O Posto de Curvas Elípticas sobre o Corpo dos Números Racionais

Rodrigo dos Santos Veloso Martins

Dissertação de Mestrado apresentada ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientadora: Luciane Quoos Conte

Rio de Janeiro

Julho de 2011

O Posto de Curvas Elípticas sobre o Corpo dos Racionais

Rodrigo dos Santos Veloso Martins

Dissertação submetida ao Corpo Docente do Instituto de Matemática Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática.

Aprovada por:

Luciane Quoos Conte

PhD - IM - UFRJ - Orientador.

José Gilvan de Oliveira

PhD - DMAT - UFES

Nicolas Paul André Puignau

PhD - IM - UFRJ

Miriam del Milagro Abdón

PhD - IM - UFF

FICHA CATALOGRÁFICA

Martins, Rodrigo dos Santos Veloso.
O Posto de Curvas Elípticas sobre o Corpo dos Números Racionais
Rodrigo dos Santos Veloso Martins.
Rio de Janeiro: UFRJ, IM, 2011.
Dissertação - Universidade Federal do Rio de Janeiro, IM.
1. Curvas Planas.
2. Curvas Elípticas
3. Pontos de Torsão.
4. O Teorema de Mordell
5. Posto de Curvas Elípticas
(Mestrado-UFRJ/IM) Conte, Luciane Quoos
II. Universidade Federal do Rio de Janeiro III. Título.

Agradecimentos

A minha família, em especial a minha mãe e ao meu irmão. A minha orientadora, pela sua dedicação, pela sua paciência e por seus bons conselhos. Aos meus amigos da pós-graduação. Ao CNPq e à CAPES, pelo apoio financeiro.

Resumo

Descrevemos uma operação binária no conjunto $E(\mathbb{Q})$ dos pontos com coordenadas racionais de uma curva elíptica que o torna um grupo abeliano. Provamos o Teorema de Nagell-Lutz sobre os pontos de torção de $E(\mathbb{Q})$. Demonstramos o Teorema de Mordell, que afirma que este grupo é finitamente gerado. Por fim, apresentamos um procedimento para determinar o posto de $E(\mathbb{Q})$ e o aplicamos para determinar o posto numa classes específicas de curvas elípticas.

Palavras Chaves: curvas elípticas, grupo de pontos racionais, pontos de torsão, posto de curvas elípticas.

Abstract

We describe the binary application in the set $E(\mathbb{Q})$ of rational points of an elliptic curve E that makes it an abelian group. We prove the Nagell-Lutz Theorem on the torsion points of $E(\mathbb{Q})$ and the Mordell Theorem, wich states that this group is finitely generated. We also present a procedure to determine the rank of $E(\mathbb{Q})$ and we apply it to a specific class of elliptic curves.

Key Words: elliptic curves, group of rational points, torsion points, rank of an alliptic curve.

Sumário

Capítulo 1

Introdução

A história das curvas elípticas remonta à Grécia antiga e arredores, mais especificamente à área de teoria de números que estuda as equações diofantinas, procurando determinar soluções nos números inteiros ou racionais para equações polinomiais. É natural buscar soluções para equações polinomiais em duas variáveis pelo seu aspecto geométrico, uma vez que estas determinam curvas no plano cartesiano.

Uma curva elíptica E sobre o corpo dos racionais $\mathbb{Q}$ é uma curva não singular de gênero um com um ponto com coordenadas racionais, e seu modelo afim pode ser descrita por uma equação polinomial em duas variáveis da seguinte forma:

$$y^2 = x^3 + ax + b,\ a, b \text{ em } \mathbb{Q} \text{ e o discriminante } \Delta = -4a^3 - 27b^2 \neq 0.$$

Em um clássico teorema de 1922, Louis Mordell provou que é possível construir todos os pontos (x, y) de uma curva elíptica E com coordenadas racionais a partir de um número finito de pontos apenas desenhando retas e tangentes; mais precisamente, que o conjunto dos pontos racionais forma um grupo finitamente gerado. Neste mesmo ano, Mordell ainda conjecturou que curvas de gênero maior que 1 possuem um número finito de pontos racionais. Esta conjectura foi generalizada substituindo o corpo $\mathbb{Q}$ por um corpo de números e provada por

Gerd Faltings, no que atualmente é conhecido como o "Teorema de Faltings"; este teorema o consagrou como ganhador da Medalha Fields em 1986. Nos dias de hoje, temos ainda um importante problema em aberto envolvendo a teoria de curvas elípticas: a Conjectura de Birch e Swinnerton-Dyer, que se encontra na lista do Instituto Clay de Matemática como um dos sete Problemas do Milênio a serem resolvidos.

Seja $E(\mathbb{Q})$ o grupo abeliano dos pontos racionais de uma curva elíptica E. Pelo teorema de Mordell este grupo pode ser decomposto na seguinte soma direta:

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r,$$

onde $E(\mathbb{Q})_{tors}$ é o subgrupo de torsão e r é o posto da curva elíptica, o qual mede o tamanho de um conjunto de geradores. O teorema de Barry Mazur de 1977 nos fornece uma caracterização completa para as possibilidades para o subgrupo de torsão de uma curva elíptica sobre os racionais. Entretanto, ainda hoje não são conhecidos os possíveis valores para o posto r de uma curvas elíptica sobre os racionais. Embora acredite-se que o posto possa ser arbitrariamente grande, o maior valor conhecido é $r = 19$ e foi determinado por Elkies em 2009.

Nesta dissertação estudamos o conjunto de pontos racionais $E(\mathbb{Q})$ de uma curva elíptica E. O segundo capítulo contém um pouco da teoria básica sobre curvas planas, em especial o teorema de Bezout sobre o número de pontos na interseção de duas tais curvas planas. No capítulo 3 definimos uma operação de soma em $E(\mathbb{Q})$, de cunho geométrico, tornando-o um grupo abeliano. Esta operação é consideravelmente simples do ponto de vista computacional, o que gerou o desenvolvimento de sistemas criptográficos envolvendo tais grupos. Curvas elípticas deram ainda origem a um teste de primalidade bastante eficiente, o que está diretamente relacionado ao algoritmo RSA de criptografia. Mais informações sobre este teste de primalidade e a conexão entre curvas elípticas e criptografia podem ser encontradas no livro [3].

A seguir obtemos expressões algébricas para a soma de pontos de uma curva elíptica

$E(\mathbb{Q})$, que são ostensivamente utilizadas no desenvolvimento da teoria, e caracterizamos os pontos de torsão em $E(\mathbb{Q})$, via a prova do teorema de Nagell-Lutz. O capítulo 5 é dedicado à demonstração do teorema de Mordell e, no capítulo seguinte, estudamos uma caracterização do posto de uma curva elíptica apresentada em [1] envolvendo a determinação de soluções de equações diofantinas particulares. Esta caracterização nos permite determinar explicitamente o posto de uma classe de curvas, veja os artigos [4], [9] e [10], a saber, as curvas do tipo

$$y^2 = x^3 - px, \text{ onde } p \text{ é um primo da forma } p = u^4 + v^4 \text{ ou } p = 2^q - 1,\ u, v \in \mathbb{Z}$$

e

$$y^2 = x^3 - 2px, \text{ onde } p \text{ é um primo e } 2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4, u, v \in \mathbb{Z}.$$

Neste capítulo, apresentaremos curvas elípticas de posto igual a zero, um, dois e três.

Capítulo 2

Curvas Planas

Neste capítulo introduzimos as definições de curvas algébricas planas(afim e projetiva) e de multiplicidade de interseção de curvas planas em um ponto. Demonstramos o Teorema de Bezout, que afirma precisamente quantos pontos temos na interseção de duas curvas planas, quando computados de maneira adequada; este teorema é essencial para a teoria de curvas elípticas.

A teoria desenvolvida neste capítulo está contida nos primeiros capítulos do livro [11], [12].

2.1 Curvas Planas e o Plano Projetivo

Neste capítulo, $\mathbb{K}$ denota um corpo e $\overline{\mathbb{K}}$ o seu fecho algébrico.

Definição 1. *Seja $p(x, y)$ um polinômio não constante em $\mathbb{K}[x, y]$. A curva plana afim C_p sobre $\mathbb{K}$ determinada por $p(x, y)$ é o conjunto*

$$C_p = \{(x, y) \in \overline{\mathbb{K}}^2;\ p(x, y) = 0\}.$$

Utilizamos também a notação $C_p : p(x, y) = 0$. *Se* $\mathbb{F}$ *é um corpo contendo* $\mathbb{K}$, *denotamos*

$$C_p(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2;\ p(x, y) = 0\}.$$

Definimos o grau da curva como o grau do polinômio que a define. Curvas de graus 1, 2 *e* 3 *são ditas, respectivamente, retas, cônicas e cúbicas.*

Sejam $y = m_1x + k_1$ e $y = m_2x + k_2$, $m_i, k_i \in \mathbb{R}$ para $i = 1, 2$, duas retas distintas. De modo geral, estas retas se intersectam em um único ponto em $\mathbb{R}^2$. Mas, se $m_1 = m_2$, então as retas são paralelas e esta interseção é vazia no plano afim $\mathbb{R}^2$. Estenderemos então o plano afim adicionando "pontos no infinito", de modo que esta interseção seja não vazia.

Para vermos de que maneira devemos adicionar pontos ao plano afim, considere r e s duas retas concorrentes e r', s' retas paralelas a r e s, respectivamente.

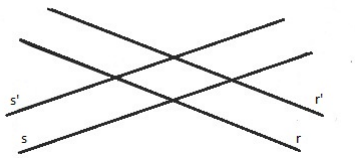

Figura 2.1: Pares de Retas Paralelas

Não podemos adicionar um único ponto no infinito definindo a interseção de qualquer par de retas paralelas, pois teríamos assim que as retas r e r' se intersectariam em dois pontos, como descrito abaixo.

Convém então adicionar um ponto no infinito para cada direção do plano afim ou, equivalentemente, para cada reta contendo a origem. A cada par de números reais (a, b), $ab \neq 0$, corresponde uma reta $ax = by$. Mas, como dois pares (a, b) e (a', b') determinam a mesma reta contendo a origem se e somente se existe um número real t não nulo tal que $ta = a'$ e $tb = b'$, adicionaremos ao plano afim os elementos do conjunto a seguir, ditos os *pontos no infinito*. Eles são definidos via a seguinte relação de equivalência em $\mathbb{R}^2$, e são denotados por

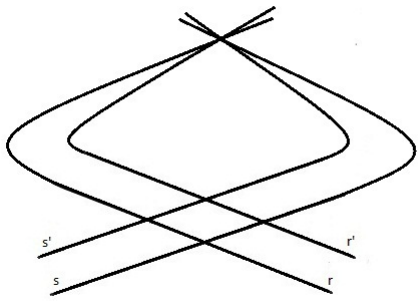

Figura 2.2: Ponto no Infinito

$\mathbb{P}^1(\mathbb{R})$:

$$(x_1, x_2) \sim (y_1, y_2) \Longleftrightarrow \exists\, t \in \mathbb{R} \setminus \{0\} \text{ tal que } tx_j = y_j,\ j = 1, 2,$$

$\mathbb{P}^1(\mathbb{R}) = \dfrac{\{(x_1, x_2) \in \mathbb{R}^2;\ (x_1, x_2) \neq (0, 0)\}}{\sim}$, o conjunto das classes de equivalência da relação $\sim$.

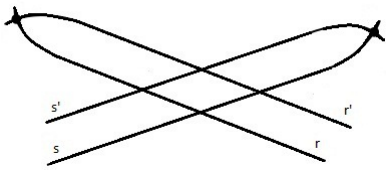

Figura 2.3: Pontos no Infinito

Seja $\mathbb{P}^2(\mathbb{R}) = \{(x_1, x_2, x_3) \in \mathbb{R}^3;\ (x_1, x_2, x_3) \neq (0, 0, 0)\}/\ \sim$, onde $\sim$ é a relação de equivalência em $\mathbb{R}^3$ definida de maneira análoga. Note que existe uma bijeção entre os pontos de $\mathbb{P}^2(\mathbb{R})$ e $\mathbb{R}^2 \cup \mathbb{P}^1(\mathbb{R})$:

$$[x : y : z] \longmapsto \begin{cases} (x/z, y/z), \text{ se } z \neq 0 \\ [x : y], \text{ se } z = 0 \end{cases}$$

Motivados por esta correspondência, definimos o plano projetivo sobre o corpo $\mathbb{K}$ da seguinte maneira.

Definição 2. *Considere seguinte a relação de equivalência entre pontos de* $\mathbb{K}^3$*:*

$$(x_1, x_2, x_3) \sim (y_1, y_2, y_3) \iff \exists\, t \in \mathbb{K} \setminus \{0\} \text{ tal que } tx_j = y_j,\ j = 1, 2, 3.$$

Definimos o Plano Projetivo sobre $\mathbb{K}$ *como o conjunto destas classes de equivalência*

$$\mathbb{P}^2(\mathbb{K}) = \frac{\{(x_1, x_2, x_3) \in \mathbb{K}^3;\ (x_1, x_2, x_3) \neq (0, 0, 0)\}}{\sim}.$$

Se (x_1, x_2, x_3) *é um ponto de* $\mathbb{K}^3$*,* $(x_1, x_2, x_3) \neq (0, 0, 0)$*, sua classe de equivalência é denotada por* $[x_1 : x_2 : x_3]$*.*

Podemos ainda visualizar o plano projetivo como o conjunto de retas de $\mathbb{K}^3$ contendo a origem, e identificar via uma projeção os pontos do plano afim $\mathbb{K}^2$ com a interseção destas retas com um plano qualquer em $\mathbb{K}^3$ que não contenha a origem, por exemplo o plano $z = 1$.

Para definirmos curvas planas projetivas, devemos destacar o fato de que um ponto no plano projetivo é uma classe de equivalência, logo possui vários representantes. Portanto, para a definição de curva plana projetiva ser consistente, devemos trabalhar com uma classe específica de polinômios.

Definição 3. *Um polinômio* $P(X, Y, Z)$ *em* $\mathbb{K}[X, Y, Z]$ *é dito homogêneo de grau* d *se cada um de seus monômios possui grau* d*.*

Proposição 1. *Seja* $F(X, Y, Z)$ *um polinômio em* $\mathbb{K}[X, Y, Z]$ *de grau* $d \geq 1$*. Então* $F(X, Y, Z)$ *é homogêneo se e somente se, para todo* $t \in \mathbb{K} \setminus \{0\}$*,* $F(tX, tY, tZ) = t^d F(X, Y, Z)$*.*

Temos então que, se $F(X, Y, Z)$ é homogêneo e $F(x, y, z) = 0$, então $F(tx, ty, tz) =$ para todo $t \in \mathbb{K} \setminus \{0\}$.

Definição 4. *Seja* $P(X, Y, Z)$ *um polinômio homogêneo não constante em* $\mathbb{K}[X, Y, Z]$*. A curva algébrica plana projetiva* C_P *sobre* $\mathbb{K}$ *determinada por* $P(X, Y, Z)$ *é o conjunto*

$$C_P = \{[x : y : z] \in \mathbb{P}^2(\overline{\mathbb{K}});\ P(x, y, z) = 0\}.$$

Se $\mathbb{F}$ é um corpo contendo $\mathbb{K}$, denotaremos

$$C_P(\mathbb{F}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F});\ P(x, y, z) = 0\}.$$

Definimos o grau da curva algébrica plana C_P como o grau do polinômio $P(X, Y, Z)$ que a define e a denotamos por $C_P : P(X, Y, Z) = 0$. Curvas projetivas de graus $1, 2$ e 3 são ditas, respectivamente, retas, cônicas e cúbicas projetivas.

Seja $C_F : F(X, Y, Z) = 0$ uma curva plana projetiva, $F(X, Y, Z) \in \mathbb{K}[X, Y, Z]$. O plano projetivo pode ser visto como $\mathbb{P}^2(\overline{\mathbb{K}}) = \overline{\mathbb{K}}^2 \cup \mathbb{P}^1(\overline{\mathbb{K}})$, onde identificamos os pontos de $\overline{\mathbb{K}}^2$ com os do conjunto $\{[x_1 : x_2 : x_3] \in \mathbb{P}^2(\overline{\mathbb{K}});\ x_3 = 1\}$. Assim motivados, dizemos que a curva plana afim C_f, definida por $f(x, y) := F(x, y, 1)$, é um modelo afim da curva C_F; este processo é chamado de desomogeneização de C_F. Note que existe uma bijeção entre o conjunto $\{[x_1 : x_2 : x_3] \in C_F;\ x_3 \neq 0\}$ e o modelo afim da curva:

$$\{[x_1 : x_2 : x_3] \in C_F;\ x_3 \neq 0\} \longmapsto C_f = \{(x, y) \in \overline{\mathbb{K}}^2;\ f(x, y) = 0\}$$
$$[x_1 : x_2 : x_3] \longmapsto \left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right).$$

A desomogeinização de curvas projetivas pode ser feita, conforme descrito acima, com respeito a qualquer uma das três variáveis. Assim temos vários modelos afim de uma mesma curva plana projetiva, que podem ser vistos como projeções da curva C_F nos planos $x = 1$, $y = 1$ ou $z = 1$.

Reciprocamente, seja $f(x, y) \in \mathbb{K}[x, y]$ um polinômio de grau d, digamos

$$f(x, y) = \sum_{j,k} a_{j,k} x^j y^k.$$

Definimos a homogeneização de $f(x, y)$ por

$$F(X, Y, Z) = \sum_{j,k} a_{j,k} X^j Y^k Z^{d-(j+k)}.$$

Note que $F(X, Y, Z)$ é um polinômio homogêneo de grau d tal que o modelo afim da curva C_F, obtido a partir da desomogeinização com respeito a variável z, é C_f.

2.2 A Resultante e Interseções entre Curvas

Considere uma reta e uma parábola definidas sobre $\mathbb{R}$. Elas podem não se intersectar em $\mathbb{R}^2$ mas, quando consideramos pontos de interseção no plano complexo $\mathbb{C}^2$, temos, de modo geral, dois pontos nesta interseção. Porém, quando a reta tangencia esta parábola, temos a princípio um único ponto de interseção; mas é razoável computar este ponto como um ponto "duplo"de interseção, uma vez que pontos distintos de interseção convergem para um ponto único de tangência, conforme descrito nas figuras abaixo.

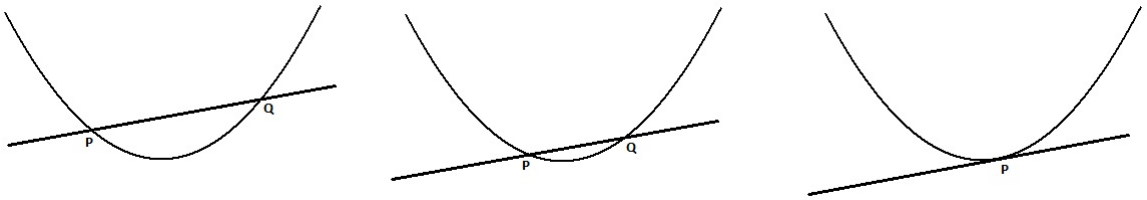

Figura 2.4: Retas Secantes e Tangente a uma Parábola

Isto nos leva à intuição de que a interseção entre curvas de graus m e n contém mn pontos. O Teorema de Bezout afirma que este raciocínio está correto, quando computamos corretamente os pontos de interseção entre curvas planas projetivas, isto é, quando buscamos os pontos no plano projetivo sobre o fecho algébrico do corpo de definição das curvas e levamos em conta como as curvas se intersectam nestes pontos. Estas curvas devem satisfazer uma outra hipótese, derivada da definição abaixo.

Um polinômio homogêneo $F(X,Y,Z) \in \mathbb{K}[X,Y,Z]$ pode ser fatorado como $F = F_1F_2$, $F_1, F_2 \in \mathbb{K}[X,Y,Z]$, se e somente se cada polinômio F_j, $j = 1,2$, é homogêneo. Logo, cada polinômio $F_j(X,Y,Z)$ define uma curva plana projetiva $C_{F_j} : F_j(X,Y,Z) = 0$.

Definição 5. *Seja $C_F : F(X,Y,Z) = 0$ uma curva plana projetiva e $F = F_1F_2...F_n$ a fatoração de F sobre $\mathbb{K}$ em polinômios irredutíveis. Cada curva $C_{F_j} : F_j(X,Y,Z) = 0$, $j = 1,...,n$, é dita uma componente irredutível de C_F.*

Mostraremos primeiramente que a interseção entre duas curvas planas afins é finita se os polinômios que as definem não possuem componente comum não constante. Utilizaremos o seguinte lema na demonstração.

