradeço, primeiramente a Deus, por sempre estar comigo e por tudo que colocou em meu caminho durante esses dois anos de mestrado;

Aos meus pais, Anilton Antonio Oliveira do Prado e Nara Moraes de Oliveira, por todo o apoio, seja ele emocional, sentimental ou financeiro, durante a realização deste trabalho;

Aos meus familiares, em especial minha avó Lásara e minha tia Nalva por serem pessoas tão especiais na minha vida e por tudo o que fizeram por mim;

Ao meu orientador, Victor Gonzalo Lopez Neumann, pelo apoio e pelas horas dedicadas a me auxiliar;

À minha amiga Fernanda, por todas as coisas maravilhosas que fez por mim nesses dois anos e por estar comigo nos momentos mais difíceis que enfrentei durante o mestrado;

Ao professor Cícero Fernandes de Carvalho, por todas as dicas, incentivo, pelas palavras de motivação e por aceitar fazer parte da banca.

Ao professor Herivelto Martins Borges Filho, por aceitar fazer parte da banca dessa dissertação.

Agradeço aos colegas da sala de estudos do mestrado, por toda ajuda e pelos momentos de descontração. Agradeço em especial, ao Murilo por ser sempre prestativo e disposto a ajudar.

Agradeço a todos, que de alguma forma contribuíram para que eu conseguisse concluir este trabalho.

OLIVEIRA, N. M. *Curvas elípticas e o caso $n = 4$ da conjectura de Euler*. 2014. 65 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Do último teorema de Fermat sabemos que a equação $X^3+Y^3 = Z^3$ não possui soluções inteiras não triviais. Euler conjecturou em 1769 que este resultado pode ser generalizado aumentando a potência e o número de variáveis. Neste trabalho damos um contra-exemplo para a conjectura de Euler no caso $n = 4$ mostrando que a equação $A^4+B^4+C^4 = D^4$ possui soluções inteiras não triviais. Para tal estudamos curvas algébricas planas, curvas elípticas e usamos resultados da teoria dos números, em especial sobre a reciprocidade quadrática. A reciprocidade quadrática é peça chave na escolha de uma curva elíptica particular, de tal forma que uma solução nesta curva elíptica, se torna uma solução não trivial da equação de Euler para $n = 4$. Por fim, a aritmética da curva elíptica nos permite encontrar infinitas soluções inteiras para $A^4 + B^4 + C^4 = D^4$.

Palavras-chave: Conjectura de Euler; Curvas elípticas; Reciprocidade quadrática.

OLIVEIRA, N. M. *Elliptic curves and the $n = 4$ case of Euler's conjecture*. 2014. 65 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

From Fermat's last theorem we know that the equation $X^3 + Y^3 = Z^3$ does not have nontrivial integral solutions. In 1769 Euler conjectured that this result may be generalized increasing the powers and the number of variables. In this work we give a counterexample to Euler's conjecture in the case of $n = 4$ showing that the equation $A^4 + B^4 + C^4 = D^4$ has nontrivial integral solutions. To do that we study plane algebraic curves, elliptic curves and use results from number theory, especially those on quadratic reciprocity. The quadratic reciprocity is the key factor in the choice of a particular elliptic curve, such that a solution in that elliptic curve becomes a nontrivial solution of the Euler's equation with $n = 4$. Finally, the arithmetic of the elliptic curves allows us to find infinite integral solutions for $A^4 + B^4 + C^4 = D^4$.

Keywords: Euler's conjecture; Elliptic curves; Quadratic reciprocity.

Sumário

Introdução

Um dos problemas mais famosos na matemática foi levantado por Pierre de Fermat (1601-1665), ele afirmou que não existem x, y, z inteiros positivos satisfazendo a equação

$$x^n + y^n = z^n, \quad n \geq 3.$$

Essa afirmação constava na margem de um de seus livros, Diophantus e é conhecida como o último teorema de Fermat. Muitos matemáticos se dedicaram a sua demonstração, Euler (1707-1783), por exemplo, demonstrou o caso $n = 3$, o que o motivou a conjecturar no ano de 1769 que a equação

$$A_1^n + \cdots + A_{n-1}^n = A_n^n \quad (n \geq 4),$$

não possui soluções inteiras não triviais. Em 1966, através de uma busca computacional, os matemáticos L. J. Lander e T. R. Parkin (ver [4]) , encontraram um contra-exemplo para o caso $n = 5$,

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Naquela época, foram feitas buscas computacionais de soluções inteiras para

$$A^4 + B^4 + C^4 = D^4,$$

porém não houve sucesso. Em 1988, usando técnicas de Geometria Algébrica e auxílio computacional, o matemático Noam D. Elkies (ver [2]) encontrou a primeira solução

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Este trabalho será dedicado a dar um contra-exemplo para o caso $n = 4$ dessa conjectura. Precisamos para isso, de conceitos básicos de geometria algébrica e teoria dos números.

No primeiro capítulo, veremos alguns conceitos e resultados básicos sobre curvas algébricas planas, em particular, veremos a definição de plano projetivo e curva plana projetiva. Estudamos ainda funções regulares e funções racionais e finalizamos este capítulo com o estudo de multiplicidades e enunciamos o teorema de Bézout, que será muito utilizado no desenvolvimento deste trabalho. Para a teoria desenvolvida neste capítulo utilizamos [11]. O segundo capítulo foi baseado em [1], [6], [9] e [10], nele abordamos o estudo de curvas elípticas e desenvolvemos nossa teoria com o objetivo de mostrar que o conjunto de pontos racionais desse tipo de curva forma um grupo, sendo assim, precisamos definir uma operação em $E(\mathbb{Q})$, onde $E(\mathbb{Q})$ denota o conjunto de pontos racionais de uma curva elíptica E. Esse grupo tem características muito interessantes, a saber, a ordem de um ponto de $E(\mathbb{Q})$ ou é infinita ou tem ordem $2, 3, \ldots, 10$ ou 12. Assim, se um ponto diferente do elemento neutro, não é de ordem menor ou igual a 12, então esse ponto gera infinitos pontos racionais. O estudo de curvas elípticas será de extrema importância ao buscarmos nosso contra-exemplo para $A^4 + B^4 + C^4 = D^4$.

No capítulo 3, o qual a referência utilizada é [5], estudamos algumas noções de teoria dos números. Provamos o teorema de Legendre, um importante resultado, que fornece condições necessárias e suficientes para que uma equação da forma $aX^2 + bY^2 + cZ^2 = 0$, possua solução

inteira não trivial. Antes de chegar a esse resultado falamos sobre reciprocidade quadrática, que terá destaque em nosso último capítulo.

Por fim, trabalhamos para obter um contra-exemplo para $A^4+B^4+C^4 = D^4$, ou equivalentemente, buscamos pontos racionais sobre a superfície $r^4+s^4+t^4 = 1$. Para isto, parametrizamos esta superfície através de um feixe de curvas de gênero um. Quando uma destas curvas possui um ponto racional, ela é chamada de curva elíptica. Este ponto racional gera o primeiro contra-exemplo para o caso $n = 4$ da conjectura de Euler e a estrutura de grupo da curva elíptica gera infinitos contra-exemplos, uma vez que provamos que este ponto não é de torção. Este capítulo é baseado no artigo de Noam D. Elkies [2].

Nathália Moraes de Oliveira
Uberlândia-MG, 21 de janeiro de 2014.

Capítulo 1

Curvas algébricas planas

De forma intuitiva, podemos dizer uma curva algébrica sobre um corpo $\mathbb{K}$, é o lugar dos pontos cujas coordenadas cartesianas satisfazem a uma dada equação polinomial

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

onde f é um polinômio não constante.

Tomando $f \in \mathbb{R}[x, y]$ então dizemos que a curva algébrica é uma curva algébrica plana real.

A definição formal se encontra na definição (1.1).

Exemplo 1.1 *(1) Reta :* $f(x, y) = ax + by + c$, $(a, b) \neq (0, 0)$.

(2) Círculo: o círculo de raio r *e centro* (a, b) *é o lugar dos pontos que satisfazem a equação*

$$(x - a)^2 + (y - b)^2 = r^2.$$

(3) Elipse: a elipse é o lugar dos pontos cujas distâncias a dois pontos fixos (digamos $(\pm c, 0)$*) tem soma soma constante* $2a$*. A elipse satisfaz*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \ ,$$

onde $b = \sqrt{a^2 - c^2}$.

(4) Hipérbole: a hipérbole é o lugar dos pontos cujas distâncias a dois pontos fixos, chamados focos (digamos $(\pm c, 0)$*), tem diferença constante* $2a$*. A hipérbole satisfaz*

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \ ,$$

onde $b = c^2 - a^2$.

(5) Parábola: a parábola é o lugar dos pontos equidistantes de um ponto fixo (foco, $(0, b)$,$b > 0$*) e de uma reta fixa (diretriz,* $y = -b$*). Sua equação é dada por*

$$x^2 = 4by \ .$$

(7) Seja $f(x, y) = x^2 + y^2$*. Fazendo* $f(x, y) = 0$*, temos que a curva algébrica possui um único ponto em* R^2*. Se permitirmos soluções complexas, a curva algébrica definida por* f *passa a ter infinitos pontos.*

1.1 O polinômio que define uma curva algébrica

Veremos a seguir em que condições dois polinômios representam a mesma curva algébrica. Vamos considerar $\mathbb{K}$ um corpo algebricamente fechado e de característica zero.

Proposição 1.1 *Sejam $f(x,y)$ e $g(x,y)$ polinômios com coeficientes em um corpo $\mathbb{K}$. Então $f(x,y)=0$ e $g(x,y)=0$ tem as mesmas soluções em $\mathbb{K}^2$ se, e somente se, os fatores irredutíveis de f e g são os mesmos.*

Demonstração:

($\Longrightarrow$) Seja $p(x,y) \in \mathbb{K}[x,y]$ um fator irredutível de $f(x,y)$. Temos que para cada $(x,y) \in \mathbb{K}^2$,

$$p(x,y)=0 \Longrightarrow g(x,y)=0, \tag{1.1}$$

pois p é um fator irredutível de f, logo $p(x,y)=0 \Longrightarrow f(x,y)=0$ e da hipótese

$f(x,y)=0 \Longrightarrow g(x,y)=0$.

Queremos provar que p também é um fator irredutível de g.

Chamemos $\mathbb{A}=\mathbb{K}[x]$, $\mathbb{F}=\mathbb{K}(x)$. Assim, $\mathbb{A}[y]=\mathbb{K}[x][y]=\mathbb{K}[x,y]$.

Como p é irredutível em $\mathbb{K}[x,y]=\mathbb{A}[y]$ (pela hipótese), então $p \notin \mathbb{K}$, pois se $p \in \mathbb{K}$ teríamos que p é invertível, pois $\mathbb{K}$ é corpo, mas isto não pode ocorrer. Isso implica que x ou y ocorre em p. Permutando x e y se necessário, podemos supor que y ocorre em p. Assim, podemos supor que $p \notin \mathbb{F}$.

Suponha por absurdo que $p \nmid g$ em $\mathbb{F}[y]$. Como $\mathbb{F}[y]$ é domínio de ideais principais e $p \nmid g$ então $mdc(p,g)=1$. Daí, existem a,$b \in \mathbb{F}[y]$, tais que $ap+bg=1$.

Temos que

$$a=a_0(x)+a_1(x)y+\cdots+a_r(x)y^r, \text{ onde } a_j(x)=\frac{a'_j(x)}{c(x)},\ a'_j(x) \in \mathbb{A} \text{ e } c(x) \in \mathbb{A}.$$

Assim,

$$a=\frac{a_1(x,y)}{c(x)}, \text{ onde } a_1(x,y)=a'_0(x)+a'_1(x)y+\cdots+a'_r(x)y^r.$$

De modo análogo, temos

$$b=\frac{b_1(x,y)}{d(x)}, \text{ onde } b_1(x,y) \in \mathbb{A}[y] \text{ e } d(x) \in \mathbb{A}.$$

Assim,

$$\begin{aligned} ap+bg=1 &\Longrightarrow \frac{a_1(x,y)}{c(x)}\cdot p+\frac{b_1(x,y)}{d(x)}\cdot g=1 \\ &\Longrightarrow a_1(x,y)d(x)p(x,y)+b_1(x,y)c(x)g(x,y)=c(x)d(x), \end{aligned}$$

Como $p(x,y) \notin \mathbb{A}$, então existem infinitos valores de x tais que $p(x,y)$ é um polinômio não constante em y. Assim existe uma sequência de pontos (x_n,y_n), tal que $p(x_n,y_n)=0$. Logo, por (1.1) temos $g(x_n,y_n)=0$, e assim $c(x_n)d(x_n)=0$. Absurdo, pois $c(x)d(x)$ possui um número finito de raízes. Isto é, $p \mid g$ em $\mathbb{F}[y]$. Como consequência do lema de Gauss, sabe-se que os fatores irredutíveis de g são os mesmos em $\mathbb{F}[y]$ e em $\mathbb{A}[y]$, logo $p \mid g$ em $\mathbb{A}[y]$.

($\Longleftarrow$) Por hipótese os fatores irredutíveis de f e g são os mesmos. Assim,

$$f(x,y) = 0 \Longrightarrow \exists p \text{ , fator irredutível de } f \text{ tal que } p(x,y) = 0.$$

Da hipótese p também é um fator irredutível de g, logo

$$g(x,y) = 0.$$

Analogamente, $g(x,y) = 0 \Longrightarrow f(x,y) = 0$.

□

A definição mais formal de curva é a seguinte:

Definição 1.1 *Uma curva algébrica plana afim é uma classe de equivalência de polinômios não constantes $f \in \mathbb{K}[x,y]$, módulo a relação de equivalência que identifica dois tais polinômios, se um é múltiplo do outro por uma constante diferente de zero.*

Dado um subcorpo $\mathbb{K}_0$ de $\mathbb{K}$, dizemos que a curva está definida sobre $\mathbb{K}_0$ se ela admitir uma equação com coeficientes em $\mathbb{K}_0$.

Observação 1.1 *(i) O conjunto de pontos de uma curva algébrica plana afim f sobre o corpo $\mathbb{K}$ é o conjunto de pontos de $\mathbb{K}^2$ que satisfazem $f(x,y) = 0$.*

(ii) O grau de uma curva f é o grau do polinômio que define a curva. Notação: ∂f.

Definição 1.2 *Dizemos que uma curva f é irredutível se o polinômio que define a curva é irredutível em $\mathbb{K}[x,y]$. As componentes irredutíveis de f são as curvas definidas por seus fatores irredutíveis. A multiplicidade de uma componente p de f é o expoente com que p aparece na fatoração do polinômio que define f em $\overline{\mathbb{K}}$.*

Observação 1.2 *Com a nova nomenclatura, a proposicao 1.1 nos diz que duas curvas tem o mesmo traço se, e somente se, possuem os mesmos fatores irredutíveis.*

Lema 1.1 *O polinômio $y^2 - p(x)$ é redutível, se e somente se, $p(x)$ é um quadrado em $\mathbb{K}[x]$.*

Demonstração:

($\Longrightarrow$) Como $y^2 - p(x)$ é redutível, então existem $g(x,y), h(x,y)$, não constantes, tais que

$$y^2 - p(x) = g(x,y)h(x,y).$$

Considerando a variável y temos que $\partial_y g + \partial_y h = 2$, pois $g \cdot h = y^2 - p(x)$.

Se $\partial_y h = 2$, então $\partial_y g = 0$. Isso implica, $g \in \mathbb{K}[x]$, isto é, $g(x,y) = a_0(x)$.

E temos $h(x,y) = b_2(x)y^2 + b_1(x)y + b_0(x)$.

Logo,

$$y^2 - p(x) = a_0(x)b_2(x)y^2 + a_0(x)b_1(x)y + a_0(x)b_0(x).$$

Da igualdade de polinômios, segue que

$a_0(x)b_2(x) = 1 \Longrightarrow a_0(x) = a_0 \in \mathbb{K} \Longrightarrow y$ constante. Contradição.

Analogamente, $\partial_y g \neq 2$. Portanto, $\partial_y g = \partial_y h = 1$.

Assim,

$$g(x,y) = a_1(x)y + a_0(x)$$

$$h(x,y) = b_1(x)y + b_0(x).$$

Logo

$$y^2 - p(x) = a_1(x)b_1(x)y^2 + (a_1(x)b_0(x) + a_0(x)b_1(x))y + a_0(x)b_0(x).$$

Temos $a_1(x)b_1(x) = 1 \Longrightarrow b_1(x) = \frac{1}{a_1(x)} = \frac{1}{a_1} \in \mathbb{K}$.

De $a_1(x)b_0(x) + a_0(x)b_1(x) = 0$, temos $a_1 b_0(x) + a_0(x) \cdot \frac{1}{a_1} = 0$. Isso implica

$$a_1^2 b_0(x) + a_0(x) = 0 \Longrightarrow a_0(x) = -a_1 b_0(x).$$

E de $a_0(x)b_0(x) = -p(x)$, temos

$$-a_1 b_0(x) b_0(x) = -p(x),$$

Portanto,

$$p(x) = (a_1 b_0(x))^2.$$

($\Longleftarrow$) Como $p(x)$ é um quadrado, então $p(x) = q(x)^2$. Assim,

$$y^2 - p(x) = y^2 - q(x)^2 = (y - q(x)) \cdot (y + q(x))$$

e portanto $y^2 - p(x)$ é redutível.

□

Exemplo 1.2 (1) *Pelo lema anterior, a curva $y^2 = x(x-1)(x+1)$ é irredutível.*

(2) *Seja $f(x,y) = x^2 - 5xy + 6y^2$, temos que $x^2 - 5xy + 6y^2 = (x-2y)(x-3y)$ e as componentes irredutíveis de f são $x - 2y$ e $x - 3y$.*

1.2 Plano projetivo

Duas retas não paralalelas r e s possuem um único ponto em comum. Se elas forem paralelas, elas não se encontram. De forma intuitiva, quando vemos duas retas paralelas, elas se encontram no infinito. Dessa forma, gostaríamos de definir um plano no qual toda par de retas se intersectam. Antes de definirmos esse plano, definiremos o plano afim.

Definição 1.3 *Dado um corpo $\mathbb{K}$, o plano afim é o espaço de dimensão 2 sobre o corpo $\mathbb{K}$ denotado por $\mathbb{K}^2$.*

Definição 1.4 *O plano projetivo $\mathbb{P}^2$ é o conjunto das retas do espaço tridimensional que passam pela origem.*

Os pontos $(x_1, y_1, z_1), (x_2, y_2, z_2)$ determinam a mesma reta em $\mathbb{K}^3$, se existe $\lambda \in \mathbb{K}$, $\lambda \neq 0$ tal que:

$$\lambda(x_1, y_1, z_1) = (x_2, y_2, z_2).$$

Denotamos por $(x : y : z)$ o ponto de $\mathbb{P}^2$ que representa a reta que liga a origem a um ponto $(x, y, z) \neq (0, 0, 0)$; x, y, z são as coordenadas homogêneas do ponto $(x : y : z)$.

Em outras palavras

$$(\lambda x : \lambda y : \lambda z) = (x : y : z)\ ,\ \forall \lambda \neq 0 \in \mathbb{K}.$$

De forma mais geral podemos definir os espaços projetivos:

Definição 1.5 *O espaço projetivo $\mathbb{P}(V)$ associado a um espaço vetorial V é o conjunto dos subespaços de V de dimensão 1. Se $V = \mathbb{K}^{n+1}$, escrevemos $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(V)$, ou simplesmente $\mathbb{P}^n$. Note que se $V = \mathbb{R}^3$ então os subespaços de dimensão 1 são justamente as retas que passam pela origem.*

As coordenadas homogêneas de um ponto $p \in \mathbb{P}(V)$ relativas a uma base $\{v_0, v_1, \ldots, v_n\}$ de V são as coordenadas $(x_0, x_1, \ldots, x_n)$ de um vetor não nulo $\sum_{i=0}^{n} x_i v_i$, pertencentes ao subespaço representado por p. Fixada a base escrevemos $p = (x_0 : \ldots : x_n)$ para indicar um ponto com essas coordenadas homogêneas.

Para cada $i = 0, \ldots, n$, o subconjunto de $\mathbb{P}^n$

$$U_i = \{(x_0 : \ldots, x_n) : x_i \neq 0\} \ ,$$

pode ser identificado com $\mathbb{K}^n$ através da bijeção

$$(x_0 : \ldots : x_n) \mapsto \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) \quad \left(\text{ omitir } \frac{x_i}{x_i}\right)$$

Vejamos que esta aplicação é injetora.
Sejam $\left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right), \left(\frac{y_0}{y_i}, \ldots, \frac{y_n}{y_i}\right) \in \mathbb{K}^n$. Temos que

$$\begin{aligned} \left(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\right) = \left(\frac{y_0}{y_i}, \ldots, \frac{y_n}{y_i}\right) &\implies \frac{x_j}{x_i} = \frac{y_j}{y_i}, \forall j \neq i \\ &\implies x_j = \frac{x_i}{y_i} y_j, \forall j \neq i. \end{aligned}$$

Chame $\frac{x_i}{y_i} = \lambda$, daí $x_j = \lambda y_j$.
Assim,

$$(x_0 : \ldots : x_n) = (\lambda y_0 : \ldots : \lambda y_n) = (y_0 : \ldots : y_n).$$

Vejamos que a aplicação é sobrejetora.
Seja $(y_1, \ldots, y_n) \in \mathbb{K}^n$. Temos

$$(y_1 : \ldots : y_{i-1} : 1 : y_{i+1} : \ldots : y_n) \mapsto \left(\frac{y_1}{1}, \ldots, \frac{y_n}{1}\right) = (y_1, \ldots, y_n).$$

Portanto a aplicação é bijetora.

Convencionamos escrever $\mathbb{A}^n = U_n$, identificando $\mathbb{K}^n$ com $\mathbb{A}^n \subset \mathbb{P}^n$. O complementar de $\mathbb{A}^n$ em $\mathbb{P}^n$ consiste de pontos da forma $(x_0 : \ldots : x_{n-1} : 0)$. Assim, $\mathbb{P}^n - \mathbb{A}^n$ identifica-se com $\mathbb{P}^{n-1}$, que é chamado hiperplano no infinito, o conjunto $\mathbb{A}^n$ é chamado de espaço afim de dimensão n.

Para $n = 2$, podemos identificar $\mathbb{K}^2$ com $\mathbb{A}^2 \subset \mathbb{P}^2$. Ou seja,

$$\mathbb{A}^2 = \{(x_0 : x_1 : x_2) : x_2 \neq 0\}$$

e a bijeção é dada por

$$\begin{aligned} \mathbb{A}^2 &\longrightarrow \mathbb{K}^2 \\ (x_0 : x_1 : x_2) &\mapsto \left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right). \end{aligned}$$

O complementar de $\mathbb{A}^2$ em $\mathbb{P}^2$, ou seja, $\mathbb{P}^2 - \mathbb{A}^2$ é:

$$\{(x_0 : x_1 : 0) : (x_0, x_1) \neq (0, 0)\},$$

que é identificado com $\mathbb{P}^1$, também chamada de reta projetiva (por ser o espaço projetivo de dimensão 1).

Para $n = 1$, podemos identificar o corpo $\mathbb{K}$ com $\mathbb{A}^1 \subset \mathbb{P}^1$, onde

$$\mathbb{A}^1 = \{(x_0 : x_1) : x_1 \neq 0\}.$$

A identificação é dada por

$$\begin{array}{rcl} \mathbb{A}^1 & \longrightarrow & \mathbb{K} \\ (x_0 : x_1) & \mapsto & \dfrac{x_0}{x_1} \end{array}$$

e o complementar $\mathbb{P}^1 - \mathbb{A}^1$ é

$$\{(x_0 : x_1) : x_1 \neq 0\}.$$

Como

$$(x_0 : 0) = \left(\frac{x_0}{x_0} : \frac{0}{x_0}\right) = (1 : 0),$$

logo

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{(1 : 0)\}.$$

Definição 1.6 *Seja $f = \sum_{i=0}^{d} f_i$, onde cada $f_i \in \mathbb{K}[x, y]$ é homogêneo de grau i, $f_d \neq 0$. A homogeneização de f é o polinômio de grau $d = \partial f$,*

$$f^*(x, y, z) = \sum_{i=0}^{d} z^{d-i} f_i(x, y).$$

Exemplo 1.3 *Seja $f(x, y) = 2 + x + y + xy + x^2 + y^2 + x^3 + y^2x$. A homogeneização de f é :*

$$\begin{array}{rcl} f^*(x, y, z) & = & z^{3-0} f_0(x, y) + z^{3-1} f_1(x, y) + z^{3-2} f_2(x, y) + z^{3-3} f_3(x, y) \\ & = & 2z^3 + (x + y)z^2 + (xy + x^2 + y^2)z + x^3 + y^2x \end{array}$$

Definição 1.7 *Uma curva plana projetiva é uma classe de equivalência de polinômios homogêneos não constantes, $F \in \mathbb{K}[x, y, z]$, módulo a relação que identifica dois tais polinômios, se um for múltiplo do outro.*

A homogeneização de uma curva plana afim f é um exemplo de curva projetiva.

Observação 1.3 *(i) O conjunto de pontos de uma curva plana projetiva $\mathcal{C}$ definida pelo polinômio homogêneo F é o conjunto*

$$\mathcal{C}(\mathbb{K}) = \{(x : y : z) \in \mathbb{P}^2 \mid F(x, y, z) = 0\}.$$

(ii) O grau de uma curva plana projetiva é o grau do polinômio que a define.

