O GRUPO DOS PONTOS RACIONAIS EM CURVAS ELÍPTICAS

DOS SANTOS JUNIOR, E. * DO NASCIMENTO, P. †

2020 RECET V01.01

RESUMO

Neste trabalho, fizemos um estudo das curvas cúbicas, dando ênfase às curvas elípticas, mostramos os principais critérios que as caracterizam, definimos o conjunto dos pontos racionais em curvas elípticas e como encontrar, geometricamente, a soma de dois pontos pertencentes a este conjunto e mostramos que esta estrutura constitui um grupo abeliano utilizando o Teorema de Mordell.

Palavras-chave: Soma de pontos. Pontos Racionais. Curvas Elípticas. Grupo Abeliano.

ABSTRACT

In this work, we study of cubic curves, emphasizing elliptical curves, showing the main criteria that characterize them, defining the set of rational points in elliptic curves and how to find, geometrically, the sum of two points belonging to this set and we show that this structure constitutes an abelian group using Mordell's theorem.

Keywords: Sum of points, Rational points, Eliptic curves, Abelian group.

Sumário

Lista de ilustrações

*Edervan dos Santos Junior. Bacharel em Ciências Exatas e Tecnológicas pela Universidade Federal do Recôncavo da Bahia (UFRB), Brasil. E-mail: edervan3@gmail.com

†Paulo Henrique Ribeiro do Nascimento. Licenciado em Matemática pela Universidade Católica do Salvador (UCSal) e Mestre em Matemática pela Universidade Federal da Bahia (UFRB). Filiação: Centro de Ciências Exatas e Tecnológicas (CETEC)/ Universidade Federal do Recôncavo da Bahia (UFRB), Brasil. E-mail: nascimento.p@ufrb.edu.br

INTRODUÇÃO

Umas das principais influências históricas das curvas elípticas está no último Teorema de Fermat.

> A história do *Último Teorema de Fermat* está ligada profundamente à história da matemática, tocando em todos os temas da teoria dos números. Ela proporciona uma visão única do que impulsiona a matemática e, talvez ainda mais importante, o que inspira diversos matemáticos. O último Teorema é o coração de uma saga de coragem, fraudes, astúcia e tragédia, envolvendo todos os grandes heróis da matemática (SINGH, 2008).

Em meados de 1635, o francês Pierre de Fermat (1601-1665), ao se debruçar sobre as anotações de Diofante, matemático contemporâneo da era helenista, a respeito da Aritmética, viu nas páginas as ternas de Pitágoras e a até então famoso Teorema $A^2 + B^2 = C^2$, em que A e B representam os catetos de um triângulo retângulo. Fermat, de maneira perspicaz, generalizou essa equação, transformando-a em $A^n + B^n = C^n$ e disse em uma anotação, nas bordas do livro Aritmética que: "*Não existe uma solução não trivial de três números inteiros A, B e C que satisfaça tal equação, para $n > 2$*" (BRUNO, 2014, pág.6), em que não trivial significa que A, B e C não podem ser admitidos para valores iguais a zero, porém, não havia demostração alguma a respeito dessa conjectura proposta pelo matemático.

Apesar de parecer uma afirmação simples, originada de um teorema muito conhecido já naquela época (Teorema de Pitágoras), para se chegar a solução desse problema foi necessário trabalhos de diversos matemáticos renomados com abordagens em várias áreas, como teoria dos números, formas modulares e curvas elípticas, dentro de um período, de aproximadamente, três séculos e meio, sendo o último assunto o foco deste trabalho (GOUVÊA, 1995).

Nos anos seguintes que foram publicadas as anotações de Fermat, publicações estas feitas postumamente por seu filho Clément-Samuel, outros matemáticos contemporâneos a Fermat ou que vieram depois de sua morte se interessaram pela conjectura, dentre eles, podemos citar, Leonard Euler (1707-1783), que teve grandes contribuições no cálculo diferencial e infinitesimal. Euler, examinando a equação para os casos em que $n = 3$ e $n = 4$, percebeu que, para esses casos, a conjectura de Fermat é válida (GOUVÊA, 1995).

Em meados do século XIX, o matemático Ernest Kummer (1810-1893) se contrapôs ao método proposto pelos franceses, Gabriel Lamé (1795-1870) e Augustin Louis Cauchy (1789-1857). Eles anunciaram uma possível resolução geral para a até então conjectura de Fermat, usando uma propriedade chamada de **fatoração única**, sendo esse um dos critérios para o Teorema Fundamental da Aritmética, nos afirma que: $\forall\ a \geq 2, a \in \mathbb{N}$, a pode ser expresso como o produto de números primos. A demostração dos matemáticos franceses envolvia o uso de números imaginários pertencentes ao conjunto do números complexos $\mathbb{C}$ e ai que Kummer foi incisivo ao afirmar que tal demostração era inviável, pois a fatoração única só é válida para números pertencentes aos $\mathbb{N}$ (SOUZA, 2010).

As contribuições de Kummer não se resumiram em apenas comprovar a invalidade do método proposto por Lamé e Cauchy, Kummer teve exito em provar que para uma gama de números primos a conjectura de Fermat era válida', com essa demonstração Kummer conseguiu achar valores que corroboraram para a conjectura até para $n < 100$, apesar dos esforços, ainda estava muito distante de se chegar a um resultado geral que contemplasse para todos os valores de $n \in \mathbb{Z}$ as suposições de Fermat, a partir da década de 40, com o avanço dos computadores e o aumento da capacidade de processamento foi possível por meio de cálculos apurados achar valores de expoentes maiores, no inicio da década de 90 era possível averiguar a validade do teorema para valores de n até $4.000.000$ (GOUVÊA, 1995).