Lema 1 (Lema de Gauss)**.** *Sejam D um domínio de fatoração única, $\mathbb{D}$ seu corpo de frações e $f(x) = a_n x^n + ... + a_1 x + a_0$ um polinômio em $D[x]$ tal que*

$$\exists\, t \in D \text{ tal que } t \mid a_j,\ \forall\, 0 \leq j \leq n \iff t \text{ é unidade em } D.$$

Então $f(x)$ é redutível em $D[x]$ se, e somente se, $f(x)$ é redutível em $\mathbb{D}[x]$.

Demonstração. A demonstração deste lema pode ser encontrada na página 54 do livro [2]. □

Proposição 2. *Sejam $f(x, y)$ e $g(x, y)$ polinômios sem componentes comuns em $\mathbb{K}[x, y]$. Então a interseção entre as curvas planas afins $C_f : f(x, y) = 0$ e $C_g : g(x, y) = 0$ é finita.*

Demonstração. Temos que $f(x, y)$ e $g(x, y)$ podem ser vistos como polinômios em $\mathbb{K}(x)[y]$, onde $\mathbb{K}(x)$ é o corpo frações de $\mathbb{K}[x]$. Pelo Lema de Gauss, temos que f e g também serão relativamente primos em $\mathbb{K}(x)[y]$, logo existem $r(x)$, $s(x) \in \mathbb{K}(x)$ tais que

$$r(x)f(x, y) + s(x)g(x, y) = 1,$$

e, escrevendo $r(x) = \dfrac{r_1(x)}{r_2(x)}$, $s(x) = \dfrac{s_1(x)}{s_2(x)}$ onde $r_1, r_2, s_1, s_2 \in \mathbb{K}[x]$, obtemos

$$\frac{r_1(x)}{r_2(x)}f(x, y) + \frac{s_1(x)}{s_2(x)}g(x, y) = 1 \iff r_1(x)s_2(x)f(x, y) + r_2(x)s_1(x)g(x, y) = r_2(x)s_2(x).$$

Vemos então que existe um número finito de valores para x_0 tais que $f(x_0, y) = g(x_0, y) = 0$, limitado pelo número de raízes de $r_2(x)s_2(x) = 0$. Para cada x_0 fixado existe um número finito de valores para y_0 tais que $f(x_0, y_0) = 0$, como gostaríamos. □

Este resultado pode ser estendido para curvas planas projetivas. Se $F(X, Y, Z)$ e $G(X, Y, Z)$ são polinômios homogêneos em $\mathbb{K}[X, Y, Z]$, a interseção entre as curvas planas projetivas

definidas por estes polinômios pode ser escrita como

$$\{[x:y:1] \in \mathbb{P}^2(\overline{\mathbb{K}}); F(x,y,1) = G(x,y,1) = 0\} \cup \{[x:y:0] \in \mathbb{P}^2(\overline{\mathbb{K}}); F(x,y,0) = G(x,y,0) = 0\}.$$

Teremos que estes dois conjuntos serão finitos se $F(X,Y,z)$ e $G(X,Y,z)$, vistos como polinômios em $\overline{\mathbb{K}}[X,Y]$, não possuírem fator comum para todo $z \in \overline{\mathbb{K}}$. Para demonstrar este fato, introduziremos o conceito de resultante.

Definição 6. *Sejam D um domínio de fatoração única e $f(y) = a_m y^m + \cdots + a_1 y + a_0$, $g(y) = b_n y^n + \cdots + b_1 y + b_0$ polinômios em $D[y]$ tais que a_m e b_n são não nulos. Definimos a resultante de f e g como o determinante*

$$R_{f,g} = \begin{vmatrix} a_m & a_{m-1} & \dots & a_0 & & & & \\ & a_m & a_{m-1} & \dots & a_0 & & & \\ & & & \ddots & & \ddots & & \\ & & & & a_m & a_{m-1} & \dots & a_0 \\ b_n & b_{n-1} & \dots & b_0 & & & & \\ & b_n & b_{n-1} & \dots & b_0 & & & \\ & & & \ddots & & \ddots & & \\ & & & & b_n & b_{n-1} & \dots & b_0 \end{vmatrix}$$

onde os coeficientes de $f(x)$ se repetem por n linhas e os de $g(x)$ por m linhas, formando uma matriz quadrada $(m+n) \times (m+n)$.

A proposição abaixo conclui o argumento acima.

Proposição 3. *Sejam $f(y) = a_d(x)y^d + \cdots + a_1(x)y + a_0(x)$ e $g(y) = b_e(x)y^e + \cdots + b_1(x)y + b_0(x)$ polinômios em $\mathbb{K}[x][y]$ tais que $a_d(x)$ e $b_e(x)$ são não nulos. Então, $R_{f,g}(x_0) = 0$ se e somente se $f(x_0, y)$ e $g(x_0, y)$ possuem raiz comum em $\overline{\mathbb{K}}$.*

Mais ainda, $R_{f,g}(x)$ é identicamente nula se e somente se f e g possuem fator comum não constante.

Demonstração. Ver [11], páginas 23 e 24. □

Proposição 4. *Sejam F e G polinômios homogêneos em $\mathbb{K}[X,Y,Z]$ sem componentes comuns. Sejam m e n os graus de F e G, respectivamente. Escrevendo*

$$F(X,Y,Z) = A_0Y^m + \cdots + A_m$$

$$G(X,Y,Z) = B_0Y^n + \cdots + B_n,$$

onde A_j, B_j são polinômios homogêneos de grau j em $\mathbb{K}[X,Z]$, a resultante $R = R_{F,G}(X,Z)$ é um polinômio homogêneo de grau mn.

Demonstração. Seja $t \neq 0$. Então,

$$R(tX,tZ) = \begin{vmatrix} A_0 & tA_1 & \dots & t^mA_m & & & & \\ & A_0 & tA_1 & \dots & t^mA_m & & & \\ & & & \ddots & & \ddots & & \\ & & & & A_0 & tA_1 & \dots & t^mA_m \\ B_0 & tB_1 & \dots & t^nB_n & & & & \\ & B_0 & tB_1 & \dots & t^nB_n & & & \\ & & & \ddots & & \ddots & & \\ & & & & B_0 & tB_1 & \dots & t^nB_n \end{vmatrix}$$

Multiplicando, na matriz que define o determinante acima, a j-ésima linha de A_i's por t^{j-1},

$j = 2, ..., n$, e a k-ésima linha de B_i's por t^{k-1}, $k = 2, ..., m$, teremos a matriz

$$\begin{pmatrix} A_0 & tA_1 & \dots & t^m A_m & & & & \\ & tA_0 & t^2A_1 & \dots & t^{m+1}A_m & & & \\ & & & \ddots & & \ddots & & \\ & & & & t^{n-1}A_0 & t^nA_1 & \dots & t^{m+n-1}A_m \\ B_0 & tB_1 & \dots & t^n B_n & & & & \\ & tB_0 & t^2B_1 & \dots & t^{n+1}B_n & & & \\ & & & \ddots & & \ddots & & \\ & & & & t^{m-1}B_0 & t^mB_1 & \dots & t^{n+m-1}B_n \end{pmatrix},$$

cujo determinante, por construção, é igual a $t^N R(tX, tZ)$, onde

$$N = (1 + \cdots + n - 1) + (1 + \cdots + m - 1).$$

Por outro lado, multiplicando a j-ésima coluna da matriz que define $R(X, Z)$ por t^{j-1}, $j = 2, \dots, (m + n)$, obtemos a matriz acima; portanto, se $M = 1 + \cdots + (m + n - 1)$,

$$t^N R(tX, tZ) = t^M R(X, Z) \Longleftrightarrow R(tX, tZ) = t^{(M-N)} R(X, Z),$$

onde $M - N = mn$. □

2.3 O Teorema de Bezout

Sejam $C_F : F(X, Y, Z) = 0$ e $C_G : G(X, Y, Z) = 0$ duas curvas planas projetivas sem componentes comuns. Para computar o número de pontos na interseção entre estas curvas, é preciso levar em conta de que maneira elas se intersectam em um dado ponto. Vamos agora definir a multiplicidade de interseção de C_F e C_G em um ponto fixado.

Definição 7. *Sejam $P_j = [x_j : y_j : z_j]$, $j \geq 1$, os pontos distintos da interseção entre C_F e C_G, que a princípio pode ser vazia, e $P_0 = [0 : 1 : 0]$. Diremos que C_F e C_G estão em boa*

posição(ou bem posicionadas) se P_0, P_i e P_j não são colineares para cada $P_i \neq P_j \in C_F \cap C_G$. Em particular, se C_F e C_G estão bem posicionadas então $P_0 \notin C_F \cap C_G$.

Note que, se C_F e C_G estão bem posicionadas, então $[x_i : z_i] \neq [x_j : z_j]$ sempre que $i \neq j$. De fato, uma reta projetiva sobre $\overline{\mathbb{K}}$ que contém P_0 é da forma $L(\overline{\mathbb{K}}) : \alpha X + \gamma Z = 0$. Se $P_i = [x_i : y_i : z_i]$ pertence a $L = L(\overline{\mathbb{K}})$, então $\alpha = -z_i$ e $\gamma = x_i$. Segue então que $P_j = [x_j : y_j : z_j]$ pertence a L se, e somente se $z_i x_j = x_i z_j$. Se $x_i = 0$, então devemos ter $z_i = 0$ pois $[x_i : z_i] \neq [x_j : z_j]$, donde $P_i = P_0$, um abusrdo. Logo x_1, z_1, x_2, z_2, são não nulos e assim

$$\frac{x_i}{x_j} = \frac{z_i}{z_j},$$

isto é, existe $t \neq 0$ tal que $x_j = t x_i$ e $z_j = t z_i$.

Escreva $F(X, Y, Z) = A_0 Y^m + \cdots + A_m$, $G(X, Y, Z) = B_0 Y^n + \cdots + B_n$, como na Proposição 4 e suponha C_F e C_G bem posicionadas. Temos que $P_0 \in C_F$ se e somente se $A_0 = 0$, logo não podemos ter simultaneamente A_0 e B_0 nulos; segue da Proposição 4 que a resultante $R(X, Z) = R_{F,G}(X, Z)$ é um polinômio homogêneo de grau mn. Mais ainda, como $A_0 = B_0 = 0$ não é possível, temos pela Proposição 3 que, para todo $[x : z] \in \mathbb{P}^1(\overline{\mathbb{K}})$,

$$R(x, z) = 0 \iff \exists\, y \in \overline{\mathbb{K}} \text{ tal que } [x : y : z] \in C_F \cap C_G.$$

Em particular, a interseção entre C_F e C_G é não vazia. Logo, se $P_i = [x_i : y_i : z_i]$, $i = 1, ..., r$, são os pontos distintos da interseção entre C_F e C_G, então $R(X, Z)$ pode ser fatorada como

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

onde $c \in \overline{\mathbb{K}}$ é não nulo e $\sum_{i=1}^{r} m_i = mn$.

Definição 8. *De acordo com a notação acima, a multiplicidade de interseção de C_F e C_G em um ponto $P \in \mathbb{P}^2(\overline{\mathbb{K}})$ é dada por*

$$(C_F, C_G)_P = \begin{cases} 0, \text{ se } P \notin C_F \cap C_G \\ m_i, \text{ se } P = P_i \in C_F \cap C_G. \end{cases}$$

Então, definindo multiplicidade de interseção de duas curvas em um ponto apropriadamente, temos demonstrado o seguinte resultado, versão preliminar do Teorema de Bezout.

Proposição 5. *Sejam $C_F : F(X,Y,Z) = 0$ e $C_G : G(X,Y,Z) = 0$ duas curvas planas projetivas sem componentes comuns de graus m e n respectivamente. Então, se elas estão em boa posição,*

$$\sum_{P \in C_F \cap C_G} (C_F, C_G)_P = mn.$$

Agora precisamos definir multiplicidade de interseção para curvas que não estejam em boa posição. Para isso,vamos trabalhar com o conceito de mudanças de coordenadas projetivas. Seja

$$T' : \overline{\mathbb{K}}^3 \longrightarrow \overline{\mathbb{K}}^3$$

$$(x,y,z) \longmapsto T'(x,y,z) = (x',y',z')$$

um isomorfismo linear entre espaços vetoriais. Tal aplicação induz uma bijeção

$$T : \mathbb{P}^2(\overline{\mathbb{K}}) \longrightarrow \mathbb{P}^2(\overline{\mathbb{K}}),$$

$$[x:y:z] \longmapsto [x':y':z']$$

bem definida pois T' preserva retas contendo a origem, que chamamos de mudança de coordenadas projetivas. Se $C_F : F(X,Y,Z) = 0$ é uma curva plana projetiva, definimos

$$T \circ C_F = \{[x:y:z] \in P^2(\overline{\mathbb{K}});\ T^{-1}([x:y:z]) \in C_F\},$$

isto é, $T \circ C_F$ é composta pelos pontos de $\mathbb{P}^2(\overline{\mathbb{K}})$ que satisfazem a equação $F(T^{-1}(X,Y,Z)) = 0$.

Lema 2. *Sejam $C_F : F(X,Y,Z) = 0$ e $C_G : G(X,Y,Z) = 0$ duas curvas planas projetivas sem componentes comuns. Então existe uma mudança de coordenadas projetivas tal que C_F e C_G estão em boa posição.*

Demonstração. Suponha que C_F e C_G não estão em boa posição e sejam $P_j = [x_j : y_j : z_j]$, $j = 1, \ldots, r$, os pontos distintos na interseção. O conjunto de retas determinadas pelos pares (Q_i, Q_j), Q_i, Q_j pontos de $(C_F \cap C_G) \cup \{P_0\}$, é finito. Segue então que, fixando P um ponto não pertencente à união destas retas e T uma mudança de coordenadas tal que $T(P) = [0 : 1 : 0]$, as novas curvas $T \circ C_F$ e $T \circ C_G$ estarão em boa posição. De fato, se $[0 : 1 : 0]$, Q_1 e Q_2 são pontos colineares em $T(C_F) \cap T(C_G)$, então P, $T^{-1}(Q_1)$ e $T^{-1}(Q_2)$ são pontos colineares e $T^{-1}(Q_1)$ e $T^{-1}(Q_2)$ pertencem à interseção $C_F \cap C_G$, um absurdo. □

Definição 9. *Sejam $C_F : F(X, Y, Z) = 0$ e $C_G : G(X, Y, Z) = 0$ duas curvas planas projetivas sem componentes comuns e T uma mudança de coordenadas projetiva tal que $T \circ C_F$ e $T \circ C_G$ estão em boa posição. Definimos a multiplicidade de interseção de C_F e C_G por*

$$(C_F, C_G)_P = (T \circ C_F, T \circ C_F)_{T(P)}.$$

O resultado abaixo mostra que a definição acima não depende da mudança de coordenadas escolhida.

Proposição 6. *Sejam $C_F : F(X, Y, Z) = 0$ e $C_G : G(X, Y, Z) = 0$ duas curvas planas projetivas sem componentes comuns, $F, G \in \mathbb{K}[X, Y, Z]$. Suponha que C_F e C_G estão bem posicionadas e T é uma mudança de coordenadas projetiva tal que $T \circ C_F$ e $T \circ C_G$ também estão em boa posição. Então*

$$(C_F, C_G)_P = (T \circ C_F, T \circ C_F)_{T(P)}.$$

Demonstração. Seja W uma mudança de coordenadas projetiva genérica definida por nove indeterminadas(elementos transcedentes sobre o corpo $\mathbb{K}$) $w_{i,j}$, $i, j = 1, 2, 3$. Sejam $\overline{\mathbb{K}}(w_{i,j})$ o corpo de frações do anel de polinômios $\overline{\mathbb{K}}[w_{i,j}]$ e $\mathbb{L}$ o seu fecho algébrico.

Temos que $\mathbb{P}^2(\overline{\mathbb{K}})$ está contido em $\mathbb{P}^2(\mathbb{L})$, mas $C_F(\mathbb{L}) \cap C_G(\mathbb{L}) = C_F(\overline{\mathbb{K}}) \cap C_G(\overline{\mathbb{K}})$. De fato, os pontos na interseção entre $C_F(\mathbb{L})$ e $C_G(\mathbb{L})$ são, como vimos na seção anterior, as raízes de

um polinômio com coeficientes em $\overline{\mathbb{K}}$; como $\overline{\mathbb{K}}$ é algebricamente fechado, as coordenadas das raízes deste polinômio estão contidas em $\overline{\mathbb{K}}$. Mais ainda, um ponto P pertence à interseção entre $C_F(\mathbb{L})$ e $C_G(\mathbb{L})$ se e somente se $W(P) \in (W \circ C_F(\mathbb{L})) \cap (W \circ C_G(\mathbb{L}))$, por definição destas curvas.

Note que $W^{-1}(X, Y, Z)$ possui coeficientes que são frações cujos denominadores são polinômios nas variáveis $w_{i,j}$, $j = 1, 2, 3$, então existe $c_W \in \overline{\mathbb{K}}[w_{i,j}]$ tal que $\overline{F}(X, Y, Z) = c_W F(W^{-1}(X, Y, Z))$ é um polinômio em $\mathbb{L}[X, Y, Z]$. Além disso, como $c_W \in \mathbb{L}$, $F(W^{-1}(X, Y, Z))$ e $\overline{F}(X, Y, Z)$ definem as mesmas curvas sobre $\mathbb{P}^2(\mathbb{L})$.

As curvas $C_{\overline{F}}(\mathbb{L})$ e $C_{\overline{G}}(\mathbb{L})$ estão bem posicionadas, pois se $P_0 = [0 : 1 : 0]$ pertence à interseção $C_{\overline{F}}(\mathbb{L}) \cap C_{\overline{G}}(\mathbb{L})$, então existe $P \in C_F(\overline{\mathbb{K}}) \cap C_G(\overline{\mathbb{K}})$ tal que $W(P) = P_0$, isto é,

$$\begin{pmatrix} w_{1,1} & w_{1,2} & w_{1,3} \\ w_{2,1} & w_{2,2} & w_{2,3} \\ w_{3,1} & w_{3,2} & w_{3,3} \end{pmatrix} \begin{pmatrix} x(P) \\ y(P) \\ z(P) \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

contrariando a condição de elementos transcendentes sobre $\mathbb{K}$ de $w_{i,j}$, $j = 1, 2, 3$. Calculando a resultante entre $\overline{F}$ e $\overline{G}$, temos que

$$R_{\overline{F},\overline{G}}(X, Z) = \overline{c} \prod_{i=1}^{\overline{r}} (\overline{z_i} X - \overline{x_i} Z)^{\overline{m_i}},$$

onde, para cada $i = 1, \ldots, r$, existe $[\overline{x_i} : \overline{y_i} : \overline{z_i}] \in C_{\overline{F}}(\overline{\mathbb{K}}) \cap C_{\overline{G}}(\overline{\mathbb{K}})$. Mas um ponto $[\overline{x_i} : \overline{y_i} : \overline{z_i}]$ pertence a esta interseção se e somente se $[\overline{x_i} : \overline{y_i} : \overline{z_i}] = W([x_i : y_i : z_i])$ para algum ponto $[x_i : y_i : z_i] \in C_F(\overline{\mathbb{K}}) \cap C_G(\overline{\mathbb{K}})$; portanto, escrevendo

$$R_{F,G}(X, Z) = c \prod_{i=1}^{r} (z_i X - x_i Z)^{m_i},$$

temos que $r_i = \overline{r_i}$ e $m_i = \overline{m_i}$ para $i = 1, \ldots, r$.

Finalmente, se T é uma mudança de coordenadas projetiva definida por $t_{i,j}$, $i, j = 1, 2, 3$, fazendo $w_{i,j} = t_{i,j}$ para $i, j = 1, 2, 3$, temos que

$$(C_F, C_G)_P = (T \circ C_F, T \circ C_F)_{T(P)},$$

como gostaríamos. □

Podemos ainda visualizar a definição de multiplicidade de interseção de curvas em um ponto de outra maneira, através do resultado a seguir que pode ser encontrado no livro [6].

Proposição 7. *Sejam P_0 um ponto qualquer do plano afim $\mathbb{K}^2$ e*

$$\mathcal{F}(\mathbb{K}) = \{(C_f, C_g);\ f, g \in \mathbb{K}[x, y] \text{ e } C_f, C_g \text{ não têm componente comum contendo } P_0\}.$$

Existe uma única aplicação $(C_f, C_g) \in \mathcal{F}(\mathbb{K}) \longmapsto (C_f, C_g)_{P_0} \in \mathbb{N}$ satisfazendo as seguintes propriedades.