(iii) Se F é um polinômio homogêneo, então

$$F(tx, ty, tz) = t^{\partial F} F(x, y, z).$$

Isso mostra que a condição de um ponto $(x : y : z)$ pertencer ao conjunto de pontos da curva plana projetiva, independe das coordenadas homogêneas.

Definição 1.8 *(i) O fecho projetivo de uma curva afim f, é a curva plana projetiva definida pela homogeneização f^*.*

(*ii*) *A desomogeneização de F com respeito a z, é o polinômio $F(x, y, 1)$, denotado por F_*.*

Observação 1.4 (*i*) *O conjunto dos pontos de uma curva algébrica plana afim, definida por $f \in \mathbb{K}[x, y]$, será considerado implicitamente, como o conjunto dos pontos do plano afim $\mathbb{A}^2$, sobre a curva plana projetiva f^*.*

(*ii*) *Os pontos do plano afim sobre uma curva F são obtidos pela equação $F(x, y, 1) = 0$.*

Exemplo 1.4 (1) *A curva $y = x^2$ (uma parábola no plano $\mathbb{R}^2$) pode ser vista como $yz = x^2$. De fato, a homogeneização de $f(x, y) = y - x^2$ é*

$$\begin{aligned} f^*(x, y, z) &= \sum_{i=0}^{2} z^{2-i} f_i(x, y) = z f_1(x, y) + f_2(x, y) \\ &= yz - x^2 \end{aligned}$$

(2) *Os pontos do plano afim da cônica $\frac{x^2}{a^2} + \frac{x^2}{b^2} = z^2$ representam um elipse (sobre $\mathbb{R}$). De fato, para encontrar os pontos do plano afim desta cônica, devemos fazer $F(x, y, 1) = 0$, daí obtemos*

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 = 0 \Longrightarrow \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

que é uma elipse.

(3) *Considere as curvas $f(x, y) = y - x^2$ e $g(x, y) = y + xy + y^3$. Temos que as homogeneizações de f e g são*

$$f^*(x, y, z) = yz - x^2 \text{ e}$$

$$g^*(x, y, z) = \sum_{i=0}^{3} z^{3-i} g_i(x, y) = yz^2 + xyz + y^3.$$

O produto das homogeneizações é

$$\begin{aligned} f^* \cdot g^* &= yz(yz^2 + xyz + y^3) - x^2(yz^2 + xyz + y^3) \\ &= y^2z^3 + xyz^2 + y^4z - x^2yz^2 - x^3yz - x^2y^3 \\ &= y^2z^3 + (xy^2 - x^2y)z^2 + (y^4 - x^3y)z - x^2y^3. \end{aligned}$$

Vejamos o que ocorre com a homogeneização do produto. Temos

$$\begin{aligned} f \cdot g &= (y - x^2)(y + xy + y^3) \\ &= y^2 + xy^2 + y^4 - x^2y - x^3y - x^2y^3 \\ &= y^2 + (xy^2 - x^2y) + (y^4 - x^3y) - x^2y^3. \end{aligned}$$

Assim,

$$\begin{aligned} (fg)^* &= \sum_{i=0}^{5} z^{5-i} (fg)(x, y) \\ &= y^2z^3 + (xy^2 - x^2y)z^2 + (y^4 - x^3y) - x^2y^3. \end{aligned}$$

Portanto, $f^* \cdot g^* = (f \cdot g)^*$.

O que obtivemos acima nos leva a questionar se $f^* \cdot g^* = (f \cdot g)^*$ vale sempre. Isso de fato ocorre.

Sejam as curvas planas afins

$$f = \sum_{i=0}^{d} f_i \text{ e } g = \sum_{j=0}^{l} g_j \ ,$$

onde $\partial f_i = i$ e $\partial g_j = j$.

Temos

$$fg = \sum_{i=0}^{d} \left(\sum_{j=0}^{l} f_i g_j \right), \text{ onde } \partial(f_i g_j) = i + j.$$

Então

$$(fg)^* = \sum_{i=0}^{d} \sum_{j=0}^{l} z^{d+l-(i+j)} f_i g_j.$$

E

$$\begin{aligned} f^* g^* &= (\sum_{i=0}^{d} z^{d-i} f_i)(\sum_{j=0}^{l} z^{l-j} g_j) \\ &= \sum_{i=0}^{d} \sum_{j=0}^{l} (z^{d-i} f_i)(z^{l-j} g_j) \\ &= \sum_{i=0}^{d} \sum_{j=0}^{l} z^{d+l-(i+j)} f_i g_j. \end{aligned}$$

Portanto, $f^* g^* = (fg)^*$ para quaisquer f, g curvas planas afins.

Proposição 1.2 *O produto de polinômios é homogêneo se, e somente se, cada fator é um polinômio homogêneo.*

Demonstração:

($\Longleftarrow$) É claro que se cada fator é um polinômio homogêneo, então, o produto será um polinômio homogêneo.

($\Longrightarrow$) Seja $f = gh$, onde f é homogêneo. Devemos provar que g e h são homogêneos. Suponha que não e tome g não homogêneo.

Seja $\partial g = d$, assim

$$g = g_d + g_{d-1} + \ldots + g_0, \text{ onde } g_d \neq 0 \text{ e } \partial g_j = j, \text{ para } 0 \leq j \leq d.$$

E seja $\partial h = l$, daí

$$h = h_l + h_{l-1} + \ldots + h_0, \text{ onde } h_l \neq 0 \text{ e } \partial h_i = i, \text{ para } 0 \leq i \leq l.$$

Temos que

$$\begin{aligned} \exists s \in \mathbb{N} \ &: \ g = g_d + \ldots + g_s \text{ e } g_s \neq 0, s < d \text{ (pois } g \text{ é não homogêneo);} \\ \exists k \in \mathbb{N} \ &: \ h = h_l + \ldots + h_k \text{ e } h_k \neq 0, k \leqslant l. \end{aligned}$$

Daí

$$f = gh = g_d h_l + \ldots + g_s h_k, \text{ com } \partial f = \partial(g_d h_l) = d + l.$$

Como $g_s \neq 0, h_k \neq 0$, temos $\partial(g_s h_k) = s + k < d + l$. Isso implica, f não é homogêneo. Contradição.

Portanto, g e h são homogêneos.

□

1.3 Curvas racionais

Definição 1.9 *Uma curva plana afim irredutível f, é racional, se existir um par de funções racionais $x(t), y(t)$, não ambas constantes, tal que $f(x(t), y(t)) = 0$ em $\mathbb{K}(t)$. O par $(x(t), y(t))$ é chamado de parametrização racional de f.*

Exemplo 1.5 (1) *A reta $f(x, y) = ax + by + c = 0, a \neq 0$ admite parametrização racional da forma*

$$x(t) = -\frac{b}{a}\, t - \frac{c}{a}, \quad y(t) = t.$$

Temos

$$\begin{aligned} f(x(t), y(t)) &= a\left(-\frac{b}{a}\, t - \frac{c}{a}\right) + bt + c \\ &= -bt - c + bt + c \\ &= 0 \end{aligned}$$

(2) *O círculo $x^2 + y^2 = 1$ (sobre $\mathbb{R}$) é racional. Para determinar a parametrização, vamos encontrar primeiro a reta que passa pelo pontos $(-1, 0), (0, t)$. Temos*

$$y - 0 = m(x + 1), \text{ onde } m = \frac{t - 0}{0 + 1} = t,$$

logo

$$y = t(x + 1).$$

Para encontrar a parametrização desejada fazemos a interseção dessa reta com o círculo $x^2 + y^2 = 1$. Ou seja, devemos resolver o sistema

$$\begin{cases} x^2 + y^2 &= 1 \\ y &= t(x + 1) \end{cases}$$

Substituindo $y = t(x + 1)$ na primeira equação temos

$$x^2 + t^2x^2 + 2t^2x + t^2 = 1.$$

Isso implica

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

Assim,

$$\begin{aligned} x &= \frac{-2t^2 \pm \sqrt{4t^4 - 4(1 + t^2)(t^2 - 1)}}{2(1 + t^2)} \\ &= \frac{-2t^2 \pm \sqrt{4t^4 + 4(1 - t^4)}}{2(1 + t^2)} \\ &= \frac{-2t^2 \pm \sqrt{4}}{2(1 + t^2)} \\ &= -1 \text{ ou } \frac{1 - t^2}{1 + t^2}. \end{aligned}$$

Assim, obtemos

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

E,

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

No exemplo anterior, vimos que a curva $x^2+y^2=1$ é racional, mas dependendo da potência de x e y, isto não ocorre. De um modo geral , temos

Lema 1.2 *A curva $x^m+y^m=1$ (sobre $\mathbb{R}$) é racional se, e somente se, $m=1$ ou $m=2$.*

Demonstração:

($\Longrightarrow$) Como $x^m+y^m=1$ é racional, então existem $x(t), y(t)$ tais que $f(x(t),y(t))=0$ e

$$x(t)=\frac{p(t)}{r(t)}\ ,\ y(t)=\frac{q(t)}{r(t)}$$

com $r(t)\neq 0$ e podemos supor q não constante, pois se

$$\begin{aligned} p,q\in\mathbb{K} &\implies r\in\mathbb{K}\ (\text{pois } p^m+q^m=r^m)\\ &\implies x,y\in\mathbb{K}, \text{ logo}\end{aligned}$$

$x(t), y(t)$ não é uma parametrização.

Por outro lado, se dois dos polinômios tem fator comum e como $p(t)^m+q(t)^m=r(t)^m$, então o terceiro polinômio também tem o mesmo fator comum. Logo podemos supor também que p, q e r são polinômios sem fator comum dois a dois.

Derivando $x^m+y^m=1$, obtemos $mx^{m-1}x'+my^{m-1}y'=0\Longrightarrow x^{m-1}x'+y^{m-1}y'=0$.

Considere o sistema linear

$$\begin{cases} xu+yv=1\\ x'u+y'v=0\end{cases}$$

Temos que $\det\begin{bmatrix} x & y\\ x' & y'\end{bmatrix}=xy'-x'y\neq 0$, pois

$$\begin{aligned} xy'-x'y=0 &\implies \frac{y'}{y}=\frac{x'}{x}\\ &\implies \ln y=\ln x+c\\ &\implies \ln\frac{y}{x}=c\\ &\implies \frac{y}{x}=e^c.\end{aligned}$$

Mas $\frac{y}{x}$ não pode ser constante, já que $\frac{y}{x}=\frac{q}{p}$, q é não constante e não possui fator comum com p.

Como $\det\begin{bmatrix} x & y\\ x' & y'\end{bmatrix}\neq 0$ temos que o sistema admite solução única e,

$$x'u+y'v=0\Longrightarrow v=-\frac{x'}{y'}u$$

Logo,

$$xu+y\left(-\frac{x'}{y'}u\right)=1\Longrightarrow u=\frac{y'}{xy'-y'x}.$$

Assim,

$$v=-\frac{x'}{xy'-x'y}.$$

Note que $u = x^{m-1}$ e $v = y^{m-1}$ é solução desse sistema, logo

$$u = \frac{y'}{xy' - x'y} \text{ e } v = \frac{-x'}{xy' - x'y},$$

implicam

$$x' = -y^{m-1}(xy' - x'y) \tag{1.2}$$

$$y' = x^{m-1}(xy' - x'y). \tag{1.3}$$

Substituindo p, q e r nas equações (1.2) e (1.3), temos

$$x' = \left(\frac{p}{r}\right)' = \frac{rp' - pr'}{r^2},$$

$$y' = \left(\frac{q}{r}\right)' = \frac{rq' - qr'}{r^2}.$$

Assim,

$$\begin{aligned} xy' - x'y &= \frac{p}{r} \cdot \frac{rq' - qr'}{r^2} - \frac{rp' - pr'}{r^2} \cdot \frac{q}{r} \\ &= \frac{pq' - qp'}{r^2}. \end{aligned}$$

Logo

$$\begin{aligned} y' = x^{m-1}(xy' - x'y) &\implies \frac{rq' - qr'}{r^2} = \frac{p^{m-1}}{r^{m-1}} \cdot \frac{pq' - qp'}{r^2} \\ &\implies r^{m-1}(rq' - qr') = p^{m-1}(pq' - qp'), \end{aligned}$$

$$\begin{aligned} x' = -y^{m-1}(xy' - x'y) &\implies \frac{rp' - pr'}{r^2} = -\frac{q^{m-1}}{r^{m-1}} \cdot \frac{pq' - qp'}{r^2} \\ &\implies r^{m-1}(rp' - pr') = q^{m-1}(pq' - qp'). \end{aligned}$$

Como $mdc(r, q) = 1$, então $mdc(r^{m-1}, p^{m-1}) = 1$. E portanto, $r^{m-1} \mid pq' - qp'$. Temos que

$$\begin{aligned} \partial(pq' - qp') &\leq \max\{\partial pq', \partial qp'\} \\ &= \max\{\partial p + \partial q - 1, \partial q + \partial q - 1\} \\ &= \partial p + \partial q - 1. \end{aligned}$$

Assim,

$$\partial r^{m-1} \leq \partial(pq' - qp') \implies (m-1)\partial r \leq \partial p + \partial q - 1.$$

Por outro lado, $mdc(r^{m-1}, p^{m-1}) = 1$, segue que $p^{m-1} \mid rq' - qr'$. Assim,

$$\partial p^{m-1} \leq \partial(rq' - qr') \text{ , logo}$$

$$p^{m-1}\partial p \leq \partial q + \partial r - 1.$$

Temos também que $mdc(r^{m-1}, q^{m-1}) = 1$, logo $q^{m-1} \mid rp' - pr'$ e analogamente

$$(m-1)\partial q \leq \partial r + \partial p - 1.$$

Obtemos

$$\begin{aligned}(m-1)\partial r &\leq \partial p + \partial q - 1,\\ (m-1)\partial p &\leq \partial q + \partial r - 1,\\ (m-1)\partial q &\leq \partial r + \partial p - 1.\end{aligned}$$

Adicionando as desigualdades

$$(m-1)(\partial p + \partial q + \partial r) \leq 2(\partial p + \partial q + \partial r) - 3,$$

assim,

$$(m-3)(\partial p + \partial q + \partial r) \leq -3.$$

Veja que $\partial p + \partial q + \partial r > 0$, para o produto ser negativo, é necessário que $m - 3 < 0$. Assim $m = 1$ ou $m = 2$.

($\Longleftarrow$) Se $m = 1$, então $f(x, y) = x + y - 1$ é uma reta, e toda reta admite uma parametrização, conforme feito anteriormente. Portanto, f é racional. Se $m = 2$, então $f(x, y) = x^2+y^2-1$ é o círculo de centro de 0 e raio 1 que também é racional.

□

1.4 Funções regulares e funções racionais

Seja $\mathbb{K}$ um corpo e $\mathcal{C}$ uma curva afim definida por $f \in \mathbb{K}[x, y]$. Escrevemos $\mathcal{C}(\mathbb{K})$ o conjunto dos pontos de $\mathcal{C}$ definidos sobre o corpo $\mathbb{K}$:

$$\mathcal{C}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}.$$

Escreveremos $\mathcal{C}$ para denotar $\mathcal{C}(\mathbb{K})$. Quando houver necessidade de deixar claro o corpo $\mathbb{K}$ no qual estamos trabalhando, escreveremos $\mathcal{C}(\mathbb{K})$.

Definição 1.10 *Seja $\mathcal{C} \subset \mathbb{A}^2$ uma curva afim irredutível, definida por um polinômio f. Uma aplicação $\varphi : \mathcal{C} \longrightarrow \mathbb{A}^1$ é chamada regular ou polinomial se for igual à restrição de uma função polinomial $\mathbb{A}^2 \longrightarrow \mathbb{A}^1$, isto é, se existir um polinômio $p(x, y)$ tal que*

$$\varphi(x, y) = p(x, y), \forall (x, y) \in \mathcal{C}.$$

O conjunto das funções regulares de $\mathcal{C}$ forma um anel, que denotamos por $A(\mathcal{C})$. De fato, seja $\mathcal{F}(\mathcal{C})$, o conjunto das funções de $\mathcal{C}$ em $\mathbb{A}^1$.

Temos que $\mathcal{F}(\mathcal{C})$ é um anel com as operações usuais de adição e multiplicação de funções. Como $A(\mathcal{C}) \subset \mathcal{F}(\mathcal{C})$, basta mostrar que $A(\mathcal{C})$ é um subanel de $\mathcal{F}(\mathcal{C})$.

Sejam $\varphi, \psi \in A(\mathcal{C})$, então existem $p, q \in \mathbb{K}[x, y] : \varphi(x, y) = p(x, y), \psi(x, y) = q(x, y)$, $\forall x, y \in \mathcal{C}$. E

$$(\varphi + \psi)(x, y) = (p + q)(x, y),$$

$$(\varphi\psi)(x, y) = (pq)(x, y).$$

Portanto, $\varphi + \psi \in A(\mathcal{C})$ e $\varphi\psi \in A(\mathcal{C})$.
Temos que $(-\varphi)(x, y) = (-p)(x, y) \Longrightarrow -\varphi \in A(\mathcal{C})$.
Portanto, $A(\mathcal{C})$ é um subanel de $\mathcal{F}(\mathcal{C})$.

Observação 1.5 *Por abuso de notação, o representante em $A(\mathcal{C})$ do elemento $p(x,y) \in \mathbb{K}[x,y]$ também será denotado por $p(x,y)$. Ou seja, dependendo do contexto, p denotará um elemento de $\mathbb{K}[x,y]$ ou de $A(\mathcal{C})$.*

Lema 1.3 *Sejam $f, g \in \mathbb{K}[x,y]$ polinômios sem fatores irredutíveis em comum. Então existe uma relação*

$$af + bg = c(x),$$

onde $a, b \in \mathbb{K}[x,y]$ e c é um polinômio não nulo na variável x.

Um resultado análogo, vale trocando x por y.

Demonstração: Considere f, g polinômios em $\mathbb{K}(x)[y]$.

Da hipótese temos que $f, g \in \mathbb{K}[x][y]$ não possuem fatores irredutíveis em comum , logo pelo lema de Gauss, não podem possuir fatores irredutíveis em comum em $\mathbb{K}(x)[y]$.

Como $\mathbb{K}(x)[y]$ é domínio principal, então existem $r, s \in \mathbb{K}(x)[y]$ tais que

$$rf + sg = 1.$$

Como $r = \dfrac{a(x,y)}{c(x)}$ e $s = \dfrac{b(x,y)}{c(x)}$, temos

$$\frac{a(x,y)}{c(x)} f(x,y) + \frac{b(x,y)}{c(x)} g(x,y) = 1$$

Isso implica,

$$a(x,y)f(x,y) + b(x,y)g(x,y) = c(x).$$

□

Proposição 1.3 *O conjunto das soluções de um sistema de duas equações polinomiais a duas incógnitas sem fatores irredutíveis em comum é finito.*

Demonstração: Sejam $f, g \in \mathbb{K}[x,y]$ polinômios sem fatores irredutíveis. Pelo lema 2.4 temos

$$a_1 f + b_1 g = c(x),\ a_1, b_1 \in \mathbb{K}[x,y]$$

$$a_2 f + b_2 g = d(y),\ a_2, b_2 \in \mathbb{K}[x,y].$$

Note que $f(x,y) = 0 = g(x,y) \Longrightarrow c(x) = 0$ e $d(y) = 0$, cujo número de soluções é finito (em uma variável o número de soluções de uma equação é finito). □

Lema 1.4 *Seja C uma curva irredutível definida por f, então $A(\mathcal{C})$ é um domínio isomorfo a $\mathbb{K}[x,y]/(f)$.*

Demonstração: Considere o homomorfismo

$$\pi : \mathbb{K}[x,y] \longrightarrow A(\mathcal{C})$$

que associa a cada polinômio a sua restrição a $\mathcal{C}$.

Tome $p \in \ker \pi$ e suponha que $f \nmid p$. Como f é irredutível, f e p não possuem fator comum, pela proposição 1.3 temos

$$af + bp = r(x)$$

$$cf + dp = s(y),$$

cujo número de soluções é finito. Assim, f e p se anulariam em um número finito de pontos. Mas, f, p se anulam em $\mathcal{C}$ que é infinito, pois $\mathbb{K}$ é algebricamente fechado. Absurdo.

Portanto, $f \mid p$, isto é, $p \in (f)$.

Observe que $(f) \subseteq \ker \pi$ é óbvio. Portanto, $\ker \pi = (f)$.

Como (f) é um ideal primo de $\mathbb{K}[x, y]$ e pelo teorema de homomorfismo então $\mathbb{K}[x, y]/(f)$ é um domínio e

$$\mathbb{K}[x, y]/(f) \simeq A(\mathcal{C}).$$

□

Exemplo 1.6 (1) *Se l é uma reta, então $A(l)$ é isomorfo a um anel de polinômios em uma variável. Se l é dada por $y = ax + b$, a aplicação*

$$\begin{aligned} \theta : \mathbb{K}[x, y] &\longrightarrow \mathbb{K}[x] \\ h &\longmapsto h(x, ax + b) \end{aligned}$$

é um homomorfismo de anéis sobrejetor.

É fácil ver que θ é um homomorfismo de anéis, cujo núcleo é gerado por $y - ax - b$ e que é sobrejetor, logo pelo teorema de isomorfismo

$$\mathbb{K}[x, y]/(y - ax - b) \simeq \mathbb{K}[x].$$

(2) *Seja $\mathcal{C}$ a hipérbole (sobre $\mathbb{R}$) $xy = 1$, temos que $A(\mathcal{C})$ é isomorfo ao anel das funções racionais, cujos denominadores são potências de x, isto é,*

$$A(\mathcal{C}) \simeq B = \{x^m p(x) : m \in \mathbb{Z}, p(x) \in \mathbb{K}[x]\} = \mathbb{K}[x, x^{-1}].$$

Considere o homomorfismo

$$\begin{aligned} \theta : \mathbb{K}[x, y] &\longrightarrow \mathbb{K}(x) \\ h &\longmapsto h\left(x, \frac{1}{x}\right). \end{aligned}$$

Seja $h(x, y) = a_m(x)y^m + \cdots + a_0(x)$, então

$$\begin{aligned} h\left(x, \frac{1}{x}\right) &= a_m(x)\frac{1}{x^m} + \cdots + a_0(x) \\ &= x^{-m}(a_m(x) + \cdots + a_0(x)x^m) \\ &= x^{-m}p(x) \end{aligned}$$

Portanto, $\operatorname{Im} \theta \subseteq B$.

Vejamos que $B \subseteq \operatorname{Im} \theta$.

Seja $t \in B$, ou seja, $t = x^m p(x)$. Se $m \geq 0$, então $h(x, y) = x^m p(x)$ e se $m < 0$, então $h(x, y) = y^{-m}p(x)$. Nesse último caso,

$$\theta(h(x, y)) = h\left(x, \frac{1}{x}\right) = x^m p(x).$$

Portanto, $\operatorname{Im} \theta = B$.

Temos ainda que, $\ker\theta = (xy-1)$. *De fato, seja* $p \in (xy-1)$, *isto é,* $p(x,y) = p_1(x,y)(xy-1)$. *Aplicando* θ, *temos* $\theta(p) = 0$.

Tome $p(x,y) \in \ker\theta$.

Dividindo $p(x,y)$ *por* $xy-1$ *em* $\mathbb{K}(x)[y]$, *temos*

$$p(x,y) = \frac{q(x,y)}{t(x)}(xy-1) + \frac{r(x,y)}{t(x)},$$

onde $\partial_y r < \partial_y(xy-1)$ *ou* $r = 0$.

Como $\partial_y(xy-1) = 1$, *então* $r(x,y) = r(x)$. *Assim,*

$$p(x,y) = \frac{q(x,y)}{t(x)}(xy-1) + \frac{r(x)}{t(x)}.$$

Isso implica,

$$t(x)p(x,y) = q(x,y)(xy-1) + r(x).$$

Aplicando θ, *obtemos*

$$\theta(r(x)) = 0.$$

Logo, $r(x) = 0$.

Assim,

$$p(x,y) = \frac{q(x,y)}{t(x)}(xy-1).$$

Em $\mathbb{K}[x,y]$:

$$t(x)p(x,y) = q(x,y)(xy-1).$$

Como $xy-1 \nmid t(x)$, $xy-1$ *é irredutível e* $\mathbb{K}[x,y]$ *é domínio fatorial, então* $xy-1 \mid p(x,y)$.

Portanto, $\ker\theta = (xy-1)$ *e temos*

$$\mathbb{K}[x,y]/(xy-1) \simeq B.$$

Definição 1.11 *O corpo das funções racionais de uma curva afim irredutível* $\mathcal{C}$ *é o corpo de frações* $\mathbb{K}(\mathcal{C})$ *do domínio* $A(\mathcal{C})$.

Um elemento de $\mathbb{K}(\mathcal{C})$ pode ser escrito na forma $\frac{p}{q}$, com $q \neq 0$ e p e q denotam funções polinomiais restritas a $\mathcal{C}$. Dizemos que $\frac{p}{q}$ e $\frac{r}{s}$ representam a mesma função racional, se e somente se, $ps - qr = 0$ (como elemento de $(A(\mathcal{C}))$, ou seja, $ps - qr$ (como elemento de $\mathbb{K}[x,y]$) é múltiplo de f.