Porém, utilizando apenas métodos numéricos avançados a resolução do problema nunca teria sucesso, por mais que fossem achados valores de expoentes cada vez maiores, a menos que fosse apontado uma proposta geral, a conjectura não podia ser provada. Percebendo que por métodos numéricos era impossível chegar a uma solução, os

RECET Revista Eletrônica de Ciências Exatas e Tecnológicas

matemáticos que se propuseram a solucionar a conjectura, passaram a utilizar outras estrategias para resolução, perceberam que caso fosse possível ligar a conjectura de Fermat com alguma outra área da matemática conceitualmente bem explorada, se tornaria viável uma melhor análise sobre a problemática (SINGH, 2008),

Com o avanço do estudo das curvas elípticas, os matemáticos Yutaka Taniyama (1927-1958) e Goro Shimura (1930-1977), conjecturaram que "*toda curva elíptica pode ser parametrizada em uma forma modular*". Anos mais tarde, a ligação necessária entre as curvas elípticas e o Teorema de Fermat foi desenvolvida pelo matemático Gehard Frey (1944-), que conseguiu, por meio de artifícios algébricos, incorporar a equação com expoentes n de Fermat $A^n + B^n = C^n$ na equação de uma curva elíptica na forma reduzida, denotada por $y^2 = x^3 + ax^2 + bx + c$. Com a manipulação desenvolvida por Frey, a equação que faz a ponte entre ambos os assuntos ficou na forma $y^2 = x^3 + (A^n - B^n)x^2 - A^nB^n$, sendo esse polinômio a representação de uma possível curva elíptica. Com esta equação em mãos, Frey teve uma uma brilhante argumentação que possibilitou que a conjectura de Fermat ficasse a um passo de ser concluída, argumentando que, se a conjectura de Taniyama-Shimura estivesse correta, a sua equação não poderia existir, pois a mesma não apresentará uma forma modular. Logo, não existiria soluções racionais para A, B e C e a conjectura de Fermat definitivamente poderia ser chamada de Teorema (SOUZA, 2010).

Com esse argumento, restou ao matemático britânico Andrew Wiles (1975-1979) verificar a veracidade da conjectura de Taniyama-Shimura. Wiles dedicou aproximadamente sete seguidos anos da sua vida para provar essa hipótese e, em 1993, conseguiu tal façanha e citou, "***Esta odisseia particular agora acabou. Minha mente pode repousar***" (SINGH, 2008).

Como foi visto, as curvas elípticas tem desempenhado um papel de suma importância na matemática e como estão inclusas no conjunto de curvas cúbicas, neste trabalho será explorado as curvas cúbicas caracterizando-as de acordo com a singularidade, mostraremos alguns exemplos de como essas singularidades se comportam graficamente. Nas primeiras seções foi apresentado conceitos fundamentais para que se possa compreender as curvas algébricas racionais, com a abordagem em espaços projetivos, pontos e retas racionais.

Daremos ênfase a uma forma reduzida de curva cúbica chamada forma de Weiertrass, mostraremos um algoritmo que nos dará o conjunto de pontos racionais de uma curva elíptica e que o conjunto desses pontos formará um grupo abeliano, como matemático **L. Mordell** (1888-1972) havia provado.

CURVAS RACIONAIS

Nesta seção, daremos início ao estudo de curvas racionais no plano, mais especificamente, das retas e das cônicas, com o propósito de dar subsídios a respeito das curvas cubicas racionais.

***Definição* 1.** *Uma curva algébrica plana em $\mathbb{K}$ é um conjunto de pontos do plano dado por*

$$\mathcal{C}(\mathbb{K}) = \{(x, y) \in \mathbb{K}^2 : f(x, y) = 0\}, \qquad (1)$$

em que $f(x, y)$ é uma função e $\mathbb{K}$ é um corpo.

É usual considerar $\mathbb{K}$ como sendo o conjunto dos complexos e f como sendo um polinômio, uma vez que o Teorema Fundamental da Álgebra assegura que existem n raízes para equações polinomiais de grau $n > 1$ (LOBO et al., 2017).

Neste artigo, o corpo utilizado é o conjunto dos números racionais ($\mathbb{Q} = \mathbb{K}$) e a função f é polinomial de grau $n \leq 3$. O grau do polinômio $f(x, y)$ definirá a classe que a curva $\mathcal{C}_f$ é representada> Se $n = 1$, uma reta, se $n = 2$, uma cônica e se $n = 3$, uma cúbica.

RETAS RACIONAIS

Inicialmente, faremos algumas considerações para conjuntos de pontos cujas coordenadas são racionais em cuvas $\mathcal{C}_f$ e algumas propriedades.

***Definição* 2.** *Dizemos que um ponto do plano é racional se suas coordenadas são racionais.*

RECET Revista Eletrônica de Ciências Exatas e Tecnológicas

***Definição* 3.** *Seja $ax + by + c = 0$, a equação de uma reta $\mathcal{R}_f$. Dizemos que $\mathcal{R}_f$ é racional se a, b e $c \in \mathbb{Q}$.*

Inicialmente, mostraremos que a reta que contém dois pontos racionais não coincidentes é racional.

***Proposição* 1.** *Se (x_1, y_1) e (x_2, y_2) são pontos racionais, com $x_1 \neq x_2$, então a reta que passa por esses pontos é racional.*

Demonstração: Seja $y = mx + n$, com $m \neq 0$, a equação da reta que passa por (x_1, y_1) e (x_2, y_2), com $x_1 \neq x_2$.

Os coeficientes angular m e linear n são então determinados por:

$$m = \frac{y_2 - y_1}{x_2 - x_1} \quad (2)$$

$$n = \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} \quad (3)$$

que, claramente, são racionais.

Observe que se $\mathcal{R}_f$ é racional, nem todo ponto de $\mathcal{R}_f$ é racional. De fato, a equação $\mathcal{R}_f : x + y - 1 = 0$ é de de uma reta racional e o ponto $(\sqrt{2}, -\sqrt{2} + 1) \in \mathcal{R}_f$.

O resultado a seguir mostra que a interseção de duas retas racionais é um ponto racional.