1. $(C_f, C_g)_{P_0} = 1$, *se* $f(x, y) = x$ *e* $g(x, y) = y$;
2. $(C_f, C_g)_{P_0} = (C_g, C_f)_{P_0}$, $\forall\ (C_f, C_g) \in \mathcal{F}(\mathbb{K})$;
3. $(C_f, C_{gh})_{P_0} = (C_f, C_g)_{P_0} + (C_f, C_h)_{P_0}$, $\forall\ (C_f, C_g), (C_f, C_h) \in \mathcal{F}(\mathbb{K})$;
4. $(C_f, C_{g+fh})_{P_0} = (C_f, C_g)_{P_0}$, $\forall\ (C_f, C_g), (C_f, C_h) \in \mathcal{F}(\mathbb{K})$;
5. $(C_f, C_g)_{P_0} = 0$, *se* $P_0 \notin C_g$ *e* $(C_f, C_g) \in \mathcal{F}(\mathbb{K})$.

Demonstração. A demonstração deste resultado pode ser encontrada no livro [6]. □

Se $C_F : F(X, Y, Z) = 0$ e $C_G : G(X, Y, Z) = 0$ são curvas planas projetivas e $P = [x : y : z]$ é um ponto qualquer de $\mathbb{P}^2(\mathbb{K})$, podemos desomogeneizar as curvas, por exemplo em relação a variável Z, e obter curvas planas afins $C_f : f(x, y) = 0$, $C_g : g(x, y) = 0$ e o ponto $P_0 = (a, b)$ correspondente a $P = [a : b : 1]$. Temos então que a multiplicidade de interseção entre C_F e C_G no ponto P coincide com $(C_f, C_g)_{P_0}$. Isto fornece uma definição equivalente de multiplicidade de interseção.

Note que esta Proposição fornece um algoritmo para o cálculo da multiplicidade de interseção entre curvas em um ponto, conforme descrito no exemplo abaixo.

Exemplo 1: Considere $f(x,y) = x$ e $g(x,y) = y^2 - x^3 + x$. A multiplicidade de interseção entre estas curvas no ponto $P = (0,0)$ é dada por:

$$(C_f, C_g)_P = (x, y^2 - x^3 + x)_P = (x, y^2 - x(x^2-1))_P = (x, y^2)_P = (x,y)_P + (x,y)_P = 1+1 = 2,$$

onde, por simplicidade, $(f(x,y), g(x,y))_P = (C_f, C_g)_P$. De fato, as curvas planas $y^2 = x^3 - x$ e $x = 0$ se tangenciam no ponto $P = (0,0)$.

Podemos agora enunciar e demonstrar o Teorema de Bezout.

Teorema 1. *Sejam $C_F : F(X,Y,Z) = 0$ e $C_G : G(X,Y,Z) = 0$ duas curvas planas projetivas sem componentes comuns de graus m e n respectivamente. Então,*

$$\sum_{P \in C_F \cap C_G} (C_F, C_G)_P = mn.$$

Demonstração. Se C_F e C_G estão em boa posição, o resultado segue diretamente da Proposição 5. Se estas curvas não estão em boa posição, existe uma mudança de coordenadas projetiva T tal que $T \circ C_F$ e $T \circ C_G$ estão em boa posição e então, novamente pela Proposição 5, segue o resultado. □

Corolário 1. *Se duas curvas de graus m e n se intersectam em mais de mn pontos, então elas possuem uma componente em comum.*

O Teorema a seguir, cuja demonstração é encontrada em [12], é essencial para a teoria de curvas elípticas.

Teorema 2. *Sejam C_{F_1} e C_{F_2} duas cúbicas sem componentes comuns. Sejam ainda $P_1, ..., P_9$ os pontos distintos na interseção $C_{F_1} \cap C_{F_2}$. Se C_F é uma terceira cúbica que contém $P_1, ..., P_8$, então $P_9 \in C_F$.*

Demonstração. Se existirem $\lambda, \mu \in \overline{\mathbb{K}}$ tais que $F = \lambda F_1 + \mu F_2$, então é claro que C_F contém P_9. Suponha que isto não ocorra, isto é, que não exista solução (λ, μ, ν) não trivial em $\overline{\mathbb{K}}^3$

para $\lambda F_1 + \mu F_2 + \nu F = 0$. Então, para cada par de pontos A, B fixados, podemos escolher $(\lambda, \mu, \nu) \in \overline{\mathbb{K}}^3$ de modo que a curva $C_{\overline{F}}$, definida por $\overline{F} = \lambda F_1 + \mu F_2 + \nu F$, contenha A e B.

Note que não podemos ter quatro pontos colineares dentre $P_1, ..., P_9$, pois seguiria do Corolário 1 que esta reta seria componente comum entre C_{F_1} e C_{F_2}. Analogamente, não podemos ter sete destes nove pontos contidos em uma única cônica.

Dividiremos a demonstração em três casos possíveis, de acordo com a disposição dos pontos $P_1, ..., P_9$.

Caso 1: Suponha P_1, P_2 e P_3 contidos em uma reta C_L. Devemos ter $P_4, ..., P_8$ contidos em uma única cônica C_Q. De fato, se duas cônicas C_{Q_1} e C_{Q_2} possuem cinco pontos distintos de interseção, então elas possuem uma componente comum; como estamos supondo que estas cônicas são distintas, segue que esta componente deve ser uma reta $C_{\widetilde{L}}$. Como as outras componentes de C_{Q_1} e C_{Q_2} são retas distintas, elas se intersectam em apenas um ponto e então temos quatros pontos dentre os nove pontos iniciais contidos em $C_{\widetilde{L}}$, impossível.

Sejam A um ponto de C_L distinto de P_1, P_2, P_3 e B um ponto qualquer fora de C_Q e C_L. Escolhendo (λ, μ, ν) de modo que $C_{\overline{F}}$ contenha os pontos A e B, temos que C_L é componente de $C_{\overline{F}}$, pois $(C_L \cap C_{\overline{F}}) \supseteq \{A, P_1, P_2, P_3\}$. Segue do argumento acima que C_L e C_Q são as componentes de $C_{\overline{F}}$, pois $P_4, \ldots, P_8$ não pertencem a C_L. Mas isto é impossível pela escolha de A e B.

Caso 2: Suponha que $P_1, ..., P_6$ estão contidos em uma cônica C_Q. Sejam C_L a reta passando por P_7 e P_8, A um ponto de C_Q distinto de $P_1, ..., P_6$ e B um ponto qualquer fora de C_Q e C_L. Escolhendo (λ, μ, ν) de modo que $C_{\overline{F}}$ contenha A e B, teremos que C_Q é componente de $C_{\overline{F}}$, pois contém sete pontos na interseção com C_Q: $A, P_1, ..., P_6$.

Seja $C_{\widetilde{L}}$ a outra componente de $C_{\overline{F}}$. Não podemos ter P_7 ou P_8 pertencentes a C_Q, pois assim C_Q seria componente comum de C_{F_1} e C_{F_2}. Como C_L e $C_{\widetilde{L}}$ têm dois pontos em comum, temos que $C_L = C_{\widetilde{L}}$, mas isto é impossível pela escolha de B.

Caso 3: Suponha que não temos três pontos colineares dentre $P_1, ..., P_9$ e que nenhuma cônica contém seis destes pontos. Sejam C_L a reta contendo P_1, P_2 e C_Q uma cônica contendo $P_3, ..., P_7$. Sejam ainda A, B pontos quaisquer de C_L distintos de P_1 e P_2 e escolha (λ, μ, ν) de modo que $C_{\overline{F}}$ contenha A e B.

Como A, B, P_1 e P_2 pertencem a C_L e $C_{\overline{F}}$, segue que C_L é componente desta cúbica. Escrevendo $\overline{F} = L.\widetilde{Q}$, temos que $P_3, ..., P_7$ devem pertencer a $C_{\widetilde{Q}}$ por hipótese. Como C_Q e $C_{\widetilde{Q}}$ possuem cinco pontos distintos em sua interseção, temos que $C_Q = C_{\widetilde{Q}}$ e assim $\overline{F} = L.Q$. Mas isto é um absurdo pois $P_8 \in C_{\overline{F}}$ mas P_8 não pertence a C_Q ou C_L. □

Capítulo 3

Curvas elípticas

3.1 Definição

Nesta seção, $\mathbb{F}$ e $\mathbb{K}$ denotam corpos de característica diferente de 2 e 3.

Definição 10. *Uma curva elíptica E sobre um corpo $\mathbb{K}$ é uma curva projetiva definida por uma equação do tipo*

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{3.1}$$

onde $a, b \in \mathbb{K}$ e o discriminante $\Delta = -4a^3 - 27b^2$ de E é não nulo.

É fácil ver que o discriminante Δ é não nulo se, e somente se a curva é não singular. Note também que esta curva projetiva possui apenas um ponto no infinito $\mathcal{O} = [0 : 1 : 0]$. Desse modo trabalharemos com o modelo afim da curva elíptica

$$E : y^2 = x^3 + ax + b \tag{3.2}$$

sabendo que a curva projetiva consiste de todos os pontos finitos e um ponto no infinito.

Cabe ressaltar que, se E é uma curva elíptica sobre $\mathbb{Q}$, a menos de uma transformação

do tipo $(x, y) \longmapsto (c^2x, c^3y)$, $c \in \mathbb{Z}$, o modelo afim da curva E sempre pode ser escrito na forma $y^2 = x^3 + ax + b$, onde a e b são inteiros.

Uma definição alternativa de curva elíptica que tambem usaremos é: cúbica não singular sobre $\mathbb{K}$ com um ponto racional. De fato, toda cúbica não singular é isomorfa a uma cúbica definida por uma equação do tipo $y^2 = x^3 + ax + b$, conforme está descrito no livro [8].

Proposição 8. *Toda cúbica não singular é isomorfa a uma cúbica do tipo* $y^2 = x^3 + ax + b$.

Demonstração. Seja

$$C : AX^3 + BY^3 + CZ^3 + DX^2Y + EX^2Z + FXY^2 + GY^2Z + HXZ^2 + IYZ^2 + JXYZ = 0$$

uma cúbica não singular com um ponto racional. Escolheremos um sistema de coordenadas tais que, nas novas coordenadas, a equação da curva seja como em (3.1). Escolhemos $\mathcal{O} = [1 : 0 : 0]$ como as novas coordenadas do ponto racional e a reta $Z = 0$ de modo que esta seja tangente à cúbica em $\mathcal{O}$; como a interseção entre C e a reta $Z = 0$ é descrita pela equação

$$AX^3 + BY^3 + DX^2Y + FXY^2 = 0, \tag{3.3}$$

devemos ter $A = D = 0$. Vamos supor que $F \neq 0$, isto é, que $\mathcal{O}$ não é ponto de inflexão da curva. Logo a reta $Z = 0$ intersecta a cúbica em um ponto diferente de $\mathcal{O}$, cujas coordenadas escolhemos ser $[0 : 1 : 0]$. Portanto, da equação (3.3), vemos que $B = 0$. Escolhemos a reta $X = 0$ como a reta tangente à cúbica em $[0 : 1 : 0]$; como a interseção entre esta reta e a cúbica é descrita por

$$CZ^3 + GY^2Z + IYZ^2 = 0,$$

devemos ter que $G = 0$. Escolhendo a reta $Y = 0$ como qualquer reta distinta de $Z = 0$ contendo o ponto $\mathcal{O}$, obtemos nas novas coordenadas uma cúbica projetiva

$$C : C'Z^3 + E'X^2Z + XY^2 + H'XZ^2 + I'YZ^2 + J'XYZ = 0. \tag{3.4}$$

Desomogeneizando em relação a variável Z, obtemos a equação

$$xy^2 + J'xy + I'y = -E'x^2 - H'x - C' \Longleftrightarrow (xy)^2 + xy(J'x + I) = -E'x^3 - H'x^2 - C'x.$$

Fazendo a mudança de coordenadas $s = xy$, $t = x$, temos

$$s^2 + s(J't + I') = -E't^3 - H't^2 - C't.$$

Fazendo agora $x = t$, $y = s + \dfrac{J't + I'}{2}$,

$$y^2 = \overline{a}x^3 + \overline{b}x^2 + \overline{c}x + \overline{d},$$

onde $\overline{a}, \overline{b}, \overline{c}$ e $\overline{d}$ dependem de C', E', H', I' e J'. Ao fazer a mudança $x = \overline{a}t$, $y = \overline{a}^2 s$, obtemos um polinômio mônico de grau 3 à direita da equação:

$$s^2 = t^3 + \alpha t^2 + \beta t + \gamma.$$

A mudança $t = x - \alpha/3$, $y = s$ nos dá uma equação que descreve o modelo afim de uma cúbica projetiva cuja equação é como em (3.1). Como todas as mudanças de coordenadas na demonstração são birracionais, a proposição está provada.

Se o ponto racional inicial é ponto de inflexão da curva, então teremos que A, D e F são nulos. Escolhendo a reta $y = 0$ como aquela tangente à cúbica no ponto $[0 : 0 : 1]$ e reta $X = 0$ como uma reta qualquer contendo $[0 : 0 : 1]$, obtemos uma cubica projetiva cuja equação é análoga àquela em (3.4). Demonstramos então o resultado fazendo mudanças de coordenadas análogas. □

Na figura a seguir, temos o modelo afim do conjunto de pontos reais de curvas elípticas definidas sobre os racionais, obtido a partir da desomogeinização em relação a variável Z.

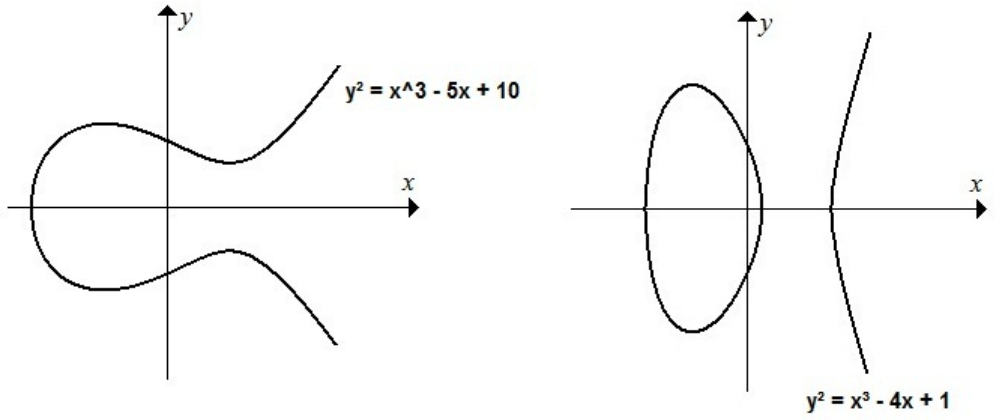

Figura 3.1: Modelo Afim de Curvas Elípticas

3.2 A Estrutura de Grupo

Seja $E : Y^2 = X^3 + aXZ^2 + bZ^3$ uma curva elíptica definida sobre um corpo $\mathbb{K}$ e seja $\mathbb{F} \supseteq \mathbb{K}$ uma extensão de $\mathbb{K}$, $E(\mathbb{F})$ denotará

$$E(\mathbb{F}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{F}); y^2 = x^3 + axz^2 + bz^3\} = \{(x, y) \in \mathbb{F}^2;\ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Mostraremos que este conjunto é um grupo comutativo munido da seguinte operação: dados dois pontos P, Q em $E(\mathbb{F})$, denotaremos por $P * Q$ o terceiro ponto na interseção da reta passando por P e Q e a curva E, que está bem definido pelo Teorema de Bezout. Se $P = Q$, consideramos a reta tangente à curva neste ponto. Definimos a soma entre P e Q por $P + Q = \mathcal{O} * (P * Q)$. Note que $\mathcal{O} * (P * Q)$ resulta em simplesmente a reflexão de $P * Q$ através do eixo x; de fato, se $P = (a, b)$ é um ponto qualquer da curva elíptica, a reta projetiva passando por P e $\mathcal{O}$ possui equação $X - aZ = 0$, cujo modelo afim é $x = a$. Usando a equação da curva vemos que sua interseção com a curva consiste dos pontos $P = (a, b)$ e $Q = (a, -b)$.

É fácil ver que $E(\mathbb{F})$ é fechado para esta operação, pois se $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pertencem a $E(\mathbb{F})$ e $P_3 = (x_3, y_3)$ é o terceiro ponto na interseção entre a cúbica e a reta

passando por P_1 e P_2, temos que x_1, x_2 e x_3 são as raízes da equação cúbica obtida ao substituir a expressão da reta na equação da cúbica. Logo, como x_1, x_2 pertencem a $\mathbb{F}$, x_3 também pertence a $\mathbb{F}$.

Por construção vemos que esta operação é comutativa, e também que $\mathcal{O}$ é o elemento neutro; além disso, dado um ponto P na curva E, seu inverso é simplesmente seu simétrico, ou seja, $P * \mathcal{O}$. Para mostrar a associatividade da operação, considere P, Q e R pontos pertencentes a E. Pelos oito pontos $\mathcal{O}, P, Q, R, P * Q, Q * R, P + Q, Q + R$ passam as cúbicas:

- E
- C_2: produto das retas passando por $(\mathcal{O}, P * Q, P + Q)$, $(R, Q, Q * R)$ e $(P, Q + R, P * (Q + R))$
- C_3: produto das retas passando por $(\mathcal{O}, Q * R, Q + R)$, $(P * Q, Q, P)$ e $(P + Q, R, (P + Q) * R))$.

Temos assim que a cúbica C_3 contém oito dos nove pontos na interseção entre E e C_2, logo, pelo Teorema 2, também deve conter o nono: $P * (Q + R)$. Segue assim que $P * (Q + R) = (P + Q) * R$, como gostaríamos.

Cabe ressaltar que a operação acima pode ser definida sobre qualquer cúbica C projetiva não singular com um ponto racional $\mathcal{O}$ fixado de maneira a tornar $C(\mathbb{F})$ um grupo.

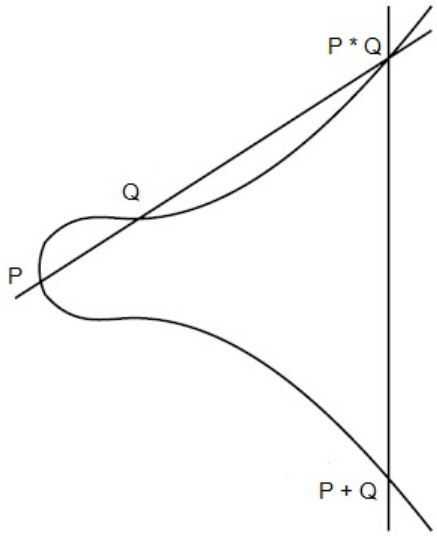

Figura 3.2: Soma de Pontos em uma Curva Elíptica

3.3 Fórmulas Explícitas para a Soma de Pontos

Sejam $E : y^2 = x^3 + ax + b$ uma curva elíptica e $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ em $E(\mathbb{F})$. Obteremos fórmulas explícitas para as coordenadas de $P_3 = P_1 + P_2 = (x_3, y_3)$, que serão amplamente usadas na teoria que segue.

Considere $P_1 \neq P_2$; podemos supor que $x_1 \neq x_2$, uma vez que se $x_1 = x_2$ temos simplesmente $P_3 = \mathcal{O}$. Neste caso, a reta definida por P_1 e P_2 é da forma $y = \lambda x + \nu$, onde $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ e $\nu \in \mathbb{F}$.

Sabemos, pelo Teorema de Bezout, que esta reta intersecta a curva elíptica em três pontos, cujas coordenadas x obtemos substituindo na equação da curva a equação da reta:

$$(\lambda x + \nu)^2 = x^3 + ax + b \iff x^3 + (-\lambda^2)x^2 + (a - 2\lambda\nu)x + (b - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

Comparando os coeficientes dos termos quadráticos temos que:

$$x_1 + x_2 + x_3 = \lambda^2 \iff x_3 = \lambda^2 - x_1 - x_2,\ \lambda = \frac{y_2 - y_1}{x_2 - x_1}, \tag{3.5}$$

e então obtemos $y_3 = -(\lambda x_3 + \nu)$.

