Hugo Santos Nunes

Curvas Elípticas e o Teorema de Mordell–Weil

Maceió

Abril de 2015

Hugo Santos Nunes

Curvas Elípticas e o Teorema de Mordell–Weil

Dissertação de mestrado apresentada como requisito parcial para obtenção do título de Mestre em Matemática

Trabalho aprovado. Maceió, 09 de abril de 2015:

Prof. Dr. André Luís Contiero
UFAL

Prof.a. Dr.a. Elisa María Cañete Molero
UFAL

Prof. Dr. Luis Guillermo Martinez Maza
UFAL

Prof. Dr. Renato Vidal da Silva Martins
UFMG

Maceió
Abril de 2015

Hugo Santos Nunes

Curvas Elípticas e o Teorema de Mordell–Weil

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

Universidade Federal de Alagoas

Insituto de Matemática

Programa de Pós-Graduação

Orientador: Prof. Dr. André Luís Contiero

Maceió

Abril de 2015

Hugo Santos Nunes
Curvas Elípticas e o Teorema de Mordell–Weil/ Hugo Santos Nunes. – Maceió, Abril de 2015-
79 p. : il. (algumas color.) ; 30 cm.

Orientador: Prof. Dr. André Luís Contiero

Dissertação de Mestado – Universidade Federal de Alagoas
Insituto de Matemática
Programa de Pós-Graduação, Abril de 2015.

1. Curvas Elíticas. 2. Pontos Racionais. 3. Teorema de Mordell I. Universidade Federal de Alagoas. I. Instituto de Matemática. III. O Teorema de Mordell-Weil

CDU 02:141:005.7

A todos que, de alguma forma, me ajudaram a chegar nesse momento tão especial!

Agradecimentos

Primeiramente, gostaria de agradecer ao meu professor e orientador André Luís Contiero. Quero dizer que foi um orgulho e uma honra tê-lo como orientador desde o quinto período, quando comecei minha iniciação científica, passando pela graduação e o mestrado. Sempre com muita paciência, companheirismo, apoio e amizade. Jamais esquecerei suas palavras, seus conselhos e sua confiança.

Ao Prof. Dr. Marcus Bronzi, que junto com o meu orientador, foi quem me confiou uma carta de recomendação e me ajudou a ingressar no programa de pós-graduação.

Aos meus professores da pós-graduação Prof. Dr. Luiz Guilhermo, Prof. Dr. Feliciano Vitório, Prof. Dr. Fernando Micena, Prof. Dr. Júlio Cesar, Prof. Dr. Krerley Oliveira, Prof. Dr. Ricardo Abreu-Blaya.

Aos professores Prof. Dr. Renato Vidal, Prof. Dr. Luiz Guilhermo e Prof.a. Dr.a. Elisa Cañete por terem aceitado, gentilmente, fazerem parte da banca examinadora de minha dissertação.

Aos amigos do mestrado Lucyan, Jamerson, Rogério, Robson, José Anderson, Fabiane, Denise e Carol, pelo apoio, pelas horas de estudo e pelas dúvidas tiradas. Sem dúvida nenhuma tiveram uma importância fundamental nessa jornada.

À Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pela concessão da bolsa durante todo o período de realização deste Mestrado, e ao Instituto de Matemática da Universidade Federal de Alagoas por todo suporte que me foi dado.

A minha família, meus pais Anacleon e Fátima, e meu irmão Yuri, que são os meus pilares.

Por fim, e não menos importante, a todos os meus amigos, em especial Didica, David, Zayr, Junior, Luiz e Emerson que sempre me apoiaram e acreditaram em mim.

A todos que de forma direta ou indireta auxiliaram na concretização deste trabalho.

"Sempre me pareceu estranho que todos aqueles que estudam seriamente esta ciência acabam tomados de uma espécie de paixão pela mesma. Em verdade, o que proporciona o máximo prazer não é o conhecimento e sim a aprendizagem, não é a posse, mas a aquisição, não é a presença, mas o ato de atingir a meta."

(Carl Friedrich Gauss)

Resumo

Na presente dissertação apresentamos uma prova do Teorema de Mordell, que nos assegura que o grupo dos pontos racionais de uma curva elíptica definida sobre o corpo dos números racionais é finitamente gerado, desde que possua pontos de ordem dois.

Palavras-chaves: Curvas Elíticas. Pontos Racionais. Teorema de Mordell.

Abstract

In this work we present a proof of the remarkable theorem of Mordell which states that the group of the rational points of an elliptic curve defined over the field of rational numbers is finitely generated.

Key-words: Elliptic Curves. Rational Points. Mordell Theorem.

Lista de ilustrações

Sumário

Introdução

O estudo de soluções inteiras de equações polinomiais com coeficientes inteiros remete a Diofanto $(200-284)$. Rapidamente tais estudos contribuíram e, ainda contribuem, com uma quase inesgotável fonte de bonitos problemas em Matemática, fáceis de serem entendidos, porém, muitos deles longe de terem soluções triviais. Não obstante, temos contato com as tão conhecidas *equações diofantinas* em qualquer curso introdutório de teoria dos números. Através da história vimos muitos grandes matemáticos dando generosas contribuições no estudo das equações diofantinas, seja com conjecturas ou seja com técnicas. Com apenas alguns poucos segundos podemos citar o *Pequeno e o Último Teoremas de Fermat*, o *Teorema de Lagrange*, o *Teorema* e os *Símbolos de Legendre*, a *Reciprocidade Quadrática de Gauss* as *Equações de Pell e Pell-Dirichlet*, etc.

Somente a partir do século XX, mais precisamente, após os anos 50, é que a geometria passou a contribuir de forma significante no estudo das equações polinomiais com coeficientes inteiros. Principalmente através do desenvolvimento da *Geometria Algébrica* feito por A. Grothendieck nos *Éléments de Géométrie Algébrique*. Após Grothendieck tivemos significantes contribuições feitas por Cassels, Manin, A. Weil, Mordell, Hasse, Hilbert, Serre, Deligne e outros tantos grandes da matemática. Assim, chegamos a *Geometria Aritmética* que, dentre outras virtudes, funde Equações Diofantinas com a Geometria Algébrica.

Agora, na Geometria Aritmética, não só os polinômios com coeficientes inteiros desempenham papel fundamental, mas sim, as variedades algébricas definidas sobre um corpo $\mathbf{k}$, em que $\mathbf{k}$ pode ser um corpo finito $\mathbb{F}_p$, o corpo dos números racionais $\mathbb{Q}$ ou um corpo de números $\mathbb{Q}[\xi]$. Logo, os problemas mais clássicos passam a ser a procura por pontos $\mathbf{k}$-racionais em $\mathbf{k}$-variedades bem como a estrutura algébrica de tais pontos. Um dos principais estudos da Geometria Aritmética recém criada foram as *Curvas Elípticas*, feitos, principalmente, através do trabalho de Cassels. Muitos dos principais problemas sobre *variedades abelianas* e suas histórias podem ser encontrados em [CT].

A presente dissertação se concentra no estudo das curvas elípticas (Def. 1.2.2), que são uma classe especial, porém genérica, de curvas cúbicas planas não singulares (Def. 1.2.1 e Teor. 1.2.1). O principal objetivo é o completo entendimento de um Teorema atribuído, primeiramente, a Mordell (1922): *se o grupo do pontos racionais sobre uma curva elíptica possui pontos de ordem dois, então ele é finitamente gerado*. Escolhemos trilhar o seguinte caminho:

No Capítulo 1 tratamos de lembrar os conceitos e teoremas da Teoria de Curvas Algébricas, que desempenham um papel fundamental desde o entendimento da definição

de uma curva elíptica, da estrutura de grupo de uma cúbica até a boa colocação do Teorema de Mordell, com destaque para os Teoremas de Bézout e Fundamental de Max Noether.

No Capítulo 2 especializamos nosso estudo para as curvas cúbicas, destacamos os teoremas de classificação das cúbicas planas singulares (Teor. 1.2.1) e das cúbicas lisas (Teor. 1.2.2). Após introduzirmos o conceito de curva elíptica (Def. 1.2.2), apresentamos a prova do importante Teorema da Forma Normal de Weierstrass. Até este último teorema, os capítulos 1 e 2 estão integralmente inseridos no livro de W. Fulton [F]. A partir da Forma Normal de Weierstrass seguimos o livro de Silverman–Tate [S-T]. Apresentamos as construções geométrica e explícita da estrutura de grupo que uma curva elíptica admite.

No Capítulo 3 estudamos os pontos de ordem 2 e 3 (Teor 3.1.1 e 3.2.1) de uma curva elíptica. Algum pré-requisito sobre classificação de grupos abelianos finitos pode ser requerido, cuja referência é [G-L]. Após lembrarmos o discriminante entre dois polinômios, apresentamos a prova do Teorema de Nagel-Lutz (Teor. 3.4.1), que nos dá condições necessárias para um ponto de uma curva elíptica ter ordem finita.

Finalmente no Capítulo 4 tratamos do Teorema de Mordell. Antes de apresentarmos sua prova, fazemos a prova do fundamental Teorema da Descida, que dá uma condição suficiente para um grupo abeliano munido de uma função altura ser finitamente gerado. Em seguida, definimos uma função altura no grupo $E(\mathbb{Q})$ dos pontos racionais de uma curva elíptica e verificamos, sob certas condições, que as hipóteses do Teorema da Descida são satisfeitas pelo grupo $E(\mathbb{Q})$, que culmina com o Teorema de Mordell.

1 Preliminares

1.1 Curvas projetivas e pontos racionais

Nesta seção lembraremos alguns resultados e conceitos essenciais para o completo entendimento desta dissertação.

Considere $\mathbf{k}$ um corpo e $\mathbb{K} := \overline{\mathbf{k}}$ seu fecho algébrico. Dados dois polinômios $F, G \in \mathbb{K}[X, Y, Z]$, dizemos que F e G são equivalentes se existe $\lambda \in \mathbb{K}^*$ tal que $F = \lambda G$.

Por uma curva entendemos uma *curva algébrica projetiva plana definida sobre* $\mathbf{k}$[1]. Assim uma curva C é o conjunto dos zeros de um representante não constante de uma classe de polinômios homogêneos em $\mathbb{K}[X, Y, Z]$ cujos coeficientes estão em $\mathbf{k}$.

Fixado um polinômio homogêneo não constante $F \in \mathbb{K}[X, Y, Z]$, definimos:

$$V(F) := \{P \in \mathbb{P}^2(\mathbb{K}) \mid F(P) = 0\}$$

e notamos que se F é equivalente a G, então $V(F) = V(G)$.

Desta forma, uma curva definida sobre $\mathbf{k}$ é dada por:

$$\mathcal{C} = V(F) \text{ onde } F \in \mathbf{k}[X, Y, Z] \text{ homogêneo}\,.$$

A relação de equivalência definida acima entre polinômios preserva o grau. Logo, *o grau de uma curva* $V(F)$ é o grau do (de qualquer) polinômio homogêneo (da classe de) F.

Definição 1.1.1. *Um ponto* $P = (a : b : c) \in \mathcal{C}$ *é dito um ponto racional se existe* $\lambda \in \mathbb{K}^*$ *tal que* $(\lambda\, a : \lambda\, b : \lambda\, c) \in \mathbb{P}^2(\mathbf{k})$.

Por definição o conjunto dos pontos racionais de uma curva $\mathcal{C}$ é $\mathcal{C} \cap \mathbb{P}^2(\mathbf{k})$.

Definição 1.1.2. *Um ponto* $(a : b : c) \in \mathcal{C} = V(F)$ *é dito um ponto singular se*

$$\frac{\partial F}{\partial x}(a : b : c) = \frac{\partial F}{\partial y}(a : b : c) = \frac{\partial F}{\partial z}(a : b : c) = 0.$$

Se $\mathcal{C}$ *tiver pelo menos um ponto singular, será chamada de uma curva singular, caso contrário será uma curva suave (ou lisa).*

Se P é um ponto não singular da curva $\mathcal{C} = V(F)$, então a reta de $\mathbb{P}^2$ dada por

$$\frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z = 0$$

é chamada a reta tangente a $\mathcal{C}$ em P e é denotada por $T_P\mathcal{C}$.

[1] sempre que $\mathbf{k}$ não for essencial, podemos supor $\mathbf{k}$ algebricamente fechado.

Definição 1.1.3. *Uma curva $V(F)$ é dita irredutível se F for um polinômio irredutível.*

Notamos que a relação de equivalência entre polinômios preserva a irredutibilidade de polinômios, logo está bem definida a irredutibilidade de uma curva. Segue, do fato que um anel de polinômios sobre um corpo é um domínio de fatoração única, que toda curva pode ser escrita de forma única como a reunião de curvas irredutíveis, que são chamadas *componentes da curva*.

Considere a carta afim $U_i := \{(a_1 : a_2 : a_3) \in \mathbb{P}^2 \,|\, a_i \neq 0\}$. Vemos diretamente que a *curva afim* $\mathcal{C} \cap U_3$ é dada por $\mathcal{C}_* := \{(a, b) \in \mathbb{A}^2 \,|\, F_*(a, b) = 0\}$ em que o polinômio $F_*(X, Y) := F(X, Y, 1)$ é a desomogeneização do polinômio F, quando tomamos $V(Z)$ como a reta no infinito. Analogamente para U_1 e U_2 e as respectivas retas $V(X)$ e $V(Y)$ no infinito. Nestes termos, vemos que uma curva projetiva plana é a *colagem* de três curvas planas afins.

Sabemos que todas as propriedades locais de uma curva projetiva são traduzidas e entendidas pelas propriedades locais de uma curva afim apropriada, ver [F, Cap. 3–6].

Seja $\mathcal{C}$ uma curva irredutível e o domínio de integridade $K[\mathcal{C}] := \mathbb{K}[X, Y, Z]/(F)$. No corpo quociente de $K[\mathcal{C}]$ definimos o corpo das funções racionais definidas em subconjuntos[2] de $\mathcal{C}$ com valores em $\mathbb{K}$, a saber:

$$K(\mathcal{C}) := \left\{ \frac{f}{g} \,|\, f, g \in K[\mathcal{C}] \text{ com } \deg f = \deg g \right\}$$

Dado um ponto $P \in \mathcal{C}$ denotamos por $\mathcal{O}_P(\mathcal{C})$ o conjunto das funções racionais que estão definidas em P, assim

$$\mathcal{O}_P(\mathcal{C}) := \left\{ \frac{f}{g} \,|\, f, g \in K[\mathcal{C}] \text{ com } \deg f = \deg g \text{ e } g(P) \neq 0 \right\}$$

Observamos que como $K[\mathcal{C}]$ não é (em geral) um domínio de fatoração única, a representação $\frac{f}{g}$ de uma função racional não é única.

Não é difícil ver que o anel local de uma curva projetiva e o da curva afim associada e apropriada são isomorfos. Assim todas as propriedades locais (que dependem somente do anel local) são propriedades locais de uma curva afim. De certa forma, afirmamos que o mundo local é afim. Se $P = (a, b) \in U_3$, então o anel local de $\mathcal{C}$ é a localização da álgebra das funções regulares $K[C_*]$ da curva afim $V(F_*)$ no ideal maximal $(X - a, Y - b)$ do ponto P. Assim $\mathcal{O}_P(\mathcal{C})$ é um anel de valorização cujo ideal maximal é o conjunto das funções que se anulam em P. Pode-se mostrar que um ponto P é não singular se, e somente se, o anel local $\mathcal{O}_P(\mathcal{C})$ é um anel de valorização discreta, i.e, um domínio local noetheriano cujo ideal maximal é principal, cf. [F, ?].

[2] subconjuntos dados pelo complementar de conjuntos finitos, ver [F, ?]

Para um bom entendimento das próximas seções precisaremos de dois resultados básicos (e fundamentais) da teoria de curvas planas, a saber, o Teorema de Bézout e o Teorema Fundamental de Max Noether, cujas provas podem ser encontradas em [F]. Nestas notas apenas enunciaremos tais resultados, introduzindo todos os objetos para um completo entendimento dos enunciados.

Sejam $\mathcal{C} = V(F)$ uma curva projetiva plana irredutível e $P \in \mathcal{C}$. Podemos supor, através de uma mudança de coordenadas que $P = (0:0:1)$. Assim tomamos a curva afim $\mathcal{C}_* := \mathcal{C} \cap U_3$, dada por $\mathcal{C}_* = V(F_*)$, e escrevemos $F_* = \sum_{i=m}^{n} F_i$, onde F_i é um polinômio homogêneo de grau i. Definimos a *multiplicidade de P em $\mathcal{C}$* como o inteiro não negativo $m_P(C) = m$. Por definição, dizemos que $m_P(\mathcal{C}) = 0$ se $P \notin \mathcal{C}$.

Segue da definição que $m_P(\mathcal{C}) = 1$ se, e somente se, P é um ponto não singular de $\mathcal{C}$. No caso de P ser singular, temos que $\deg F_m > 1$, como $F_m \in \mathbb{K}[X,Y]$ podemos escrever $F_m = \prod_{i=1}^{m} L_{m,i}$ onde cada $L_{m,i}$ é um polinômio homogêneo de grau 1. Neste caso, dizemos que cada $L_{m,i}$ é uma tangente a $\mathcal{C}$ em P, contadas com multiplicidade[3].

Sejam $\mathcal{C} = V(F)$ e $\mathcal{D} = V(G)$ duas curvas planas projetivas. Para cada $P \in \mathbb{P}^2$ considere uma carta afim $U_i \cong \mathbb{A}^2$ tal que $P \in U_i$. Sem perda de generalidade, vamos supor $U_i = U_3$. Tomando as respectivas curvas afins $\mathcal{D}_* := \mathcal{D} \cap U_i = V(G_*)$ e $\mathcal{C}_* = \mathcal{C} \cap U_i = V(F_*)$, consideramos:

$$I(P, F \cap G) := \dim_{\mathbb{K}} \left(\frac{\mathcal{O}_P(\mathbb{A}^2)}{(F_*, G_*)} \right)$$

denominado *índice de intersecção de $\mathcal{C}$ e $\mathcal{D}$ em P*.

Teorema 1.1.1. *O inteiro $I(P, F \cap G)$ dado acima é o único que satisfaz as seguintes condições:*

1. $0 \leq I(P, F \cap G) < \infty$ *se $\mathcal{C}$ e $\mathcal{D}$ não possuem componente em comum passando por P, e $I(P, F \cap G) = \infty$ caso contrário;*

2. $I(P, F \cap G) = 0 \Leftrightarrow P \notin \mathcal{C} \cap \mathcal{D}$;

3. $I(P, F \cap G)$ *é invariante por mudança de coordenadas (projetivas);*

4. $I(P, F \cap G) = I(P, G \cap F)$;

5. $I(P, F \cap G) \geq m_P(\mathcal{C}) \cdot m_P(\mathcal{D})$, *e a igualdade ocorre se, e somente se, $\mathcal{C}$ e $\mathcal{D}$ não possuem reta tangente comum em P;*

6. *Se* $F = \prod F_i^{r_i}$ *e* $G = \prod G_j^{s_j}$, *então* $I(P, F \cap G) = \sum_{i,j} r_i s_j I(P, F_i \cap G_j)$;

7. $I(P, F_* \cap G_*) = I(P, F_* \cap (G_* + AF_*))$ *para todo* $A \in \mathbb{K}[X,Y]$.

