ADENILCE OLIVEIRA SOUZA

PONTOS RACIONAIS EM CURVAS ELÍPTICAS

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2012

ADENILCE OLIVEIRA SOUZA

Pontos Racionais em Curvas Elípticas

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

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

Orientador(a): Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2012

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

S729p 2012

Souza, Adenilce Oliveira, 1979-
Pontos racionais em curvas elípticas / Adenilce Oliveira Souza. - 2012.
62 f. : il.

Orientador: Victor Gonzalo Lopez Neumann.

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

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

CDU: 51

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

ALUNO(A): Adenilce Oliveira Souza.

NÚMERO DE MATRÍCULA: 11012MAT002.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Pontos Racionais em Curvas Elípticas.

ORIENTADOR(A): Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 20 de abril de 2012, às 10h 00 min, pela seguinte Banca Examinadora:

NOME	ASSINATURA
Prof. Dr. Victor Gonzalo Lopez Neumann. UFU - Universidade Federal de Uberlândia	
Prof. Dr. Fernando Eduardo Torres Orihuela. UNICAMP - Universidade Estadual de Campinas	
Prof. Dr. Cícero Fernandes de Carvalho UFU - Universidade Federal de Uberlândia	

Uberlândia-MG, 20 de abril de 2012.

Dedicatória

Á minha família, esposo e amigos que de muitas formas me incentivaram e ajudaram para que fosse possível a concretização deste trabalho. Ao meu orientador, por sua dedicação, competência e profissionalismo.

Agradecimentos

Agradeço primeiramente a Deus por ter me concedido sabedoria, saúde, disposição e condições espirituais e materiais para que eu conseguisse finalizar mais uma etapa de minha vida. Á minha família, em especial a meu esposo e a meus pais, pela dedicação e incentivo nos momentos mais difíceis para que eu não desistisse desse trabalho, grandes incentivadores e amigos. Aos meus colegas e professores do curso de mestrado que muito me incentivaram e me auxiliaram. Ao professor Victor Gonzalo Lopez Neumann um orientador que muito contribuiu para minha formação acadêmica, uma pessoa que consegue unir a competência profissional à uma grande sensibilidade.

OLIVEIRA SOUZA, Adenilce *Pontos Racionais em Curvas Elípticas.* 2012. 62 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

Nesta dissertação estudamos as Curvas Elípticas. Inicialmente descrevemos uma operação sobre a curva que torna o conjunto de pontos de uma Curva Elíptica, sobre um corpo qualquer, um grupo abeliano. Apresentamos o Teorema de Nagell-Lutz o qual mostra as condições necessárias para que um ponto racional sobre a curva tenha ordem finita no grupo. A seguir provamos o Teorema de Mordell para curvas definidas por $y^2 = x^3 + ax^2 + bx$. Este teorema diz que o conjunto de pontos racionais de uma Curva Elíptica é um grupo abeliano finitamente gerado. Na demonstração deste resultado, construímos um algoritmo que, em alguns casos, permite calcular o posto deste grupo. Utilizamos este algoritmo e o Teorema de Nagell-Lutz para estudar o grupo de Mordell-Weil de Curvas Elípticas da forma $y^2 = x^3 - px$, onde p é um número primo.

Palavras-chave: (Curvas Elípticas, Teorema de Mordell, Grupo de Mordell-Weil).

OLIVEIRA SOUZA, Adenilce. *Rational Points on Elliptic Curves* 2012. 62 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

We study Elliptic Curves. Initially we describe an operation on the curve which makes the set of points of an elliptic curve, over any field, an abelian group. We introduce the Nagell-Lutz theorem which shows the necessary conditions for a rational point to have finite order. Next, we prove Mordell's theorem for curves defined by $y^2 = x^3 + ax^2 + bx$. This theorem says that the set of rational points on an elliptic curve is a finitely generated abelian group. On the proof of this result, an algorithm is constructed. With this algorithm, it is possible, in some cases, to calculate the rank of the elliptic curve. We use this algorithm and the Nagell-Lutz theorem to study the Mordell-Weil Group of Elliptic Curves of the form $y^2 = x^3 - px$, where p is a prime number.

Keywords: (Elliptic curves, Mordell Theorem, Mordell-Weil Group).

Sumário

Introdução

As curvas elípticas têm sido utilizadas para lançar luz sobre alguns problemas importantes, como em criptografia, reticulados e o problema de empacotamento da esfera e a rápida fatoração de números inteiros.

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

$$y^2 = x^3 + ax^2 + bx + c \quad \text{com} \quad a, b, c \in \mathbb{Q}\,,$$

tal que o discriminante

$$\Delta = -4a^3 + a^2b^2 + 18abc - 4b^3 - 27c^3 \neq 0\,.$$

O problema de calcular pontos racionais sobre uma curva elíptica $\mathcal{C}$ tem fascinado matemáticos desde a época dos gregos antigos, mas só em 1922 foi provado que é possível a construção de todos os pontos a partir de um número finito de secantes e tangentes. Este é o famoso Teorema de Mordell, que foi provado por Louis Mordell, o qual mostra com mais precisão que todos os pontos racionais formam um grupo abeliano finitamente gerado. O conjunto de pontos racionais da curva elíptica é denotado por $\mathcal{C}(\mathbb{Q})$.

Nesta dissertação, nós nos concentramos nas curvas elípticas definidas sobre o corpo de números racionais.

No primeiro capítulo, fizemos uma breve introdução às curvas elípticas; definindo curva afim, plano projetivo, curvas projetivas. Usando o Teorema de Bézout, construímos uma lei de grupo sobre o conjunto de pontos de uma curva elíptica; esta operação é bastante natural e torna a curva elíptica um grupo abeliano. O elemento neutro deste grupo é o ponto no infinito. A operação é feita de modo a preservar o corpo sobre o qual estamos trabalhando, ou seja, a soma de dois pontos racionais será um ponto racional. Foram utilizadas neste primeiro capítulo as referências bibliográficas [1], [2], [7], [8], como apoio nos tópicos de teoria de números e álgebra, as referências [4], [5] para estruturar o estudo de curvas elípticas.

No segundo capítulo, começamos mostrando que propriedade deve satisfazer um ponto para ser de ordem 2 ou 3. A seguir, enunciamos os teoremas de Nagell-Lutz e de Mazur, que nos ajudam a encontrar todos os pontos racionais de ordem finita de uma curva elíptica. Neste capítulo foram utilizadas as referências bibliográficas [5], [9], [10]; a primeira nos auxilia nas demonstrações e enunciados dos teoremas, os quais são muito importantes para acharmos o Grupo de Mordell-Weil para algumas curvas elípticas, e as duas últimas referências direcionam o leitor para a demonstração do teorema de Mazur.

No terceiro capítulo, demonstramos o Teorema de Mordell e apresentamos um algoritmo para achar a estrutura de grupo do conjunto dos pontos racionais de algumas curvas elípticas. Neste capítulo foram utilizadas as referências bibliográficas [4], [5] que nos auxiliaram na domonstração do Teorema de Mordell. Esta demonstração contém elementos importantes do algoritmo apresentado no presente capítulo para acharmos a estrutura do Grupo de Mordell-Weil de algumas curvas elípticas.

No quarto capítulo mostramos o grupo de Mordell-Weil para algumas curvas específicas usando os teoremas anteriores e o algorítmo apresentado no capítulo 3. Foram utilizadas as referências bibliográficas [4], [5] para complementar a teoria e calculamos a estrutura do grupo de Mordell-Weil das curvas definidas por $y^2 = x^3 - x$ e $y^2 = x^3 - 2x$. As referencias [3] e [6], foram utilizadas para o estudo do grupo de Mordell-Weil das curvas definidas por $y^2 = x^3 - px$, onde p é um número primo. Na referência [3], p é um número primo de Mersenne ou de Fermat, e na referência [6], p é um número primo da forma $p = u^4 + v^4$, com u e v inteiros.

Adenilce Oliveira Souza
Uberlândia-MG, 20 de abril de 2012.

Capítulo 1

Curvas Elípticas

Neste capítulo usaremos $\mathbb{K}$ para denotar um corpo e $\overline{\mathbb{K}}$ seu fecho algébrico.

1.1 Curvas Planas e o Plano Projetivo

Definição 1.1 *Seja $f(x,y)$ um polinômio não constante em $\mathbb{K}[x,y]$. A curva plana afim C_f sobre $\mathbb{K}$ determinada por $f(x,y)$ é o conjunto:*

$$C_f = \left\{(x,y) \subset \overline{\mathbb{K}}^2 : f(x,y) = 0\right\}.$$

Utilizaremos também a notação $C_f : f(x,y) = 0$. Se $\mathbb{F}$ é um corpo contendo $\mathbb{K}$ denotaremos:

$$C_f(\mathbb{F}) = \left\{(x,y) \in \mathbb{F}^2 : f(x,y) = 0\right\}.$$

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

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

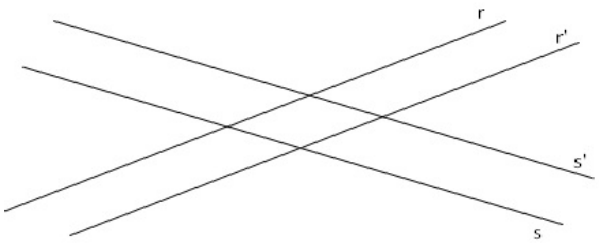

Figura 1.1: Pares de retas paralelas

Não podemos adicionar um único ponto no infinito, pois todo par de retas se intersectaria nesse ponto. Teríamos por exemplo, que as retas r e s da figura 1.3 se intersectariam em

dois pontos. Convém então adicionar um ponto no infinito para cada direção do plano afim ou, equivalentemente, para cada reta contendo a origem. A cada par de números reais (a, b), $ab \neq 0$, corresponde uma reta $ax = by$. Mas, como dois pares (a, b) e (a', b') determinam a mesma reta contendo a origem se e somente se existe um número real t não nulo tal que $ta = a'$ e $tb = b'$, adicionaremos ao plano afim os elementos do conjunto a seguir, ditos os pontos no infinito. Eles são definidos via a seguinte relação de equivalência em $\mathbb{R}^2$, e são denotados por $\mathbb{P}^1(\mathbb{R})$:

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

Sendo assim $\mathbb{P}^1(\mathbb{R}) = \{(x_1, x_2) \in \mathbb{R}^2 : (x_1, x_2) \neq (0, 0)\} / \sim$ é o conjunto das classes de equivalência da relação $\sim$. Seja $\mathbb{P}^2(\mathbb{R}) = \{(x_1, x_2, x_3) \in \mathbb{R}^3 : (x_1, x_2, x_3) \neq (0, 0, 0)\} / \sim$ onde $\sim$ é a relação de equivalência em $\mathbb{R}^3$. Note que existe uma bijeção entre os pontos de $\mathbb{P}^2(\mathbb{R})$ e $\mathbb{R}^2 \cup \mathbb{P}^1(\mathbb{R})$:

$$|x : y : z| \to \begin{cases} (\frac{x}{z}, \frac{y}{z}) & se \quad z \neq 0 \\ |x : y| & se \quad z = 0 \end{cases} .$$

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

Definição 1.2 *Considere a seguinte relação de equivalência entre os pontos de $\mathbb{K}^3$:*

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

Definimos o plano projetivo sobre $\mathbb{K}$ como o conjunto destas classes de equivalência:

$$\mathbb{P}^2(\mathbb{K}) = \left\{(x_1, x_2, x_3) \in \mathbb{K}^3 : (x_1, x_2, x_3) \neq (0, 0, 0)\right\} / \sim .$$

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

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

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

Seja $\mathbb{K}$ um subcorpo dos números complexos, denotaremos por $\mathbb{K}[x, y]$ o anel (de fato, domínio de integridade) de todos os polinômios sobre $\mathbb{K}$ nas variáveis x e y. Também queremos frizar que usaremos o termo "ponto racional"para aqueles pontos (x, y) do plano tais que $x, y \in \mathbb{Q}$.

Veja que se $f \in \mathbb{K}[x, y, z]$ é um polinômio homogêneo de grau k, então $f(\lambda x, \lambda y, \lambda z) = \lambda^k f(x, y, z)$, ou seja, se f se anula em um ponto (x, y, z), ele se anula também em $(\lambda x, \lambda y, \lambda z)$.

Podemos assim definir uma curva projetiva plana associada a um polinômio homogêneo.

Definição 1.3 *Um polinômio homogêneo não constante $f(x, y, z) \in \mathbb{K}[x, y, z]$ define uma curva projetiva plana $\mathcal{C}_f$ sobre $\mathbb{K}$. O conjunto de pontos de $\mathcal{C}_f$ em uma extensão $\mathbb{L} \mid \mathbb{K}$ é o conjunto:*

$$\mathcal{C}_f(\mathbb{L}) = \left\{[x : y : z] \in \mathbb{P}^2(\mathbb{L}) \mid f(x, y, z) = 0\right\}.$$

Observação 1.1 *Veja que estamos utilizando a mesma notação $\mathcal{C}_f$ para curvas afins e curvas projetivas. Ficará claro no contexto se estamos trabalhando com curvas afins ou curvas projetivas.*

Os casos mais interessantes ocorrem quando $f \in \mathbb{Q}[x,y,z]$ e é obvio que temos:

$$\mathcal{C}_f(\mathbb{Q}) \subset \mathcal{C}_f(\mathbb{R}) \subset \mathcal{C}_f(\mathbb{C}).$$

O interesse aritmético é conhecer $\mathcal{C}_f(\mathbb{Q})$. Separaremos os casos que serão aboradados de acordo com o grau do polinômio f e só trataremos daqueles em que este grau é menor ou igual a 3. Nos capítulos seguintes abordaremos os casos em que o grau do polinômio f é 3. Estudaremos aquelas curvas que possuem pontos racionais, isto é, $\mathcal{C}_f(\mathbb{Q}) \neq 0$. Procuraremos descrever este conjunto da maneira mais simples possível. Usaremos a notação $grau(f)$ para denotar o grau total do polinômio f.

Já vimos a função injetora:

$$\begin{array}{ccc} \mathbb{K}^2 & \longrightarrow & \mathbb{P}^2(\mathbb{K}) \\ (x,y) & \longmapsto & [x:y:1] \end{array}$$

que identifica pontos do plano afim, com pontos do plano projetivo. Chamando de U_3 a imagem desta função, $\mathcal{C}_f \cap U_3$ pode ser vista como a curva plana afim definida por $f(x,y,1)$. Da mesma forma, uma curva plana afim, definida por $g(x,y) \in \mathbb{K}[x,y]$, pode ser extendida a uma curva projetiva definida pela função homogênea $\tilde{g}(x,y,z) = z^k g(\frac{x}{z}, \frac{y}{z})$, onde k é o grau da função $g(x,y)$.

Definimos também os planos afins U_1 e U_2 da seguinte forma: Considere a função injetora:

$$\begin{array}{ccc} \mathbb{K}^2 & \longrightarrow & \mathbb{P}^2(\mathbb{K}) \\ (y,z) & \longmapsto & [1:y:z] \end{array}$$

Chamamos U_1 a imagem desta função e $\mathcal{C}_f \cap U_1$ pode ser vista como a curva plana afim definida por $f(1,y,z)$.

Considere também a função injetora:

$$\begin{array}{ccc} \mathbb{K}^2 & \longrightarrow & \mathbb{P}^2(\mathbb{K}) \\ (x,z) & \longmapsto & [x:1:z] \end{array}$$

Chamamos U_2 a imagem desta função e $\mathcal{C}_f \cap U_2$ pode ser vista como a curva plana afim definida por $f(x,1,z)$.

1.2 O Teorema de Bézout

As noções de reta tangente, multiplicidade, número de intersecção podem ser estendidas de curvas afins para curvas projetivas notando que cada ponto P de uma curva projetiva $\mathcal{C}$ se encontra em pelo menos uma das curvas afins $\mathcal{C}_f \cap U_1$, $\mathcal{C}_f \cap U_2$, $\mathcal{C}_f \cap U_3$.

Sejam $\mathcal{C}_f : f(X,Y,Z) = 0$ e $\mathcal{C}_g : g(X,Y,Z) = 0$ duas curvas projetivas planas sem componentes comuns. Para computar o número de pontos na interseção destas curvas é preciso levar em conta de que maneira elas se intersectam em um dado ponto. Vamos agora definir a multiplicidade de interseção de duas curvas afins $\mathcal{C}_f$ e $\mathcal{C}_g$ em um ponto fixo P.

Proposição 1.1 *Sejam P um ponto qualquer do plano afim $\mathbb{K}^2$ e*

$$F(\mathbb{K}) = \{(\mathcal{C}_f, \mathcal{C}_g) : f,g \in \mathbb{K}[x,y] \text{ e } \mathcal{C}_f, \mathcal{C}_g \text{ não têm componente comum contendo } P\}.$$

Existe uma única aplicação $F(\mathbb{K}) \to \mathbb{N}$ tal que o par $(\mathcal{C}_f, \mathcal{C}_g)$ é enviado em um número $(\mathcal{C}_f, \mathcal{C}_g)_P$ satisfazendo as seguintes propriedades:

1) $(\mathcal{C}_f, \mathcal{C}_g)_P = 1$ se $f(x,y) = x - a$ e $g(x,y) = y - b$;

2) $(\mathcal{C}_f, \mathcal{C}_g)_P = (\mathcal{C}_g, \mathcal{C}_f)_P$, $\forall$ $(\mathcal{C}_f, \mathcal{C}_g) \in F(\mathbb{K})$;

3) $(\mathcal{C}_f, \mathcal{C}_{gh})_P = (\mathcal{C}_f, \mathcal{C}_g)_P + (\mathcal{C}_f, \mathcal{C}_h)_P, \ \forall \ (\mathcal{C}_f, \mathcal{C}_g), (\mathcal{C}_f, \mathcal{C}_h) \in F(\mathbb{K})$*;*

4) $(\mathcal{C}_f, \mathcal{C}_{g+fh})_P = (\mathcal{C}_f, \mathcal{C}_g)_P, \ \forall \ (\mathcal{C}_f, \mathcal{C}_g), (\mathcal{C}_f, \mathcal{C}_h) \in F(\mathbb{K})$*;*

5) $(\mathcal{C}_f, \mathcal{C}_g)_P = 0$ *se* $P \notin \mathcal{C}_g \cap \mathcal{C}_f$ *e* $(\mathcal{C}_f, \mathcal{C}_g) \in F(\mathbb{K})$.

Demonstração. Ver [4], proposição 1.8. ■

Exemplo 1.1 *Considere* $f(x, y) = x$ *e* $g(x, y) = y^2 - x^3 + x$*. A multiplicidade de interseção entre estas curvas no ponto* $P = (0, 0)$ *é dada por:*

$$(\mathcal{C}_f, \mathcal{C}_g)_P = (x, y^2 - x^3 + x) = (x, y^2 - x(x^2 - 1))_P = (x, y^2)_P = (x, y)_P + (x, y)_P = 1 + 1 = 2$$

De fato a reta $x = 0$ *é tangente à curva* $y^2 = x^3 - x$ *no ponto* $P = (0, 0)$.

Sejam $\mathcal{C}_f$ e $\mathcal{C}_g$ curvas projetivas e P um ponto que se encontra em U_3 (por exemplo). Sejam as curvas planas afins $\mathcal{C}_{\overline{f}}$ e $\mathcal{C}_{\overline{g}}$ definidas pelas funções :

$$\overline{f}(x, y) = f(x, y, 1) \quad \text{e} \quad \overline{g}(x, y) = g(x, y, 1)\,,$$

respectivamente. Se $P = [x : y : 1] \in \mathcal{C}_f \cap \mathcal{C}_g$, então $\overline{P} = (x, y) \in \mathcal{C}_{\overline{f}} \cap \mathcal{C}_{\overline{g}}$. A interseção no plano projetivo está definida pela interseção no plano afim da seguinte forma:

$$(\mathcal{C}_f, \mathcal{C}_g)_P := (\mathcal{C}_{\overline{f}}, \mathcal{C}_{\overline{g}})_{\overline{P}}\,,$$

onde a interseção da direita está definida pela proposição 1.1. Construções similares podem ser feitas nos planos afins U_1 e U_2.

Podemos agora enunciar o Teorema de Bézout.

Teorema 1.1 (Teorema de Bézout) *Sejam* $\mathcal{C}_f : f(x, y, z) = 0$ *e* $\mathcal{C}_g : g(x, y, z) = 0$ *duas curvas projetivas planas sem componentes comuns de graus* m *e* n *respectivamente. Então:*

$$\sum_{P \in \mathcal{C}_f \cap \mathcal{C}_g} (\mathcal{C}_f, \mathcal{C}_g)_P = mn.$$

Demonstração. Ver [5] Apêndice A, seção 4. ■

1.3 Curvas Elípticas

Nesta seção $\mathbb{K}$ denota um corpo de característica diferente de 2 e 3.

Definição 1.4 *Uma curva elíptica* $\mathcal{C}$ *sobre* $\mathbb{K}$ *pode ser definida como uma das seguintes condições equivalentes:*

(a) Uma curva plana projetiva não singular $\mathcal{C}$ *sobre* $\mathbb{K}$ *de grau* 3*, juntamente com o ponto racional* $\mathcal{O} \in \mathcal{C}(\mathbb{K})$.

