BRUNO ANDRADE DE SOUZA

Curvas Elípticas e Números Congruentes

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
2013

BRUNO ANDRADE DE SOUZA

Curvas Elípticas e Números Congruentes

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: Geometrica Algébrica.

Orientador: Prof. Dr. Victor Gonzalo Lopez Neumann.

UBERLÂNDIA - MG
2013

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

S729c 2013

Souza, Bruno Andrade de, 1989-
Curvas elípticas e números congruentes / Bruno Andrade de Souza. - 2013.
72 p. : 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

iv

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
Av. João Naves de Ávila, 2121, Bloco 1F, Sala 1F 159
Campus Santa Mônica, Uberlândia - MG, CEP 38400-902

ALUNO: Bruno Andrade de Souza.

NÚMERO DE MATRÍCULA: 11112MAT006.

ÁREA DE CONCENTRAÇÃO: Matemática.

LINHA DE PESQUISA: Geometria Algébrica.

PÓS-GRADUAÇÃO EM MATEMÁTICA: Nível Mestrado.

TÍTULO DA DISSERTAÇÃO: Curvas Elípticas e Números Congruentes.

ORIENTADOR: Prof. Dr. Victor Gonzalo Lopez Neumann.

Esta dissertação foi **APROVADA** em reunião pública realizada na Sala Multiuso da Faculdade de Matemática, Bloco 1F, Campus Santa Mônica, em 26 de Fevereiro de 2013, às 14h00min, pela seguinte Banca Examinadora:

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

Uberlândia-MG, 26 de Fevereiro de 2013.

Dedicatória

Dedico este trabalho a todos meus familiares, em especial à minha Mãe Edvania Aragão Andrade, ao meu Pai Sergio Luiz de Souza e a minha Avó Aparecida Lucizzano, pela maravilhosa criação e por todo apoio dado ao longo da minha vida acadêmica.

Agradecimentos

Agradeço a Deus em primeiro lugar por todas as bençãos realizadas em minha vida.

À minha mãe Edvania Aragão Andrade que foi a única pessoa que nunca deixou de acreditar em mim, até mesmo quando eu desacreditava. É por ela e para ela que luto todos os dias. Quando eu penso em desistir, eu lembro que tem uma guerreira lá em Andradina torcendo e orando por mim.

Ao meu Pai Sergio Luiz de Souza por todo amor, carinho e apoio dado ao longo desta trajetória acadêmica. Por ser meu porto seguro e por nunca medir esforços para me ajudar.

À minha Avó Aparecida Lucizzano, que contribuiu muito em minha criação para que eu me tornasse um homem de caráter.

Ao meu orientador Victor Gonzalo Lopez Neumann, pela dedicação e paciência durante esse periodo. Por ser um excelente profissional, esclarecendo sempre as minhas dúvidas com muita disposição e por ter um baita coração.

Aos professores Cícero Fernandes de Carvalho e Herivelto Martins Borges Filho, por terem aceito o convite para fazer parte desta banca.

Aos meus amigos de Andradina, que considero como irmãos: Homero, Fabricio Acialdi, Bruno Henrique, Herik, Raniery (Ranão) e Marlon Uatanabe por estarem sempre ao meu lado em todos os momentos. Em especial, ao meu parceiro Edcarlos Santos (Kidão), que sabe bem o que eu passei e sempre esteve junto comigo. A amizade é tudo !

Aos amigos do DEX/CPTL-UFMS, Thiago Madalena (Tubias), Wendhel Raffa, Leandro, Joel Becker, Rogério Lima, Ana Carla Lelis, Janaina, por todos os momentos especiais que passamos juntos durante a graduação. De modo especial, aos parceiros Marcos Eduardo (Marcão) e Raildo Lima, pelo companheirismo e fortalecimento da nossa amizade. Ao Raildo, um agradecimento a parte, pela ajuda com as figuras da Dissertação.

Aos amigos da turma do mestrado Iego, Rafael, Otoniel e aos alunos das outras turmas também, que contribuiram muito em minha formação. Em especial, agradeço a minha grande amiga Leticia, que é uma pessoa extraordinária e responsável por grande parte do meu amadurecimento matemático.

Ao meu amigo Romerson, que me acolheu em Uberlândia e me ajudou o tempo que foi necessário para me estabilizar em Uberlândia.

A todos os professores da Pós-Graduação em Matemática da UFU, em especial aos que ministraram alguma disciplina durante o mestrado.

Aos professores do DEX/CPTL-UFMS, em especial aos meus grandes mestres Antônio Carlos Tamarozzi, Renato César, Sônia Angelina, Eugenia, Rosana Takehara e Paulo Henrique

pelo incentivo e pela confiança.

À FAPEMIG pelo apoio financeiro.

A todos mencionados anteriormente, e aos que eu venha a ter esquecido, meu MUITO OBRIGADO!

SOUZA, B. A. *Curvas Elípticas e Números Congruentes.* 2012. 69 p. Dissertação de Mestrado, Universidade Federal de Uberlândia, Uberlândia-MG.

Resumo

O objetivo deste trabalho é relacionar Curvas Elípticas e Números Congruentes. Descrevemos uma operação sobre a curva, que torna o conjunto de seus pontos, sobre um corpo qualquer, um grupo abeliano. Em seguida, apresentamos o Teorema de Nagell-Lutz, que nos dá as condições necessárias para que um ponto tenha ordem finita no grupo. Feito isto, provamos o Teorema de Mordell para curvas do tipo $y^2 = x^3 + ax^2 + bx$; tal teorema nos diz que o conjunto dos pontos racionais sobre a Curva Elíptica é um grupo abeliano finitamente gerado. Finalmente, definimos números congruentes, apresentamos algumas propriedades e exemplos sobre tais números e estabelecemos a conexão entre Números congruentes e Curvas Elípticas.