[3] não estamos supondo que $L_{m,i} \neq L_{m,j}$ para $i \neq j$.

Demonstração. Ver [F, thm. 3, p. 37]. □

Já estamos em condições de enunciar o célebre Teorema de Bézout, que de maneira informal diz que duas curvas de graus m e n e sem componentes em comum se encontram em $m \cdot n$ pontos, contados com multiplicidades. Uma prova do referido teorema pode ser encontrada em [F, p. 57].

Teorema de Bézout. *Sejam $\mathcal{C} = V(F)$ e $\mathcal{D} = V(G)$ duas curvas planas projetivas de graus m e n, respectivamente. Assumindo que $\mathcal{C}$ e $\mathcal{D}$ não possuem componentes em comum, vale:*

$$\sum_{P \in \mathbb{P}^2} I(P, F \cap G) = m \cdot n$$

Passamos a trilhar um curto caminho para enunciar o teorema Fundamental de Max Noether para curvas planas.

Definição 1.1.4. *Sejam $P \in \mathbb{P}^2$ e $V(F)$ e $V(G)$ duas curvas projetivas sem componentes em comum passando por P e $V(H)$ uma curva projetiva qualquer. Dizemos que as condições de Max Noether são satisfeitas em P com respeito as curvas $V(F)$, $V(G)$ e $V(H)$ se $H_* \in (F_*, G_*) \subset \mathcal{O}_P(\mathbb{P}^2)$.*

Proposição 1.1.1. *Sejam $V(F), V(G)$ e $V(H)$ curvas planas, com $P \in V(F) \cap V(G)$. Então as condições de Max Noether são satisfeitas se qualquer uma das seguintes condições são satisfeitas:*

1. *$P \in V(H)$ e $V(F)$ e $V(G)$ se encontram transversalmente em P;*
2. *P é um ponto não singular de $V(F)$ e $I(P, H \cap F) \geq I(P, F \cap G)$;*
3. *$V(F)$ e $V(G)$ possuem tangente distintas em P e $m_P(V(H)) \geq m_P(V(F)) + m_P(V(G)) - 1$.*

Demonstração. Ver [F, prop. 1, p. 61]. □

Teorema Fundamental de Max Noether. *Sejam $V(F)$, $V(G)$ e $V(H)$ curvas planas projetivas com $V(F)$ e $V(G)$ sem componentes em comum. Existem polinômios homogêneos A e B tais que $H = AF + BG$ se, e somente se, as condições de Max Noether são satisfeitas para todo $P \in V(F) \cap V(G)$.*

Demonstração. Pode ser encontrada em [F, p. 61]. □

1.2 Cúbicas e Formas Normais

Definição 1.2.1. *Uma curva plana projetiva de grau três é denominada cúbica.*

Para uso posterior fazemos a seguinte aplicação do Teorema Fundamental de Max Noether.

Proposição 1.2.1. *Sejam três cúbicas C, C' e C'' com C irredutível. Se C e C' se intersectam em nove pontos não singulares e distintos de C e, adicionalmente, C'' e C se intersectam em oito desses nove pontos, então o nono ponto da intersecção de C'' com C é também um ponto de interseção de C com C'.*

Demonstração. Temos que $C' \cdot C = \sum_{i=1}^{9} P_i$, enquanto que $C'' \cdot C = \sum_{i=1}^{8} P_i + Q$. Seja L um reta através de P_9 que não passa por Q., então $L \cdot C = P_9 + R + S$. Tomando $V(L) \cup C''$, temos que $LC'' \cdot C = C' \cdot C + Q + R + S$. Logo, pelo Teorema Fundamental de Max Noether, existe uma reta L' tal que $L' \cdot C = Q + R + S$. Logo, $L = L'$ e $Q = P_9$. □

Tratemos da classificação projetiva das cúbicas irredutíveis. Primeiramente das cúbicas singulares.

Teorema 1.2.1. *Supondo* $\mathbf{k}$ *algebricamente fechado e* $char\,\mathbf{k} \neq 3$*, a menos de transformações projetivas existem apenas duas cúbicas singulares, a saber:*

$$V(XYZ + X^3 + Y^3) \quad \textit{cúbica nodal}$$
$$V(Y^2Z + X^3) \quad \textit{cúbica cuspidal}$$

Demonstração. Podemos supor que o ponto singular da cúbica $\mathcal{C}$ é $P = (0:0:1)$. Então $F_*(X,Y) = F(X,Y,1) = F_2 + F_3$ com F_2 e F_3 homogêneos de grau 2 e 3 respectivamente, com $F_2 \neq 0$ visto que F_* é irredutível. Logo, podemos supor que $F_2 = XY$ ou $F_2 = Y^2$, a menos de mudança de coordenadas.

$F_2 = XY$**:** neste caso $F = XYZ + a_0X^3 + a_1X^2Y + a_2XY^2 + a_3Y^3$. Como F é irredutível temos que $a_0 \neq 0$ e $a_3 \neq 0$. Fazendo a transformação $X' = (a_0)^{1/3}X$, $Y' = (a_3)^{1/3}Y$ e $Z' = \frac{Z}{(a_0\,a_3)^{1/3}}$, podemos supor que $a_0 = a_3 = 1$. Fazendo, então $Z' = Z + a_1X + a_2Y$, podemos supor que $a_1 = a_2 = 0$. Logo a cúbica é projetivamente equivalente a cúbica nodal.

$F_2 = Y^2$**:** neste caso $F = Y^2Z + a_0X^3 + a_1X^2Y + a_2XY^2 + a_3Y^3$. Como F é irredutível, temos que $a_0 \neq 0$, logo podemos supor $a_0 = 1$. Transformando $X' = X + \frac{1}{3}a_1Y$ podemos supor $a_1 = 0$. Transformando agora, $Z' = Z + a_2X + a_3Y$, podemos supor $a_2 = a_3 = 0$. Logo a cúbica é projetivamente equivalente a cúbica cuspidal.

Notamos que as duas cúbicas não são profeticamente equivalentes, visto que uma possui um nó como singularidade e a outra uma cúspide, e não possui outras singularidades. □

Teorema 1.2.2. *Seja* $\mathbf{k}$ *algebricamente fechado e char*$\mathbf{k} \neq 2$*. Se* $\mathcal{C}$ *é uma cúbica não singular, então* $\mathcal{C}$ *é projetivamente equivalente a* $V(F)$ *onde* $F = Y^2Z - X(X-Z)(X-\lambda Z)$ *com* $\lambda \in \mathbf{k} \setminus \{0, 1\}$.

Demonstração. Sabemos que $\mathcal{C} = V(F)$ possui um ponto de inflexão[4], logo podemos supor que tal inflexão é $(0 : 1 : 0)$ e sua tangente é $V(Z)$. Assim $F(X, 1, Z) = Z + a_1XZ + a_2YZ + a_3X^3 + a_4X^2Z + a_5XZ^2 + a_6Z^3$. Homogeinizando por Y e depois desomonegeizando por Z temos $F_* = Y^2 + a_1XY + a_2Y + a_3X^3 + a_4X^2 + a_5X + a_6$. Como $\deg F_* = 3$ podemos supor $a_3 \neq 0$. Tomamos a seguinte transformação $Y' = Y + \frac{1}{2}a_1X + \frac{1}{2}a_2Z$, logo podemos supor $a_1 = a_2 = 0$. Des forma, podemos escrever F_* da forma $F_* = Y^2 + a_3(X - \lambda_0)(X - \lambda_1)(X - \lambda)$ com $\lambda_i \in \mathbf{k}$. Como $\mathcal{C}$ é suposta não singular, temos que λ_0, λ_1 e λ_2 são distintos dois a dois. Fazendo uma transformação projetiva, podemos supor que $\lambda_0 = 0$, $\lambda_1 = 1$ e $a_3 = 1$. □

Os dois últimos teoremas nos dão uma classificação projetiva de cúbicas, supondo que o corpo $\mathbf{k}$ seja algebricamente fechado e com característica distintas de dois e três. Nos concentramos agora no caso em que o corpo base $\mathbf{k}$ não é algebricamente fechado e possui característica zero. Tomando uma cúbica definida sobre $\mathbf{k}$, buscamos transformações projetivas em $\mathbb{P}^2(\mathbf{k})$ afim de obtermos resultados semelhantes aos dos teoremas acima.

Definição 1.2.2. *Uma curva elíptica definida sobre* $\mathbf{k}$ *é um par* $(E, \mathcal{Q})$ *em que* E *é uma cúbica plana projetiva (não singular) definida sobre* $\mathbf{k}$ *e* $\mathcal{Q}$ *é um ponto racional de* E *e que não é de inflexão.*

Forma Normal de Weierstrass. *Toda curva elíptica (podendo ser singular) pode ser escrita da forma* $E = V(F)$ *com* $F = Y^2Z - X^3 - aX^2Z - bXZ - cZ^3$ *com* $a, b, c \in \mathbf{k}$.

Demonstração. Como $F \in \mathbf{k}[X, Y, Z]$ e $\mathcal{Q} \in \mathbb{P}^2(\mathbf{k})$ podemos assumir que a reta tangente a E em $\mathcal{Q}$ é $V(Z)$. Tal reta tangente intersecta E em outro ponto, que também será um ponto racional, pois $I(P, F \cap T_{\mathcal{Q}}(\mathcal{C})) = 2$ (resolvemos uma equação de grau três onde duas soluções já são racionais). Novamente, podemos assumir que a tangente a $\mathcal{C}$ neste último ponto é $V(X)$. Tome qualquer secante racional em P e suponha que seja $V(Y)$. Assim, o polinômio F_* tem a forma $F_* = XY^2 + (aX + b)Y - cX^2 - dX - e$, com $a, b, c, d, e \in \mathbf{k}$. Trabalhando no anel de funções coordenadas $K[\mathcal{C}_*]$ de $\mathcal{C}_*$, podemos escrever $xy^2 + (ax+b)y = cx^2 + dx + e$. Onde x, y são as classes de X e Y em $\mathbb{K}[C_*]$. Multiplicando por x, obtemos $(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex$ e denotando xy por y', podemos

[4] um ponto simples cujo índice de intersecção em P de $\mathcal{C}$ com a tangente a $\mathcal{C}$ em P é maior que 2.

supor que $y^2 + (ax + b)y = cx^3 + dx^2 + ex$. Fazendo a transformação $y' = y - \frac{1}{2}(ax + b)$, podemos supor que $y^2 = \alpha x^3 + ax^2 + bx + c$, com $\alpha, a, b, c \in \mathbf{k}$. Temos que $\alpha \neq 0$, assim podemos normalizar $\alpha = 1$. □

2 O Grupo de uma Curva Elíptica

Deste ponto em diante uma curva elíptica será uma curva elíptica definida sobre o corpo dos números racionais $\mathbb{Q}$.

2.1 Construção geométrica do grupo de uma curva elíptica

Se temos quaisquer dois pontos sobre uma curva elíptica, dizemos P e Q, então traçamos uma reta ligando P a Q, obtendo um terceiro ponto que denotaremos por $P*Q$. Poderíamos perguntar sobre a estrutura algébrica deste conjunto e esta lei de composição, por exemplo se seria um grupo. Notavelmente estamos bastante perto de ter uma estrutura de grupo, mas é bastante claro que não há nenhum elemento de neutro.

Fixe $\mathcal{O} \in E$ um ponto racional[1] qualquer sobre E. Seja $(+)$ a operação que dado dois pontos de E associa o ponto $P + Q \in E$ da seguinte forma:

constução: tomemos a reta que passa pelos pontos P e Q, ambos pertencentes a E. Seja $P * Q$ o terceiro ponto de intersecção com a curva elíptica. A reta que passa por $\mathcal{O}$ e por $P * Q$ intersecta a cúbica num novo ponto que chamaremos $\mathcal{O} * (P * Q)$. Por definição, chamaremos esse ponto $\mathcal{O} * (P * Q)$ de $P + Q$.

Lema 2.1.1. *Seja S un conjunto com uma lei de composição $(*)$ satisfazendo as seguintes propriedades:*

1. *$P * Q = Q * P$, para todo $P, Q \in S$.*
2. *$P * (P * Q) = Q$, para todo $P, Q \in S$.*

Fixemos um elemento $\mathcal{O} \in S$, e defina uma nova lei de composição $(+)$ da seguinte forma

$$P + Q = \mathcal{O} * (P * Q).$$

Assuma que $R * (\mathcal{O} * (P * Q)) = P * (\mathcal{O} * (Q * R))$ para todo $P, Q, R \in S$. Então S carrega a estrutura de um grupo abeliano.

Demonstração. Primeiramente devemos mostrar que $(+)$ é comutativo com $\mathcal{O}$. Temos que

$$P+Q = \mathcal{O}*(P*Q) = \mathcal{O}*(Q*P) = Q+P \text{ (por 1)} \quad \text{e} \quad P+\mathcal{O} = \mathcal{O}*(\mathcal{O}*P) = P \text{ (por 1 e 2).}$$

[1] para estrutura de grupo em uma cúbica não é necessário supor $\mathcal{O}$ racional, porém no corolário 2.1.1 abaixo essa suposição se faz necessária.

Agora, mostraremos que para qualquer $P, Q \in S$, a equação $X + P = Q$ tem a única solução $X = P * (Q * \mathcal{O})$, em particular, se definir $-P$ para $P * (\mathcal{O} * \mathcal{O})$, então $-P$ é a única solução para a equação $X + P = \mathcal{O}$. Primeiramente

$$\begin{aligned}(P * (Q * \mathcal{O})) + P &= \mathcal{O} * ((P * (Q * \mathcal{O})) * P) \\ &= \mathcal{O} * (P * (P * (Q * \mathcal{O}))) \quad \text{por (1)} \\ &= \mathcal{O} * (Q * \mathcal{O}) \quad \text{por (2)} \\ &= \mathcal{O} * (\mathcal{O} * Q) \quad \text{por (1)} \\ &= Q \quad \text{por (ii)}\end{aligned}$$

Agora, vamos supor que $X + P = Y + P$. Então

$$\begin{aligned}\mathcal{O} * (X * P) = \mathcal{O} * (Y * P) &\Leftrightarrow \mathcal{O} * (\mathcal{O} * (X * P)) = \mathcal{O} * (\mathcal{O} * (Y * Q)) \\ &\Leftrightarrow X * P = Y * P \quad \text{por (2)} \\ &\Leftrightarrow P * X = P * Y \quad \text{por (1)} \\ &\Leftrightarrow P * (P * X) = P * (P * Y) \\ &\Leftrightarrow X = Y \quad \text{por (2)}\end{aligned}$$

Agora mostraremos que $(+)$ é associativa se, e somente se $R * (\mathcal{O} * (P * Q)) = P * (\mathcal{O} * (Q * R))$, para todo $P, Q, R \in S$. Temos

$$\begin{aligned}(P + Q) + R = P + (Q + R) &\Leftrightarrow (\mathcal{O} * (P * Q)) + R = P + (\mathcal{O} * (Q * R)) \\ &\Leftrightarrow \mathcal{O} * ((\mathcal{O} * (P * Q)) * R) = \mathcal{O} * (P * (\mathcal{O} * (Q * R))) \\ &\Leftrightarrow \mathcal{O} * (\mathcal{O} * ((\mathcal{O} * (P * Q)) * R)) = \mathcal{O} * (\mathcal{O} * (P * (\mathcal{O} * (Q * R)))) \\ &\Leftrightarrow (\mathcal{O} * (P * Q)) * R = P * (\mathcal{O} * (Q * R)) \quad \text{por (2)} \\ &\Leftrightarrow R * (\mathcal{O} * (P * Q)) = P * (\mathcal{O} * (Q * R)) \quad \text{por (1)}\end{aligned}$$

Pela nossa afirmação, vemos que $(+)$ é associativa. □

Este resultado nos dá uma maneira de estender a nossa lei de composição de modo que o conjunto E torna-se um grupo abeliano. Usamos a operação $(*)$ para obter $P * Q$. Então, traçamos a reta que liga nosso ponto racional $\mathcal{O}$ e $P * Q$ e definimos o terceiro ponto desta reta com a curva, que é $P + Q$. Em outras palavras $P + Q = \mathcal{O} * (P * Q)$. Sob esta operação que fizemos, de fato temos um grupo com $\mathcal{O}$ como o elemento neutro.

Teorema 2.1.1. *Seja E uma curva elíptica definida sobre $\mathbb{Q}$. Então $(E, +)$ é um grupo abeliano.*

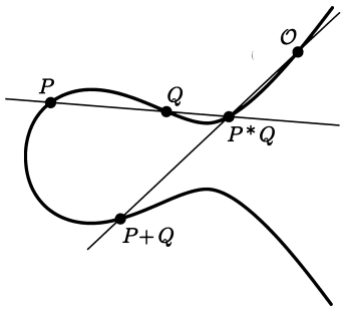

Figura 1 – Comutatividade

Demonstração. A comutatividade é direta, temos que

$$P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P.$$

Para obtermos o elemento neutro, tomamos $P \in \mathcal{C}$ um ponto qualquer da curva. Traçamos uma reta pelos pontos P e $\mathcal{O}$, obtendo assim o terceiro ponto de interssecção com a cúbica que chamaremos de $P * O$. Dessa forma, vemos que P, $\mathcal{O}$ e $P * \mathcal{O}$ estão sobre a mesma reta. Traçando uma reta pelos pontos $\mathcal{O}$ e $P * \mathcal{O}$ obtemos o ponto $\mathcal{O} * (P * \mathcal{O})$. Assim, obtemos P como o terceiro ponto. Temos que

$$\mathcal{O} * (P * \mathcal{O}) = P \Longrightarrow P + \mathcal{O} = P.$$

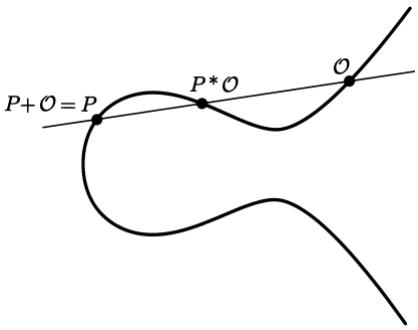

Figura 2 – Elemento Neutro

O fato da cúbica ser não singular, nos dá que a reta tangente está bem definida em todo ponto. Sendo assim, seja a reta tangente à $\mathcal{C}$ no ponto $\mathcal{O}$. Tomemos o ponto de intersseção da reta com a curva e chamemos esse ponto e S. Seja P um ponto qualquer na curva. Tracemos uma reta entre P e S, obtendo assim o ponto $P * S$. Depois tracemos uma reta entre P e $P * S$, obtendo assim o ponto S. Passando uma reta pelos pontos S e $\mathcal{O}$ obtemos $\mathcal{O}$, pois a reta que passa pelos pontos S e $\mathcal{O}$ é tangente a $\mathcal{C}$, logo passa duas vezes por $\mathcal{O}$ e uma por S. Portanto

$$P + (P * S) = \mathcal{O} * [P * (P * S)] = \mathcal{O} * S = \mathcal{O} \Longrightarrow P * S = -P.$$

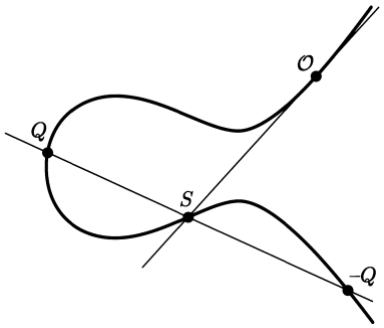

Figura 3 – Inverso

Sejam $P, Q, R \in \mathcal{C}$. Queremos mostrar que $(P+Q)+R = P+(Q+R)$. Traçando uma reta pelos ponto $P * Q$ e $\mathcal{O}$ obtemos o terceiro ponto da interssecção da reta com a cúbica, o ponto $P+Q$. Em seguida, traçamos a reta que passa pelos pontos $P+Q$ e R, assim, encontramos o ponto $(P+Q)*R$. Traçamos uma reta pelos pontos Q e R, obtendo o ponto $Q*R$. Em seguida, traçamos uma reta pelos pontos $Q*R$ e $\mathcal{O}$ e obtemos $Q+R$. Agora ligamos os pontos $Q+R$ e P, obtendo assim o ponto $P*(Q+R)$. Seja $\mathcal{C}_1$ o conjuntos dos pontos situados sobre as retas tracejadas e $\mathcal{C}_2$ o conjunto dos pontos sobre as retas não tracejadas. Temos assim duas cúbicas degeneradas. Dessa forma, temos os pontos $\mathcal{O}, P, Q, R, P*Q, Q*R, P+Q, P+R$ e o ponto de interssecção entre as duas retas. Por construção, temos que as cúbicas $\mathcal{C}_1$ e $\mathcal{C}_2$ passam por nove pontos, mas a cúbica original passa por oito pontos desses nove pontos, logo ela passará pelo nono, que é a interssecção das duas retas que passam por $\mathcal{C}$. Portanto, temos que $(P+Q)*R = P*(Q+R)$.