***Proposição* 2.** *A interseção entre duas retas racionais é um ponto racional.*

Demonstração: Sejam $\mathcal{R}_f$ e $\mathcal{R}_g$ retas racionais de equações dadas, respectivamente, por $y = ax + b$ e $y = cx + d$. Se $P(x, y)$ é a interseção entre essas duas retas, temos:

$$\begin{cases} -ax + y = b \\ -cx + y = d \end{cases}$$

Pela regra de Crammer, temos que:

$$x = \frac{b - d}{c - a}$$

$$y = \frac{d - a}{c - a} + \frac{c - b}{c - a},$$

e assim, o ponto $P(x, y) \in \mathbb{Q}$.

***Proposição* 3.** *Seja $\mathcal{R}_f$ uma reta racional. Se $\mathcal{R}_g$ é paralela a $\mathcal{R}_f$, então ela é racional.*

Demonstração: Considere uma reta racional r, de equação $y = ax + b, a \neq 0$. Se s é paralela a r e não coincidente, temos que sua equação é $y = ax + c, b \neq c$. Sendo $S(x_s, y_s)$ um ponto racional pertencente à reta s, temos que $y_S = ax_s + c$ ou, ainda, $c = y_s - ax_s$, concluindo que c é racional.

CÔNICAS RACIONAIS

Com os resultados até aqui estabelecidos sobre retas racionais, vamos estender o mesmo conceito para as cônicas racionais, apresentando, previamente, alguns conceitos e resultados.

***Definição* 4.** *As cônicas racionais são curvas que apresentam equações dadas por polinômios de duas variáveis reais de grau dois:*

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0, \quad (4)$$

sendo A, B, C, D, E e $F \in \mathbb{Q}$, com pelo menos um dos coeficientes A, B ou C diferentes de zero.

De forma análoga às retas racionais, temos que uma curva cônica racional não é formada apenas de pontos racionais. Para mostrarmos isso, apresentaremos três resultados que auxiliarão a demonstração.

***Lema* 1.** *(Gauss) Um polinômio em $\mathbb{Z}$ de grau $n \geq 1$ é irredutível em $\mathbb{Z}$ se, e somente se, os coeficientes são primos entre si e irredutível em $\mathbb{Q}$.*

***Corolário* 1.** *Seja $f \in \mathbb{Z}$ de grau $n \geq 1$. Se não é possível decompor f como um produto de polinômios ambos de grau $n \geq 1$ em $\mathbb{Z}$, então f é irredutível em $\mathbb{Q}$.*

As demonstrações do Lema 1 e do Corolário 1 podem ser encontradas, respectivamente, em (BIAZZI, 2014, p. 43) e (CRUZ, 2013, p. 32).

Para provarmos que f não pode ser escrito como produto de polinômios de grau $n \geq 1$, podemos usar o critério de Eisenstein:

RECET Revista Eletrônica de Ciências Exatas e Tecnológicas

***Proposição* 4** (Critério de Eisenstein)**.** *Seja,*

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \qquad (5)$$

um polinômio de coeficientes inteiros. Se existe um inteiro primo p tal que

1. $p|a_i$, *para* $i = 0, 1, \ldots, n-1$;
2. $p \nmid a_n$;
3. $p^2 \nmid a_0$,

então f não pode ser escrito como produto de polinômios em $\mathbb{Z}$ de grau maior ou igual a 1. Em particular, f é irredutível sobre $\mathbb{Q}$ (COELHO, 2019).

Agora, considere a curva de equação

$$x^2 + y^2 = 3, \qquad (6)$$

que representa uma circunferência de raio $\sqrt{3}$. Uma expressão mais abrangente para a cônica de equação (6) é dada por

$$x^2 + y^2 = 3u^2, \qquad (7)$$

isso para situações não triviais com $x, y, u \in \mathbb{Z}$.

Para que se tenham valores inteiros que satisfaçam (7), x e y devem ser divisíveis por 3. Por redução ao absurdo, suponha que 3 seja divisor comum de x e y. Sendo assim, temos que $3|x$ e $3|y$, concluindo que $9|(x^2+y^2) \Rightarrow 9|3u^2 \Rightarrow 3|u$. Isso mostra que 3 é um divisor comum de x, y e u. Porém, essa afirmação não procede, uma vez que a equação está na sua forma irredutível, podemos afirmar que x, y e u são primos entre si. Logo, o único divisor comum será 1. Por isso, no conjunto $\mathbb{Z}$, 3 não poderá ser solução da equação (7) e, pelo Corolário 1, polinômios irredutíveis em $\mathbb{Z}$ são irredutíveis em $\mathbb{Q}$ e, assim, não haverá solução pertencente aos conjunto dos racionais.

Concluímos, assim, que nem todo ponto de uma curva racional é racional.

Um resultado importante sobre retas racionais secantes a uma cônica racional é dado pela proposição a seguir:

***Proposição* 5.** *A interseção entre retas racionais e cônicas racionais que tenham um ponto previamente definido como racional, tem um segundo ponto de interseção também racional.*

Demonstração: Considere uma reta racional $\mathcal{R}$ secante a uma cônica racional $\mathcal{G}$ de equações dadas, respectivamente, por: $yt = -sx - v$, com $t \neq 0$, e $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$.

Isolado-se y na equação de $\mathcal{R}$ e substituindo-se na equação de $\mathcal{G}$, obteremos os coeficientes:

$$\begin{aligned} \varphi &= A - \frac{Bs}{t} + \frac{Cs^2}{t^2} \\ \sigma &= \frac{2Csv}{t^2} - \frac{Bv}{t} + D - \frac{Es}{t} \\ \psi &= -\frac{Ev}{t} + \frac{Cv^2}{t^2} + F, \end{aligned}$$

que claramente são racionais.

Assim, temos a equação que determina a interseção entre a cônica e a reta pode ser escrita como:

$$\varphi x^2 + \sigma x + \psi = 0.$$

Como estamos supondo que a reta é secante à cônica, temos que $\varphi \neq 0$ e suas raízes são dadas por:

$$\begin{aligned} x_1 &= \frac{-\sigma + \sqrt{\Delta}}{2\varphi} \\ x_2 &= \frac{-\sigma - \sqrt{\Delta}}{2\varphi} \end{aligned}$$

em que $\Delta = \sigma^2 - 4\varphi\psi \in \mathbb{Q}$.