Se $P_1 = P_2 = (x, y)$, o coeficiente angular da reta tangente à curva em P_1 é dado por derivação implícita. Denotando $f(x) = x^3 + ax + b$,

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

Temos analogamente que:

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

Obtemos assim uma fórmula para a coordenada x de 2P: usando $f'(x) = 3x^2 + a$ e $y^2 = x^3 + ax + b$ na equação acima obtemos

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

Vejamos agora outras fórmulas para a soma de pontos em $E(\mathbb{F})$, que serão usadas na demonstração do Teorema Fraco de Mordell. Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ em $E(\mathbb{F})$, $P_1 \neq \pm P_2$ e $P_1 + P_2 = P_3 = (x_3, y_3)$. A reta passando por P_1 e P_2 é definida pela equação:

$$y = y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1),$$

cuja interseção com a curva é dada por

$$\left(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\right)^2 = x^3 + ax + b.$$

Seja α uma raiz de $f(x) = x^3 + ax + b$. Definimos $x = X + \alpha$, $x_j = X_j + \alpha$, $j = 1, 2, 3$. Nas novas coordenadas, a equação acima assume a forma

$$\left(y_1 + \frac{y_2 - y_1}{x_2 - x_1}(X - X_1)\right)^2 = X^3 + C_2X^2 + C_1X, \tag{3.7}$$

onde não há monômio de grau zero à direita pois $f(\alpha) = 0$. Reescrevendo (3.7), temos

$$-X^3 + \overline{C_2}X^2 + \overline{C_1}X + \left(y_1 - \frac{y_2 - y_1}{x_2 - x_1}X_1\right)^2 = 0.$$

Como as raízes de (3.7) são $X = x_j - \alpha$, $j = 1, 2, 3$, segue que

$$(x_1 - \alpha)(x_2 - \alpha)(x_3 - \alpha) = \left(y_1 - \frac{y_2 - y_1}{x_2 - x_1}(x_1 - \alpha) \right)^2,$$

ou seja,

$$x_3 - \alpha = \frac{1}{(x_1 - \alpha)(x_2 - \alpha)} \left(\frac{y_1(x_2 - \alpha) - y_2(x_1 - \alpha)}{x_2 - x_1} \right)^2. \tag{3.8}$$

Para obtermos uma fórmula análoga para a duplicação de um ponto, se $P = (x, y)$ é um ponto de $E(\mathbb{F})$, $y \neq 0$, usamos o mesmo raciocínio alterando apenas o coeficiente angular da reta, que agora é dada por derivação implícita:

$$\frac{dy}{dx} = \frac{3x^2 + a}{2y},$$

e então

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

logo

$$x_3 - \alpha = \frac{1}{(x - \alpha)^2} \left(\frac{2y^2 - (3x^2 + a)(x - \alpha)}{2y} \right)^2. \tag{3.9}$$

Capítulo 4

Pontos de Torção

Estudaremos, nos próximos capítulos que se segue, curvas elípticas definidas sobre o corpo dos racionais. Neste capítulo faremos um estudo dos pontos de ordem finita de $E(\mathbb{C})$. Primeiramente descreveremos os pontos de ordem dois e três, e então demonstraremos o Teorema de Nagell-Lutz, que afirma que os pontos de ordem finita possuem coordenadas inteiras e formam um subgrupo finito de $E(\mathbb{Q})$, dito o subgrupo de torção da curva. Denotaremos o subgrupo de torção de $E(\mathbb{Q})$ por $E(\mathbb{Q})_{tor}$.

4.1 Pontos de Ordem Dois e Três

Iniciaremos o estudo dos pontos de ordem finita por aqueles de ordem dois ou três. Se P é um ponto qualquer do plano (x, y), denotaremos suas coordenadas por $x(P)$ e $y(P)$.

Proposição 9. *Seja $E : y^2 = x^3 + ax + b$ uma curva elíptica e $o(P)$ a ordem do ponto P como elemento do grupo $E(\mathbb{C})$.*

(a) O conjunto de pontos $E(\mathbb{C})_2 = \{P \in E(\mathbb{C})\,;\, o(P) \mid 2\}$ é um subgrupo de $E(\mathbb{C})$ de ordem

quatro, produto direto de dois grupos cíclicos de ordem dois. Mais ainda, $\mathcal{O} \neq P \in E(\mathbb{C})$ *tem ordem dois se, e somente se,* $P = (x, 0)$, $x \in \mathbb{C}$.

(b) O conjunto de pontos $E(\mathbb{C})_3 = \{P \in E(\mathbb{C})\,;\, o(P) \mid 3\}$ *é um subgrupo de* $E(\mathbb{C})$ *de ordem nove, produto direto de dois grupos cíclicos de ordem três. Mais ainda,* $\mathcal{O} \neq P = (x, y) \in E(\mathbb{C})$ *tem ordem três se, e somente se,* x *é raiz de* $\psi_3(x) = 3x^4 + 6ax^2 + 12bx - a^2$.

Demonstração. Seja $P = (x, y) \neq \mathcal{O}$, um ponto em $E(\mathbb{C})$. Sabemos que $2P = \mathcal{O}$ se e somente se $(x, y) = P = -P = (x, -y)$, i.e., se $y = 0$. Assim, para as soluções de $0 = x^3 + ax + b$ obtemos três pontos distintos de ordem dois, uma vez que a curva é não singular. O conjunto formado por estes três pontos e o ponto $\mathcal{O}$ é exatamente $E(\mathbb{C})_2$, subgrupo de $E(\mathbb{C})$ pois este é abeliano. O item (a) segue do fato que, a menos de isomorfismo, existe um único grupo de ordem quatro onde todos os elementos, exceto o neutro, têm ordem dois.

Temos que um ponto $P \neq \mathcal{O}$ tem ordem três se, e somente se $x(2P) = x(P)$. De fato, se $x(2P) = x(P) = x(-P)$, então $2P = \pm P$. Como $2P = P$ se e somente se $P = \mathcal{O}$, temos que $2P = -P$, ou seja, $3P = \mathcal{O}$ e segue daí que $o(P) = 3$. A recíproca é imediata.

Das fórmulas explícitas para a soma de pontos temos que, se $f(x) = x^3 + ax + b$,

$$x(2P) = \lambda^2 - 2x,\ \lambda = \frac{f'(x)}{2y}.$$

Então, se $x(2P) = x(P)$,

$$\frac{f'(x)^2}{4f(x)} - 2x = x \iff 2f(x)(6x) - f'(x)^2 = 0.$$

Note que $2f(x)(6x) - f'(x)^2 = 3x^4 + 6ax^2 + 12bx - a^2 = \psi_3(x)$ e, lembrando que $f''(x) = 6x$, obtemos uma nova expressão para $\psi_3(x)$:

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2 = 0.$$

Observando que $\psi_3'(x) = 2f(x)f'''(x) = 12f(x)$, temos que ψ_3 tem uma raiz dupla x se e somente se

$$12f(x) = 0 \text{ e } 2f(x)f''(x) - f'(x)^2 = 0,$$

e daí teríamos que $f(x) = f'(x) = 0$, impossível. Temos então que ψ_3 possui quatro raízes complexas distintas, que serão denotadas por $\beta_j, j = 1, 2, 3, 4$. Escrevendo $\delta_j = \sqrt{f(\beta_j)}$ temos que

$$E(\mathbb{C})_3 = \{\mathcal{O}, (\beta_1, \pm\delta_1), (\beta_2, \pm\delta_2), (\beta_3, \pm\delta_3), (\beta_4, \pm\delta_4)\}.$$

Temos, de fato, nove pontos distintos neste conjunto, pois se $\delta_j = 0$ para algum $1 \leq j \leq 4$ teríamos que a ordem do ponto (β_j, δ_j) seria 2, impossível. Portanto o subgrupo $E(\mathbb{C})$ consiste exatamente de oito pontos de ordem três e o ponto $\mathcal{O}$. Como existe apenas um grupo abeliano de ordem 9 onde todos os elementos têm ordem dividindo 3, segue que tal subgrupo de $E(\mathbb{C})$ é produto direto de dois grupos cíclicos de ordem três. □

Geometricamente, podemos descrever os pontos de ordem três como os pontos de inflexão da nossa curva. De fato,

$$\frac{dy}{dx} = \frac{f'(x)}{2y} \Longrightarrow \frac{d^2y}{dx^2} = \left(2yf''(x) - \frac{f'(x)}{y}f'(x)\right)\left(\frac{1}{4y^2}\right),$$

logo

$$\frac{d^2y}{dx^2} = \frac{2f(x)f''(x) - f'(x)^2}{4y^3} = \frac{\psi_3(x)}{4y^3}.$$

Portanto, pela Proposição 9, um ponto P na curva é ponto de inflexão se e somente se P é ponto de ordem três.

4.2 O Teorema de Nagell-Lutz

Um importante teorema na teoria de curvas elípticas é o Teorema de Nagell-Lutz que, além de afirmar que o subgrupo de torção do grupo de pontos racionais é finito, fornece uma

lista de candidatos a tais pontos. Este teorema foi publicado separadamente por Trygve Nagell e Élisabeth Lutz na década de 30 e a demonstração apresentada aqui é baseada no texto encontrado em [3].

Primeiramente apresentamos uma série de definições e lemas que são necessários para a demonstração deste resultado.

A partir de agora, até o final desta seção, p é um número primo fixado.

Definição 11. *Seja x um número racional não nulo. Temos que x pode ser escrito na forma $x = p^l\dfrac{m}{n}$ de maneira única, onde $m, l \in \mathbb{Z}$, $n \in \mathbb{N}^*$ e $mdc(m,p) = mdc(n,p) = 1$. A avaliação p-ádica de x em p é definida por $ord(x) = l$.*

Mostraremos que, se $P = (x_0, y_0)$ é um ponto de torção na curva elíptica, então $\text{ord}(x_0) \geq 0$ e $\text{ord}(y_0) \geq 0$, ou seja, que P possui coordenadas inteiras.

A partir de agora, sempre que escrevermos um número racional x na forma $x = p^l\dfrac{m}{n}$, está implícito que $m, l \in \mathbb{Z}$, $n \in \mathbb{N}^*$ e $\text{mdc}(m,p) = \text{mdc}(n,p) = 1$.

Seja (x, y) um ponto na curva elíptica tal que p divide o denominador de x, digamos $x = \dfrac{m}{p^\mu n}$, $y = \dfrac{u}{p^\sigma w}$ onde $\mu > 0$, $\sigma \in \mathbb{Z}$. Da equação da curva temos que

$$\frac{u^2}{p^{2\sigma}w^2} = \frac{m^3 + amn^2p^{2\mu} + bn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Como o numerador à direita na igualdade acima não é divisível por p, temos que

$$-2\sigma = ord\left(\frac{u^2}{p^{2\sigma}w^2}\right) = ord\left(\frac{m^3 + amn^2p^{2\mu} + bn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Mas $\mu > 0$ implica em $\sigma > 0$, i.e., p divide o denominador de y. Mais ainda, de $2\sigma = 3\mu$ temos que $\mu = 2\nu$ e $\sigma = 3\nu$ para algum $\nu > 0$ inteiro. Obtemos analogamente os mesmos resultados supondo que p divide o denominador de y: com a mesma notação, teremos que $\mu = 2\nu$ e $\sigma = 3\nu$, para algum $\nu > 0$ inteiro. Definindo, para cada $\nu \in \mathbb{N}$, o conjunto

$$E(p^\nu) = \{(x,y) \in E(\mathbb{Q}); ord(x) \leq -2\nu \text{ e } ord(y) \leq -3\nu\},$$

o argumento acima mostra que

$$P = (x, y) \in E(\mathbb{Q}),\ \text{ord}(x) < 0 \text{ ou } \text{ord}(y) < 0 \Longrightarrow P \in E(p^\nu),\ \nu \geq 1. \tag{4.1}$$

Incluiremos por convenção o elemento $\mathcal{O}$ em cada $E(p^\nu)$.

Note que $E(\mathbb{Q}) \supseteq E(p) \supseteq E(p^2) \supseteq \ldots$. Para mostrar que todo ponto $P = (x, y) \in E(\mathbb{Q})_{tor}$ tem coordenadas inteiras, é suficiente provar que $E(p)$ não contém nenhum ponto de torção. Para este fim faremos a seguinte mudança de coordenadas:

$$t = \frac{x}{y},\ s = \frac{1}{y}. \tag{4.2}$$

Nossa curva assumirá nas novas coordenadas a forma de uma curva elíptica

$$s = t^3 + ats^2 + bs^3, \tag{4.3}$$

onde o ponto no infinito corresponde à origem. Note que, excetuando os pontos de ordem dois($y = 0$) e o ponto $\mathcal{O}$ da curva original, temos uma bijeção entre os pontos do plano (x, y) e aqueles do plano (t, s). Definimos $E'(\mathbb{Q})$ como o grupo de pontos racionais da curva no plano (t, s).

Veja agora que existe uma correspondência entre as retas destes planos: dada uma reta $y = \lambda x + \nu$ no plano (x, y), $\nu \neq 0$, de (4.2) temos no novo plano

$$\frac{1}{s} = \lambda\frac{t}{s} + \nu \Longleftrightarrow \lambda t + \nu s = 1. \tag{4.4}$$

As retas passando pela origem no plano (x, y) correspondem àquelas verticais no plano (t, s).

Considere o anel $R = \left\{\frac{m}{n} \in \mathbb{Q}; p \nmid n\right\} = \{x \in \mathbb{Q}; ord(x) \geq 0\}$; o lema a seguir caracteriza os pontos racionais da curva nas novas coordenadas.

Lema 3. *Sejam $(x, y) \in E(\mathbb{Q})$ e $(t, s) = (x/y, 1/y)$. Então (x, y) pertence a $E(p^\nu)$ se, e somente se, $(t, s) \in E'(p^\nu) = \{(t, s) \in E'(\mathbb{Q});\ t \in p^\nu R$ e $s \in p^{3\nu}R\}$.*

Demonstração. De fato, se $(x, y) \in E(p^\nu)$, então

$$x = \frac{m}{p^{2(\nu+l)}n},\ y = \frac{u}{p^{3(\nu+l)}w},\ l \geq 0.$$

Logo

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+l},\ s = \frac{1}{y} = \frac{w}{u}p^{3(\nu+l)}.$$

Reciprocamente, se $t \in p^\nu R$ e $s \in p^{3\nu}R$ então,

$$t = p^{\nu+i}\frac{a}{b},\ s = p^{3\nu+j}\frac{m}{n},\ \text{com } i, j \geq 0,$$

logo

$$y = \frac{1}{s} = \frac{n}{p^{3\nu+j}m},\ x = \frac{t}{s} = \frac{an}{p^{(2\nu+j-i)}bm}.$$

Portanto, se $(t, s) \in E'(\mathbb{Q})$, então (x, y) é um ponto da curva cujos denominadores de suas coordenadas são divisíveis por p, logo

$$y = \frac{n}{p^{3(\nu+l)}m},\ x = \frac{an}{p^{2(\nu+l)}bm},\ l \geq 0,$$

como gostaríamos. □

Agora que temos uma caracterização dos pontos de $E(p^\nu)$, encontraremos uma fórmula para a soma de pontos da curva elíptica no plano (t, s).

Lema 4. *Sejam $P_j = (t_j, s_j) \in E'(p^\nu)$, $j = 1, 2$, e $P_3 = P_1 + P_2 = (t_3, s_3)$. Então existem inteiros k, m tais que*

$$t_1 + t_2 - t_3 = -\frac{2amk + 3bm^2k}{1 + am^2 + bm^3}.$$

Demonstração. Vejamos primeiramente que não podemos ter $t_1 = t_2$ se $P_1 \neq P_2$; de fato, se $t_1 = t_2$ e $x_j = t_j/s_j$ e $y_j = 1/s_j$, $j = 1, 2$,

$$\frac{x_1}{y_1} = \frac{x_2}{y_2} \Longrightarrow x_1^2y_2^2 = x_2^2y_1^2$$

logo, pela equação da curva,

$$x_1^2(x_2^3 + ax_2 + b) = x_2^2(x_1^3 + ax_1 + b) \iff x_1^2x_2^2(x_2 - x_1) = ax_1x_2(x_2 - x_1) + b(x_2^2 - x_1^2).$$

Temos que $x_2 - x_1 \neq 0$ pois $P_2 \neq P_1$, logo

$$x_1^2x_2^2 = ax_1x_2 + b(x_2 + x_1).$$

Pelo Lema 3, temos que $(x, y) \in E(p^\nu)$. Escrevendo $x_1 = \dfrac{m_1}{p^{2\nu}n_1}$ e $x_2 = \dfrac{m_2}{p^{3\nu}n_2}$, $\nu \geq 1$, e reduzindo os termos acima ao mesmo denominador obtemos

$$m_1^2m_2^2 = am_1m_2n_1n_2p^{5\nu} + b(m_1n_1n_2^2p^{8\nu} + m_2n_1^2n_2p^{7\nu}),$$

mas isto é impossível, pois o lado direito da equação é divisível por p enquanto o lado esquerdo não é.

Temos então que $t_1 \neq t_2$. Seja $s = mt + k$ a reta passando por P_1 e P_2, onde $m = \dfrac{s_2 - s_1}{t_2 - t_1}$. Expressaremos m de outra maneira: como (t_j, s_j) satisfazem a equação (4.3) para $j = 1, 2$, subtraindo as equações temos

$$s_2 - s_1 = (t_2^3 - t_1^3) + a[(t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)] + b(s_2^3 - s_1^3).$$

Dividindo a equação por $t_2 - t_1$ e isolando o termo $\dfrac{s_2 - s_1}{t_2 - t_1}$ obtemos outra expressão para m:

$$m = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1t_2 + t_1^2 + as_2^2}{1 - at_1(s_2 + s_1) - b(s_2^2 + s_1s_2 + s_1^2)} \tag{4.5}$$

Para $P_1 = P_2$, m é dado por derivação implícita:

$$m = \frac{ds}{dt}(P_1) = \frac{3t_1^2 + as_1^2}{1 - 2at_1s_1 - 3bs_1^2}.$$

Note que essa expressão é exatamente igual a (4.5) quando $(t_1, s_1) = (t_2, s_2)$, portanto usaremos (4.5) em todos os casos.

Sabemos de (4.3) que $P_3' = (-t_3, -s_3)$ é o terceiro ponto de interseção da reta $s = mt + k$ com a curva no plano (t,s) e $t_1, t_2, -t_3$ são as soluções de

$$mt + k = t^3 + at(mt + k)^2 + b(mt + k)^3 \iff 0 = (1 + am^2 + bm^3)t^3 + (2amk + 3bm^2k)t^2 + ...,$$

logo

$$(1 + am^2 + bm^3)t^3 + (2amk + 3bm^2k)t^2 + ... = (1 + am^2 + bm^3)(t - t_1)(t - t_2)(t + t_3)$$

Desse modo

$$t_1 + t_2 - t_3 = -\frac{2amk + 3bm^2k}{1 + am^2 + bm^3}, \tag{4.6}$$

como gostaríamos. □

Encontramos desta maneira fórmulas para a soma de pontos de $E'(p^\nu)$: após encontrar a coordenada t de P_3 usando a equação acima, basta tomar a interseção da reta $s = mt + k$ com a curva elíptica para encontrar o valor de s_3.

Proposição 10. *$E'(p^\nu)$ é um subgrupo de $E'(\mathbb{Q})$, $\forall \nu \in \mathbb{N}$.*

Demonstração. De acordo com a notação do Lema 4, se $t_1, t_2, s_1, s_2 \in p^\nu R$, o numerador de (4.5) está em $p^{2\nu}R$. Pelo mesmo argumento temos que

$$-at_1(s_2 + s_1) - b(s_2^2 + s_1s_2 + s_1^2) = p^{2\nu}\frac{u}{w},$$

logo

$$1 - at_1(s_2 + s_1) - b(s_2^2 + s_1s_2 + s_1^2) = \frac{w + p^{2\nu}u}{w}.$$

Segue então que o denominador de (4.5) tem ordem 0, e portanto $m \in p^{2\nu}R$. Da equação $k = s_1 - mt_1$ temos que $k \in p^{3\nu}R$, já que s_1 e mt_1 estão neste mesmo ideal. Como o denominador de (4.6) é uma unidade em R, $t_1 + t_2 - t_3 \in p^{5\nu}R \subseteq p^\nu R$, logo $t_3 \in p^\nu R$ uma vez que t_1, t_2 também pertencem a este ideal. Finalmente, vemos que $s_3 \in p^{3\nu}R$ pois $s_3 = mt_3 + k$, e assim segue pelo Lema 1 que $E'(p^\nu)$ é fechado para a soma.

Para concluir que $E'(p^\nu)$ é um subgrupo de $E'(\mathbb{Q})$, observe que se $P = (t, s) \in E'(p^\nu)$ então $-P = (-t, -s) \in E'(p^\nu)$. □

Vejamos agora que esta mudança de coordenadas é essencialmente um isomorfismo de grupos entre $E(\mathbb{Q})$ e $E'(\mathbb{Q})$.