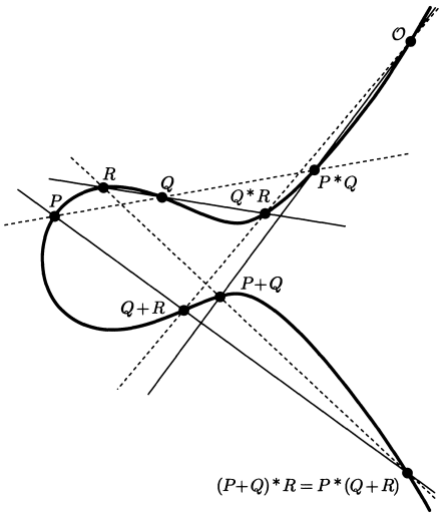

Figura 4 – Associatividade

□

Corolário 2.1.1. *Seja* $E(\mathbb{Q}) := E \cap \mathbb{P}^2(\mathbf{k})$ *o conjunto dos pontos racionais de* E*. Então* $(E(\mathbb{Q}), +)$ *é um subgrupo de* $(E, +)$*.*

Demonstração. Dados dois pontos P, $Q \in E(\mathbb{Q})$, a reta L que passa por estes dois pontos está definida sobre $\mathbb{Q}$. Logo, o terceiro ponto de intersecção $P * Q$ de L com E é um ponto racional, pois é a terceira solução de uma equação cúbica sobre $\mathbb{Q}$ que já possui duas soluções racionais. Deste que $\mathcal{O} \in E(\mathbb{Q})$, obtemos que $P + Q \in E(\mathbb{Q})$. □

2.2 Fórmulas Explicitas para a lei de Grupo

Seja E uma curva elíptica escrita na forma normal de Weierstrass

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3.$$

Substituindo $Z = 0$ nesta equação temos $X^3 = 0$, que tem a raíz tripla $X = 0$. Isto significa que a cúbica encontra a reta no infinito no ponto $(0 : 1 : 0)$ com multiplicidade 3. Então, a cúbica tem exatamente um ponto no infinito que é de inflexão.

Observação 2.2.1. *Denotaremos por* $\mathcal{O}$ *o único ponto do infinito da curva elíptica* E*.*

Agora iremos discutir a estrutura do grupo um pouco mais perto. Para adicionarmos dois pontos P e Q sobre uma equação cúbica na forma de Weierstrass primeiramente traçamos um reta através P e Q e encontramos o terceiro ponto de interssecção, que chamamos de $P * Q$. A vantagem de E estar na forma normal de Weierstrass está no seguinte roteiro:

Observação 2.2.2. *A reta através de* $P * Q$ *e* $\mathcal{O}$*, é a reta vertical através de* $P * Q$*. E como a curva elípita está na forma normal de Weierstrass, ela é simétrica em relação ao eixo-x. Podemos, então, refletir o ponto* $P * Q$*, encontrando assim a soma* $P + Q$*.*

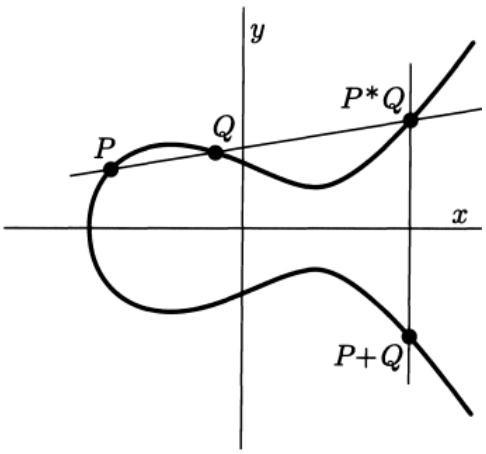

Figura 5 – Adicionando pontos na forma normal de Weierstrass

Naturalmente gostaríamos de saber qual é o negativo do ponto Q. O negativo de Q é a reflexão dele através do eixo x, a saber, se $Q = (x, y)$, então $-Q = (x, -y)$. Para verificarmos isso, suponha que adicionaremos Q ao ponto que chamamos de $-Q$. A reta através de Q e $-Q$ é vertical, de modo que o terceiro ponto de interseção é o ponto $\mathcal{O}$. Agora tracemos a tangente a $\mathcal{O}$. Essa é a reta no infinito e possui multiplicidade 3 em $\mathcal{O}$, logo $\mathcal{O} * \mathcal{O} = \mathcal{O}$. Portanto,

$$Q + (-Q) = \mathcal{O},$$

logo $-Q$ é o inverso de Q. Vale destacar que isso não se aplica no caso em que $Q = \mathcal{O}$, mas obviamente $-\mathcal{O} = \mathcal{O}$.

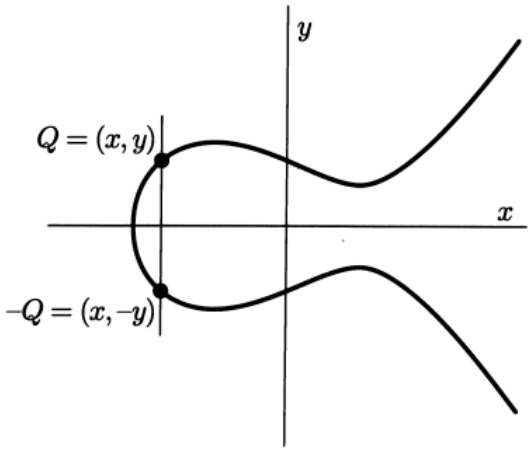

Figura 6 – O ponto negativo

Vamos, finalmente, às contas. Vimos que uma curva elíptica possui somente um ponto no infiito, a saber $(0 : 1 : 0)$. Afim de buscar fórmulas explítitas para a operação de grupo da curva elíptica, podemos, sem perda de generalidade, supor que a curva elípitica E é afim. Ou seja, determinada pela forma normal de Weierstrass:

$$y^2 = x^3 + ax^2 + bx + c.$$

Considere dois pontos da curva elípitca E, $P_1 = (x_1, y_1)$, e $P_2 = (x_2, y_2)$. Buscamos as descrições das coordenadas dos pontos

$$P_1 * P_2 = (x_3, y_3) \quad \text{e} \quad P_1 + P_2 = (x_3, -y_3).$$

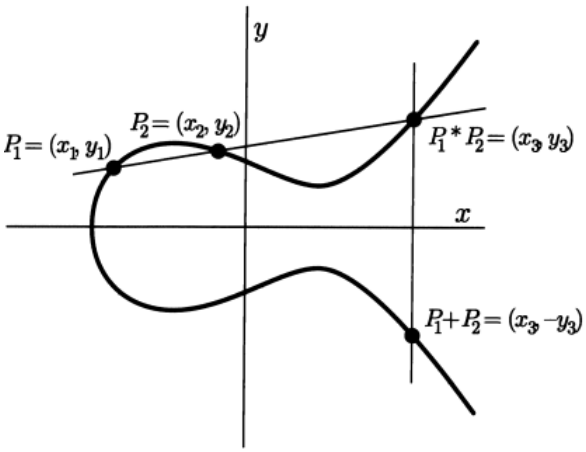

Figura 7 – Derivando a fórmula para a lei de adição

Primeiramente, olhemos para a equação da reta que passa por (x_1, y_1) e (x_2, y_2), que é dada por

$$y = \lambda x + v, \qquad \text{onde } \lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{e} \qquad v = y_1 - \lambda x_1 = y_2 - \lambda x_2,$$

supondo que $x_1 \neq x_2$. Por construção, a reta acima intersecta a curva elíptica nos dois pontos (x_1, y_1) e (x_2, y_2). Para encontrarmos o terceiro ponto de intersecção, substituiremos a equação da reta na cúbica, desenvolvemos a equação e obteremos uma equação do terceiro grau na variável x:

$$\begin{aligned} y^2 = (\lambda x + v)^2 &= x^3 + ax^2 + bx + c \\ \lambda^2 x^2 + 2\lambda x v + v^2 &= x^3 + ax^2 + bx + c \end{aligned}$$

Colocando todos os termos para um lado obtemos:

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

Temos uma equação cúbica na variável x, e suas três raízes x_1, x_2, x_3 são as coordenadas das três interssecções. Portanto,

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda v)x + (c - v^2) = (x - x_1)(x - x_2)(x - x_3),$$

e assim,

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

Igualando os coeficientes de termo x^2 em ambos os lados, temos que

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

Então

$$x_3 = \lambda^2 - a - x_1 - x_2, \qquad y_3 = \lambda x_3 + v.$$

Estas fórmulas são a forma mais eficiente para calcular a soma de dois pontos com abcissas distintas.

Exemplo 1. *Consideremos a curva elíptica*

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

Sejam $P_1 = (-1, 4)$ *e* $P_2 = (2, 5)$ *dois pontos sobre a curva. Calcule* $P_1 + P_2$.

Solução. Primeiro, devemos achar a reta que passa pelos dois pontos. Assim:

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

Agora,

$$v = y_1 - \lambda x_1 = 4 - \frac{1}{3} \cdot (-1) = 4 + \frac{1}{3} = \frac{13}{3}$$

Dessa forma, temos

$$\begin{aligned} x_3 &= \lambda^2 - a - x_1 - x_2 = \left(\frac{1}{3}\right)^2 - 0 - (-1) - 2 = -\frac{8}{9}. \\ y_3 &= \lambda x_3 + v = \frac{1}{3} \cdot \left(-\frac{8}{9}\right) + \frac{13}{9} = \frac{109}{27} \end{aligned}$$

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

As fórmulas dadas acima envolve a inclinação da reta que passa pelos dois pontos. Veremos agora o caso em que os dois pontos coincidem. Vamos supor que temos $P_0 = (x_0, y_0)$ e queremos achar $P_0 + P_0 = 2P_0$. Precisamos achar a reta que liga P_0 a P_0. Não podemos usar a fórmula para λ, pois temos $x_1 = x_2$ e $y_1 = y_2$. A fórmula que descrevemos para a adição de um ponto a ele mesmo é a reta que liga P_0 a P_0, ou seja, é a reta tangente a cúbica em P_0. Derivamos implicitamente a relação $y^2 = f(x)$ e encontramos

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

para calcularmos o dobro de um ponto procedendo como no caso em que as abcissas são distintas.

Exemplo 2. *Usando a mesma curva cúbica*

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

e o ponto $P_1 = (-1, 4)$. *Calcule* $2P_1$.

Solução. Primeiro achamos λ. Assim:

$$\lambda = \frac{f'(x_1)}{2y_1} = \frac{3x_1^2}{2y_1} = \frac{3(-1)^2}{2 \cdot 4} = \frac{3}{8}$$

Para acharmos v, temos

$$v = y_1 - \frac{3}{8}x_1 = \frac{35}{8}$$

Logo, a reta tangente a curva que passa por P_1 é

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

Usamos a fórmula que temos para achar (x_2, y_3) e temos que

$$2P_1 = (x_3, -y_3) = \left(\frac{137}{64}, -\frac{2651}{512}\right).$$

□

Algumas vezes é conveniente ter uma expressão explícita para $2P$ em termos das coordenadas de P. Para isso, substituiremos

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

nas fórmulas dadas acima. Seja $2P = (x_{2P}, y_{2P})$ Assim:

$$\begin{aligned} x_{2P} &= \lambda^2 - a - x_1 - x_2 = \lambda^2 - a - 2x = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x \\ &= \left(\frac{3x^2 + 2ax + b}{4y}\right)^2 - a - 2x \\ x_{2P} &= \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} \end{aligned}$$

Para achar a coordenada y_{2P} de $2P$ basta substituir em

$$y_{2P} = \frac{f'(x)}{2y}x_{2P} + v.$$

Esta fórmula é frequentemente chamada de *fórmula de duplicação*. Estas são as fórmulas básicas para adição de pontos sobre uma cúbica quando ela está na forma de Weierstrass. Essas fórmulas serão usadas para provarmos muitos fatos sobre pontos racionais sobre curvas cúbicas, inclusive o Teorema de Mordell.

3 Pontos de Ordem Finita

Seja P um elemento de um grupo qualquer. Dizemos que P tem ordem m se

$$mP = P + P + \cdots + P = \mathcal{O},$$

mas $m'P \neq 0$ para todo inteiro $1 \leq m' < m$. Se tal m existe, então P tem ordem finita, caso contrário tem ordem infinita. Começaremos nosso estudo sobre pontos de ordem finita sobre curvas elípticas olhando para pontos de ordem dois e três. Como de costume, assumiremos nossa curva elíptica na forma de Weierstrass

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

e que o ponto no infinito $\mathcal{O}$ é o elemento zero para a lei de grupo.

3.1 Pontos de Ordem Dois

Dizemos que um ponto $P = (x, y)$, com $P \neq \mathcal{O}$, tem ordem dois se $2P = \mathcal{O}$. Temos que

$$2P = \mathcal{O} \Leftrightarrow P = -P \Leftrightarrow (x, y) = (x, -y),$$

ou seja, $y = 0$.

Teorema 3.1.1. *Os pontos de ordem 2 de uma curva elíptica é um grupo isomorfo ao produto de dois grupos cíclicos de ordem 2.*

Demonstração. Seja P um ponto de ordem dois, logo temos que $y = 0$, assim

$$x^3 + ax^2 + bx + c = 0.$$

Admitindo raízes complexas, a equação acima terá três raízes

$$P_1 = (\alpha_1, 0), \qquad P_2 = (\alpha_2, 0), \qquad P_3 = (\alpha_3, 0),$$

todas de ordem dois e distintas, já que uma curva elíptica não tem singularidades. Logo, os pontos que satisfazem a equação são $\mathcal{O}, P_1, P_2$ e P_3. Temos que $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ é o único grupo com quatro elementos de ordem dois, com exceção de $\mathcal{O}$. Portanto

$$\{\mathcal{O}, P_1, P_2, P_3\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}.$$

□

3.2 Pontos de Ordem Três

Dizemos que um ponto $P = (x, y)$, com $P \neq \mathcal{O}$, tem ordem três se $3P = \mathcal{O}$. Dessa forma, podemos escrever $2P = -P$, então um ponto de ordem três deve satisfazer

$$x_{2P} = x_P = x_{-P}.$$

Reciprocamente, se $P \neq \mathcal{O}$ satisfaz $x_{2P} = x_P$, então $2P = \pm P$. Então, $P = \mathcal{O}$ ou $3P = \mathcal{O}$. Em outras palavras, os pontos de ordem três são os pontos que satisfazem

$$x_{2P} = x_P.$$

Para achar esses pontos que satisfazem essas condições, usamos a fórmula de duplicação do ponto. Assim

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x$$

donde

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$$

Portanto, um ponto $P = (x, y) \neq 0$ sobre E tem ordem três se, e somente se, x é raiz do polinômio

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0.$$

Teorema 3.2.1. *Os pontos de ordem 3 de uma curva elíptica é um grupo isomorfo ao produto de dois grupos cíclicos de ordem 3.*

Demonstração. Chamemos a equação acima de $g(x)$ e derivemos, temos

$$\begin{aligned} g(x) &= 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 \\ g'(x) &= 12x^3 + 12ax^2 + 12bx + 12c \\ g'(x) &= 12(x^3 + ax^2 + bx + c) \\ g'(x) &= 12f(x) \end{aligned}$$

A reta tangente a P tem equação

$$y = \lambda x + (y_1 - \lambda x_1),$$

onde

$$P = (x_1, y_1) \quad \text{e} \quad \lambda = \frac{f'(x)}{2y}.$$

Sabemos que a coordenada x_{2P} do ponto $2P$ é igual a coordenada x da interssecção de y a curva. Assim,

$$\begin{aligned} x_{2P} &= \lambda^2 - a - 2x \\ &= \left(\frac{f'(x)}{2y}\right)^2 - a - 2x \\ &= \frac{f'(x)^2}{4f(x)} - a - 2x \end{aligned}$$

Sabemos que P tem ordem 3 se, e somente se

$$\begin{aligned} x_{2P} &= x \Leftrightarrow \\ \frac{f'(x)^2}{4f(x)} - a - 2x &= x \Leftrightarrow \\ \frac{f'(x)^2}{4f(x)} - a - 3x &= 0 \Leftrightarrow \\ \frac{f'(x)^2}{4f(x)} - \frac{1}{2}f''(x) &= 0 \Leftrightarrow \\ \frac{f'(x)^2 - 2f(x)\cdot f''(x)}{4f(x)} &= 0 \Leftrightarrow \\ f'(x)^2 - 2f(x)\cdot f''(x) &= 0 \end{aligned}$$

Mas $f'(x)^2 - 2f(x)\cdot f''(x)$ e $g(x)$ são polinômios com as mesmas raízes, donde

$$f'(x)^2 - 2f(x)\cdot f''(x) = g(x),$$

o que contraria a afirmação de que E é não singular. Portanto $g(x)$ tem quatro raízes complexas distintas.