Como, por hipótese, um dos pontos é racional, digamos que seja x_1, temos que Δ é um quadrado perfeito e x_2 é racional. Segue que $y_2 = -\frac{s}{t}x_2 - \frac{v}{t}$ é também racional.

CÚBICAS RACIONAIS

O conteúdo a respeito das curvas cúbicas e mais especificamente, as elípticas, podem ser vistos em (SOUZA, 2012) e (SOUZA, 2013).

É natural pensar em estender o tratamento do conjunto de pontos racionais em retas e cônicas a curvas expressas por polinômios de graus ainda maiores. Entretanto, nos limitaremos ao estudo de

uma classe específica de curvas cúbicas, que foram tratadas pelo alemão Karl Weierstrass (1815-1897) ao transformar uma equação cúbica homogênea de grau 3, representada por;

$$\begin{aligned} & ax^3 + by^3 + cz^3 + dx^2y \\ + \quad & ex^2z + fy^2x + gy^2z \\ + \quad & hz^2x + iz^2y + jxyz = 0 \end{aligned} \tag{8}$$

na equação

$$y^2 = x^3 + ax^2 + bx + c \tag{9}$$

utilizando o espaço projetivo.

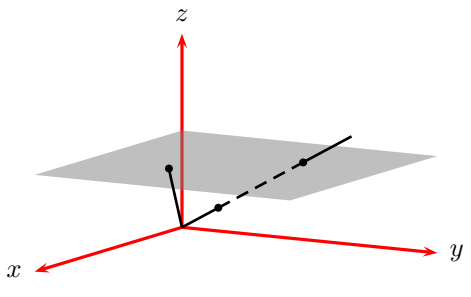
É possível encontrar o conjunto de pontos racionais sobre a curva $C(\mathbb{Q})$, representada pela equação de Weierstrass (9) pois a forma geral (8) e a reduzida (9) apresentam uma correspondência bijetora (ver (TAVARES, 2011, p. 22)).

Nas próximas seções, daremos foco ao estudo da geometria projetiva. Veremos que as curvas cúbicas podem ser definidas como redutíveis e irredutíveis e, nas curvas cúbicas irredutíveis podem ser dotadas de pontos singulares ou serem suaves em toda sua extensão, sendo essa última categorizada como curvas elípticas.

INTERSEÇÃO DE CURVAS NO ESPAÇO PROJETIVO

Seja $\pi \subset \mathbb{R}^3$ um plano afim (plano que não contém a origem e, por isso, um ponto arbitrário deste plano possui pelo menos uma coordenada diferente de zero) paralelo ao plano xOy e observe, na Figura 1, que para cada $P' \notin \pi$, existe um ponto $P \in \pi$ resultante da interseção da reta que passa por P' e por O. Dessa forma, existe uma correspondência biunívoca entre o conjunto de pontos do plano π e o conjunto das retas que passam por P' e por O.

Figura 1 – Representação do plano π com um ponto P



Fonte – Elaborada pelo autor

Denotaremos as coordenadas da projeção de $P'(x, y, z)$ em π por $P(x : y : z)$, uma vez que $(x : y : z) = (x_1 : y_1 : z_1)$ se, e somente se, $(x, y, z) = \lambda(x_1, y_1, z_1)$, $\lambda \neq 0$.

De forma análoga, dada uma reta $\nu \subset \pi$, temos que para cada ponto $P \in \nu$, existe uma reta em $\mathbb{R}^3$ que passa por P e por O.

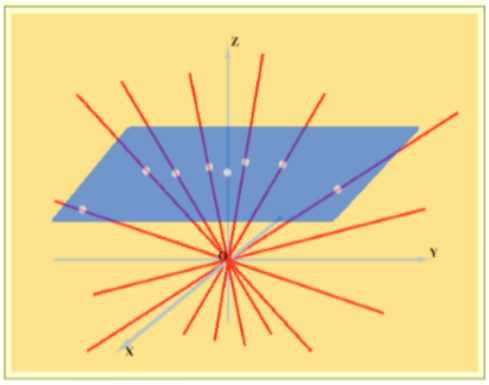
Podemos, assim, associar o espaço projetivo real de dimensão n, com o espaço euclidiano de dimensão $n + 1$.

Definição 5. *O espaço projetivo de dimensão $n \in \mathbb{R}$ ($\mathbb{PR}^n$) é o conjunto das retas no espaço euclidiano de dimensão $n+1$ ($\mathbb{R}^{n+1}$), que passam pela origem, excluindo-se o ponto que representa a origem.*

Assim, por exemplo, $\mathbb{PR}^2$ é o conjunto dos pontos do $\mathbb{R}^3 \setminus \{(0, 0, 0)\}$ tais que $(x, y, z) = (a, b, c)t, t \in \mathbb{R}$.

O conjunto dos pontos projetivos pode ser visto em duas classes, aquela em os pontos estão contidos nos planos $z \neq 0$ e aquela que possuem representação no plano projetivo, uma vez que $\left(\frac{x}{z} : \frac{y}{z} : 1\right)$, ou seja, o plano $\pi : z = 1$ é um representante de todo ponto projetivo e os que estão no plano $z = 0$.

Figura 2 – Representação de pontos no plano π.



Fonte – (TAVARES, 2011)

Observarmos, na Figura 2, que à medida que atribuirmos as coordenadas projetivas valores cada vez menores de z, a reta intercepta pontos cada vez mais distantes da origem, ao atribuirmos $z = 0$, a reta que se conecta a P' não possui representante no plano π, e assim dizemos que este ponto esta no infinito e $P(x : y : 0)$ é chamado de ponto ideal ou ponto no infinito.