(b) O mesmo que (a), exceto que o ponto $\mathcal{O}$ *é um ponto de inflexão.*

(c) Uma curva plana projetiva não singular $\mathcal{C}$ *sobre* $\mathbb{K}$ *da forma:*

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

Demostração da equivalência das definições. Ver [4], Definição 1.1. ■

Seja

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

a equação geral de uma cúbica. Vamos dizer que uma cúbica é definida sobre os racionais se os coeficientes da equação são números racionais. Um famoso exemplo é:

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

ou na forma homogênea teremos:

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

Para achar soluções racionais de $x^3 + y^3 = 1$ vamos achar soluções inteiras de $x^3 + y^3 = z^3$, este é o primeiro caso não trivial do último teorema de Fermat. Não podemos usar o princípio geométrico que funciona tão bem para cônicas porque pelo Teorema de Bézout uma reta geralmente encontra uma cúbica em três pontos. E se temos um ponto racional, não podemos projetar a cúbica sobre uma reta, porque cada ponto sobre a reta seria, em seguida, correspondente a dois pontos sobre a curva.

Mas existem propriedades geométricas que podemos utilizar. Pelo Teorema de Bézout se podemos encontrar dois pontos racionais sobre a curva, então nós podemos geralmente encontrar um terceiro. Ou seja, desenhar a reta que conecta os dois pontos que você tenha encontrado. Esta será uma reta racional, e se encontra com a cúbica em mais um ponto. Se olhar e ver o que acontece quando tentamos encontrar as três intersecções de uma reta racional com uma cúbica racional, achamos uma equação cúbica com coeficientes racionais. Se duas das raízes são racionais, então a terceira também será. Vamos trabalhar alguns exemplos explícitos abaixo, mas o princípio é claro. Então isso dá algum tipo de lei de composição: Começando com dois pontos P e Q, vamos traçar a reta que passa por P e Q e vamos denotar $P * Q$ o terceiro ponto da interseção da reta com a cúbica.

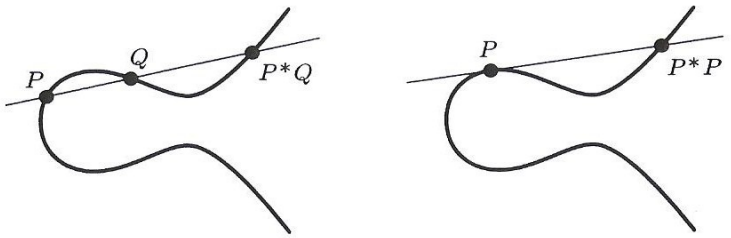

Figura 1.2: Composição de pontos em uma cúbica

Mesmo se só temos um ponto P racional, podemos traçar a reta tangente à cúbica em P. Esta reta tangente intersecta a cúbica duas vezes em P e pelo Teorema de Bezout , esta reta intersecta a cúbica em um novo ponto. O mesmo argumento usado anteriormente mostra que este novo ponto de intersecção é racional. Então, podemos juntar esses novos pontos acima e conseguir mais pontos. Assim, se começarmos com alguns pontos racionais, em seguida, desenhando retas, obteremos outros pontos. Um dos principais teoremas que provaremos nesta dissertação é o teorema de Mordell que afirma que se $\mathcal{C}$ é uma curva cúbica definida sobre os racionais, não singular, então existe um conjunto finito de pontos racionais de tal forma que todos os outros pontos racionais podem ser obtidos da forma como descrevemos acima. Nós iremos provar o teorema de Mordell para uma ampla classe de curvas cúbicas, usando apenas a teoria elementar dos números.

O princípio da prova nos casos gerais é exatamente o mesmo, mas requer algumas ferramentas da teoria de números algébricos. O teorema pode ser reformulado para ser mais

esclarecedor. Para fazer isso, primeiro apresentaremos uma propriedade geométrica elementar de curvas cúbicas. Pelo Teorema de Bézout duas curvas cúbicas encontram-se em nove pontos. Para fazer essa afirmação, deve-se antes de tudo usar o plano projetivo, que tem pontos extras no infinito. Em segundo lugar, devemos introduzir multiplicidades de interseções, contando os pontos de tangência por exemplo, como interseções de multiplicidade maior que um. E, finalmente, deve-se permitir os números complexos para as coordenadas. Em seguida, uma curva de grau m e uma curva de grau n se intersectam em mn pontos. Este é o teorema de Bézout, um dos teoremas básicos da teoria de curvas planas que mostramos anteriormente.

Queremos reformular o teorema de Mordell de uma forma a ter grandes vantagens estéticas e técnicas. Se temos quaisquer dois pontos racionais em uma cúbica definida sobre os racionais, digamos P e Q, então podemos traçar uma reta que une P a Q, obtendo o terceiro ponto que nós já denotamos por $P * Q$. Se considerarmos o conjunto de todos os pontos racionais sobre a cúbica, podemos dizer que o conjunto tem uma lei de composição. Dados quaisquer dois pontos P , Q temos definido um terceiro ponto $P*Q$. Podemos nos perguntar sobre a estrutura algébrica do conjunto com esta lei de composição, por exemplo, é um grupo? Infelizmente, ela não é um grupo; para começar é razoavelmente claro que não há nenhum elemento neutro.

No entanto, podemos definir uma lei de grupo, com a seguinte regra:

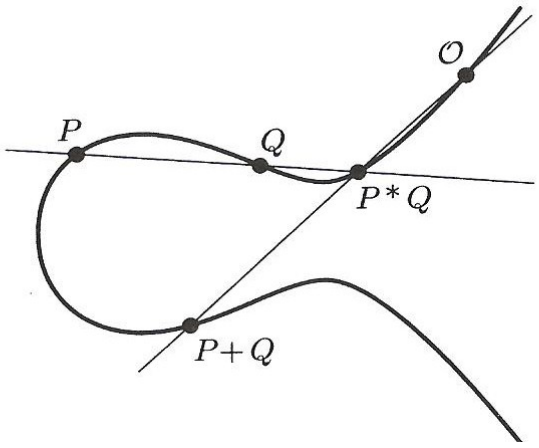

Figura 1.3: A Lei de Grupo em uma Cúbica

"Tome a reta qua passa por P e Q, sendo $P * Q$ o terceiro ponto de intersecção com a cúbica. A reta que passa por $\mathcal{O}$ e por $P * Q$ intersecta a cúbica em um novo ponto denotado por $P + Q$. Assim, por definição, $P + Q = \mathcal{O} * (P * Q)$."

A lei de grupo é ilustrada na figura 1.3 , e o fato de que $\mathcal{O}$ atua como o elemento neutro é mostrado na figura 1.4.

Teorema 1.2 *Seja $\mathcal{C}$ uma curva elíptica sobre um corpo $\mathbb{K}$ com um ponto $\mathcal{O} \in \mathcal{C}(\mathbb{K})$. Então $\mathcal{C}(\mathbb{K})$ é um grupo abeliano com a lei + definida acima.*

Demonstração. É claro que esta operação é comutativa, isto é, $P + Q = Q + P$. Provemos que $P + \mathcal{O} = P$. Seja l a reta que passa por P e $\mathcal{O}$. Pelo teorema de Bézout, existe um terceiro ponto $P * \mathcal{O}$ na interseção $\mathcal{C} \cap l$. Observe que a reta que passa por $\mathcal{O}$ e por $P * \mathcal{O}$ é a própria reta l e o terceiro ponto de interseção é o ponto P. Isto é $P + \mathcal{O} = P$.

Assim $\mathcal{O}$ é o elemento neutro da lei de grupo.

Achemos o inverso $-Q$ de um ponto Q. Seja l a reta tangente à cúbica no ponto $\mathcal{O}$, e seja S o terceiro ponto de interseção de $\mathcal{C}$ e l (obseve que se $\mathcal{O}$ satisfaz a propriedade (b) da definição 1.4, então $S = \mathcal{O}$).

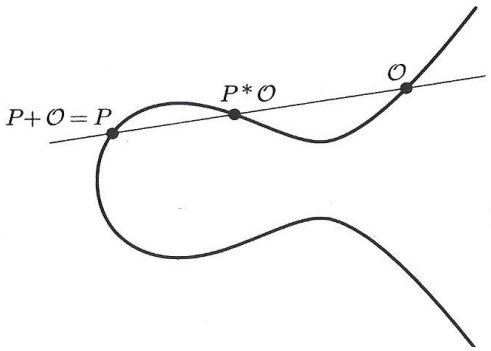

Figura 1.4: Verificando se $\mathcal{O}$ é o elemento neutro

Seja r a reta que passa por Q e S. Então $-Q$ será o terceiro ponto de interseção de $\mathcal{C}$ e r. Pois a reta que passa por Q e $-Q$ é a reta r, logo $Q * (-Q) = S$. A reta que passa por $\mathcal{O}$ e S é a reta l, que é tangente a $\mathcal{C}$ no ponto $\mathcal{O}$, isto é, $\mathcal{O} * S = \mathcal{O}$. Assim $Q + (-Q) = \mathcal{O}$.

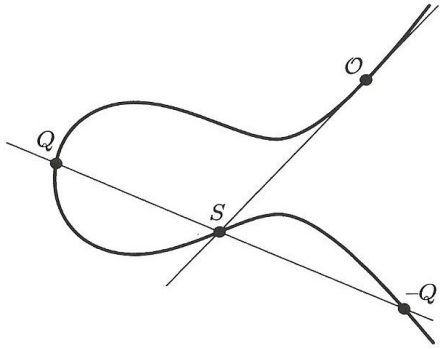

Figura 1.5: O inverso de um ponto

Agora nos falta provar a assossiatividade de $+$. Sejam P, Q, R três pontos sobre a curva $\mathcal{C}$. Provar que $(P+Q)*R = P*(Q+R)$ é suficiente para provar que $(P+Q)+R = P+(Q+R)$. Seja l_1 a reta que passa por P e Q e $P*Q$. Seja r_1 a reta que passa por $\mathcal{O}$, $P*Q$ e $P+Q$. Seja l_2 a reta que passa por $P+Q$, R e $(P+Q)*R$. Seja r_2 a reta que passa por Q, R e $Q*R$. Notemos l_3 a reta que passa por $\mathcal{O}$, $Q*R$ e $Q+R$. Finalmente seja r_3 a reta que passa por P, $Q+R$ e $P*(Q+R)$. Na figura as retas r_1, r_2, r_3 estão desenhadas por um traço contínuo e as retas l_1, l_2, l_3 por um traço pontilhado. Considere agora as cúbicas $\mathcal{C}_l$ definida pela união de l_1, l_2 e l_3 e $\mathcal{C}_r$ definida pela união $r_1 \cup r_2 \cup r_3$. Observe que $\mathcal{C}$ e $\mathcal{C}_l$ se intersectam nos pontos P, Q, $P*Q$, $P+Q$, R, $(P+Q)*R$, $\mathcal{O}$, $Q*R$ e $Q+R$.

Observe também que $\mathcal{C}$ e $\mathcal{C}_r$ se intersectam nos pontos $\mathcal{O}$, $P*Q$, $P+Q$, Q, R, $Q*R$, $Q+R$, P e $P*(Q+R)$.

Assim $\mathcal{C} \cap \mathcal{C}_l$ e $\mathcal{C} \cap \mathcal{C}_r$ possuem 8 pontos em comum. Agora, pela proposição a seguir o nono ponto de interseção deve ser o mesmo. Ou seja $(P+Q)*R = P*(Q+R)$. ■

Proposição 1.2 *Se duas curvas cúbicas em $\mathbb{P}^2$ se intersectam em exatamente nove pontos, então toda curva cúbica que passa por oito desses nove pontos, também passará pelo nono ponto.*

Demonstração. Ver [4] Proposição 3.2. ■

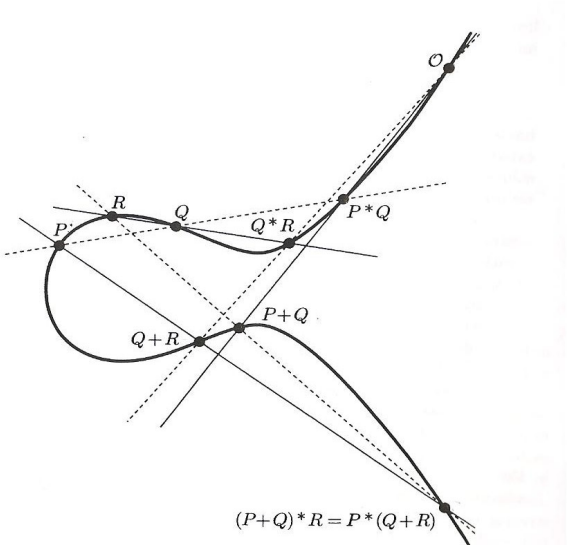

Figura 1.6: Verificando que a Lei é assossiativa

1.4 A Equação de Weierstrass de uma Curva Elíptica

Vamos provar o Teorema de Mordell, usando fórmulas explícitas para a lei de adição. Para fazer com que essas fórmulas sejam tão simples quanto possível, é importante saber que qualquer cúbica com um ponto racional pode ser transformada em uma certa forma especial chamada Forma Normal de Weierstrass. Não vamos completamente provar isso, mas vamos dar uma indicação da prova para que qualquer pessoa que esteja familiarizada com a geometria projetiva possa realizar os detalhes. Além disso, vamos elaborar um exemplo específico para ilustrar a teoria geral. Depois disso, nós iremos restringir a atenção para cúbicas, que são dadas sob a forma Normal de Weiestrass, o que classicamente consiste em uma equação da forma:

$$y^2 = 4x^3 - g_2x - g_3$$

Nós iremos utilizar uma equação um pouco mais geral. Seja $\mathcal{C}$ uma curva elíptica sobre $\mathbb{K}$. Uma equação na forma:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

Quando $\mathbb{K}$ tem característica diferente de 2 e 3. Fazendo a substituição de variáveis onde $x = x'$, $y = y' - \frac{a_3}{2}x$ e $z = z'$, eliminaremos o termo xyz na equação acima. Fazendo uma nova substituição de variáveis onde $x' = x" + \frac{a_2}{3}z$, $y' = y - \frac{a_3}{2}z$ e $z' = z"$ eliminaremos os termos y e chegaremos em uma equação da forma:

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

Trabalhando no plano afim $z = 1$ teremos a equação:

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

que será a Equação de Weierstrass que utilizaremos neste trabalho.

Teorema 1.3 *Seja $\mathbb{K}$ um corpo de característica diferente de 2 e 3. Cada curva elíptica $\mathcal{C}$ é isomorfa a uma curva da forma:*

$$\mathcal{C}(a,b) : y^2z = x^3 + ax^2z + bxz^2 + cz^3 \;\; a, b \in \mathbb{K}.$$

Demonstração. Ver [4] Teorema 2.1. ■

1.5 Fórmulas explícitas para a lei de grupo.

Seja $\mathcal{C}$ a curva elíptica definida por:

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3.$$

No plano afim $z = 1$ esta curva está definida por:

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

Substituindo $z = 0$ na equação original, obtemos $x^3 = 0$, ou seja, $[0 : 1 : 0]$ possui multiplicidade 3 na intersecção $\mathcal{C} \cap z = 0$. Assim este ponto é ponto de inflexão da cúbica. Assim, para uma curva elíptica na forma de Weierstrass, o ponto $\mathcal{O}$ é o ponto $[0 : 1 : 0]$ que se encontra no infinito (em relação ao plano afim $z = 1$). Podemos então afirmar que o conjunto de pontos da curva elíptica $\mathcal{C}$ é o conjunto de pares (x, y) satisfazendo $y^2 = x^3 + ax^2 + bx + c$ juntamente com o ponto no infinito $\mathcal{O}$. A figura 1.7 ilustra o processo de adição dos pontos P e Q sobre uma curva elíptica na forma de Weierstrass, visto que a reta que passa por um ponto qualquer e o ponto $\mathcal{O}$ é uma reta vertical no plano afim.

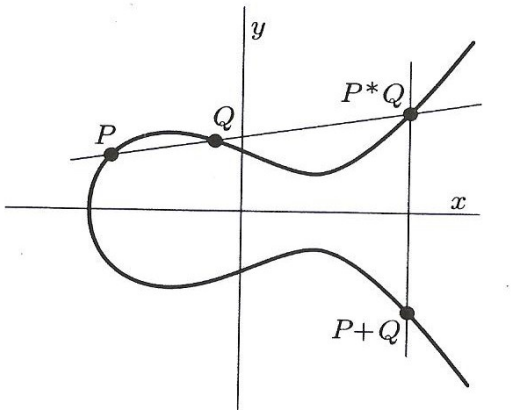

Figura 1.7: Adicionando pontos em uma Cúbica de Weierstrass

O inverso de Q, que chamaremos de $-Q$, é o ponto Q refletido através do eixo x na curva elíptica. Ou seja, se $Q = (x, y)$, teremos $-Q = (x, -y)$.

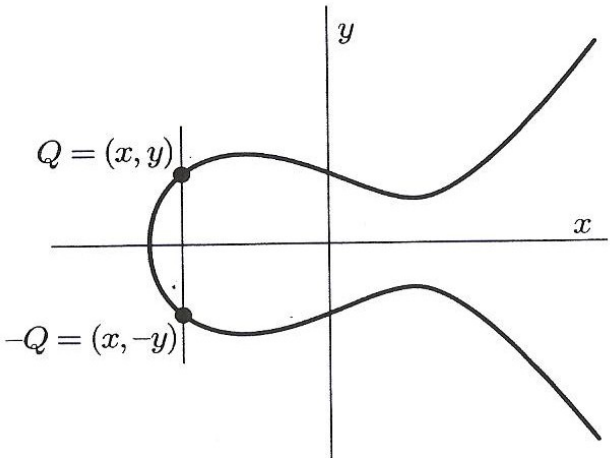

Figura 1.8: O inverso de um ponto na Cúbica de Weierstrass

Para verificarmos isso, suponha que nós adicionaremos Q ao ponto que afirmamos é $-Q$. A reta através de Q e $-Q$ é vertical, de modo que o terceiro ponto de interseção é o ponto $\mathcal{O}$. Agora trace a tangente a $\mathcal{O}$. Esta reta é a reta no infinito, que possui interseção tripa em $\mathcal{O}$, logo $\mathcal{O} * \mathcal{O} = \mathcal{O}$. Isso mostra que $Q + (-Q) = \mathcal{O}$, então $-Q$ é o inverso de Q. É claro que esta fórmula não se aplica ao caso $Q = \mathcal{O}$ mas obviamente $-\mathcal{O} = \mathcal{O}$.

Agora vamos desenvolver algumas fórmulas que nos permitam calcular $P + Q$ de forma explícita. Vamos mudar a notação. Usaremos:

$$P_1 = (x_1, y_1), \;\; P_2 = (x_2, y_2), \;\; P_1 * P_2 = (x_3, y_3), \;\; P_1 + P_2 = (x_3, -y_3).$$

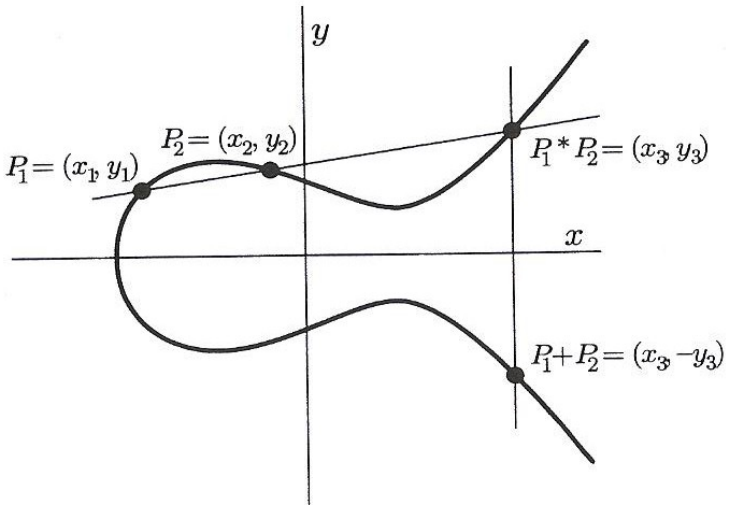

Figura 1.9: A lei de Adição na Cúbica de Weierstrass

Nós assumiremos que (x_1, y_1) e (x_2, y_2) são dados, e queremos calcular (x_3, y_3). Primeiro vamos observar a equação da reta que passa por (x_1, y_1) e (x_2, y_2). Esta reta tem como equação: $y = \lambda x + \nu$, onde $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ e $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Pelo Terema de Bézout, a reta corta a cúbica nos pontos (x_1, y_1) , (x_2, y_2) e (x_3, y_3). Para podermos obter este terceiro ponto de intersecção nós substituiremos a equação da reta na cúbica:

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

Assim:

$$\lambda^2 x^2 + 2\lambda x\nu + \nu^2 = x^3 + ax^2 + bx + c.$$

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

Esta é uma equação cúbica em x, e suas três raízes x_1, x_2, x_3 são as coordenadas X dos três pontos de intersecção. Assim:

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

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

Igualando os coeficientes do termo x^2 em ambos os lados, encontramos que:

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

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

Ou seja:

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad \text{e} \qquad y_3 = \lambda x_3 + \nu.$$

Essas são as fórmulas para calcular a soma $P_1 + P_2 = (x_3, -y_3)$.

Veja alguns exemplos:

Exemplo 1.2 *Seja a curva elíptica:* $y^2 = x^3 + 17$ *e os dois pontos pertencentes a ela:* $P_1 = (-1, 4)$ *e* $P_2 = (2, 5)$. *Agora calcularemos* $P_1 + P_2$.