Agora, sejam $\beta_1, \beta_2, \beta_3, \beta_4$ as quatro raízes de $g(x)$. Para cada valor de x teremos dois valores para y. Assim, sejam $\pm\delta_1, \pm\delta_2, \pm\delta_3, \pm\delta_4$ os valores de y. Logo, a curva terá oito pontos distintos de ordem três e mais um único ponto de ordem um, a saber o ponto $\mathcal{O}$, formando assim um grupo abeliano com nove elemento. O único grupo abeliano com nove elementos tais que todo elemento têm ordem três é o $\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}$.

$$\{\mathcal{O}, (\beta_1, \pm\delta_1), (\beta_2, \pm\delta_2), (\beta_3, \pm\delta_3), (\beta_4, \pm\delta_4)\} \cong \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

□

3.3 O Discriminante

O objetivo dessa seção é provar o Teorema de Nagel-Lutz, que nos dirá como achar todos os pontos racionais de ordem finita. Esse teorema diz que um ponto racional (x, y) de ordem finita deve ter coordenadas inteiras. Em particular, uma curva cúbica tem somente um número finito de pontos racionais de ordem finita.

Lema 3.3.1. *Suponha que D é um dominio de fatoração única, e*

$$\begin{aligned} f(x) &= a_0x^m + \cdots + a_m \quad (a_0 \neq 0), \\ g(x) &= b_0x^n + \cdots + b_n \quad (b_0 \neq 0), \end{aligned}$$

são polinômios sobre D. Então uma condição necessária e suficiente para f e g possuirem um fator comum não trivial é que existam dois polinômios $F, G \in D[x]$, ambos não nulos, que satisfaça

$$\deg F < m, \qquad \deg G < n, \qquad fG = gF.$$

Demonstração. Pelo Lema de Gauss, $D[x]$ é também um domínio de fatoração única. Suponha que h é um fator comum não trivial de f e g. Então,

$$\begin{aligned} f &= Fh, \qquad F \in D[x], \qquad \deg F < m, \\ g &= Gh, \qquad G \in D[x], \qquad \deg G < n. \end{aligned}$$

Isto é, temos

$$fG = gF.$$

Reciprocamente, se existem dois polinômios $F, G \in D[x]$, não ambos 0, que satisfazem

$$\deg F < m, \qquad \deg G < n, \qquad fG = gF,$$

então os fatores não triviais de f não podem ser todos fatores de F, uma vez que $\deg F < \deg f$. Como $D[x]$ é um D.F.U, deve existir um fator não trivial de f que divide g. □

Os polinômios F e G no lema acima podem ser escritos explictiamentre como

$$\begin{aligned} F(x) &= A_0 x^{m-1} + \cdots + A_{m-1}, \\ G(x) &= B_0 x^{n-1} + \cdots + B_{n-1}. \end{aligned}$$

Comparando os coeficientes de ambos os lados de $fG = gF$, temos

$$\begin{aligned} a_0 B_0 &= b_0 A_0, \\ a_1 B_0 + a_0 B_1 &= b_1 A_0 + b_0 A_1, \\ &\vdots \\ a_m B_{n-1} &= b_n A_{m-1}. \end{aligned}$$

Podemos pensar da expressão acima como um sistema de equação lineares homogêneas em $B_0, \ldots, B_{n-1}, A_0, \ldots, A_{m-1}$, de modo que uma condição necessária e suficiente para

este sistema ter uma solução não nula é que o determinante seja igual a 0

$$\begin{vmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ \vdots & a_1 & \vdots & & \vdots & b_1 & \vdots & \\ \vdots & \vdots & \vdots & a_0 & \vdots & \vdots & \vdots & \\ \vdots & \vdots & \vdots & a_1 & b_n & \vdots & \vdots & b_0 \\ a_m & \vdots & \vdots & \vdots & & b_n & \vdots & b_1 \\ & a_m & \vdots & \vdots & & & \vdots & \vdots \\ & & & \vdots & & & & \vdots \\ & & & a_m & & & & b_n \\ & & & & & & & \end{vmatrix} = 0.$$

Ao transpor a matriz deste determinante podemos resumir o que foi mencionado acima no seguinte teorema.

Teorema 3.3.1. *Suponha que D é um D.F.U, e*

$$\begin{aligned} f(x) &= a_0x^m + a_1x^{m-1} + \cdots + a_m \quad (a_0 \neq 0), \\ g(x) &= b_0x^n + b_1x^{n-1} + \cdots + b_n \end{aligned}$$

são dois polinômios em D. Então para f e g terem um fator comum não trivial, uma condição necessária e suficiente é que

$$R(f, g) = 0,$$

onde

$$R(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & \dots & a_m & & & & \\ & a_0 & a_1 & \dots & \dots & \dots & a_m & & & \\ & & \dots & \dots & \dots & \dots & \dots & & & \\ & & & a_0 & a_1 & \dots & \dots & \dots & a_m & \\ b_0 & b_1 & \dots & \dots & b_n & & & & & \\ & b_0 & b_1 & \dots & \dots & b_n & & & & \\ & & \dots & \dots & \dots & \dots & \dots & & & \\ & & & & b_0 & b_1 & \dots & \dots & b_n & \end{vmatrix}$$

Definição 3.3.1. *Este determinante, $R(f, g)$, é chamado resultante de f e g.*

Corolário 3.3.1. *Sobre a hípotese no teorema acima, existem polinômios $a, b \in D[x]$, com $\deg a < n$, $\deg b < m$, tal que*

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

Demonstração. No resultante, denote o cofator do elemento na $(m+n)$-ésima coluna e i-ésima linha porA_i, e escreva

$$\begin{aligned} a(x) &= A_1x^{n-1} + \cdots + A_n, \\ b(x) &= A_{n+1}x^{m-1} + \cdots + A_{n+m}. \end{aligned}$$

Podemos ver que

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

□

Definição 3.3.2. *Suponha que D é um D.F.U., $f \in D[x]$ e sua derivada $f' \in D[x]$. O elmento de D denotado por*

$$\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \cdot \frac{1}{a_n} \cdot R(f,f'),$$

onde n é o grau de f e a_n é seu coeficiente líder, é chamado o discriminante de f.

Exemplo 3. *Seja $f(x) = x^3 + ax^2 + bx + c$ a equação da curva elíptica. Temos que o polinômio f é mônico e o seu grau é 3. Assim*

$$\begin{aligned} \Delta(f) &= (-1)^{\frac{3(3-1)}{2}} \cdot \frac{1}{1} \cdot R(f,f') \\ \Delta(f) &= (-1)^3 \cdot R(f,f') \\ \Delta(f) &= -R(f,f') \\ \Delta(f) &= -\begin{vmatrix} 1 & a & b & c & 0 \\ 0 & 1 & a & b & c \\ 3 & 2a & b & 0 & 0 \\ 0 & 3 & 2a & b & 0 \\ 0 & 0 & 3 & 2a & b \end{vmatrix} \\ &= -\begin{vmatrix} 1-(0\cdot a) & a-(0\cdot b) & b-(0\cdot c) & c-(0\cdot 0) \\ 2a-(3\cdot a) & b-(3\cdot b) & 0-(3\cdot c) & 0-(0\cdot 0) \\ 3-(0\cdot a) & 2a-(0\cdot b) & b-(0\cdot c) & 0-(0\cdot 0) \\ 0-(0\cdot a) & 3-(0\cdot b) & 2a-(0\cdot c) & b-(0\cdot 0) \end{vmatrix} \\ &= -\begin{vmatrix} 1 & a & b & c \\ -a & -2b & -3c & 0 \\ 3 & 2a & b & 0 \\ 0 & 3 & 2a & b \end{vmatrix} \\ &= -\begin{vmatrix} -2b-(-a\cdot a) & -3c-(-a\cdot b) & 0-(-a\cdot c) \\ 2a-(3\cdot a) & b-(3\cdot b) & 0-(3\cdot c) \\ 3-(0\cdot a) & 2a-(0\cdot b) & b-(0\cdot c) \end{vmatrix} \end{aligned}$$

$$\begin{aligned} &= -\begin{vmatrix} -2b+a^2 & -3c+ab & ac \\ -a & -2b & -3c \\ 3 & 2a & b \end{vmatrix} \\ &= -(4b^3 - 2a^2b^2 + 27c^2 - 9abc - 2a^3c - 3abc + a^2b^2 - 12abc + 6a^3c + 6abc) \\ \Delta(f) &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \end{aligned}$$

Corolário 3.3.2. *Suponha que D é um D.F.U.. Então uma condição necessária e suficiente para $f \in D[x]$ ter fatores múltiplos é que seu discriminante seja igual a 0*

$$\Delta(f) = R(f, f') = 0.$$

Tomemos nossa curva elíptica na forma normal de Weierstrass

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

onde a, b, c são números racionais. Se tomamos

$$X = d^2x \qquad \text{e} \qquad Y = d^3t,$$

então nossa equação

$$\begin{aligned} Y^2 &= X^3 + d^2aX^2 + d^4bX + d^6c \\ (d^3y)^2 &= (d^2x)^3 + d^2a(d^2x)^2 + d^4bd^2x + d^6c \\ d^6y^y &= d^6x^3 + d^6ax^2 + d^6bx + d^6c \\ d^6y^2 &= d^6(x^3 + ax^2 + bx + c) \\ y^2 &= x^3 + ax^2 + bx + c. \end{aligned}$$

Observação 3.3.1. *Ao escolher um número inteiro d suficientemente grande, podemos limpar os denominadores em a, b, c, assumindo que nossa curva é dada por uma equação com coeficientes inteiros.*

Nosso objetivo é provar o Teorema de Nagel-Lutz, que nos diz como procurar todos os pontos racionais de ordem finita. Esse teorema diz que um ponto (x, y) de ordem finita deve ter coordenadas inteiras, nesse caso ou $y = 0$, para pontos de ordem dois, ou $y \mid \Delta$, onde Δ é o discriminante do polinômio $f(x)$. Em particular, uma curva elíptica tem somente um número finito de pontos racionais de ordem finita.

Portanto, o problema de procurar os pontos racionais de ordem finita pode ser determinado em um número finito de passos. Tome o inteiro Δ, e considere um número finito de inteiros y com $y \mid \Delta$. Pegue todos esses valores de y e os substitua na equação $y^2 = f(x)$. O polinômio $f(x)$ tem coeficientes inteiros e coeficiente líder 1.

Se ele tem uma raiz inteira, essa raiz dividirá o termo constante. Portanto, existe um número finito de casos para checar, e assim teremos a certeza de encontrar todos os

pontos de ordem finita em um número finito de passos. Uma observação que precisa ser feita é que não estamos afirmando que um ponto (x, y) com coordenadas inteiras e $y \mid \Delta$ deve ter ordem finita. O teorrema de Nagell-Lutz não é um "se e somente se".

Lema 3.3.2. *Seja $P = (x, y)$ um ponto sobre nossa curva elíptica tal que ambos P e $2P$ tenham coordenadas inteiras. Então, ou $y = 0$ ou $y \mid \Delta$.*

Demonstração. Vamos assumir que $y \neq 0$ e provar que $y \mid \Delta$. Sabemos que

$$y \neq 0 \Longrightarrow 2P \neq \mathcal{O}\,.$$

Então, podemos escrever $2P = (X, Y)$. Por hípotese, x, y, X, Y são todos inteiros. Usando a fórmula da duplicação, temos

$$2x + X = \lambda^2 - a, \qquad \text{onde }, \;\; \lambda = \frac{f'(x)}{2y}.$$

Como x, X e a são todos inteiros, segue que λ também é inteiro. Uma vez que $2y$ e $f'(x)$ são inteiros, vemos que $2y \mid f'(x)$, em particular, $y \mid f'(x)$. Mas $y^2 = f(x)$, então $y \mid f(x)$. Usando a relação

$$\Delta = a(x)f(x) + b(x)f'(x).$$

Os coeficientes de a e b são inteiros, então $a(x)$ e $b(x)$ tomam valores inteiros quando calculados no inteiro x. Logo $y \mid \Delta$. □

3.4 O Teorema de Nagell-Lutz

Agora, mostraremos que todos os pontos racionais de ordem finita sobre uma curva elíptica deve ter coordenadas inteiras. Seja p um primo qualquer, vamos tentar mostrar que p não divide os denominadores de x e y. Para isso, consideremos os pontos racionais (x, y) onde p divide os denominadores de x e y.

Definição 3.4.1. *Todo número racional não nulo pode ser escrito de forma única como $r = \frac{m}{n}p^\nu$, em que $mdc(m, p) = mdc(n, p) = 1$, $m, \nu \in \mathbb{Z}$ e $n \in \mathbb{Z}^*$ .Definimos a ordem de tal número racional como*

$$ord_p(r) = \nu$$

Observação 3.4.1. *Fixado um primo p, $ord_p(r)$ é a valorização p-ádica de $\mathbb{Q}$ em $\mathbb{Z}$.*

Se p divide o denominador do número racional, então a ordem do número racional será negativa. Similarmente, se p divide o numerador do número racional, então a ordem do número racional será positiva. A ordem de um número racional é zero se, e somente se p não divide nem seu numerador e nem seu denominador.

Proposição 3.4.1. *Seja (x, y) um ponto racional na curva elíptica. Para cada primo p temos $ord_p(x) < 0$ se, e somente se, $ord_p(y) < 0$.*

Demonstração. Seja (x, y) um ponto sobre a curva elíptica, onde existe um primo p que divida o denominador de x. Como x e y são números racionais, podemos expressá-los da seguinte forma

$$x = \frac{m}{np^{\mu}} \quad \text{e} \quad y = \frac{u}{wp^{\sigma}}.$$

Como p divide o denominador de x, temos que $\mu > 0$. Com isso, temos como objetivo mostrar que $\sigma > 0$. Por construção, temos também que $p \nmid m, n, u, w$. Substituindo x e y na equação da nossa curva elíptica, temos

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3}{n^3p^{3\mu}} + \frac{am^2}{n^2p^{2\mu}} + \frac{bm}{np^{\mu}} + c.$$

Colocando em denominador comum

$$\frac{u^2}{w^2p^{2\sigma}} = \frac{m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}.$$

Agora, podemos examinar as ordens de ambos os lados da equação. Temos que

$$p \nmid u \Longrightarrow p \nmid u^2 \quad \text{e} \quad p \nmid w \Longrightarrow p \nmid w^2,$$

assim

$$ord\left(\frac{u^2}{w^2p^{2\sigma}}\right) = ord\left(\frac{u^2}{w^2}p^{-2\sigma}\right) = -2\sigma.$$

Para o outro lado da equação, sabemos que

$$p \nmid n \Longrightarrow p \nmid n^3 \quad \text{e} \quad p \nmid m \Longrightarrow p \nmid (m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}).$$

Portanto, temos

$$ord\left(\frac{m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}\right) = -3\mu.$$

Como ambos os lados da nossa equação devem ter a mesma ordem, temos então que $2\sigma = 3\mu$. Como afirmamos que $\mu > 0$, este resultado prova que $\sigma > 0$, e portanto p divide o denominador de y. □

Além disso, a relação $2\sigma = 3\mu$ significa que $2 \mid \mu$ e $3 \mid \sigma$, assim, temos que $\mu = 2\nu$ e $\mu = 3\nu$ para algum inteiro $\nu > 0$. Então, se ν divide x ou y, então divide ambos, e a recíproca da prova acima também é verdade. ou seja, se assumirmos que p divide o denominador de y, acharemos o mesmo resultado.

Suplemento 3.4.1. *Um ponto racional de uma curva elíptica C pode ser escrito da forma $P = (\frac{m}{\ell^2}, \frac{n}{\ell^3})$ onde $m,\ n,\ \ell$ são inteiros, $\ell > 0$ e $mdc(m, \ell) = mdc(n, \ell) = 1$.*

Demonstração. Suponha que

$$x = \frac{m}{M} \quad \text{e} \quad y = \frac{n}{N},$$

irredutíveis e com $M, N > 0$. Substituindo na equação da nossa curva elíptica temos:

$$\begin{aligned}
y^2 &= x^3 + ax^2 + bx + c \\
\left(\frac{n}{N}\right)^2 &= \left(\frac{m}{M}\right)^3 + a\left(\frac{m}{M}\right)^2 + b\left(\frac{m}{M}\right) + c \\
\frac{n^2}{N^2} &= \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c \\
\frac{n^2M^3}{N^2M^3} &= \frac{m^3N^2 + aN^2Mm^2 + bN^2M^2m + cN^2M^3}{N^2M^3} \\
M^3n^2 &= N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3.
\end{aligned}$$

Temos, do lado direito da equação, que N^2 é um fator comum a todos os termos, logo $N^2 \mid M^3n^2$. Porém $mdc(n, N) = 1$, logo $N^2 \mid M^3$. Agora, vamos mostrar em três passos que $M^3 \mid N^2$. Da equação acima, temos que $M \mid N^2m^3$, e como $mdc(m, M) = 1$ temos $M \mid N^2$. Assim,

$$M^2 \mid M^3n^2, \quad M^2 \mid aN^2Mm^2, \quad M^2 \mid bN^2M^2m \quad \text{e} \quad M^2 \mid cN^2M^3.$$

Dessa forma $M^2 \mid N^2m^3$, e como $mdc(m, M) = 1$, temos que $M^2 \mid N^2$, ou seja $M \mid N$. Com isso, temos que

$$M^3 \mid M^3n^2 - aN^2Mm^2 - bN^2M^2m - cN^2M^3.$$

Dai, temos que $M^3 \mid N^2m^3$ e como $mdc(m, M) = 1$ temos $M^3 \mid N^2$. Assim, vemos que $N^2 \mid M^3$ e $M^3 \mid N^2$, logo $M^3 = N^2$.

Durante a demonstração, mostramos que $M \mid N$. Então, se nós deixarmos $\ell = \frac{N}{M}$, então teremos que

$$\ell^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M \quad \text{e} \quad \ell^3 = \frac{N^2}{M^3} = \frac{N^3}{N^2} = N.$$

Portanto,

$$x = \frac{m}{\ell^2} \quad \text{e} \quad y = \frac{n}{\ell^3}.$$

□

Definição 3.4.2. *Definimos $C(p^\nu)$ como o conjunto dos pontos racionais sobre a curva elíptica tal que $p^{2\nu}$ divide o denominador de x e $p^{3\nu}$ divide o denominador de y. Em outras palavras,*

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

Por convenção, incluiremos o elemento $\mathcal{O}$ em todo $C(p^\nu)$.

Por exemplo, temos que $C(p)$ é o conjunto onde p está no denominador de x e y, e então existe ao menos um p^2 em x e um p^3 em y. Temos a inclusão

$$E(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \supset \cdots .$$

Nosso objetivo é mostrar que se (x, y) é um ponto de ordem finita, então x e y são inteiros. Para isso, nossa estratégia é mostrar que para todo primo p, os denominadores de x e y não são divisíveis por p. Isto significa que queremos mostrar que um ponto de ordem finita não pertence a $C(p^\nu)$. O primeiro passo para mostrar isso é provar a proposição a seguir.