Definição 1.12 *Dizemos que a função racional* $\varphi \in \mathbb{K}(\mathcal{C})$ *é regular no ponto* $P \in \mathcal{C}$, *se* φ *admitir uma representação* $\frac{p}{q}$, *com* $p, q \in A(\mathcal{C})$ *e* $q(P) \neq 0$.

Exemplo 1.7 (1) *Seja* $\varphi \in \mathbb{K}(l)$. *Temos que* φ *é regular no ponto* $P \in \mathcal{C}$, *se* φ *admitir uma representação* $\dfrac{p}{q}$, *com* $p, q \in \mathbb{K}[x]$ *e* $q(P) \neq 0$. *Tomando* $\varphi = \dfrac{x}{x-1}$, *temos que* φ *é regular em todo ponto da reta* $y = ax + b$, *com* $x \neq 1$.

(2) *Seja* $\mathcal{C}$ *o círculo* $x^2 + y^2 = 1$ *e seja* $\varphi = \dfrac{y-1}{x}$. *Temos que* φ *é regular em todo ponto de* $\mathcal{C}$ *com* $x \neq 0$. *Note que podem existir mais pontos onde* φ *é regular, por exemplo,* φ *é regular no ponto* $(0,1)$, *basta tomar uma outra representação, a saber* $\varphi = \dfrac{-x}{y+1}$.

Observe que toda função regular é racional, pela definição de função regular. Queremos estabelecer uma condição para que uma função racional seja regular. Mas antes precisamos de algumas definições e resultados.

Considere um sistema de equações $f_1 = \cdots = f_n = 0$. Note que toda solução desse sistema, também é solução de $f_1g_1 + \cdots + f_ng_n = 0$, onde $g_i \in \mathbb{K}[x, y], i = 1, \ldots, n$.

Considere $I = (f_1, \ldots, f_n) = \left\{\sum_{j=1}^{n} g_j f_j \mid g_j \in \mathbb{K}[x, y]\right\}$, um ideal de $\mathbb{K}[x, y]$.

Definição 1.13 *Dizemos que P é um zero do ideal I, se $f(P) = 0, \forall f \in I$.*

Assim, P é um zero do ideal, se todos os polinômios do ideal gerado por $f_1, \ldots, f_n$ se anulam em P. Observe que se $1 \in I$, então I não admite nenhum zero.

Um importante resultado, Nullstellensatz de Hilbert, afirma que se I é um ideal próprio do anel de polinômios com coeficientes num corpo algebricamente fechado, então I admite um zero. Uma demonstração para este resultado pode ser encontrada em [3].

Seja $M = (x - a, y - b)$. Temos que M é maximal. De fato, considere a aplicação

$$\begin{array}{rcl} \theta : \mathbb{K}[x, y] & \longrightarrow & \mathbb{K} \\ f(x, y) & \longmapsto & f(a, b) \end{array}$$

É claro que aplicação θ é um homomorfismo sobrejetor. Logo

$$\mathbb{K}[x, y]/\ker\theta \simeq \mathbb{K},$$

o que implica $\ker\theta$ é maximal.

Temos que

$$\begin{array}{rcl} \ker\theta & = & \{f \in \mathbb{K}[x, y] \mid \theta(f) = 0\} \\ & = & \{f \in \mathbb{K}[x, y] \mid f(a, b) = 0\} \end{array}$$

Seja $g \in (x - a, y - b)$, então $g = g_1(x, y)(x - a) + g_2(x, y)(y - b)$. Aplicando θ, temos $\theta(g) = 0$.

Portanto, $g \in \ker\theta$.

Assim, $(x - a, y - b) \subseteq \ker\theta$.

Seja $g \in \ker\theta$. Temos

$$g = \sum_{i,j\geq 0} a_{ij}x^i y^j.$$

Assim

$$\begin{array}{rcl} g(x - a + a, y - b + b) & = & \displaystyle\sum_{i,j} a_{ij}(x - a + a)^i(y - b + b)^j \\ & = & \displaystyle\sum_{i,j} b_{ij}(x - a)^i(y - b)^j \\ & = & g_1(x, y)(x - a) + g_2(x, y)(y - b) + b_{00} \end{array}$$

Como $g \in \ker\theta \Longrightarrow \theta(g(x, y)) = 0 \Longrightarrow b_{00} = 0$.

Assim,

$$g(x, y) = g_1(x, y)(x - a) + g_2(x, y)(y - b).$$

Isto é, $g \in (x - a, y - b)$.

Portanto $\ker\theta = (x - a, y - b)$.

Observação 1.6 (*a*) *Em um domínio vale que, se a é primo, então a é irredutível. De fato, dado a primo e* $a = bc$, *devemos mostrar que b ou c é invertível. Como a é primo,* $a \mid bc \Longrightarrow a \mid b$ *ou* $a \mid c$. *Digamos que* $a \mid b \Longrightarrow b = ad$. *Logo,*

$$a = bc \Longrightarrow a = adc \Longrightarrow 1 = dc \Longrightarrow c \text{ é invertível.}$$

Portanto, a é irredutível.

(*b*) *Se I é um ideal maximal de um anel A, então I é um ideal primo de A. Pois, se I é maximal, então* A/I *é um corpo. Em particular,* A/I *é um domínio, logo I é primo.*

Proposição 1.4 *Se* $\mathbb{K}$ *é um corpo algebricamente fechado, então todo ideal maximal M de* $\mathbb{K}[x, y]$ *é do tipo* $(x - a, y - b)$, *para algum* $(a, b) \in \mathbb{K}^2$.

Demonstração: Seja $f \in M$ um polinômio não constante, f existe, pois $M \not\subset K$. Podemos supor ainda, f irredutível, pois como $\mathbb{K}[x, y]$ é domínio fatorial, então $f = f_1 \dots f_n$, onde f_j é irredutível, $\forall j = 1, \dots, n$. Como M é maximal, então M é primo, logo algum dos $f_j, j = 1, \dots, n$, pertence a M. Chamaremos f_j simplesmente de f.

Como $\mathbb{K}$ é algebricamente fechado temos que, f possui um zero, digamos $f(x_0, y_0) = 0$. Se $M = (x - x_0, y - y_0)$, acabou. Se não, existe $g \in M$ tal que $g(x_0, y_0) \neq 0$. Em particular $f \nmid g$ e pelo lema (2.4) existem $a_1, a_2, b_1, b_2 \in \mathbb{K}[x, y]$ tais que

$$a_1(x, y)f(x, y) + b_1(x, y)g(x, y) = c(x)$$

$$a_2(x, y)f(x, y) + b_2(x, y)g(x, y) = d(y).$$

Como $c(x) \in M$, $d(y) \in M$ e $\mathbb{K}$ é algebricamente fechado, então $c(x)$ e $d(y)$ se fatoram como produto de fatores lineares. Como M é primo, algum desses fatores pertence a M, isto é, M possui elementos da forma $x - a, y - b$. Como $(x - a, y - b)$ é maximal, então $M = (x - a, y - b)$. □

Proposição 1.5 *Se* $\varphi \in \mathbb{K}(\mathcal{C})$ *é uma função racional regular em cada ponto de* $\mathcal{C}$, *então* $\varphi \in A(\mathcal{C})$, *isto é,* φ *é regular.*

Demonstração: Da hipótese temos que para todo ponto $P \in \mathcal{C}$, φ admite uma representação $\frac{p}{q}$, com $p, q \in A(\mathcal{C})$ e $q(P) \neq 0$. Temos $\varphi = \frac{p}{q} \Longrightarrow q = q\varphi$, com $q \in A(\mathcal{C})$.

Assim, vamos considerar o ideal

$$I = \{q' \in A(\mathcal{C}) : q'\varphi \in A(\mathcal{C})\}.$$

Se mostrarmos que $1 \in I \Longrightarrow 1 \cdot \varphi \in A(\mathcal{C})$, isto é, $\varphi \in A(\mathcal{C})$.

Mostremos primeiro que I é de fato um ideal de $A(\mathcal{C})$.

Temos que $0 \in I$, pois $0 = 0 \cdot \varphi \in A(\mathcal{C})$.

Sejam $q_1, q_2 \in I \Longrightarrow q_1\varphi, q_2\varphi \in A(\mathcal{C}) \Longrightarrow q_1\varphi + q_2\varphi \in A(\mathcal{C}) \Longrightarrow (q_1 + q_2)\varphi \in A(\mathcal{C}) \Longrightarrow q_1 + q_2 \in I$.

Sejam $q' \in I$ e $\psi \in A(\mathcal{C})$.

Como $q' \in I$, então $q'\varphi \in A(\mathcal{C})$. Isso implica, $\psi(q'\varphi) \in A(\mathcal{C})$. Então, $(\psi q')\varphi \in A(\mathcal{C})$.

Portanto, $\psi q' \in A(\mathcal{C})$.

Suponha por absurdo que $1 \notin I$. Então I está contido em algum ideal maximal de

$A(\mathcal{C}) \simeq \mathbb{K}[x, y]/(f)$. Pelo Nullstellensatz, I admite um zero, isto é, existe $P \in \mathcal{C}$, tal que $q'(P) = 0, \forall q' \in I$. Absurdo, pois φ não seria regular nesse ponto. □

1.5 Interseção de uma curva com uma reta

Sejam $f = y - x^2$ e $l = y - 2x - 3$. Para encontrar a interseção de f e l, determinamos o valor de y em função de x (em l) e substituimos em f. Ou seja, em l temos $y = 2x + 3$, substituindo em f temos

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

Resolvendo a equação $-x^2 + 2x + 3 = 0$, temos duas abcissas para os pontos de interseção entre l e f. A saber, $x = -1$ e $x = 3$. E portanto, os pontos de interseção são $(-1, 1)$ e $(3, 9)$.

Dada uma curva f e uma reta de equação $y = ax + b$ resolvemos a equação

$$f_l(x) = f(x, ax + b) = 0,$$

para determinar os pontos de $f \cap l$.

Temos as seguintes possibilidades para o polinômio $f_l(x)$:

(1) $f_l(x)$ é identicamente nulo, neste caso, l uma componente de f.

(2) $f_l(x)$ é uma constante diferente de zero, caso em que $f \cap l = \emptyset$.

(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 x_i são as abcissas dos pontos de interseção.

Um processo análogo é feito para l da forma $x = cy + d$.

Com base no polinômio $f_l(x)$ definimos:

Definição 1.14 *A multiplicidade ou índice de interseção de l, f no ponto P é dada por*

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

Se $l \not\subseteq f$, chamamos o inteiro

$$m_\infty = \partial f - \sum_{i=1}^{r} m_i$$

de multiplicidade de l, f no infinito.

Para a curva $f = y - x^2$ e a reta $l = y - 2x - 3$ temos

$$f_l(x) = (-1)(x + 1)(x - 3),$$

logo $(l, f)_P = 1$, para $P = (-1, 1)$ e $P = (3, 9)$.

Exemplo 1.8 (1) *Seja $f = y - x^2$, $l = y - (ax + b)$. Temos $f_l(x) = f(x, ax + b)$. Fazendo $f_l(x) = 0$, temos*

$$ax + b - x^2 = 0 \Longrightarrow \Delta = a^2 + 4b.$$

Se $a^2 + 4b > 0$ temos duas interseções distintas.

Se $a^2 + 4b = 0$ temos uma interseção com multiplicidade 2.

(2) *Seja* $f = y - x^3$ *e* $l = ax + by + c$.

Se $b \neq 0$ *e* $a = c = 0$ *temos* $l = by$. *Assim,*

$$f_l(x) = f(x, 0) = -x^3.$$

$f_l(x) = 0 \Longrightarrow -x^3 = 0 \Longrightarrow (0,0)$ *é ponto de interseção com multiplicidade 3.*

Portanto $(l, f)_P = 3$, *para* $P = (0,0)$.

Se $a \neq 0 = b$, $l = ax + c$. *Assim,*

$$f_l(x) = 0 \Longrightarrow f\left(\frac{-c}{a}, y\right) = 0 \Longrightarrow y - \left(\frac{-c}{a}\right)^3 = 0 \Longrightarrow y = \frac{-c^3}{a^3}.$$

Portanto, há uma interseção com multiplicidade 1 *e no infinito temos*

$$m_\infty = 3 - 1 = 2.$$

Portanto o ponto de interseção no infinito tem multiplicidade 2.

Se $b \neq 0$ *temos que* $l = ax + by + c$, *implica*

$$f\left(x, \frac{-a}{b}x - \frac{c}{b}\right) = 0 \Longrightarrow x^3 + \frac{a}{b}x + \frac{c}{b} = 0.$$

Como uma cúbica tem sempre três soluções (em um corpo algebricamente fechado), então l *e* f *se intersectam em três pontos (contando as multiplicidades).*

(3) *Seja* $f = y^2 - x^2(x+1)$ *e* $l = y - x$.

Temos $f_l(x) = f(x, x) = 0 \Longrightarrow x^2 - x^2(x+1) = 0 \Longrightarrow -x^3 = 0$.

Portanto, $(l, f)_P = 3$, *onde* $P = (0,0)$.

(4) *Para a mesma curva do exemplo anterior, se* $l = y - ax$, *temos*

$$f_l(x) = f(x, ax) = a^2x^2 - x^2(x+1) = x^2(a^2 - x - 1).$$

Logo,

$$f_l(x) = 0 \Longrightarrow x^2(a^2 - x - 1) = 0.$$

Assim, a origem é um ponto de interseção com multiplicidade 2.

Lema 1.5 *Seja* $f = f_m + \cdots + f_d$, *com* f_i *homogêneo de grau* i, $m \leq i \leq d$ *e* $f_m \neq 0$. *Se* $x \nmid f_m$, *então*

$$f(0, y) = y^m \left(f_m(0,1) + \cdots + f_d(0,1)y^{d-m}\right) \text{ e } f_m(0,1) \neq 0.$$

Demonstração: Substituindo $x = 0$ em $f(x, y)$ temos

$$\begin{aligned} f(0,y) &= f_m(0,y) + \cdots + f_d(0,y) \\ &= y^m f(0,1) + \cdots + y^d f(0,1) \\ &= y^m(f_m(0,1) + \cdots + y^{d-m} f(0,1)). \end{aligned}$$

Observe que f_m é um polinômio da forma $a_m y^m + \cdots + a_0 x^m$. Se x não divide $f_m \neq 0$, então $a_m \neq 0$, logo $f_m(0,1) = a_m \neq 0$. □

1.6 Pontos múltiplos

Nesta seção queremos caracterizar os pontos de uma curva f. Mais precisamente, queremos identificar se P é singular ou não, mas antes precisamos de algumas definições.

Proposição 1.6 *Seja f uma curva e P um ponto de f. Existe um inteiro $m = m_P(f) \geq 1$, tal que, para toda reta l passando por P,*

$$(l, f)_P \geq m,$$

ocorrendo a desigualdade estrita para no máximo m retas e no mínimo uma.

Demonstração: Sem perda de generalidade suponha $P = (0, 0)$ (podemos supor $P = (0, 0)$ pois para um ponto P qualquer basta fazer uma translação).

Existe $m \geq 0$, tal que

$$f(x, y) = f_0 + f_1(x, y) + f_2(x, y) + \cdots + f_n(x, y),$$

onde $n = \partial f$ e $\partial f_j = j$, para $0 \leq j \leq n$.

Observe que $f(0, 0) = f_0(x, y)$ e como $P \in f$, então $f_0(x, y) = 0$.

Seja $m \geq 1$ o menor inteiro positivo, tal que

$$f_0(x, y) = \cdots = f_{m-1}(x, y) = 0 \text{ e } f_0(x, y) \neq 0.$$

Assim

$$f(x, y) = f_m(x, y) + \cdots + f_n(x, y),$$

onde $1 \leq m \leq n$.

Para uma reta $l = y - tx$ passando pela origem, tem-se

$$f_l(x) = f(x, tx) = x^m(f_n(1, t) + \cdots + f_d(1, t)x^{d-m}).$$

Se $f_m(1, t) \neq 0$, então $(l, f)_0 = m$. Veja que $f_n(1, t) = 0$, para no máximo m retas l (aquelas para as quais t é raiz de $f_m(1, t)$). □

Definição 1.15 *O inteiro $m = m_P(f)$ descrito na proposição acima é a multiplicidade do ponto P na curva f ou a multiplicidade de f em P.*

Se $P \notin f$, convencionamos $m_P(f) = 0$.

Se $P = (a, b) \in f$, escrevemos

$$f(x + a, y + b) = f_m(x, y) + (\text{ termos de grau } > m).$$

O polinômio homogêneo $f_m(x, y)$ pode ser decomposto de maneira única,

$$f_m(x, y) = \prod_{i=0}^{s} (\alpha_i x + \beta_i y)^{\gamma_i},$$

onde os fatores lineares $\alpha_i x + \beta_i y$ são retas distintas.

Definição 1.16 *As retas*

$$l_i = \gamma_i(x - a) + \beta_i(y - b)$$

são as retas tangentes de f em $P = (a, b)$, o expoente γ_i é a multiplicidade da tangente l_i.

Definição 1.17 *Dizemos que um ponto P de uma curva f é não singular em P se $m_P(f) = 1$. Caso contrário dizemos que P é singular. A curva f é não singular se $m_P(f) = 1, \forall P \in f$. Se $m_P(f) = 2, \ldots, m$, dizemos que P é um ponto duplo, ... , m-úplo.*

Dizemos que P é ordinário se f admitir m tangentes distintas em P.

Uma cúspide é um ponto duplo com tangentes coincidentes.

Um nó é um ponto duplo ordinário.

Proposição 1.7 (1) *Um ponto $P \in f$ é não singular, se e somente se, uma das derivadas parciais f_x, f_y não se anula em P.*

(2) *Se $P = (a, b) \in f$ é não singular, então a tangente a f em P é dada por*

$$f_x(P)(x - a) + f_y(P)(y - b) = 0.$$

Demonstração:

(1) ($\Longrightarrow$) Seja $P = (a, b)$.

$$f = f_1 + f_2 + \cdots,$$

onde f_j é da forma

$$f_j = \sum_{i=0}^{j} \alpha_i j (x - a)^i (y - b)^{j-i},$$

isto é, f_j é homogêneo nas variáveis $x - a, y - b$. Em particular

$$f_1 = \alpha_{01}(y - b) + \alpha_{11}(x - a).$$

P não singular $\Longrightarrow m_P(f) = 1 \Longrightarrow f_1 \neq 0 \Longrightarrow \alpha_{01} \neq 0$ ou $\alpha_{11} \neq 0$.

Observe que

$$(f_j)_x(a, b) = 0, \forall j \geq 2,$$
$$(f_j)_y(a, b) = 0, \forall j \geq 2,$$
$$f_x(a, b) = (f_1)_x(a, b) = \alpha_{11},$$
$$f_y(a, b) = (f_1)_y(a, b) = \alpha_{01}.$$

Isso implica

$$f_x(a, b) \neq 0 \text{ ou } f_y(a, b) \neq 0.$$

($\Longleftarrow$) Seja $P = (a, b)$.

Pela fórmula de Taylor, temos

$$f(x, y) = f(a, b) + f_x(a, b)(x - a) + f_y(a, b)(y - b) + g(x - a, y - b),$$

onde todos os termos de g nas variáveis $x - a, y - b$ têm grau ≥ 2.

Da hipótese $f_1 = f_x(a, b)(x - a) + f_y(a, b)(y - b) \neq 0$, logo $m_P(f) = 1$.

(2) Como P é não singular temos $m_P(f) = 1$, isto é, $f_1 \neq 0$. Como

$$f_1 = f_x(P)(x-a) + f_y(P)(y-b),$$

então a reta tangente de f em P é

$$f_x(P)(x-a) + f_y(P)(y-b) = 0.$$

□

Exemplo 1.9 (1) *As tangentes a* $f(x,y) = x^2 - y^2 + x^3 + y^3$ *na origem são* $x - y$ *e* $x + y$, *pois*

$$f_2(x,y) = x^2 - y^2 = (x-y)(x+y).$$

E no ponto $(1,-1)$ *a única tangente é* $5(x-1) + 5(y+1)$. *Chame* $u = x - 1$ *e* $v = y + 1$.

$$\begin{aligned} f(u,v) &= (u+1)^2 - (v-1)^2 + (u+1)^3 + (v-1)^3 \\ &= u^2 + 2u + 1 - v^2 + 2v - 1 + u^3 + 3u^2 + 3u + 1 - v^3 - 3v^2 + 3v - 1 \\ &= 5u + 5v + 4u^2 - 2v^2 + u^3 + v^3 \\ &= 5(x-1) + 5(y+1) + 4(x-1)^2 - 2(y+1)^2 + (x-1)^3 + (y+1)^3 \end{aligned}$$

Portanto, $f_1 = 5(x-1) + 5(y+1)$ *é a reta tangente em* $P = (1,-1)$.

Podemos encontrar a tangente usando a proposição anterior, para isso encontramos as derivadas parciais de f *no ponto* $(1,-1)$.

$$f_x(P) = 2x + 3x^2 = 5$$

$$f_y(P) = -2y + 3y^2 = 5$$

Assim, P *é não singular e a tangente é* $5(x-1) + 5(y+1)$.

(2) *Seja* $f = x^2 - y(y^2 + x^2)$. *Temos*

$$f_x = 2x - 2yx$$

$$f_y = -3y^2 - x^2$$

Na origem $f_x(0) = 0$ *e* $f_y(0) = 0$. *Então a origem é um ponto singular de* f *e como* $f_2 = x^2$ *a tangente é* x.

Portanto, f *tem cúspide na origem.*

(3) *Seja* $f(x,y) = x^2 + y^2 - y^3$. *Temos que* $P = (0,0) \in f$ *e* $m_P(f) = 2$, *isto é,* P *é um ponto duplo.*

Como $f_2 = x^2 + y^2 = (x - yi)(x + yi)$, *temos as tangentes de* f *em* P *dadas por*

$$l_1 = x - yi$$

$$l_2 = x + yi$$

Assim P *é duplo e possui tangentes distintas (não reais), logo* P *é um nó.*

Proposição 1.8 *Se f é uma curva sem componentes múltiplas, então o conjunto dos pontos singulares de f é finito.*

Demonstração: Temos que f é uma curva sem componentes múltiplas, isto é, não existe p componente de f tal que $p^2 \mid f$.

O conjunto dos pontos singulares de f é o conjunto de pontos de f tais que $f_x = 0 = f_y$. Isto é

$$f = f_x = f_y = 0.$$

Temos que $f = f_m + \cdots + f_d$ e $f_m \neq 0$. Seja

$$f_m = a_0x^m + a_1x^{n-1}y + \cdots + a_my^m,$$

onde pelo menos um dos $a_i \neq 0$. Como

$$(f_m)_x = ma_0x^{m-1} + \cdots + a_{m-1}y^{m-1} \quad \text{e}$$

$$(f_m)_y = a_1x^{m-1} + \cdots + ma_my^m,$$

então

$$(f_m)_x = 0 \Longrightarrow a_m \neq 0 \Longrightarrow (f_m)_y \neq 0 \quad \text{e}$$
$$(f_m)_y = 0 \Longrightarrow a_0 \neq 0 \Longrightarrow (f_m)_x \neq 0.$$

Assim, podemos supor que uma das derivadas parciais é não identicamente nula, digamos $f_x \neq 0$. Temos que $f = f_x = 0$ admite um número finito de soluções. Caso contrário, pela proposição (1.3) existiria uma componente irredutível p comum a f e f_x. Mas isso implica que $p^2 \mid f$, o que é absurdo. □

1.7 Interseção de uma reta com uma curva (caso projetivo)

Nesta seção estamos interessados na interseção de uma reta L com uma curva plana projetiva F. O que foi feito no caso afim será aproveitado para o caso projetivo. Já vimos que o conjunto de pontos de uma curva plana afim, $f(x, y) = 0$, pode ser considerado implicitamente como o conjunto dos pontos do plano afim sobre uma curva plana projetiva $f^*(x, y, z) = 0$ e além disso os pontos do plano afim sobre uma curva plana projetiva F são obtidos pela equação $F_* = F(x, y, 1) = 0$, isto é, a desomogeneização de F com relação a variável z (ou em relação a qualquer outra variável).

A multiplicidade de interseção de uma reta L com uma curva F no ponto $P \in \mathbb{P}^2$ será denotada por $(L, F)_P$. Podemos supor P um ponto do plano afim. Como os pontos do plano afim são obtidos através da desomogeneização de F, temos

$$(L, F)_P = (L_*, F_*)_{P'} \ ,$$

onde P' é obtido através da bijeção de U_2 com $\mathbb{A}^2$,

$$(x_0 : x_1 : x_2) \longmapsto \left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right) \ .$$

Seja $P = (0 : 0 : 1)$ então $(L, F)_P = (L_*, F_*)_{P'}$, onde $P' = (0, 0)$. Sabemos também que $L \cap F$ pode ter um ponto de interseção no infinito, nesse caso $P = (a : b : 0)$ e ao menos a ou b é diferente de 0, e portanto podemos estudar esse caso em U_0 ou U_1.