Primeiramente acharemos a reta que passa por esses dois pontos:

$$\lambda = \frac{5-4}{2-(-1)} = \frac{1}{3} \quad y = \frac{1}{3}x + \nu \Rightarrow \nu = \frac{13}{3} \Rightarrow y = \frac{1}{3}x + \frac{13}{3}.$$

Assim:

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

$$x_3 = \frac{1}{3}^2 - 0 - (-1) - (2) = -\frac{8}{9}.$$

E $y_3 = \lambda x_3 + \nu \Rightarrow y_3 = \frac{1}{3} \cdot -\frac{8}{9} + \frac{13}{3} = \frac{109}{27}$. *Isto é:*

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

As fórmulas anteriores envolvem o ângulo de inclinação da reta que passa pelos dois pontos da cúbica (λ). E se os dois pontos coincidirem? Então, suponhamos que temos $P_0 = (x_0, y_0)$ e queremos encontrar $P_0 + P_0 = 2P_0$. Precisamos encontrar a reta tangente a curva que passa por P_0. Como $x_1 = x_2$ e $y_1 = y_2$, não podemos usar a mesma fórmula para λ. A partir da relação $y^2 = f(x)$ encontramos por diferenciação que:

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

Esta é a fórmula de λ quando queremos calcular o dobro de um ponto.

Exemplo 1.3 *Seja a curva elíptica* $\mathcal{C} : y^2 = x^3 + 17$ *e o ponto* $P_1 = (-1, 4) \in \mathcal{C}(\mathbb{Q})$. *Queremos calcular* $2P_1$. *Primeiramente acharemos o* $\lambda = \frac{f'(x_1)}{2y_1} = \frac{3\cdot(-1)^2}{2\cdot 4} = \frac{3}{8}$.

Achamos também $\nu = y_1 - \frac{3}{8}x_1 = \frac{35}{8}$. *Assim a reta tangente a* $\mathcal{C}$ *que passa por* P_1 *é* $y = \frac{1}{3}x + \frac{35}{8}$, *e* x_3 *e* y_3 *são determinados por:*

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

$$x_3 = \frac{3}{8}^2 - 0 - (-1) - (-1) = \frac{137}{64}$$

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

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

É conveniente ter uma expressão explícita para $2P$ em termos das coordenadas de $P = (x, y)$. Para isso devemos substituir $\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$ nas fórmulas apresentadas anteriormente.

$$x_3 = \lambda^2 - a - x_1 - x_2$$
$$x_3 = \lambda^2 - a - 2x$$
$$x_3 = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x$$
$$x_3 = \left(\frac{(3x^2 + 2ax + b)^2}{4y^2}\right) - a - 2x$$
$$x_3 = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Esta é a fórmula para achar a coordenada x de $2P$ que é muitas vezes chamada de fórmula de duplicação do ponto. Observe que:

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

Estas são as fórmulas básicas aplicáveis a adição de pontos sobre uma cúbica quando a cúbica está na forma de Weierstrass. Usaremos estas fórmulas para provar muitos fatos sobre pontos racionais em curvas cúbicas, incluindo o Teorema de Mordell.

Capítulo 2

Pontos de Ordem Finita

Dizemos que um elemento P de um grupo tem ordem m se

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

mas $nP \neq \mathcal{O}$, para todo inteiro $1 \leq n < m$. Se m existe, então P tem ordem finita, se não, ele é de ordem infinita. Neste capítulo $\mathcal{C}$ será a curva elíptica definida por

$$\mathcal{C}: y^2z = x^3 + ax^2z + bxz^2 + cz^3\,, \quad \text{com } a, b, c \in \mathbb{Z} \quad \text{e}$$
$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0\,.$$

O modelo afim desta curva é dado pela equação

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

Denotaremos por $\mathcal{C}(\mathbb{Q})_{tors}$ o subgrupo de torção de $\mathcal{C}(\mathbb{Q})$, isto é, o subgrupo de $\mathcal{C}(\mathbb{Q})$ dos pontos de ordem finita.

2.1 Pontos de Ordem 2 e de Ordem 3

Proposição 2.1 *Seja $\mathcal{C}$ uma curva cúbica não singular, definida por:*

$$\mathcal{C}: y^2 = x^3 + ax^2 + bx + c.$$

(a) Um ponto $P = (x, y) \neq \mathcal{O}$ em $\mathcal{C}$ tem ordem 2 se, e somente se, $y = 0$.

(b) $\mathcal{C}$ tem exatamente três pontos de ordem 2. Estes pontos juntamente com o ponto $\mathcal{O}$ formam um grupo isomorfo a $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Demonstração.

(a) Os pontos $P = (x, y) \in \mathcal{C}$, do plano afim, que satisfazem $2P = \mathcal{O}$, são os pontos que satisfazem $P = -P$, ou seja:

$$(x, y) = (x, -y) \Leftrightarrow y = 0\,.$$

(b) Seja $P = (x, y) \in \mathcal{C}$, um ponto de ordem 2. Já vimos que $y = 0$, isto é, x deve satisfazer a equação

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

Assim, se permitirmos raízes complexas, esta equação terá 3 raízes, ou seja três pontos de ordem 2 pois a não singularidade da curva garante que $f(x)$ tem raízes distintas. Sendo assim o conjunto de pontos que satisfazem a equação será $\mathcal{O}, P_1, P_2, P_3$ e facilmente vemos que este conjunto é um grupo de 4 elementos onde cada elemento diferente de $\mathcal{O}$ é de ordem 2. Como $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ é o único grupo de 4 elementos que não possui elementos de ordem 4, então $\{\mathcal{O}, P_1, P_2, P_3\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

■

Proposição 2.2 *Seja $\mathcal{C}$ uma curva cúbica não singular, definida por:*

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx + c\,.$$

(a) Um ponto $P = (x, y) \neq \mathcal{O}$ em $\mathcal{C}$ tem ordem 3 se, e somente se, x é raiz do polinômio

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

(b) $\mathcal{C}$ tem exatamente oito pontos de ordem 3. Estes pontos juntamente com o ponto $\mathcal{O}$ formam um grupo isomorfo a $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Demonstração.

(a) Os pontos $P = (x, y) \neq \mathcal{O} \in \mathcal{C}$ satisfazem $3P = \mathcal{O} \Leftrightarrow 2P = -P \Longleftrightarrow x(2P) = x(-P) = x(P)$. Pela fórmula de duplicação de um ponto, temos:

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

que é equivalente a

$$\psi(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2) = 0\,.$$

Veja que $\psi'(x) = 12f(x)$. Uma raiz múltipla de $\psi(x)$, será então raiz de $f(x)$. Logo o ponto correspondente $P = (x, 0)$ será um ponto de ordem 2. Como P é um ponto de ordem 3, $\psi(x) = 0$ possui 4 raízes distintas.

Sendo assim um ponto $P = (x, y) \neq \mathcal{O}$ em $\mathcal{C}$ tem ordem 3 se, e somente se, x é raiz do polinômio

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

(b) O polinômio $3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$ tem quatro raízes distintas e complexas. Sejam β_1 , β_2 , β_3 , β_4 , estas raízes, para cada valor de x temos dois valores para y em nossa cúbica. Sejam $\pm\delta_1$, $\pm\delta_2$, $\pm\delta_3$, $\pm\delta_4$ esses valores de y, para as respectivas coordenadas x. Assim, a curva $\mathcal{C}$ tem exatamente oito pontos de ordem três e juntamente com o ponto $\mathcal{O}$ formam um grupo abeliano de nove elementos. Finalmente, observa-se que há apenas um grupo (abeliano) com nove elementos tais que cada elemento tem ordem 3: $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

■

2.2 Teorema de Nagell-Lutz e Teorema de Mazur

Teorema 2.1 (Teorema de Nagell-Lutz) *Sejam $a, b, c \in \mathbb{Z}$ e seja $\mathcal{C}$ a curva elíptica definida por*

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

Em particular, $f(x)$ não possui raízes múltiplas. Seja Δ o discriminante do polinômio cúbico $f(x)$,

$$\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0\,.$$

Se $P = (x, y)$ é um ponto racional de ordem finita sobre a curva. Então x e y são inteiros e temos que $y = 0$ (e nesse caso P é de ordem 2) ou y^2 divide Δ.

Demonstração. Ver Proposição 2.3 e Proposição 2.4. ■

O teorema fornece um algorítmo para encontrar todos os pontos racionais de torção sobre uma curva elíptica $\mathcal{C}$, definida por $y^2 = x^3 + ax^2 + bx + c$. Para cada $y \in \mathbb{Z}$, satisfazendo $y = 0$ ou $y^2 \mid \Delta$, deve-se achar as raízes inteiras de $x^3 + ax^2 + bx + c - y^2 = 0$ (uma raiz inteira divide $c - y^2$) e depois deve-se verificar se $P = [x : y : 1] \in \mathcal{C}(\mathbb{Q})$ é um ponto de torção.

A recíproca do teorema não é verdadeira: um ponto $P = [x : y : 1] \in \mathcal{C}(\mathbb{Q})$ pode satisfazer as condições do teorema sem que ele seja um ponto de torção. O teorema pode, muitas vezes, ser usado para provar que um ponto $P \in \mathcal{C}(\mathbb{Q})$ é de ordem finita. O teorema seguirá a partir dos dois próximos resultados: O primeiro diz que se P e $2P$ têm coordenadas inteiras (quando $z = 1$), então $y = 0$ ou $y \mid \Delta$. A segunda implica que todos os pontos de torção têm coordenadas inteiras.

Proposição 2.3 *Seja $P = [x_1 : y_1 : 1] \in \mathcal{C}(\mathbb{Q})$. Se P e $2P$ têm coordenadas inteiras (quando estabelecemos $z = 1$) então $y_1 = 0$ ou $y_1^2 \mid \Delta$.*

Demonstração. Sejam $P = [x_1 : y_1 : 1]$ e $2P = [x_2 : y_2 : 1]$ em $\mathcal{C}(\mathbb{Q})$, com coordenadas inteiras. Isto é $x_1, y_1, x_2, y_2 \in \mathbb{Z}$. Suponha ainda $y_1 \neq 0$. Pela fórmula de duplicação, temos

$$x_2 = \frac{x_1^4 - 2bx_1^2 - 8cx_1 + b^2 - 4ac}{4x_1^3 + 4ax_1^2 + 4bx_1 + 4c}\,.$$

Notemos

$$\begin{aligned} f(x) &= x^3 + ax^2 + bx + c\,, \\ g(x) &= x^4 - 2bx^2 - 8cx + b^2 - 4ac\,. \end{aligned}$$

Assim $x_2 = \dfrac{g(x_1)}{4f(x_1)} \in \mathbb{Z}$. Como $y_1^2 = f(x_1)$, então

$$y_1^2 \mid f(x_1) \quad \text{e} \quad y_1^2 \mid g(x_1)\,.$$

Da seguinte identidade:

$$(3x^3 - ax^2 - 5bx + 2ab - 27c)f(x) - (3x^2 + 2ax + 4b - a^2)g(x) = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2\,,$$

concluímos que $y_1^2 \mid \Delta$. ■

Observação 2.1 *Os polinômios*

$$3x^3 - ax^2 - 5bx + 2ab - 27c \quad e \quad 3x^2 + 2ax + 4b - a^2$$

foram achados utilizando o sistema de álgebra computacional Máxima.

Proposição 2.4 *Se $P = [x : y : 1] \in \mathcal{C}(\mathbb{Q})_{tors}$ então $x, y \in \mathbb{Z}$.*

Demonstração. Ver [5], Capítulo II, Seção 4. ■

Teorema 2.2 (Teorema de Mazur) *Seja $\mathcal{C}$ uma curva elíptica, definida sobre os racionais, e suponha que $\mathcal{C}(\mathbb{Q})$ contenha um ponto de ordem m. Então*

$$1 \leq m \leq 10 \quad ou \quad m = 12\,.$$

Mais precisamente, o conjunto de todos os pontos de ordem finita em $\mathcal{C}(\mathbb{Q})$ formam um subgrupo isomorfo a um dos seguintes grupos.

(i) $\mathbb{Z}/m\mathbb{Z}$, *onde* $1 \leq m \leq 10$ *ou* $m = 12$.

(ii) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, *onde* $1 \leq m \leq 4$.

Demonstração. Ver [9] e [10]. ■

Observação 2.2 *Para cada grupo listado nos itens (i) e (ii) do Teorema de Mazur, existe uma curva elíptica $\mathcal{C}$ tal que o subgrupo de torção $\mathcal{C}(\mathbb{Q})_{tors}$ é isomorfo a esse grupo dado.*

Capítulo 3

Teorema de Mordell

O objetivo principal deste capítulo é a demonstração do Teorema de Mordell, e apresentação de um método para achar a estrutura de grupo do conjunto de pontos racionais de algumas curvas elípticas.

3.1 Altura

A altura de um ponto racional mede o quanto o ponto é complexo do ponto de vista de Teoria dos Números. Seja $x = \frac{m}{n}$ um número racional escrito na forma irredutível. Definiremos a altura $H(x)$ sendo o máximo valor absoluto do numerador e do denominador.

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

A altura de um número racional é um inteiro positivo. Por que a altura é uma boa forma de medir o quanto um número racional é complicado? Por exemplo, porque não basta tomar o valor absoluto de $|x|$? Considere os dois números racionais 1 e $\frac{99999}{100000}$. Ambos tem aproximadamente o mesmo valor absoluto, mas o último é claramente muito mais "complicado"que o anterior, pelo menos se alguém estiver interessado em fazer teoria dos números. Se esta razão não é convincente o suficiente, então possivelmente a seguinte propriedade de altura explicará por que é uma noção útil.

3.2 Propriedade da Altura

Proposição 3.1 *Seja $M \in \mathbb{R}$. O conjunto $\left\{x = \frac{m}{n} \in \mathbb{Q} \ : \ H(x) \leq M\right\}$ é finito.*

Demonstração. Seja $x \in \mathbb{Q}$ tal que $H(x) \leq M$ então x pode ser escrito na forma $x = \frac{m}{n}$, com $m, n \in \mathbb{Z}, n > 0$ onde $|m|, |n| \leq M$. Seja k a parte inteira de M. Podemos ter os seguintes valores para $m : \{-k, -k+1, \cdots, 0, 1, \cdots, k\}$ ($2k+1$ valores possíveis) e n pode ter os seguintes valores $\{1, 2, \cdots, k-1, k\}$ (k valores possíveis). Então existem, no máximo $k(2k+1)$ valores possíveis para x. Isto é:

$$\sharp\left\{x \in \mathbb{Q} \ : \ H(x) \leq M\right\} \leq k(2k+1) .$$

■

Se a altura de $x = \frac{m}{n}$ é menor que alguma constante fixa, então ambos $|m|$ e $|n|$ são menores que esta constante, por isso há somente um número finito de possibilidades para m e n . Se $y^2 = f(x) = x^3 + ax^2 + bx + c$ é uma curva cúbica não singular com coeficientes inteiros a, b, c e se $P = (x, y)$ é um ponto racional na curva, definiremos a altura de P sendo simplesmente a altura da coordenada x.

$$H(P) := H(x)\,.$$

Veremos que a altura se comporta como se fosse uma função multiplicativa. Por exemplo, vamos comparar $H(P+Q)$ com o produto $H(P)\cdot H(Q)$. Por razões de notação é mais conveniente ter uma função que possui um comportamento aditivo, então definimos o h "minúsculo"como altura tomando o logaritmo de H.

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

Então $h(P)$ é sempre um número real não negativo. Pois $H(P) \geq 1 \Rightarrow h(P) \geq \log 1 = 0$.
Definimos esta altura para o ponto no infinito como:

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

Nosso objetivo final é provar que o grupo dos pontos racionais $\mathcal{C}(\mathbb{Q})$ é finitamente gerado. Este fato irá seguir de quatro lemas, os quais vamos enunciar e usá-los para demonstrar que $\mathcal{C}(\mathbb{Q})$ é um grupo finitamente gerado.

Lema 3.1 *Para todo número real M, o conjunto $\{P \in \mathcal{C}(\mathbb{Q}) \,:\, h(P) \leq M\}$ é finito.*

Demonstração. Considere $P \in \mathcal{C}(\mathbb{Q})$ tal que $h(P) \leq M$. Se $P \neq \mathcal{O}$, então $P = (x, y)$, onde (x, y) satisfazem a equação $y^2 = x^3 + ax^2 + bx + c$. Por definição $h(P) = h(x) = \log H(x) \leq M$ ou seja $1 \leq H(x) \leq e^M$. Pela proposição 3.1, existem no máximo $k(2k+1)$ valores possíveis para x, onde k é a parte inteira de e^M. Para cada valor de x, existem no máximo 2 valores possíveis para y. Daí:

$$\sharp\{P \in \mathcal{C}(\mathbb{Q}) \,:\, P \neq \mathcal{O}, h(P) \leq M\} \leq 2k(2k+1)\,,$$

ou seja

$$\sharp\{P \in \mathcal{C}(\mathbb{Q}) \,:\, h(P) \leq M\} \leq 2k(2k+1) + 1\,.$$

Isto é, o conjunto é finito. ■

Lema 3.2 *Seja P_0 um ponto racional fixo em $\mathcal{C}$. Existe uma constante k_0, dependendo de P_0 e de a, b, c tal que:*

$$h(P + P_0) \leq 2h(P) + k_0 \quad \forall\ P \in \mathcal{C}(\mathbb{Q})\,.$$

Demonstração. Ver seção 3.3. ■

Lema 3.3 *Existe uma constante k , dependendo de a, b, c tal que:*

$$h(2P) \geq 4h(P) - k \quad \forall\ P \in \mathcal{C}(\mathbb{Q})\,.$$

Demonstração. Ver seção 3.4. ■

Note que os lemas 3.2 e 3.3 relacionam a Lei de grupo em $\mathcal{C}$, que é definida geometricamente como a altura dos pontos que é uma ferramenta de Teoria dos Números. Assim de certa forma pode-se pensar na altura como uma ferramenta para traduzir informação geométrica em informação aritmética.

Lema 3.4 *O índice $[\mathcal{C}(\mathbb{Q}) : 2\mathcal{C}(\mathbb{Q})]$ é finito.*

Demonstração. Ver seção 3.6. ■

Usamos a notação $2\mathcal{C}(\mathbb{Q})$ para denotar o subgrupo de $\mathcal{C}(\mathbb{Q})$ consistindo dos pontos que são o dobro dos pontos de $\mathcal{C}(\mathbb{Q})$. Para qualquer grupo comutativo Γ, a multiplicação por m

$$\Gamma \xrightarrow{[m]} \Gamma\,, \quad P \longmapsto \underbrace{P + \cdots + P}_{m \text{ termos}} = mP$$

é um homomorfismo; e a imagem deste homomorfismo é o subgrupo $m\Gamma$ de Γ. O Lema 3.4 afirma que, para $\Gamma = \mathcal{C}(\mathbb{Q})$, o subgrupo 2Γ tem índice finito em Γ.

Esses lemas estão em ordem crescente de dificuldade. Já provamos o lema 3.1. Os lemas 3.2 e 3.3 estão relacionados a teoria das alturas de números racionais. Já o lema 3.4 é mais sutil e como queremos nos restringir ao trabalho com números racionais só o provaremos para uma classe de curvas cúbicas. Provaremos o teorema de Mordell para curvas elípticas da forma $y^2 = f(x)$ que possuem pelo menos um ponto racional de ordem 2, isto é $f(x)$ deve ter pelo monos uma raiz racional. Fazendo uma mudança de variáveis, podemos supor que $f(x) = x^3 + ax^2 + bx$.

Para começar mostraremos como estes quatro lemas implicam que $\mathcal{C}(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

Podemos esquecer completamente os pontos racionais de uma curva e somente supor que temos um grupo comutativo Γ , escrito aditivamente, e a função altura $h : \Gamma \mapsto [0, \infty)$ de Γ no conjunto de números reais não negativos. Suponha também que Γ e h satisfazem os quatro lemas. Agora apresentamos de novo nossas hipóteses e provaremos que Γ precisa ser finitamente gerado.

Definição 3.1 *O grupo $\Gamma = \mathcal{C}(\mathbb{Q})$ é chamado de grupo de Mordell-Weil da curva elíptica $\mathcal{C}$.*

Teorema 3.1 *Seja Γ um grupo comutativo. Suponha que existe uma função $h : \Gamma \mapsto [0, \infty)$ com as três propriedades abaixo:*

1. *Para cada número real M, o conjunto $\{P \in \Gamma : h(P) \leq M\}$ é finito.*
2. *Para cada $P_0 \in \Gamma$ existe uma constante k_0 tal que $h(P + P_0) \leq 2h(P) + k_0 \ \forall \ P \in \Gamma$.*
3. *Existe uma constante k tal que $h(2P) \geq 4h(P) - k \ \forall \ P \in \Gamma$.*

   Suponha ainda que o subgrupo 2Γ tem índice finito em Γ. Então Γ é finitamente gerado.

Demonstração.