Proposição 3.4.2. *$C(p^\nu)$ é um subgrupo de $E(\mathbb{Q})$.*

Demonstração. Façamos a seguinte mudança de coordenada

$$t = \frac{x}{y} \quad \text{e} \quad s = \frac{1}{y}.$$

Então, a nossa curva $y^2 = x^3 + ax^2 + bx + c$ ficará da seguinte forma

$$s = t^3 + at^2 s + bts^2 + cs^3.$$

Com isso, transformamos nosso plano (x, y) no plano (t, s). Com exceção de $\mathcal{O}$ no plano (x, y) e quando $y = 0$, os pontos de ordem dois, no plano (t, s), existe uma bijeção entre os planos. Temos também que retas no plano (x, y) também corresponde a retas no plano (t, s). Tomemos a equação da reta no plano (x, y)

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

Podemos dividir a equação acima por νy, que nos dá uma equação para a reta correspondente no plano (t, s)

$$\frac{1}{\nu} = \frac{\lambda}{\nu}\frac{x}{y} + \frac{1}{y}, \quad \text{então} \quad s = \frac{\lambda}{\nu}t + \frac{1}{\nu}.$$

Observe que as retas que passam pela origem no plano (x, y) correspondem as retas verticais no plano (t, s). Portanto, podemos somar pontos no plano (t, s) pelo mesmo procedimento como no plano (x, y). Precisamos encontrar fórmulas explicítas.

Definimos o anel R_p como o conjunto de todos os números racionais tal que p não divide o denominador. Isto significa que

$$\{\forall\, x \in R_p \mid ord(x) \geq 0\}.$$

As unidades em R_p serão os números de ordem zero onde p não aparece no numerador ou no denominador.

Vamos olhar para a divisibilidade de nossas coordenadas t, s por potências de p, em particular, para pontos em $C(p)$. Seja (x, y) um ponto com coordenadas racionais em

$C(p^\nu)$. Por definição, temos que $ord(x) \leq -2\nu$ e $ord(y) \leq -3\nu$, então podemos escrever x e y como

$$x = \frac{m}{np^{2(\nu+i)}} \quad \text{e} \quad y = \frac{u}{wp^{3(\nu+i)}},$$

para algum $i \neq 0$. Usando nossas equações para t e s, temos

$$t = \frac{x}{y} = \frac{mw}{nu}p^{\nu+i} \quad \text{e} \quad s = \frac{1}{y} = \frac{w}{u}p^{3(\nu+i)}.$$

Portanto, nosso ponto (t, s) está em $C(p^\nu)$ se, e somente se $t \in p^\nu R_p$ e $s \in p^{3\nu}R_p$. Isto nos diz que p^ν divide o número dor de t e $p^{3\nu}$ divide o numerador de s. Então, para mostrar que $C(p^\nu)$ é um subgrupo, basta mostrar que se uma potência arbitrária de p divide a coordenada t de dois pontos P_1 e P_2, então a mesma potência de p dividirá a coordenada t da soma desses dois pontos.

Seja $P_1 = (t_1, s_1)$ e $P_2 = (t_2, s_2)$ dois pontos distintos sobre a curva. Existem dois casos possíveis a considerar:

- $t_1 = t_2$

  Se $t_1 = t_2$, então $P_1 = -P_2$, pela lei de adição. Então $P_1 + P_2$ deve ser um elemento de $C(p^\nu)$, pois a soma desses pontos é o ponto $(0, 0)$.

- $t_1 \neq t_2$

  Seja $s = \alpha t + \beta$ a reta que passa pelos pontos P_1 e P_2. O coeficiente angular da reta é dado por

  $$\alpha = \frac{s_2 - s_2}{t_2 - t_1}.$$

  Também sabemos que P_1 e P_2 satisfazem a equação

  $$s = t^3 + at^2s + bts^2 + cs^3.$$

  Assim, podemos tentar expressar o coeficente angular como uma função das coordenadas de P_1 e P_2. Assim,

  $$s_1 = t_1^3 + at_1^2s_1 + bt_1s_1^2 + cs_1^3 \quad \text{e} \quad s_2 = t_2^3 + at_2^2s_2 + bt_2s_2^2 + cs_2^3.$$

  Subtraímos a equação para P_1 da equação para P_2.

  $$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2s_2 - t_1^2s_1) + b(t_2s_2^2 - t_1s_1^2) + c(s_2^3 - s_1^3)$$

  Escrevemos de modo a incluir elementos em forma de $(t_2 - t_1)$ e $(s_2 - s_1)$

  $$s_2 - s_1 = t_2^3 - t_1^3 + a(t_2^2 - t_1^2) + at_1^2(s_2 - s_1) + b(t_2 - t_1) + bt(s_2^2 - s_1^2) + c(s_2^3 - s_1^3)$$

  Achamos agora uma equação para $(t_2 - t_1)$

  $$t_2 - t_1 = \frac{-s_1 + t_1^3 - t_2^3 + at_1^2s_1 + cs_1^3}{bs_2^2} + \frac{1 - a(t_2^2 - t_1^2) - at_1}{bs_2} + \frac{t_1s_1^2}{s_2^2} - \frac{cs_2}{b} - t_1$$

Temos que alguns termos são divisíveis por $(s_2 - s_1)$ e outros são divisíveis por $(t_2 - t_1)$. Podemos expressar essa relação em termos das equações acima, assim

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a(t_2 - t_1)s_2 + bs_2^2}{1 - at_1^2 - bt_1(s_2 + s_1) - c(s_2^2 + s_1 s_2 + s_1^2)}. \tag{3.1}$$

Por definição, sabemos que t_1, t_2, s_1, s_2 são todos elementos de $p^\nu R_p$. O numerador, satisfaz a condição que todo termo inclui dois dos elementos multiplicados juntos. Portanto, $p^{2\nu}$ divide o numerador, portanto é um elemento de $p^{2\nu}R_p$. O denominador, em que todos os termos, excepto 1, são divisíveis por $p^{2\nu}$ pelo mesmo argumento. Assim, se olharmos para todo o α, temos que $p^{2\nu}$ divide o numerador e não o denominador, o que nos dá que $\alpha \in p^{2\nu}R$.

Similarmente, se $P_1 = P_2$, então o coeficiente angular da reta tangente a curva em P_1 é dando derivando implicitamente

$$\alpha = \frac{ds}{dt}(P_1) = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2}.$$

Podemos ver que a expressão para α não muda quando $(t_1, s_1) = (t_2, s_2)$, portanto usaremos sempre a equação 3.1.

Seja $P_3 = (t_3, s_3)$ o terceiro ponto de intersecção da curva elíptica com a reta $s = \alpha t + \beta$ que passa pelos pontos P_1 e P_2. Para econtrarmos a equação que tem t_1, t_2 e t_3 como raiz, tomemos a equação da reta e a equação da curva no plano (t, s)

$$s = \alpha t + \beta \quad \text{e} \quad s = t^3 + at^2 s + bts^2 + cs^3,$$

fazendo a substituição

$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3,$$

fazendo a expansão

$$0 = (1 + a\alpha + \alpha^2 b + c\alpha^3)t^3 + (\alpha\beta + 2\alpha b\beta + 3c\alpha^2\beta)t^2 + (b\beta^2 + 3c\alpha\beta^2 - \alpha)t + c\beta^3 - \beta.$$

Com isso, comparamos os coeficientes de t^3 e t^2 e achamos a soma das raízes

$$t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2\alpha b\beta + 3c\alpha^2\beta}{1 + a\alpha + \alpha^2 b + c\alpha^3}.$$

Com isto, temos uma fórmula para calcular t_3 dados apenas t_1 e t_2, e portanto nos permite achar $P_1 + P_2$ para qualquer P_1, P_2 sobre a curva.

Da nossa equação da reta que passa por P_1 e P_2, sabemos que

$$s_1 = \alpha t_1 + \beta,$$

pois $s_1 \in p^\nu R_p$, sabemos que

Uma vez que $s_1 \in p^{3\nu}R_p$, $\alpha \in p^{2\nu}R_p$ e $t_1 \in p^{\nu}R_p$, segue da fórmula

$$\beta = s_1 - \alpha t_1$$

que $\beta \in p^{3\nu}R_p$. Portanto, vemos que o denominador de $t_1 + t_2 + t_3$ é uma unidade em R_p. Assim, temos que

$$t_1 + t_2 + t_3 \in p^{3\nu}R_p.$$

Sabemos, por afirmação, que t_1 e t_2 são elementos de $p^{\nu}R_p$, então t_3 deve ser um elemento de $p^{\nu}R_p$, o que implica que $-t_3 \in p^{\nu}R_p$. Portanto, se as coordenadas t de P_1 e P_2 estão em $p^{\nu}R_p$, então a coordenada t de $P_1 + P_2$ também está em $p^{\nu}R_p$. Portanto, se a coordenada t de $P = (t, s)$ pertence a $p^{\nu}R$, então é claro que a coordenada t de $-P = (-t, -s)$ tam,bém pertence a $p^{\nu}R$. Com isso, temos que $C(p^{\nu})$ é fechado sobre a adição, e portanto é um subgrupo de $E(\mathbb{Q})$.

□

Ao provar que $C(p^{\nu})$ é um subgrupo de $E(\mathbb{Q})$, também provamos um resultado um pouco mais forte. Provamos que

$$t_1 + t_2 + t_3 \in p^{3\nu}R_p.$$

Assim, sabemos que, para qualquer $P_1, P_2 \in C(p^{\nu})$,

$$t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\nu}R_p,$$

onde $t(P)$ é a coordenada t de P. Então, se P é dado em coordenadas (x, y), ou seja, $(x_P, y(P))$, então

$$t(P) = \frac{x_P}{y(P)}.$$

Essa última fórmula nos diz mais do que o simples fato de que $C(p^{\nu})$ é um subgrupo. Ela nos diz que t_1, t_2 e t_3 devem ser divisiveis por $p^{3\nu}R_p$. Em outras palavras

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu}R_p}.$$

Note que o $(+)$ em $P_1 + P_2$ é a adição sobre nossa curva, enquanto o $(+)$ em $t(P_1) + t(P_2)$ é a adição em R_p, que é apenas uma adição de números racionais.

Considere a aplicação

$$\begin{array}{rcl} C(p^{\nu}) & \longrightarrow & \mathbb{Q} \\ P = (x, y) & \longmapsto & t(P) = \dfrac{x}{y} \end{array}$$

Essa aplicação parece ser um homomorfismo de elementos que segue a lei de adição de uma curva elíptica a um grupo aditivo de números racionais, mas o fato de que

$$t(P_1 + P_2) \neq t(P_1) + t(P_2)$$

não chega a torná-lo um homomorfismo.

Contudo, o que queremos é um homomorfismo de $C(p^\nu)$ para o grupo quociente

$$\frac{p^\nu R_p}{p^{3\nu} R_p},$$

enviando P em $t(P)$. O núcleo desse homomorfismo consiste de todos os pontos P tal que $t(P) \in p^{3\nu} R_p$. Portanto, o núcleo é apenas $C(p^{3\nu})$, e pelo Teorema do Isomorfismo obtemos

$$\begin{aligned} \frac{C(p^\nu)}{C(p^{3\nu})} &\longrightarrow \frac{p^\nu R_p}{p^{3\nu} R_p} \\ P = (x, y) &\longmapsto t(P) = \frac{x}{y}, \end{aligned}$$

que é um o homomorfismo.

Corolário 3.4.1. *Para todo primo p, o subgrupo $C(p)$ não contém pontos de ordem finita, exceto $\mathcal{O}$.*

Demonstração. Seja P um ponto de ordem m. Seja p algum número primo. Como $P \neq \mathcal{O}$, sabemos que $m > 1$. Queremos mostrar que $P \notin C(p)$. Vamos supor que $P \in C(p)$. O ponto P está contido em algum subgrupo menor $C(p^\nu)$, pois o denominador de x não pode ser divísivel por potências arbitrariamentes altas de p. Portanto, deve existir algum $\nu > 0$ tal que $P \in C(p^\nu)$, mas $P \notin C(p^{\nu+1})$. Tomemos esse p, nesse caso existe dois casos possíveis para considerar.

Vamos supor primeiro que $p \nmid m$. Temos que

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu} R_p},$$

pois P é um ponto de ordem m. Somando ele m vezes, temos

$$t(mP) \equiv mt(P) \pmod{p^{3\nu} R_p}.$$

Uma vez que $mP = \mathcal{O}$, temos $t(\mathcal{O}) = 0$. Por outro lado, como $mdc(m, p) = 1$, ele é uma unidade em R. Portanto

$$0 \equiv t(P) \pmod{p^{3\nu} R_p}.$$

Isto significa que $P \in C(p^{3\nu})$, o que contradiz o fato de que $P \notin C(p^{\nu+1})$.

Agora, suponha que $p \mid m$. Como p divide m, temos que $m = pn$ para algum $n \in \mathbb{Z}$. Se tomarmos $P' = nP$, então P' tem ordem p e é um elemento de $C(p)$, pois $P \in C(p)$. Como $C(p)$ é um subgrupo, vemos que $P' \in C(p^\nu)$, mas $P' \notin C(p^{\nu+1})$. Simirlamente ao primeiro caso, temos

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \pmod{p^{3\nu} R_p}.$$

Isso signfica que

$$t(P') \equiv 0 \pmod{p^{3\nu-1}R_p}.$$

Isto nos dá que $P' \in C(p^{3\nu-1})$, o que contradiz o fato de que $P' \notin C(p^{\nu+1})$, uma vez que $3\nu - 1 > \nu + 1$. □

Corolário 3.4.2. *Se $P = (x, y) \neq \mathcal{O}$ é um ponto racional de ordem finita, então x e y são inteirios.*

Demonstração. Uma vez que não existe pontos de ordem finita em $C(p)$, para qualquer p primo, todos os pontos de ordem finita não tem um denominador que possa ser divido por qualquer primo, e portanto deve ter coordenadas inteiras. □

O Teorema de Nagell-Lutz é importante na medida em que ele fornece um método para encontrar os pontos de ordem finita em uma curva elíptica. Isso faz com que o teorema seja uma ferramenta muito útil para analizar uma curva elíptica.

Teorema 3.4.1 (Nagell-Lutz)**.** *Seja*

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

uma curva elíptica com coeficentes inteiros, e seja

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

o discriminante da curva. Seja $P = (x, y)$ um ponto de ordem finita. Então x e y são inteiros, e ou $y = 0$, no caso P tem ordem dois, ou então $y \mid \Delta$.

Demonstração. Já "está" provado acima. □

Devemos deixar claro que o Teorema de Nagell-Lutz não é uma afirmação "se e somente se". É completamente possível que tenhamos pontos com coordeadas inteiras e com $y \mid \Delta$, mas que tenha ordem infinita. O teorema pode ser usado para fornecer uma lista de pontos que inclui todos os pontos de ordem finita, mas isso nunca pode ser usado para provar que qualquer ponto em particular, na verdade, tem ordem finita.

4 Tereoma de Mordell

O objetivo deste capítulo é demonstrar o teorema de Mordell. Para isso, existe uma ferrmamenta usada na prova chamada altura. A altura de um ponto racional mede o quanto o ponto é complexo do ponto de vista da Teoria dos Números.

4.1 Teorema de Descida

Teorema 4.1.1 (Descida)**.** *Seja $E(\mathbb{Q})$ um grupo comutativo. Suponha que existe uma função*

$$h : E(\mathbb{Q}) \longrightarrow [0, \infty)$$

com as seguintes propriedades.

1. *Para cada número real M, o conjunto*

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq M\} < \infty$$

2. *Para cada $P_0 \in E(\mathbb{Q})$, existe uma constante κ_0 tal que*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \qquad \forall\, P \in E(\mathbb{Q}).$$

3. *Existe uma constante κ tal que*

$$h(2P) \geq 4h(P) - \kappa, \qquad \forall\, P \in E(\mathbb{Q}).$$

4. *O subgrupo $2E(\mathbb{Q})$ tem índice finito em $E(\mathbb{Q})$.*

Então $E(\mathbb{Q})$ é finitamente gerado.

Demonstração. Como $2E(\mathbb{Q})$ é um subgrupo de $E(\mathbb{Q})$ com indíce finito então existem somente um número finito de classes laterais de $2E(\mathbb{Q})$ em $E(\mathbb{Q})$. Seja

$$\begin{aligned} \overline{P} &= \{Q \in E(\mathbb{Q}) \mid P - Q \in 2E(\mathbb{Q})\} \\ &= \{Q \in E(\mathbb{Q}) \mid P \sim Q\} \\ E(\mathbb{Q}) &= \bigsqcup_{P \in E(\mathbb{Q})} \overline{P} \end{aligned}$$

Assuma que

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} = \{\overline{Q_1}, \ldots, \overline{Q_n}\}.$$

Temos que

$$\forall\, P \in E(\mathbb{Q}) \Longrightarrow \overline{P} = \overline{Q_i}, \quad P - Q_{i_1} \in 2E(\mathbb{Q}),$$

ou seja,

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

para algum $P_1 \in E(\mathbb{Q})$. Fazendo esse processo, podemos escrever

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

Onde $\overline{Q_{i_j}} \in \{\overline{Q_1}, \ldots, \overline{Q_n}\}$. Dessa forma, temos

$$\begin{aligned} P &= Q_{i_1} + 2P_1 \\ P &= Q_{i_1} + 2Q_{i_2} + 4P_2 \\ P &= Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + 8P_3 \\ &\vdots \\ P &= Q_{i_1} + 2Q_{i_2} + 2^2Q_{i_3} + 2^3Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^mP_m. \end{aligned}$$

Assim, todo $P \in E(\mathbb{Q})$ pode ser reprensentado pelo conjunto finito $\{\overline{Q_1}, \ldots, \overline{Q_n}\}$ e algum P_m. Agora, se provarmos que se escolhermos um m suficientemente grande, então a altura de P_m é sempre menor que alguma constante. Pelo item (a), sabemos que os conjuntos de P_m será finito.

Usando o item (b) e substituindo P_0 por $-Q_i$, acharemos a constante κ_i, e assim

$$h(P - Q_i) \leq 2h(P) + \kappa_i, \qquad \forall\, P \in E(\mathbb{Q}).$$

Repetimos o processo para cada Q_i, $1 \leq i \leq n$. Seja $\kappa' = \max\{k_i, i = 1, 2, \ldots, n\}$, então

$$h(P - Q_i) \leq 2h(P) + \kappa', \qquad \forall\, P \in E(\mathbb{Q}) \text{ e todo } 1 \leq i \leq n.$$

Podemos fazer isso pois existe um número finito de Q_i. Dos itens (b) e (c), temos a desigualdade

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

Logo

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)). \end{aligned}$$

De modo que, se $h(P_{j-1}) \geq \kappa' + \kappa$, então

$$h(P_j) \leq \frac{3}{4}(P_{j-1}).$$

Se $h(P_m) \leq \kappa' + \kappa$, temos por (a) que P_m é um conjunto finito. Se $h(P_m) \geq \kappa' + \kappa$, então

$$h(P_j) \leq \frac{3}{4}(P_{j-1}).$$

De fato, sempre poderemos achar um $h(P_{m+i})$ para algum $i > 0$ tal que $h(P_{m+i}) \leq \kappa' + \kappa$. Ou seja, $h(P_{m+i})$ é um conjunto finito.