Consideremos, agora, um polinômio homogêneo F (aquele que possui os seus monômios com mesmo grau) de graus menores ou iguais a 3, representados por $F(x, y, z)$, onde a equação $F(x, y, z) = 0$ representa uma superfície em $\mathbb{R}^3$ que será representada no plano projetivo de equação $z = 1$.

A condição de homogeneidade nos trará $F(\lambda x, \lambda y, \lambda z) = \lambda^d F(x_1, y_1, z_1)$ (VAINSENCHER, 1996), sendo $d \geq 1$ o grau do polinômio F. Isso que dizer que ao homogeneizarmos um polinômio, estamos inserindo uma nova variável com a intenção de que os monômios tenham graus iguais. No caso dos polinômios de duas variáveis e de grau n, superfícies em $\mathbb{R}^3$, ao o homogeneizarmos, a medida que estabelecemos valores a nova variável, o que estamos encontrando são interseções entre o plano e a superfície, curvas planas projetivas, e assim, a condição de homogeneidade mostra que à medida que interceptamos planos, as curvas resultantes dessas interseções serão proporcionais entre si.

Para determinarmos curvas no espaço projetivo é necessário colocarmos o polinômio na forma homogênea, processo chamado homogeneização. Assim, ao homogeneizarmos a reta $g : ax + by + c = 0$, obtemos $G : ax + by + cz = 0$, contendo os mesmos pontos da curva g para $z = 1$.

Um importante resultado (Corolário 2) sobre o número de interseções de duas curvas projetivas é uma consequência do Teorema 1 (ver (SANTOS; CARVALHO, 2007, p. 267)).

***Teorema* 1** (Teorema de Bezout (1730-1783))**.** *Duas curvas algébricas planas C_f e C_g, sem componentes irredutíveis em comum e com graus m e n, respectivamente, se intersectam em t pontos, sendo $0 < t \leq mn$.*

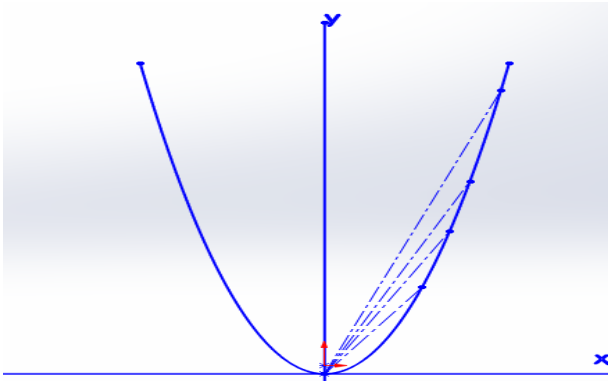
***Corolário* 2.** *Se as curvas C_f e C_g são projetivas, então o número de interseções é dada pelo produto mn, ou seja, leva-se em consideração suas multiplicidades.*

Uma prova do Corolário 2 pode ser encontrada em (TAVARES, 2011, p. 66).

Se tomarmos por exemplo uma parábola de equação $f : y = x^2$ e uma reta qualquer, esta interceptará a cônica em exatamente dois pontos (ver Figura 3), inclusive se esta reta é horizontal e tangente ao gráfico de f a raiz terá multiplicidade 2. Observe que a raiz de f é também raiz de f'.

Observemos, na parábola $f : y = x^2$, que a reta de equação $x = 0$ a intercepta somente na origem. Na geometria projetiva esta reta possui o segundo ponto de interseção com a cônica no infinito.

Figura 3 – Interseções entre retas e a parábola.

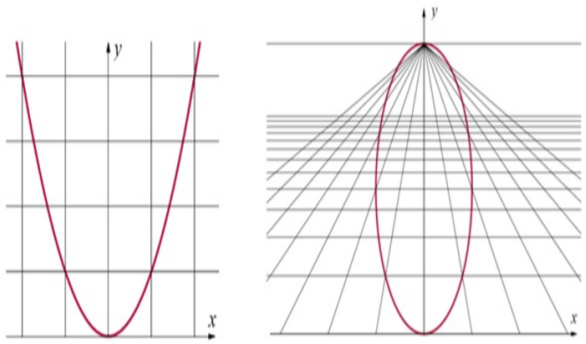


Fonte – Elaborada pelo autor

RECET Revista Eletrônica de Ciências Exatas e Tecnológicas

Se homogeneizarmos o polinômio f, obtemos $F : yz - x^2 = 0$, os pontos que aparecem no infinito são aqueles os quais $z = 0$, logo o ponto no infinito (ou ideal) da cônica projetiva será o ponto $(0 : 1 : 0)$.

Figura 4 – Segundo ponto da parábola.



Fonte – (GONÇALVES, 2013)

Na Figura 4 é mostrada a segunda raiz de uma parábola na geometria projetiva.

CURVAS ELÍPTICAS

As curvas cúbicas de Weirstrass (10) são encontradas através de uma série de passos algébricos e transformações projetivas partindo do polinômio homogêneo

$$\begin{aligned} F(X,Y,Z) = \quad & aX^3 + bY^3 + cZ^3 + dX^2Y \\ + \quad & eX^2Z + fY^2X + gY^2Z \\ + \quad & hZ^2X + iZ^2Y + jXYZ = 0, \end{aligned}$$

para obter a equação

$$y^2 = x^3 + ax^2 + bx + c. \qquad (10)$$

(SOUZA, 2013), (MILNE, 1996) e (VIEZZER et al., 2000).

As equações de Weirstrass (10) podem ser classificadas de acordo com a presença de singularidades (cúspide ou nó). Se para cada ponto dessa curva houver uma reta tangente associada, é correto afirmar que ela não possui pontos singulares (curva lisa, suave, regular ou não singular), caso contrário, dizemos que a curva é singular.