Tomaremos um representante de cada classe lateral de 2Γ em Γ. Sabemos por hipótese que existem apenas um número finito de classes laterais. Sejam $Q_1, Q_2, ..., Q_n$ representantes das classes laterais, onde n é o índice de 2Γ em Γ. Isto significa que dado um elemento $P \in \Gamma$, existe um índice i_1, de tal forma que P está na mesma classe lateral de Q_{i_1}; em outras palavras $P - Q_{i_1} \in 2\Gamma$. Portanto, existe $P_1 \in \Gamma$ tal que $P - Q_{i_1} = 2P_1$. Repetindo o mesmo processo obtemos:

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

onde os elementos $Q_{i_1}, Q_{i_2}, ..., Q_{i_m}$ são escolhidos no conjunto dos representantes das classes laterais $\{Q_1, ..., Q_n\}$ e $P_1, ..., P_m$ e são elementos de Γ. A ideia básica é que P_i é mais ou menos igual a $2P_{i+1}$ e a altura de P_{i+1} é mais ou menos um quarto da altura de P_i. A sequência de

pontos $P, P_1, P_2, ...$ deve ter altura decrescente, e finalmente vamos acabar em um conjunto de pontos com altura limitada, o que completará a demonstração. Agora transformaremos essas observações vagas em uma demonstração válida.

Da equação $P - Q_{i_1} = 2P_1$ temos que $P = Q_{i_1} + 2P_1$.

Da equação $P_1 - Q_{i_2} = 2P_2$ obteremos $P_1 = Q_{i_2} + 2P_2$. E teremos $P = Q_{i_1} + 2Q_{i_2} + 4P_2$ e assim sucessivamente obteremos que:

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Em particular, isto diz que P é um ponto que se encontra no subgrupo de Γ gerado por $Q_i's$ e P_m. Mostramos que escolhendo m suficientemente grande, podemos fazer P_m ter altura menor que um certo valor fixo. Pelo lema 3.1, o conjunto de elemento de altura menor que esse valor fixo é finito. Logo Γ está gerado pela união deste conjunto e o conjunto $\{Q_1, ..., Q_n\}$. O que implica que Γ é finitamente gerado. Vamos então examinar a relação entre a altura de P_j e de P_{j+1}. Pelo item 2, existe uma constante $k_i > 0$, $1 \leq i \leq n$, que depende de $-Q_i$ tal que:

$$h(P - Q_i) \leq 2h(P) + k_i, \quad \forall \ \ P \in \Gamma\,.$$

Tomando $k' = max\,\{k_i, 1 \leq i \leq n\}$ a desigualdade acima pode ser reformulada, assim:

$$h(P - Q_i) \leq 2h(P) + k' \quad \forall \ \ P \in \Gamma, \quad 1 \leq i \leq n\,.$$

Pelo lema 3.3, existe uma constante k tal que:

$$h(2P) \geq 4h(P) - k \quad \forall \ \ P \in \Gamma\,.$$

Assim:

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

ou seja

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

Se $h(P_j) \geq k' + k$, então $h(P_j) \leq \dfrac{3}{4}h(P_{j-1})$.

Provemos que $\exists\ m \in \mathbb{N}$ tal que $h(P_m) < k' + k$. Por absurdo suponha que $h(P_j) \geq k'+k\ \ \forall\ j \in \mathbb{N}$. Então $h(P_j) \leq \dfrac{3}{4}h(P_{j-1}) - \dfrac{1}{4}\,(h(P_{j-1}) - (k'+k))$. Como por hipotese $h(P_{j-1}) - (k'+k) \geq 0$, teremos $h(P_j) \leq \dfrac{3}{4}h(P_{j-1}),\ \ \forall\ j \in \mathbb{N}$. Então $h(P_m) \leq \left(\dfrac{3}{4}\right)^m h(P)$.

Como $\lim\limits_{m\to\infty} \left(\dfrac{3}{4}\right)^m = 0$, então existe $m \in \mathbb{N}$ tal que $h(P_m) < k + k'$, contradição.

Portanto, $\exists\ m \in \mathbb{N}$ tal que $h(P_m) < k' + k$. O que completa a demonstração. ■

Chamamos este teorema de Teorema da descida, pois a demonstração é feita no estilo do método de Fermat de descida finita. Começamos com um ponto arbitrário, em nosso caso o ponto $P \in \mathcal{C}(\mathbb{Q})$, e com algumas manipulações produzimos um ponto com altura menor. Aplicando repetida vezes este processo achamos um ponto que se encontra em um conjunto finito. No método de Fermat usualmente se demonstra a existência de um inteiro entre zero e um, o que produz uma contradição. Tendo em vista o Teorema da Descida, e a demonstração do lema 3.1 acima, resta-nos provar os lemas 3.2, 3.3 e 3.4.

3.3 A altura de $P + P_0$

Nesta seção provaremos o lema 3.2, o que dá uma relação entre a altura de P, P_0 e $P + P_0$. Antes de começarmos faremos algumas observações. A primeira observação é que se $P = (x, y)$ é um ponto racional em nossa curva, então x e y tem a forma:

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

com m, n inteiros, $e > 0$ e $mdc(m, e) = mdc(n, e) = 1$. Em outras palavras, se você escrever as coordenadas de um ponto racional na forma irredutível então o denominador de x é o quadrado de um número cujo cubo é o denominador de y. Suponha $x = \frac{m}{M}$ e $y = \frac{n}{N}$ na forma irredutível com $M > 0$ e $N > 0$. Substituindo na equação da curva temos:

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c \\ \frac{n^2}{N^2} &= \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c \\ \frac{n^2M^3}{N^2M^3} &= \frac{m^3N^2 + aN^2Mm^2 + bN^2M^2m + cN^2M^3}{N^2M^3} \\ M^3n^2 &= N^2m^3 + aN^2Mm^2 + bN^2M^2m + cN^2M^3\,. \end{aligned} \tag{3.1}$$

Vemos que N^2 é um fator de todos os termos do lado direito, assim $N^2 \mid M^3n^2$. Como $mdc(n, N) = 1$, então $N^2 \mid M^3$.

Agora queremos provar que $M^3 \mid N^2$. Isto é feito em três etapas. Primeiro pela equação (3.1) vemos que $M \mid N^2m^3$, e como $mdc(m, M) = 1$, então obtemos $M \mid N^2$, ou seja:

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

Aplicando isto em (3.1) temos $M^2 \mid N^2m^3$. Como $mdc(m, M) = 1$, temos $M^2 \mid N^2$, ou seja $M \mid N$. Isso implica $M^3 \mid M^3n^2 - (aN^2Mm^2 + bN^2M^2m + cN^2M^3)$. Por (3.1) novamente $M^3 \mid N^2m^3$ e como $mdc(m, M) = 1$, temos $M^3 \mid N^2$. Concluímos então que $M^3 = N^2$, pois $M, N > 0$.

Como $M \mid N$, seja $e = \frac{N}{M} \in \mathbb{N}$. Logo

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

Portanto $x = \frac{m}{e^2}$ e $y = \frac{n}{e^3}$ onde x, y estão escritos na forma iredutível.

Nossa segunda observação diz respeito de como definimos a altura de um ponto racional em nossa curva. Se o ponto P é dado por $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, então a altura de P é o máximo entre $|m|$ e e^2. Em particular, $|m| \leq H(P)$ e $e^2 \leq H(P)$. Podemos também vincular o numerador da coordenada y em termos de $H(P)$. Precisamente, há uma constante $K > 0$, dependendo de a, b, c tal que $|n| \leq KH(P)^{\frac{3}{2}}$. Provaremos isto usando o fato de que o ponto P satisfaz a equação. Substituiremos o ponto na equação e multiplicaremos por e^6 e excluiremos o denominador.

$$\begin{aligned} y^2 &= x^3 + ax^2 + bx + c \\ \frac{n^2}{e^6} &= \frac{m^3}{e^6} + a\frac{m^2}{e^4} + b\frac{m}{e^2} + c \\ n^2 &= m^3 + am^2e^2 + bme^4 + ce^6 \end{aligned}$$

Agora tomemos o valor absoluto e consideremos as desigualdades $|m| \leq H(P)$ e $e^2 \leq H(P)$ e a desigualdade triangular e teremos:

$$\begin{aligned} |n^2| &\leq |m^3| + |am^2e^2| + |bme^4| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \\ &= (H(P))^3(1 + |a| + |b| + |c|) \end{aligned}$$

Tomando $K = \sqrt{1 + |a| + |b| + |c|}$, teremos:

$$|n^2| \leq K^2(H(P))^3 \quad \Rightarrow |n| \leq K(H(P))^{\frac{3}{2}}$$

Provemos agora o lema 3.2.

Demonstração.

A demonstração do lema 3.2 é escrevermos a fórmula para a soma de dois pontos e usar a desigualdade triangular. Primeiramente observemos que o lema é trivial se $P_0 = \mathcal{O}$, pois para qualquer $P \in \mathcal{C}(\mathbb{Q})$:

$$h(P + P_0) = h(P) < 2h(P) < 2h(P) + k$$

Seja então $P \neq \mathcal{O}$. Seja $P_0 = (x_0, y_0)$, note que é sufuciente provar que a desigualdade vale para todo P exceto para P em algum conjunto finito.

Isto é verdade porque, se P pertence a um conjunto finito, existe somente um número finito de diferenças $h(P+P_0)-2h(P)$. Basta tomar $k = max\,\{h(P + P_0) - 2h(P) \mid P \text{ no conjunto finito}\}$.

Seja então $P \in \mathcal{C}(\mathbb{Q})$, $P \notin \{P_0, -P_0, \mathcal{O}\}$. Escreva $P = (x, y)$. Como $P \notin \{P_0, -P_0, \mathcal{O}\}$ então $x \in \mathbb{Q}$, $x \neq x_0$.

Assim podemos evitar de utilizar a fórmula de duplicação.

Seja $P + P_0 = (\xi, \eta)$.

Para obter a altura de $P + P_0$, precisamos calcular a altura de ξ, precisamos da fórmula de ξ em termos de (x, y) e (x_0, y_0).

$$\xi + x + x_0 = \lambda^2 - a \quad \text{com} \quad \lambda = \frac{y - y_0}{x - x_0}$$

Assim

$$\xi = \lambda^2 - a - x - x_0$$

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

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

Desenvolvendo este quociente, encontramos a expressão $y^2 - x^3$ a qual pode ser substituída por ax^2+bx+c pois o ponto P está na curva. Após o desenvolvimento desta expressão acharemos o seguinte:

$$\xi = \frac{y^2 - 2yy_0 + {y_0}^2 - x^3 + x^2x_0 - ax^2 + xx_0^2 + 2xx_0a - x_0^3 - ax_0^2}{(x - x_0)^2},$$

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

Podemos escrevê-la da seguinte maneira $\xi = \frac{Ay+Bx^2+Cx+D}{Ex^2+Fx+G}$ onde A, B, C, D, E, F, G são certamente números racionais que podem ser expressos em termos de a, b, c e (x_0, y_0). Mas, multiplicando o numerador e o denominador pelo mínimo denominador comum de $A, \cdots, G$ podemos assumir que $A, \cdots, G$ são inteiros. Em resumo, temos inteiros $A, \cdots, G$ que dependem somente de a, b, c e (x_0, y_0) de modo que para ponto $P = (x, y)$ não pertencente a $\{P_0, -P_0, \mathcal{O}\}$, a coordenada x de $P + P_0$ é igual a $\xi = \frac{Ay+Bx^2+Cx+D}{Ex^2+Fx+G}$.

Um ponto importante é que, uma vez que a curva e o ponto P_0 são fixos, então esta expressão é correta para todo ponto P. Por isso temos que nossa constante k depende de $A, \cdots, G$, contando que não dependa de (x, y). Agora substituiremos $x = \frac{m}{e^2}$ e $y = \frac{n}{e^3}$ e multiplicaremos a fração por $\frac{e^4}{e^4}$ e acharemos $\xi = \frac{Ane+Bm^2+Cme^2+De^4}{Em^2+Fne^2+Ge^4}$ e temos uma expressão de ξ com um inteiro dividido por outro inteiro. Não conhecemos esta expressão na forma irredutível, mas por cancelamento a altura é menor que o máximo entre estes números. Assim:

$$H(\xi) \leq max\left\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fne^2 + Ge^4|\right\}$$

Por outro lado, temos as seguintes estimativas:

$$e \leq H(P)^{\frac{1}{2}}, \quad n \leq KH(P)^{\frac{3}{2}}, \quad m \leq H(P),$$

onde K depende somente de a, b, c. Usando estas desigualdades e a desigualdade triangular temos:

$$|Ane+Bm^2+Cme^2+De^4| \leq |Ane|+|Bm^2|+|Cme^2|+|De^4| \leq (|AK|+|B|+|C|+|D|)H(P)^2$$

e

$$|Em^2 + Fne^2 + Ge^4| \leq |Em^2| + |Fme^2| + |Ge^4| \leq (|E| + |F| + |G|)H(P)^2$$

Portanto

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

Aplicando logaritmo em ambos os lados temos

$$h(P + P_0) \leq 2h(P) + k$$

onde a constante $k = \log max\left\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\right\}$ dependendo somente de a, b, c e (x_0, y_0) e não depende de $P = (x, y)$. Isto completa a nossa demonstração. ■

3.4 A altura de 2P

Na seção anterior provamos que a altura da soma $P + P_0$ (essencialmente) é menor que duas vezes a altura de P. Nesta seção queremos provar o Lema 3.3, que nos diz:

"Existe uma constante k , dependendo de a, b, c tal que $h(2P) \geq 4h(P) - k \quad \forall \ P \in \mathcal{C}(\mathbb{Q})$."

Ou seja, nos diz que a altura de $2P$ é (essencialmente) maior que quatro vezes a altura de P.

Assim como na prova do lema 3.2, podemos ignorar qualquer conjunto finito de pontos, já que podemos escolher k maior que $4h(P)$ para todos os pontos desse conjunto finito. Então descartaremos o conjunto finito de pontos que satisfazem $2P = \mathcal{O}$. Seja $P = (x, y)$, e escreva $2P = (\xi, \eta)$. A fórmula de duplicação é:

$$\xi + 2x = \lambda^2 - a \quad \text{onde} \quad \lambda = \frac{f'(x)}{2y}$$

$$\xi + 2x = \lambda^2 - a$$

$$\xi = \lambda^2 - a - 2x$$

$$\xi = \frac{(f'(x))^2}{(2y)^2} - a - 2x$$

colocando tudo sobre um denominador comum e usando $y^2 = f(x)$ e como $f(x) = x^3 + ax^2 + bx + c$ obtemos uma fórmula explicita para ξ em termos de:

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

Note que $f(x) \neq 0$ porque $2P \neq \mathcal{O}$. Assim ξ é o quociente de dois polinômios em x com coeficientes inteiros. A cúbica $y^2 = f(x)$ é não singular por suposição, sabemos que $f(x)$ e $f'(x)$ não têm raízes em comum. Segue que os polinômios do numerador e do denominador também não têm raízes em comum.

Sabendo que $h(P) = h(x)$ e $h(2P) = h(\xi)$ estamos tentando provar que $h(\xi) \geq 4h(x) - k$.

O seguinte lema conclui a prova.

Lema 3.5 *Sejam $\phi(x)$ e $\psi(x)$ polinômios com coeficientes inteiros e raízes não comuns. Seja d o máximo dos graus de $\phi(x)$ e $\psi(x)$.*

1. *Existe um inteiro $R \geq 1$, dependendo de $\phi(x)$ e $\psi(x)$, tal que para todo número racional $\frac{m}{n}$ temos:*
$$mdc\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \quad \text{divide} \quad R$$

2. *Existem constantes K_1 e K_2, dependendo de $\phi(x)$ e $\psi(x)$, tal que para todo número racional $\frac{m}{n}$ que não são raízes de ψ:*
$$dh\left(\frac{m}{n}\right) - K_1 \leq h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + K_2$$

Demonstração.

1. Primeiro observamos que $\phi(x)$ e $\psi(x)$ têm grau menor ou igual a d, logo os números $n^d\phi\left(\frac{m}{n}\right)$ e $n^d\psi\left(\frac{m}{n}\right)$ são ambos inteiros pois:

$$\phi(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

$$\phi\left(\frac{m}{n}\right) = a_d\frac{m^d}{n^d} + a_{d-1}\frac{m^{d-1}}{n^{d-1}} + \cdots + a_0 \quad \text{logo} \quad n^d\phi\left(\frac{m}{n}\right) \in \mathbb{Z}$$

da mesma forma $n^d\psi\left(\frac{m}{n}\right) \in \mathbb{Z}$. Então faz sentido achar o seu maior divisor comum. O resultado que queremos provar é que não há muito a simplificar quando realizamos o quociente desses dois números. O que devemos simplificar está limitado por R.

Sem perda de generalidade podemos supor $grau\,\phi \geq grau\,\psi$, pois:

$$mdc\left(n^d\psi\left(\frac{m}{n}\right), n^d\phi\left(\frac{m}{n}\right)\right) = mdc\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right)$$

Temos então $grau\,\phi = d$ e $grau\,\psi = e \leq d$. Assim podemos escrever:

$$n^d\phi\left(\frac{m}{n}\right) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$$

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

Para facilitar a notação escreveremos:

$$\Phi(m,n) = n^d\phi\left(\frac{m}{n}\right) \quad \text{e} \quad \Psi(m,n) = n^d\psi\left(\frac{m}{n}\right)$$

Precisamos achar uma estimativa para $mdc(\Phi(m,n), \Psi(m,n))$ que não dependa de m ou n. Como $\phi(x)$ e $\psi(x)$ não tem raízes comuns, eles são primos entre si no anel euclidiano $\mathbb{Q}[x]$. Eles geram o ideal unitário, assim podemos achar polinômios $F(x)$ e $G(x)$ com coeficientes racionais satisfazendo $F(x)\phi(x) + G(x)\psi(x) = 1$. Seja A um inteiro, grande o suficiente, tal que $AF(x)$ e $AG(x)$ tenham coeficientes inteiros. Mas seja D o máximo dos graus de F e G. Note que A e D não dependem de m ou n. Substituindo $x = \frac{m}{n}$ na identidade $F(x)\phi(x) + G(x)\psi(x) = 1$ e multiplicando ambos os lados por An^{D+d}, temos:

$$n^DAF\left(\frac{m}{n}\right)n^d\phi\left(\frac{m}{n}\right) + n^DAG\left(\frac{m}{n}\right)n^d\psi\left(\frac{m}{n}\right) = An^{D+d}$$

Seja $\gamma = \gamma(m,n)$ o maior divisor comum de $\Phi(m,n)$ e $\Psi(m,n)$. Teremos:

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

Já que os números indicados entre chaves são inteiros vemos que γ divide An^{D+d}. Isto não é bom o suficiente pois devemos mostrar que γ divide um número fixo que não depende de n. Na realidade mostraremos que γ divide $Aa_0{}^{D+d}$, onde a_0 é o coeficiente dominante de $\phi(x)$. Provaremos isto observando que γ divide $\Phi(m,n)$ e certamente divide $An^{D+d-1}\Phi(m,n)$, assim como:

$$An^{D+d-1}\Phi(m,n) = An^{D+d-1}n^d\phi\left(\frac{m}{n}\right) = An^{D+d-1}\left(a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d\right)$$

$$An^{D+d-1}\Phi(m,n) = \left(a_0Am^dn^{D+d-1} + a_1Am^{d-1}n^{D+d} + \cdots + a_dAn^{D+2d-1}\right)$$

Como γ divide o primeiro termo temos que γ também dividirá o segundo termo, pois são iguais, assim temos que todos os termos menos o primeiro possuem An^{D+d} como fator e já provamos que γ divide An^{D+d} então temos que γ também dividirá o primeiro termo do segundo menbro da igualdade acima. Assim teremos que $\gamma \mid a_0Am^dn^{D+d-1}$. Logo:

$$\gamma \mid An^{D+d}$$

e

$$\gamma \mid a_0Am^dn^{D+d-1}$$

assim temos que:

$$\gamma \mid mdc\left(An^{D+d}, a_0Am^dn^{D+d-1}\right) = An^{D+d-1}mdc(n, a_0m^d)$$

como

$$mdc(n,m) = 1 \Longrightarrow mdc(n, a_0m^d) = mdc(n, a_0) \quad \text{e} \quad mdc(n, a_0) \mid a_0 \quad \text{então} \quad \gamma \mid Aa_0n^{D+d-1}$$

Por processos idênticos conseguimos provar que $\gamma \mid Aa_0^2n^{D+d-2}$, $\gamma \mid Aa_0^3n^{D+d-3}$, $\gamma \mid Aa_0^4n^{D+d-4}$, $\cdots$, $\gamma \mid Aa_0^{D+d}n^{D+d-(D+d)} = Aa_0^{D+d}$.

O que termina a demostração 1 do lema 3.5. ■

Demonstração.

2.

$$dh\left(\frac{m}{n}\right) - K_1 \leq h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + K_2$$

Existem duas desigualdades a serem provadas. Iniciaremos pela demostração da primeira desigualdade. Como anteriormente , excluiremos um conjunto finito de números racionais quando provamos uma desigualdade desta forma.

Assumiremos que o número racional $\frac{m}{n}$ não é uma raiz de ϕ. Se r é qualquer número racional diferente de zero, fica claro a partir da definição que $h(r) = h\left(\frac{1}{r}\right)$. Para inverter o papel de ϕ e ψ se necessário, podemos pegar o mesmo pressuposto no item 1 do lema, a saber que, ϕ tem grau d e ψ tem grau e, com $e \leq d$. Continuando com a notação usada em 1, o número racional cuja altura pretendemos estimar é:

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

A expressão de ξ é o quociente de números inteiros, assim a altura $H(\xi)$ é o máximo valor entre os inteiros $|\Phi(m,n)|$ e $|\Psi(m,n)|$ exceto se eles têm fatores comuns.