Se $P \in E(\mathbb{Q})$, então podemos expressar P da seguinte forma

$$P = a_1Q_1 + a_2Q_2 + \cdots + a_nQ_n + 2^mR$$

para certos inteiros $a_1, \cdots, a_n$ e algum ponto $R \in E(\mathbb{Q})$ satisfazendo a desigualdade $h(R) \leq \kappa' + \kappa$. Uma vez que P é um ponto arbitrário de $E(\mathbb{Q})$, temos que o conjunto

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in E(\mathbb{Q}) \mid h(R) \leq \kappa' + \kappa\}$$

gera $E(\mathbb{Q})$. Dos itens (a) e (d), este conjunto é finito. Portanto $E(\mathbb{Q})$ é finitamente gerado. □

4.2 Altura de Pontos Racionais

Definição 4.2.1. *Para todo $x \in \mathbb{Q}$, com $x = \frac{m}{n}$, onde $mdc(m, n) = 1$, definimos a altura $H : \mathbb{Q} \longrightarrow \mathbb{Z}^+$ como*

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

Propriedade 1 (Propriedade da finitude da Altura)**.** *Seja K uma constante. Temos que*

$$\left\{x = \frac{m}{n} \in \mathbb{Q} \mid H(x) \leq K\right\} < \infty$$

Demonstração. Seja $x = \frac{m}{n}$. Assim, temos que

$$-k \leq m \leq k \quad \text{e} \quad 1 \leq n \leq k,$$

pois não precisamos considerar os valores negativos de n. Temos assim $2k + 1$ escolhas para m e k valores para n. Portanto, há, no máximo $(2k+1)k = 2k^2+k$ números racionais com a altura menor ou igual a k. □

Definição 4.2.2. *Se*

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

é uma curva elíptica com $a, b, c \in \mathbb{Z}$, e $P = (x, y)$ é um ponto racional sobre a curva, definiremos a altura de P como a altura da coordenada x.

$$H(P) = H(x).$$

Definição 4.2.3. *Seja a curva elíptica E com coeficientes inteiros. Definimos a altura $h : \mathcal{C} \longrightarrow \mathbb{R}^+$ como*

$$h(P) = \log H(P)$$

Por motivos de notação, é mais interessante ter uma função que se comporta de forma aditiva e, por isso, trabalhar com h é mais conveniente.

Definição 4.2.4. *Seja $\mathcal{O}$ o ponto no infinito. Definimos a altura de $\mathcal{O}$ como*

$$H(\mathcal{O}) = 1 \quad ou \quad h(\mathcal{O}) = 0.$$

Observação 4.2.1. *A condição de que $mdc(m, n) = 1$ na definição de $H(x)$ implica que $H(0) = 1$, pois a única possibilidade de escrever o 0 na forma $\frac{m}{n}$ com $mdc(m, n) = 1$ é quando $\frac{0}{\pm 1}$. Como $|n| = |-n|$, $\forall n \in \mathbb{Z}$, a altura H está bem definida para qualqer número racional. Dai, temos*

$$h(x) = \log H(x) \geq \log 1 = 0.$$

Portanto, $h \in \mathbb{R}^+$.

Nosso objetivo é mostrar que o grupo dos pontos racionais $E(\mathbb{Q})$ é finitamente gerado. Para isso, precisamos mostrar quatro lemas.

Lema 4.2.1. *Para todo numéro real M, temos que o conjunto*

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq M\} < \infty.$$

Demonstração. Seja $x = \frac{m}{n}$, com $m, n \in \mathbb{Z}, n \neq 0$, e $mdc(m, n) = 1$ e $H(x) = \max\{|m|, |n|\}$. Temos que

$$h(P) = h(x) = \log H(x) < M \iff H(x) < e^M \iff |m|, |n| < e^M.$$

Como $-e^M < m, n < e^M$, existe um número finito de possibilidades para escolhe-los. Portanto, existe um número finito de escolhas para x, mas para cada x temos no máximo dois pontos, uma vez que y é dado por $y^2 = f(x)$. Portanto, existe somente um número finito de escolhas para $P = (x, y) \in E(\mathbb{Q})$. □

Lema 4.2.2. *Seja P_0 um ponto racional fixo sobre a curva. Existe uma constante κ_0, dependendo de P_0 e de a, b, c tal que*

$$h(P + P_0) \leq 2h(P) + \kappa_0, \, \forall \, P \in E(\mathbb{Q}).$$

Demonstração. Se $P_0 = \mathcal{O}$, o resultasdo é trivial pois

$$h(P) \leq 2h(P) + \kappa_0.$$

Suponha agora que $P_0 = (x_0, y_0) \neq \mathcal{O}$ e $P \in E(\mathbb{Q})$ com $P = (x, y) \notin \{P_0, -P_0, \mathcal{O}\}$. Tomemos $P + P_0 = (\widetilde{x}, \widetilde{y})$. Assim,

$$\widetilde{x} + x + x_0 = \lambda^2 - a, \quad \lambda = \frac{y - y_0}{x - x_0}.$$

Daí,

$$\begin{aligned}
\widetilde{x} &= \lambda^2 - a - x - x_0 \\
\widetilde{x} &= \left(\frac{y - y_0}{x - x_0}\right)^2 - a - x - x_0 \\
\widetilde{x} &= \frac{(y - y_0)^2 - a(x - x_0)^2 - (x - x_0)^2(x + x_0)}{(x - x_0)^2} \\
\widetilde{x} &= \frac{y^2 - 2yy_0 + y_0^2 - x^3 + x^2x_0 - ax^2 + xx_0 + 2axx_0 - x_0^3 - ax_0^2}{x^2 - 2xx_0 + x_0^2}
\end{aligned}$$

Podemos substituir $y^2 - x^3$ usando a equação da curva elíptica, pois o ponto $P = (x, y) \in E(\mathbb{Q})$, assim

$$\widetilde{x} = \frac{(-2y_0)y + (x_0)x^2 + (b + x_0^2 + 2ax_0)x + (c + y_0^2 - x_0^3 - ax_0^2)}{x^2 + (-2x_0)x + x_0^2}$$

e ficamos com a expressão

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

onde $A, B, C, D, E, F, G \in \mathbb{Q}$ são constantes que dependem a, b e (x_0, y_0). Conseguimos uma expressão semelhante para $\widetilde{x}$ com $A, B, C, D, E, F, G \in \mathbb{Z}$ multiplicando o numerador e o denominador por um inteiro conveniente. Substituindo $x = \frac{m}{\ell^2}$ e $x = \frac{n}{\ell^3}$, temos

$$\begin{aligned}
\widetilde{x} &= \frac{A\frac{n}{\ell^3} + B\frac{m^2}{\ell^4} + C\frac{m}{\ell^2} + D}{E\frac{m^2}{\ell^4} + F\frac{m}{\ell^2} + G} \\
\widetilde{x} &= \frac{A\ell n + Bm^2 + Cm\ell^2 + D\ell^4}{Em^2 + Fm\ell^2 + G\ell^4}
\end{aligned}$$

Agora, estamos próximos do resultado que queremos. Note que temos uma expressão para $\widetilde{x}$ como um inteiro divido por um inteiro. Não sabemos como é esta expressão na forma irredutível, mas certamente temos que

$$H(P + P_0) = H(\widetilde{x}) \leq \max\{|A\ell n + Bm^2 + Cm\ell^2 + D\ell^4|, |Em^2 + Fm\ell^2 + G\ell^4|\}.$$

Temos que

$$H(P) = \max\{|m|, |\ell^2|\} \Longrightarrow |m| \leq H(P) \quad \text{e} \quad \ell^2 \leq H(P) \Rightarrow \ell \leq H(P)^{\frac{1}{2}}.$$

Podemos também limitar o numerador da coordenada y em termos de $H(P)$. Para mostrar isso, usamos o fato de que o ponto $P = \left(\frac{m}{\ell^2}, \frac{n}{\ell^3}\right)$ satisfaz a equação, assim

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c \\ \frac{n^2}{\ell^6} &= \frac{m^3}{\ell^6} + a\frac{m^2}{\ell^4} + b\frac{m}{\ell^2} + c \\ n^2 &= m^3 + am^2\ell^2 + bm\ell^4 + c\ell^6 \\ |n^2| &\leq |m^3| + |am^2\ell^2| + |bm\ell^4| + |c\ell^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \\ &= (1 + |a| + |b| + |c|)H(P)^3 \end{aligned}$$

Tome $K = \sqrt{1 + |a| + |b| + |c|}$, assim

$$\begin{aligned} |n^2| &\leq K^2 H(P)^3 \\ |n| &\leq K H(P)^{\frac{3}{2}} \end{aligned}$$

Usando essas desigualdades e a desigualdade triangular, temos

$$|A\ell n + Bm^2 + Cm\ell^2 + D\ell^4| \leq |A\ell n| + |Bm^2| + |Cm\ell^2| + |D\ell^4| \leq (|Ak| + |B| + |C| + |D|)H(P)^2,$$

e

$$|Em^2 + Fm\ell^2 + G\ell^4| \leq |Em^2| + |Fm\ell^2| + |G\ell^4| \leq (|E| + |F| + |G|)H(P)^2.$$

Portanto

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

Aplicando o logarítmo em ambos od lados

$$h(P + P_0) = \log H(P + P_0) \leq 2h(P) + \kappa_0,$$

onde $\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$ dependedo somente de a, b, c e (x_0, y_0) não depende de $P = (x, y)$. □

Lema 4.2.3. *Existe uma constante κ, dependendo de a, b, c tal que*

$$h(2P) \geq 4h(P) - \kappa, \, \forall \, P \in E(\mathbb{Q}).$$

Demonstração. Seja $P = (x, y)$ e $2P = (\overline{x}, \overline{y})$. Da fórmula da duplicação, temos

$$\overline{x} + 2x = \lambda^2 - a, \quad \lambda = \frac{f'(x)}{2y}.$$

Assim,

$$\begin{aligned}
\overline{x} &= \lambda^2 - a - 2x \\
\overline{x} &= \left(\frac{f'(x)}{2y}\right)^2 - a - 2x \\
&= \frac{f'(x)^2}{4f(x)} - a - 2x \\
&= \frac{f'(x)^2 - 4(a+2x)f(x)}{4f(x)} \\
\overline{x} &= \frac{\varphi(x)}{\psi(x)},
\end{aligned}$$

onde $\varphi, \psi \in \mathbb{Z}[x]$ e $\deg\varphi = 4$ e $\deg\psi = 3$. Se φ e ψ têm raízes comum, então f e f' teriam raízes em comum, o que contradiz o fato de que a curva elíptica é não singular. Para finalizar a demonstração, precisamos do seguinte lema.

Lema 4.2.4. *Seja $\varphi(x), \psi(x) \in \mathbb{Z}[x]$ polinômios sem raízes complexas comuns. Seja $d = \max\{\deg(\varphi), \deg(\psi)\}$. Então*

1. *Existe um inteiro $R \geq 1$, dependendo de φ e ψ, tal que*
$$\forall\, \frac{m}{n} \in \mathbb{Q}, \quad mdc\left(n^d\varphi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \mid R.$$

   Demonstração. Note que
$$\deg(\varphi), \deg(\psi) \leq d \Longrightarrow n^d\varphi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right) \in \mathbb{Z}.$$
   Sem perda de generalidade, suponha $\deg(\varphi) = d \geq \deg(\psi) = e$, com
$$\begin{aligned}
\varphi(x) &= a_0x^d + a_1x^{d-1} + \cdots + a_d \\
\psi(x) &= b_0x^e + b_1x^{e-1} + \cdots + b_e,
\end{aligned}$$
   daí
$$\begin{aligned}
\Phi(m,n) &= n^d\varphi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d \\
\Psi(m,n) &= n^d\psi\left(\frac{m}{n}\right) = b_0m^en^{d-e} + b_1m^{e-1}n^{d-e-1} + \cdots + b_en^d.
\end{aligned}$$
   Temos que $mdc(\varphi(x), \psi(x)) = 1$ em $\mathbb{Q}[x]$, portanto eles geram um ideal unitário, logo existem $F(x), G(x) \in \mathbb{Q}[x]$ tais que
$$F(x)\varphi(x) + G(x)\psi(x) = 1.$$
   Seja $A \in \mathbb{Z}$, grande o suficiente, de tal maneira que valha $AF(x), AG(x) \in \mathbb{Z}[x]$. Tome $D = \max\{\deg F(x), \deg G(x)\}$. Note que A e D não dependem de m ou n. Segue que
$$\left\{n^dDF\left(\frac{m}{n}\right)\right\}\Phi(m,n) + \left\{n^dAG\left(\frac{m}{n}\right)\right\}\Psi(m,n) = An^{D+d}.$$

Seja $E(\mathbb{Q}) = E(\mathbb{Q})(m,n) = mdc(\Phi(m,n), \Psi(m,n))$. Da equação acima, temos que $E(\mathbb{Q}) \mid An^{D+d}$. Temos que

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

Disto, concluímos que

$$E(\mathbb{Q}) \mid Aa_0m^dn^{D+d-1},$$

portanto

$$\begin{aligned} E(\mathbb{Q}) \mid mdc(An^{D+d}, Aa_0m^dn^{D+d-1}) &= An^{D+d-1}mdc(a_0m^d, n) \\ &= An^{D+d-1}mdc(a_0, n) \\ &= Aa_0n^{D+d-1}. \end{aligned}$$

Portanto, $E(\mathbb{Q}) \mid Aa_0n^{D+d-1}$. Para $i > 0$, conseguimos provar que $E(\mathbb{Q}) \mid Aa_0^in^{D+d-i}$. E para $i = D + d$, temos que

$$E(\mathbb{Q}) \mid Aa_0^{D+d}n^{D+d-(D+d)} = Aa_0^{D+d}.$$

Ou seja, provamos que $E(\mathbb{Q}) \mid Aa_0^{D+d}$. Tomando $R = Aa_0^{D+d}$, o lema segue. □

2. *Existem constantes κ_1, κ_2, dependendo de φ e ψ, tal que,*

$$\forall\, \frac{m}{n} \in \mathbb{Q},\ \textit{que não são raízes de } \psi,\quad dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\varphi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2.$$

Demonstração. Nesse caso, temos duas desigualdades a serem provadas. Porém, só estamos interessados na primeira desigualdade, isto é, na existência de κ_1. A existência de κ_2 é provada de forma análoga ao Lema 2. Seja $\frac{m}{n} \in \mathbb{Q}$ que não anula φ. Por definição, para qualquer número $r \in \mathbb{Q}^+$, temos que

$$h(r) = h\left(\frac{1}{r}\right).$$

Mais uma vez, podemos assumir que $\deg(\varphi) = d \geq \deg(\psi) = e$. Queremos uma estimativa para $h(\overline{x})$, tal que

$$h(\overline{x}) = \frac{\varphi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{n^d\varphi\left(\frac{m}{n}\right)}{n^d\psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}.$$

Provamos acima que existe um inteiro $R \geq 1$, que não depende de m e n, tal que

$$mdc(\Phi(m,n), \Psi(m,n)) \mid R.$$

Dai, temos que

$$\begin{aligned} H(\overline{x}) &= \max\left\{\frac{|\Phi(m,n)|}{mdc(\Phi(m,n),\Psi(m,n))}, \frac{|\Psi(m,n)|}{mdc(\Phi(m,n),\Psi(m,n))}\right\} \\ &\geq \frac{1}{R}\max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &= \frac{1}{R}\max\left\{\left|n^d\varphi\left(\frac{m}{n}\right)\right|, \left|n^d\psi\left(\frac{m}{n}\right)\right|\right\} \\ &\geq \frac{1}{2R}\left(\left|n^d\varphi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right). \end{aligned}$$

Queremos comparar

$$H(\overline{x}) = H\left(\frac{\varphi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \quad \text{e} \quad H\left(\frac{m}{n}\right)^d = \max\{|m|^d, |n|^d\}.$$

Assim, condiremos o quociente

$$\begin{aligned} \frac{H(\overline{x})}{H\left(\frac{m}{n}\right)^d} &\geq \frac{1}{2R}\frac{\left|n^d\varphi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|}{\max\{|m|^d, |n|^d\}} \\ &= \frac{1}{2R}\frac{\left|\varphi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}. \end{aligned}$$

Consideremos a função

$$p(t) = \frac{1}{2R}\frac{|\varphi(t)| + |\psi(t)|}{\max\{|t|^d, 1\}}.$$

Como o denominador não se anula, temos que

$$p(t) = 0 \Rightarrow |\varphi(t)| + |\psi(t)| = 0 \Rightarrow \varphi(t) = \psi(t),$$

o que contradiz a hípotese de que $\varphi(t)$ e $\psi(t)$ não tem raízes em comum. Logo, $p(t)$ é uma função contínua que não se anula. Assim,

$$\lim_{t\to\infty} p(t) = \lim_{t\to\infty} \frac{1}{2R}\frac{|\varphi(t)| + |\psi(t)|}{|t|^d} \in \mathbb{R}^*.$$

Por afirmação, temos que $\deg(\varphi) = d$ e $\deg\psi$ é no máximo d, logo $p(t)$ tem limite diferente de zero quanto $|t| \to \infty$. A continuidade nos garante que $p(t)$ tem um máximo e um mínimo em todo intervalo fechado, e o fato de que nunca se anula nos diz que dentro de um compacto $p(t)$ possui um minimo positivo $C_1 > 0$ tal que $p(t) > C_1$. Dai,

$$\frac{H(\overline{x})}{H\left(\frac{m}{n}\right)^d} \geq \frac{C_1}{2R} \Rightarrow H(\overline{x}) \geq \frac{C_1}{2R}H\left(\frac{m}{n}\right)^d,$$

aplicando o log em ambos os lados

$$\log H(\overline{x}) \geq \log\left(\frac{C_1}{2R}H\left(\frac{m}{n}\right)^d\right) \Rightarrow h(\overline{x}) \geq dh\left(\frac{m}{n}\right) - \kappa_1, \qquad \kappa_1 = \log\left(\frac{2R}{C_1}\right),$$

onde C_1 e R não dependem de m e n, para todo $\frac{m}{n} \in \mathbb{Q}$. □

Com isso, concluímos a demonstração do lema. □

4.3 Teorema de Mordell

A equação de $E(\mathbb{Q})$ é dada por

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

com $a, b, c \in \mathbb{Z}$ e $\Delta_f \neq 0$. Vimos que os pontos $P = (x, y) \in E(\mathbb{Q})$ de ordem dois são dados quando

$$y = 0 \Leftrightarrow f(x) = 0.$$

Uma vez que $f(x) = 0$, e f é um polinômio com coeficientes inteiros e coeficiente líder 1, temos que x é um número inteiro. Suponha que x_0 é uma raiz inteira de f. Fazendo uma mudança de coordenadas

$$x \to x - x_0,$$

podemos assumir que

$$x_0 = 0 \Rightarrow c = 0.$$

A condição para a não singularidade de C é

$$\begin{aligned} \Delta_f &= -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \\ &= a^2b^2 - 4b^3 \\ &= b^2(a^2 - 4b) \neq 0 \end{aligned}$$

Defina a curva $\overline{E}$ dada pela equação

$$\overline{E} : y^2 = \overline{f}(x) = x^3 + \overline{a}x^2 + \overline{b}x,$$

onde

$$\overline{a} = -2a \quad \text{e} \quad \overline{b} = a^2 - 4b.$$

Temos que

$$\begin{aligned} \Delta_{\overline{f}} &= \overline{b}^2(\overline{a}^2 - 4\overline{b}) \\ &= (a^2 - 4b)^2(4a^2 - 4a^2 + 16b) \\ &= 16b(a^2 - 4b)^2 \neq 0, \end{aligned}$$

e portanto, $\overline{E}(\mathbb{Q})$ é uma curva elíptica suave.