Assim, voltamos ao caso afim e valem as definições:

Definição 1.18 *(i)* $(L,F)_P$ *é a multiplicidade de interseção de uma reta* L *com uma curva* F *e é definida por*

$$(L,F)_P = \begin{cases} \infty & , \text{ se } P \in L \subset F \\ 0 & , \text{ se } P \notin L \cap F \\ m_i & , \text{ se } P = P_i \end{cases},$$

onde P_i *é o ponto de interseção de uma reta* $L \cap F$ *e* m_i *é o expoente que aparece no polinômio ao substituir* L *em* F*;*

(ii) O inteiro $m_P(F)$ *tal que para toda reta* L *passando por* P*,*

$$(L,F)_P \geq m_P(F)$$

é a multiplicidade de F *em* P*;*

(iii) $P \in F$ *é não singular em* F *se* $m_P(F) = 1$*;*

(iv) $P \in F$ *é singular se* $m_P(F) \geq 2$*.*

Se f é uma curva afim e $F = f^*$ então $m_P(F) = m_{P'}(f), \forall P' \in \mathbb{A}^2$. Para determinar $m_P(F)$ e as retas tangentes, reduzimos ao caso afim, desomogeneizando F em relação a uma variável que não se anula em P.

Exemplo 1.10 *Seja a parábola cúbica* $y = x^3$*. Temos que a homogeneização de* $f(x,y) = y - x^3$ *com relação a variável* z *é* $F(x,y,z) = z^2y - x^3$*.*

Vamos determinar a interseção da reta $z = 0$ *com a curva plana projetiva* F *no ponto* $P = (0:1:0)$*. Para isso façamos*

$$(z,F)_P = (z,F_*)_{P'} = (z, z^2 - x^3)_{P'} \ ,$$

onde $P' = (0,0)$*, pois* $(0:1:0) \in U_1 \longmapsto (0,0) \in \mathbb{A}^2$*.*

Fazendo $z = 0$ *e substituindo em* $F_* = 0$*, temos* $-x^3 = 0 \Longrightarrow (z,F)_P = 3$*.*

Agora vamos determinar $m_P(F) = m_{P'}(F_*)$*.*

Como $F_* = z^2 - x^3 \Longrightarrow m_P(F) = 2$*.*

Exemplo 1.11 *Seja o círculo* $x^2 + y^2 = 1$*.*

Temos $f^*(x,y,z) = x^2 + y^2 - z^2$*. Tomando* $P = (a:b:1) \in \mathbb{P}^2$ *temos no plano afim* $P' = (a,b)$*.*

Suponha ainda que P *pertence à curva. Chamando* $u = x - a$ *e* $v = y - b$ *temos*

$$\begin{aligned} f(x,y) = f(u,v) &= (u+a)^2 + (v+b)^2 - 1 \\ &= u^2 + 2ua + a^2 + v^2 + 2vb + b^2 - 1 \\ &= (x-a)^2 + (y-b)^2 + 2(x-a)a + 2(y-b)b + a^2 + b^2 - 1 \\ &= (x-a)^2 + (y-b)^2 + 2(x-a)a + 2(y-b)b \end{aligned}$$

Logo, $f_1 = 2(x-a)a + 2(y-b)b \Longrightarrow m_{P'}(f) = 1 \Longrightarrow m_P(f^*) = 1, \forall (a:b:1) \in f^*$*.*

Proposição 1.9 *Seja* F *uma curva de grau* d *e seja* $P \in \mathbb{P}^2$*. Então*

(1) P *é singular* $\Longleftrightarrow F_x(P) = F_y(P) = F_z(P) = 0$*;*

(2) Se P *é não singular, então a reta tangente a* F *em* P *é:*

$$F_x(P)x + F_y(p)y + F_z(P)z = 0.$$

Demonstração: A demonstração é similar à que foi feita no caso afim. □

O teorema que segue é um teorema importantíssimo da Álgebra Comutativa e será muito importante nesse estudo.

Teorema 1.1 *Duas curvas planas projetivas F, G sobre um corpo $\mathbb{K}$, sem componente em comum, tem $(\partial F)(\partial G)$ pontos em comum (em $\overline{\mathbb{K}}$) contados com multiplicidade, isto é,*

$$\sum_{P \in F \cap G} (F, G)_P = (\partial F)(\partial G).$$

Demonstração: Uma demonstração para este teorema pode ser encontrada em [3]. □

Corolário 1.1 *Sejam F, G curvas sem componente em comum. Então*

$$\sum_{P \in F \cap G} m_p(F) m_P(G) \leq (\partial F)(\partial G).$$

Demonstração: Ver [11]. □

Capítulo 2

Curvas Elípticas

Neste capítulo nosso objeto de estudo são curvas elípticas, que são curvas de gênero um (isto é, curvas de grau 3 no plano projetivo sem singularidades) com um ponto específico. Estamos interessados em estudar o conjunto dos pontos racionais de uma curva elíptica, para isso precisamos definir uma operação em $E(\mathbb{Q})$, veremos que $E(\mathbb{Q})$ com tal operação forma um grupo abeliano, o que é de grande importância, pois dependendo do ponto da curva elíptica que conhecemos podemos determinar infinitos pontos. Mostraremos ainda que toda curva elíptica pode ser escrita na forma de Weierstrass.

2.1 Curvas elípticas como cúbicas não singulares

Definição 2.1 *Uma curva elíptica E sobre $\mathbb{Q}$ é uma curva plana projetiva não singular definida sobre $\mathbb{Q}$ de grau 3, juntamente com um ponto racional $\mathcal{O} \in E(\mathbb{Q})$.*

Usualmente o ponto $\mathcal{O}$ será o ponto no infinito da curva projetiva E. Assim, podemos pensar em E como uma curva afim com um ponto no infinito.

Proposição 2.1 *As seguintes definições de curva elíptica são birracionalmente equivalentes:*

(*i*) *A definição 2.1.*

(*ii*) *Uma curva elíptica E sobre $\mathbb{Q}$ é uma curva plana projetiva não singular de grau 3 com um ponto de inflexão racional (isto é, a multiplicidade de interseção da reta tangente a E em P é maior ou igual do que 3).*

(*iii*) *Uma curva plana projetiva não singular E sobre $\mathbb{Q}$ da forma:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_5Z^3. \tag{2.1}$$

Essa equação é chamada equação de Weierstrass da curva elíptica.

Demonstração: Vejamos que $(i) \implies (ii)$. Seja $\mathcal{C}$ uma curva projetiva plana não singular sobre $\mathbb{Q}$ e seja $\mathcal{O} \in \mathcal{C}(\mathbb{Q})$. Suponha que $\mathcal{O}$ não seja um ponto de inflexão, assim a reta tangente a $\mathcal{C}$ no ponto $\mathcal{O}$ intersecta $\mathcal{C}$ em um ponto $P \neq \mathcal{O}$. Podemos fazer uma mudança de variáveis de modo que a reta tangente seja o eixo Y e $P = (0 : 0 : 1)$. Temos que uma cúbica está representada por um polinômio homogêneo de grau 3, podemos escrever o polinômio ordenado pelo grau de Z, assim

$$F_0(X,Y)Z^3 + F_1(X,Y)Z^2 + F_2(X,Y)Z + F_3(X,Y) = 0,$$

onde F_j é um polinômio homogêneo nas variáveis X, Y de grau j. Logo, F_0 é uma constante. O ponto $(0:0:1)$ pertence à cúbica, logo

$$F_0(0,0) + F_1(0,0) + F_2(0,0) + F_3(0,0) = 0$$

como F_j é homogêneo de grau j, então $F_j(0,0) = 0$, para $j > 0$. Logo a equação se torna $F_0(0,0) + 0 + 0 + 0 = 0$. Como F_0 é constante, então $F_0(X,Y) = F_0(0,0) = 0$. Portanto, a cúbica é

$$\mathcal{C} : F_1(X,Y)Z^2 + F_2(X,Y)Z + F_3(X,Y) = 0,$$

onde cada $F_i, i = 1,2,3$ é homogêneo de grau i. Fazendo a desomogeneização em relação a variável Z obtemos a curva afim

$$\mathcal{C}^{aff} : F_1(X,Y) + F_2(X,Y) + F_3(X,Y) = 0.$$

Seja $\mathcal{O} = (0,y),\ y \neq 0$, então y é raiz dupla de

$$F_1(0,1)Y + F_2(0,1)Y^2 + F_3(0,1)Y^3 = 0.$$

Temos que $F_1(0,1)Y + F_2(0,1)Y^2 + F_3(0,1)Y^3 = Y(F_1(0,1) + F_2(0,1)Y + F_3(0,1)Y^2) = 0$. Como $y \neq 0$, temos que ter $F_1(0,1)+F_2(0,1)y+F_3(0,1)y^2 = 0$ e isso implica que o discriminante dessa equação deve ser igual a 0, isto é,

$$F_2(0,1)^2 - 4F_1(0,1)F_3(0,1) = 0. \tag{2.2}$$

Considere a reta $Y = tX$, essa reta intersecta a curva afim nos pontos cuja coordenada X satisfaz

$$XF_1(1,t) + X^2F_2(1,t) + X^3F_3(1,t) = 0,$$

assim temos $X(F_1(1,t) + XF_2(1,t) + X^2F_3(1,t)) = 0$. A solução $X = 0$, implica $Y = 0$ e

$$F_1(1,t) + XF_2(1,t) + X^2F_3(1,t) = 0, \tag{2.3}$$

que pode ser reescrita como

$$(2F_3(1,t)X + F_2(1,t))^2 = F_2(1,t) - 4F_3(1,t)F_1(1,t).$$

Escrevendo

$$s = 2F_3(1,Y/X)X + F_2(1,Y/X), \quad t = Y/X, \tag{2.4}$$

obtemos a equação

$$s^2 = G(t), \qquad G(t) = F_2(1,t)^2 - 4F_1(1,t)F_3(1,t).$$

A relação (2.4) define um mapa regular $\mathcal{C}^{aff} \setminus \mathcal{O} \longrightarrow E$, onde E é a curva afim definida pela equação $s^2 = G(t)$. O polinômio $G(t)$ tem grau 3: de fato, o polinômio $F_2(s,t)^2 - 4F(s,t)F_3(s,t)$ é homogêneo em s,t de grau 4. Podemos escrevê-lo assim: $H(s,t) = as^4+bs^3t+cs^2t^2+dst^3+et^4$, logo $G(t) = H(1,t) = a + bt + ct^2 + dt^3 + et^4$. Observe que $H(0,1) = e$. Em outras palavras $F_2(0,1)^2 - 4F_1(0,1)F_3(0,1) = 0$ é o coeficiente de t^4. Podemos estender o homomorfismo $\mathcal{C}^{aff} \setminus \mathcal{O} \longrightarrow E$ para um isomorfismo de $\mathcal{C}$ na homogeneização de E. Façamos

$$s \longmapsto \frac{s}{w}, \quad t \longmapsto \frac{t}{w}.$$

Temos que

$$\frac{s}{w} = 2F_3(1,Y/X)X/Z + F_2(1,Y/X),$$

$$\frac{t}{w} = \frac{Y}{X}.$$

Para eliminar denominador escrevemos: $w = ZX^2$, o que implica, $t = XYZ$ e logo

$$\begin{aligned} s &= ZX^2\left(\frac{2F_3(X,Y)}{X^2Z} + \frac{F_2(X,Y)}{X^2}\right) \\ &= 2F_3(X,Y) + F_2(X,Y)Z \end{aligned} \tag{2.5}$$

Temos assim $\varphi : \mathcal{C} \longmapsto E$ definida por $\varphi(X : Y : Z) = (t : s : w)$, onde

$$\begin{aligned} t &= XYZ \\ s &= 2F_3(X,Y) + F_2(X,Y)Z \\ w &= X^2Z \end{aligned}$$

Se $Z \neq 0$, podemos considerar $Z = 1$ e nesse caso

$$\varphi(X : Y : 1) = (XY : 2F_3(X,Y) + F_2(X,Y) : X^2).$$

A imagem de $\mathcal{O} = (0 : y : 1)$ é

$$\begin{aligned} \varphi(\mathcal{O}) &= (0 : 2F_3(0,y) + F_2(0,y) : 0) \\ &= (0 : 1 : 0), \end{aligned}$$

que é um ponto de inflexão.

Mostremos agora que $(ii) \Longrightarrow (iii)$. Uma cúbica tem a forma

$$F(X,Y,Z) = c_1X^3 + c_2X^2Y + c_3X^2Z + c_4XY^2 + c_5XYZ + c_6XZ^2 + c_7Y^3 + c_8Y^2Z + c_9YZ^2 + c_{10}Z^3.$$

Seja F o polinômio que define E e seja P o ponto de inflexão. Considere uma transformação do plano, que envia P em $(0 : 1 : 0)$. Esta transformação envia F em um polinômio G, que define a curva $\tilde{E}$, com $\mathcal{O}$ como ponto de inflexão. De $F(0 : 1 : 0) = 0$ obtemos $c_7 = 0$.

A desomogeneização de F em relação a variável Y é

$$F(X,1,Z) = c_1X^3 + c_2X^2 + c_3X^2Z + c_4X + c_5XZ + c_6XZ^2 + c_7 + c_8Z + c_9Z^2 + c_{10}Z^3,$$

identificando U_1 com $\mathbb{A}^2$, temos $(0 : 1 : 0) \mapsto (0,0)$. Também temos que

$$\frac{\partial F}{\partial X}(X,Z) = 3c_1X^2 + 2c_2X + 2c_3XZ + c_4 + c_5Z + c_6Z^2,$$

$$\frac{\partial F}{\partial Z}(X,Z) = c_5X + 2c_6XZ + c_8 + 2c_3Z + 3c_10Z^2,$$

então, $\dfrac{\partial F}{\partial X}(0,0) = c_4$ e $\dfrac{\partial F}{\partial Z}(0,0) = c_8$. Como E é não singular, então a reta tangente a E em $\mathcal{O}$ é $c_4X + c_8Z = 0$. Também temos que a reta no infinito é $Z = 0$, assim devemos ter $c_4 = 0$ e portanto $c_8 \neq 0$. Se $c_4 \neq 0$, então realizamos a mudança de variáveis $\tilde{Z} = X + \frac{c_8}{c_4}Z$.

Substituindo $Z = 0$ em $F(X,1,Z)$, obtemos

$$F = c_7 + c_4X + c_2X^2 + c_1X^3.$$

Como $\mathcal{O}$ é ponto de inflexão, então $(X,E)_{\mathcal{O}} \geq 3$, logo $c_2 = 0$. Assim, E fica

$$c_1X^3 + c_3X^2Z + c_5XYZ + c_6XZ^2 + c_8Y^2Z + c_9YZ^2 + c_{10}Z^3, \quad c_8 \neq 0. \tag{2.6}$$

Observe que $c_1 \neq 0$, pois caso contrário o polinômio acima seria divisível por Z. Queremos que os coeficientes de X^3 e de Y^2Z sejam iguais a 1, então vamos dividir (2.6) por c_1 e substituir Z por $-\frac{c_1}{c_8}Z$, assim obtemos E na forma

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_5Z^3.$$

Por fim, temos que $(iii) \Longrightarrow (i)$, pois o ponto $\mathcal{O}$ é um ponto da cúbica dada em (iii).

□

Seja $\mathcal{C}$ uma cúbica definida por

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

A desomogeneização de E em relação a variável Z é dada por

$$F_\star = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6,$$

ou seja, no plano afim, $\mathcal{C}$ pode ser vista como

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

O ponto $P = (0:1:0) \in \mathcal{C}$ é o ponto no infinito cuja multiplicidade é 3, pois tomando a reta no infinito $Z = 0$, temos

$$(Z, \mathcal{C})_P = (Z, F_\star)_{(0,0)} = (Z, Z + a_1XZ + a_3Z^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3) = 3.$$

Assim, P é um ponto de inflexão.

Quando for conveniente podemos fazer uma mudança de variáveis e trabalhar com $\mathcal{C}$ numa forma mais fácil. No caso em que $\mathbb{K} = \mathbb{Q}$ (isso pode ser feito sempre que a característica de $\mathbb{K} \neq 2$ ou 3) fazemos

$$X' = X, \quad Y' = Y + \frac{a_1}{2}X\,, Z' = Z\,,$$

e eliminamos o termo $X'Y'Z'$.

Renomeando as variáveis como X,Y,Z, podemos realizar uma nova mudança de variáveis

$$X' = X + \frac{a_2}{3}, \quad Y' = Y + \frac{a_3}{2}, Z' = Z.$$

Renomeamos novamente as variáveis como X, Y, Z e realizamos uma nova mudança de variáveis e por fim eliminamos os termos em X^2 e Y, obtendo a equação

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

A proposição a seguir nos ajudará a provar que com uma dada operação no conjunto dos pontos racionais de uma curva elíptica vale a lei associativa. Antes de passarmos a essa proposição vamos fazer um lema.

Lema 2.1 *Sejam $P_1, \ldots, P_5$ cinco pontos distintos, então existe uma cônica $\mathbb{Q}$ (possivelmente degenerada) que passa por eles.*

Demonstração: Sabemos que uma cônica Q tem equação

$$aX^2 + bY^2 + cXY + dXZ + eYZ + fZ^2, \tag{2.7}$$

onde $(a,b,c,d,e,f) \neq 0$. Dados cinco pontos quaisquer, substituindo-os na equação da cônica obtemos um sistema com cinco equações e seis incógnitas. Isto pode ser representado por uma aplicação linear $T : \mathbb{K}^6 \longrightarrow \mathbb{K}^5$, cujo núcleo é cujo núcleo está composto pelos pontos (a,b,c,d,e,f) tais que os cinco pontos dados pertencem à cônica definida por (2.7). Pelo teorema do núcleo e da imagem, temos $\dim \ker T + \dim \mathrm{ImT} = 6$ e $\dim \mathrm{ImT} \leq 5$, então $\dim \ker T \geq 1$. Isto é, dados cinco pontos distintos quaisquer, existe uma cônica Q que passa por eles. □

Proposição 2.2 *Se duas curvas cúbicas em $\mathbb{P}^2(\mathbb{Q})$ se intersectam em nove pontos, então toda cúbica que passa por oito desses pontos, também passará pelo nono ponto.*

Demonstração: Faremos o caso em que os pontos $P_i, i = 1, \ldots, 9$ são distintos. Sejam E_1 e E_2 duas cúbicas que se intersectam exatamente nos pontos $P_1, \ldots, P_9$ e seja E uma cúbica que passa por $P_1, \ldots, P_8$. Se E é dependente de E_1 e E_2, então $E = \lambda_1 E_1 + \lambda_2 E_2$, para algum $\lambda_1, \lambda_2 \in \mathbb{Q}$ e portanto $P_9 \in E$. Se E, E_1 e E_2 são independentes, então $\lambda_1, \lambda_2, \lambda_3$ podem ser escolhidos de modo que $F = \lambda_1 E_1 + \lambda_2 E_2 + \lambda_3 E$ passe por quaisquer dois pontos dados. De fato, dados os pontos distintos A e B, $(\lambda_1, \lambda_2, \lambda_3)$ pertence ao núcleo da transformação linear $T : \mathbb{Q}^3 \longrightarrow \mathbb{Q}^2$ definida pela matriz

$$\begin{pmatrix} E_1(A) & E_2(A) & E(A) \\ E_1(B) & E_2(B) & E(B) \end{pmatrix}.$$

Pelo teorema do núcleo e da imagem, temos $3 = \dim \ker T + \dim \mathrm{Im}T$ e além disso $\dim \mathrm{Im}T \leq 2$, então existe ao menos um $(\lambda_1, \lambda_2, \lambda_3) \neq (0, 0, 0)$ no núcleo de T.

Vejamos que a existência de F, satisfazendo as condições acima, levam a uma contradição, mas antes faremos algumas observações.

Observação 2.1 (1) *Vejamos primeiro que dos nove pontos P_i, quatro não podem estar em uma mesma reta. De fato, pelo teorema de Bézout, uma reta e uma cúbica sem componente comum (isto é, a reta não é uma componente da cúbica) tem multiplicidade de interseção igual a 3, assim essa reta seria uma componente de E_1 e E_2, mas essas duas cúbicas não possuem componente comum.*

(2) *Também temos que sete desses pontos não podem estar em uma mesma cônica $\mathcal{C}$, pois pelo teorema de Bézout, uma cônica e uma cúbica sem componente comum se intersectam em seis pontos, logo a cônica e a cúbica devem ter uma componente comum, mas E_1 e E_2 não tem componente comum, logo a única possibilidade é que $\mathcal{C} = L_1 \cup L_2$, onde $L_1 \subseteq E_1$ e $L_2 \subseteq E_2$. Observe que*

$$\begin{aligned} \mathcal{C} \cap E_1 \cap E_2 &= (L_1 \cup L_2) \cap E_1 \cap E_2 \\ &= (L_1 \cap E_1 \cap E_2) \cup (L_2 \cap E_1 \cap E_2) \\ &= (L_1 \cap E_2) \cup (L_2 \cap E_1). \end{aligned}$$

Por hipótese E_1 e E_2 não tem componente comum, então

$$|\mathcal{C} \cap E_1 \cap E_2| \leq |L_1 \cap E_2| + |L_2 \cap E_1| = 3 + 3 = 6 < 7,$$

impossível. Isso prova a afirmação inicial.

Vamos dividir nossa demonstração em alguns casos:

(i) Suponha que P_1, P_2, P_3 estão em L. Afirmamos que existe uma única cônica que contem os pontos $P_4, \ldots, P_8$. Pelo lema 2.1, temos que existe uma cônica que passa pelos pontos acima. Vejamos agora que essa cônica Q é única. Suponha que exista uma outra cônica Q' passando pelos pontos acima, pelo teorema de Bézout temos que duas cônicas sem componente comum se intersectam em quatro pontos, assim Q e Q' devem ter uma componente comum. Seja L' essa componente, isto é, $L' \subseteq Q \cap Q'$, assim $Q = L' \cup L_1$ e $Q' = L' \cup L_2$ e portanto $Q \cap Q' = (L' \cup L_1) \cap (L' \cup L_2) = L' \cup (L_1 \cap L_2)$. Mas $L_1 \cap L_2$ tem um ponto comum, logo L' deve ter pelo menos quatro dos pontos P_i, $i = 4, \ldots, 8$, mas já vimos que isso não pode ocorrer.

Seja A um ponto em L, distinto de P_1, P_2 e P_3 e seja B um ponto que não está nem em Q nem em L. Temos que $F = \lambda_1 E_1 + \lambda_2 E_2 + \lambda_3 E$ contem $P_1, \ldots, P_8$ e podemos escolher $\lambda_1, \lambda_2, \lambda_3$ de modo que F contenha A e B. Observe que L será necessariamente uma componente de F, pois intersecta F em pelo menos quatro pontos, isto é, F se fatora como um polinômio de grau 1 e um polinômio de grau 2 (que pode ou não se fatorar). Isto é, $F = L \cup Q''$, onde Q'' é uma cônica que pode ou não se fatorar. Como $P_4, \ldots, P_8 \in F$ e L contem P_1, P_2, P_3, então $P_4, \ldots, P_8 \in Q''$. Mas Q é a única cônica que contem $P_4, \ldots, P_8$, logo $Q'' = Q$ e $F = L \cup Q$. Mas isso não pode ocorrer, pois $B \notin Q$ e $B \notin L$.

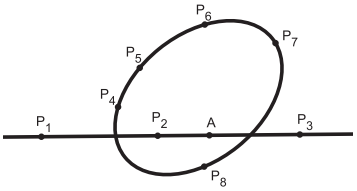

Figura 2.1: Caso (i)

(ii) Suponha que $P_1, \ldots, P_6$ são pontos de uma cônica Q. Seja L a reta que passa por P_7 e P_8. Tomando A como um ponto de Q e B um ponto que não está em Q e nem em L temos que Q deve ser uma componente de F, de fato, como E e Q têm pelo menos 7 pontos em comum e pelo teorema de Bézout uma cônica e uma cúbica sem componente comum se intersectam em seis pontos, então Q e F devem ter uma componente comum. Seja $\tilde{L}$ essa componente, então $Q = \tilde{L} \cup \tilde{\tilde{L}}$ e $F = \tilde{L} \cup \tilde{Q}$ (onde $\tilde{Q}$ pode ou não se fatorar), assim $Q \cap F = \tilde{L} \cup (\tilde{\tilde{L}} \cap \tilde{Q})$. Pelo teorema de Bézout, $\tilde{\tilde{L}} \cap \tilde{Q}$ tem dois pontos de interseção, então cinco dos sete pontos pertencem a $\tilde{L}$ e portanto $\tilde{L}$ passa por quatro dos pontos P_i, mas isso não é possível, então $\tilde{\tilde{L}}$ e $\tilde{Q}$ possuem uma componente comum, ou seja, $\tilde{\tilde{L}} \subseteq \tilde{Q}$, logo $Q = \tilde{L} \cup \tilde{\tilde{L}} \subseteq \tilde{L} \cup \tilde{Q} = F$. Assim, $F = Q \cup \tilde{\tilde{L}}$, onde $P_7, P_8 \in \tilde{\tilde{L}}$, ou seja, $L = \tilde{\tilde{L}}$. Mas $B \in F = Q \cup L$ e $B \notin Q$ e $B \notin L$. Contradição.