Um critério utilizado para determinar se a curva é singular é feito da seguinte forma: fazemos $f(x,y) = x^3 + ax^2 + bx + c - y^2$ e verificamos a existência de pontos da curva que anulem as derivadas parciais de f, ou seja, (x_0, y_0) é ponto singular da curva se

$$\frac{\partial f}{\partial x}(x_0, y_0) = \frac{\partial f}{\partial y}(x_0, y_0) = 0.$$

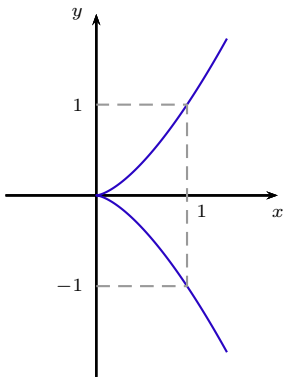
Outra forma, é utilizando o discriminante:

$$\Delta = \alpha(r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2,$$

em que r_1, r_2 e r_3 são as raízes do polinômio $g(x) = x^3 + ax^2 + bx + c$ e classificamos a curva em não-singular, se $\Delta \neq 0$.

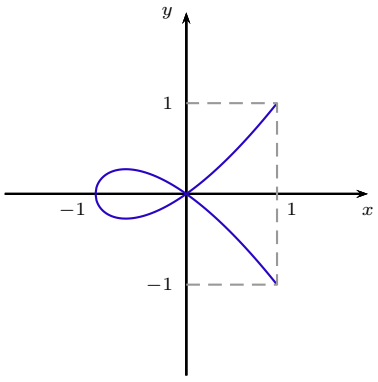
Se as raízes de $g(x)$ são todas distintas, a curva é não-singular. Nos outros casos que apresentam raízes iguais, teremos $\Delta = 0$. Ocorrendo apenas duas raízes iguais, teremos que a curva apresentará um ponto singular em forma de nó (ver Figura 5) e, com três raízes iguais, a singularidade será representada em forma de uma cúspide (ver Figura 6) (GOUVÊA, 1995).

Figura 5 – Curva cúbica $y^2 = x^3$.



Fonte – Elaborada pelo autor

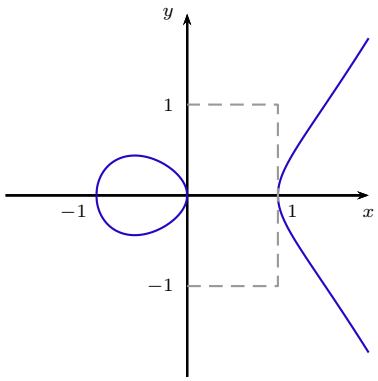
Figura 6 – Curva cúbica $\sqrt{2}y^2 = x^3 + x^2$.



Fonte – Elaborada pelo autor

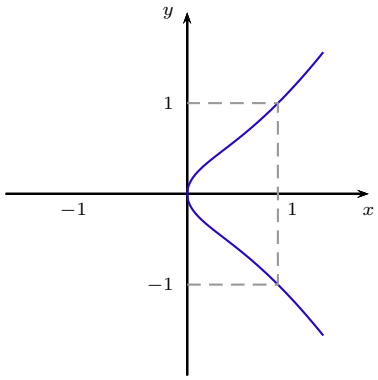
As derivadas parciais das equações das curvas, representadas nas figuras 7 e 8, são diferentes de zero e suas raízes são distintas. Por isso, temos que os discriminantes dos polinômios que as representam também são diferentes de zero. As equações das curvas na forma de Weierstrass não singulares, são denominadas **curvas elípticas**.

Figura 7 – Curva elíptica $y^2 = x^3 - x$.



Fonte – Elaborada pelo autor

Figura 8 – Curva elíptica $y^2 = x^3 - x$.



Fonte – Elaborada pelo autor

A ESTRUTURA DE GRUPO ABELIANO DO CONJUNTO DE PONTOS RACIONAIS EM CURVAS ELÍPTICAS RACIONAIS

A respeito desta seção, temos como referências (SOUZA, 2012), (VIEZZER et al., 2000) e (CARNEIRO; ALMEIDA, 2015) como textos base.

Considere uma curva elíptica racional $C \subset \mathbb{R}^2$, ou seja,

$$y^2 = x^3 + ax^2 + bx + c, \tag{11}$$

com a, b e $c \in \mathbb{Q}$, $\Delta \neq 0$ e seja F a homogeneização da equação (11) dada por:

$$F : zy^2 = x^3 + azx^2 + bz^2x + cz^3. \tag{12}$$

Claramente, se tomarmos o plano projetivo $z = 0$, a projeção de um ponto da cúbica se dará no infinito. Denotaremos esse ponto por O. Sendo ele um ponto racional (VIEZZER et al., 2000), toda reta perpendicular ao eixo x intercepta C no ponto O.

Com as afirmações citadas nos dois parágrafos anteriores, podemos adicionar pontos racionais em uma curva elíptica, mesmo não se tratando de uma operação convencional. Mais adiante, veremos que essa estrutura é a de um grupo abeliano, como o matemático francês Louis Mordell (1906-1998) provou.

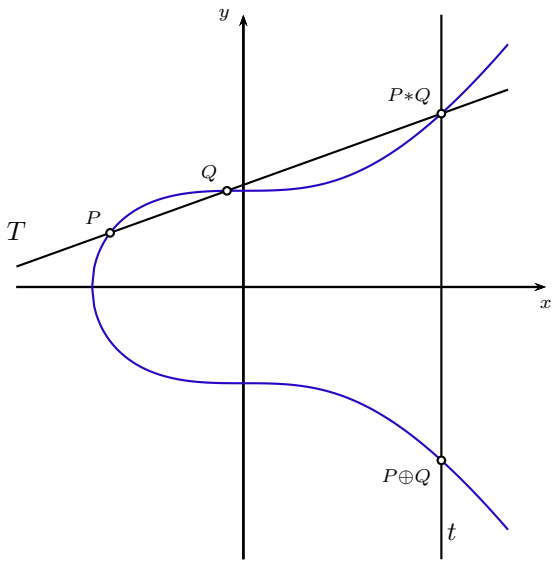
Uma fato interessante sobre esse subconjunto de pontos racionais, é que ele é finito (ver (NUNES, 2015, p.)), ou seja todos os pontos racionais sobre uma curva elíptica podem ser obtidos a partir desse subconjunto, porém nosso trabalho se restringirá a demonstrar que a estrutura de grupo desse subconjunto é abeliana [1].