Proposição 11. *A aplicação*

$$\begin{aligned} \phi : \frac{E(\mathbb{Q})}{E(\mathbb{Q})_2} &\longrightarrow E'(\mathbb{Q}) \\ P + E(\mathbb{Q})_2 &\longmapsto \begin{cases} \psi(P), \text{ se } P \neq \mathcal{O} \\ (0,0), \text{ se } P = \mathcal{O} \end{cases} \end{aligned}$$

é um isomorfismo de grupos, onde ψ denota a mudança de coordenadas (4.2).

Demonstração. Mostraremos primeiramente que ψ é aditiva em $E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$; este fato será necessário para mostrar que a aplicação ϕ está bem definida.

Sejam P_1 e P_2 pontos de $E(\mathbb{Q})$, $P_1, P_2 \notin E(\mathbb{Q})_2$. Sabemos de (4.4) que a mudança de coordenadas (4.2) preserva retas, logo se P_1 e P_2 são distintos, $\psi(P_1 * P_2) = \psi(P_1) * \psi(P_2)$. Suponha agora $P_1 = P_2 = P = (x_0, y_0)$; mostraremos que a imagem da reta tangente à curva em P é a reta tangente à curva em $\psi(P)$.

Considere $Q = (x, y) \neq P$ e $\lambda(Q)$ o coeficiente angular da reta passando por P e Q, cuja equação é da forma $L_{PQ} : y = \lambda(Q)x + \nu(Q)$. Denotaremos por $y = \lambda(P)x + \nu(P)$ a reta tangente à curva em P. Se $\nu(P) \neq 0$, como $Q \longmapsto \nu(Q) = y_0 - \lambda(Q)x_0$ é uma aplicação contínua, temos uma vizinhança V do ponto P tal que $\nu(Q) \neq 0$, $\forall\, Q \in V$. Usando (4.4), a imagem da reta L_{PQ} pode ser escrita como

$$L_{\psi(P)\psi(Q)} : 1 = \lambda(Q)t + \nu(Q)s \iff s = -\frac{\lambda(Q)}{\nu(Q)}t + \frac{1}{\nu(Q)}.$$

Note que

$$\begin{aligned} \varphi : \mathbb{R} &\longrightarrow \mathbb{R} \\ \lambda(P_2) &\longmapsto -\tfrac{\lambda(P_2)}{\nu(P_2)} \end{aligned}$$

é uma aplicação contínua que associa o coeficiente angular de $L_{\psi(P_1)\psi(P_2)}$ ao coeficiente angular de $L_{P_1P_2}$.

Do resultado acima temos que $\varphi(\lambda(Q)) = \lambda(\psi(Q)),\ \forall\, Q \in V$, logo $\varphi(\lambda(P)) = \lambda(\psi(P))$ segue por continuidade, como queríamos demonstrar. O caso $\nu(P) = 0$ é tratado analogamente.

Segue daí que, se P_1 e P_2 são pontos de $E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$, $\psi(P_1 * P_2) = \psi(P_1) * \psi(P_2)$, e então $\psi(P_1 + P_2) = \psi(P_1) + \psi(P_2)$. De fato, se

$$P_j = (x_j, y_j),\ \psi(P_j) = (t_j, s_j),\ j = 1, 2\ e\ P_1 * P_2 = (x_3, y_3),$$

então

$$P_1 + P_2 = (x_3, -y_3) \Longrightarrow \psi(P_1 + P_2) = \left(-\frac{x_3}{y_3}, -\frac{1}{y_3}\right)$$

e

$$\psi(P_1) + \psi(P_2) = (-t_3, -s_3) = \left(-\frac{x_3}{y_3}, -\frac{1}{y_3}\right),$$

mostrando que ψ é aditiva.

Para ver que a aplicação ϕ está bem definida, considere $P \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$ e $Q \in E(\mathbb{Q})_2$. Então

$$(0, 0) = \phi(Q) = \phi((P + Q) - P) = \phi(P + Q) - \phi(P)$$

pois $P + Q$ e P são pontos de $E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$. Logo $\phi(P) = \phi(P + Q)$, como gostaríamos. A aditividade de ψ sobre $E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$ conclui a demonstração. □

Seja P um ponto de torção de $E(\mathbb{Q})_{tor} \setminus E(\mathbb{Q})_2$. Segue da Proposição 11 que $\psi(P) \in E'(\mathbb{Q})_{tor}$. Se mostrarmos que não existem pontos de torção de $E'(\mathbb{Q})$ pertencentes a $E'(p)$, teremos, pelo Lema 3, que $P \notin E(p)$.

Na demonstração da Proposição 10 provamos que se $P_1, P_2 \in E'(p^\nu)$ então $t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{5\nu}R$, i.e.,

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2)\ (mod\ p^{5\nu}R) \tag{4.7}$$

Consideremos a aplicação que a cada ponto racional $P = (t, s)$ em $E'(p^\nu)$ associa a classe de sua coordenada t em $p^\nu R/p^{5\nu}R$. O núcleo dessa aplicação é o conjunto $\{P \in E'(p^\nu);\ t(P) \in p^{5\nu}R\} = E'(p^{5\nu})$, logo pelo Teorema de Isomorfismos temos que a aplicação

$$\begin{aligned} \frac{E'(p^\nu)}{E'(p^{5\nu})} &\longrightarrow \frac{p^\nu R}{p^{5\nu}R} \\ P &\longmapsto t(P) \end{aligned}$$

é um homomorfismo injetivo. Por convenção, $\mathcal{O} \longmapsto 0$. Podemos agora concluir a demonstração do Teorema de Nagell-Lutz.

Teorema 3 (Nagell-Lutz)**.** *Sejam $y^2 = x^3 + ax + b$ uma curva elíptica com coeficientes inteiros e Δ o discriminante de $f(x) = x^3 + ax + b$. Se $P = (x_0, y_0) \in E(\mathbb{Q})$ é um ponto de torção então P tem coordenadas inteiras e, além disso, y_0^2 divide Δ.*

Demonstração. Mostraremos que nenhum ponto de torção de $E'(\mathbb{Q})$ pertence a $E'(p)$. Dessa maneira, se $P \in E(\mathbb{Q})_{tor} \setminus E(\mathbb{Q})_2$ então $\psi(P) \notin E'(p)$ e, portanto, P não pertence a $E(p)$. Note que os pontos de $E(\mathbb{Q})_2$ têm coordenadas inteiras pois toda solução racional de $0 = x^3 + ax + b$, onde $a, b \in \mathbb{Z}$, é inteira.

Sejam $P' = (t, s) \in E'(\mathbb{Q})$ um ponto de ordem finita $m > 1$ e $P = (x, y)$, onde $x = t/s$ e $y = 1/s$. Suponha que $P' \in E'(p)$. Como $P' \in E'(p)$ se e somente se $P \in E(p)$ e o denominador de $x(P)$ não pode ser divisível por potências arbitrariamente altas de p, existe $\nu > 0$ tal que $P' \in E'(p^\nu)$ e $P' \notin E'(p^{\nu+1})$.

(i) Suponha que p não divide m. De (4.7) temos que

$$t(mP') \equiv mt(P') \,(mod\, p^{5\nu}R),$$

mas como $mP' = \mathcal{O}$ temos que $t(mP') = 0$ e portanto

$$mt(P') \equiv 0 \,(mod\, p^{5\nu}R) \Longleftrightarrow t(P') \equiv 0 \,(mod\, p^{5\nu}R).$$

Segue então que $P' \in E'(p^{5\nu}) \subseteq E'(p^{\nu+1})$, impossível.

(ii) Suponha agora que $p \mid m$. Seja $m = pn$ e considere $Q' = nP'$. Como $P' \in E'(p)$, temos que $Q' \in E'(p)$ e analogamente existe $\nu > 0$ tal que $Q' \in E'(p^\nu)$ e $Q' \notin E'(p^{\nu+1})$. Então

$$t(pQ') \equiv pt(Q')\,(mod\, p^{5\nu} R)$$

$$0 \equiv pt(Q')\,(mod\, p^{5\nu} R)$$

$$t(Q') \equiv 0\,(mod\, p^{5\nu-1} R),$$

mas isto significa que $Q' \in E'(p^{5\nu-1}) \subseteq E'(p^{\nu+1})$, um absurdo.

Seja $P = (x, y) \in E(\mathbb{Q})_{tor}$, $y \neq 0$; mostraremos agora que y^2 divide $\Delta = -4a^3 - 27b^2$. Se $2P = (x(2P), y(2P))$, sabemos da seção 3.3 que

$$x(2P) = \lambda^2 - 2x,\ \lambda = \frac{f'(x)}{2y},$$

portanto devemos ter que $y \mid f'(x) = 3x^2 + a$ pois x e $x(2P)$ são números inteiros. Além disso, vale que

$$27(x^3 + ax + b)(x^3 + ax - b) = (3x^2 + a)^2(3x^2 + 4a) - (4a^3 + 27b^2),$$

logo $y^2 \mid 4a^3 + 27b^2$, pois $y^2 = x^3 + ax + b$. □

Capítulo 5

O Teorema de Mordell

Neste capítulo demonstramos o Teorema de Mordell, o qual afirma que o grupo de pontos racionais de uma curva elíptica é finitamente gerado. Este teorema foi conjecturado primeiramente por Poincaré em 1901 e demonstrado em 1922 por Louis Mordell; na mesma década, André Weil generalizou este resultado para variedades abelianas. A demonstração do Teorema de Mordell para curvas elípticas neste texto é baseada em [8] com exceção da demonstração do Teorema Fraco de Mordell, que se encontra em [1].

Começamos introduzindo as seguintes funções: dado um número racional $x = m/n$, $\text{mdc}(m, n) = 1$, definimos sua altura como

$$H(x) = max\{|m|, |n|\} \text{ e,}$$

e frequentemente também nos referimos à seguinte função como altura:

$$h(x) = \log H(x).$$

Se $P = (x, y) \in E(\mathbb{Q})$, definimos $H(P) = H(x)$ e $h(P) = \log H(P)$. Esta função $h : E(\mathbb{Q}) \mapsto [0, +\infty)$ será crucial na demonstração do Teorema de Mordell, que segue do seguinte teorema mais geral para grupos abelianos.

Teorema 4. *Sejam Γ um grupo abeliano aditivo e $h : \Gamma \mapsto [0, +\infty)$ uma função com as seguintes propriedades:*

(a) *para cada número real $M > 0$ o conjunto $\{P \in \Gamma;\ h(P) \leq M\}$ é finito;*

(b) *para cada $P_0 \in \Gamma$ existe uma constante $k' = k'(P_0)$ tal que $h(P + P_0) \leq 2h(P) + k',\ \forall P \in \Gamma$;*

(c) *existe uma constante k tal que $h(2P) \geq 4h(P) - k,\ \forall P \in \Gamma$;*

(d) *o subgrupo 2Γ tem índice finito em Γ.*

Então o grupo Γ é finitamente gerado.

Demonstração. Seja $[\Gamma : 2\Gamma] = n$ e considere $Q_1, ..., Q_n$ em $\Gamma/2\Gamma$, $Q_i \neq Q_j$ se $i \neq j$. Fixado P_0 em Γ, existe $Q_{i_1}, 1 \leq i_1 \leq n$, tal que $P_0 - Q_{i_1} = 2P_1 \in 2\Gamma$; como $P_1 \in \Gamma$, existe $Q_{i_2}, 1 \leq i_2 \leq n$, tal que $P_1 - Qi_2 = 2P_2 \in 2\Gamma$. Repetindo este processo obtemos uma sequência de pontos $(P_m)_{m\in\mathbb{N}}$ tal que

$$P_0 - Q_{i_1} = 2P_1$$

$$P_1 - Q_{i_2} = 2P_2$$

$$\vdots$$

$$P_m - Q_{i_{m+1}} = 2P_{m+1}$$

$$\vdots$$

onde $P_m \in \Gamma$ e $Q_{i_m} \in \{Q_1, ..., Q_n\},\ \forall m \in \mathbb{N}$. Vemos então que

$$P_0 = Q_{i_1} + 2Q_{i_2} + 4P_2$$

$$P_0 = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + 8P_3$$

$$\vdots$$

$$P_0 = Q_{i_1} + 2Q_{i_2} + ... + 2^{m-1}Q_{i_m} + 2^m P_m$$

Mostraremos agora que, para m suficientemente grande, $h(P_m) \leq K$, onde K é uma constante fixada; dessa maneira teremos que Γ é gerado pelo conjunto

$$\{Q_1, ..., Q_n\} \cup \{P \in \Gamma; h(P) \leq K\},$$

que é um conjunto finito pelo item (a).

Seja P_j um ponto da sequência anterior. Da hipótese (b) temos que, para cada $i = 1, 2, ..., n$, existe k_i' tal que $h(P - Q_i) \leq 2h(P) + k_i',\ \forall P \in \Gamma,\ i = 1, ..., n$. Definindo $k' = max\{k_i',\ i = 1, ..., n\}$ temos $h(P - Q_i) \leq 2h(P) + k',\ \forall P \in \Gamma,\ i = 1, ..., n$. Portanto, usando a hipótese (c),

$$4h(P_j) \leq h(2P_j) + k = h(P_{j-1} - Q_{i_j}) + k \leq 2h(P_{j-1}) + k' + k,$$

logo

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{k' + k}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}[h(P_{j-1}) - (k' + k)],$$

de modo que se $h(P_{j-1}) \geq k' + k$ então $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. Segue assim que para algum $m \in \mathbb{N}$ teremos $h(P_m) \leq k' + k$, como gostaríamos. □

Devemos agora mostrar que o grupo de pontos racionais de uma curva elíptica satisfaz as quatro hipóteses do Teorema 2, trabalho que ocupará as próximas seções.

5.1 A Altura de Pontos Racionais

Nesta seção apresentaremos estimativas para $h(P + P_0),\ P_0 \in E(\mathbb{Q})$ fixado, e $h(2P)$. Primeiramente vejamos que a primeira hipótese do Teorema 4 segue imediatamente da definição de altura de um ponto.

Proposição 12. *Para cada número real M o conjunto $\{P \in E(\mathbb{Q}); h(P) \leq M\}$ é finito.*

Demonstração. Basta notar que para número cada real $M > 0$ fixado existe uma quantidade finita de números racionais x tais que $H(x) \leq M$, e o mesmo vale portanto para os números racionais x tais que $h(x) \leq M$; mas para cada racional fixado x temos no máximo dois pontos $P \in E(\mathbb{Q})$ tais que $x(P) = x$. Segue daí o resultado. □

Lembramos agora, de acordo com o argumento apresentado na seção 4.2, que se $P \in E(\mathbb{Q})$, então $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, onde $m, n, e \in \mathbb{Z}$ e $\text{mdc}(m, e) = \text{mdc}(n, e) = 1$, de modo que $H(P) = max\{|m|, e^2\}$. Usando a equação da curva obtemos uma estimativa importante:

$$P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q}) \Longrightarrow \exists\ K > 0 \text{ tal que } |n| \leq KH(P)^{3/2}. \tag{5.1}$$

De fato,

$$\frac{n^2}{e^6} = \frac{m^3}{e^6} + a\frac{m}{e^2} + b \Longleftrightarrow n^2 = m^3 + ame^4 + be^6,$$

logo

$$n^2 \leq |m^3| + |am|e^4 + |b|e^6 \leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 = (1 + |a| + |b|)H(P)^3,$$

e assim $|n| \leq KH(P)^{3/2}$, onde $K = \sqrt{1 + |a| + |b|}$.

Proposição 13. *Para cada $P_0 \in E(\mathbb{Q})$ existe uma constante $k' = k'(P_0)$ tal que $h(P + P_0) \leq 2h(P) + k'$, $\forall\ P \in E(\mathbb{Q})$.*

Demonstração. O resultado é trivial se $P_0 = \mathcal{O}$; fixemos então $P_0 \neq \mathcal{O}$ e considere $P \in E(\mathbb{Q})$ diferente de $P_0, -P_0, \mathcal{O}$. Note que não há perda de generalidade ao excluírmos um conjunto finito de pontos, pois basta escolher uma nova constante que torne a afirmativa verdadeira para o conjunto de pontos que foi excluído.

Sejam $P_0 = (x_0, y_0),\ P = (x, y),\ P + P_0 = (\xi, \eta)$. Sabemos de (3.5) que $\xi + x + x_0 = \lambda^2$, onde $\lambda = \dfrac{y - y_0}{x - x_0}$. Segue então que

$$\xi = \frac{(y - y_0)^2 - (x + x_0)(x - x_0)^2}{(x - x_0)^2}$$

e, usando equação da curva $y^2 = x^3 + ax + b$ para o ponto $P = (x, y)$, podemos reescrever esta expressão obtendo

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G},$$

onde $A, B, C, D, E, F, G \in \mathbb{Q}$ são constantes que dependem somente de a, b, x_0, y_0. Note que obtemos uma expressão equivalente para ξ com A, B, C, D, E, F e G inteiros multiplicando o numerador e o denominador acima por um inteiro adequado. Substituindo $x = \dfrac{m}{e^2}$ e $y = \dfrac{n}{e^3}$ obtemos

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4} \in \mathbb{Q},$$

e então

$$H(\xi) = \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}.$$

Como $e^2 \leq H(P)$ e vale a equação (5.1), temos que

$$H(\xi) = H(P + P_0) \leq \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\} H(P)^2$$

e assim

$$h(P + P_0) = \log H(P + P_0) \leq 2h(P) + k_0,$$

onde $k_0 = \log(\max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\})$ depende apenas de a, b, x_0, y_0, como gostaríamos. □

Proposição 14. *Existe uma constante k tal que $h(2P) \geq 4h(P) - k,\ \forall P \in E(\mathbb{Q})$.*

Demonstração. Já vimos que podemos excluir da demonstração um conjunto finito de pontos sem perda de generalidade. Sejam então $P = (x, y) \in E(\mathbb{Q}) \setminus E(\mathbb{Q})_2$ e $2P = (\xi, \eta)$; sabemos da seção 1.3 que, se $f(x) = x^3 + ax + b$,

$$\xi + 2x = \lambda^2,\ \lambda = \frac{f'(x)}{2y},$$

logo

$$\xi = \frac{f'(x)^2 - 8xf(x)}{4f(x)} = \frac{P_1(x)}{P_2(x)},$$

onde $P_1(x), P_2(x) \in \mathbb{Z}[x]$ e $\deg P_1(x) = 4,\ \deg P_2(x) = 3$. Note que $P_1(x)$ e $P_2(x)$ não têm raízes comuns, uma vez que a curva $y^2 = f(x)$ é não singular. A demonstração estará concluída com o seguinte lema sobre polinômios em $\mathbb{Z}[x]$. □

Lema 5. *Sejam $\phi(x),\ \psi(x) \in \mathbb{Z}[x]$ polinômios primos entre si e $d = \max\{\deg\phi, \deg\psi\}$. Então*

(a) *existe um inteiro $R = R(\phi, \psi) \geq 1$ tal que $mdc\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$ divide R, $\forall\, m/n \in \mathbb{Q}$.*

(b) *existe $k = k(\phi, \psi)$ tal que para todo racional m/n que não anula ψ temos*

$$dh\left(\frac{m}{n}\right) - k \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right).$$

Demonstração. Note primeiramente que $n^d\phi(m/n),\ n^d\psi(m/n) \in \mathbb{Z}$. Suponha que $\deg\phi = d$, $\deg\psi = e \leq d$,

$$\phi(x) = a_0x^d + a_1x^{d-1} + ... + a_d \text{ e}$$

$$\psi(x) = b_0x^e + b_1x^{e-1} + ... + b_e.$$

Fixe $m/n \in \mathbb{Q}$ e defina

$$\Phi(m,n) = n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1nm^{d-1} + ... + a_dn^d,$$

$$\Psi(m,n) = n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e+1} + ... + b_en^d.$$

(a) Como $\text{mdc}(\phi(x), \psi(x)) = 1$ em $\mathbb{Q}[x]$, existem $F(x),\ G(x) \in \mathbb{Q}[x]$ tais que

$$F(x)\phi(x) + G(x)\psi(x) = 1. \tag{5.2}$$

Considere $A \in \mathbb{Z}$ tal que $AF(x),\ AG(x) \in \mathbb{Z}[x]$ e seja $D = \max\{\deg F(x),\ \deg G(x)\}$; note que A e D não dependem do racional fixado. Segue de (5.2) que

$$An^D F\left(\frac{m}{n}\right)\Phi(m,n) + An^D G\left(\frac{m}{n}\right)\Psi(m,n) = An^{d+D}.$$

Seja $\gamma = \gamma(m,n) = \text{mdc}(\Phi(m,n), \Psi(m,n))$; mostraremos que $\gamma \mid Aa_0^{d+D}$. Da equação acima vemos que $\gamma \mid An^{d+D}$ e, da sua definição, γ também divide

$$An^{d+D-1}\Phi(m,n) = Aa_0m^dn^{d+D-1} + Aa_1m^{d-1}n^{d+D} + ... + Aa_dn^{2d+D-1},$$

logo $\gamma \mid Aa_0m^dn^{d+D-1}$. Segue assim que γ divide

$$\text{mdc}(An^{d+D}, Aa_0m^dn^{d+D-1}) = mdc(An^{d+D}, Aa_0n^{d+D-1})$$

e portando $\gamma \mid Aa_0n^{d+D-1}$.