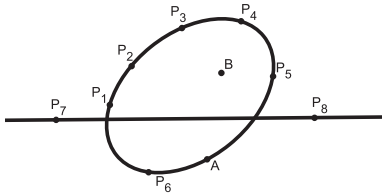

Figura 2.2: Caso (ii)

(iii) Suponha agora que três dos pontos $P_1, \ldots, P_8$ não se encontram em uma reta e que seis dos pontos não se encontram em uma cônica. Considere L a reta que passa por P_1 e P_2 e Q a cônica que passa por $P_3, \ldots, P_7$. Como $L \cap F = 4$, então L é uma componente de F, assim $F = L \cup \tilde{Q}$. Como $P_3, \ldots, P_7 \notin L$, então $P_3, \ldots, P_7 \in \tilde{Q}$, logo $\tilde{Q} = Q$. Assim, $F = L \cup Q$, mas $P_8 \notin Q$ e $P_8 \notin L$. Absurdo.

□

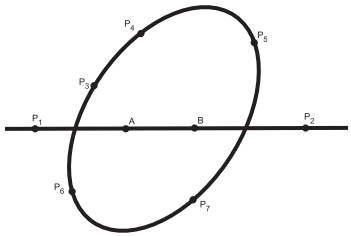

Figura 2.3: Caso (*iii*)

2.2 A lei de grupo

Sejam E uma curva elíptica e $L \subset \mathbb{P}^2$ uma reta, como E tem grau 3, pelo teorema de Bezout, L intersecta E em exatamente 3 pontos , digamos P, Q e R. Observe que se L é tangente a E, então P, Q e R não são distintos.

Considere P e Q pontos da curva elíptica E e seja L a reta que passa por esses dois pontos. Pelo teorema de Bezout, L intersecta a curva E em um terceiro ponto que será denotado por $P \star Q$. Queremos introduzir uma lei de grupo sobre o conjunto dos pontos de E. Temos que $(E(\mathbb{Q}), \star)$ não é um grupo, já que nem sequer possui elemento neutro. Iremos definir a lei de grupo da seguinte maneira:

Definição 2.2 *(Lei de composição) Sejam $P, Q \in E$, L a reta que liga P e Q (a reta é tangente a E se $P = Q$) e R o terceiro ponto de interseção de L com E. Seja L' a reta que liga R e $\mathcal{O}$, então $P + Q$ é o terceiro ponto de interseção de L' com E.*

Teorema 2.1 *Sejam E uma curva elíptica sobre $\mathbb{Q}$ e $\mathcal{O} \in E(\mathbb{Q})$, então $(E(\mathbb{Q}), +)$ é um grupo abeliano.*

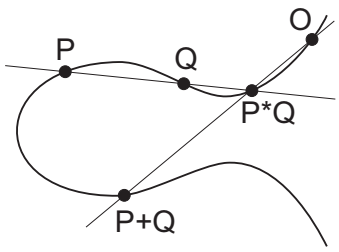

Figura 2.4: Lei de grupo

Demonstração: Vejamos que $+$ é comutativa, isto é, $P + Q = Q + P$. Temos que $P \star Q = Q \star P$, logo $\mathcal{O} \star (P \star Q) = \mathcal{O} \star (Q \star P)$.

Para ver que $P + \mathcal{O} = P$, considere L_1 a reta que passa por P e $\mathcal{O}$, pelo teorema de Bezout existe um terceiro ponto $P \star \mathcal{O} \in E \cap L_1$. Agora, seja L_2 a reta que passa por $\mathcal{O}$ e por $P \star \mathcal{O}$. Observe que $L_2 = L_1$ e o terceiro ponto em L_2 que intersecta E é o ponto P. Assim,

$$P = \mathcal{O} \star (P \star \mathcal{O}) = P + \mathcal{O},$$

isto é, $\mathcal{O}$ é o elemento neutro de $+$.

Agora queremos determinar o inverso de um ponto $Q \in E$. Para isso tome L_1 a reta tangente à cúbica no ponto $\mathcal{O}$ e seja S o terceiro ponto de interseção da curva E e a reta L_1.

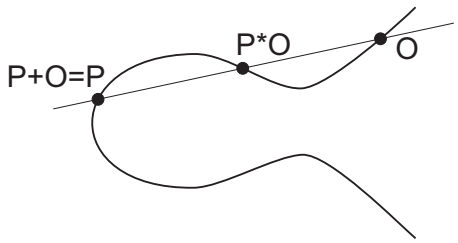

Figura 2.5: Elemento neutro

Seja L_2 a reta que passa por Q e S, então existe um terceiro ponto em $L_2 \cap E$, que chamaremos de P, assim $Q \star P = S$. Como a reta que passa por $\mathcal{O}$ e S é L_1, então $\mathcal{O} \star S = \mathcal{O}$, isto é,

$$Q + P = \mathcal{O} \star (Q \star P) = \mathcal{O} \star S = \mathcal{O}$$

e P é o inverso de Q.

Portanto, $P = -Q$.

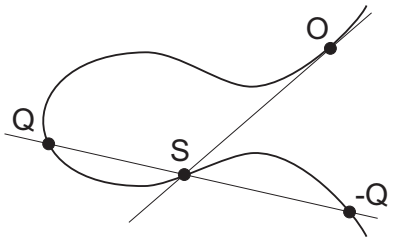

Figura 2.6: Inverso de um ponto Q

Vejamos que + é associativa.

Temos que

$$(P + Q) + R = \mathcal{O} \star ((P + Q) \star R),$$
$$P + (Q + R) = \mathcal{O} \star (P \star (Q + R)).$$

Assim, devemos mostrar que $(P + Q) \star R = P \star (Q + R)$.

Considere as retas

- L_1, que passa por P, Q e $P \star Q$;
- R_1, que passa por $\mathcal{O}$, $P \star Q$ e $P + Q$;
- L_2, que passa por $P + Q$, R e $(P + Q) \star R$;
- R_2, que passa por Q, R e $Q \star R$;
- L_3, que passa por $\mathcal{O}$, $Q \star R$ e $Q + R$;
- R_3, que passa por P, $Q + R$ e $P \star (Q + R)$.

Considere as cúbicas E_l definida pela união de L_1, L_2 e L_3 e E_r definida pela união de R_1, R_2 e R_3. Temos que

$$E \cap E_l = \{P, Q, P \star Q, R, (P + Q) \star R, \mathcal{O}, Q \star R, Q + R\}.$$

Veja que E_r passa por oito desses pontos, logo pela proposição 2.2, E_r passa também pelo nono ponto, $(P + Q) \star R$.

Por outro lado

$$E \cap E_r = \{\mathcal{O}, P \star Q, P + Q, Q, R, Q \star R, Q + R, P, P \star (Q + R)\},$$

logo $(P + Q) \star R = P \star (Q + R)$.

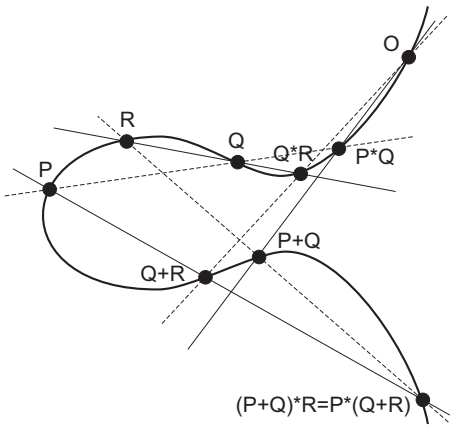

Figura 2.7: Lei associativa

□

2.2.1 Fórmulas explícitas para a lei de grupo

Seja E uma cúbica na forma de Weierstrass. Já vimos que uma equação nesta forma pode ser transformada em uma equação do tipo

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Além disso uma curva elíptica na forma de Weierstrass possui o ponto $\mathcal{O} = (0 : 1 : 0)$. Observe que uma reta que passa por esse ponto e por um ponto qualquer de $\mathbb{P}^2$ é uma reta vertical no plano afim. De fato, seja $L : aX + bY + cZ = 0$ e tome $P = (x : y : 1)$. O sistema

$$\begin{cases} ax + by + c = 0 \\ a \cdot 0 + b \cdot 1 + c \cdot 0 = 0 \end{cases}$$

implica, $c = -ax$, logo $L : aX - axZ = 0$ e portanto $L : X = xZ$.

Queremos descrever algebricamente a adição de dois pontos P e Q de uma curva elíptica E. Vamos considerar as seguintes equações da curva elíptica (no plano afim):

$$Y^2 = X^3 + AX + B, \tag{2.8}$$

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{2.9}$$

A reta que passa por $\mathcal{O}$ e por $P = (x_3, y_3)$ é $X = x_3$, intersectando essa reta com a curva elíptica (2.8), obtemos

$$Y^2 = x_3^3 + ax_3 + B,$$

isso implica $Y^2 = y_3^2$, assim temos $(Y - y_3)(Y + y_3) = 0$, portanto a reta $X = x_3$ intersecta a curva elíptica nos pontos $\mathcal{O}, (x_3, y_3)$ e $(x_3, -y_3)$.

Agora vamos fazer o mesmo para a curva elíptica (2.9). Intersectando a reta $X = x_3$ com essa cúbica, obtemos

$$Y^2 + a_1x_3Y + a_3Y = x_3^2 + a_2x_3^2 + a_4x_3 + a_6,$$

isso implica

$$Y^2 + a_1x_3Y + a_3Y = y_3^2 + a_1x_3y_3 + a_3y_3,$$

logo

$$(Y^2 - y_3^2) + a_1x_3(Y - y_3) + a_3(Y - y_3) = 0,$$

portanto $(Y - y_3)(Y + y_3 + a_1x_3 + a_3) = 0$.

Segue que a reta $X = x_3$ tem os seguintes pontos de interseção com a cúbica:

$$\mathcal{O}, (x_3, y_3), (x_3, -y_3 - a_1x_3 - a_3).$$

As figuras abaixo nos mostram o inverso de um ponto Q e a adição de pontos na cúbica da forma (2.8).

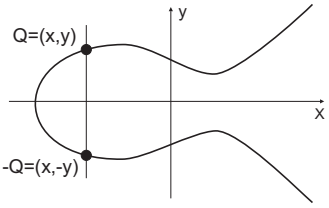

Figura 2.8: Inverso de um ponto Q

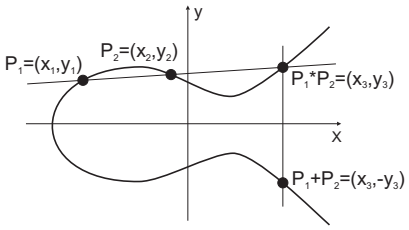

Figura 2.9: Adição de pontos de E

Sejam $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, pontos de uma curva elíptica E, pelo teorema de Bézout existe $P \star Q = (x_3, y_3) \in E \cap L$, onde L é a reta que que passa por P e Q e intersecta E nesses pontos. Temos algumas possibilidades:

(i) se $x_1 \neq x_2$, então o coeficiente angular é dado por $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ e L possui equação $Y = \lambda(X - x_1) + y_1$.

(ii) se $x_1 = x_2$ e $y_1 = y_2$, então λ é o coeficiente angular da reta tangente no ponto P. No caso em que E é dada pela equação (2.9), temos

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

e no caso em que E é dada pela equação (2.8), temos

$$\lambda = \frac{3x_1^2 + A}{2y_1}$$

e L é dada também por $Y = \lambda(X - x_1) + y_1$.

(iii) se $x_1 = x_2$ e $y_1 \neq y_2$, então $P + Q = \mathcal{O}$.

Vamos encontrar as coordenadas de $P + Q$ quando a curva elíptica se encontra tanto na forma (2.8), quanto na forma (2.9).

Caso em que a curva elíptica se encontra na forma (2.8):

Encontremos primeiro as coordenadas do ponto $P \star Q$, de acordo com (i) e (ii). Devemos substituir a equação da reta L em (2.8), ou seja,

$$(\lambda X - \lambda x_1 + y_1)^2 = X^3 + AX + B,$$

o que implica

$$X^3 - \lambda^2 X^2 + (A + 2x_1\lambda^2 - 2\lambda y_1)X + (B - x_1^2\lambda^2 + 2\lambda x_1 y_1 - y_1^2) = 0.$$

As raízes dessa cúbica em X são as abcissas de P, Q e $P \star Q$. Assim,

$$X^3 - \lambda^2 X^2 + (A + 2x_1\lambda^2 - 2\lambda y_1)X + (B - x_1^2\lambda^2 + 2\lambda x_1 y_1 - y_1^2) = (X - x_1)(X - x_2)(X - x_3).$$

Como

$$(X - x_1)(X - x_2)(X - x_3) = X^3 + (-x_1 - x_2 - x_3)X^2 + (x_1x_3 + x_2x_3 + x_1)X - x_1x_2x_3,$$

então da igualdade de polinômios, temos $\lambda^2 = -x_1 - x_2 - x_3$. Isto é,

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

Temos ainda, $y_3 = \lambda(x_3 - x_1) + y_1$, logo

$$P + Q = (x_3, -y_3) = (\lambda^2 - x_1 - x_2, -\lambda(x_3 - x_1) - y_1).$$

Caso em que a curva elíptica se encontra na forma (2.9):

Como antes, encontramos primeiro as coordenadas do ponto $P \star Q$, de acordo com (i) e (ii). Substituindo a equação da reta L em (2.9), obtemos

$$-X^3 + \left(\lambda^2 + a_1\,\lambda - a_2\right)\,X^2 + \left(-2\,x_1\,\lambda^2 + (a_3 + 2\,y_1 - a_1\,x_1)\,\lambda - a_4 + a_1\,y_1\right)\,X +$$

$$x_1^2\,\lambda^2 + (-x_1\,a_3 - 2\,x_1\,y_1)\,\lambda - a_6 + y_1\,a_3 + y_1^2 = 0.$$

Um raciocínio análogo ao anterior nos fornece

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$$

e além disso $y_3 = \lambda(x_3 - x_1) + y_1$ e com isso obtemos

$$P + Q = (x_3, -y_3 - a_1x_3 - a_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -a_1x_3 - a_3 - \lambda(x_3 - x_1) - y_1).$$

No caso (iii), temos que se $P = (x_1, y_1)$ e $Q = (x_1, y_2)$, com $y_1 \neq y_2$, então a reta que liga P e Q é uma reta vertical e tem equação $X = x_1$, que em coordenadas projetivas tem a forma $X = x_1Z$. O terceiro ponto de interseção dessa reta com E é o ponto $\mathcal{O}$. Assim,

$$P + Q = \mathcal{O} \star \mathcal{O} = \mathcal{O}.$$

Exemplo 2.1 *Seja a curva elíptica* $Y^2 = X^3 + 1$ *e sejam* $P = (0,1)$, $Q = (2,3) \in E(\mathbb{Q})$. *Temos que o coeficiente angular da reta que liga* P *e* Q *é* $\lambda = 1$. *Assim,*

$$x_3 = \lambda^2 - x_1 - x_2 = 1^2 - 0 - 2 = -1 \ ,$$

$$y_3 = \lambda(x_3 - x_1) + y_1 = 1(-1 - 0) + 1 = 0.$$

Logo, $P + Q = (-1, 0)$.

Vamos obter agora $P + P$. *Nesse caso temos* $\lambda = \dfrac{3x_1^2 + A}{2y_1} = \dfrac{3 \cdot 0^2 + 0}{2 \cdot 1} = 0$. *Também temos que*

$$x_3 = \frac{9x_1^2 + 6x_1^2 A + A^2 - 8x_1 y_1^2}{4y_1^2} = 0,$$

$$y_3 = \lambda(x_3 - x_1) + y_1 = 1.$$

Portanto, $P + P = (0, -1)$.
Observe que $3P = \mathcal{O}$, *pois* $3P = 2P + P = (0,-1) + (0,1) = \mathcal{O}$.

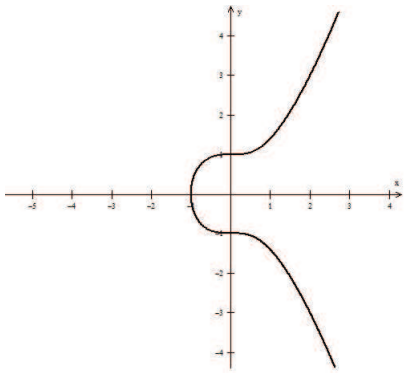

Figura 2.10: Curva elíptica $E : Y^2 = X^3 + 1$

2.3 Pontos de torção

Dizemos que um elemento P do grupo $E(\mathbb{Q})$ tem ordem m se

$$mP = \underbrace{P + P + \cdots + P}_{m \ vezes} = \mathcal{O},$$

e $nP \neq \mathcal{O}$, para todo inteiro $1 \leq n < m$. Se m existe, então P tem ordem finita, caso contrário dizemos que P tem ordem infinita. No exemplo 2.1, vimos que o ponto $P = (0,1)$ é tal que $3P = \mathcal{O}$ e tanto P quanto $2P$ são diferentes de $\mathcal{O}$. Assim, $(0,1)$ é um ponto de ordem finita.

Vamos denotar por $E(\mathbb{Q})_{tors}$ o subgrupo de torção de $E(\mathbb{Q})$, isto é, o subgrupo de $E(\mathbb{Q})$ dos pontos de ordem finita. Simbolicamente,

$$E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) \mid nP = \mathcal{O}, \text{ para algum inteiro positivo } n\}.$$

Durante o século XIX muitos cálculos foram realizados para encontrar a ordem dos elementos de uma curva elíptica. Os valores obtidos por eles sempre eram um dos valores da lista abaixo

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12.$$

Ninguém conseguiu encontrar uma curva E na qual $E(\mathbb{Q})$ continha um ponto de ordem $11, 13$ ou maior. Este resultado foi provado pelo matemático Barry Mazur em 1978.

Teorema 2.2 *(Mazur) Suponha que P é um ponto de ordem n em $E(\mathbb{Q})_{tors}$, então $1 \leq n \leq 10$ ou $n = 12$. Além disso,*

(i) $E(\mathbb{Q})_{tors}$ é um grupo cíclico de ordem $1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ ou 12. Isto é,

$$E(\mathbb{Q})_{tors} = \langle A_1 \rangle$$

para algum ponto A_1 que tem ordem $1, 2, \ldots, 10$ ou 12; ou

(ii) $E(\mathbb{Q})_{tors}$ é gerado por dois elementos A_1 e A_2, onde a ordem de A_1 é $2, 4, 6$ ou 8 e a ordem de A_2 é 2. Isto significa que

$$E(\mathbb{Q})_{tors} = \langle A_1, A_2 \rangle,$$

onde as possíveis ordens de A_1 e A_2 estão acima.

O teorema a seguir também é bastante útil para encontrar todos os pontos de torção de uma curva elíptica.

Teorema 2.3 *(Teorema de Nagel-Lutz) Seja*

$$Y^2 = X^3 + aX^2 + bX + c,$$

uma cúbica não singular com coeficientes inteiros, a, b, c e seja Δ o discriminante da cúbica polinomial $f(x)$,

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Seja $P = (x, y)$ um ponto racional de ordem finita da curva elíptica. Então x e y são inteiros e temos $y = 0$ (neste caso P tem ordem 2) ou $y \mid \Delta$.

Demonstração: Ver [10], Chapter II, Section 5. □

Corolário 2.1 *Nas condições acima, se $P = (x, y)$ é um ponto racional de ordem finita com $y \neq 0$, então $y^2 \mid \Delta$.*

Demonstração: Ver [9], Corollary 7.2. □

Exemplo 2.2 *Considere a curva elíptica E definida por $Y^2 = X^3 + X - 2$. O ponto $(1, 0)$ é um ponto de 2-torção de E. De fato,*

$$(1, 0) + (1, 0) = \mathcal{O} \star ((1, 0) \star (1, 0)) = \mathcal{O} \star \mathcal{O} = \mathcal{O}.$$

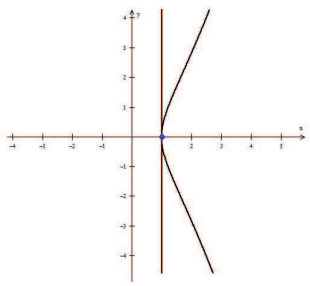

Figura 2.11: $E : Y^2 = X^3 + X - 2$

Exemplo 2.3 *Seja E a curva elíptica definida por $E : Y^2 = X^3 + X + 2$, então*

$$E(\mathbb{Q})_{tors} = \{(-1, 0), (1, -2), (1, 2), \mathcal{O}\}.$$

Temos que

$$(-1, 0) + (-1, 0) = \mathcal{O} \star ((-1, 0) \star (-1, 0)) = \mathcal{O} \star \mathcal{O} = \mathcal{O}.$$

logo $(-1, 0)$ é um ponto de 2-torção.

O ponto $P = (1, 2)$ é um ponto de 4-torção. De fato, temos que $2P = (-1, 0)$, pois

$$x_3 = \lambda^2 - 2x_1 = 1 - 2 \cdot 1 = -1,$$

$$y_3 = \lambda(x_3 - x_1) + y_1 = 1(-1 - 1) + 2 = 0.$$

Assim,

$$4P = 2P + 2P = (-1, 0) + (-1, 0) = \mathcal{O}.$$

Também temos que

$$(1, -2) + (1, -2) = (-1, 0),$$

logo $4(1, -2) = \mathcal{O}$.

Queremos ainda ver que os pontos acima são os únicos pontos de torção de $E(\mathbb{Q})$. Temos que o discriminante $\Delta = -112$. Pelo corolário 2.1, temos que um ponto (x, y) da curva elíptica é de torção, se $x, y \in \mathbb{Z}$, $y = 0$ ou $y^2 \mid \Delta$. Como $\Delta = -112$, então os valores possíveis de y são: $0, \pm 1, \pm 2, \pm 4$. Para $y = 0$ e $y = \pm 2$, obtemos os pontos acima. Para $y = \pm 1$, a cúbica correspondente em x é $x^3 + x + 1 = 0$ e para $y = \pm 4$ a cúbica correspondente em x é $x^3 + x - 14 = 0$. Ambas as cúbicas não possuem soluções inteiras.

2.4 Curvas projetivas planas e divisores

Seja $\mathcal{C}$ uma curva projetiva plana sobre $\mathbb{Q}$ definida por um polinômio F irredutível, de grau m. Um divisor D da curva $\mathcal{C}$ é uma soma formal de pontos da curva, isto é,

$$D = \sum_{P \in \mathcal{C}} n_p P,$$

onde P percorre todos os pontos de $\mathcal{C}$ e os inteiros n_p são zero, salvo em um número finito de pontos de $\mathcal{C}$. O conjunto de todos os divisores de $\mathcal{C}$ formam um grupo chamado $Div(\mathcal{C})$. A soma

$$\deg D = \sum_{P \in \mathcal{C}} n_p$$

é o grau de D.

Seja f uma função racional de $\mathcal{C}$ tal que $f = \dfrac{G}{H}$, $\deg(G) = \deg(H) = n$ e H não é múltiplo de F. Podemos associar a f um divisor

$$Div(f) = \sum_{P \in \mathcal{C}} ord_P(f) P,$$

onde $ord_P(f) = (F, G)_P - (F, H)_P$. Pelo teorema de Bézout, temos

$$\sum_{P \in \mathcal{C}} ord_P(f) = \sum_{P \in \mathcal{C}} (F, G)_P - \sum_{P \in \mathcal{C}} (F, H)_P = nm - nm = 0.$$

O divisor de uma função racional sobre $\mathcal{C}$ é dito divisor principal. O conjunto dos divisores principais é denotado por $\mathcal{P}(\mathcal{C})$. Denotaremos ainda o conjunto dos divisores de grau 0 por

$Div^0(\mathcal{C})$. Dizemos que dois divisores, D e D' são equivalentes se $D - D'$ é um divisor principal, simbolicamente

$$D \sim D' \Longleftrightarrow D - D' \text{ é principal.}$$

Temos as seguintes inclusões

$$\mathcal{P}(\mathcal{C}) \subseteq Div^0(\mathcal{C}) \subseteq Div(\mathcal{C}),$$

definimos os grupos de Picard como

$$Pic(\mathcal{C}) = Div(\mathcal{C})/\mathcal{P}(\mathcal{C}), \quad Pic^0(\mathcal{C}) = Div^0(\mathcal{C})/\mathcal{P}(\mathcal{C})$$

(para mais detalhes sobre este assunto ver [6]).

O gênero de uma curva não será tratado neste trabalho, um texto sobre esse assunto pode ser encontrado em [6], ainda assim iremos dizer o que é gênero de uma curva projetiva plana. Seja $\mathcal{C}$ uma curva projetiva plana não singular, o gênero de $\mathcal{C}$ é dado por

$$g(\mathcal{C}) = \frac{(\deg \mathcal{C} - 1)(\deg \mathcal{C} - 2)}{2}.$$

Observe que uma curva projetiva plana de grau 1 ou 2 tem gênero 0 e no caso em que o grau da curva é 3, temos que o gênero é 1. Uma curva elíptica é uma curva de gênero 1 com um ponto $\mathcal{O} \in E(\mathbb{K})$.

Proposição 2.3 *Seja $\mathcal{C}$ uma curva projetiva não singular de gênero 1 e seja $\mathcal{O} \in \mathcal{C}(\mathbb{K})$. A função*

$$P \longmapsto [P] - [\mathcal{O}] : \mathcal{C}(\mathbb{K}) \longrightarrow Pic^0(\mathcal{C})$$

é uma bijeção.

Demonstração:

Ver [6] página 35.