Provamos em 1 que existe um inteiro $R \geq 1$ independente de m e n, de modo que o maior divisor comum de $\Phi(m,n)$ e $\Psi(m,n)$ divide R. Assim:

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

$$\frac{1}{R}max\left\{|n^d\phi\left(\frac{m}{n}\right)|, |n^d\psi\left(\frac{m}{n}\right)|\right\} \geq \frac{1}{2R}\left\{|n^d\phi\left(\frac{m}{n}\right)| + |n^d\psi\left(\frac{m}{n}\right)|\right\}$$

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

Na penúltima linha acima usamos a observação trivial $max\{a,b\} \geq \frac{1}{2}(a+b)$.

Na notação multiplicativa queremos comparar $H(\xi)$ à quantidade

$$H\left(\frac{m}{n}\right)^d = max\left\{|m|^d, |n|^d\right\}.$$

Assim consideramos o quociente:

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

Isto sugere que devemos estudar a função $p(t) = \frac{|\phi(t)|+|\psi(t)|}{max\left\{|t|^d,1\right\}}$. Uma vez que ϕ tem grau d e ψ tem grau máximo d, vemos que p tem limite diferente de zero quando $|t|$ se aproxima do infinito. Este limite é $|a_0|$, se ψ tem grau menor que d, ou será $|a_0| + |b_0|$ se ψ tem grau igual a d.

Observe que o denominador $max\left\{|t|^d, 1\right\}$ não se anula, logo $p(t)$é uma função contínua. Observe também que o numerador não se anula, pois ϕ e ψ não têm raízes em comum.

Por continuidade, $p(t)$ tem máximo e mínimo em todo intervalo fechado e como seu limite é finito quando $t \to \infty$, então existe uma constante $c_1 > 0$ tal que $p(t) > c_1$, $\forall\ t \in \mathbb{R}$.

Usando este fato na desigualdade acima percebemos que $H(\xi) \geq \frac{c_1}{2R}H\left\{\left(\frac{m}{n}\right)^d\right\}$. As constantes c_1 e R não dependem de m e n, assim aplicando logaritmo temos a seguinte desigualdade:

$$h(\xi) \geq dh\left(\frac{m}{n}\right) - K_1;\ \text{ onde }\ K_1 = \log\left(\frac{2R}{c_1}\right)$$

Agora para demonstrar a outra desigualdade $\left(h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + K_2\right)$ continuaremos considerando:

$$\xi = \frac{\Phi(m,n)}{\Psi(m,n)} \quad \text{onde} \quad H(\xi) \leq max\left\{|\Phi(m,n)|, |\Psi(m,n)|\right\}$$

$$\Phi(m,n) = a_0m^d + a_1m^{d-1}n + \cdots + a_dn^d$$

$$|\Phi(m,n)| \leq (|a_0| + |a_1| + \cdots |a_d|)\, max\left\{|m|^d, |n|^d\right\}$$

$$|\Psi(m,n)| \leq (|b_0| + |b_1| + \cdots |b_r|)\, max\left\{|m|^r, |n|^r\right\} \leq (|b_0| + |b_1| + \cdots |b_r|)\, max\left\{|m|^d, |n|^d\right\}$$

onde $r \leq d$. Seja $C = max\left\{|a_0| + |a_1| + \cdots |a_d|, b_0| + |b_1| + \cdots |b_r|\right\}$ assim:

$$H(\xi) \leq max\left\{|\Phi(m,n)|, |\Psi(m,n)|\right\} \leq C\left(max\left\{|m|, |n|\right\}\right)^d = C\left(H\left(\frac{m}{n}\right)\right)^d$$

Aplicando logaritmo em ambos os lados temos:

$$h(\xi) \leq dh\left(\frac{m}{n}\right) + \log C$$

Assim temos $h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + K_2$ onde $K_2 = \log C$

Isto conclui a demostração do lema 3.5. ■

3.5 Um Homomorfismo importante

Para completar a demonstração do Teorema de Mordell precisamos provar o lema 3.4, que diz que o subgrupo $2\mathcal{C}(\mathbb{Q})$ tem índice finito em $\mathcal{C}(\mathbb{Q})$. Esta é a parte mais sutil da demostração do Teorema de Mordell. Para facilitar um pouco a notação, escreveremos Γ em vez de $\mathcal{C}(\mathbb{Q})$, ou seja $\Gamma = \mathcal{C}(\mathbb{Q})$.

Infelizmente, não podemos provar o lema 3.4 para todas as curvas cúbicas sem utilizar ferramentas de Teoria Algébrica de Números, e nós queremos trabalhar somente com os números racionais. Por isso faremos a suposição adicional, de que o polinômio $f(x)$ tem pelo menos uma raiz racional x_0, o que equivale a dizer que a curva tem pelo menos um ponto racional de ordem dois. Nesta seção desenvolveremos algumas ferramentas que precisaremos para demonstrar o lema 3.4 completando assim a demonstração do Teorema de Mordell.

Como $f(x_0) = 0$, e f é um polinômio com coeficientes inteiros e coeficiente dominante 1, então temos que x_0 é um número inteiro. Fazendo uma mudança de coordenadas, podemos mover o ponto $(x_0, 0)$ para a origem. Isto obviamente não afeta o grupo $\mathcal{C}(\mathbb{Q}) = \Gamma$. A nova equação terá coeficientes inteiros e a curva terá a forma:

$$\mathcal{C} : y^2 = f(x) = x^3 + ax^2 + bx \quad \text{com} \quad a, b \in \mathbb{Z}$$

onde $T = (0, 0)$ é um ponto racional em $\mathcal{C}$ que satisfaz $2T = \mathcal{O}$.

A fórmula do discriminante de f dada anteriormente torna-se neste caso $\Delta = b^2(a^2 - 4b)$ pois:

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

Assumiremos que nossa curva é não singular, isso significa que $\Delta \neq 0$, assim $b \neq 0$ e $a^2 - 4b \neq 0$. Estamos interessados no índice $[\Gamma : 2\Gamma]$ ou equivalentemente na ordem do grupo quociente $\Gamma/2\Gamma$, é extremamente útil saber que a função de duplicação $P \to 2P$ pode ser dividida em duas operações simples.

A função de duplicação é de alguma forma de grau quatro porque a função racional dada pela coordenada x de $2P$ é de grau quatro na coordenada x de P. Nós escreveremos a função $P \mapsto 2P$ como a composição de duas funções de grau dois, as quais serão mais fáceis de manusear. Contudo, as duas funções não serão de $\mathcal{C}$ em $\mathcal{C}$, mas de $\mathcal{C}$ para outra curva $\overline{\mathcal{C}}$ e novamente para $\mathcal{C}$. A outra curva $\overline{\mathcal{C}}$ que consideraremos é a curva dada pela equação:

$$\overline{\mathcal{C}} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x \quad \text{onde} \quad \overline{a} = -2a \quad \text{e} \quad \overline{b} = a^2 - 4b.$$

Estas duas curvas estão intimamente relacionadas e é natural estudarmos $\mathcal{C}$ e $\overline{\mathcal{C}}$ comparando uma com a outra.

Aplicaremos novamente o procedimento e olharemos para $\overline{\overline{\mathcal{C}}} : y^2 = x^3 + \overline{\overline{a}}x^2 + \overline{\overline{b}}x$ onde $\overline{\overline{a}} = -2\overline{a} = 4a$ e $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = (-2a)^2 - 4(a^2 - 4b) = 16b$. Então a curva $\overline{\overline{\mathcal{C}}} : y^2 = x^3 + 4ax^2 + 16bx$.

Esta curva é essencialmente a mesma curva que $\mathcal{C}$, só precisamos trocar y por $8y$ e x por $4x$, e dividir a equação por 64. Assim o grupo $\overline{\overline{\Gamma}}$ de pontos racionais em $\overline{\overline{\mathcal{C}}}$ é isomorfo ao grupo Γ de pontos racionais em $\mathcal{C}$. Agora vamos definir a função $\phi : \mathcal{C} \to \overline{\mathcal{C}}$ que será um homomorfismo de grupos e levará os pontos racionais de Γ nos pontos racionais de $\overline{\Gamma}$. Depois, pelo mesmo procedimento definiremos a função $\psi : \overline{\mathcal{C}} \to \overline{\overline{\mathcal{C}}}$. Tendo em vista o isomorfismo $\overline{\overline{\mathcal{C}}} \cong \mathcal{C}$ a composição $\psi \circ \phi$ é um homomorfismo de $\mathcal{C}$ em $\mathcal{C}$ que acabará sendo a multiplicação por dois.

A função $\phi : \mathcal{C} \to \overline{\mathcal{C}}$ é definida por: Se $P = (x, y) \in \mathcal{C}$ é um ponto com $x \neq 0$, então o ponto $\phi(x, y) = (\overline{x}, \overline{y})$ é dado pelas fórmulas:

$$\overline{x} = x + a + \frac{b}{x} = \frac{x^2 + ax + b}{x}.\left(\frac{x}{x}\right) = \frac{y^2}{x^2}$$

e

$$\overline{y} = y\frac{x^2 - b}{x^2}$$

Veja que ϕ está bem definida, temos apenas que checar se $\overline{x}$ e $\overline{y}$ satisfazem a equação de $\overline{\mathcal{C}}$ o que é simples (usamos que $y^2 = x^3 + ax^2 + bx$):

$$\overline{x}^3 + \overline{a}\overline{x}^2 + \overline{b}\overline{x} =$$

$$= \overline{x}\left[\overline{x}^2 + \overline{a}.\overline{x} + \overline{b}\right] = \overline{x}\left[\overline{x}^2 - 2a\overline{x} + (a^2 - 4b)\right] =$$

$$= \frac{y^2}{x^2}\left[\frac{y^4}{x^4} - \frac{2ay^2}{x^2} + a^2 - 4b\right] =$$

$$= \frac{y^2}{x^2}\left[\frac{y^4 - 2ay^2x^2 + a^2x^4 - 4bx^4}{x^4}\right] =$$

$$= \frac{y^2}{x^2}\left[\frac{(y^2 - ax^2)^2 - 4bx^4}{x^4}\right] = \frac{y^2}{x^6}\left[(x^3 + ax^2 + bx - ax^2)^2 - 4bx^4\right] =$$

$$= \frac{y^2}{x^6}\left[(x^3 + bx)^2 - 4bx^4\right] = \frac{y^2}{x^6}\left[x^6 + 2bx^4 + b^2x^2 - 4bx^4\right] = \frac{y^2}{x^6}(x^3 - bx)^2 =$$

$$= \left(\frac{y(x^3 - bx)}{x^3}\right)^2 = \left(\frac{y(x^2 - b)}{x^2}\right)^2 = \overline{y}^2$$

Proposição 3.2 *Sejam $\mathcal{C}$ e $\overline{\mathcal{C}}$ curvas elípticas dadas pelas equações:*

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx \quad e \quad \overline{\mathcal{C}} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x \quad onde \quad \overline{a} = -2a \quad e \quad \overline{b} = a^2 - 4b$$

$$e\ sejam \quad T = (0, 0) \in \mathcal{C} \quad e \quad \overline{T} = (0, 0) \in \overline{\mathcal{C}}$$

1. *Existe um homomorfismo $\phi : \mathcal{C} \to \overline{\mathcal{C}}$ definido por:*

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & se \quad P = (x, y) \neq \mathcal{O}, T \\ \\ \overline{\mathcal{O}} & se \quad P = \mathcal{O} \quad ou \quad T \end{cases}$$

   onde $\ker \phi = \{\mathcal{O}, T\}$.

2. *Aplicando o mesmo processo para $\overline{\mathcal{C}}$ temos a função $\overline{\phi} : \overline{\mathcal{C}} \to \overline{\overline{\mathcal{C}}}$. A curva $\overline{\overline{\mathcal{C}}}$ é isomorfa a $\mathcal{C}$ pela função $(x, y) \mapsto \left(\frac{x}{4}, \frac{y}{8}\right)$. Existe assim um homomorfismo $\psi : \overline{\mathcal{C}} \to \mathcal{C}$ definido por:*

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

   A composição de $\psi \circ \phi : \mathcal{C} \to \mathcal{C}$ é a multiplicação por dois: $\psi \circ \phi(P) = 2P$.

Demonstração.

1. Verificamos anteriormente que a função ϕ leva pontos de $\mathcal{C}$ em pontos de $\overline{\mathcal{C}}$ e supondo que ϕ é um homomorfismo, é obvio que o núcleo de ϕ consiste em $\mathcal{O}$ e T. Pois $\phi(\mathcal{O}) = \overline{\mathcal{O}}$ e $\phi(T) = \overline{\mathcal{O}}$ e $\phi(P) \neq \overline{\mathcal{O}} \ \ \forall \ \ P \neq \mathcal{O}$ e $P \neq T$. Então precisamos provar que ϕ é um homomorfismo, ou seja, $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \ \ \forall \ \ P_1, P_2 \in \mathcal{C}$. Note que o primeiro sinal $+$ é adição em $\mathcal{C}$ e o segundo é adição em $\overline{\mathcal{C}}$

   Se $P_1 = \mathcal{O}$ e $P_2 = P \in \mathcal{C}$, teremos:

$$\phi(\mathcal{O} + P) = \phi(P)$$

$$\phi(\mathcal{O}) + \phi(P) = \phi(P)$$

   Se $P_1 = T$ e $P_2 = T \in \mathcal{C}$, teremos:

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

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

   Se $P_1 = T$ e $P_2 = P \in \mathcal{C}$ com $x \neq 0$ teremos:

$$P = (x_1, y_1) = (x, y) \ \text{ e } \ T = (x_2, y_2) = (0, 0)$$

$$P + T = (x_3, -y_3) \ \text{ pela fórmula de soma de pontos temos:}$$

$$x_3 = \lambda^2 - a - x_1 - x_2 \qquad \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y}{x} \qquad y_3 = \lambda x_3 + v$$

   onde v é o coeficiente linear da reta que passa por P e T

$$x_3 = \lambda^2 - a - x_1 - x_2 = \left(\frac{y}{x}\right)^2 - a - (x) - (0) = \frac{b}{x} \qquad y_3 = \frac{y}{x}\frac{b}{x} + 0 = \frac{by}{x^2}$$

   Logo $P + T = (x_3, -y_3) = (x(P+T), y(P+T)) = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$ e temos que

$$\phi(P + T) = (\overline{x}(P + T), \overline{y}(P + T))$$

   e então:

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

$$\therefore \phi(P+T) = \phi(P) = \phi(P) + \phi(T)$$

Para o inverso de P temos:

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

Para provar que ϕ é um homomorfismo, basta mostrar que se $P_1 + P_2 + P_3 = \mathcal{O}$ então $\phi(P_1) + \phi(P_2) + \phi(P_3) = \overline{\mathcal{O}}$, pois uma vez que sabemos que $\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$. Ainda mais, a partir do que já fizemos, podemos assumir que nenhum dos pontos P_1, P_2 ou P_3 são iguais a $\mathcal{O}$ ou T. Pela definição da lei de grupo em uma curva cúbica, a condição $P_1 + P_2 + P_3 = \mathcal{O}$ é equivalente a afirmação que P_1, P_2, P_3 são colineares. (Se dois ou três deles coincidem, então a reta deve ser adequadamente tangente à curva). Mostraremos que $\phi(P_1), \phi(P_2), \phi(P_3)$ são os pontos de interseção de uma reta com $\overline{\mathcal{C}}$. Note que $v \neq 0$, porque se $v = 0$ significaria que a reta $y = \lambda x + v$ passaria por T, o que contraria a nossa suposição de que P_1, P_2, P_3 são distintos de T.

A reta de interseção com $\overline{\mathcal{C}}$ que pegamos é: $y = \overline{\lambda}x + \overline{v}$, onde

$$\overline{\lambda} = \frac{v\lambda - b}{v} \quad \text{e} \quad \overline{v} = \frac{v^2 - av\lambda + b\lambda^2}{v}.$$

Para verificar que $\phi(P_1) = \phi(x_1, y_1) = (\overline{x}_1, \overline{y}_1)$ está na reta $y = \overline{\lambda}x + \overline{v}$, calculamos $\overline{\lambda}\overline{x}_1 + \overline{v}$, substituindo os valores de $\overline{\lambda}$, $\overline{x}_1$ e $\overline{v}$:

$$\begin{aligned}
\overline{\lambda}\overline{x}_1 + \overline{v} &= \frac{v\lambda - b}{v}\left(\frac{y_1}{x_1}\right)^2 + \frac{v^2 - av\lambda + b\lambda^2}{v} = \frac{(v\lambda - b)(y_1)^2 + (v^2 - av\lambda + b\lambda^2)x_1^2}{vx_1^2} \\
&= \frac{(v\lambda(y_1)^2 - b(y_1)^2 + v^2x_1^2 - av\lambda x_1^2 + b\lambda^2 x_1^2)}{vx_1^2} \\
&= \frac{v\lambda\left(y_1^2 - ax_1^2\right) - b\left(y_1^2 - \lambda^2 x_1^2\right) + v^2x_1^2}{vx_1^2} \\
&= \frac{v\lambda\left(y_1^2 - ax_1^2\right) - b\left(y_1 + \lambda x_1\right)\left(y_1 - \lambda x_1\right) + v^2x_1^2}{vx_1^2}
\end{aligned}$$

Substituindo $y_1^2 - ax_1^2 = x_1^3 + bx_1$ e $y_1 - \lambda x_1 = v$ obtemos:

$$\begin{aligned}
\overline{\lambda}\overline{x}_1 + \overline{v} &= \frac{v\lambda\left(x_1^3 + bx_1\right) - bv\left(y_1 + \lambda x_1\right) + v^2x_1^2}{vx_1^2} \\
&= \frac{\lambda\left(x_1^3 + bx_1\right) - b\left(y_1 + \lambda x_1\right) + vx_1^2}{x_1^2} \\
&= \frac{\lambda x_1^3 + \lambda b x_1 - by_1 - b\lambda x_1 + vx_1^2}{x_1^2} = \frac{x_1^2\overbrace{(\lambda x_1 + v)}^{y_1} - by_1}{x_1^2} \\
&= \frac{y_1(x_1^2 - b)}{x_1^2} = \overline{y_1}
\end{aligned}$$

$$\therefore \overline{y_1} = \lambda\overline{x_1} + \overline{v}$$

O cálculo para $\phi(P_2)$ e $\phi(P_3)$ é exatamente o mesmo. Note que não é suficiente mostrar que os três pontos $\phi(P_1), \phi(P_2)$ e $\phi(P_3)$ estão na mesma reta $y = \overline{\lambda}x + \overline{v}$. Será suficiente

se $\phi(P_1), \phi(P_2)$ e $\phi(P_3)$ são distintos, mas temos que mostrar que $\overline{x}(P_1), \overline{x}(P_2)$ e $\overline{x}(P_3)$ são as três raízes cúbicas de $\left(\overline{\lambda}x + \overline{v}\right)^2 = \overline{f}(x)$. Como alternativa podemos notar que ϕ é contínua como uma função de $\mathcal{C}$ em $\overline{\mathcal{C}}$, portanto, uma vez que sabemos que ϕ é um homomorfismo para pontos distintos, temos por continuidade que é um homomorfismo geral.

2. Observamos acima que a curva $\overline{\overline{\mathcal{C}}}$ é dada pela equação $\overline{\overline{\mathcal{C}}} : y^2 = x^3 + 4ax^2 + 16bx$ por isso é claro que a função $(x, y) \mapsto \left(\frac{x}{4}, \frac{y}{8}\right)$ é um isomorfismo de $\overline{\overline{\mathcal{C}}}$ para $\mathcal{C}$. De (1) temos um homomorfismo $\overline{\phi} : \overline{\mathcal{C}} \to \overline{\overline{\mathcal{C}}}$ definido pela mesma equação que define ϕ, mas com $\overline{a}$ e $\overline{b}$ no lugar de a e b. Uma vez que a função $\psi : \overline{\mathcal{C}} \to \mathcal{C}$ é a composição de $\overline{\phi} : \overline{\mathcal{C}} \to \overline{\overline{\mathcal{C}}}$ com o isomorfismo $\overline{\overline{\mathcal{C}}} \to \mathcal{C}$, obtemos imediatamente que ψ é um homomorfismo bem definido de $\overline{\mathcal{C}}$ para $\mathcal{C}$. Resta-nos verificar que $\psi \circ \phi$ é multiplicação por dois. Usando um pouco de álgebra e resultados anteriores temos:

$$2P = 2(x, y) = \left(\frac{(x^2 - b)^2}{4y}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2}{8y^3}\right)$$

Por outro lado temos:

$$\phi(x, y) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) \quad \text{e} \quad \psi(\overline{x}, \overline{y}) = \left(\frac{\overline{y}^2}{4\overline{x}^2}, \frac{\overline{y}(\overline{x}^2 - \overline{b})}{8\overline{x}^2}\right)$$

E também

$$\overline{x} = \frac{y^2}{x^2} \quad \text{e} \quad \overline{y} = \frac{y(x^2 - b)}{x^2} \quad \text{e} \quad \overline{b} = a^2 - 4b$$

Agora podemos calcular $\psi \circ \phi(x, y)$.