Usando o mesmo argumento para Aa_0n^{d+D-1} concluímos que $\gamma \mid Aa_0^2n^{d+D-2}$, e assim teremos que $\gamma \mid Aa_0^{d+D}$. Esolhendo $R = Aa_0^{d+D}$, temos o resultado.

(b) Novamente excluiremos um conjunto finito de elementos: considere m/n um racional que não anula ϕ.

Desejamos uma estimativa para $h(\xi)$, onde

$$\xi = \frac{\phi(m/n)}{\psi(m/n)} = \frac{n^d\phi(m/n)}{n^d\psi(m/n)} = \frac{\Phi(m,n)}{\Psi(m,n)}.$$

Mostramos no item (a) que existe $R = R(\phi,\psi)$ tal que $\text{mdc}(\Phi(m,n), \Psi(m,n))$ divide $R,\ \forall\ m/n \in \mathbb{Q}$. Logo, como $H(\xi) = \max\left\{\frac{|\Phi(m,n)|}{\text{mdc}(\Phi(m,n),\Psi(m,n))}, \frac{|\Psi(m,n)|}{\text{mdc}(\Phi(m,n),\Psi(m,n))}\right\}$,

$$H(\xi) \geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} = \frac{1}{R}\max\{|n^d\phi(m/n)|, |n^d\psi(m/n)|\}$$

$$\Longrightarrow H(\xi) \geq \frac{1}{2R}(|n^d\phi(m/n)| + |n^d\psi(m/n)|),$$

logo

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R}\frac{(|n^d\phi(m/n)| + |n^d\psi(m/n)|)}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{(|\phi(m/n)| + |\psi(m/n)|)}{\max\{|m/n|^d, 1\}}.$$

Considere então a função $p(t) = \dfrac{(|\phi(t)| + |\psi(t)|)}{\max\{|t|^d, 1\}}$; note que

$$\lim_{t\to\pm\infty} p(t) = \lim_{t\to\pm\infty} \frac{q(t)}{|t|^d} \in \mathbb{R}^*$$

pois $q(t)$ é um polinômio de grau d. Segue assim que para algum $M_0 \in \mathbb{R}$ a função $p(t)$ é limitada e não nula fora do compacto $[-M_0, M_0]$. Mas $p(t)$ é uma função contínua que nunca se anula, já que $\phi(t)$ e $\psi(t)$ não tem raízes comuns; logo dentro deste compacto $p(t)$ possui um mínimo positivo C_0. Segue então que para algum $C_1 > 0$,

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{C_1}{2R} \iff H(\xi) \geq \frac{C_1}{2R} H(m/n)^d, \ \forall\ m/n \in \mathbb{Q},$$

e então

$$\log H(\xi) \geq \log\left(\frac{C_1}{2R} H(m/n)^d\right) \iff h(\xi) \geq dh(m/n) + \log\left(\frac{C_1}{2R}\right),$$

para todo $m/n \in \mathbb{Q}$, onde C_1 e $2R$ não dependem do racional m/n fixado. □

5.2 O Teorema Fraco de Mordell

Demonstramos agora o Teorema Fraco de Mordell, que afirma que o subgrupo $2E(\mathbb{Q})$ tem índice finito em $E(\mathbb{Q})$. Existe na verdade o seguinte resultado mais geral, que pode ser encontrado em [7].

Teorema 5 (Mordell-Weil)**.** *Sejam $\mathbb{K}$ um corpo de números, $E : y^2 = x^3 + ax + b$ uma curva elíptica sobre $\mathbb{K}$ e $m \geq 2$ um inteiro. Então o índice $[E(\mathbb{K}) : mE(\mathbb{K})]$ é finito, onde $mE(\mathbb{K}) = \{mP;\ P \in E(\mathbb{K})\}$.*

Destinamos esta seção à demonstração da finitude do índice $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$.

Considere $\beta : \mathbb{Q}^* \mapsto \mathbb{Q}^*/\mathbb{Q}^{*2}$ o homomorfismo canônico e suponha que as raízes de $f(x) = x^3 + ax + b$ são $a_1, a_2, a_3 \in \mathbb{Q}$. Caso as raízes de $f(x)$ não sejam racionais, a mesma demonstração vale para um corpo de números que as contenha.

Definimos em $E(\mathbb{Q})$, para $j = 1, 2, 3$, as funções:

$$\phi_j(P) = \begin{cases} \beta(1), \text{ se } P = \mathcal{O} \\ \prod_{i \neq j} \beta(x(P) - a_i), \text{ se } P = (a_j, 0) \\ \beta(x(P) - a_j), \text{ caso contrário.} \end{cases} \tag{5.3}$$

Note que se $x_0 \neq a_i$, $i = 1, 2, 3$ então $\prod_{i=1}^{3} \beta(x_0 - a_i) = \beta(y_0)^2 = 1$, logo $\prod_{i \neq j} \beta(x_0 - a_i) = \beta(x_0 - a_j)$. Definimos ainda

$$\phi : E(\mathbb{Q}) \mapsto \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$$

$$P \mapsto (\phi_1(P), \phi_2(P), \phi_3(P))$$

Usando as fórmulas para soma (3.8) e (3.9), é fácil ver que esta aplicação é um homomorfismo. Mostraremos agora que o núcleo deste homomorfismo é exatamente $2E(\mathbb{Q})$ e sua imagem é finita; o Teorema dos Isomorfismos para grupos concluirá a demonstração do Teorema Fraco de Mordell.

Lema 6. *O conjunto $\phi(E(\mathbb{Q}))$ é finito.*

Demonstração. Seja $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q})$, $P \notin \{\mathcal{O}, (a_1, 0), (a_2, 0), (a_3, 0)\}$; da equação da curva temos que:

$$n^2 = (m - a_1 e^2)(m - a_2 e^2)(m - a_3 e^2). \tag{5.4}$$

Seja d um divisor comum de $m - a_i e^2$ e $m - a_j e^2$, $i \neq j$, então d divide $(m - a_j e^2) - (m - a_i e^2) = (a_i - a_j)e^2$, mas como $\text{mdc}(m, e) = 1$ temos que $\text{mdc}(d, e) = 1$. Segue que d divide $(a_i - a_j)$.

Seja p um primo. Se p é um fator primo na fatoração de apenas um dos $m - a_j e^2$, $j = 1, 2, 3$, então de (5.4) temos que o expoente deste primo é par; se p é fator de mais de um dos $m - a_j e^2$, $j = 1, 2, 3$, então $p \mid M = \prod_{i \neq j} (a_i - a_j)$. Segue que para $j = 1, 2, 3$, $m - a_j e^2 = \mu_j \eta_j^2$, μ_j um divisor de M; logo

$$\beta(x(P) - a_j) = \beta\left(\frac{m}{e^2} - a_j\right) = \beta\left(\frac{1}{e^2}\right) \beta(\mu_j)\beta(\eta_j^2) = \beta(\mu_j).$$

Portanto cada um dos homomorfismos ϕ_j tem imagem finita, e segue o resultado. □

Lema 7. *Com a mesma notação,* $\ker(\phi) = 2E(\mathbb{Q})$.

Demonstração. Se $P = (x, y) \in E(\mathbb{Q})$, $y \neq 0$, então de (3.9) temos que $x(2P) - a_j,\ j = 1, 2, 3,$ é um quadrado e portanto $P \in \ker \phi$. Se $y = 0$ então $2P = \mathcal{O}$ e $P \in \ker \phi$. Por outro lado, seja $P \in \ker \phi$; desejamos encontrar $Q \in E(\mathbb{Q})$ tal que $P = 2Q$.

Note que, se $P \in \ker \phi$ então para $j = 1, 2, 3$ temos que $x(P) - a_j = \alpha_j^2$, para algum $\alpha_j \in \mathbb{Q}$; considere então o sistema de equações nas variáveis u_1, u_2, u_3

$$u_1 + a_j u_2 + a_j^2 u_3 = \alpha_j,\ j = 1, 2, 3, \tag{5.5}$$

ou ainda, na forma matricial,

$$\begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ 1 & a_3 & a_3^2 \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

Temos uma única solução para este sistema uma vez que

$$\begin{vmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ 1 & a_3 & a_3^2 \end{vmatrix} = \prod_{i>j} (a_i - a_j) \neq 0,$$

pois a curva é não singular. Usando agora (5.5) e a equação da curva obtemos

$$x(P) - a_j = \alpha_j^2 = (u_1 + a_j u_2 + a_j^2 u_3)^2 =$$

$$= u_1^2 - 2u_2u_3b + 2u_1u_2a_j - 2u_2u_3aa_j - bu_3^2a_j + u_2^2a_j^2 + 2u_1u_3a_j^2 - au_3^2a_j^2,$$

logo,

$$(u_1^2 - 2u_2u_3b - x(P))1 + (2u_1u_2 - 2u_2u_3a - bu_3^2 + 1)a_j + (u_2^2 + 2u_1u_3 - au_3^2)a_j^2 = 0,\ j = 1, 2, 3.$$

Então

$$(u_1^2-2u_2u_3b-x(P))\begin{pmatrix}1\\1\\1\end{pmatrix}+(2u_1u_2-2u_2u_3a-bu_3^2+1)\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}+(u_2^2+2u_1u_3-au_3^2)\begin{pmatrix}a_1^2\\a_2^2\\a_3^2\end{pmatrix}=0.$$

Mas estes vetores são linearmente independentes, logo esta combinação linear deve ter coeficientes nulos. Segue que

$$u_1^2 - 2u_2u_3b = x(P) \tag{5.6}$$

$$2u_1u_2 - 2u_2u_3a - bu_3^2 = -1 \tag{5.7}$$

$$u_2^2 + 2u_1u_3 + au_3^2 = 0, \tag{5.8}$$

onde não podemos ter $u_3 = 0$, pois teríamos assim que $u_2 = 0$ de (5.8) e isto entraria em contradição com (5.7). Isolando u_1 em (5.8) e substituindo em (5.7) obtemos

$$\left(\frac{1}{u_3}\right)^2 = \left(\frac{u_2}{u_3}\right)^3 + a\left(\frac{u_2}{u_3}\right) + b,$$

logo $Q := (x_0, y_0) = \left(\frac{u_2}{u_3}, \frac{1}{u_3}\right) \in E(\mathbb{Q})$. Dividindo (5.8) por u_3^2 vemos que

$$u_1 = \frac{-x^2 + a}{2y}$$

e usando (5.5) obtemos

$$x(P) - a_j = \alpha_j = \frac{-x^2 + a + 2a_jx + 2a_j^2}{2y},\ j = 1, 2, 3.$$

Portanto $x(P) = x(2Q)$ pela equação (3.9). Daí temos que $P = 2(\pm Q)$, mostrando que $P \in 2E(\mathbb{Q})$ e assim $\ker\phi \subseteq 2E(\mathbb{Q})$, como gostaríamos. □

Teorema 6 (Fraco de Mordell)**.** *Seja $E : y^2 = x^3 + ax + b$ uma curva elíptica e $E(\mathbb{Q})$ o seu grupo de pontos racionais. Então o subgrupo $2E(\mathbb{Q})$ tem índice finito em $E(\mathbb{Q})$.*

Demonstração. Do Teorema dos Isomorfismos temos que

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \cong \phi(E(\mathbb{Q})).$$

O resultado segue dos Lemas 6 e 7. □

5.3 O Teorema de Mordell

Para concluirmos a demonstração do Teorema de Mordell, precisamos das definições a seguir.

Definição 12. *Seja G um grupo abeliano aditivo. Dizemos que os elementos $g_1, g_2, \ldots, g_r$ em G são linearmente independentes se não há solução inteira $(m_1, m_2, \ldots, m_r)$ não-trivial para $m_1 g_1 + m_2 g_2 + \cdots + m_r g_r = 0$.*

Definição 13. *Seja $E : y^2 = x^3 + ax + b$ uma curva elíptica e $E(\mathbb{Q})$ seu grupo de pontos racionais. Definimos o posto $r_{\mathbb{Q}}(E)$ como o número máximo de elementos linearmente independentes de $E(\mathbb{Q})$.*

Precisamos ainda do seguinte teorema sobre grupos abelianos, encontrado na página 309 de [6].

Teorema 7 (Teorema da Classificação de Grupos Abelianos Finitamente Gerados)**.** *Seja G um grupo abeliano finitamente gerado e $\mathcal{T}$ seu subgrupo de torção. Então existe um inteiro $r \geq 0$ tal que*

$$G \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ vezes}} \oplus \mathcal{T}.$$

Se G é um grupo abeliano finito, então existem primos $p_1, \ldots, p_k$ e inteiros $n_1, \ldots, n_k \geq 1$ unicamente determinados tais que

$$G \cong \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \oplus \ldots \oplus \frac{\mathbb{Z}}{p_k^{n_k}\mathbb{Z}}.$$

Teorema 8 (Mordell)**.** *Sejam $E : y^2 = x^3 + ax + b$ uma curva elíptica, $E(\mathbb{Q})$ o seu grupo de pontos racionais e $\mathcal{T}$ seu subgrupo de torção. Então*

$$E(\mathbb{Q}) \cong \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{r \text{ vezes}} \oplus \mathcal{T}, \tag{5.9}$$

onde $r = r_{\mathbb{Q}}(E)$*, e existem primos* $p_1, \ldots, p_k$ *e inteiros* $n_1, \ldots, n_k \geq 1$ *unicamente determinados tais que*

$$\mathcal{T} \cong \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{p_k^{n_k}\mathbb{Z}}. \tag{5.10}$$

Demonstração. Temos que $E(\mathbb{Q})$ é um grupo abeliano aditivo. Pelo Teorema Fraco de Mordell e pelas Proposições 12, 13 e 14, temos que $h : E(\mathbb{Q}) \longmapsto [0, +\infty)$ é uma função que satisfaz as hipóteses do Teorema 4, logo $E(\mathbb{Q})$ é finitamente gerado. Segue do Teorema 7 que existe $r \geq 0$ tal que $E(\mathbb{Q})$ pode ser escrito como em (5.9).

Por (5.9), temos que $r_{\mathbb{Q}}(E) \geq r$. Se $r_{\mathbb{Q}}(E) > r$, então existem $g_1, \ldots, g_s$ em $E(\mathbb{Q})$ para algum $s > r$ tais que

$$m_1 g_1 + \cdots + m_s g_s = \mathcal{O} \Longleftrightarrow m_1 = \cdots = m_s = 0,$$

contrariando (5.9).

Sabemos do Teorema de Nagell-Lutz que $\mathcal{T}$ é finitamente gerado, logo existem primos $p_1, \ldots, p_k$ e inteiros $n_1, \ldots, n_k \geq 1$ unicamente determinados tais que $\mathcal{T}$ é como em (5.10). □

É fácil ver que $r_{\mathbb{Q}}(E) = 0$ se e somente se $E(\mathbb{Q})$ é um grupo finito, pois sabemos que o subgrupo de torção de $E(\mathbb{Q})$ é finito. Barry Mazur descreveu em 1975 as possibilidades para o subgrupo de torção de uma curva elíptica(veja [5]).

Teorema 9 (Mazur)**.** *Seja* E *uma curva elíptica e* $E(\mathbb{Q})$ *seu grupo de pontos racionais. Então seu subgrupo de pontos racionais* $E(\mathbb{Q})_{tor}$ *é isomorfo a um dos seguintes grupos:*

$$\frac{\mathbb{Z}}{m\mathbb{Z}},\ m = 1, \ldots, 10 \text{ ou } m = 12,$$

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}},\ m = 1, \ldots, 4.$$

Além disso, para cada grupo G *descrito acima, existe uma curva elíptica* E *tal que* $E(\mathbb{Q})_{tor} = G$.

Capítulo 6

O Posto de Curvas Elípticas

Mostramos no capítulo anterior que o grupo de pontos racionais de uma curva elíptica é finitamente gerado. Mas como saber quantos pontos são necessários para gerar, a menos de um conjunto finito, todos os pontos racionais? Esta pergunta não pode ainda ser respondida em toda a sua generalidade, mas neste capítulo apresentaremos um algoritmo para responder esta pergunta no caso específico em que a curva elíptica E é do tipo

$$E : y^2 = x^3 + Ax,\ A \in \mathbb{Q}. \tag{6.1}$$

Denotemos por simplicidade $\Gamma = E(\mathbb{Q})$, $\mathbf{0} = (0, 0)$ e $r = r_{\mathbb{Q}}(E)$ o posto da curva $E(\mathbb{Q})$. Pelo Teorema de Mordell

$$\Gamma = \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{r\ vezes} \oplus \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{p_k^{n_k}\mathbb{Z}},$$

onde p_j é primo e $n_j \geq 1$, $j = 1, ..., k$. Segue então que, se q é o número de elementos do conjunto $\{p_j,\ j = 1, ..., k;\ p_j = 2\}$,

$$\frac{\Gamma}{2\Gamma} \cong \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}}_{r\ vezes} \oplus \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}}_{q\ vezes}.$$

Podemos ainda mostrar que

$$[\Gamma : 2\Gamma] = 2^r.2^q,$$

onde $2^q = |\Gamma_2| = \sharp\{P \in \Gamma;\ 2P = \mathcal{O}_E\}$. De fato, sejam Q_j pontos na curva correspondentes aos geradores de $\mathbb{Z}/p_j^{n_j}\mathbb{Z}$, $j = 1, ..., k$, e P um ponto de Γ tal que $2P = \mathcal{O}$; como P é ponto de torção, devemos ter $P = \sum_{j=1}^{k} m_j Q_j$, onde $0 \leq m_j \leq p_j^{n_j} - 1$. Então

$$2P = \sum_{j=1}^{k} 2m_j Q_j = \mathcal{O} \Longleftrightarrow 2m_j \equiv 0 \bmod p_j^{n_j}.$$

Logo, para cada primo p_j ímpar devemos ter $m_j = 0$ e, para cada primo $p_j = 2$, podemos ter $m_j = 0$ ou $m_j = p_j^{n_j - 1}$.

Por outro lado, sabemos que se $P \in \Gamma$, $2P = \mathcal{O}$ se e somente se $P = \mathcal{O}$ ou $y(P) = 0$. Mas $f(x) = x^3 + Ax$ possui três raízes racionais se $-A \in \mathbb{Q}^{*2}$, e $f(x)$ possui apenas uma se $-A \notin \mathbb{Q}^{*2}$; logo

$$2^r = \frac{[\Gamma : 2\Gamma]}{|\Gamma_2|},\ |\Gamma_2| = \begin{cases} 4, \text{ se } -A \in \mathbb{Q}^{*2} \\ 2, \text{ caso contrário.} \end{cases} \tag{6.2}$$

Estudaremos mais detalhadamente a aplicação de duplicação de um ponto em Γ a fim de encontrarmos o valor de $[\Gamma : 2\Gamma]$, para podermos assim determinar o posto da curva elíptica.