A bijeção $\mathcal{C}(\mathbb{K}) \longrightarrow Pic^0(\mathcal{C})$ define uma estrutura de grupo abeliano em $\mathcal{C}(\mathbb{K})$, que é determinada pela condição

$$P + Q = S \Longleftrightarrow [P] + [Q] = [S] + [\mathcal{O}].$$

Afirmamos que esta estrutura de grupo é a mesma que já definimos conforme teorema 2.1. Sejam $P, Q \in \mathcal{C}(\mathbb{K})$ e suponha $P + Q = S$ com a lei de composição já vista. Considere também L_1 a reta que passa por P e Q e L_2 a reta que passa por $\mathcal{O}$ e S, sabemos que L_1 e L_2 tem um ponto comum na interseção com $\mathcal{C}$, chamaremos esse ponto de R. Considere L_1 e L_2 como formas lineares em X, Y, Z e seja $\varphi = \dfrac{L_1}{L_2}$, então φ tem zeros simples nos pontos P, Q e R e polos simples em $\mathcal{O}, S$ e R e portanto

$$Div(\varphi) = [P] + [Q] + [R] - [\mathcal{O}] - [S] - [R] = [P] + [Q] - [S] - [\mathcal{O}],$$

assim, $[P] + [Q] \sim [S] + [\mathcal{O}]$ e $P + Q = S$, de acordo com a estrutura de grupo já vista.

Observação 2.2 *Quando escolhemos um elemento neutro diferente $\mathcal{O}' \in E(\mathbb{K})$ basta transladar $\mathcal{O}$, para obter a lei de grupo.*

□

2.5 Um exemplo interessante

Vamos encontrar uma fórmula de duplicação de um ponto numa quártica.

Seja $\mathcal{C}_1$ definida por

$$y^2 = x^4 + x^3 + x^2 + 1. \tag{2.10}$$

Observe que os pontos $(1,2),(1,-2) \in \mathcal{C}_1(\mathbb{Q})$, denotaremos esses pontos por P_+ e P_-, respectivamente. Considere também $\mathcal{C}_2$ obtida através da mudança de variáveis

$$x = \frac{1}{u}, \quad y = \frac{w}{u^2},$$

ou seja, $\mathcal{C}_2$ é definida por

$$w^2 = u^4 + u^2 + u + 1. \tag{2.11}$$

Observe que P_+ e P_- são pontos de $\mathcal{C}_2$ e além disso $(0,1)$ e $(0,-1)$ também pertencem a $\mathcal{C}_2$, denotaremos estes pontos por ∞^+ e ∞^-, respectivamente e serão chamados de pontos no infinito de C_1.

Considere a curva $E = \mathcal{C}_1 \cup \mathcal{C}_2$, onde um ponto (x,y) de $\mathcal{C}_1$ é equivalente a um ponto (u,w) de $\mathcal{C}_2$ se $y = \frac{w}{u^2}$ e $x = \frac{1}{u}$. Através de uma mudança de variáveis é possível transformar este tipo de curva em uma cúbica no plano projetivo, um algoritmo para isso pode ser encontrado em [8]. Isto é, a curva E é isomorfa a uma curva elíptica e portanto seu conjunto de pontos racionais possui estrutura de grupo abeliano.

Vamos calcular o divisor de x. Para isso fazemos $x = 0$ na equação em (2.10), logo $y = \pm 1$, assim

$$\begin{aligned} Div\,(x) &= (0,1) + (0,-1) - (\infty^+ + \infty^-) \\ &= (0,1) - \infty^+ + (0,-1) - \infty^- \end{aligned} \tag{2.12}$$

Calculemos agora o divisor de $x-1$, isto é, fazemos $x = 1$ em (2.10), logo $y = \pm 2$, assim

$$Div(x-1) = (1,2) + (1,-2) - (\infty^+\infty^-) = P_+ + P_- - (\infty^+ + \infty^-).$$

Exemplo 2.4 *Queremos obter a adição de pontos numa quártica, para isso procuramos uma parábola f que se anula 3 vezes em P_+, assim $(f, \mathcal{C}_1) = P_+ + P_+ + P_+ + Q = 3P_+ + Q$, logo*

$$Div(f) = 3P_+ + Q - 2(\infty^+ + \infty^-).$$

A parábola f deve se anular em P_+, assim temos $y - 2 = (x-1)(ax+b)$, logo

$$y^2 = (x-1)^2(ax+b)^2 + 4(x-1)(ax+b) + 4.$$

Como $y^2 = x^4 + x^3 + x^2 + 1$, então

$$\begin{aligned} (x-1)(ax+b) + 4(x-1)(ax+b) &= x^4 + x^3 + x^2 - 3 \\ &= (x-1)(x^3 + 2x^2 + 3x + 3), \end{aligned}$$

logo $(x-1)(ax+b)^2 = x^3 + 2x^2 + (3-4a)x + 3 - 4b$ e por fim obtemos

$$a^2x^3 + (2ab - a^2)x^2 + (b^2 - 2ab)x - b^2 = x^3 + 2x^2 + 3x - 4ax - 3 + 4b.$$

Da igualdade de polinômios segue que

$$\begin{cases} a^2 = 1 \\ 2ab - a^2 = 2 \\ b^2 - 2ab = 3 - 4a \\ 3 - 4b = -b^2 \end{cases},$$

daí $a^2 = 1$, *assim* $-2ab = -3$, *portanto* $b^2 = 6 - 4a$ *e por fim obtemos* $3 - 4a = 4a - 6$.

Dividindo $x^3 + 2x^2 + (3 - 4a)x + 4a - 6$ *por* $x - 1$, *obtemos como quociente* $x^2 + 3x + (6 - 4a)$ *e resto* 0. *Com isso temos*

$$(x-1)^2(ax+b)^2 = (x-1)(x^2 + 3x + 6 - 4a),$$

portanto $(ax + b)^2 = x^2 + 3x + 6 - 4a$. *Tomando* $x = 1$, *temos* $(a + b)^2 = 10 - 4a$ *e de* $3 - 4b = 4a - 6$ *temos* $9 = 4a + 4b$, *então* $a + b = \frac{9}{4}$. *Assim,* $\dfrac{81}{16} = 10 - 4a$ *e temos* $a = \dfrac{79}{64}$ *e* $b = \dfrac{65}{64}$. *Com isso temos que* $x = 1$ *é raiz tripla e* $x = \dfrac{-127}{2145}$ *é raiz simples.*

Fazendo a mudança de variáveis $x = \dfrac{1}{u}$ *e* $y = \dfrac{w}{u^2}$ *na parábola* $f = y - ((x-1)(ax+b)+2)$, *temos*

$$f = \frac{w}{u^2} - \left(\left(\frac{1}{u} - 1\right)\left(\frac{a}{u} + b\right) + 2\right),$$

portanto

$$f = \frac{w - ((1-u)(a+ub) + 2u^2}{u^2}).$$

Quando $x = 0$ *temos os pontos no infinito com multiplicidade* 2, *logo*

$$Div(y - f(x)) = 3(1,2) + \left(-\frac{127}{2145}, \frac{4608634}{4601025}\right) - 2(\infty^+ + \infty^-),$$

assim $3P_+ + Q = -2(\infty^+ + \infty^-)$.

Seja

$$g = \frac{y - ((x-1)(ax+b) + 2}{(x-1)^2)}$$

.

Temos que $Div((x-1)^2) = 2(P_+ + P_-) - 2(\infty^+ + \infty^-)$, *então*

$$Div(g) = 3P_+ + Q - 2(\infty^+ + \infty^-) - 2(P_+ + P_-) + 2(\infty^+ + \infty^-) = P_+ + Q - 2P_-,$$

assim $P_+ + Q = 2P_-$ *e segue que o inverso de* $P_+ - P_-$ *é* $Q - P_-$.

A partir da definição 2.2, encontramos uma fórmula para adicionar pontos em uma curva elíptica, quando ela está definida por uma cúbica plana. No caso acima, a curva elíptica se encontra definida por uma quártica. Se os coeficientes da curva elíptica na forma quártica forem muitos grandes, eles podem ser maiores ainda quando essa curva elíptica for dada na forma cúbica e nesse caso os cálculos da adição de pontos serão quase irrealizáveis. Assim, dependendo do quão grande forem os coeficientes é mais conveniente trabalhar com a curva elíptica na forma quártica, um exemplo claro disto será dado no último capítulo.

Capítulo 3

Teoria dos Números

Neste capítulo apresentamos alguns resultados de teoria dos números, falamos especialmente sobre resíduos quadráticos, tema de extrema importância para o nosso último capítulo. Um resultado muito importante que será demonstrado neste capítulo é sobre as condições para que uma equação do tipo $ax^2 + by^2 + cz^2 = 0$ possua soluções inteiras. Começamos este capítulo com o teorema de Legendre.

Teorema 3.1 *(Legendre) Sejam a, b, c inteiros livres de quadrados, primos entre si, dois a dois e não todos do mesmo sinal. A equação $ax^2+by^2+cz^2 = 0$ tem solução $(x, y, z) \neq (0, 0, 0)$ com x, y, z inteiros se, e somente se, $-bc$ é quadrado módulo a, $-ac$ é quadrado módulo b e $-ab$ é quadrado módulo c.*

Demonstração:

($\Longrightarrow$) Vejamos que $-bc$ é quadrado módulo a. Podemos supor que x, y, z são relativamente primos dois a dois, pois se p é um primo tal que $p \mid (x, y)$, então $p^2 \mid cz^2$, mas c é livre de quadrados, logo $p \mid z^2$, ou seja, $p \mid z$. Assim, $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p}\right)$ seria solução da equação.

Analisando a equação módulo a, temos $by^2 + cz^2 \equiv 0 \pmod{a}$, logo $by^2 \equiv -cz^2 \pmod{a}$. Observe que z é primo com a, pois se p é um primo tal que $p \mid a$ e $p \mid z$, então $p \mid by^2$, mas $(a, b) = 1$, logo $p \mid y^2$, assim $p \mid y$. Absurdo, pois x, y, z são relativamente primos e portanto z é invertível módulo a (vamos denotar o inverso de z módulo a por z^{-1}) e temos $(byz^{-1})^2 \equiv -bc \pmod{a}$.

De modo análogo, mostra-se que $-ac$ é quadrado módulo b e $-ab$ é quadrado módulo c.

($\Longleftarrow$) Suponha sem perda de generalidade, $a < 0, b < 0$ e $c > 0$. Por hipótese existem $u, v, w \in \mathbb{Z}$ tais que $u^2 \equiv -bc \pmod{a}, v^2 \equiv -ac \pmod{b}$ e $w^2 \equiv -ab \pmod{c}$. Assim, módulo a temos que

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \equiv b^{-1}((by)^2 + bcz^2) \equiv b^{-1}((by)^2 - u^2z^2) \\ &\equiv b^{-1}((by - uz)(bu + uz)) \equiv (y - b^{-1}uz)(by + uz) \pmod{a}. \end{aligned}$$

Escrevendo $L_1(x, y, z) = y - b^{-1}uz$ e $M_1(x, y, z) = by + uz$, temos

$$ax^2 + by^2 + cz^2 \equiv L_1(x, y, z)M_1(x, y, z) \pmod{a}.$$

Analisando a equação módulo b, temos

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + cz^2 \equiv a^{-1}((ax)^2 + acz^2) \equiv a^{-1}((ax)^2 - v^2z^2) \\ &\equiv a^{-1}((ax - vz)(ax + vz)) \equiv (x - a^{-1}vz)(ax + vz) \pmod{b}. \end{aligned}$$

Escrevendo $L_2(x,y,z) = x - a^{-1}vz$ e $M_2(x,y,z) = ax + vz$, temos

$$ax^2 + by^2 + cz^2 \equiv L_2(x,y,z)M_2(x,y,z) \pmod{b}.$$

Por fim, módulo c temos

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv ax^2 + by^2 \equiv a^{-1}((ax)^2 + aby^2) \equiv a^{-1}((ax)^2 - w^2y^2) \\ &\equiv a^{-1}((ax - wz)(ax + wz)) \equiv (x - a^{-1}wz)(x + wz) \pmod{c}. \end{aligned}$$

Escrevendo $L_3(x,y,z) = x - a^{-1}wz$ e $M_3(x,y,z) = ax + wz$, temos

$$ax^2 + by^2 + cz^2 \equiv L_3(x,y,z)M_3(x,y,z) \pmod{c}.$$

Agora, procuramos uma forma linear $L(x,y,z) = \alpha x + \beta y + \gamma z$, tal que

$$\begin{cases} L \equiv L_1 \pmod{a} \\ L \equiv L_2 \pmod{b} \\ L \equiv L_3 \pmod{c} \end{cases}$$

Como isto deve ser válido para quaisquer x, y, z, isto se resume a resolver os sistemas

$$\begin{cases} \alpha \equiv 0 \pmod{a} \\ \alpha \equiv 1 \pmod{b} \\ \alpha \equiv 1 \pmod{c} \end{cases} \quad \begin{cases} \beta \equiv 1 \pmod{a} \\ \beta \equiv 0 \pmod{b} \\ \beta \equiv 0 \pmod{c} \end{cases} \quad \begin{cases} \gamma \equiv -b^{-1}u \pmod{a} \\ \gamma \equiv -a^{-1}v \pmod{b} \\ \gamma \equiv -a^{-1}w \pmod{c} \end{cases}$$

como a, b, c são relativamente primos dois a dois, temos pelo teorema chinês dos restos que existem $\alpha_0, \beta_0, \gamma_0$, respectivamente, que é solução dos sistemas acima módulo abc. Esta forma linear satisfaz $L \equiv L_1 \pmod{a}$, $L \equiv L_2 \pmod{b}$ e $L \equiv L_3 \pmod{c}$. De modo análogo podemos obter também, $M(x,y,z) = \alpha' x + \beta' y + \gamma' z$, tal que $M \equiv M_1 \pmod{a}$, $M \equiv M_2 \pmod{b}$ e $M \equiv M_3 \pmod{c}$. Logo

$$ax^2 + by^2 + cz^2 \equiv L(x,y,z)M(x,y,z) \pmod{abc}.$$

Considere agora todas as triplas $(x,y,z) \in \mathbb{Z}^3$, com $0 \leq x \leq \sqrt{|bc|}$, $0 \leq y \leq \sqrt{|ac|}$ e $0 \leq z \leq \sqrt{|ab|}$. Temos

$$\begin{aligned} (\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ac|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) &> \sqrt{|bc|}\sqrt{|ac|}\sqrt{|ab|} \\ &= \sqrt{|a^2b^2c^2|} = |abc| = (-a)(-b)c = abc, \end{aligned}$$

pelo princípio da casa dos pombos existem duas triplas distintas, (x_1, y_1, z_1) e (x_2, y_2, z_2) com

$$L(x_1,y_1,z_1) \equiv L(x_2,y_2,z_2) \pmod{abc} \iff L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0 \pmod{abc}.$$

Fazendo $\tilde{x} = x_1 - x_2$, $\tilde{y} = y_1 - y_2$ e $\tilde{z} = z_1 - z_2$, temos

$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x},\tilde{y},\tilde{z})M(\tilde{x},\tilde{y},\tilde{z}) \equiv 0 \pmod{abc}.$$

Note que $(\tilde{x},\tilde{y},\tilde{z}) \neq (0,0,0)$, além disso a, b, c são primos entre si e livre de quadrados, então $\sqrt{|bc|}$, $\sqrt{|ac|}$ e $\sqrt{|ab|}$ não são inteiros, logo $|\tilde{x}| < \sqrt{|bc|}$, $|\tilde{y}| < \sqrt{|ac|}$ e $|\tilde{z}| < \sqrt{|ab|}$, já que $\tilde{x}, \tilde{y}, \tilde{z}$ são inteiros.

Como $|\tilde{x}| < \sqrt{|bc|}$, temos $|bc| > \tilde{x}^2$, assim como $|ac| > \tilde{y}^2$. Temos que $a < 0, b < 0$, logo $a|bc| < a\tilde{x}^2$ e $b|ac| < b\tilde{y}^2$, assim

$$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 \leq a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < c|ab| = abc.$$

Como $abc \mid a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, devemos ter $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$ (o que resolve o problema) ou $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$, nesse último caso temos

$$\begin{aligned} 0 &= (a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 + abc)(\tilde{z} + ab) \\ &= a(\tilde{x}\tilde{z} + b\tilde{y})^2 + b(\tilde{y}\tilde{z} - a\tilde{x})^2 + c(\tilde{z}^2 + ab)^2, \end{aligned}$$

que fornece a solução $(\tilde{x}\tilde{z} + b\tilde{y}, \tilde{y}\tilde{z} - a\tilde{x}, \tilde{z}^2 + ab)$, com $\tilde{z}^2 + ab \neq 0$ (pois $\tilde{z}^2 + ab \geq ab > 0$).

□

3.1 Resíduos quadráticos

Definição 3.1 *Seja $p > 2$ um primo. Dizemos que um número inteiro a é um resíduo quadrático módulo p, se existe um inteiro x, tal que*

$$x^2 \equiv a \pmod{p}.$$

Gostaríamos de saber quantos resíduos quadráticos módulo p existem, para isso considere os números $1, \ldots, p-1$ e sejam $y_i = i^2, i = 1, \ldots, p-1$. Temos que

$$\begin{aligned} y_i \equiv y_j \pmod{p} &\iff i^2 \equiv j^2 \pmod{p} \iff i^2 - j^2 \equiv 0 \pmod{p} \\ &\iff (i-j)(i+j) \equiv 0 \pmod{p} \iff i \equiv j \pmod{p} \text{ ou } i \equiv -j \pmod{p}. \end{aligned}$$

Como $0 \leq i, j \leq p-1$, então no caso em que $i \equiv j \pmod{p}$ devemos ter $i = j$. No caso $i \equiv -j \pmod{p}$, temos $i + j = p$, pois $0 < i + j < 2p$. Assim,

$$\begin{aligned} 1^2 &\equiv (p-1)^2 \pmod{p}, \\ 2^2 &\equiv (p-2)^2 \pmod{p}, \\ &\vdots \\ \left(\frac{p-1}{2}\right)^2 &\equiv \left(\frac{p+1}{2}\right)^2 \pmod{p}, \end{aligned}$$

logo, há $\frac{p-1}{2}$ resíduos quadráticos distintos módulo p. Temos ainda que 0 é um resíduo quadrático módulo p, então existem $\frac{p+1}{2}$ resíduos quadráticos módulo p e existem $\frac{p-1}{2}$ números que não são resíduos quadráticos módulo p.

Definição 3.2 *Seja p um primo ímpar e a um inteiro qualquer. Definimos o símbolo de Legendre por*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático módulo } p \\ 0, & \text{se } p \mid a \\ -1, & \text{se } p \nmid a \text{ e } a \text{ não é um resíduo quadrático módulo } p \end{cases}$$

Proposição 3.1 *(Critério de Euler) Seja $p > 2$ um primo e a um inteiro, então*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Demonstração: No caso em que $p \mid a$, temos $\left(\frac{a}{p}\right) = 0$ e como $a \equiv 0 \pmod{p}$, então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

No caso em que $p \nmid a$, temos duas situações a considerar $\left(\frac{a}{p}\right) = 1$ e $\left(\frac{a}{p}\right) = -1$. Na primeira situação, temos que existe $y \in \mathbb{Z}$ tal que $y^2 \equiv a \pmod{p}$. Observe que $p \nmid y$, pois p $\mid y^2 - a$ e $p \nmid a$. Assim, $(y, p) = 1$ e pelo pequeno teorema de Fermat temos $y^{p-1} \equiv 1 \pmod{p}$ e portanto

$$a^{\frac{p-1}{2}} \equiv (y^2)^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \pmod{p}.$$

Para o outro caso, considere a função $f(x) = x^{\frac{p-1}{2}} - \overline{1} \in \mathbb{Z}/p\mathbb{Z}[x]$, como $\mathbb{Z}/p\mathbb{Z}$ é corpo, essa função tem no máximo $grau(f) = \frac{p-1}{2}$ raízes, por outro lado, sabemos que existem $\frac{p-1}{2}$ resíduos quadráticos não nulos, os quais satisfazem $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, assim esses resíduos quadráticos são exatamente as raízes de $f(x)$ e portanto se a não for um resíduo quadrático, então $a^{\frac{p-1}{2}}$ não é conguente a 1 módulo p, mas como

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \text{ e } a^{p-1} - 1 \equiv 0 \pmod{p},$$

devemos ter $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, pois $p \nmid a^{\frac{p-1}{2}} - 1$. □

Teorema 3.2 *O símbolo de Legendre é uma função completamente multiplicativa, isto é,*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Demonstração: Pelo critério de Euler temos

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

como o símbolo de Legendre assume somente $-1, 0$ ou 1, a congruência acima implica na igualdade

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Teorema 3.3 *Para p um primo ímpar, temos*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, \text{ se } p \equiv 1 \pmod{4} \\ -1, \text{ se } p \equiv -1 \pmod{4} \end{cases}.$$

Demonstração: Pelo critério de Euler temos

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Se $\frac{p-1}{2}$ for par, então $\left(\frac{-1}{p}\right) \equiv 1 \pmod{p}$ e se $\frac{p-1}{2}$ for ímpar teremos $\left(\frac{-1}{p}\right) \equiv -1 \pmod{p}$. No caso em que $\frac{p-1}{2}$ é par, temos $\frac{p-1}{2} = 2k$, logo $p - 1 = 4k$ e isso implica $p \equiv 1 \pmod{4}$. Se $\frac{p-1}{2}$ é ímpar, então $\frac{p-1}{2} = 2k + 1$, isso implica $p - 3 = 4k$, logo $p \equiv 3 \pmod{4}$. □

Teorema 3.4 *Para p um primo ímpar, temos*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, \text{ se } p \equiv \pm 1 \pmod{8} \\ -1, \text{ se } p \equiv \pm 3 \pmod{8} \end{cases}.$$

Demonstração: No caso em que $p \equiv \pm 1 \pmod 8$, temos $p = 8k \pm 1$, assim $p^2 = 64k^2 \pm 16k + 1$ e portanto $\frac{p^2-1}{8} = 8k^2 \pm 2k$ e isso mostra que $\frac{p^2-1}{8}$ é par. Se $p \equiv \pm 3 \pmod 8$, temos $p = 8k \pm 3$, logo $p^2 = 64k^2 \pm 48k + 9$, assim $\frac{p^2-1}{8} = 8k^2 \pm 6k + 1$ e portanto $\frac{p^2-1}{8}$ é ímpar.

Vejamos que $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Temos que para i ímpar, $p - i \equiv i(-1)^i \pmod p$ e para i par, temos $i \equiv i(-1)^i \pmod p$. Considere as congruências

$$p - 1 \equiv 1(-1)^1 \pmod p$$

$$2 \equiv 2(-1)^2 \pmod p$$

$$p - 3 \equiv 3(-1)^3 \pmod p$$

$$4 \equiv 4(-1)^4 \pmod p$$

$$\vdots$$

$$t \equiv \frac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod p,$$

onde $t = \frac{p-1}{2}$ se $\frac{p-1}{2}$ é par, caso contrário $t = p - \frac{p-1}{2}$. Multiplicando membro a membro as congruências acima obtemos

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{1+2+\ldots+\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p. \tag{3.1}$$

Temos que

$$2 \cdot 4 \cdot 6 \cdots (p-1) = (2 \cdot 1)(2 \cdot 2) \cdots \left(2 \cdot \frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

e também temos que a soma dos termos da progressão aritmética $1 + 2 + \ldots + \frac{p-1}{2}$ é

$$S_n = \frac{\left(1 + \frac{p-1}{2}\right)\frac{p-1}{2}}{2} = \frac{p^2-1}{8}.$$

Assim, substituindo em (3.1) obtemos

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^{\frac{p^2-1}{8}} \left(\frac{p-1}{2}\right)! \pmod p.$$

Como $\left(\left(\frac{p-1}{2}\right)!, p\right) = 1$, então

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p,$$

logo

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

Isto é, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. □

Observação 3.1 *Observe que* $2(-1) = -2$*, logo se dois deles são resíduos quadráticos módulo um primo ímpar, então o terceiro também é um resíduo quadrático módulo esse primo.*

Proposição 3.2 *Seja* p *um primo ímpar. Se* 2 *e* -2 *(ou* -1 *e* 2*) são resíduos quadráticos módulo* p*, então* $p \equiv 1 \pmod 8$.

Demonstração: Como 2 é um resíduo quadrático e $p \nmid 2$, então $\left(\frac{2}{p}\right) = 1$ e nesse caso temos $p \equiv \pm 1 \pmod 8$. Também temos que -2 é um resíduo quadrático, logo $\left(\frac{-2}{p}\right) = 1$ e como

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) \cdot \left(\frac{-1}{p}\right),$$

devemos ter $\left(\frac{-1}{p}\right) = 1$ e nesse caso $p \equiv 1 \pmod 4$. Observe que $p \equiv -1 \pmod 8$, implica $p \equiv -1 \pmod 4$ e logo $p \equiv 3 \pmod 4$. Assim, p só pode ser congruente a 1 módulo 8. $\square$

Capítulo 4

Conjectura de Euler

4.1 Um pouco de história

O último teorema de Fermat diz que a equação

$$x^n + y^n = z^n,\ n \geq 3$$

não possui soluções inteiras. O caso $n = 3$ foi demonstrado por Euler, o que o motivou a conjecturar no ano de 1769 que a equação

$$A_1^n + \cdots + A_{n-1}^n = A_n^n \quad (n \geq 4),$$

não possui soluções inteiras não triviais.