Proposição 4.3.1. *Seja $P = (x, y) \in E$, com $x \neq 0$. A aplicação*

$$\begin{aligned} \varphi : E &\longrightarrow \overline{E} \\ (x, y) &\longmapsto (\overline{x}, \overline{y}) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right) \end{aligned}$$

está bem definida.

Demonstração. Para mostrar que φ está bem definido, basta mostrar que $\overline{x}$ e $\overline{y}$ satisfazem a equação de $\overline{E}$.

$$\begin{aligned}
\overline{x}^3 + \overline{ax}^2 + \overline{bx} &= \overline{x}(\overline{x}^2 + \overline{ax} + b) \\
&= \overline{x}(\overline{x}^2 - 2a\overline{x} + (a^2 - 4b)) \\
&= \frac{y^2}{x^2}\left(\frac{y^4}{x^4} - \frac{2ay^2}{x^2} + a^2 - 4b\right) \\
&= \frac{y^2}{x^2}\left(\frac{y^4 - 2ax^2y^2 + a^2x^4 - 4bx^4}{x^4}\right) \\
&= \frac{y^2}{x^2}\left(\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right) \\
&= \frac{y^2}{x^6}((x^3 + ax^2 + bx - ax^2)^2 - 4bx^4) \\
&= \frac{y^2}{x^6}((x^3 + bx)^2 - 4bx^4) \\
&= \frac{y^2}{x^6}x^6 + 2bx^4 + b^2x^2 - 4bx^4 \\
&= \frac{y^2}{x^6}(x^3 - bx)^2 \\
&= \left(\frac{y(x^3 - bx)}{x^3}\right)^2 \\
&= \left(\frac{yx(x^2 - b)}{x^3}\right)^2 \\
&= \left(\frac{y(x^2 - b)}{x^2}\right)^2 = \overline{y}^2.
\end{aligned}$$

□

Com a mesma construção acima para $\overline{E}$, temos

$$\overline{\overline{E}}(\mathbb{Q}) : y^2 = \overline{\overline{f}}(x) = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x,$$

onde

$$\overline{\overline{a}} = -2\overline{a} = 4a \quad \text{e} \quad \overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = 4a^2 - 4(a^2 - 4b) = 16b.$$

Fazendo uma mudança de coordenas

$$\begin{aligned}
\overline{\varphi}\colon \overline{E} &\to \overline{\overline{E}} \\
(x, y) &\mapsto \left(\frac{x}{4}, \frac{y}{8}\right)
\end{aligned}$$

temos que

$$\begin{aligned}
(x, y) \in E(\mathbb{Q}) \Leftrightarrow y^2 &= x^3 + ax^2 + bx \\
64y^2 &= 64x^3 + 64ax^2 + 64bx \\
(8y)^2 &= (4x)^3 + 4a(4x)^2 + 16b(4x) \\
(8y)^2 &= (4x)^3 + \overline{\overline{a}}(4x)^2 + \overline{\overline{b}}(4x) = (4x, 8y) \in \overline{\overline{E}}(\mathbb{Q}).
\end{aligned}$$

Assim, o grupo de pontos racionais em $\overline{\overline{E}}$ é isomorfo ao grupo de pontos racionas em E.

Proposição 4.3.2. *Sejam E e $\overline{E}$ as curvas elípticas definidas acima.*

1. *Existe um homomorfismo $\varphi : E \to \overline{E}$ definido por:*

$$\varphi(P) = \begin{cases} \left(\dfrac{y^2}{x^2}, \dfrac{y(x^2-b)}{x^2}\right), & \text{se } P = (x,y) \neq \mathcal{O}, T, \\ \overline{\mathcal{O}}, & \text{se } P \in \{\mathcal{O}, T\} \end{cases}$$

Assim $\ker\varphi = \{\mathcal{O}, T\}$*, onde* $T = (0,0)$*.*

Demonstração. Vamos primeiro mostrar que φ está bem definida, ou seja, $\varphi(P) \in \overline{E}$, $\forall P \in E$. Se $P \in \{\mathcal{O}, T\}$, então $\varphi(P) = \overline{\mathcal{O}} \in \overline{E}$. Se $P \notin \{\mathcal{O}, T\}$, implica que $x \neq 0$. Temos que $\varphi(P) \in \overline{E}$ se, e somente se

$$\begin{aligned} \left(\frac{y(x^2-b)}{x^2}\right)^2 &= \left(\frac{y^2}{x^2}\right)^3 + \overline{a}\left(\frac{y^2}{x^2}\right)^2 + \overline{b}\left(\frac{y^2}{x^2}\right) \\ \frac{y^2(x^2-b)^2}{x^4} &= \frac{y^6}{x^6} - 2a\frac{y^4}{x^4} + (a^2-4b)\frac{y^2}{x^2} \end{aligned}$$

Se $y = 0$, a igualdade é verdadeira. Se $y \neq 0$, então a igualdade é equivalente a

$$\begin{aligned} (x^2-b)^2x^2 &= y^4 - 2ay^2x^2 + (a^2-4b)x^4 \\ (x^2-b)^2x^2 &= (y^2-ax^2)^2 - 4bx^4 \\ (x^3-bx)^2 &= (x^3+bx)^2 - 4bx^4 \end{aligned}$$

que equivale a

$$\begin{aligned} (a-b)^2 &= (a+b)^2 - 4ab \\ &= a^2 + 2ab + b^2 - 4ab \\ (a-b)^2 &= a^2 - 2ab + b^2 \end{aligned}$$

Logo, φ está bem definida. Dessa forma, vemos que $\varphi(E(\mathbb{Q})) \subset \overline{E}(\mathbb{Q})$. Provamos que φ é um homomorfismo de grupos. Temos que

$$\begin{cases} \varphi(\mathcal{O}) = \overline{\mathcal{O}}. \\ \varphi(P+\mathcal{O}) = \varphi(P) = \varphi(P) + \overline{\mathcal{O}} = \varphi(P) + \varphi(\mathcal{O}). \end{cases}$$

Queremos provar que

$$\varphi(P+T) = \varphi(P) + \varphi(T) = \varphi(P) + \varphi(\overline{\mathcal{O}}) = \varphi(P),\ \forall P \in E.$$

Para $P = \mathcal{O}$:

$$\varphi(\mathcal{O}+T) = \varphi(T) = \overline{\mathcal{O}} = \varphi(\mathcal{O}).$$

Para $P = T$:

$$\varphi(T+T) = \varphi(2T) = \varphi(\mathcal{O}) = \overline{\mathcal{O}} = \varphi(T).$$

Lembrando que, como $T = (0,0)$, então T é um ponto de ordem dois, pois $y = 0$. Agora, vamos assumir que $P \neq \{\mathcal{O}, T\}$. Assim, temos que $x \neq 0$. Agora, tomemos $P_1 = T =$ e pela fórmula da soma $P + T = (x_2, -y_2)$. Usando as fórmulas

$$\begin{cases} x_2 = \lambda^2 - a - x - x_1 \\ \lambda = \dfrac{y_1 - y}{x_1 - x} = \dfrac{y}{x} \\ y_2 = \lambda x_2 + \nu \end{cases}$$

Dai, temos

$$\begin{aligned} x(P+T) &= \lambda^2 - a - x - x_1 \\ &= \left(\frac{y}{x}\right)^2 - a - x - 0 \\ &= \left(\frac{y}{x}\right)^2 - a - x - 0 \\ &= \frac{b}{x} \end{aligned}$$

e

$$\begin{aligned} y(P+T) &= \lambda x(P+T) + \nu \\ &= \frac{y}{x}\frac{b}{x} \\ &= \frac{yb}{x^2} \end{aligned}$$

Assim, $P + T = (x_2, -y_2) = (x(P+T), y(P+T))$, ou seja, $\varphi(P+T) = (\overline{x}(P+T), \overline{y}(P+T))$. Daí, temos que

$$\begin{aligned} \overline{x}(P+T) &= \left(\frac{y(P+T)}{x(P+T)}\right)^2 \\ &= \left(\frac{\left(\frac{-by}{x^2}\right)^2}{\left(\frac{b}{x^2}\right)^2}\right) \\ &= \frac{b^2y^2}{x^4}\frac{x^2}{b^2} \\ &= \frac{y^2}{x^2} = \overline{x}(P), \end{aligned}$$

e também

$$\begin{aligned}
\overline{y}(P+T) &= \frac{y(P+T)x(P+T)^2 - b}{(x(P+T))^2} \\
&= \frac{\dfrac{-by}{x^2}\left(\left(\dfrac{b}{x}\right)^2 - b\right)}{\left(\dfrac{b}{x}\right)^2} \\
&= \frac{x^2}{b^2}\left(\frac{-by}{x^2}\frac{b^2 - bx^2}{x^2}\right) \\
&= \frac{b^2(-by + x^2 y)}{x^2 b^2} \\
&= \frac{y(x^2 - b)}{x^2} = \overline{y}(P).
\end{aligned}$$

Portanto, isso mostra que

$$\varphi(P+T) = \varphi(P).$$

Uma observação importante a se fazer é que, nos calculos acima, sempre assumimos que $b \neq 0$, pois $\Delta_f = b^2(a^2 - 4b) \neq 0$. Da definição do inverso de P, temos:

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

Agora, queremos provar que

$$\varphi(P_1) + \varphi(P_2) = \varphi(P_1 + P_2),\ \forall\, P_1, P_2 \in E(\mathbb{Q}).$$

Isso é equivalente a mostrar que

$$\varphi(P_1) + \varphi(P_2) - \varphi(P_1 + P_2) = \overline{\mathcal{O}}.$$

Para isso, é suficiente mostrar que dados três pontos colineares $P_1, P_2, P_3 \in E(\mathbb{Q})$ temos que $\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = 0$. A colinearidade de P_1, P_2, P_3 é equivalente a $P_1 + P_2 + P_3 = 0$. Pelas observações anteriores é suficiente considerar $P_i \notin \{\mathcal{O}, T\}$ com $i = 1, 2, 3$. Se dois ou três destes pontos coincidem, então a reta deve ser apropriadamente tangente a curva. Vamos assumir que os três pontos são distintos. Seja $r : y = \lambda x + \nu$ a equação da reta que passa pelos três pontos colineares P_1, P_2 e P_3. Para a reta que intercepta $\overline{E}$, tomamos

$$y = \overline{\lambda}x + \overline{\nu}, \quad \text{onde} \quad \overline{\lambda} = \frac{\nu\lambda - b}{\nu} \quad \text{e} \quad \overline{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}.$$

Notemos que $\nu \neq 0$, caso contrário, se $\nu = 0$ significaria que a reta r contém T, e por Bezout P_1, P_2 ou P_3 seriam igual a T, contradizendo a nossa suposição de

que P_1, P_2, P_3 são distintos de T. Seja $\varphi(P_i) = \varphi(x_i, y_i) = (\overline{x}_i, \overline{y}_i)$, $i = 1, 2, 3$. Para mostrar que $\varphi(P_i)$ está na reta r é sufciente mostrar que $\overline{y} = \overline{\lambda}\overline{x} + \overline{\nu}$.

$$\begin{aligned}
\overline{\lambda}\overline{x}_i + \overline{\nu} &= \frac{\nu\lambda - b}{\nu}\frac{y_i^2}{x_i^2} + \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu} \\
&= \frac{(\nu\lambda - b)y_i^2 + (\nu^2 - a\nu\lambda + b\lambda^2)x_i^2}{\nu x_i^2} \\
&= \frac{\nu\lambda y_i^2 - by_i^2 + \nu^2 x_i^2 - a\nu\lambda x_i^2 + b\lambda^2 x_i^2}{\nu x_i^2} \\
&= \frac{\nu\lambda(y_i^2 - ax_i^2) - b(y_i^2 - \lambda^2 x_i^2) + \nu^2 x_i^2}{\nu x_i^2} \\
&= \frac{\nu\lambda(y_i^2 - ax_i^2) - b(y_i - \lambda x_i)b(y_i + \lambda x_i) + \nu^2 x_i^2}{\nu x_i^2}
\end{aligned}$$

Substituindo $y_i^2 - ax_i^2 = x_i^3 + bx_i$ e $y_i - \lambda x_i = \nu$

$$\begin{aligned}
\overline{\lambda}\overline{x}_i + \overline{\nu} &= \frac{\nu\lambda(x_i^3 + b_i) - b\nu(y_i + \lambda x_i) + \nu^2 x_i^2}{\nu x_i^2} \\
&= \frac{\lambda(x_i^3 + b_i) - b(y_i + \lambda x_i) + \nu x_i^2}{x_i^2} \\
&= \frac{\lambda x_i^3 + \lambda b x_i - by_i - b\lambda x_i + \nu x_i^2}{x_i^2} \\
&= \frac{\lambda x_i^3 - by_i + \nu x_i^2}{x_i^2} \\
&= \frac{x_i^2(\lambda x_i + \nu - by_i)}{x_i^2} \\
&= \frac{y_i(x_i^2 - b)}{x_i^2} \\
&= \overline{y}_i,
\end{aligned}$$

para $i = 1, 2, 3$. Portanto, $\varphi(P_1)$, $\varphi(P_2)$ e $\varphi(P_3)$ são colineares. Temos que $\varphi : E \to \overline{E}$ é contínua, portanto, uma vez que φ é um homomorfismo para pontos distintos, por continuidade temos que é um homomorfismo geral. □

2. *Existe um homomorfismo $\psi : \overline{E} \to E$ definido por*

$$\psi(\overline{P}) = \begin{cases} \left(\dfrac{\overline{y}^2}{4\overline{x}^2}, \dfrac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right), & \text{se } \overline{P} = (\overline{x}, \overline{y}) \neq \overline{\mathcal{O}}, \overline{T}, \\ \mathcal{O}, & \text{se } \overline{P} \in \{\overline{\mathcal{O}}, \overline{T}\} \end{cases}$$

A composição $\psi \circ \varphi : C \to C$ é a multiplicação $\psi \circ \varphi(P) = 2P$.

Demonstração. Podemos ver de duas formas diferentes que ψ é um homomorfismo bem definido. De forma análoga que fizemos para φ, mostramos que ψ é um homomorfismo de grupos bem definido com $\ker \psi = \{\overline{\mathcal{O}}, \overline{T}\}$. Vimos acima que, $\overline{\overline{E}}$ é

isomorfa a E. Do item acima, temos um homomorfismo $\overline{\varphi} : \overline{E} \to \overline{\overline{E}}$. Uma vez que $\psi : \overline{E} \to E$ é uma composição de $\overline{\varphi}$ com o isomorfismo $\overline{\overline{E}} \to E$, mais uma vez, vemos que ψ é um homomorfismo de grupos bem definido. No resta verificar que $\psi \circ \varphi(P) = 2P, \forall P \in E(\mathbb{Q})$. Se $P \in \{\mathcal{O}, T\}$, temos que $\psi \circ \varphi(P) = \psi(\overline{\mathcal{O}}) = \mathcal{O} = 2P$, lembrando que T tem ordem dois em $E(\mathbb{Q})$. Agora, seja $P \notin \{\mathcal{O}, T\}$, isto é, $x, y \in \mathbb{Q}$ e $x \neq 0$. Assim,

$$\begin{aligned}
\psi \circ \varphi(P) &= \psi\left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) \\
&= \left(\frac{\frac{y^2(x^2-b)^2}{x^4}}{4\frac{y^4}{x^4}}, \frac{\frac{y(x^2-b)^2}{x^2}\left(\frac{y^4}{x^4} - a^2 + 4b\right)}{8\frac{y^4}{x^4}}\right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{x^2(x^2-b)}{8y^3}\left(\frac{y^4}{x^4} - a^2 + 4b\right)\right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4 + (4b-a^2)x^4)}{8y^3x^2}\right)
\end{aligned}$$

Temos que $\varphi(P) = \overline{T} \Leftrightarrow y = 0 \Leftrightarrow 2P = \mathcal{O}$. Se $2P = \mathcal{O}$, então $\psi(\varphi(P)) = \psi(\overline{T}) = \mathcal{O} = 2P$. Vamos assumir que $y \neq 0$. Temos que $y^2 = x^3 + ax^2 + bx \Rightarrow y^2 = x(x^2 + ax + n)$, logo $y^4 = x^2(x^2 + ax + n)^2$. Substiuindo na última expressão, temos

$$\begin{aligned}
\psi \circ \varphi(P) &= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^2(x^2+ax+n)^2 + (4b-a^2)x^4)}{8y^3x^2}\right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)((x^2+ax+n)^2 + (4b-a^2)x^4)}{8y^3}\right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)((x^2+ax+n)^2 + (4b-a^2)x^4)}{8y^3}\right) \\
&= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3}\right)
\end{aligned}$$

Agora, para mostrar a igual, devemos calcularx_{2P} e y_{2P}.

$$\begin{aligned}
x_{2P} &= \lambda^2 - a - 2x \\
&= \frac{f'(x)^2}{4y^2} - a - 2x \\
&= \frac{(3x^2 + 2ax + b)^2}{4(x^3 + ax^2 + bx)} - a - 2x \\
&= \frac{(3x^2 + 2ax + b)^2 - 4(x^3 + ax^2 + bx)(2x + a)}{4y^2} \\
&= \frac{9x^4 + 12ax^3 + (4a^2 + 6b)x^2 + 4abx + b^2 - 8x^4 - 12ax^3 - (4a^2 + 8b)x^2 - 4abx}{4y^2} \\
&= \frac{x^4 - 2bx^2 + b^2}{4y^2} \Rightarrow x_{2P} = \frac{(x^2-b)^2}{4y^2}
\end{aligned}$$

E agora y_{2P}

$$\begin{aligned}
y_{2P} &= -\lambda x_{2P} - \nu \\
&= -\lambda x_{2P} - (y - \lambda x) \\
&= -\left(\frac{f'(x)}{2y}\left(\frac{(x^2-b)^2}{4y^2} - x\right) + y\right) \\
&= -\frac{3x^2+2ax+b}{2y}\frac{x^4-2bx^2+b^2-4x(x^3+ax^2+bx)}{4y^2} - y \\
&= -\frac{(3x^2+2ax+b)(x^4-2bx^2+b^2-4x(x^3+ax^2+bx)) + 8(x^3+ax^2+bx)^2}{8y^3} \\
&= -\frac{f'(x)((x^2-b)^2-4xf(x)) + 8(f(x))^2}{8y^3} \\
&= -\frac{f'(x)(x^2-b)^2 - 4f(x)(xf'(x) - 2f(x))}{8y^3} \\
&= -\frac{f'(x)(x^2-b)^2 - 4f(x)(3x^3+2ax^2+bx-2x^3-2ax^2-2bx)}{8y^3} \\
&= -\frac{f'(x)(x^2-b)(x^2-b) + 4xf(x)}{4xf(x)} \\
&= \frac{(x^2-b)(-3x^4-2ax^3+2bx^2+2abx+b^2+4x^4+4ax^3+4bx^2)}{8y^3} \\
y_{2P} &= \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}
\end{aligned}$$

Portanto, $\psi \circ \varphi(P) = 2P$. Analogamente, temos que $\varphi \circ \psi(\overline{P}) = 2\overline{P}$. □

Podemos argumentar que sendo φ um homomorfismo, temos

$$\varphi(2P) = \varphi(P+P) = \varphi(P) + \varphi(P) = 2\varphi(P).$$

Ou seja, provamos que $\psi \circ \varphi(P) = 2P$, sendo $\psi(\varphi(P)) = 2(\varphi(P))$. Agora, $\varphi : E \to \overline{E}$ é uma função de pontos complexos, então para qualquer $\overline{P} \in \overline{E}$, nós podemos achar $P \in E$ com $\varphi(P) = \overline{P}$. Portanto $\varphi \circ (\overline{P}) = 2\overline{P}$.