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

Agora como temos $y^2 = x^3 + ax^2 + bx$ então $y^2 = x(x^2 + ax + b)$ logo $y^4 = x^2(x^2 + ax + b)^2$ e esta última expressão substituiremos na equação acima para terminarmos nossos cálculos.

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

$$\therefore \psi \circ \phi(x, y) = 2(x, y)$$

Similar ao calculado acima teríamos $\phi \circ \psi(\overline{x}, \overline{y}) = 2(\overline{x}, \overline{y})$ ou podemos argumentar como sendo ϕ um homomorfismo, sabemos que:

$$\phi(2P) = \phi(P + P) = \phi(P) + \phi(P) = 2\phi(P)$$

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

Os pontos P com $x = 0$ ou $y = 0$ são os pontos de ordem 2. Para estes pontos podemos provar que: se $P = (x, 0)$, $x \neq 0$ então $\phi(P) = \overline{T}$, logo $\psi \circ \phi(P) = \mathcal{O}$. Se $x = 0$, então $P = T$ e nesse caso $\phi(T) = 0$.

■

3.6 Demonstração do Lema 3.4

Nesta seção completaremos a demonstração do lema 3.4 e com ele a demonstração do Teorema de Mordell. Continuaremos com as mesmas notações usadas anteriormente.

Temos duas curvas

$$\mathcal{C} : y^2 = x^3 + ax^2 + bx \quad \text{e}$$

$$\overline{\mathcal{C}} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x \quad \text{onde } \overline{a} = -2a \text{ e } \overline{b} = a^2 - 4b$$

e temos os homomorfismos $\phi : \mathcal{C} \to \overline{\mathcal{C}}$ e $\psi : \overline{\mathcal{C}} \to \mathcal{C}$ de tal forma que as composições $\phi \circ \psi : \overline{\mathcal{C}} \to \overline{\mathcal{C}}$ e $\psi \circ \phi : \mathcal{C} \to \mathcal{C}$ são cada uma, a multiplicação por dois. Além disso, o núcleo de ϕ consiste em dois pontos $\mathcal{O}$ e $T = (0, 0)$, e o núcleo de ψ consiste em $\overline{\mathcal{O}}$ e $\overline{T} = (0, 0)$. As imagens de ϕ e ψ são extremamente interessantes.

É claro que dado qualquer ponto $\overline{P} \in \overline{\mathcal{C}}$, existe um ponto $P \in \mathcal{C}$ tal que $\phi(P) = \overline{P}$ quando trabalhamos sobre os números complexos. Em outras palavras, trabalhando sobre o corpo dos complexos a função ϕ é sobrejetora. Mas agora examinaremos o que acontece sobre o corpo dos racionais.

Fica claro a partir da definição que a função ϕ é de Γ para $\overline{\Gamma}$, mas se tomarmos um ponto racional em $\overline{\Gamma}$, não fica claro que sua preimagem esteja em Γ. Se aplicarmos a função ϕ em Γ obteremos um subgrupo de $\overline{\Gamma}$ e denotaremos este subgrupo por $\phi(\Gamma)$ e o chamaremos de imagem de Γ por ϕ. Faremos três afirmações a seguir que em conjunto, fornecem uma boa descrição da imagem:

(i) $\overline{\mathcal{O}} \in \phi(\Gamma)$

(ii) $\overline{T} = (0, 0) \in \phi(\Gamma)$ se e somente se $\overline{b} = a^2 - 4b$ é um quadrado perfeito.

(iii) Seja $\overline{P} = (\overline{x}, \overline{y}) \in \overline{\Gamma}$ com $\overline{x} \neq 0$. Então $\overline{P} \in \phi(\Gamma)$ se e somente se $\overline{x}$ é o quadrado de um número racional.

Demonstração.

(i) É óbvio porque $\overline{\mathcal{O}} = \phi(\mathcal{O})$ e $\mathcal{O} \in \Gamma$.

(ii) Apartir da definição de ϕ vemos que $\overline{T} \in \phi(\Gamma)$ se e somente se existe um ponto racional $(x, y) \in \Gamma$ tal que $\frac{y^2}{x^2} = 0$. Note que $x \neq 0$, pois se $x = 0$ significa que $(x, y) = T$ e $\phi(T) = \overline{\mathcal{O}} \neq \overline{T}$. Então $\overline{T} \in \phi(\Gamma)$ se e somente se existe um ponto racional $(x, y) \in \Gamma$ com $x \neq 0$ e $y = 0$. Colocando $y = 0$ na equação de Γ temos:

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

Esta equação tem uma raiz racional diferente de zero se e somente se a equação quadrática $x^2 + ax + b$ tem uma raiz racional, o que acontecerá se, e somente se, o discriminante $a^2 - 4b$ for um quadrado perfeito.

(iii) Se $(\overline{x}, \overline{y}) \in \phi(\Gamma)$ é um ponto com $\overline{x} \neq 0$, então a definição de ϕ mostra que $\overline{x} = \frac{y^2}{x^2}$ é o quadrado de um número racional $w = \frac{y}{x}$. Queremos achar um ponto racional sobre $\mathcal{C}$ que é enviado em $(\overline{x}, \overline{y})$.

O homomorfismo ϕ tem dois elementos em seu núcleo, $\mathcal{O}$ e T. Assim se $(\overline{x}, \overline{y})$ estão em $\phi(\Gamma)$ existirão dois pontos de Γ que são enviados em $(\overline{x}, \overline{y})$. Sejam eles:

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\overline{y}}{w}\right) \qquad y_1 = x_1 w$$

$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\overline{y}}{w}\right) \qquad y_2 = -x_2 w\,.$$

Afirmamos que os pontos $P_i = (x_i, y_i)$ estão em $\mathcal{C}$ e que $\phi(P_i) = (\overline{x}, \overline{y})$ para $i = 1, 2$. Visto que P_1 e P_2 são claramente pontos racionais, isto provará que $(\overline{x}, \overline{y}) \in \phi(\Gamma)$.

Provemos que P_1 e P_2 são pontos da curva $\mathcal{C}$. Veja que:

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\left((w^2 - a)^2 - \frac{\overline{y}^2}{w^2}\right) = \frac{1}{4}\left((\overline{x} - a)^2 - \frac{\overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \end{aligned}$$

Como $\overline{y}^2 = \overline{x}^3 - 2a\overline{x}^2 + (a^2 - 4b)\overline{x}$, temos:

$$\begin{aligned} x_1 x_2 &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) \\ &= \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{x}^3 + 2a\overline{x}^2 - a^2\overline{x} + 4b\overline{x}}{\overline{x}}\right) \\ &= b\,. \end{aligned}$$

Mostrar que $P_i = (x_i, y_i)$ está em $\mathcal{C}$ é equivalente a mostrar que:

$$\frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}$$

Como já provamos que $b = x_1 x_2$, e por definição de y_1 e y_2 temos $\frac{y_i}{x_i} = \pm w$ isto é o mesmo que provar que $w^2 = x_1 + a + x_2$, que é uma igualdade óbvia por definição de x_1 e x_2. Resta verificarmos que $\phi(P_i) = (\overline{x}, \overline{y})$. Para isto devemos mostrar que:

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

A primeira igualdade é clara a partir da definição de $y_i = \pm x_i w$ e $\overline{x} = w^2$.

Para a segunda usaremos $b = x_1 x_2$ e a definição de y_i. Assim:

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \frac{x_1 w(x_1^2 - x_1 x_2)}{x_1^2} = \frac{x_1^2 w(x_1 - x_2)}{x_1^2} = w(x_1 - x_2)$$

e

$$\frac{y_2(x_2^2-b)}{x_2^2}=\frac{-x_2w(x_2^2-x_1x_2)}{x_2^2}=\frac{-x_2^2w(x_2-x_1)}{x_2^2}=w(x_1-x_2)\,.$$

Assim verificamos que $\overline{y}=w(x_1-x_2)$ pela definição de x_1 e x_2.

Com isto completamos a verificação da afirmação (iii).

■

Lembremos que nosso objetivo é provar o Lema 3.4, que diz que o subgrupo 2Γ tem índice finito dentro de Γ. Como veremos em breve isto é consequência de poder provar que os índices $[\overline{\Gamma}:\phi(\Gamma)]$ e $[\Gamma:\psi(\overline{\Gamma})]$ são finitos. Na verdade mostraremos que $[\overline{\Gamma}:\phi(\Gamma)]\leq 2^{s+1}$, onde s é o número de fatores primos distintos de $\overline{b}=a^2-4b$ e também que $[\Gamma:\psi(\overline{\Gamma})]\leq 2^{r+1}$, onde r é o número de fatores primos distintos de b.

A partir das afirmações (i),(ii) e (iii) sabemos que $\psi(\overline{\Gamma})$ é o conjunto de pontos $(x,y)\in\Gamma$ tal que x é o quadrado de um número racional $\neq 0$ juntamente com o $\mathcal{O}$, e também T se b é um quadrado perfeito.

A idéia da demonstração é achar um homomorfismo a partir do grupo quociente $\frac{\Gamma}{\psi(\overline{\Gamma})}$ para um grupo finito.

Seja $\mathbb{Q}^*$ o grupo multiplicativo de números racionais $\neq 0$, e seja $\mathbb{Q}^{*2}$ o subgrupo dos quadrados dos elementos de $\mathbb{Q}^*$.

$$\mathbb{Q}^{*2}=\left\{u^2\ :\ u\in\mathbb{Q}^*\right\}$$

Introduziremos a função α de Γ para $\mathbb{Q}^*/\mathbb{Q}^{*2}$ definida por:

Definição 3.2 *Seja α uma função definida de Γ para $\mathbb{Q}^*/\mathbb{Q}^{*2}$ tal que:*

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

Proposição 3.3 *a) A função $\alpha:\Gamma\to\mathbb{Q}^*/\mathbb{Q}^{*2}$ descrita acima é um homomorfismo.*

b) O núcleo de α é a imagem $\psi(\overline{\Gamma})$. Por isso α induz um homomorfismo injetor

$$\Gamma/\psi(\overline{\Gamma})\longrightarrow\mathbb{Q}^*/\mathbb{Q}^{*2}$$

Por abuso de notação também chamaremos de α este homomorfismo.

c) Seja $p_1,p_2,\cdots,p_t$ primos distintos que dividem b. Então a imagem de α está contida no subgrupo de $\mathbb{Q}^*/\mathbb{Q}^{*2}$ que consiste nos elementos:

$$\left\{\pm {p_1}^{\xi_1}{p_2}^{\xi_2}\cdots{p_t}^{\xi_t}\ \mid\quad \xi_i=0\quad ou\quad \xi_i=1\right\}$$

d) O índice $\left[\Gamma:\psi(\overline{\Gamma})\right]$ é no máximo 2^{t+1}. Onde t é o número de fatores primos distintos de b.

Demonstração.

a) Primeiramente observe que α envia inversos em inversos porque:

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

Portanto, provar que α é um homomorfismo é suficiente mostrar que:

$$\alpha(P_1+P_2)=\alpha(P_1)\bullet\alpha(P_2)$$

onde $+$ é adição em Γ e $\bullet$ multiplicação em $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Afim de provar que α é um homomorfismo, é suficiente mostrar que sempre que $P_1+P_2+P_3=\mathcal{O}$, então $\alpha(P_1)\alpha(P_2)\alpha(P_3)\equiv 1 \pmod{\mathbb{Q}^{*2}}$. Se a reta que passa por esses três pontos é dada por $y=\lambda x+v$ e as coordenadas x das interseções da curva com a reta são x_1,x_2,x_3 então elas são raízes da equação:

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

Logo:

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

$$x_1x_2+x_2x_3+x_1x_3=b-2\lambda v$$

$$x_1x_2x_3=v^2-c$$

Para a cúbica $y^2=x^3+ax^2+bx+c$.

A última equação é $x_1x_2x_3=v^2$, $c=0$. Assim $\alpha(P_1)\alpha(P_2)\alpha(P_3)=x_1x_2x_3=v^2\equiv 1 \pmod{\mathbb{Q}^{*2}}$. Isto completa a demonstração para os casos em que P_1,P_2,P_3 são distintos de $\mathcal{O}$ e T.

Os casos onde $P_1,P_2,P_3:=\{\mathcal{O},\mathcal{O},\mathcal{O}\},\{T,T,\mathcal{O}\}$ são imediatos, o caso $\{P,-P,\mathcal{O}\}$ já foi feito no início da demonstração.

A reta que passa por T e $-P$ é dada por $y=-\frac{y_0}{x_0}x$. Assim a interseção da reta com a cúbica é $x\left(x^2+\left(a-\frac{y_0^2}{x_0^2}\right)x+b\right)=0$. As raízes x_1 e x_2 que satisfazem $x_1+x_2=\frac{y_0^2}{x_0^2}-a$ e $x_1x_2=b$ são as coordenadas x dos pontos P e T. Assim: $\alpha(T)\alpha(-P)\alpha(T-P)=x_1\bullet b\bullet x_2=b\bullet b=b^2=1 \pmod{\mathbb{Q}^{*2}}$

b) Por abuso de notação chamaremos também de α o homomorfismo:

$$\Gamma/\psi(\overline{\Gamma}) \xrightarrow{\quad\alpha\quad} \mathbb{Q}^*/\mathbb{Q}^{*2}$$

$$[P] \xrightarrow{\qquad} \alpha(P)$$

onde $[P]$ é a classe de P módulo $\psi(\overline{\Gamma})$.

Observe que:

$$\alpha(P)=1 \pmod{\mathbb{Q}^{*2}} \iff \begin{cases} P=\mathcal{O}\,, & \text{ou} \\ P=T\,, & \text{se b é um quadrado, ou} \\ P=(x,y)\,, & \text{se x é um quadrado.} \end{cases}$$

Esta é exatemente a descrição dos elementos de $\psi(\overline{T})$. Isto é $Ker(\alpha)=\psi(\overline{T})$. Pelo primeiro teorema de homomorfismo, concluímos que: $\alpha:\Gamma/\psi(\overline{\Gamma})\to\mathbb{Q}^*/\mathbb{Q}^{*2}$ definida por $\alpha([P])=\alpha(P)$ é um homomorfismo injetor.

c) Seja $P=(x,y)\in\Gamma$, $P\neq\mathcal{O}$, $P\neq T$. Sabemos que tais pontos tem coordenadas da forma $x=\dfrac{m}{e^2}$ e $y=\dfrac{n}{e^3}$. Substituindo na equação e cancelando os denominadores teremos:

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

$$\left(\frac{n}{e^3}\right)^2=\left(\frac{m}{e^2}\right)^3+a\left(\frac{m}{e^2}\right)^2+b\frac{m}{e^2}$$

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

$$\frac{n^2}{e^6} = \frac{m^3 + am^2e^2 + bme^4}{e^6}$$
$$n^2 = m(m^2 + ame^2 + be^4)$$

Está equação expressa n^2 como o produto de dois inteiros. Se m e $m^2 + ame^2 + be^4$ são relativamente primos entre si, então cada um deles seria o quadrado de um número e então $x = \frac{m}{e^2}$ seria o quadrado de um número racional. Seja $d = mdc(m, m^2 + ame^2 + be^4)$ e assumindo que x está na forma irredutivel, temos $d = mdc(m, m^2 + ame^2 + be^4) = mdc(m, be^4) = mdc(m, b)$. Pois $mdc(m, e) = 1$.

Logo $m = ud$ e também $m^2 + ame^2 + be^4 = vd$, com $mdc(u, v) = 1$ e $n^2 = uvd^2$.

Isto é u e v são quadrados e d é um inteiro tal que $d \mid b$. Sejam então $p_1, p_2, \cdots, p_t$ os primos que dividem b, então $m = \pm {p_1}^{\xi_1}, \cdots, {p_t}^{\xi_t} \pmod{\mathbb{Q}^{*2}}$ onde $\xi_i = 0$ ou 1, $1 \leq i \leq t$.

Se $P = \mathcal{O}$ então $\alpha(P) = 1 \pmod{\mathbb{Q}^{*2}}$. Se $P = T$ então $\alpha(P) = b \pmod{\mathbb{Q}^{*2}}$. Logo a conclusão do item c) está provada.

d) O subgrupo descrito em (c) tem precisamente 2^{t+1} elementos. Como α é injetora e a imagem de $\Gamma/\psi(\overline{\Gamma})$ em $\mathbb{Q}^*/\mathbb{Q}^{*2}$ está contido no conjunto definido em (c), então $\sharp\left(\Gamma/\psi(\overline{\Gamma})\right) \leq 2^{t+1}$. Assim o índice de $\left[\Gamma : \psi\left(\overline{\Gamma}\right)\right]$ é no máximo 2^{t+1}.

■

Agora temos as ferramentas necessárias para provar o Lema 3.4. Queremos provar que 2Γ tem índice finito em Γ.

Lema 3.6 *Sejam A e B grupos abelianos e considere dois homomorfismos $\phi : A \to B$ e $\psi : B \to A$. Suponha que $\psi \circ \phi(a) = 2a \ \ \forall \ \ a \in A$ e que $\phi \circ \psi(b) = 2b \ \ \forall \ \ b \in B$. Suponha ainda que $\phi(A)$ tem índice finito em B e que $\psi(B)$ tem índice finito em A. Então $2A$ tem índice finito em A. Mais precisamente, os índices satisfazem*

$$[A : 2A] \leq [A : \psi(B)]\,[B : \phi(A)]$$

Demonstração. Como $\psi(B)$ tem índice finito em A, existem $a_1, \cdots, a_n \in A$ representantes das classes laterais de B em A. Da mesma forma, sejam $b_1, \cdots, b_m \in B$ representantes das classes laterais de $\phi(A)$ em B. Afirmamos que $\{a_i + \psi(b_j) \ : \ 1 \leq i \leq n; 1 \leq j \leq m\}$ inclui um conjunto completo de representantes das classes laterais de $2A$ em A. Seja $a \in A$. Seja $1 \leq i \leq n$ tal que a está na classe de a_i módulo $\psi(B)$. Isto é, existe $b \in B$ tal que $a - a_i = \psi(b)$. Seja $1 \leq j \leq m$ tal que $b - b_j \in \phi(A)$, isto é, existe $a' \in A$ tal que $b - b_j = \phi(a')$.

Assim

$$\begin{array}{rcll} a & = & a_i + \psi(b) & = a_i + \psi(b_j + \phi(a')) \\ & & & = a_i + \psi(b_j) + \psi(\phi(a')) \\ & & & = a_i + \psi(b_j) + 2a' \end{array}$$

Logo a está na classe de $a_i + \psi(b_j)$ módulo $2A$. Ou seja:

$$a - (a_i + \psi(b_j)) \in 2A$$
$$A/2A \subseteq \left\{\overline{a_i + \psi(b_j)}, 1 \leq i \leq n \ \ , \ \ 1 \leq j \leq m\right\}$$

e

$$[A : 2A] \leq n \cdot m = [A : \psi(B)] \cdot [B : \phi(A)]$$

■

Teorema 3.2 (Teorema de Mordell) *Seja $\mathcal{C}$ uma curva cúbica não singular dada pela equação $\mathcal{C} : y^2 = x^3 + ax^2 + bx$, onde a e b são inteiros. Então o grupo de pontos racionais $\mathcal{C}(\mathbb{Q})$ é um grupo abeliano finitamente gerado.*

Demonstração. Os lemas 3.1, 3.2, 3.3 e 3.4 indicam que as condições do Teorema 3.1 são satisfeitas, logo $\mathcal{C}(\mathbb{Q})$ é finitamente gerado. ■

Capítulo 4

Grupo de Mordell-Weil para curvas específicas

Neste capítulo ilustraremos o Teorema de Mordell com alguns exemplos numéricos.

Temos mostrado que o grupo Γ de pontos racionais na curva $\mathcal{C} : y^2 = x^3 + ax^2 + bx$ é um grupo abeliano finitamente gerado. Escrevendo $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ o grupo de inteiros módulo m, do teorema de estrutura de grupos abelianos finitamente gerados (ver [2], Teorema $IX.1.1$) segue que o grupo Γ é isomorfo a:

$$\Gamma \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \mathbb{Z}}_{r \text{ vezes}} \oplus \mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \cdots \mathbb{Z}_{p_s^{v_s}}$$

Sejam então $P_1, \ldots, P_r, Q_1, \ldots, Q_s \in \Gamma$ os geradores de Γ. Isto é, para todo $P \in \Gamma$, existem $n_1, \ldots, n_r, m_1, \ldots, m_s \in \mathbb{N}$ tais que:

$$P = n_1 P_1 + \cdots + n_r P_r + m_1 Q_1 + \cdots + m_s Q_s \,,$$

onde os inteiros n_i são unicamente determinados por P, enquanto que os inteiros m_i são determinados módulo $p_j^{v_j}$.

O inteiro r é chamado de posto de Γ. O grupo Γ é finito se, e somente se, o grupo tiver posto $r = 0$. O subgrupo isomorfo a $\mathbb{Z}_{p_1^{v_1}} \oplus \mathbb{Z}_{p_2^{v_2}} \cdots \mathbb{Z}_{p_s^{v_s}}$ corresponde ao subgrupo de Γ dos elementos de ordem finita. É claro que os pontos $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ não são únicos. Existem muitas escolhas possíveis para os geradores de Γ.