Em 1966 os matemáticos L. J. Lander e T. R. Parkin encontraram um contra-exemplo para o caso $n = 5$,

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Foram feitas tentativas de buscar computacionalmente as soluções inteiras para

$$A^4 + B^4 + C^4 = D^4,$$

porém não houve sucesso. Em 1988, usando técnicas de Geometria Algébrica e auxílio computacional, o matemático Noam D. Elkies (ver [2]) encontrou a primeira solução

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Posteriormente, Roger Frye (ver [4]) encontrou um menor contra-exemplo para o caso $n = 4$ da conjectura de Euler

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

Elkies exibiu vários contra-exemplos, dando uma construção recursiva de infinitas soluções para

$$A^4 + B^4 + C^4 = D^4$$

em números naturais, A, B, C e D primos entre si. Ele usou o fato de que buscar uma solução inteira para $A^4 + B^4 + C^4 = D^4$, é equivalente a encontrar um ponto racional

$$(r, s, t) = \left(\pm\frac{A}{D}, \pm\frac{B}{D}, \pm\frac{C}{D}\right).$$

sobre a superfície $r^4 + s^4 + t^4 = 1$.

4.2 O caso $n = 4$ da conjectura de Euler

4.2.1 A superfície $\mathcal{S}_2 : r^4 + s^4 + t^2 = 1$

Seja $\mathcal{S}_2$ a superfície definida por f, onde $f = r^4 + s^4 + t^2 - 1$. Observe que, se encontrarmos um ponto racional (r, s, t), nesta superfície e se t for um quadrado, então encontramos um ponto racional da superfície $r^4 + s^4 + t^4 = 1$ e isto é equivalente a obter uma solução inteira de

$$A^4 + B^4 + C^4 = D^4.$$

A superfície $\mathcal{S}_2$ pode ser parametrizada por um feixe de cônicas $\mathcal{X}$, definida por

$$g = (u^2 + 2)y^2 + (3u^2 - 8u + 6)x^2 + 2(u^2 - 2)x + 2u. \tag{4.1}$$

Observe que para cada valor de u fixo, obtemos uma cônica nas variáveis (x, y). Por isso é que $\mathcal{X}$ é chamado de feixe de cônicas.

Definimos a parametrização $\psi : \mathcal{X} \longrightarrow \mathcal{S}_2$ da seguinte forma: dado $(x, y, u) \in \mathcal{X}$, escrevemos $\psi(x, y, u) = (r, s, t)$, onde

$$r = x + y \ , s = x - y \tag{4.2}$$

$$(u^2 + 2)t = 4(u^2 - 2)x^2 + 8ux + 2 - u^2 \tag{4.3}$$

Lema 4.1 *A aplicação*

$$\begin{array}{rcl} \psi : X & \longrightarrow & \mathcal{S}_2 \\ (x, y, u) & \longmapsto & \left(x + y, x - y, \dfrac{4(u^2 - 2)x^2 + 8ux + 2 - u^2}{u^2 + 2} \right) \end{array}$$

é uma aplicação racional definida em $\mathcal{X}$, exceto para $u^2 + 2 = 0$.

Demonstração: A aplicação ψ está bem definida para $u^2 + 2 \neq 0$. Resta provar que se $(x, y, u) \in X$, então $\psi(x, y, u) \in \mathcal{S}_2$.

Usando o maple [7], calculamos $f(r, s, t) = f(\psi(x, y, u))$ e obtemos

$$f(r, s, t) = \frac{2(y^2u^2 + 2y^2 - 2u + 4x - 2xu^2 + 6x^2 + 8x^2u + 3x^2u^2) \cdot g(x, y, u)}{(u^2 + 2)^2}.$$

Como $g(x, y, u) = 0$, então $f(r, s, t) = 0$. □

Queremos definir $\phi = \psi^{-1}$, ou seja,

$$\phi(r, s, t) = (x, y, u).$$

De (4.1), obtemos uma equação do segundo grau em u:

$$(y^2 + 3x^2 + 2x)u + (-8x^2 + 2)u + 6x^2 - 4x + 2y^2 = 0,$$

cujo discriminante é $4(1 - (2x^4 + 12x^2y^2 + 2y^4))$. Assim,

$$\begin{array}{rcl} u & = & \dfrac{-2 + 8x^2 \pm 2\sqrt{1 - (2x^4 + 12x^2y^2 + 2y^4)}}{2(y^2 + 3x^2 + 2x} \\ & = & \dfrac{-1 + 4x^2 \pm \sqrt{1 - (2x^4 + 12x^2y^2 + 2y^4)}}{3x^2 + y^2 + 2x} \end{array} \tag{4.4}$$

Para ϕ ser a inversa de ψ, devemos ter $r = x + y$ e $s = x - y$. Assim,

$$r + s = 2x \Longrightarrow x = \frac{r+s}{2},$$

$$r - s = 2y \Longrightarrow y = \frac{r-s}{2}.$$

Queremos escrever u em função de r, s, t, logo devemos substituir x e y em (4.4). Temos

$$2x^4 = 2\left(\frac{r+s}{2}\right)^4 = \frac{1}{8}(r^4 + 4r^3s + 6r^2s^2 + 4rs^3 + s^4),$$

$$12x^2y^2 = 12\left(\frac{r+s}{2}\right)^2\left(\frac{r-s}{2}\right)^2 = \frac{3}{4}(r^4 - 2r^2s^2 + s^4),$$

$$2y^4 = \left(\frac{r-s}{2}\right)^4 = \frac{1}{8}(r^4 - 4r^3s + 6r^2s^2 - 4rs^3 + s^4),$$

$$2x^4 + 12x^2y^2 + 2y^4 = r^4 + s^4,$$

$$y^2 = \left(\frac{r-s}{2}\right)^2 = \frac{r^2 - 2rs + s^2}{4},$$

$$3x^2 = \frac{3r^2 + 6rs + 3s^2}{4},$$

$$3x^2 + y^2 + 2x = r^2 + s^2 + rs + r + s.$$

Substituindo os valores encontrados em (4.4), temos

$$\begin{aligned} u &= \frac{-1 + (r+s)^2 \pm \sqrt{1 - (r^4 + s^4)}}{r^2 + s^2 + rs + r + s} \\ &= \frac{-1 + (r+s)^2 \pm t}{r^2 + s^2 + rs + r + s} \end{aligned}$$

Escolhendo o sinal positivo para t , definimos

$$\begin{aligned} \phi : \mathcal{S}_2 &\longrightarrow \mathcal{X} \\ (r,s,t) &\longmapsto \left(\frac{r+s}{2}, \frac{r-s}{2}, \frac{-1 + (r+s)^2 + t}{r^2 + s^2 + rs + r + s}\right). \end{aligned}$$

Lema 4.2 *A aplicação $\psi : \mathcal{X} \longrightarrow \mathcal{S}_2$, é uma aplicação birracional, cuja aplicação racional inversa é $\phi : \mathcal{S}_2 \longrightarrow \mathcal{X}$. Esta aplicação esta definida em todo $\mathcal{S}_2$, exceto nos pontos que satisfazem*

$$r^2 + s^2 + rs + r + s = 0.$$

Demonstração:

- Primeiro, vejamos que $\phi(\mathcal{S}_2) \subseteq \mathcal{X}$. Com o auxílio do maple calculamos $g(\phi(r,s,t)$, obtemos

$$g(x,y,u) = \frac{f(r,s,t)}{r^2 + s^2 + rs + r + s}.$$

  Como $f = 0$, então $g = 0$.

- Vejamos que ϕ é a inversa de ψ. Devemos mostrar que

$$\begin{aligned} \phi \circ \psi_{|_{\mathcal{X}'}} &= id_{\mathcal{X}'} \\ \psi \circ \phi_{|_{\S'}} &= id'_{\mathcal{S}_2}. \end{aligned}$$

Temos

$$\begin{aligned} (\psi \circ \phi)(r,s,t) &= \psi\left(\frac{r+s}{2}, \frac{r-s}{2}, \frac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}\right) \\ &= (r',s',t'), \end{aligned}$$

onde

$$r' = \frac{r+s}{2} + \frac{r-s}{2} = r,$$

$$s' = \frac{r+s}{2} - \frac{r+s}{2} = s,$$

$$t' = \frac{4\left(\left(\frac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}\right)^2 - 2\right) + 8\left(\frac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}\right)x + 2 - \left(\frac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}\right)^2}{\left(\frac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}\right)^2 + 2}.$$

Usando o maple, obtemos $t' = \dfrac{a}{b}$, onde

$$a = -1 + 8trs^2 + 8tr^2s + 8r^3ts + 4ts^3 - 2r^5s - r^4s^2 + 2t^2s + 2s^4t + 8s^3tr + 12s^2tr^2$$

$$+r^4 - s^4r^2 - 2s^5r - r^6 + 4tr^3 - s^6 + 2rs + s^2 + 2r^4t + s^4 + r^2 + 2t + t^2s^2 + t^2r^2 - t^2$$

$$b = 1 - 2t + 3r^4 + 3s^4 + t^2 + 8s^2r + 2s^2t + 8r^3s + 12r^2s^2 + 2tr^2 + 8rs^3 + 4rst + 4r^3 + 4s^3 + 8r^2s.$$

Temos que

$$\begin{aligned} a - tb &= -(t + r^2 - 1 + 2rs + s^2)(r^4 + s^4 + t^2 - 1) \\ &\Longrightarrow \quad t' - t = \frac{a - tb}{b} = \frac{-(t + r^2 - 1 + 2rs + s^2) \cdot f}{b}. \end{aligned}$$

Como $f = 0$, então $t' = t$.

Vejamos agora que $\phi \circ \psi = Id_{\mathcal{X}}$.

$$\begin{aligned} (\phi \circ \psi)(x,y,u) &= \phi\left(x+y, x-y, \frac{4(u^2-2)+8ux+2-u^2}{u^2+2}\right) \\ &= \left(\frac{x+y+x-y}{2}, \frac{x+y-x+y}{2}, u'\right) \\ &= (x,y,u') \end{aligned}$$

Temos que $u' = \dfrac{-1+(r+s)^2+t}{r^2+s^2+rs+r+s}$. Substituindo r, s e t, obtemos $u' = \dfrac{a}{b}$, onde

$$a = 2u(-u + 4x^2u + 4x), \quad b = (u^2+2)(3x^2+y^2+2x),$$

assim

$$a - ub = -u(y^2u^2 + 2y^2 + 2u - 4x + 2xu^2 + 3x^2u^2 - 8x^2u + 6x^2) = -ug.$$

Como $g = 0$, então $u' - u = 0$, logo $u' = u$.

□

Queremos reescrever (4.3) com coeficientes inteiros. Desejamos fazer o mesmo para $g = 0$, onde g está definida em (4.1). Para isso considere a involução abaixo:

Lema 4.3 *A aplicação*

$$\begin{array}{rcl} \sigma : \mathcal{X} & \longrightarrow & \mathcal{X} \\ (x, y, u) & \longmapsto & \left(-x, y, -\dfrac{2}{u}\right) \end{array}$$

é uma involução de $\mathcal{X}$, isto é, $\sigma^2 = Id_{\mathcal{X}}$. Em $\mathcal{S}_2$, a involução correspondente é

$$\begin{array}{rcl} \tau : \mathcal{S}_2 & \longrightarrow & \mathcal{S}_2 \\ (r, s, t) & \longmapsto & (-s, -r, -t), \end{array} \tag{4.5}$$

pois $\tau \circ \psi = \psi \circ \sigma$.

Demonstração: Vejamos que σ é de fato uma involução.

$$(\sigma \circ \sigma)(x, y, u) = \sigma\left(-x, y, -\frac{2}{u}\right) = \left(-(-x), y, \frac{-2}{-\frac{2}{u}}\right) = (x, y, u).$$

Isto é, $\sigma^2 = Id$.
Seja $(x, y, u) \in \mathcal{X}$ e $\psi(x, y, u) = (r, s, t)$.
Vejamos que $\psi(\sigma(x, y, u)) = (-s, -r, -t) = \tau(r, s, t) = \tau(\psi(x, y, u))$. Temos

$$\begin{array}{rcl} \psi(\sigma(x, y, u) & = & \psi(-x, y, -2/u) \\ & = & (-x + y, -x - y, t') \\ & = & (-s, -r, t'), \end{array}$$

onde

$$t' = \frac{(4(\frac{4}{u^2} - 2))x^2 - \frac{16x}{u} + 2 - \frac{4}{u^2}}{\frac{4}{u^2} + 2}.$$

Com auxílio computacional obtemos $t + t' = 0$, logo $t' = -t$ e portanto

$$\psi(\sigma(x, y, u)) = \tau(\sigma(x, y, u)).$$

□

Seja $(x, y, u) \in \mathcal{X}$ uma solução racional de $\mathcal{X}$, então existem $p, q \in \mathbb{Z}, p, q \neq 0$, $mdc(p, q) = 1$, tais que $u = \frac{p}{q}$. Se $2 \nmid p$, então pelo lema 4.3, temos $\sigma(x, y, u) = (-x, y, u) = \left(-x, y, -\frac{2q}{p}\right)$ é também um ponto racional do feixe de cônicas $\mathcal{X}$. Observe que $\dfrac{-2q}{p}$ tem numerador múltiplo de 2. Assim, se $\mathcal{X}$ possui soluções racionais, existirá uma solução racional (x, y, u), tal que $u = \dfrac{2m}{n}$,

com $m, n \in \mathbb{Z}$ não nulos e $mdc(n, 2m) = 1$. Em particular, n será ímpar. Substituindo u em $g = 0$ temos

$$\left(\frac{4m^2}{n^2} + 2\right) y^2 = \left(-3 \cdot \frac{4m^2}{n^2} - \frac{16m}{n} + 6\right) x^2 - 2\left(\frac{4m^2}{n^2} - 2\right) x - 2mn$$

e multiplicando por $\frac{n^2}{2}$, obtemos

$$(2m^2 + n^2)y^2 = (-6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2)x - 2mn \tag{4.6}$$

Substituindo agora, u em (4.3), obtemos

$$(2m^2 + n^2)t = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2).$$

Definição 4.1 *Dado um número inteiro $k \neq 0$ definimos*

(*i*) *$S(k)$ como o maior inteiro cujo quadrado divide k;*

(*ii*) $R(k) = \dfrac{k}{S(k)^2}$.

Exemplo 4.1 *Sejam $k_1 = 24$ e $k_2 = -36$, temos $k_1 = 2^3 \cdot 3 = 2^2 \cdot 2 \cdot 3$, logo $S(k_1) = 2$ e $R(k_1) = 6$. Para k_2, temos $k_2 = -6^2$, logo $S(k_2) = 6$ e $R(k_2) = -1$.*

Note que dado um número k que apresenta fatoração $k = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p^{\alpha_k}$. Então, $R(k) = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p^{\beta_k}$, onde

$$\beta_i = \begin{cases} 0 \text{ , se } 2 \mid \alpha_i \\ 1 \text{ , se } 2 \nmid \alpha_i \end{cases}$$

Antes de passar ao resultado que nos dá condições para que a cônica (4.6) tenha infinitos pontos racionais, precisamos do lema a seguir.

Lema 4.4 *Sejam m, n inteiros, com n ímpar e $(m, n) = 1$. Então, $m, n, 2m^2 + n^2$, $2m^2 - 2mn + n^2$ e $2m^2 - 4mn + n^2$ são relativamente primos dois a dois.*

Demonstração: Sabemos que $(a, b) = 1 = (a, c) \iff (a, bc) = 1$ e $(a, b) = (a, b - ka)$, onde (a, b) denota o máximo divisor comum entre a e b.

Vejamos que o *mdc* entre números acima é 1.

(*a*) $(n, 2m^2 + n^2) = (n, 2m^2 + n^2 - n \cdot n) = (n, 2m^2) = 1$, pois $(2, n) = 1$ e $(m, n) = 1$.

(*b*) $(n, 2m^2 - 2mn + n^2) = (n, 2m^2 - 2mn + n^2 - (-2m + n)n) = (n, 2m^2) = 1$.

(*c*) $(n, 2m^2 - 4mn + n^2) = (n, 2m^2 - 4mn + n^2 - (-4m + n)n) = (n, 2m^2) = 1$.

(*d*) $(m, 2m^2 + n^2) = (m, 2m^2 + n^2 - (2m)m) = (m, n^2) = 1$.

(*e*) $(m, 2m^2 - 2mn + n^2) = (m, 2m^2 - 2mn + n^2 - (2m - 2n)m) = (m, n^2) = 1$.

(*f*) $(m, 2m^2 - 4mn + n^2) = (m, 2m^2 - 4mn + n^2 - (-2m + 4n)m) = (m, n^2)$.

(*g*) $(2m^2 + n^2, 2m^2 - 2mn + n^2) = (2m^2 + n^2, -2mn) = 1$, pois $(2m^2 + n^2, 2) = 1$, $(2m^2 + n^2, m) = 1$ e $(2m^2 + n^2, n) = 1$.

(*h*) $(2m^2 + n^2, 2m^2 - 4mn + n^2) = (2m^2 + n^2, -4mn) = 1$.

(i) $(2m^2 - 2mn + n^2, 2m^2 - 4mn + n^2) = (2m^2 - 2mn + n^2, -2mn) = (2m^2 + n^2, 2mn) = 1.$

□

Lema 4.5 *Sejam m, n inteiros, com n ímpar e $(m, n) = 1$. Os números $2m^2 + 2mn + n^2$, $2m^2 - 2mn + n^2, 2m^2 + n^2$ e $2m^2 - n^2$ são relativamente primos dois a dois.*

Demonstração: Pelo item (g) do lema 4.4, temos que $(2m^2 + n^2, 2m^2 - 2mn + n^2) = 1$. Vejamos que $(2m^2 + n^2, 2m^2 + 2mn + n^2) = 1$. De fato,

$$(2m^2 + n^2, 2m^2 + 2mn + n^2) = (2m^2 + n^2, 2mn) = 1,$$

pois $(2m^2 + n^2, 2) = 1$, $(2m^2 + n^2, m) = 1$ e $(2m^2 + n^2, n) = 1$.

Também temos

$$\begin{aligned}(2m^2 - n^2, 2m^2 + 2mn + n^2) &= (2m^2 - n^2, 2mn + 2n^2) = (2m^2 - n^2, 2n(n + m)) \\ &= (2m^2 - n^2, n + m) = (2m^2 - n^2 - 2m(n + m), n + m) \\ &= (-n(n + 2m), n + m) = (n + 2m, n + m) = (-m, n + m) = 1\end{aligned}$$

Por fim, temos

$$\begin{aligned}(2m^2 - n^2, 2m^2 - 2mn + n^2) &= (2m^2 - n^2, 2n^2 - 2mn) \\ &= (2m^2 - n^2, 2n(n - m)) = (2m^2 - n^2, n - m) = 1\end{aligned}$$

□

Observação 4.1 *Sejam a, b inteiros com $(a, b) = 1$ e considere também suas fatorações em produto de primos distintos, isto é,*

$$a = p_1^{\alpha_1} \dots p_k^{\alpha_k} \ , \ b = q_1^{\beta_1} \dots q_l^{\beta_1}.$$

Temos que $R(a) = p_1^{\gamma_1} \dots p_k^{\gamma_k}$, onde $\gamma_i = 0$, se $2 \mid \alpha_i$ e $\gamma_i = 1$, se $2 \nmid \alpha_i$. E temos $R(b) = q_1^{\theta_1} \dots q_l^{\theta_l}$, onde $\theta_j = 0$, se $2 \mid \beta_j$ e $\theta_j = 1$, se $2 \nmid \beta_j$.

Como $a \cdot b = p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_1}$, então

$$R(ab) = p_1^{\gamma_1} \dots p_k^{\gamma_k} q_1^{\theta_1} \dots q_l^{\theta_l} = R(a)R(b).$$

Observe que se p é primo, temos $p = R(p)$. Assim,

$$R(a) = R(p_1^{\alpha_1}) \dots R(p_k^{\alpha_k}),$$

onde

$$R(p_j^{\alpha_j}) = \begin{cases} p_j \ , \ se \ 2 \nmid \alpha_j \\ 1 \ , \ se \ 2 \mid \alpha_j \end{cases} .$$

Lema 4.6 *A cônica (4.6) tem infinitos pontos racionais (x, y), se e somente se,*

$$R(2m^2 + n^2) \ , \ R(2m^2 - 4mn + n^2)$$

são ambos produtos de primos congruentes a 1 módulo 8.

Demonstração: Vamos colocar (4.13) na forma

$$aX^2 + bY^2 + cZ^2 = 0,$$

onde a, b, c são inteiros livres de quadrados, não todos do mesmo sinal e relativamente primos dois a dois. Para isso, tome $X = 2mn + (2m^2 + n^2)x$, então

$$\begin{aligned} X^2 &= (2mn^2) + 4mn(2m^2 - n^2)x + (2m^2 - n^2)^2x^2 \\ &= 2mn(2mn + 2(2m^2 - n\ 2)x) + (2m^2 - n^2)x^2 \end{aligned} \tag{4.7}$$

De (4.13) temos que $2(2m^2 - n^2)x = -(6m^2 - 8mn + 3n^2)x^2 - 2mn - (2m^2 + n^2)y^2$, assim substituindo em (4.7) temos

$$\begin{aligned} X^2 &= 2mn(2mn - (6m^2 - 8mn + 3n^2)x^2 - 2mn - (2m^2 + n^2)y^2) + (2m^2 - n^2)^2x^2 \\ &= -2mn(2m^2 + n^2)y^2 + (-2mn(6m^2 - 8mn + 3n^2) + (2m^2 - n^2)^2x^2 \\ &= -2mn(2m^2 + n^2)y^2 + (4m^4 + n^4 - 12m^3n - 6mn^3 + 12m^2n^2)x^2 \\ &= -2mn(2m^2 + n^2)y^2 + (2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)x^2. \end{aligned}$$

Vamos tomar $X^2 = -a\alpha^2y^2 + b\beta^2x^2$, onde $a = R(2mn(2m^2 + n^2))$, $\alpha = S(2mn(2m^2 + n^2))$, $b = R((2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2))$ e $\beta = S((2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2))$. Chamando $Y = \alpha y$ e $Z = \beta x$, temos

$$X^2 + aY^2 - bZ^2 = 0, \tag{4.8}$$

nas condições desejadas. Já vimos que para n ímpar (ver proposição 4.4) temos que $m, n, 2m^2 + n^2, 2m^2 - 2mn + n^2$ e $2m^2 - 4mn + n\ 2$ são relativamente primos dois a dois. Pelo teorema 3.1, temos que a equação (4.8) possui solução inteira não trivial se, e somente se, $-a$ é um quadrado módulo b e b é um quadrado módulo a. Assim,

$$-a \equiv c^2 \pmod{b}, \quad b \equiv d^2 \pmod{a}.$$

Como $(2mn(2m^2+n^2), (2m^2-2mn+n^2)(2m^2-4mn+n^2)) = 1$, então $(\alpha^2, b) = 1$ e $(\beta^2, a) = 1$. Assim,

$$-2mn(2m^2 + n^2) \equiv (\alpha c)^2 \pmod{b} \text{ e}$$

$$(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2) \equiv (\beta d)^2 \pmod{a}.$$

Como $b = R((2m^2-2mn+n^2)(2m^2-4mn+n^2))$ e $(2m^2-2mn+n^2, 2m^2-4mn+n^2) = 1$, então pela observação (4.1), temos que

$$b = R(2m^2 - 2mn + n^2)R(2m^2 - 4mn + n^2).$$

É claro que todo primo na fatoração de $R(2mn(2m^2 + n^2))$ e $R(2m^2 - 4mn + n^2)$ divide $-R(2mn(2m^2 + n^2)) - (\alpha c)^2$ (pois $b \mid -2mn(2m^2 + n^2)) - (\alpha c)^2$). Isto é, $-2mn(2m^2 + n^2)$ é um quadrado módulo cada primo que divide $R(2mn(2m^2 + n^2))$ e $R(2m^2 - 4mn + n^2)$.

Também temos

$$a = R(2mn(2m^2 + n^2)) = R(2m)R(n)R(2m^2 + n^2).$$

Observe que todo número ímpar é um quadrado módulo 2, por isso pede-se que o número $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ seja um quadrado módulo cada primo que divide $R(m)$, pois se isso acontecer, esse número será um quadrado módulo cada primo que divide $R(2m)$. Devemos pedir agora que $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ seja um quadrado módulo cada primo na fatoração de $R(m), R(n)$ e $R(2m^2 + n^2)$.

Três dessas condições sempre ocorrem:

(*i*) $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ é congruente módulo m ao quadrado n^4, isto é, $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2) \equiv n^4 \pmod{n}$.

(*ii*) $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ é congruente módulo n ao quadrado $4m^4$, ou seja, $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2) \equiv 4m^4 \pmod{n}$.