Lembremos que provamos que $\psi \circ \varphi(P) = 2P$ para pontos com $x, y \neq 0$, pois as fórmulas acima não são válidas se x ou y é zero. Nos casos em que P é um ponto de ordem dois, temos que $\psi \circ \varphi(P) = \mathcal{O}$. Ou seja, se $P = (x, 0) \Rightarrow \varphi(P) = \overline{T}$, logo $\psi \circ \varphi(P) = \mathcal{O}$. Se $x = 0 \Rightarrow P = T$, e então $\varphi(T) = \mathcal{O}$.

Sejam as curvas

$$E : y^2 = x^3 + ax^2 + bx \quad \text{e} \quad \overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x,$$

onde

$$\overline{a} = -2a \quad \text{e} \quad \overline{b} = a^2 - 4b,$$

e temos os homomorfismos

$$\varphi : E \to \overline{E} \quad \text{e} \quad \psi : \overline{E} \to E.$$

Propriedade 2. *Seja $\varphi(E(\mathbb{Q}))$ o subgrupo de $\overline{E(\mathbb{Q})}$, tal que $\overline{P} \in \overline{E(\mathbb{Q})}$ é $\varphi(P)$, com $P \in E(\mathbb{Q})$. Temos:*

1. $\overline{\mathcal{O}} \in \varphi(E(\mathbb{Q}))$

   Demonstração. Temos que $\overline{\mathcal{O}} \in \varphi(E(\mathbb{Q}))$, uma vez que nosso homomorfismo define que $\varphi(\mathcal{O}) = \overline{\mathcal{O}}$. □

2. $\overline{T} = (0,0) \in \varphi(E(\mathbb{Q}))$ *se, e somente se* $\overline{b} = a^2 - 4b$ *é um quadrado perfeito*

   Demonstração. Já vimos que

   $$\varphi(\overline{T}) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right).$$

   Sabemos que $(x,y) \neq 0$, uma vez que $(0,0) \to \mathcal{O}$. Então $\varphi(\overline{T}) = (0,0) \Leftrightarrow x \neq 0$ e $y = 0$. Sobre a condição de que $y = 0$, temos

   $$0 = x^3 + ax^2 + bx = x(x^2 + ax + b).$$

   Precisamos que isso seja racional e não nula, por isso precisamos $x^2 + ax + b$ tenha uma raiz racional. Note que x é racional se, e somente se $a^2 - 4b$ é um quadrado perfeito. Portanto $\overline{T} \in \varphi(E(\mathbb{Q}))$ se, e somente se $a^2 - 4b = \overline{b}$ é um quadrado perfeito. □

3. *Seja $\overline{P} = (\overline{x}, \overline{y}) \in \overline{E(\mathbb{Q})}$ com $\overline{x} \neq 0$. Então, $\overline{P} \in \varphi(E(\mathbb{Q}))$ se, e somente se $\overline{x}$ é o quadrado de um número racional.*

   Demonstração. Se $(\overline{x}, \overline{y}) \in \overline{E(\mathbb{Q})}$, com $\overline{x} \neq 0$, então da definição de φ segue que

   $$\overline{P} \in \varphi(E(\mathbb{Q})) \Rightarrow \overline{x} = \frac{y^2}{x^2} = \left(\frac{y}{x}\right)^2.$$

   Então $\overline{x}$ é o quadrado de um número racional. Reciprocamente, suponha que $\overline{x} = w^2$, com $w \in \mathbb{Q}$. O homomorfismo φ tem dois elementos em seu núcleo, são eles $\mathcal{O}$ e T. Assim, se $(\overline{x}, \overline{y}) \in \varphi(E(\mathbb{Q}))$ existirão dois pontos de $E(\mathbb{Q})$ que são enviados em $(\overline{x}, \overline{y})$. Sejam eles

   $$\begin{aligned} x_1 &= \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right), \quad y_1 = x_1 w \\ x_2 &= \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right), \quad y_2 = -x_2 w. \end{aligned}$$

Afirmamos que $P_i = (x_i, y_i) \in E$ e $\varphi(P_i) = (\overline{x}, \overline{y})$, para $i = 1, 2$. Assim,

$$\begin{aligned} x_1x_2 &= \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right) \cdot \frac{1}{2}\left(w^2 - a - \frac{\overline{y}}{w}\right) \\ &= \frac{1}{4}\left((w^2 - a)^2 - \frac{\overline{y}^2}{w^2}\right) \\ &= \frac{1}{4}\left((\overline{x} - a)^2 - \frac{\overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{x}^3 + 2a\overline{x}^2 - a^2\overline{x} + 4b\overline{x}}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{4b\overline{x}}{\overline{x}}\right) \\ &= b \end{aligned}$$

Temos que

$$\begin{aligned} P_i = (x_1, y_1) \in E &\iff \frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i} \\ &\iff w^2 = x_i + a + \frac{x_1x_2}{x_i} \\ &\iff w^2 = x_1 + x_2 + a \end{aligned}$$

Resta verificar que $\varphi(P_i) = (\overline{x}, \overline{y})$. Pra isso, devemos mostrar que

$$\frac{y_i^2}{x_i^2} = \overline{x} \quad \text{e} \quad \frac{y_i(x_i^2 - b)}{x_i^2} = \overline{y}.$$

Da primeira igualdade temos

$$\frac{y_i^2}{x_i^2} = \frac{(\pm x_i w)^2}{x_i^2} = \frac{x_i^2 w^2}{x_i^2} = w^2 = \overline{x}.$$

Da segunda igualdade usaremos o fato de que $b = x_1x_2$. Logo,

$$\begin{aligned} \frac{y_1(x_1^2 - b)}{x_1^2} &= \frac{x_1 w(x_1^2 - x_1x_2)}{x_1^2} = \frac{x_1^2 w(x_1 - x_2)}{x_1^2} = w(x_1 - x_2) \\ \frac{y_2(x_2^2 - b)}{x_2^2} &= \frac{-x_2 w(x_2^2 - x_1x_2)}{x_2^2} = \frac{-x_2^2 w(x_2 - x_1)}{x_2^2} = w(x_1 - x_2). \end{aligned}$$

E assim,

$$\begin{aligned} \frac{y_i(x_i^2 - b)}{x_i^2} &= w(x_1 - x_2) \\ &= w\left(\frac{1}{2}\frac{\overline{y}}{w} + \frac{1}{2}\frac{\overline{y}}{w}\right) \\ &= w\left(\frac{\overline{y}}{w}\right) \\ &= \overline{y} \end{aligned}$$

Portanto, temos que $\varphi((x_i, y_i)) = (\overline{x}, \overline{y})$. □

Isto é uma aplicação dois a um, que resulta do fato que pontos racionais sobre uma curva elíptica pode ser refletida sobre o eixo x. Queremos criar um homomorfismo um a um a partir da aplicação dois a um.

Proposição 4.3.3. *Seja $\mathbb{Q}^*$ o grupo multiplicativo de números racionais não nulos, e seja $\mathbb{Q}^{*2} = \{u^2 \mid u \in \mathbb{Q}^*\}$, o subgrupo dos quadrados dos elementos de $\mathbb{Q}^*$. Definimos*

$$\alpha : E(\mathbb{Q}) \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}},$$

tal que

$$\alpha(P) = \begin{cases} 1 \pmod{\mathbb{Q}^{*2}}, & \text{se } P = \mathcal{O} \\ b \pmod{\mathbb{Q}^{*2}}, & \text{se } P = T \\ x \pmod{\mathbb{Q}^{*2}}, & \text{se } P = (x, y) \text{ com } x \neq 0. \end{cases}$$

Então

1. *α é um homomorfismo.*

   Demonstração. Primeiramente, vemos que α está bem definida, isto porque $b \neq 0$, logo $\Delta_f = b^2(a^2 - 4b) \neq 0$, e $x \neq 0$ se $P = (x, y) \neq \mathcal{O}, T$. Temos, da definição de α e de $x_P = x_{-P}$, $\forall\, P \in E(\mathbb{Q})$, que $\alpha(P) = \alpha(-P)$. Assim,

   $$\alpha(-P) = \alpha((x, -y)) = x \Rightarrow \alpha(P)\alpha(-P) = x^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}$$

   e

   $$\alpha(T)\alpha(-T) = b^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

   Seja $P_1, P_2, P_3 \neq \mathcal{O}, T$. Então

   $$\begin{aligned} \alpha(P_1)\alpha(P_2) = \alpha(P_1 + P_2) &\Leftrightarrow \alpha(P_1)\alpha(P_2)\alpha(P_1 + P_2)^{-1} = 1 \\ &\Leftrightarrow \alpha(P_1)\alpha(P_2)\alpha(-(P_1 + P_2)) = 1 \\ &\Leftrightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) = 1 \quad \text{onde } P_3 = -P_1 + P_2. \end{aligned}$$

   Para α ser um homomorfismo é suficiente provar que se P_1, P_2, P_3 são pontos colineares em $E(\mathbb{Q})$, então $\alpha(P_1)\alpha(P_2)\alpha(P_3) \equiv 1 \pmod{\mathbb{Q}^{*2}}$. Se $P_1, P_2, P_3 \neq \mathcal{O}, T$, então seja $y = \lambda x + \nu$ a equação da reta que passa por esses três pontos. A condição de que $P_1, P_2, P_3 \neq \mathcal{O}, T$ implica que $\nu \neq 0$. Seja $x(P_1) = x_1, x(P_2) = x_2, x(P_3) = x_3$ as raízes da equação

   $$\begin{cases} y^2 = x^3 + ax^2 + bx \\ y = \lambda x + \nu \end{cases} \Rightarrow x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x - \nu^2 = 0.$$

Isto é, para a curva $y^2 = x^3 = ax^2 + bx$ temos

$$\begin{aligned} x_1 + x_2 + x_3 &= \lambda^2 - a \\ x_1x_2 + x_2x_3 + x_1x_3 &= b - 2\lambda\nu \\ x_1x_2x_3 &= \nu^2. \end{aligned}$$

Daí, temos que

$$x_1x_2x_3 = \nu^2 \Rightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Se um dos P_1, P_2 ou P_3 é $\mathcal{O}$, então sem perda de generalidade podemos assumir que $P_3 = \mathcal{O}$ e que $P_2 = -P_1$. Assim,

$$\alpha(P_1)\alpha(P_2)\alpha(P_3) = \alpha(P_1)\alpha(-P_1)\alpha(\mathcal{O}) = \alpha(P_1)\alpha(P_1)\cdot 1 = \alpha(P_1)^2 = x_1^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Para $P_3 = T$, e simirlamente para P_1 e $P_2 = -P_1$, a equação da reta que passa por P_1, P_2 e T é $y = \lambda x$. Então x_1, x_2 e $x(T) = 0$ são as raízes da equação

$$\begin{cases} y^2 = x^3 + ax^2 + bx \\ y = \lambda x \end{cases} \Rightarrow x^3 + (a - \lambda^2)x^2 + bx = 0.$$

Assim,

$$x_1x_2 = b \Rightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2b = b \cdot b = b^2 \equiv 1 \pmod{\mathbb{Q}^{*2}}.$$

Os casos onde $P_1, P_2, P_3 = \mathcal{O}$ e $P_1 = T, P_2 = T, P_3 = \mathcal{O}$ são triviais. Portanto, α é um homomorfismo. □

2. $\ker \alpha = Im\ \psi$.

Demonstração. Temos que a $\psi(\overline{E(\mathbb{Q})})$ consiste dos quadrados. Uma vez que α pega os pontos em $E(\mathbb{Q})$ e leva em $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$, podemos ver que $\psi(\overline{E(\mathbb{Q})})$ é o núcleo de α. Tomando $E(\mathbb{Q})$ módulo o núcleo, $\psi(\overline{E(\mathbb{Q})})$, fazemos a aplicação injetiva.

$$\frac{E(\mathbb{Q})}{\psi(\overline{E(\mathbb{Q})})} \hookrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}.$$

□

3. *Sejam $p_1, p_2, \ldots, p_t$ primos distintos que dividem b. Então a imagem de α está contida no subgrupo de $\frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$ que consiste dos elementos*

$$\{\pm p_1^{\epsilon_1}p_2^{\epsilon_2}\cdots p_t^{\epsilon_t} \mid \textit{cada } \epsilon_i = 0 \textit{ ou } \epsilon_i = 1\}.$$

Demonstração. Se $P = (x, y) \in E(\mathbb{Q})$, $P \neq \mathcal{O}, T$. Sabemos que existem $m, n, \ell \in \mathbb{Z}$, com $\ell \neq 0$, $mdc(m, \ell) = mdc(n, \ell) = 1$ tal que $x = \frac{m}{\ell^2}$ e $y = \frac{n}{\ell^3}$. Dai, teremos que $m \neq 0$, caso contrário $P = T$. Substituindo na equação de E, temos

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx \\ \frac{n^2}{\ell^6} &= \frac{m^3}{\ell^6} + a\frac{m^2}{\ell^4} + b\frac{m}{\ell^2} \\ n^2 &= m^3 + am^2\ell^2 + bm\ell^4 \\ n^2 &= m(m^2 + am\ell^2 + b\ell^4) \end{aligned}$$

Seja $d = mdc(m, m^2+am\ell^2+b\ell^4)$. Uma vez que $d \mid m$, ele também deve dividir $b\ell^4$, já que todo outro termo em $m^2+am\ell^2+b\ell^4$ contém m nele. Mas como $mdc(m, \ell) = 1$, $d \mid b$. Podemos escrever d como um produto destes fatores primos, e estes fatores devem dividir m, b ou ambos. Afirmamos que todo primo que divide m é ainda uma potência, exceto, possivelmente, os primos que dividem b. Suponha que p_1 é um fator primo de d que não divide b. Então $p_1 \nmid m^2 + am\ell^2 + b\ell^4$ e deve dividir m. Uma vez que $m(m^2 + am\ell^2 + b\ell^4)$ é um quadrado, p_1 deve ser a mesma potência. Agora, podemos escrever

$$m = \pm q^2 p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t},$$

onde $q \in \mathbb{Q}$, e cada $\epsilon_i = 0$ ou $\epsilon_i = 1$, e $p_1, \ldots, p_t$ são primos distintos que dividem b. Lembremos que α pega um ponto P sobre nossa curva e aplica na coordenada x módulo um quadrado. Assim, podemos escrever

$$\alpha(P) = x = \frac{m}{\ell^2} \equiv \pm p_1^{\epsilon_1} p_2^{\epsilon_2} \cdots p_t^{\epsilon_t} \pmod{\mathbb{Q}^{*2}}.$$

□

4. $(E(\mathbb{Q}) : \psi(\overline{E(\mathbb{Q})})) \leq 2^{t+1}$

Demonstração. Temos que o subgrupo acima tem exatamente 2^{t+1} elementos. Sabemos que α é injetiva e a imagem de $\frac{E(\mathbb{Q})}{\psi(\overline{E(\mathbb{Q})})}$ está contido no conjunto deste subgrupo. Portanto, o indíce de $\psi(\overline{E(\mathbb{Q})})$ é no máximo 2^{t+1}. E, portanto,

$$(E(\mathbb{Q}) : \psi(\overline{E(\mathbb{Q})})) \leq 2^{t+1}.$$

□

Lema 4.3.1. *Sejam A e B dois grupos abelianos. Seja $\varphi : A \to B$ e $\psi : B \to A$ dois homomorfismos de grupos tais que*

1. $\psi \circ \varphi = 2a$, $\forall\, a \in A$ *e* $\varphi \circ \psi = 2b$, $\forall\, b \in B$.
2. $(B : \varphi(A)) < \infty$ *e* $(A : \psi(B)) < \infty$.

Então $(A : 2A) < \infty$. *Mais precisamente*

$$(A : 2A) \leq (A : \psi(B))(B : \varphi(A)).$$

Demonstração. Como o homomorfismo $\psi \circ \varphi : A \to 2A$ não é necessariamente sobrejetivo temos que

$$(A : 2A) \leq (A : \psi \circ \varphi(A)) = (A : \psi(B))(\psi(B) : \psi \circ \varphi(A)).$$

A imagem de $\varphi(A)$ através da projeção canônica é dada por

$$B \longrightarrow \psi(B) \longrightarrow \frac{\psi(B)}{\psi \circ \varphi(A)}.$$

Portanto, existe um homomorfismo sobrejetivo

$$\begin{aligned} \frac{B}{\varphi(A)} \longrightarrow \frac{\psi(B)}{\psi \circ \varphi(A)} \Rightarrow (B : \varphi(A)) &\geq \frac{\psi(B)}{\psi \circ \varphi(A))} \\ &= (\psi(B) : \psi \circ \varphi(A)). \end{aligned}$$

Portanto

$$(A : 2A) \leq (A : \psi(B))(\psi(B) : \psi \circ \varphi(A)) \leq (A : \psi(B))(B : \varphi(A)).$$

□

Finalmente e após todos os lemas, proposições e teoremas obtemos:

Teorema de Mordell-Weil. *Seja E uma curva elíptica lisa definida sobre $\mathbb{Z}$. Se E admite um ponto racional de ordem dois, então o grupo dos pontos racionais $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.*

A vantagem de se ter um grupo abeliano finitamente gerado é que existe uma lista de pontos racionais da curva, ou equivalentemente, de soluções da equação em números racionas, tais que todos os outros pontos racionais, ou outras soluções, são obtidos a partir desses usando a operação de somar pontos. Como a operação é relativamente simples, uma lista deste tipo seria uma solução completa do problema de achar pontos racionais.

Vale ressaltar que aplicando métodos da Cohomologia Galoisiana e o Teorema da Descida obtem-se a prova do Teorema de Mordell–Weil para curvas elípticas, que nos diz a condição imposta no Teorema de Mordell para $E(\mathbb{Q})$ satisfazer as hipóteses do Teorema da Descida pode ser retirada, provando que $E(\mathbb{Q})$ é finitamente gerado sob quaisquer condições. Porém, a parte crucial do Teorema de Mordell–Weil é o Teorema de Mordell aqui apresentado.

Referências

[CT] J-L Colliot-Thélène, *L'arithmétique des variétés rationnelles*. Ann. Fac. Sci. Toulouse Math. (6), 1(3):295–336, 1992.

[F] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, New York, W. A. Benjamin,1969.

[G-L] A. Garcia e Y. Lequain, *Álgebra: Um Curso de Introdução*, Rio de Janeiro, IMPA, Projeto Euclides,1988.

[S-T] J. Silverman e J. Tate, *Rational Points on Elliptic Curves*, New York, Springer-Verlage, 1994.