Já estudamos como calcular os elementos de ordem finita em Γ através de um algoritmo finito. É muito mais difícil calcular a ordem do grupo Γ. Queremos dar algumas ilustrações de como fazer isso em casos especiais. Antes de começar, observemos algumas propriedades adicionais.

A demonstração do Teorema de Mordell, irá nos permitir (em alguns casos) determinar o grupo quociente $\Gamma / 2\Gamma$. Como acima, o subgrupo 2Γ é isomorfo a:

$$2\Gamma = \underbrace{2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \cdots 2\mathbb{Z}}_{} \oplus 2\mathbb{Z}_{p_1^{v_1}} \oplus 2\mathbb{Z}_{p_2^{v_2}} \cdots 2\mathbb{Z}_{p_s^{v_s}}$$

então o grupo quociente será da forma:

$$\frac{\Gamma}{2\Gamma} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \cdots \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}_{p_1{}^{v_1}}}{2\mathbb{Z}_{p_1{}^{v_1}}} \oplus \cdots \oplus \frac{\mathbb{Z}_{p_s{}^{v_s}}}{2\mathbb{Z}_{p_s{}^{v_s}}} \,.$$

Observe que $\frac{\mathbb{Z}}{2\mathbb{Z}} = \mathbb{Z}_2$ é cíclico de ordem dois, ou seja $\frac{\mathbb{Z}_2}{2\mathbb{Z}_2} \cong \mathbb{Z}_2$. De forma mais geral, temos:

$$\frac{\mathbb{Z}_{p^v}}{2\mathbb{Z}_{p^v}} \cong \begin{cases} \mathbb{Z}_2, & \text{se} \quad p = 2 \\ 0, & \text{se} \quad p \neq 2 \end{cases}$$

Assim $[\Gamma : 2\Gamma] = 2^{r+(\text{número de } j \text{ com } p_j=2)}$.

Notemos $\Gamma[2]$ o subgrupo dos elementos $Q \in \Gamma$ tal que $2Q = \mathcal{O}$. Isto é, $\Gamma[2]$ é o subgrupo de Γ de elementos de ordem 2. Um elemento $P \in \Gamma$ é de ordem 2, se

$$2(n_1P_1 + \cdots n_rP_r + m_1Q_1 + \cdots + m_sQ_s) = 0\,.$$

Isso acontece se $n_i = 0$ para cada i , e $2m_j \equiv 0 \pmod{p_j^{v_j}}$. Observe que se $p \neq 2$, primo e $2m \equiv 0 \pmod{p^v}$, então $m \equiv 0 \pmod{p^v}$. Mas, se $p = 2$ e $2m \equiv 0 \pmod{p^v}$, então $m \equiv 0 \pmod{p^{v-1}}$. Assim a ordem do subgrupo $\Gamma[2]$ é

$$\sharp\ \Gamma[2] = 2^{(\text{número de } j \text{ com } p_j=2)}.$$

Combinando estas fórmulas, obtemos o seguinte resultado:

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

Note que esta fórmula é válida para qualquer grupo abeliano finitamente gerado de posto r.

Em nosso caso quais são os possíveis valores que $\sharp\,\Gamma[2]$ pode tomar? Em outras palavras, quantos pontos podemos ter que satisfazem $2Q = 0$ além de $\mathcal{O}$? Sabemos que estes pontos, são os pontos $P = (x, y)$ satisfazendo $y = 0$. Daí é claro que a resposta será:

$$\sharp\,\Gamma[2] = \begin{cases} 2, & se \quad a^2 - 4b \text{ não é um quadrado} \\ 4, & se \quad a^2 - 4b \text{ é um quadrado} \end{cases}$$

Lembramos que $\psi \circ \phi$ é a multiplicação por dois, onde $\phi : \Gamma \to \overline{\Gamma}$ e $\psi : \overline{\Gamma} \to \Gamma$ são os homomorfismos definidos na proposição 3.2.

Como $\psi \circ \phi(\Gamma) = 2\Gamma \quad \subseteq \quad \psi(\overline{\Gamma}) \quad \subseteq \quad \Gamma$ então:

$$[\Gamma : 2\Gamma] = \left[\Gamma : \psi\left(\overline{\Gamma}\right)\right]\left[\psi\left(\overline{\Gamma}\right) : \psi \circ \phi\left(\Gamma\right)\right]\ .$$

Analisemos este último índice $\left[\psi\left(\overline{\Gamma}\right) : \psi \circ \phi\left(\Gamma\right)\right]$.

Lema 4.1 *Sejam A e A' grupos abelianos, B subgrupo de A, e $\psi : A \to A'$ um homomorfismo de grupos. Então*

$$[\psi(A) : \psi(B)] = \frac{[A : B]}{[ker(\psi) : (Ker(\psi) \cap B)]}\,.$$

Demonstração. Considere o homomorfismo $\overline{\psi} : A/B \to \psi(A)/\psi(B)$ definido por $\overline{\psi}(\overline{a}) = \overline{\Gamma(a)}$, onde $\overline{a} \in A/B$ e $\overline{\Gamma(a)} \in \psi(A)/\psi(B)$. $\overline{\Gamma}$ está bem definida pois se $b \in B$, então $\psi(b) \in \psi(B)$. É obvio que $Im(\overline{\psi}) = \psi(A)/\psi(B)$ Calculemos o núcleo de $\overline{\psi}$:

Seja $\overline{a} \in A/B$, assim temos que:

$$\begin{aligned} \overline{a} \in Ker\overline{\Gamma} \quad &\Leftrightarrow \quad \psi(a) \in \psi(B) \\ &\Leftrightarrow \quad \exists\ b \in B : \psi(A) = \psi(B) \\ &\Leftrightarrow \quad a - b \in Ker\Gamma \\ &\Leftrightarrow \quad a \in B + Ker\Gamma \end{aligned}$$

Logo $Ker\overline{\Gamma} = (B + Ker\psi)/B$

Pelo primeiro Teorema do Homomorfismo:

$$\frac{A/B}{(B + ker\psi)/B} \cong \frac{\psi(A)}{\psi(B)}$$

Concluímos pelo segundo Teorema do Homomorfismo que:

$$(B + ker\psi)/B \cong ker\psi/(ker\psi \cap B)$$

O resultado é então imediato. ■

Aplicando este lema obtemos:

$$\left[\psi\left(\overline{\Gamma}\right) : 2\Gamma\right] = \left[\psi\left(\overline{\Gamma}\right) : \psi\left(\phi\left(\Gamma\right)\right)\right] = \frac{\left[\overline{\Gamma} : \phi\left(\Gamma\right)\right]}{\left[Ker\left(\psi\right) : \left(Ker\left(\psi\right) \cap \phi\left(\Gamma\right)\right)\right]}$$

Lembremos que $Ker\psi = \left\{\overline{\mathcal{O}}, \overline{T}\right\}$ e $\overline{T} \in \phi(\Gamma)$ se, e somente se, $\overline{b} = a^2 - 4b$ é um quadrado. Assim $[\Gamma : 2\Gamma] = \frac{\left[\Gamma:\psi(\overline{\Gamma})\right].\left[\overline{\Gamma}:\phi(\Gamma)\right]}{\epsilon}$ onde:

$$\epsilon = [Ker\psi : (Ker\psi \cap \phi\left(\Gamma\right))] = \begin{cases} 1, & se\ \ \overline{b}\ \text{é um quadrado} \\ 2, & se\ \ \overline{b}\ \text{não é um quadrado} \end{cases}$$

Com esta notação temos: $\sharp\Gamma\left[2\right] = \frac{4}{\epsilon}$. Comparando as duas fórmulas de $[\Gamma : 2\Gamma]$, temos:

$$2^r \cdot \frac{4}{\epsilon} = \frac{\left[\Gamma : \psi(\overline{\Gamma})\right] \cdot \left[\overline{\Gamma} : \phi(\Gamma)\right]}{\epsilon}.$$

Ou seja:

$$2^r = \frac{\left[\Gamma : \psi(\overline{\Gamma})\right] \cdot \left[\overline{\Gamma} : \phi(\Gamma)\right]}{4}.$$

No capítulo anterior, provamos $\alpha(\Gamma) \cong \Gamma/\psi(\overline{\Gamma})$.

De forma similar temos $\overline{\alpha}(\overline{\Gamma}) \cong \overline{\Gamma}/\phi(\Gamma)$, onde $\overline{\alpha} : \overline{\Gamma} \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ é o homomorfismo definido por:

$$\overline{\alpha}(P) = \begin{cases} 1, & se\ \ P = \mathcal{O} \\ \overline{b}, & se\ \ P = T \\ \overline{x}, & se\ \ P = (\overline{x}, \overline{y}), \overline{x} \neq 0 \end{cases}.$$

Uma alternativa para a fórmula acima, seria:

$$2^r = \frac{\sharp\,\alpha\left(\Gamma\right)\ \cdot\ \sharp\,\overline{\alpha}\left(\overline{\Gamma}\right)}{4}.$$

Esta fórmula será essencial para o cálculo do posto de Γ.

Afim de determinar a imagem de α, temos que achar os números racionais, módulo quadrado, que podem ser coordenadas x dos pontos $P \in \Gamma$. Sejam então:

$$x = \frac{m}{e^2}\ \text{ e }\ y = \frac{n}{e^3}\ \ \text{escritos na forma irredutível}\ \ e > 0.$$

Se $m = 0$, então $(x, y) = T$ e $\alpha\left(T\right) = b$. Portanto $b\ \left(\text{mod}\ \mathbb{Q}^{*2}\right)$ está sempre em $\alpha\left(\Gamma\right)$. Se $a^2 - 4b$ é um quadrado, então $a^2 - 4b = d^2$, então Γ tem dois outros pontos de ordem dois a saber:

$$\left(\frac{-a+d}{2}, 0\right)\ \ \text{e}\ \ \left(\frac{-a-d}{2}, 0\right).$$

Assim, se $a^2 - 4b = d^2$, então $\alpha\left(T\right)$ contém $\frac{-a\pm d}{2}$. Agora analisaremos os pontos com $m, n \neq 0$. Estes pontos satisfazem:

$$n^2 = m^3 + am^2e^2 + bme^4 = m\left(m^2 + ame^2 + be^4\right).$$

No capítulo anterior vimos que se m e $m^2 + ame^2 + be^4$ são primos entre si, então m e $m^2 + ame^2 + be^4$ são ambos quadrados. Assim, seja $b_1 = \pm mdc\left(m, b\right)$, onde $mb_1 > 0$. Então escrevemos:

$$m = b_1 m_1 \quad \text{e} \quad b = b_1 b_2 \quad \text{com} \quad mdc\,(m_1, b_2) = 1 \quad \text{e} \quad m_1 > 0$$

Se substituirmos na equação da curva acharemos:

$$n^2 = b_1 m_1 \left({b_1}^2 {m_1}^2 + a b_1 m_1 e^2 + b_1 b_2 e^4 \right) = {b_1}^2 m_1 \left(b_1 {m_1}^2 + a m_1 e^2 + b_2 e^4 \right)$$

Então ${b_1}^2 | n^2$, logo $b_1 | n$ e podemos escrever $n = b_1 n_1$. Da mesma forma, temos:

$${b_1}^2 {n_1}^2 = {b_1}^2 m_1 \left(b_1 {m_1}^2 + a m_1 e^2 + b_2 e^4 \right)$$

$${n_1}^2 = m_1 \left(b_1 {m_1}^2 + a m_1 e^2 + b_2 e^4 \right)$$

Como $mdc(b_2, m_1) = 1$ e $mdc(e, m_1) = 1$ temos que m_1 e $b_1 {m_1}^2 + a m_1 e^2 + b_2 e^4$ são primos entre si. O produto deles é um quadrado e $m_1 > 0$, então concluímos que cada um deles é um quadrado. Então podemos fatorar n_1 como $n_1 = MN$ onde $M^2 = m_1$ e $N^2 = b_1 {m_1}^2 + a m_1 e^2 + b_2 e^4$. Substituindo m_1 por M^2 teremos: $N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$

Assim se $(x, y) \in \Gamma$ com $y \neq 0$, podemos escrever:

$$x = \frac{b_1 M^2}{e^2} \text{ e } y = \frac{b_1 MN}{e^3}$$

Assim o módulo quadrado da coordenada x de qualquer ponto da curva é um dos valores de b_1, onde b_1 é um divisor, do inteiro b. Existe um número finito de valores para b_1. Agora fica mais fácil encontrar a ordem de $\alpha\,(T)$. Pegaremos um inteiro b e fatoramos no produto de dois inteiros $b = b_1 b_2$ com todas as possibilidades. Para cada possibilidade de fatoração escreveremos a equação abaixo:

$$N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$$

Observe também que $\alpha \left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3} \right) = b_1 \pmod{\mathbb{Q}^{*2}}$. Logo basta estudar a equação acima para $b_1 \mid b$ livre de quadrado.

Podemos, então resumir nossos resultados na seguinte proposição:

Proposição 4.1 *Seja Γ o grupo de Mordell-Weil da curva definida por $y^2 = x^3 + ax^2 + bx$. Seja $\alpha : \Gamma \to \mathbb{Q}^* / \mathbb{Q}^{*2}$ a função definida em (3.2). Então $b_1 \in \alpha(\Gamma)$ se, e somente se,*

$$b_1 = 1, \quad b_1 = b, \quad b_1 = \frac{-a \pm d}{2}, \text{ se } a^2 - 4b = d^2$$

ou b_1 satisfaz a seguinte propriedade:

$b_1 \mid b$ e $\exists\ M, N, e \in \mathbb{N}^*$, tais que $mdc(M, e) = mdc(N, e) = mdc(b, e) = 1$, $mdc(b_1, M) = mdc(M, N) = 1$ e $N^2 = b_1 M^4 + a M^2 e^2 + b^2 e^4$, onde $b_2 = \frac{b}{b_1}$.

Demonstração. Só resta ver que como $b = b_1 . b_2$ e $b_1 = \pm mdc(m, b)$ então $mdc(b_2, M) = 1$. Por outro lado

$$x = \frac{b_1 M^2}{e^2} \text{ e } y = \frac{b_1 MN}{e^3}$$

estão escritos na forma irredutível, logo $mdc(M, e) = 1$ e da equação $N^2 = b_1 M^4 + a M^2 e^2 + b_2 e^4$ temos $mdc(M, N) = 1$. ■

Observação 4.1 *Como trabalhamos módulo $\mathbb{Q}^{*2}$, os valores de b_1 que devemos estudar são:*

$$b_1 = \pm {p_1}^{\epsilon_1} \dots {p_t}^{\epsilon_t},$$

com $\epsilon_i = 0$ ou 1, para $1 \leq i \leq t$ e $p_1, \cdots p_t$ são todos os primos que aparecem na fatoração de b.

Para cada fatorção de $b = b_1 b_2$ teremos que observar se a equação $N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4$ tem solução nos inteiros, com $M \neq 0$, e cada vez que encontrarmos uma equação com uma solução (M, e, N) obtemos um novo ponto na curva pela fórmula:

$$x = \frac{b_1 M^2}{e^2} \quad \text{e} \quad y = \frac{b_1 MN}{e^3}.$$

O único problema é que não há um método conhecido para decidir se uma equação como esta tem ou não solução. Para cada fatoração $b_1 b_2$ teremos que apresentar um solução ou demonstrar que a equação não tem solução. Desta forma podemos obter informações suficientes para resolver nosso problema.

Os resultados são idênticos para a curva $\overline{\mathcal{C}}$.

Agora apresentaremos alguns exemplos:

4.1 Grupo de Mordell-Weil para a curva $\mathcal{C} : y^2 = x^3 - x$

Teorema 4.1 *Sejam $\mathcal{C}$ e $\overline{\mathcal{C}}$ as curvas elípticas definidas por*

$$\mathcal{C} : y^2 = x^3 - x \qquad e \qquad \overline{\mathcal{C}} : y^2 = x^3 + 4x\,.$$

e sejam $\Gamma = \mathcal{C}(\mathbb{Q})$ e $\overline{\Gamma} = \overline{\mathcal{C}}(\mathbb{Q})$ os grupos de Mordell-Weil de $\mathcal{C}$ e $\overline{\mathcal{C}}$, respectivamente. Então

$$\Gamma \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad e \qquad \overline{\Gamma} \cong \mathbb{Z}/4\mathbb{Z}\,.$$

Demonstração.

Neste caso $a = 0$ e $b = -1$. Como b não possui fatores primos, então $\alpha(\Gamma)$ está contido no conjunto $\{-1, +1\} \pmod{\mathbb{Q}^{*2}}$.

Como $\alpha(\mathcal{O}) = 1$ e $\alpha(T) = -1$, então

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

Consideremos agora a curva $\overline{\mathcal{C}} : y^2 = x^3 + 4x$. Neste caso $\overline{a} = 0$ e $\overline{b} = 4$. Como $\overline{b} = 4$, só possui 2 como fator primo, então $\overline{\alpha}(\overline{T})$ é um subgrupo de $\{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}}$.

Assim $\overline{b_1} = \pm 1$ ou ± 2 e $\overline{b} = \overline{b_1} \cdot \overline{b_2}$.

Observe que $\overline{\alpha}\left(\overline{\mathcal{O}}\right) = \overline{\alpha}\left(\overline{T}\right) = 1$.

Por outro lado se $\overline{b_1} < 0$, então $\overline{b_2} < 0$, pois $\overline{b_1}.\overline{b_2} = 4$. A equação associada é:

$$N^2 = b_1 M^4 + b_2 e^4 < 0$$

que não possui solução real, não nula. Logo, resta estudar o caso $\overline{b_1} = 2$ e $\overline{b_2} = 2$. A equação associada é:

$$N^2 = 2M^4 + 2e^4$$

que possui uma solução $(M, e, N) = (1, 1, 2)$. O ponto P associado a estes valores é $P = (2, 4)$. Portanto

$$\overline{\alpha}\left(\overline{T}\right) = \{1, 2\} \pmod{\mathbb{Q}^{*2}}.$$

Temos então

$$2^r = \frac{\sharp\alpha(\Gamma).\sharp\overline{\alpha}(\overline{\Gamma})}{4} = \frac{2.2}{4} = 1$$

Isto é $r = 0$. Veja que esta fórmula também calcula o posto r' de $\overline{\Gamma}$: $r' = r = 0$.

Pelo teorema de Nagel-Lutz, $P = (x_0, y_0) \in \Gamma$ é um ponto de torção se $x_0, y_0 \in \mathbb{Z}$ e $y_0 = 0$ ou ${y_0}^2 \mid \Delta$. Assim $y_0 \neq 0$, então ${y_0}^2 \mid -4b^3 = 4$. Logo $y_0 = \pm 1, \pm 2$. A equação $x^3 - x = {y_0}^2$ não possui solução inteira para nenhum destes valores. Se $y_0 = 0$, tem $x_0 = 0, 1, -1$. Assim:

$$\Gamma = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Similarmente $P = (x_0, y_0) \in \overline{\Gamma}$ é um ponto de torção com $y_0 \neq 0$ se $x_0, y_0 \in \mathbb{Z}$ e ${y_0}^2 \mid \Delta$. Assim ${y_0}^2 \mid -4\overline{b}^3 = -4.4^3 = -2^8$, isto é $y_0 \mid 2^4$.

Utilizando o sistema de álgebra computacional Máxima, vemos que existe solução somente para $y_0 = \pm 4$. Nesse caso $x = 2$. Por outro lado se $y_0 = 0$, então $x_0 = 0$. Pela fórmula de duplicação, $2(2,4) = T = (0,0)$.

Logo $\overline{\Gamma} = \{\mathcal{O}, (0,0), (2,4), (2,-4)\} \cong \mathbb{Z}/4\mathbb{Z}$. ■

4.2 Grupo de Mordell-Weil da curva $\mathcal{C} : y^2 = x^3 - 2x$

Teorema 4.2 *Sejam $\mathcal{C}$ e $\overline{\mathcal{C}}$ as curvas elípticas definidas por*

$$\mathcal{C} : y^2 = x^3 - 2x \qquad e \qquad \overline{\mathcal{C}} : y^2 = x^3 + 8x\,.$$

e sejam $\Gamma = \mathcal{C}(\mathbb{Q})$ e $\overline{\Gamma} = \overline{\mathcal{C}}(\mathbb{Q})$ os grupos de Mordell-Weil de $\mathcal{C}$ e $\overline{\mathcal{C}}$, respectivamente. Então

$$\Gamma \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad e \qquad \overline{\Gamma} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

Demonstração. Pela proposição 4.2, que será provada posteriormente, o subgrupo de torção de Γ é isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Sabemos que $\overline{\mathcal{O}}$ e $\overline{T}$ são pontos de torção de $\overline{\Gamma}$. Para achar os outros pontos de torção, calculamos $\overline{\Delta} = -4\overline{b}^3 = -4 \cdot 8^3 = -2^{11}$. Pelo teorema de Nagell-Lutz, um ponto $P = (x_0, y_0)$ é de torção se $x_0, y_0 \in \mathbb{Z}$ e $y_0 = 0$ ou $y_0^2 \mid \overline{\Delta}$. Se $y_0 \neq 0$, então $y_0 \mid 2^5$. Utilizando o sistema de álgebra computacional Máxima, vemos que a equação $x^3 + 8x = y_0^2$ não possui solução inteira para $y_0 = \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32$. Portanto, o subgrupo de torção de $\overline{\Gamma}$ é também isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

Para calcular o posto de Γ e $\overline{\Gamma}$, devemos calcular as imagens de α e $\overline{\alpha}$. Como 2 é o único primo que aparece na fatoração de $b = -2$ e $\overline{b} = 8$, então:

$$\begin{aligned} \alpha(\Gamma) &\subseteq \{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}}\,, \\ \overline{\alpha}(\overline{\Gamma}) &\subseteq \{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}}\,. \end{aligned}$$

Observe que $\alpha(\mathcal{O}) = 1$ e $\alpha(T) = b = -2$. Por outro lado, como $(-1) \cdot 2 = -2$, então

$$-1 \in \alpha(\Gamma) \Longleftrightarrow 2 \in \alpha(\Gamma)\,.$$

Dessa forma, basta estudar o caso $b_1 = -1$. A equação associada é:

$$N^2 = -M^4 + 2e^4 \qquad \text{pois} \qquad b_2 = 2\,.$$

Uma solução é $(M, e, N) = (1, 1, 1)$. Que corresponde ao ponto $P = (-1, -1)$. Veja que $\alpha(P) = -1$.