Se tomarmos dois pontos P e Q racionais sobre a curva elíptica e traçarmos uma reta T contendo esses pontos (ver Figura 9), como foi provado, a reta T terá coeficientes racionais e, pelo Teorema de Bezout, haverá um terceiro ponto de interseção também racional. Mesmo que a reta T tangencie a curva elíptica, o Teorema de Bezout não é contrariado, pois o ponto P terá multiplicidade 2 em P e interceptará a cúbica em um novo ponto PP.

Para encontrarmos a soma de dois pontos racionais sobre uma curva elíptica, consideremos dois pontos $P(x_1, y_1)$ e $Q(x_2, y_2)$ racionais. Em seguida, traçamos uma reta t contendo os pontos P e Q (claramente racional) que interceptará a curva em $P * Q(x_3, y_3)$. Haja vista que toda reta vertical contém o ponto no infinito O, esta reta vertical que passa por $P * Q$ interceptará a curva $P \oplus Q$ (ver Figura 9), sendo este o resultado da soma de P e Q.

[1] Um grupo abeliano é constituído das propriedades de comutatividade, associatividade, a presença de um elemento neutro e admite um elemento simétrico

Figura 9 – Representação do ponto $P \oplus Q$.



Fonte – Elaborada pelo autor

Observemos que o ponto $P \oplus Q$ é simétrico ao ponto $P * Q$ em relação ao eixo x. Com isso, o ponto $P \oplus Q$ será definido pelo par ordenado $(x_3, -y_3)$.

De forma algébrica, dados dois pontos racionais (x_1, y_1) e (x_2, y_2), contidos na reta t, temos que a equação que a define é $y = \alpha x + d$, para $\alpha = (y_2 - y_1)/(x_2 - x_1)$, e intercepta a curva elíptica $y^2 = x^3 + ax^2 + bx + c$, com a, b e $c \in \mathbb{Q}$. O ponto de interseção entre a reta e a curva elíptica é raiz da equação:

$$x^3 + (-\alpha^2 + a)x^2 + (-2\alpha x d + b)x + (-d^2 + c) = 0.$$

Utilizando as relações de Girard, a relação entre os pontos de interseção e os coeficientes do polinômio que representa a curva elíptica é dada por:

$$x_1 + x_2 + x_3 = -(-\alpha^2 + a).$$

Logo, o terceiro ponto é:

$$x_3 = (\alpha^2 - a) - x_1 - x_2.$$

Segue que,

$$y_3 = \alpha x_3 + d$$

e o ponto $P \oplus Q(x_3, -y_3)$.

Se uma reta tangencia a curva elíptica em um ponto P, temos que $x_1 = x_2$ e $y_1 = y_2$. Devemos adotar um novo passo algébrico para encontrar o ponto $P * P$ e, consequentemente, a resultante da soma de pontos. Para isso, devemos derivar implicitamente a equação reduzida de Weierstrass $y^2 = g(x)$, para $g(x) = x^3 + ax^2 + bx + c$, para encontrar o coeficiente angular da reta tangente, ou seja,

$$y' = \frac{g'(x)}{2y}$$

Com $\alpha = y'$, temos que a relação entre as raízes do polinômio e seus coeficientes é

$$x_1 + x_2 + x_3 = -(a - y'^2).$$

Como $x_1 = x_2$, temos $x_3 = (y'^2 - a) - 2x_1$ e $y_3 = y'x_3 + d$ e, com $P * P$ determinado, temos que as coordenadas da soma de pontos $(x_3, -y_3)$.

Como o conjunto $C(\mathbb{Q}) \cup \{O\}$ munido da operação $\oplus$ que associa dois elementos desse conjunto a outro pertencente a ele mesmo, e esta operação satisfaz as condições de associatividade, elemento inverso e elemento neutro, temos então um grupo. Além disso, veremos que esta operação é comutativa e a estrutura é então de um grupo abeliano.

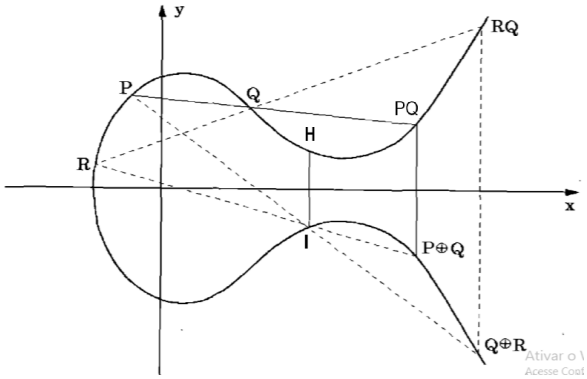
A respeito da comutatividade, podemos perceber, na Figura 9, que a reta que passa por P e Q é dada por $\overline{PQ}$ que será congruente a reta $\overline{QP}$, por isso a operação interna do conjunto $P \oplus Q = Q \oplus P$ é válida.

Se traçarmos uma reta vertical partindo do ponto O (no infinito) até um ponto P encontraremos um terceiro ponto R na cúbica, porém se traçarmos uma reta vertical partindo do ponto R até o ponto O, esta intersectará a cúbica no ponto P. Logo, o ponto O é o elemento neutro, ou identidade do conjunto e, consequentemente, R o elemento oposto.

Para demonstrar a associatividade dos elementos do conjunto $C(\mathbb{Q}) \cup \{O\}$ de forma geométrica, primeiro devemos encontrar $Q \oplus R$ (ver Figura 10). Traçando a reta que liga Q a R, encontramos o ponto $R * Q$. Em seguida, traçamos uma reta vertical partindo do ponto O, no infinito, até o ponto $R * Q$. Pelo Teorema de Bezout, encontramos $Q \oplus R$. O passo seguinte consiste em traçar uma reta que liga o ponto $Q \oplus R$ ao ponto P. Observemos que a

interseção estará entre o ponto $Q \oplus R$ e P, que denotaremos de I. De forma análoga, traçamos uma reta vertical até o ponto O e encontramos o ponto $H = P \oplus (Q \oplus R)$.