(*iii*) $-2mn(2m^2 + n^2) \equiv (2m^2 - n^2)^2 \pmod{2m^2 - 2mn + n^2}$. De fato,

$$\begin{aligned} -2mn(2m^2 + n^2) - (2m^2 - n^2)^2 &= -4m^4 + 4m^2n^2 - n^4 - 2mn(2m^2 + n^2) \\ &= (2m^2 - 2mn + n^2)(-2m^2 - 4mn - n^2). \end{aligned}$$

A próxima condição diz que

(*iv*) $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2)$ deve ser um quadrado módulo cada fator primo de $R(2m^2 + n^2)$. Como

$$(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2) \equiv 2(2mn)^2 \pmod{2m^2 + n^2},$$

(pois $(2m^2 - 2mn + n^2)(2m^2 - 4mn + n^2) - 2(2mn)^2 = (2m^2 + n^2)(n^2 - 6mn + 2m^2)$), então esse número deve ter 2 como resíduo quadrático. Também temos -2 como resíduo quadrático, pois $n^2 \equiv -2m^2 \pmod{2m^2 + n^2}$ e $(m^2, 2m^2 + n^2) = 1$.

(*v*) Como $-2mn(2m^2 + n^2) \equiv -2(2mn)^2 \pmod{2m^2 - 4mn + n^2}$ (pois $-2mn(2m^2 + n^2) + 2(2mn)^2 = -2mn(2m^2 - 4mn + n^2)$, então -2 é um resíduo quadrático módulo cada fator primo de $2m^2 - 4mn + n^2$.

Para ver que 2 também é um quadrado módulo cada fator primo de $2m^2 - 4mn + n^2$, observe que $2m^2 - 4mn + n^2 = 2(m - n)^2 - n^2$ e portanto,

$$2(m - n)^2 \equiv n^2 \pmod{2m^2 - 4mn + n^2}.$$

Como os resíduos quadráticos de cada um desses primos são -2 e 2 , então pela proposição 3.2, todos esses primos devem ser congruentes a 1 módulo 8. □

Exemplo 4.2 *Seja $(m, n) = (2, 1)$, o que implica $u = 4$. Temos $S(2m^2 + n^2) = S(9) = 3$, logo $R(2m^2 + n^2) = \frac{9}{3^2} = 1$. Além disso, $S(2m^2 - 4mn + n^2) = S(1) = 1$ e $R(2m^2 - 4mn + n^2) = 1$. Assim , estão verificadas as condições do lema 4.6.*

Substituindo $(m, n) = (2, 1)$ em (4.6), obtemos a cônica

$$9y^2 = -11x^2 - 14x - 4. \tag{4.9}$$

Observe que o ponto $(x, y) = \left(-\frac{1}{2}, \frac{1}{6}\right)$ é solução da equação acima. Assim, $(x, y, u) = \left(-\frac{1}{2}, \frac{1}{6}, 4\right)$, obtemos $(r, s, t) = \left(\frac{1}{3}, \frac{2}{3}, \frac{8}{9}\right)$.

Vamos obter uma parametrização a partir do ponto $(x, y) = \left(-\frac{1}{2}, \frac{1}{6}\right)$, considerando a reta de inclinação $\frac{k}{3}$, que passa por esse ponto. A equação dessa reta é $y = \frac{k}{3}x + \frac{k+1}{6}$. Assim, substituindo em (4.9) temos

$$(k^2 + 11)x^2 + (k^2 + k + 14)x + \frac{1}{4}k^2 + \frac{1}{2}k + \frac{17}{4} = 0.$$

Daí obtemos a parametrização

$$(x, y) = \left(-\frac{k^2 + 2k + 17}{2k^2 + 22}, -\frac{k^2 + 6k - 11}{6k^2 + 66}\right).$$

Com isso uma solução para $r^4 + s^4 + t^2 = 1$ é

$$(r, s, t) = \left(\frac{2k^2 + 6k + 20}{3k^2 + 33}, \frac{k^2 + 31}{3k^2 + 33}, \frac{4(2k^4 - 3k^2 + 28k^2 - 75k + 80)}{(3k^2 + 33)^2}\right).$$

Em geral, quando u satisfaz a hipótese do lema 4.6 encontramos r e s de grau 2 e t de grau 4 com quadrado no denominador.

4.2.2 A superfície $\mathcal{S}_4 : r^4 + s^4 + t^4 = 1$

Para encontrar uma solução racional (r, s, t) de

$$r^4 + s^4 + t^4 = 1 \tag{4.10}$$

devemos resolver $r^4 + s^4 + t^2 = 1$ com a restrição adicional de que $\pm t$ seja um quadrado. Pelo realizado anteriormente, temos que

$$r = x + y \ , s = x - y; \tag{4.11}$$

$$(2m^2 + n^2)y^2 = -(6m^2 - 8mn + 3n^2)x^2 - 2(2m^2 - n^2x - 2mn); \tag{4.12}$$

$$\pm(2m^2 + n^2)t^2 = 4(2m^2 - n^2)x^2 + 8mnx + (n^2 - 2m^2); \tag{4.13}$$

onde m, n são inteiros relativamente primos e n é ímpar.

Exemplo 4.3 *Façamos por exemplo,* $(m, n) = (0, 1)$. *Obtemos*

$$y^2 = -3x^2 + 2x, \tag{4.14}$$

$$\pm t^2 = -4x^2 + 1 \tag{4.15}$$

O ponto $(0, 0)$ *é um ponto da primeira cônica. A reta que passa por* $(0, 0)$ *e cujo coeficiente angular é* k*, fornece a seguinte parametrização para* (4.14)*:*

$$(x, y) = \left(\frac{2}{k^2 + 3}, \frac{2k}{k^2 + 3}\right).$$

Substituindo o valor acima em (4.15) *temos*

$$\pm t^2 = -4\left(\frac{2}{k^2 + 3}\right)^2 + 1 \Longrightarrow \pm t^2 = \frac{-16}{k^4 + 6k^2 + 9}$$

Com a nova variável $z = (k^2 + 3)t$*, temos*

$$\pm z^2 = k^4 + 6k^2 - 7.$$

Essas são duas curvas de gênero um com o ponto racional $(k, z) = (1, 0)$. *São portanto curvas elípticas. Para obter a forma de Weierstrass associada, realizamos a mudança de coordenadas*

$$k = \pm 1 - \frac{4}{1 \mp X},$$
$$z = \frac{8Y}{(1 \mp X)^2}.$$

Para $z^2 = k^4 + 6k^2 - 7$*, substitua* $k = 1 - \dfrac{4}{1 - X}$ *e* $z = \dfrac{8Y}{(1 - X)^2}$*. Assim, encontramos*

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

Para $-z^2 = k^4 + 6k^2$*, substitua* $k = 1 - \dfrac{4}{1 + X}$ *e* $z = \dfrac{8Y}{(1 + X)^2}$*. Logo,*

$$Y^2 = X^3 + X - 2.$$

A curva $Y^2 = X^3 + X - 2$ tem os pontos racionais: $(1, 0)$, ponto de 2-torção e o ponto no infinito. Já a curva $Y^2 = X^3 + X + 2$ possui os pontos racionais: $(-1, 0)$, ponto de 2-torção, (1,± 2), pontos de 4-torção e o ponto no infinito. Para ver que esses são os únicos pontos de torção da curva $Y^2 = X^3 + X + 2$, consulte o exemplo 2.3.

Tomando por exemplo, $Y^2 = X^3 + X + 2$ e o ponto $(1, 2)$, temos $k = -1$ e portanto $(x, y) = \left(\frac{1}{2}, -\frac{1}{2}\right)$. Substituindo o valores de x e y na parametrização de $\mathcal{S}_2$, temos $r = 0$, $s = 1$ e $t = \pm 1$. Na verdade para qualquer uma das curvas elípticas acima e seus pontos racionais obtemos os valores $0, +-1$ para as variáveis r, s, t. Portanto, essa não foi uma boa escolha de m e n; uma boa escolha de m e n deve fornecer uma curva de gênero um com um ponto racional e que gere soluções não triviais para $\mathcal{S}_2$. Para diminuir nossas escolhas de m e n, usamos o lema 4.6 e o lema a seguir.

Lema 4.7 *A cônica (4.13) possui infinitos pontos racionais (x, t) se, e somente se,*

$$R(2m^2 - 2mn + n^2),\ R(2m^2 + n^2) \quad e \quad R(2m^2 + 2mn + n^2)$$

são todos produtos de primos congruentes a 1 módulo 8.

Demonstração: Seja $X = 4mnx + (n^2 - 2m^2)$. Temos

$$\begin{aligned} X^2 &= (4mnx)^2 + 8mnx(n^2 - 2m^2) + (n^2 - 2m^2)^2 \\ &= (n^2 - 2m^2)(8mnx + n^2 - 2m^2) + (4mn)^2x^2 \end{aligned}$$

Somando e subtraindo $4(2m^2 - n^2)x^2(n^2 - 2m^2)$, temos

$$\begin{aligned} X^2 &= (n^2 - 2m^2)(8mnx + n^2 - 2m^2 + 4(2m^2 - n^2)x^2) - 8m^2n^2x^2 + 16m^4x^2 \\ &+ 4n^4x^2 - 8n^2m^2x^2 + 16m^2n^2x^2 \\ &= (n^2 - 2m^2)(8mnx + n^2 - 2m^2 + 4(2m^2 - n^2)x^2) + 4(4m^4 + n^4)x^2 \\ &= \mp(2m^2 - n^2)(2m^2 - n^2)t^2 + 4(2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2) \end{aligned}$$

Assim, $X^2 = \mp a\alpha^2t^2 + 4b\beta^2x^2$, onde

$$a = R(2m^2 - n^2)(2m^2 + n^2)), \quad \alpha = S(2m^2 - n^2)(2m^2 + n^2)),$$

$$b = R((2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2)) \text{ e } \beta = S((2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2)).$$

Chamando $Y = \alpha t$ e $Z = \beta x$, temos $X^2 \pm aY^2 - 4bZ^2 = 0$. Observe que $(2m^2 - 2mn + n^2)(2m^2 + 2mn + n^2) = 4m^4 + n^4 > 0$, logo $b > 0$, assim o sinal dos coeficientes da equação acima não são todos iguais. Além disso, $2m^2 - 2mn + n^2, 2m^2 + 2mn + n^2, 2m^2 + n^2$ e $2m^2 - n^2$ são relativamente primos dois a dois (veja lema 4.5) e logo $(a, b) = 1$. Pelo teorema 3.1, a equação acima tem solução inteira não trivial se, e somente se, $\pm a$ é um quadrado módulo $4b$ e $4b$ é um quadrado módulo a. Assim devemos ter

$$\mp\frac{4m^4 - n^4}{\alpha^2} \equiv c^2 \pmod{4b} \Longrightarrow \mp 4m^4 - n^4 \equiv (\alpha c)^2 \pmod{4b},$$

pois $(\alpha^2, 4b) = 1$, logo $\mp 4m^4 - n^4$ deve ser um quadrado módulo cada primo que divide $R(2m^2 - 2mn + n^2)$ e $R(2m^2 + 2mn + n^2)$.

Também devemos ter

$$\frac{4(4m^4 + n^4}{\beta^2}) \equiv d^2 \pmod{a} \Longrightarrow (\beta d)^2 \pmod{a},$$

logo $4m^4+n^4$ deve ser um quadrado módulo $R(2m^2-n^2)$ e $R(2m^2+n^2)$. Como

$$4m^4-n^4 \equiv 2(2m^2)^2 \equiv -2n^24 \pmod{2m^2 \pm 2mn+n^2},$$

então 2 e -2 devem ser resíduos quadráticos de cada fator primo de $R(2m^2 \pm 2mn+n^2)$. As congruências acima de fato ocorrem, pois

$$4m^4-n^4-8m^4 = -4m^4-n^4 = -(2m^2-2mn+n^2)(2m^2+2mn+n^2),$$

$$4m^4-n^4+2n^4 = (2m^2-2mn+n^2)(2m^2+2mn+n^2).$$

Temos

$$4m^4+n^4 \equiv 4m^4+n^4-(2m^2+n^2)(2m^2-n^2) \equiv 2n^4 \pmod{2m^2+n^2},$$

$$4m^4+n^4-(2m^2+n^2)^2 \equiv -(2m^2+n^2)^2 \pmod{2m^2+n^2}.$$

Assim, 2 e -1 devem ser resíduos quadráticos de cada fator primo de $R(2m^2+n^2)$. A condição que resta é sempre satisfeita, pois

$$4m^4+n^4 \equiv (2mn)^2 \pmod{2m^2-n^2}.$$

Observe que os resíduos quadráticos de cada fator primo dos números acima são $-2, -1$ ou 2, logo pela proposiçao 3.2, todos esses primos devem ser congruentes a 1 módulo 8. □

Os lemas 4.6 e 4.7 nos fornecem condições para que as cônicas (4.6) e (4.13), respectivamente tenham infinitos pontos racionais. Observe que a existência de pontos racionais nessas cônicas são condições necessárias para haver pontos racionais na curva elíptica.

Exemplo 4.4 *Vejamos que* $(m,n) = (4,-7)$*, satisfaz as condições do lema 4.7. Temos* $2m^2-2mn+n^2 = 137$*,* $2m^2+2mn+n^2 = 25$ *e* $2m^2+n^2 = 81$*, assim* $R(2m^2-2mn+n^2) = 137$*,* $R(2m^2+2mn+n^2) = 1$ *e* $R(2m^2+n^2) = 1$*. Como todos esses primos são congruentes a* 1 *módulo* 8*, então a cônica*

$$\pm 81t^2 = -68x^2-224x+17,$$

tem infinitos pontos racionais. Substituindo $(m,n) = (4,-7)$ *em* (4.12) *obtemos*

$$81y^2 = -467x^2+34x+56.$$

Essas duas equações não tem solução comum. De fato, vejamos que a primeira equação faz com que x *tenha denominador não divisível por* 5*. Suponha* $t = \frac{t_1}{t_2}$*,* $(t_1,t_2) = 1$*,* $x = \frac{x_1}{x_2}$*,* $(x_1,x_2) = 1$*. Temos*

$$\pm 81\frac{t_1^2}{t_2^2} = -68\frac{x_1^2}{x_2^2}-224\frac{x_1}{x_2}+17,$$

logo

$$\pm 81t_1^2x_2^2 = -68x_1^2t_2^2-224x_1x_2t_2^2+17x_2^2t_2^2.$$

Suponha que $5 \mid x_2$*, então* $5 \mid x_1$ *(pois* $(x_1,x_2) = 1$*). Como* $5 \mid \pm 81t_1^2x_2^2$*, então* $5 \mid -68x_1^2t_2^2$*, mas* $5 \nmid -68$ *e* $5 \nmid x_1^2$*, logo* $5 \mid t_2$*. Sejam* α *e* β *a maior potência de* 5 *em* x_2 *e* t_2 *respectivamente.*

Assim,

$$\pm 81t^2\tilde{x}_2^25^{2\alpha} = -68x_1^2\tilde{t}_25^{2\beta}-224x_1\tilde{x}_2\tilde{t}_25^{\alpha}5^{2\beta}+17\tilde{x}_2\tilde{t}_25^{2\alpha}5^{2\beta},$$

isso implica

$$5^{2\alpha}(\pm 81t_1^2{\tilde{x}_2}^2) = 5^{2\beta}(-68x_1^2{\tilde{t}_2}^2-224\tilde{x}_25^{\alpha}+17\tilde{x}_2\tilde{t}_25^{2\alpha}).$$

Como $2 \nmid -68x_1^2{\tilde{t}_2}^2-224\tilde{x}_25^{\alpha}+17\tilde{x}_2\tilde{t}_25^{2\alpha}$*, então* $\alpha = \beta$*. Assim,*

$$\pm 81t_1^2{\tilde{x}_2}^2 = -68x_1^2{\tilde{t}_2}^2-224\tilde{x}_25^{\alpha}+17\tilde{x}_2\tilde{t}_25^{2\alpha}.$$

Módulo 5 *esta equação fica*

$$\pm t_1^2 \tilde{x_2}^2 = 2x_1^2 \tilde{t_2} \pmod 5,$$

logo ± 2 *é um quadrado módulo* 5. *Absurdo.*

Também temos que

$$\begin{aligned} \pm 81t^2 &\equiv -68x^2 - 224x + 17 \pmod 5 \\ \Longrightarrow \pm t^2 &\equiv 2x^2 - 4x + 2 \pmod 5 \\ \Longrightarrow \pm t^2 &\equiv 2(x-1)^2 \pmod 5. \end{aligned}$$

Se $5 \nmid t$, *então* $5 \nmid x-1$, *logo* $\left(\frac{2}{5}\right) = 1$, *o que é absurdo. Logo* $5 \mid t$ *e* $5 \mid x-1$, *assim* $x = 5\tilde{x} + 1$ *e portanto*

$$-467x^2 + 34x + 56 = -11675\tilde{x}^2 - 4500\tilde{x} - 377 \equiv -2 \pmod 5.$$

Assim,

$$81y^2 \equiv -2 \pmod 5,$$

mas -2 *não é um resíduo quadrático módulo* 5. *Portanto, as equações* $81y^2 = -467x^2+34x+56$ *e* $\pm 81t^2 = -68x^2 - 224x + 17$ *não ocorrem simultaneamente.*

4.3 O contra-exemplo para $A^4 + B^4 + C^4 = D^4$

Como não obtivemos sucesso com $(m, n) = (4, -7)$, vamos tentar outros valores de m e n. Vamos tomar agora $(m, n) = (8, -5)$. Temos $R(2m^2 - 2mn + n^2) = R(233) = 1$, $R(2m^2 + 2mn + n^2) = R(73) = 1$ e $R(2m^2 + n^2) = R(153) = 17$. Observe que todos esses números são congruentes a 1 módulo 8. Substituindo $(m, n) = (8, -5)$ em (4.12) e (4.13), obtemos

$$153y^2 = -779x^2 - 206x + 80, \quad \pm 153t^2 = 412x^2 - 320x - 103.$$

Observe que $(x, y) = \left(\frac{3}{14}, \frac{1}{42}\right)$ é uma solução racional da primeira curva. Considere a reta que passa por esse ponto e tem coeficiente angular $\frac{k}{3}$, isto é, $r : y = \frac{k}{3}x - \frac{k}{14} + \frac{1}{42}$. Substituindo y na equação da primeira curva, obtemos

$$(17k^2 + 779)x^2 + \left(-\frac{51}{7}k^2 + \frac{17}{7}k + 206\right)x + \frac{153}{156}k^2 - \frac{51}{98}k - \frac{15663}{196} = 0.$$

Resolvendo esta equação em relação a x, obtemos

$$x_1 = \frac{3}{14}, \quad x_2 = \frac{51k^2 - 34k - 5221}{14(17k^2 + 779)}.$$

Assim,

$$y = \frac{k}{3}x_2 - \frac{k}{14} + \frac{1}{42} = -\frac{(17k^2 + 7558k - 779}{42(17k^2 + 779)}.$$

Isto nos fornece uma parametrização de $153y^2 = -779x^2 - 206x + 80$. Observe que tomando y positivo, também temos uma parametrização; para os próximos cálculos iremos considerar y dessa forma.

Substituindo $x(k) = \dfrac{51k^2 - 34k - 5221}{14(17k^2 + 779)}$ na segunda cônica, obtemos

$$\pm 29988(17k^2+779)^2t^2+8646880k^4-1160624k^3+533984960k^2-264928816k-17200608704 = 0.$$

Multiplicando esta equação por $\frac{1}{68}$, temos

$$\pm 21^2(17k^2+779)^2t^2 = -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532). \quad (4.16)$$

Módulo 3, o lado direito da equação (4.16) fica

$$\begin{aligned} -4(31790k^4 - 4267k^3 + 1963180k^2 - 974003k - 63237532) &\equiv 2(2k^4 - k^3 + k^2 + k - 1) \\ &\equiv k^4 - 3k^3 - k^2 + 2k + 1 \\ &\equiv (k^2 - k - 1)^2 \pmod 3 \end{aligned}$$

Isso mostra que para manter x e t racionais, devemos escolhar o sinal positivo em (4.16). Façamos agora a mudança de coordenadas

$$X = \frac{k+2}{7}, \quad Y = \frac{3(17k^2+779)t}{14}.$$

Observe que $Y^2 = \frac{9}{16}(17k^2+779)^2t^2$, logo $196Y^2 = 9(17k^2+779)^2t^2$, assim $21^2(17k^2+779)^2t^2 = 7^2 \cdot 196Y$. Com o auxílio do maple, o segundo membro de (4.16) após a mudança de coordenadas fica

$$-305311160X^4 + 354781364X^3 - 53934143Xx^2 + 277065796X + 211576120.$$

Finalmente obtemos a equação

$$Y^2 = -31790X^4 + 36941X^3 - 56158X^2 + 28849X + 22030. \quad (4.17)$$

Com auxílio computacional buscamos (X, Y) racionais satisfazendo (4.17), essa busca retornou

$$(X, Y) = \left(-\frac{31}{467}, \frac{30731278}{467^2}\right).$$

Como $X = \frac{k+2}{7}$, então $k = -\frac{1151}{467}$. Substituindo k em $x(k)$ e $y(k)$, temos

$$x = -\frac{2685720}{6871891}, \quad y = -\frac{10739600}{20615673}.$$

Devemos substituir ainda x e y na parametrização dada para a superfície $\mathcal{S}_2$, logo

$$(r, s, t) = \left(-\frac{18796760}{20615673}, \frac{2682440}{20615673}, \frac{15365639}{20615673}\right).$$

Assim, obtemos o primeiro contra-exemplo para a conjectura de Euler, que é

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Este contra-exemplo foi dado por Noam D. Elkies em [2].

4.4 Obtendo mais soluções racionais para $r^4 + s^4 + t^4 = 1$

Queremos obter mais pontos racionais para (4.17) a partir dos pontos conhecidos

$$P_\pm = \left(-\frac{31}{467}, \pm\frac{30731278}{467^2}\right).$$

Observe que a curva elíptica (4.17) é da forma $Y^2 = \text{quartica}(X)$, então um processo análogo ao que fizemos no exemplo 2.4, nos fornece a adição de pontos de E. Lembre que devemos encontrar a e b tal que a parábola $Y = aX^2 + bX + c$ tenha um ponto de interseção tripla com E no ponto P_+, isto é, dado $P_\pm = (X_0, \pm Y_0)$, temos $Y - Y_0 = (X - X_0)(aX + b)$, logo

$$Y^2 = (X - X_0)^2(aX + b)^2 - 2Y_0(X - X_0)(aX + b) + Y_0^2.$$

Substitua Y^2 em (4.17) para obter a e b e com isso encontrar a raiz desejada. Definindo

$$g = \frac{Y - ((X - X_0)(aX + b)) + Y_0}{(X - X_0)^2},$$

calculamos $Div(g)$ e assim conseguimos encontrar o ponto $-Q = -(P_+ - P_-)$. Para nossa curva elíptica de interesse os resultados obtidos (conforme [2]) foram

$$\alpha = \frac{937766474523}{467 \cdot 15365639},$$

$$\beta = -\frac{2096569897386251210893331}{2 \cdot 15365639^3},$$

$$a = -\frac{2096569897386251210893331}{2 \cdot 15365639^3},$$

$$b = \frac{334937219677623362815466}{15365639^3},$$

$$c = \frac{1076124066222818157529571}{2 \cdot 15365639^3},$$

a partir do qual encontramos a coordenada X de $-Q$

$$\frac{12747393449396682022186564231356328 3}{12975955948587243128295271066869856 9},$$

e assim conseguimos a segunda solução para $A^4 + B^4 + C^4 = D^4$

$$A = 1439965710648954492268506771833175267850201426615300442218292336336633,$$

$$B = 4417264698994538496943597489754952845854672497179077898864124209346920,$$

$$C = 9033964557748253238805948242939845729100494792500574302814746573264588 0,$$

$$D = 9161781830035436847832452398267266038227002962257243662070370888722169.$$

Para decidir se conseguimos infinitas soluções racionais a partir dos pontos P_+ e P_-, devemos mostrar que $Q = P_+ - P_-$ é um ponto de ordem infinita, isto é, Q não é um ponto de torção, pelo teorema de Mazur, precisamos calcular nQ, para $n = 2, \ldots, 10$ e $n = 12$. Isso será um tanto quanto trabalhoso e não será feito neste trabalho.

Referências Bibliográficas

[1] Ash, A ; Gross, R. *Elliptic Tales: curves, couting and number theory.* Princeton University Press, 2012.

[2] Elkies, N. D. On $a^4+b^4+c^4 = d^4$. *Mathematics of Computation 51*, 184 (october 1988), 825–835.

[3] Hassett, B. *Introduction to Algebric Geometry.* University Press, 2007.

[4] Lander, L. J., and R., P. T. Counterexamples to euler's conjecture on sums of like powers. *Bull. Amer. Math Soc. 72* (1966), 1079.

[5] Martinez, F. B., Moreira, C. G., Nicolau, S., and Eduardo, T. *Teoria dos Números: um passeio com primos e outros números familiares.* IMPA, Rio de Janeiro, 2010.

[6] Milne, J. *Elliptic Curves.* Springer-Verlag, 2006.

[7] Monagan, M. B., Geddes, K. O., Heal, K. M., Labahn, G., Vorkoetter, S. M., McCarron, J., and DeMarco, P. *Maple 12 Programming Guide.* Maplesoft, Waterloo ON, Canada, 2008.

[8] Rusin, D. J. The mathematical atlas @ONLINE. `http://www.math.niu.edu/~rusin/known-math/96/quartic.maple`.

[9] Silverman, J. H. *The Arithmetic of Elliptic Curves*, vol. 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[10] Silverman, J. H., and J., T. *Rational points on elliptic curves.* Springer, 2010.

[11] Vaisencher, I. *Introdução às Curvas Algébricas Planas.* IMPA, 1979.