Isso implica que

$$\alpha(\Gamma) = \{\pm 1, \pm 2\} \pmod{\mathbb{Q}^{*2}}\,.$$

Estudemos a imagem de $\overline{\alpha}$. Novamente, começamos por observar as imagens de $\overline{\mathcal{O}}$ e $\overline{T}$:

$$\overline{\alpha}(\overline{\mathcal{O}}) = 1 \quad \text{e} \quad \overline{\alpha}(\overline{T}) = 8 = 2 \pmod{\mathbb{Q}^{*2}}.$$

Como $(-1)\cdot(-2) = 2$, desta vez temos

$$-1 \in \overline{\alpha}(\overline{\Gamma}) \Longleftrightarrow -2 \in \overline{\alpha}(\overline{\Gamma}).$$

Consideremos então unicamente o caso $\overline{b}_1 = -1$ e $\overline{b}_2 = -8$. A equação agora é

$$N^2 = -M^4 - 8e^4,$$

que não possui solução real, não nula. Logo

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 2\} \pmod{\mathbb{Q}^{*2}}.$$

Pela fórmula do posto:

$$2^r = \frac{4\cdot 2}{2} = 2 \Longrightarrow r = 1.$$

Concluímos que $\Gamma \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ e $\overline{\Gamma} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. ■

4.3 Grupo de Mordell-Weil para a curva $\mathcal{C} : y^2 = x^3 - 5x$

Teorema 4.3 *Sejam $\mathcal{C}$ e $\overline{\mathcal{C}}$ as curvas elípticas definidas por*

$$\mathcal{C} : y^2 = x^3 - 5x \qquad e \qquad \overline{\mathcal{C}} : y^2 = x^3 + 20x.$$

e sejam $\Gamma = \mathcal{C}(\mathbb{Q})$ e $\overline{\Gamma} = \overline{\mathcal{C}}(\mathbb{Q})$ os grupos de Mordell-Weil de $\mathcal{C}$ e $\overline{\mathcal{C}}$, respectivamente. Então

$$\Gamma \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \qquad e \qquad \overline{\Gamma} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Demonstração. Pela proposição 4.2, que será provada posteriormente, o subgrupo de torção de Γ é isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Sabemos que $\overline{\mathcal{O}}$ e $\overline{T} \in \overline{\Gamma}_{tors}$. Pelo Teorema de Nagell-Lutz, se um ponto $P = (x_0, y_0)$, com $y_0 \neq 0$ é de torção, então x_0 e $y_0 \in \mathbb{Z}$ e ${y_0}^2 \mid \overline{\Delta}$; onde $\overline{\Delta} = -4\overline{b}^3 = -2^8.5^3$. Logo $y_0 \mid 2^4.5$. Assim

$$y_0 = \pm 1, \pm 2, \pm 4, \pm 5, \pm 8, \pm 10, \pm 16, \pm 20, \pm 40, \pm 80$$

.

Utilizando o sistema de álgebra computacional Máxima, vemos que a equação $x^3 + 20x = {y_0}^2$ não possui solução inteira para nenhum desses valores de y_0. Portanto $\overline{\Gamma}_{tors} \cong \mathbb{Z}/2\mathbb{Z}$. Observe que:

$$\alpha(\Gamma) \subseteq \{\pm 1, \pm 5\}$$

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{\pm 1, \pm 2, \pm 5, \pm 10\}.$$

Como $\alpha(\mathcal{O}) = 1$ e $\alpha(T) = b = -5$, então

$$-1 \in \alpha(\Gamma) \Leftrightarrow 5 \in \alpha(\Gamma).$$

Considere $b_1 = -1$, $b_2 = 5$. A equação associada é:

$$N^2 = -M^4 + 5e^4$$

que possui como solução $(M, e, N) = (1, 1, 2)$. Logo o ponto $P = (-1, 2)$ tem como imagem -1.

Assim

$$\alpha(\Gamma) = \{\pm 1, \pm 5\}.$$

Veja que

$$\overline{\alpha}(\overline{\mathcal{O}}) = 1 \text{ e } \overline{\alpha}(\overline{T}) = 20 = 5 \pmod{\mathbb{Q}^{*2}}.$$

Por outro lado se $\overline{b_1} < 0$ então $\overline{b_2} < 0$ e $N^2 = -\overline{b_1}M^4 - \overline{b_2}e^4$ não possui solução real, não nula.

Portanto

$$2 \in \overline{\alpha}(\overline{\Gamma}) \Leftrightarrow 10 \in \overline{\alpha}(\overline{\Gamma}).$$

Seja $\overline{b_1} = 2$ e $\overline{b_2} = 10$, então $N^2 = 2M^4 + 10e^4$.

Como $5 \nmid N$, $5 \nmid M$ então para esta equação possuir solução, 2 deve ser um resíduo quadrático módulo 5. Como não é, então

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 5\}.$$

Daí $2^r = \dfrac{4.2}{4} = 2$. Portanto $r = 1$ e $\Gamma \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ e $\overline{\Gamma} \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. ■

4.4 Grupo de Mordell-Weil para Curvas Elípticas do tipo $y^2 = x^3 - px$, p primo

Nosso objetivo agora é estudar o grupo de Mordell-Weil da curva $y^2 = x^3 - px$, onde p é um número primo.

Em 2005, Kude e Matose (Ver [3]) calcularam o posto desta curva para p número primo de Fermat e para p número primo de Mersenne. Em 2007, Spearman (Ver [6]), estende o resultado de Kudo e Matose para primos da forma $p = u^4 + v^4$. Um primo de Fermat é um primo da forma $p = 2^{2^n} + 1$, com $n \geq 0$. Fazendo $u = 2^{2^{n-2}}$ e $v = 1$, vemos que um primo de Fermat maior que 5 é da forma $p = u^4 + v^4$.

Os teoremas a seguir mostram o resultado para primos ímpares da forma $p = u^4 + v^4$ e primos de Mersenne. Os primos de Fermat que não são da forma $p = u^4 + v^4$, são $p = 3$ e $p = 5$. Para $p = 5$, o resultado se encontra no Teorema 4.3 e como $p = 3$ também é um primo de Mersenne, seu grupo de Mordell-Weil esta descrito no teorema 4.5. Para $p = 2 = 1^4 + 1^4$ o resultado se encontra no teorema 4.2.

A lista abaixo mostra os números primos menores que 1000 para os quais o grupo de Mordell-Weil da curva $y^2 = x^3 - px$ foi calculado. Lembrando que todo número de Fermat maior que 5 é da forma $p = u^4 + v^4$.

Entre 1000 e 10000, $8191 = 2^{13} - 1$ é um número primo de Mersenne e 1297, 2417, 2657, 3697, 4177, 4721, e 6577 são primos da forma $p = u^4 + v^4$.

A proposição a seguir mostra que o subgrupo de pontos de ordem finita do grupo de Mordell-Weil da curva $y^2 = x^3 - px$, onde p é primo, é isomorfo a $\mathbb{Z}/2\mathbb{Z}$.

Proposição 4.2 *Sejam p um número primo e $\mathcal{C}$ a curva elíptica definida por $y^2 = x^3 - px$. Denotaremos $\Gamma = \mathcal{C}(\mathbb{Q})$ o grupo de Mordell-Weil da curva e Γ_{tors} o subgrupo de pontos de ordem finita de Γ. Então $\Gamma_{tors} \cong \mathbb{Z}/2\mathbb{Z}$.*

Demonstração. Seja $P = (x, y) \in \Gamma$, $P \neq \mathcal{O}$ e T. Sabemos do Teorema de Nagell-Lutz que se $P \in \Gamma_{tors}$ então $x, y \in \mathbb{Z}$ e $y^2 | \Delta$, onde $\Delta = 4p^3$. Vejamos que os pontos que satisfazem estas condições não pertencem a Γ_{tors}. Seja $P = (x, y) \in \Gamma_{tors}$, como $y^2 | \Delta$ então $y^2 = 1, 4, p^2, 4p^2$. Note que $y^2 = x^3 - px = x(x^2 - p)$, onde x e $x^2 - p$ são números inteiros.

Número primo	Mersenne, Fermat ou $p = u^4 + v^4$	
2	$u^4 + v^4$	$2 = 1^4 + 1^4$
3	Mersenne, Fermat	$3 = 2^2 - 1 = 2^{2^0} + 1$
5	Fermat	$5 = 2^{2^1} + 1$
7	Mersenne	$7 = 2^3 - 1$
17	Fermat	$17 = 2^{2^2} + 1$
31	Mersenne	$31 = 2^5 - 1$
97	$u^4 + v^4$	$97 = 3^4 + 2^4$
127	Mersenne	$127 = 2^7 - 1$
257	Fermat	$257 = 2^{2^3} + 1$
337	$u^4 + v^4$	$337 = 3^4 + 4^4$
641	$u^4 + v^4$	$641 = 2^4 + 5^4$
881	$u^4 + v^4$	$881 = 4^4 + 5^4$

• Se $y^2 = 1$, então $x(x^2 - p) = 1$. Daí $x = \pm 1$ e então $1 - p = \pm 1$.
Logo $p = 2$ e $x = -1$. Nesse caso $P = (-1, 1)$ ou $P = (-1, -1)$.

• Se $y^2 = 4$ então $x(x^2 - p) = 4$.
Se $x = \pm 1$, então $1 - p = \pm 4$, logo $p = 5$, $x = -1$, $y = \pm 2$.
Se $x = \pm 2$, então $4 - p = \pm 2$, logo $p = 2$, $x = 2$, $y = \pm 2$.
Se $x = \pm 4$, então $16 - p = \pm 1$, logo $p = 17$, $x = -4$, $y = \pm 2$.

• Se $y^2 = p^2$ então $x(x^2 - p) = p^2$.
Se $x = \pm 1$, então $1 - p = \pm p^2$. Impossível.
Se $x = \pm p$, então $p^2 - p = \pm p$, logo $p = 2$, $x = 2$, $y = \pm 2$.
Se $x = \pm p^2$, então $p^4 - p = \pm 1$. Impossível.

• Se $y^2 = 4p^2$, então $x(x^2 - p) = 4p^2$.
Se $p^2 | x$ então $p | x^2 - p$ e portanto $p^3 | 4p^2$. Isto é $p = 2$, mas $x(x^2 - 2) = 16$ não possui solução inteira. Assim $p^2 \nmid x$. Da relação $p^2 | x(x^2 - p)$ obtemos então que $p | (x^2 - p) \Rightarrow p | x$. Isto implica $x = px_0$ e a equação se torna:

$$px_0 \left(p^2 {x_0}^2 - p\right) = 4p^2$$
$$x_0 \left(p {x_0}^2 - 1\right) = 4$$

Se $2 \mid x_0 \Rightarrow 2 \mid p{x_0}^2 - 1$, mas $p{x_0}^2 - 1$ não pode ser ± 1, pois $p{x_0}^2 \geq 8$.
Resta o caso $x_0 = \pm 1$. Nesse caso $p - 1 = \pm 4$, logo $p = 5$, $x_0 = 1$, $x = 5$, $y = \pm 10$.
Observamos acima que apenas três curvas possuem pontos diferentes de $\mathcal{O}$ e T, candidatos à pontos de torção.

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

Usando a fórmula de duplicação de um ponto vemos que, em cada um destes casos, $2P$ não possui coordenadas inteiras e portanto $P \notin \Gamma_{tors}$. Segue que os únicos pontos de torção Γ são $\mathcal{O}$ e T. ■

O teorema a seguir calcula o grupo de Mordell-Weil para o caso $p = u^4 + v^4 > 2$.

Teorema 4.4 *Seja p um número primo ímpar da forma $p = u^4 + v^4$, onde $u, v \in \mathbb{N}$ inteiros. Seja $\mathcal{C}$ a curva elíptica definida por $y^2 = x^3 - px$. Notemos $\Gamma = \mathcal{C}(\mathbb{Q})$ o grupo de Mordell-Weil da curva. Então $\Gamma \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z}$.*

Demonstração.

Pelo teorema anterior $\Gamma_{tors} \cong \mathbb{Z}/2\mathbb{Z}$. Calcularemos então o posto r. Considere $\overline{\mathcal{C}}$, a curva $y^2 = x^3 + 4px$, $\overline{\Gamma} = \overline{\mathcal{C}}(\mathbb{Q})$ e $\alpha, \overline{\alpha}$ os homomorfismos da definição 3.2.

Como $b = -p$, então

$$\alpha(\Gamma) \subseteq \{\pm 1, \pm p\}.$$

Sabemos que $\alpha(\mathcal{O}) = 1$ e $\alpha(T) = -p$. Portanto

$$-1 \in \alpha(\Gamma) \Leftrightarrow p \in \alpha(\Gamma).$$

Estudaremos então o caso $b_1 = -1$, $b_2 = p$. A equação associada é

$$N^2 = -M^4 + pe^4.$$

Veja que $(M, e, N) = (u, 1, v^2)$ é solução da equação. O ponto da curva associado a esta solução é:

$$P = \left(\frac{b_1 M^2}{e^2}, \frac{b_1 MN}{e^3}\right) = \left(-u^2, -uv^2\right)$$

Assim

$$\alpha(\Gamma) = \{\pm 1, \pm p\}.$$

Calcularemos agora $\overline{\alpha}(\overline{\Gamma})$. Como $\overline{b} = 4p$, então

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{\pm 1, \pm 2, \pm p, \pm 2p\}.$$

Observe que $\alpha(\mathcal{O}) = 1$ e $\alpha(\overline{T}) = \overline{b} = p \pmod{\mathbb{Q}^{*2}}$.

Se $\overline{b_1} < 0$, então $\overline{b_2} < 0$ e a equação $N^2 = \overline{b_1} M^4 + \overline{b_2} e^4$ não possui solução real, não nula.

Logo

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{1, 2, p, 2p\}$$

e

$$2 \in \overline{\alpha}(\overline{\Gamma}) \Leftrightarrow 2p \in \overline{\alpha}(\overline{\Gamma}).$$

A equação associada será:

$$N^2 = 2M^4 + 2pe^4.$$

Esta equação possui a solução:

$$(M, e, N) = (u - v, 1, 2u^2 - 2uv + 2v^2)$$

o ponto associado a esta solução será:

$$P = \left(2(u-v)^2, 2(u-v)(2u^2 - 2uv + 2v^2)\right),$$

satisfazendo

$$\overline{\alpha}(P) = 2(u-v)^2 = 2 \pmod{\mathbb{Q}^{*2}}.$$

Logo

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 2, p, 2p\}.$$

Segue que

$$2^r = \frac{4.4}{4} = 2^2.$$

Portanto o posto de Γ é $r = 2$ e então $\Gamma \cong \mathbb{Z}^2 \oplus \mathbb{Z}/2\mathbb{Z}$. ■

Teorema 4.5 *Sejam p um número primo de Mersenne e seja $\mathcal{C}$ a curva elíptica definida por $y^2 = x^3 - px$. Usaremos a notação $\Gamma = \mathcal{C}(\mathbb{Q})$ para o grupo de Mordell-Weil da curva $\mathcal{C}$. Então:*

$$\Gamma \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} & se \quad p = 3 \\ \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & se \quad p > 3. \end{cases}$$

Demonstração.

Como p é um número primo de Mersenne, seja q o número primo tal que $p = 2^q - 1$. Pela proposição 4.2, $\Gamma_{tors} \cong \mathbb{Z}/2\mathbb{Z}$.

Considere $p = 3$:

$$\mathcal{C} : y^2 = x^3 - 3x; \qquad b = -3 \qquad \text{e} \qquad \overline{\mathcal{C}} : y^2 = x^3 + 12x; \qquad \overline{b} = 12.$$

Então

$$\alpha(\Gamma) \subseteq \{\pm 1, \pm 3\}$$

e

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{\pm 1, \pm 2, \pm 3, \pm 6\}.$$

Primeiramente veja que $\alpha(\mathcal{O}) = 1$, $\alpha(T) = -3$. Então:

$$-1 \in \alpha(\Gamma) \Leftrightarrow 3 \in \alpha(\Gamma).$$

Estudaremos o caso $b_1 = -1$ e $b_2 = 3$. A equação será:

$$N^2 = -M^4 + 3e^4.$$

Como $mdc(M, N) = 1$ então $3 \nmid M$ e $3 \nmid N$. Daí

$$N^2 \equiv -M^4 \pmod 3.$$

Como -1 não é um quadrado módulo 3, $N^2 = -M^4 + 3e^4$ não possui solução módulo 3, com $3 \nmid M$ e $3 \nmid N$. Logo

$$\alpha(\Gamma) = \{1, -3\}.$$

Veja que $\overline{\alpha}(\overline{\mathcal{O}}) = 1$, $\overline{\alpha}(\overline{T}) = 12 = 3 \pmod{\mathbb{Q}^{*2}}$. Novamente, escolhendo $\overline{b_1} < 0$, teremos $\overline{b_2} < 0$ e $N^2 = \overline{b_1}M^4 + \overline{b_2}e^4$ não possui solução real, não nula.

Assim

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{1, 2, 3, 6\}$$

e

$$2 \in \overline{\alpha}(\overline{\Gamma}) \Leftrightarrow 6 \in \overline{\alpha}(\overline{\Gamma})$$

Estudaremos o caso $\overline{b_1} = 2$ e $\overline{b_2} = 6$. A equação associada será:

$$N^2 = 2M^4 + 6e^4.$$

Novamente $3 \mid N \Leftrightarrow 3 \mid M$, logo $3 \nmid N$ e $3 \nmid M$. Módulo 3 a equação será:

$$N^2 \equiv 2M^4 \pmod 3$$

que não possui solução, pois 2 não é um quadrado módulo 3.

Portanto

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 3\}$$

e

$$2^r = \frac{2.2}{4} = 1.$$

Isto é $r = 0$, ou seja $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$.

Seja agora $p = 2^q - 1$, $q > 2$, p primo de Mersenne e q primo. Como antes devemos verificar se $-1 \in \alpha(\Gamma)$ e se $2 \in \overline{\alpha}(\overline{\Gamma})$, pois

$$\alpha(\Gamma) \subseteq \{\pm 1, \pm p\}$$

e

$$\overline{\alpha}(\overline{\Gamma}) \subseteq \{\pm 1, \pm 2, \pm p, \pm 2p\}\,.$$

Seja $b_1 = -1$ e $b_2 = p$. A equação associada será:

$$N^2 = -M^4 + pe^4.$$

Novamente $p \mid N$ e $p \mid M$. A equação módulo p será:

$$N^2 \equiv -M^4 \pmod{p}.$$

Mas -1 não é resíduo quadrático módulo p, pois se -1 fosse resíduo quadrático módulo p, então existiria um inteiro $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod{p}$.

Pelo pequeno teorema de Fermat $a^p - 1 \equiv 1 \pmod{p}$, logo

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

Mas $(-1)^{\frac{p-1}{2}} = (-1)^{2^{q-1}-1} = -1$. Contradição.

Logo

$$\alpha(\Gamma) = \{1, -p\}\,.$$

Seja $\overline{b_1} = 2$ e $\overline{b_2} = 2p$. A equação associada será:

$$N^2 = 2M^4 + 2pe^4$$

que possui como solução $(M, e, N) = (1, 1, 2^{\frac{q+1}{2}})$, pois:

$$2^{q+1} = 2 + 2(2^q - 1).$$

Logo

$$\overline{\alpha}(\overline{\Gamma}) = \{1, 2, p, 2p\}\,.$$

Assim $2^r = \dfrac{2.4}{4} = 2$ então $r = 1$. Portanto $\Gamma \cong \mathbb{Z}/2\mathbb{Z}$. ■

Referências Bibliográficas

[1] Chahal, J.S., Topics in Number Theory, Springer, 1998.

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

[3] Kudo, T., Matose, K., On Group Structure of Some Special Elliptic Curves. Mathematical Journal of Okayama University, 47. 81-84, 2005.

[4] Milne, J.S., Elliptic Curves, BookSerge Publishing, 2006.

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

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

[7] Burton, D.M., Elemetary Number Theory, Fifth Edition, McGraw-Hill Higher Education, 2002.

[8] Hardy, G. H., Wright, E.M., An Introduction to the Theory of Numbers, Fifth edition Oxford Science Publications 1979.

[9] Mazur, B., Modular curves and the Eisenstein ideal. IHES Publ. Math. 47 (1977), 33-186.

[10] Mazur, B., Rational isogenies of prime degree. Invent. Math. 44 (1978),129-162.