Figura 10 – Associatividade de pontos.



Fonte – (VIEZZER et al., 2000)

Por outro lado, ao traçarmos uma reta que passe por P e Q (Figura 10), encontramos o ponto $P * Q$ e ao traçamos uma reta do ponto O até $P * Q$, encontramos $P \oplus Q$. Em seguida, traçamos outra reta do ponto $P \oplus Q$ ao ponto R. É possível notar que essa reta interceptará a curva elíptica também no ponto I. Por último, traçamos uma reta vertical de I até O, encontrando o ponto $H = (P \oplus Q) \oplus R$, coincidindo com o ponto $P \oplus (Q \oplus R)$. Provando que o conjunto de pontos racionais pertencentes a curva elíptica possui uma estrutura de grupo abeliano.

CONSIDERAÇÕES FINAIS

A construção deste artigo possibilitou o breve contato com vários temas da Matemática, dentre elas, a influência das curvas elípticas na resolução do Teorema de Fermat, a aritmética modular, a geometria projetiva e a estrutura de grupo.

Foi visto que, para encontrar pontos racionais sobre curvas, apesar de envolver muito algebrismo, a utilização de formas geométricas tornou o trabalho mais compreensível, inclusive ao provar a estrutura de grupo abeliano do conjunto de pontos racionais em curvas elípticas com a operação de adição de pontos.

Vimos que ao definir uma operação geométrica sobre o conjunto de pontos racionais de uma curva elíptica, determinamos uma estrutura de grupo abeliano.

Referências

BIAZZI, R. N. Polinômios irredutíveis: critérios e aplicações. Universidade Estadual Paulista (UNESP), 2014. Citado na página 4.

BRUNO, S. da S. *O Último Teorema de Fermat para* $n = 3$. 86 f. Dissertação (PROFMAT Mestrado Profissional em Matemática em Rede Nacional) — UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO, Rio de Janeiro, 2014. Citado na página 2.

CARNEIRO, J. S.; ALMEIDA, K. E. D. **Uma Introdução às Curvas Elípticas com Aplicações para o Ensino Médio**. *Ciência e Natura*, Universidade Federal de Santa Maria, v. 37, n. 3, p. 452–462, 2015. Citado na página 9.

COELHO, L. A. *Congruências e Aplicações em Polinômios*. 65 p. Dissertação (Mestrado) — Universidade Federal de São João del-Rei, São João Del-Rei, 2019. Citado na página 5.

CRUZ, K. B. ***Introdução à Teoria de Galois***. 2013. 73 p. Disponível em: <https://www.dm.ufscar.br/dm/index.php/component/attachments/download/20>. Acesso em: 13.11.2020. Citado na página 4.

GONÇALVES, T. d. S. ***Uma introdução à geometria projetiva para o ensino fundamental***. Dissertação (Mestrado), 2013. Citado na página 8.

GOUVÊA, F. Q. Uma demonstraçao maravilhosa. *Matemática Universitária*, n. 19, p. 16–43, 1995. Citado 2 vezes nas páginas 2 e 8.

LOBO, F. C. G. D. et al. Números complexos, polinômios e equações algébricas. [sn], 2017. Citado na página 3.

MILNE, J. Elliptic curves. *Available on http://www. jmilne. org/math/CourseNotes/math679. html*, Citeseer, 1996. Citado na página 8.

NUNES, H. S. ***Curvas Elípticas e o Teorema de MordellWeil***. 2015. 73 p. Disponível em: <https://im.ufal.br//pt-br/pos-graduacao/matematica/defesas/mestrado/2015/65a-defesa-de-dissertacao-hugo-santos-nunes/dissertacao>. Acesso em: 13.11.20. Citado na página 9.

SANTOS, P. B. D.; CARVALHO, C. F. de. **Introdução à Teoria das Curvas Algébricas Afins**. *FAMAT em Revista*, p. 259, 2007. Disponível em: <http://www.antigo.famat.ufu.br/sites/famat.ufu.br/files/Anexos/Bookpage/Famat_Revista_09.pdf>. Citado na página 7.

SINGH, S. *Último Teorema de Fermat. tradução CALIFE, Jorge L*. [S.l.]: Rio de Janeiro: Record, 2008. Citado 2 vezes nas páginas 2 e 3.

SOUZA, A. O. *Pontos Racionais em Curvas Elípticas*. 62p. p. Dissertação (Mestrado) — Universidade Federal de Uberlândia, 2012. Citado 2 vezes nas páginas 5 e 9.

SOUZA, F. N. B. de. Uma abordagem geométrica para as equações cúbicas. 2013. Citado 2 vezes nas páginas 5 e 8.

SOUZA, T. B. Os três séculos do último teorema de fermat. In: UEOP. *XXIV Semana Acadêmica da Matemática*. [S.l.], 2010. Citado 2 vezes nas páginas 2 e 3.

TAVARES, J. N. ***Tópicos de Geometria***. 2011. 95 p. Disponível em: <http://arquivoescolar.org/bitstream/arquivo-e/35/1/Topicos_Geometria.pdf>. Citado 2 vezes nas páginas 6 e 7.

VAINSENCHER, I. *Introdução às curvas algébricas planas*. [S.l.]: Instituto de Matemática Pura e Aplicada, 1996. Citado na página 7.

VIEZZER, E. R. et al. *Curvas algébricas racionais*. 2000. Disponível em: <https://repositorio.ufsc.br/bitstream/handle/123456789/96819/Elizandra_Regina_Viezzer.PDF?sequence=1>. Citado 3 vezes nas páginas 8, 9 e 11.

RECET Revista Eletrônica de Ciências Exatas e Tecnológicas