Considere a nova curva elíptica $\overline{E}$ definida por $\overline{E} : y^2 = x^3 + \overline{A}x$, onde $\overline{A} = -4A$, $\overline{\Gamma} = \overline{E}(\mathbb{Q})$ e a aplicação $\phi : \Gamma \longmapsto \overline{\Gamma}$ definida por

$$\phi(P) = \begin{cases} \mathcal{O}_{\overline{E}}, \text{ se } P = \mathcal{O}_E \text{ ou } \mathbf{0} \\ (\overline{x}, \overline{y}) = \left(x + \dfrac{A}{x}, \dfrac{y}{x}\left(x - \dfrac{A}{x}\right)\right), \text{ se } P = (x, y) \neq \mathcal{O}_E, \mathbf{0}. \end{cases} \tag{6.3}$$

Considere ainda $\overline{\overline{E}}$ definida por $\overline{\overline{E}} : y^2 = x^3 + \overline{\overline{A}}x$, onde $\overline{\overline{A}} = 16A$, $\overline{\overline{\Gamma}} = \overline{\overline{E}}(\mathbb{Q})$ e a aplicação $\overline{\phi} : \overline{\Gamma} \longmapsto \overline{\overline{\Gamma}}$ definida analogamente por

$$\phi(\overline{P}) = \begin{cases} \mathcal{O}_{\overline{\overline{E}}}, \text{ se } P = \mathcal{O}_{\overline{E}} \text{ ou } \overline{\mathbf{0}} \\ (\overline{\overline{x}}, \overline{\overline{y}}) = \left(\overline{x} + \dfrac{A}{\overline{x}}, \dfrac{\overline{y}}{\overline{x}}\left(\overline{x} - \dfrac{A}{\overline{x}}\right)\right), \text{ se } \overline{P} = (\overline{x}, \overline{y}) \neq \mathcal{O}_{\overline{E}}, \overline{\mathbf{0}}. \end{cases}$$

Mostraremos que ϕ é homomorfismo de grupos na Proposição 15. Mais ainda, que a aplicação $P \longmapsto 2P$ em Γ pode ser escrita como a composição de ϕ, $\overline{\phi}$ e a aplicação

$$\psi : \overline{\overline{\Gamma}} \longrightarrow \Gamma$$

$$(x, y) \longmapsto \left(\frac{x}{4}, \frac{y}{8}\right),$$

que é isomorfismo de grupos. Podemos ilustrar esta composição com o seguinte diagrama:

$$\Gamma \xrightarrow{\phi} \overline{\Gamma} \xrightarrow{\overline{\phi}} \overline{\overline{\Gamma}} \overset{\psi}{\cong} \Gamma$$

Proposição 15. *A aplicação $\phi : \Gamma \longmapsto \overline{\Gamma}$ é um homomorfismo de grupos com* $\ker(\phi) = \{\mathcal{O}, \boldsymbol{0}\}$.

Demonstração. Vejamos primeiramente que ϕ está bem definida. Para isto basta observar que, se (x, y) pertence a Γ, então

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

Sejam P_1 e P_2 pontos de Γ; devemos mostrar que $\phi(P_1+P_2) = \phi(P_1)+\phi(P_2)$. Dividiremos a demonstração em casos.

Se $P_1 = \mathbf{0}$ e $P_2 = \mathbf{0}$ então $\phi(P_1 + P_2) = \phi(\mathcal{O}_E) = \mathcal{O}_{\overline{E}}$ e $\phi(\mathbf{0}) + \phi(\mathbf{0}) = \mathcal{O}_{\overline{E}} + \mathcal{O}_{\overline{E}} = \mathcal{O}_{\overline{E}}$ e o teorema está demonstrado neste caso.

Se $P_1 = \mathbf{0}$ e $P_2 = (x_2, y_2) \neq \mathbf{0}$, vemos através de (3.5) que

$$P_1 + P_2 = \left(\frac{A}{x_2}, -\frac{Ay_2}{x_2^2}\right)$$

e, pela definição de ϕ, $\phi(P_1 + P_2) = (\overline{x}(P_1 + P_2), \overline{y}(P_1 + P_2))$ onde

$$\overline{x}(P_1 + P_2) = \frac{y_2^2}{x_2^2} = \overline{x}(P_2),$$

$$\overline{y}(P_1 + P_2) = \frac{-\frac{Ay_2}{x_2^2}\left(\left(\frac{A}{x_2^2}\right)^2 - A\right)}{(A/x_2)^2} = \frac{y_2(x^2 - A)}{x_2^2} = \overline{y}(P_2).$$

Suponha $P_1 \neq \mathbf{0}$. Vejamos agora que, se $P = (x, y)$ é um elemento de Γ,

$$\phi(-P) = \phi(x, -y) = \left(\left(\frac{-y}{x} \right)^2, \frac{-y(x^2 - A)}{x^2} \right) = \left(\left(\frac{y}{x} \right)^2, \frac{-y(x^2 - A)}{x^2} \right) = -\phi(P).$$

Logo, para concluir a demonstração, basta mostrarmos que $\phi(P_1) + \phi(P_2) + \phi(P_3) = \mathcal{O}_{\overline{E}}$ sempre que $P_1 + P_2 + P_3 = \mathcal{O}_E$, pois teremos assim que se $P_1, P_2 \in \Gamma$ e P_3 é tal que $P_1 + P_2 + P_3 = \mathcal{O}_E$, então

$$\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2).$$

Sejam então P_1, P_2 e P_3 pontos de Γ tais que $P_1 + P_2 + P_3 = \mathcal{O}_E$. Vamos supor ainda que $P_j \neq \mathbf{0}$ e $P_j \neq \mathcal{O}_E$, $j = 1, 2, 3$, já que estes casos foram tratados anteriormente. Por hipótese existe uma reta $y = \lambda x + \nu$ que contém estes três pontos; mostraremos que $\phi(P_1), \phi(P_2), \phi(P_3)$ pertencem à reta $y = \overline{\lambda} x + \overline{\nu}$, onde

$$\overline{\lambda} = \frac{\nu\lambda - A}{\nu}, \ \overline{\nu} = \frac{\nu^2 + A\lambda^2}{\nu}.$$

Lembramos que $\nu \neq 0$ pois $P_j \neq \mathbf{0}$, $j = 1, 2, 3$. Denotando $\phi(P_j) = (\overline{x}_j, \overline{y}_j)$, $j = 1, 2, 3$, e usando a definição de ϕ temos de fato que

$$\overline{\lambda}\overline{x}_j + \overline{\nu} = \frac{\nu\lambda - A}{\nu} \left(\frac{\overline{y}_j}{\overline{x}_j} \right)^2 + \frac{\nu^2 + A\lambda^2}{\nu} = \frac{\nu\lambda y_j^2 - A(y_j^2 - \lambda^2 x_j^2) + \nu^2 x_j^2}{\nu x_j^2},$$

logo,

$$\overline{\lambda}\overline{x}_j + \overline{\nu} = \frac{\nu\lambda(x_j^3 + Ax_j) - A\nu(y_j + \lambda x_j) + \nu^2 x_j^2}{\nu x_j^2} = \frac{x_j^2(\lambda x_j + \nu) - Ay_j}{x_j^2} = \frac{y_j(x_j^2 - A)}{x_j^2} = \overline{y_j},$$

para $j = 1, 2, 3$. Logo $\phi(P_1), \phi(P_2), \phi(P_3)$ são colineares.

Finalmente, vemos diretamente da definição que $\ker \phi = \{\mathcal{O}_E, \mathbf{0}\}$. □

Proposição 16. *A aplicação* $\Phi : \Gamma \longrightarrow \Gamma$ *definida por* $\Phi = \psi \circ \overline{\phi} \circ \phi$ *satisfaz* $\Phi(P) = 2P$, $\forall P \in \Gamma$.

Demonstração. A demonstração deste resultado é simples, porém trabalhosa. Das definições acima vemos que, se $P = (x, y)$ é um ponto de Γ com $y \neq 0$,

$$\Phi(P) = \psi \circ \overline{\phi}\left(\frac{y^2}{x^2}, \frac{y(x^2 - A)}{x^2}\right) = \psi\left(\frac{\left(\frac{y(x^2-A)}{x^2}\right)^2}{\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-A)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 + 4A\right)}{\left(\frac{y^2}{x^2}\right)^2}\right),$$

isto é,

$$\Phi(P) = \left(\frac{\left(\frac{y(x^2-A)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-A)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 + 4A\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right).$$

Logo

$$\Phi(P) = \left(\frac{(x^2 - A)^2}{4y^2}, \frac{x^6 + 5Ax^4 - 5A^2x^2 - A^3}{8y^3}\right).$$

Por outro lado, das fórmulas de (3.6) temos que

$$x(2P) = \frac{x^4 - 2Ax + A^2}{4y^2} \text{ e}$$

$$y(2P) = -(\lambda x(2P) + \nu), \text{ onde } \lambda = \frac{3x^2 + A}{2y}, \text{ e } \nu = y - \lambda x = \frac{-4x^6 + 4A^2x^2}{8y^3}.$$

Obtemos assim $\Phi(P) = (x(2P), y(2P))$, como gostaríamos. □

Pelo Teorema Fraco de Mordell e pela seguinte inclusão de grupos

$$\Gamma \supseteq \overline{\phi}(\overline{\Gamma}) \supseteq \overline{\phi}(\phi(\Gamma)) \cong 2\Gamma,$$

temos que

$$[\Gamma : 2\Gamma] = [\Gamma : \overline{\phi}(\overline{\Gamma})][\overline{\phi}(\overline{\Gamma}) : 2\Gamma]. \tag{6.4}$$

Reescreveremos o lado direito de (6.4) através do seguinte resultado, encontrado na página 27 do livro [1].

Lema 8. *Sejam G um grupo abeliano, H um subgrupo de G e $f : G \longrightarrow G'$ um homomorfismo de grupos. Se o índice $[G : H]$ é finito, então $[f(G) : f(H)]$ e $[\ker f : \ker f \cap H]$ também o são. Mais ainda,*

$$[f(G) : f(H)] = \frac{[G : H]}{[\ker\ f : \ker f \cap H]}.$$

Aplicando o lema com $G = \overline{\Gamma}$, $H = \phi(\Gamma)$ e $f = \overline{\phi}$, temos que

$$[\overline{\phi}(\overline{\Gamma}) : 2\Gamma] = [\overline{\phi}(\overline{\Gamma}) : \overline{\phi}(\phi(\Gamma))] = \frac{[\overline{\Gamma} : \phi(\Gamma)]}{[\ker \overline{\phi} : \ker \overline{\phi} \cap \phi(\Gamma)]},$$

e de (6.4) segue que

$$[\Gamma : 2\Gamma] = \frac{[\Gamma : \overline{\phi}(\overline{\Gamma})][\overline{\Gamma} : \phi(\Gamma)]}{[\ker \overline{\phi} : \ker \overline{\phi} \cap \phi(\Gamma)]}. \tag{6.5}$$

Simplificaremos a expressão acima com a proposição a seguir.

Proposição 17. *Seja $\phi : \Gamma \longrightarrow \overline{\Gamma}$ como em (6.3). Um ponto $(\overline{x}, \overline{y}) \in \overline{\Gamma}$, $\overline{x} \neq 0$, pertence à imagem $\phi(\Gamma)$ se e somente se $\overline{x} \in \mathbb{Q}^{*2}$. Além disso, $\boldsymbol{0} \in \phi(\Gamma)$ se e somente se $-A \in \mathbb{Q}^{*2}$.*

Demonstração. Seja $(\overline{x}, \overline{y}) \in \overline{\Gamma}$, $\overline{x} \neq 0$. Segue diretamente da definição que se $(\overline{x}, \overline{y}) \in \phi(\Gamma)$, então $\overline{x} \in \mathbb{Q}^{*2}$. Por outro lado, se $\overline{x} = t^2$, $t \in \mathbb{Q}^*$, definimos $P = (x, y)$, onde

$$x = \frac{1}{2}\left(\overline{x} + \frac{\overline{y}}{t}\right),\ y = tx.$$

Então

$$x^3 + Ax = x(x^2 + A) = x\left(\frac{1}{4}\left(\overline{x}^2 + 2\overline{x}\frac{\overline{y}}{t} + \frac{\overline{y}^2}{t^2}\right) + A\right) = x\left(\frac{\overline{x}^2t^2 + 2\overline{x}\overline{y}t + \overline{y}^2 + 4At^2}{4t^2}\right),$$

logo

$$x^3 + Ax = x\left(\frac{\overline{x}^3 + 2\overline{x}\overline{y}t + \overline{y}^2 + 4A\overline{x}}{4\overline{x}}\right).$$

Mas $\overline{y}^2 = \overline{x}^3 + \overline{A}\overline{x} = \overline{x}^3 - 4A\overline{x}$, logo

$$x^3 + Ax = x\frac{\overline{x}^3 + 2\overline{x}\overline{y}t + \overline{x}^3}{4\overline{x}} = \frac{1}{2}x(\overline{x}^2 + \overline{y}t) = \frac{1}{2}x\overline{x}(\overline{x} + \frac{\overline{y}}{t}) = \overline{x}x^2 = (tx)^2 = y^2,$$

portanto (x, y) é de fato um ponto de Γ. Além disso,

$$x(\phi(P)) = x + \frac{A}{x} = \frac{x^3 + Ax}{x^2} = \frac{y^2}{x^2} = \frac{(tx)^2}{x^2} = t^2 = \overline{x},$$

logo $\phi(x, y)$ coincide com $(\overline{x}, \overline{y})$, exceto possivelmente pelo sinal da coordenada y. Mas $y(\phi(x, -y)) = -y(\phi(x, y))$, portanto $(\overline{x}, \overline{y}) \in \phi(\Gamma)$.

Note que, se $(x, y) \in \Gamma$,

$$\phi(x, y) = \left(\frac{x^3 + Ax}{x^2}, \frac{y}{x}\left(x - \frac{A}{x}\right)\right) = \left(\frac{y^2}{x^2}, \frac{y}{x}\left(x - \frac{A}{x}\right)\right).$$

Logo $\mathbf{0} \in \phi(\Gamma)$ se, e somente se existe um ponto $P = (x, 0)$ em Γ com $x \neq 0$; mas isto ocorre se, e somente se $-A \in \mathbb{Q}^{*2}$, concluindo a demonstração. □

Segue pelas Proposições 15 e 17 que

$$[\ker \overline{\phi} : \ker \overline{\phi} \cap \phi(\Gamma)] = \begin{cases} 1, \text{ se } -A \in \mathbb{Q}^{*2} \\ 2, \text{ caso contrário.} \end{cases} \tag{6.6}$$

Desse modo, substituindo a equação (6.5) em (6.2) e usando (6.6), temos que

$$2^r = \frac{[\Gamma : \overline{\phi}(\overline{\Gamma})][\overline{\Gamma} : \phi(\Gamma)]}{4} \tag{6.7}$$

Apresentaremos agora um método para encontrar indiretamente o valor de $[\Gamma : \overline{\phi}(\overline{\Gamma})]$ e $[\overline{\Gamma} : \phi(\Gamma)]$. Defina a aplicação $\alpha : \Gamma \longmapsto \mathbb{Q}^*/\mathbb{Q}^{*2}$ por

$$\alpha(P) = \begin{cases} \beta(1), \text{ se } P = \mathcal{O} \\ \beta(A), \text{ se } P = \mathbf{0} \\ \beta(x(P)), \text{ se } P \neq \mathcal{O}, \mathbf{0}, \end{cases} \tag{6.8}$$

onde $\beta : \mathbb{Q}^* \longmapsto \mathbb{Q}^*/\mathbb{Q}^{*2}$ é o homomorfismo canônico.

Proposição 18. *A aplicação α é um homomorfismo de grupos e* $\ker \alpha = \overline{\phi}(\overline{\Gamma})$.

Demonstração. Segue diretamente da definição que $\alpha(P) = \alpha(-P)$ para todo P em Γ; basta então mostrarmos que $\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$ sempre que $P_1, P_2, P_3 \in \Gamma$ são pontos tais que $P_1 + P_2 + P_3 = \mathcal{O}$.

Sejam $P_j = (x_j, y_j) \in \Gamma\backslash\{\mathcal{O}\}$, $j = 1, 2, 3$, pontos tais que $P_1 + P_2 + P_3 = \mathcal{O}$. Existe uma reta $y = mx + k$ contendo estes três pontos e

$$(mx + k)^2 = x^3 + Ax \iff x^3 - m^2x^2 + (A - 2mk)x - k^2 = 0. \tag{6.9}$$

Se $x_1x_2x_3 \neq 0$ então $x_1x_2x_3 = k^2$ e

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \beta(x_1)\beta(x_2)\beta(x_3) = \beta(x_1x_2x_3) = \beta(k^2) = 1.$$

Se $x_j = 0$ para algum $j = 1, 2, 3$, digamos $x_3 = 0$, teremos que $k = 0$ e, de (6.9),

$$x(x^2 - m^2x + A) = 0,$$

logo $x_1x_2 = A$ e

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \beta(x_1)\beta(x_2)\beta(A) = \beta(x_1x_2)\beta(A) = \beta(A)\beta(A) = 1,$$

como gostaríamos. A segunda afirmação segue diretamente da Proposição 17. □

Ilustramos os homomorfismos definidos nesta seção da seguinte maneira:

$$\begin{array}{ccccccc} \Gamma & \xrightarrow{\phi} & \overline{\Gamma} & \xrightarrow{\overline{\phi}} & \overline{\overline{\Gamma}} & \overset{\psi}{\cong} & \Gamma \\ \downarrow \alpha & & \downarrow \overline{\alpha} & & & & \\ \mathbb{Q}^*\backslash\mathbb{Q}^{*2} & & \mathbb{Q}^*\backslash\mathbb{Q}^{*2} & & & & \end{array}$$

Usando a Proposição 18 e a equação (6.7) temos que

$$2^r = \frac{|\alpha(\Gamma)||\overline{\alpha}(\overline{\Gamma})|}{4}, \tag{6.10}$$

onde $\overline{\alpha} : \overline{\Gamma} \longmapsto \mathbb{Q}^*/\mathbb{Q}^{*2}$ é definido analogamente. Vejamos agora como determinar os elementos dos conjuntos $\alpha(\Gamma)$ e $\overline{\alpha}(\overline{\Gamma})$, e em particular a sua ordem.

Proposição 19. *O grupo $\alpha(\Gamma)$ é composto por:*

(a) $1, \beta(A)$*;*

(b) $\beta(\widehat{x}), -\beta(\widehat{x})$*, se $x^2 = -A$ tem solução $\widehat{x} \in \mathbb{Z}$;*

(c) $\beta(d)$*, onde d é um divisor de A tal que a equação*

$$dS^4 + \frac{A}{d}T^4 = U^2 \tag{6.11}$$

tem solução inteira (S, T, U) onde

$$S, T \geq 1 \text{ e } mdc\left(\frac{A}{d}, S\right) = 1 \tag{6.12}$$

Demonstração. Vejamos primeiramente que $\alpha(\Gamma)$ está contido no conjunto descrito nos ítens (a), (b) e (c), que denotaremos por $\mathcal{B}$. Claramente $\alpha(\Gamma_2) \subseteq \mathcal{B}$, pois a imagem destes elementos são exatamente aqueles descritos nos itens (a) e (b). Seja $P = (x, y)$ em $\Gamma \setminus \Gamma_2$, onde $x = \dfrac{s}{T^2}$, $y = \dfrac{u}{T^3}$ com $\text{mdc}(s, T) = \text{mdc}(u, T) = 1$ e $T > 0$. Note que devemos ter u e s não nulos.

Seja $d = \text{mdc}(A, s)$ e escreva $A = dA_1$ e $s = ds_1$, onde o sinal de d é escolhido de modo que $s_1 > 0$. Da equação da curva temos

$$\frac{u^2}{T^6} = \frac{s^3}{T^6} + A\frac{s}{T^2} \iff u^2 = s^3 + AsT^4,$$

logo $d \mid u$; escrevendo $u = du_1$ temos que

$$d^2u_1^2 = d^3s_1^3 + dA_1ds_1T^4 \iff u_1^2 = ds_1^3 + A_1s_1T^4,$$

logo

$$u_1^2 = s_1(ds_1^2 + A_1T^4). \tag{6.13}$$

Note que $\text{mdc}(s_1, ds_1^2 + A_1T^4) = 1$ pois $\text{mdc}(s_1, A_1) = 1$. Segue de (6.13) que s_1 e $ds_1^2 + A_1T^4$ são quadrados e escrevemos

$$s_1 = S^2,\ S > 0,\ \text{e}\ ds_1^2 + A_1T^4 = U^2.$$

Então

$$dS^4 + \frac{A}{d}T^4 = U^2$$

tem solução inteira (S, T, U) satisfazendo (6.12). Além disso,

$$\alpha(P) = \beta(x(P)) = \beta\left(\frac{ds_1}{T^2}\right) = \beta\left(\frac{dS^2}{T^2}\right) = \beta(d).$$

Por outro lado, é claro que $\{\beta(1), \beta(A)\} \subseteq \alpha(\Gamma)$ e, se $x^2 - A = 0$ tem solução inteira $\hat{x}$, $\{\pm\beta(\hat{x})\} \subseteq \alpha(\Gamma)$. Se d é um divisor de A tal que (6.11) tem solução inteira (S, T, U) satisfazendo (6.12), então definindo $P = \left(\frac{dS^2}{T^2}, \frac{dUS}{t^3}\right)$ temos

$$U^2 = dS^4 + \frac{A}{d}T^4 \iff d^2U^2 = d^3S^4 + dAT^4 \iff d^2U^2S^2 = d^3S^6 + dAS^2T^4,$$

logo

$$\frac{d^2U^2S^2}{T^6} = \frac{d^3S^6}{T^6} + \frac{AdS^2}{T^2} \iff \left(\frac{dUS}{t^3}\right)^2 = \left(\frac{dS^2}{T^2}\right)^3 + A\left(\frac{dS^2}{T^2}\right),$$

como gostaríamos. □

6.1 Curvas Elípticas do tipo $y^2 = x^3 - px$, p primo

Na seção anterior determinamos um algoritmo para calcular o posto de uma classe de curvas elípticas. Agora vamos nos restringir um pouco mais para poder aplicá-lo de fato, uma vez que nem sempre é possível decidir sobre a existência de soluções de equações diofantinas. Nesta seção nos baseamos nos artigos [4] e [9] para estudarmos curvas elípticas da forma

$$y^2 = x^3 - px,\ p \text{ primo}. \tag{6.14}$$

Proposição 20. *Sejam p um primo, $E : y^2 = x^3 - px$, $\Gamma = E(\mathbb{Q})$ seu grupo de pontos racionais e $\mathcal{T}$ seu subgrupo de torção. Então $\mathcal{T} \cong \mathbb{Z}/2\mathbb{Z}$.*

Demonstração. Seja $P = (x, y) \in \Gamma$, $P \neq \mathcal{O}, \mathbf{0}$. Sabemos do Teorema de Nagell-Lutz que $x, y \in \mathbb{Z}$ e $y^2 \mid \Delta = 4p^3$ são condições necessárias para que P seja um ponto de torção; vejamos que os pontos satisfazendo estas condições não pertencem a $\mathcal{T}$.

Seja $P = (x, y) \in \Gamma$ tal que $x, y \in \mathbb{Z}$ e $y^2 \mid \Delta = 4p^3$. Como $y^2 \mid 4p^3$ então $y^2 = 1, 4, p^2$ ou $4p^2$. Note que $y^2 = x^3 - px = x(x^2 - p)$, onde x e $x^2 - p$ são números inteiros.

Se $y^2 = 1$ temos uma única solução $(p, x) = (2, -1)$. Se $y^2 = 4$ temos três soluções: $(p, x) = (2, 2), (5, -1)$ ou $(17, -4)$. Para os casos $y^2 = p^2$ e $y^2 = 4p^2$, temos que $x = pt$, $t \in \mathbb{Z}$. Fixando $y^2 = p^2$, obtemos $t(pt^2 - 1) = 1$ e temos assim uma única solução $(p, x) = (2, 2)$. Para $y^2 = 4p^2$, analogamente temos que $t(pt^2 - 1) = 4$ e existe também uma única solução $(p, x) = (5, 5)$.

Vemos acima que apenas três curvas possuem pontos diferentes de $\mathcal{O}$ e $\mathbf{0}$ candidatos à pontos de torção:

- $y^2 = x^3 - 2x$ e os pontos $(-1, -1), (-1, 1), (2, 2)$ e $(2, -2)$;
- $y^2 = x^3 - 5x$ e os pontos $(-1, 2), (-1, -2), (5, 10)$ e $(5, -10)$;
- $y^2 = x^3 - 17x$ e os pontos $(-4, 2)$ e $(-4, -2)$.

Mas usando (3.6) vemos que, em cada um destes casos, $2P$ não possui coordenadas inteiras e portanto $2P \notin \mathcal{T}$. Segue que os únicos pontos de torção para curvas do tipo (6.14) são $\mathcal{O}$ e $\mathbf{0}$. □

Teorema 10. *Seja $E : y^2 = x^3 - px$ uma curva elíptica, p um primo ímpar da forma $p = u^4 + v^4$, u, v inteiros. Então $E(\mathbb{Q}) \cong \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.*

Cabe ressaltar que todo primo de Fermat $p = 2^{2^n} + 1$ com $n \geq 2$ é da forma $p = u^4 + v^4$, $u, v \in \mathbb{Z}$.

Demonstração. Pela Proposição 20 o subgrupo de torção de Γ é isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Usaremos a equação (6.10) e, com a mesma notação, a Proposição 19 para demonstrar que o posto de $E(\mathbb{Q})$ é 2.

Suponha sem perda de generalidade que u e v são inteiros positivos. Sabemos que $x^2 = p$ não tem soluções inteiras. Devemos determinar para quais divisores d de $A = -p$ a equação (6.11) tem solução (S, T, U) satisfazendo (6.12), mas como já sabemos que $\{\beta(1), \beta(-p)\}$ está contido em $\alpha(\Gamma)$, será necessário verificar apenas se $\beta(-1), \beta(p) \in \alpha(\Gamma)$. Para $d = p$, a equação $pS^4 - T^4 = U^2$ tem solução $(S, T, U) = (1, v, u^2)$ satisfazendo claramente (6.12). Como $\alpha(\Gamma)$ é um grupo, $\beta(p)\beta(-p) = \beta(-1) \in \alpha(\Gamma)$ e então $|\alpha(\Gamma)| = 4$.

Para encontrar o valor de $|\overline{\alpha}(\overline{\Gamma})|$, para cada divisor d de $\overline{A} = 4p$ devemos verificar se $dS^4 + \frac{4p}{d}T^4 = U^2$ possui solução. Claramente para $d < 0$ tal equação não tem solução e, além disso, $\beta(\{1, 2, 4, p, 2p, 4p\}) = \{\beta(1), \beta(2), \beta(p), \beta(2p)\}$. Novamente, sabemos que $\{1, \beta(p)\} \subseteq \overline{\alpha}(\overline{\Gamma})$ e, ao mostrarmos que $\beta(2) \in \overline{\alpha}(\overline{\Gamma})$, teremos que $\beta(2p) \in \overline{\alpha}(\overline{\Gamma})$. De fato, para $d = 2$, a equação $2S^4 + 2pT^4 = U^2$ possui solução $(S, T, U) = (u - v, 1, 2u^2 - 2uv + 2v^2)$ e, supondo sem perda de generalidade que $u > v$, temos que tal solução satisfaz (6.12): se $2 \mid (u - v)$ então u e v têm a mesma paridade e assim $2 \mid p$, um absurdo; se $p \mid (u - v)$ então

$$u \equiv v \pmod{p} \Longrightarrow 0 \equiv p \equiv u^4 + v^4 \equiv 2u^4 \pmod{p},$$

e como p não divide 2 teríamos que p é divisor de u e v, absurdo pois p é primo.

Segue então que $|\overline{\alpha}(\overline{\Gamma})| = 4$ e, pela equação (6.10), o posto r da curva é 2. □

Teorema 11. *Seja $E : y^2 = x^3 - px$ uma curva elíptica, p um primo de Mersenne. Então*

$$\Gamma = \begin{cases} \mathbb{Z}/2\mathbb{Z}, \text{ se } p = 3 \\ \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \text{ se } p > 3. \end{cases}$$

Demonstração. Pela Proposição 20, o subgrupo de torção de uma curva deste tipo é isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Para determinar o posto destas curvas, usaremos novamente, com a mesma notação, a Proposição 19.

Seja $p = 3$. Já sabemos que $\{\beta(1), \beta(-3)\} \subseteq \alpha(\Gamma)$ e $x^2 = 3$ não tem solução inteira. Devemos portanto verificar se $\beta(-1), \beta(3) \in \alpha(\Gamma)$. Como $\alpha(\Gamma)$ é grupo, temos que $\beta(-1) \in \alpha(\Gamma)$ se e somente se $\beta(3) \in \alpha(\Gamma)$.

Note que para $d = -1$ a equação $dS^4 - \frac{p}{d}T^4 = U^2$ não tem solução: se $-S^4 + 3T^4 = U^2$ tem solução inteira, teremos que $-S^4 \equiv U^2 \equiv 1 \pmod 3$ pelo Pequeno Teorema de Fermat; mas isto é impossível pois $(S^2)^2 \equiv -1 \pmod 3$ não tem solução. Logo $\beta(-1) \notin \alpha(\Gamma)$ e portanto $\alpha(\Gamma) = \{\beta(1), \beta(-3)\}$.

Para encontrar o valor de $\overline{\alpha}(\overline{\Gamma})$, observamos que para d divisor negativo de 12, a equação $dS^4 + \frac{12}{d}T^4 = U^2$ não tem solução, logo $\overline{\alpha}(\overline{\Gamma}) \subseteq \beta(\{1, 2, 3, 4, 6, 12\}) = \{\beta(1), \beta(2), \beta(3), \beta(6)\}$. Já sabemos que $\{\beta(1), \beta(3)\} \subseteq \overline{\alpha}(\overline{\Gamma})$, logo devemos verificar se $\beta(2), \beta(6) \in \overline{\alpha}(\overline{\Gamma})$ onde, analogamente, $\beta(2) \in \overline{\alpha}(\overline{\Gamma})$ se e somente se $\beta(6) \in \overline{\alpha}(\overline{\Gamma})$.

Para $d = 2$, se $2S^4 + 6T^4 = U^2$ tem solução satisfazendo (6.12), temos, pelo Pequeno Teorema de Fermat, que

$$2S^4 \equiv U^2 \pmod 3 \iff 2(S^2)^2 \equiv U^2 \pmod 3 \iff 2 \equiv 1 \pmod 3),$$

um absurdo. Portanto, $\beta(2) \notin \overline{\alpha}(\overline{\Gamma})$ e, por (6.10), temos que o posto r da curva é 0.

Seja agora $p = 2^q - 1$ um primo de Mersenne, $q > 2$. Devemos ter q primo também, pois se $t \mid q$, $1 < t < p$, teríamos que $(2^t - 1)$ divide p. Para encontrar o valor de $|\alpha(\Gamma)|$, como já sabemos que $\{\beta(1), \beta(-p)\} \subseteq \alpha(\Gamma)$, devemos verificar se $\beta(-1), \beta(p) \in \alpha(\Gamma)$. Como $\alpha(\Gamma)$ é grupo, $\beta(-1) \in \alpha(\Gamma)$ se e somente se $\beta(p) \in \alpha(\Gamma)$.

Para $d = -1$, vemos que a equação $dS^4 - \frac{p}{d}T^4 = U^2$ não tem solução, pois teríamos assim que

$$-S^4 \equiv U^2 \pmod p \iff -1 \equiv (U(S^{-1})^2)^2 \pmod p),$$

impossível pois -1 não é resíduo quadrático módulo p, para $p > 3$ primo de Mersenne; a demonstração deste fato pode ser encontrada no livro [1]. Segue que $|\alpha(\Gamma)| = 2$.

Sabemos que a equação $dS^4 + \frac{4p}{d}T^4 = U^2$ não tem solução para d divisor negativo de $4p$ e, da Proposição 19, que $\{\beta(1), \beta(4p)\} \subseteq \overline{\alpha}(\overline{\Gamma})$. Como $\overline{\alpha}(\overline{\Gamma})$ é subgrupo de

$$\beta(\{1, 2, 4, p, 2p, 4p\}) = \{\beta(1), \beta(2), \beta(p), \beta(2p)\},$$

resta verificar se $\beta(2), \beta(2p) \in \overline{\alpha}(\overline{\Gamma})$, onde $\beta(2) \in \overline{\alpha}(\overline{\Gamma})$ se e somente se $\beta(2p) \in \overline{\alpha}(\overline{\Gamma})$. A equação $2S^4 + 2pT^4 = U^2$ tem solução $(S, T, U) = (1, 1, 2^{(q+1)/2})$ satisfazendo claramente (6.12), logo $\overline{\alpha}(\overline{\Gamma}) = \{\beta(1), \beta(2), \beta(p), \beta(2p)\}$. Finalmente, pela equação (6.10), temos que o posto r da curva é 1, como gostaríamos. □

6.2 Curvas Elípticas do tipo $y^2 = x^3 - 2px$, p primo

Nesta seção determinaremos qual a estrutura do grupo de pontos racionais de curvas elípticas do tipo

$$E : y^2 = x^3 - 2px, \ p \text{ primo tal que } 2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4, \ u, v \in \mathbb{Z}. \tag{6.15}$$

O texto desta seção é baseado no artigo [10].

Proposição 21. *Seja E uma curva elíptica do tipo* (6.15) *e $\mathcal{T}$ o subgrupo de torsão do seu grupo de pontos racionais. Então $\mathcal{T} \cong \mathbb{Z}/2\mathbb{Z}$.*

Para demonstrar este resultado, faremos a redução desta curva módulo p, isto é, estudaremos a curva elíptica definida pela mesma equação sobre $\mathbb{F}_p$, $p \neq 2, 3$:

$$\overline{E}(\mathbb{F}_p) : Y^2Z = X^3 - \overline{2p}XZ^2 = \{[\overline{a} : \overline{b} : \overline{c}] \in \mathbb{P}^2(\mathbb{F}_p); \ \overline{b}^2\overline{c} = \overline{a}^3 - \overline{2pa}\overline{c}^2\}.$$

Faremos esta redução módulo primos p que não dividem o discriminante da curva, de modo que a curva elíptica sobre $\mathbb{F}_p$ é não singular.

Seja $P \in E(\mathbb{Q})$. Temos que existem únicos inteiros a, b e c relativamente primos tais que $P = [a : b : c]$. Se $\overline{a}, \overline{b}$ e $\overline{c}$ denotam, respectivamente, as classes de a, b e c módulo p, temos que $\phi : \ P = [a : b : c] \in \mathcal{T} \longmapsto \overline{P} = [\overline{a} : \overline{b} : \overline{c}] \in \overline{E}(\mathbb{F}_p)$ é homomorfismo de grupos, pois esta aplicação preserva retas. Além disso, $\ker(\phi) = \{\mathcal{O}_E\}$, pois, se $P \in \mathcal{T} \setminus \{\mathcal{O}\}$, segue do Teorema de Nagell-Lutz que existem a e b inteiros tais que $P = [a : b : 1]$; portanto $\phi(P) = [\overline{0} : \overline{1} : \overline{0}]$ se e somente se $P = \mathcal{O}_E$. Segue do Teorema de Isomorfismos que $\mathcal{T}$ é isomorfo a um subgrupo de $\overline{E}(\mathbb{F}_p)$, e portanto $|\mathcal{T}|$ divide $|\overline{E}(\mathbb{F}_p)|$.

Podemos agora demosntrar a Proposição 21.

Demonstração. Temos que 3 e 5 não podem ser escritos na forma acima, logo não dividem o discriminante $\Delta = 2^5 p^3$ da curva. Fazendo a redução módulo 3 da curva, temos que ela se reduz a $\overline{E} : y^2 = x^3 - x$ ou $\overline{E} : y^2 = x^3 - \overline{2}x$; é possível verificar que ambas as curvas possuem 4 pontos sobre o corpo $\mathbb{F}_3$. Fazendo a redução mod 5, a curva é reduzida a $\overline{E} : y^2 = x^3 - \overline{2}x$, pois $2p = (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4 \equiv 1 + 1 \equiv 2 \pmod 5$, pelo Pequeno Teorema de Fermat; esta curva possui 10 pontos sobre $\mathbb{F}_5$. Como $|\mathcal{T}|$ divide $\overline{E}(\mathbb{F}_p)$ para todo primo que não divide $\Delta = 2^5 p^3$, temos que $|\mathcal{T}| \leq 2$; como $\{\mathcal{O}, \mathbf{0}\} \subseteq \mathcal{T}$, segue que $\mathcal{T} \cong \mathbb{Z}/2\mathbb{Z}$. □

Teorema 12. *Seja E uma curva elíptica do tipo* (6.15)*. Então $r_{\mathbb{Q}}(E) = 3$.*

Demonstração. Utilizaremos novamente a Proposição 19, com a mesma notação. Sabemos que $\{\beta(1), \beta(-2p)\} \subseteq \alpha(\Gamma)$ e que $x^2 - 2p = 0$ não tem solução inteira, logo devemos verificar apenas se $\beta(-1), \beta(2), \beta(-2), \beta(p), \beta(-p), \beta(2p) \in \alpha(\Gamma)$.

Seja $A = -2p$. Note que, para $d = -1$, a equação $dS^4 + \frac{A}{d}T^4 = U^2$ possui uma solução $(S, T, U) = (u^2 + 2v^2, 1, (u^2 + 2v^2)^2)$ satisfazendo (6.12): de fato, temos $\text{mdc}(2p, u^2 + 2v^2) = 1$, pois se $2 \mid (u^2 + 2v^2)$ teríamos que $2 \mid u$ e assim $2^4 \mid (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4 = 2p$, impossível; se $p \mid (u^2 + 2v^2)$ então teríamos de (6.15) que $p \mid (u^2 - 2v^2)$, e assim

$$p^4 \mid (u^2 + 2v^2)^4 + (u^2 - 2v^2)^4 = 2p,$$

impossível. Logo $\beta(-1) \in \alpha(\Gamma)$.

Para $d = p$, é possível verificar que $(S, T, U) = (1, 2uv, u^4 - 4v^4)$ é solução de (6.11) satisfazendo $1, 2uv \geq 1$ e $\text{mdc}(-2, 1) = 1$; logo $\beta(p) \in \alpha(\Gamma)$. Como $\alpha(\Gamma)$ é um grupo, temos que $\beta(-p), \beta(2p), \beta(2)$ e $\beta(-2)$ também pertencem a $\alpha(\Gamma)$, pois $\beta(-p) = \beta(-1)\beta(p)$, $\beta(2p) = \beta(-1)\beta(-2p)$, $\beta(2) = \beta(-2p)\beta(-p)$ e $\beta(-2) = \beta(-2p)\beta(p)$. Portanto $|\alpha(\Gamma)| = 8$.

Para encontrar o valor de $|\overline{\alpha}(\overline{\Gamma})|$, observamos que a equação $dS^4 + \frac{8p}{d}T^4 = U^2$ não possui solução (S, T, U) inteira para $d < 0$, logo

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \beta(\{1, 2, 4, 8, p, 2p, 4p, 8p\}) = \{\beta(1), \beta(2), \beta(p), \beta(2p)\}.$$

Já sabemos que $\beta(1), \beta(2p) \in \overline{\alpha}(\overline{\Gamma})$, logo basta verificar se $\beta(2), \beta(p) \in \overline{\alpha}(\overline{\Gamma})$, onde $\beta(2) \in \overline{\alpha}(\overline{\Gamma})$ se e somente se $\beta(p) \in \overline{\alpha}(\overline{\Gamma})$.

Para $d = 8$, temos que $8S^4 + pT^4 = U^2$ possui solução $(S, T, U) = (u^2, 1, 3u^4 + 4v^4)$ satisfazendo $\text{mdc}(p, u^2) = 1$: se $p \mid u^2$ então, como $2p = 16v^8 + 24u^4v^4 + u^8$, temos que $p \mid v$ e portanto p^8 divide $16v^8 + 24u^4v^4 + u^8 = 2p$, impossível. Segue que $\beta(2) \in \overline{\alpha}(\overline{\Gamma})$ e então $|\overline{\alpha}(\overline{\Gamma})| = 4$. O resultado segue diretamente de (6.10). □

Referências Bibliográficas

[1] Chahal, J.S., *Topics in Number Theory*, Springer, 1988.

[2] Garcia, A., Lequain, Y., *Elementos de Álgebra*, IMPA, 2003.

[3] Koblitz, N., *A Course in Number Theory and Cryptography*, Springer, 1994.

[4] Kudo, M., *On Group Structure of Some Special Elliptic Curves*, Mathematical Journal of Okayama University, **47**, 81-84, 2005.

[5] Mazur, B., *Rational Points on Modular Curves*, Springer, 1977.

[6] Milne, J.S., *Elliptic Curves*, BookSurge Publishing, 2006.

[7] Silverman, J., *The Arithmetic of Elliptic Curves*, Springer, 2010.

[8] Silverman J., Tate, J., *Rational Points on Elliptic Curves*, Springer, 2010.

[9] Spearman, B., *Elliptic Curves $y^2 = x^3 - px$ of Rank Two*, Mathematical Journal of Okayama University, **49**, 183-184, 2007.

[10] Spearman, B., *On the Group Structure of Elliptic Curves $y^2 = x^3 - 2px$*, International Journal of Algebra, Vol. 1, no. 5, 247-250, 2007.

[11] Vainsemcher, I., *Curvas Algébricas Planas*, IMPA, 2005.

[12] Walker, R.J., *Algebraic Curves*, Springer, 1978.