Palavras-chave: (Curvas Elípticas, Teorema de Mordell, Números Congruentes).

SOUZA, B. A. *Congruent Numbers and Elliptic Curves* 2013. 69 p. M. Sc. Dissertation, Federal University of Uberlândia, Uberlândia-MG.

Abstract

The aim of this paper is to relate Congruent Numbers and Elliptic Curves. We describe an operation on the curve, which makes the set of its points, on any field, an abelian group. Next we present the Nagell-Lutz theorem, which gives us the necessary conditions for a point that has finite order in the group. Having done this, we prove the Mordell theorem for curves like $y^2 = x^3 + ax^2 + bx$; this theorem tells us that the set of rational points on elliptic curve is a finitely generated abelian group. Finally, we define congruent numbers, we present some properties and examples of such numbers and establish the connection between Congruent Numbers and Elliptic Curves.

Keywords: (Elliptic curves, Mordell Theorem, Congruent numbers).

SUMÁRIO

INTRODUÇÃO

As curvas elípticas têm sido muito utilizadas para lançar luz sobre alguns problemas importantes como problemas em criptografia, o problema de empacotamentos de esferas e o problema dos números congruentes.

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

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

onde $a, b, c \in \mathbb{K}$ e o discriminante $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27b^2$ de E é não nulo.

Um dos fatos mais interessantes sobre as curvas elípticas é que, o conjunto dos pontos racionais sobre ela tem uma estrutura de grupo abeliano finitamente gerado, mais especificamente, temos o seguinte teorema:

Teorema de Mordell: Seja E uma curva elíptica dada pela equação

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

onde a,b,c são inteiros e seja $E(\mathbb{Q}) = \{[x : y : z] \in E : x, y, z \in \mathbb{Q}\}$. Então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

Através do Teorema 3.6.5 da teoria dos grupos finitamente gerados, podemos decompor:

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

onde $E(\mathbb{Q})_{tors}$ é o grupo de pontos de torção e o inteiro r é o posto da curva elíptica.

Um número racional é dito congruente, se for a área de um triângulo retângulo cujos lados são racionais.

Estamos interessados no problema dos números congruentes, que consiste em saber se um dado número racional é congruente ou não.

A relação entre números congruentes e curvas elípticas se dá, através do seguinte resultado:

"Um número n é congruente se, e somente se, o posto da curva elíptica $y^2 = x^3 - n^2x$ é positivo."

Nossa dissertação está organizada da seguinte maneira:

No primeiro capítulo daremos alguns conceitos sobre as curvas elípticas. Começamos com alguns conceitos de curvas algébricas, definindo curva afim, plano projetivo, curvas projetivas. A seguir enunciamos o Teorema de Bézout, que é essencial na construção da lei de grupo sobre o conjunto de pontos de uma curva elíptica.

O segundo capítulo trata sobre o conjunto de pontos de ordem 2 e 3. Começamos mostrando as propriedades que satisfazem pontos de ordem 2 e 3. A seguir enunciamos os teoremas de Nagell-Lutz e de Mazur, que nos ajudarão a encontrar todos os pontos racionais de torção de uma curva elíptica.

No terceiro capítulo demonstraremos o Teorema de Mordell para uma classe de curvas e daremos alguns resultados da teoria de grupos, úteis no próximo capítulo.

No quarto capítulo daremos algumas propriedades sobre os números congruentes, enunciaremos e provaremos a relação entre Números Congruentes e Curvas Elípticas.

Bruno Andrade de Souza

Uberlândia-MG, 26 de Fevereiro de 2013.

CAPÍTULO 1

CURVAS ELÍPTICAS

Neste capítulo, apresentaremos alguns conceitos da teoria das curvas elípticas. Denotaremos por $\mathbb{K}$ um corpo e por $\overline{\mathbb{K}}$ seu fecho algébrico. A teoria deste capítulo pode ser encontrada em [2] e [4].

1.1 Curvas Algébricas e o Plano Projetivo

Definição 1.1.1. *Seja $f(x,y)$um polinômio não constante em $\mathbb{R}[x,y]$. Chamamos o conjunto*

$$C_f = \{(x,y) \in \mathbb{R}^2 : f(x,y) = 0\}$$

uma curva algébrica plana real.

Exemplo 1.1.2. *a) Retas: $f(x,y) = ax + by + c$, $(a,b) \neq (0,0)$;*

b) Círculo: $f(x,y) = x^2 + y^2 - 1$;

c) Parábola: $f(x,y) = y - x^2$;

d) Seja $f(x,y) = x^2 + y^2$ então $C_f = \{(0,0)\}$;

e) Seja $f(x,y) = x^2 + y^2 + 1$ então $C_f = \varnothing$.

Observação 1.1.3. *Estamos chamando C_f de "curva", logo nos exemplos d) e e) esta nomenclatura pode parecer estranha. Agora, se nós permitirmos soluções complexas para a equação $f(x,y) = 0$ em d) e e), então, C_f passa a ter infinitos pontos.*

Definição 1.1.4. *Seja $\mathbb{K}$ um corpo algebricamente fechado. O espaço afim de dimensão n de $\mathbb{K}$ é o conjunto $\mathbb{K}^n$.*

Seja $S \subset \mathbb{K}[x_1, \ldots, x_n]$. O conjunto,

$$C_S = \{(x_1, \ldots, x_n) \in \mathbb{K}^n : f(x_1, \ldots, x_n) = 0, \forall f \in S\},$$

é chamado uma variedade algébrica afim.

É natural buscar soluções para equações polinomiais em duas variáveis pelo seu aspecto geométrico. Estamos interessados no caso em que $n = 2$ e $S = \{f(x, y)\}$, onde $f(x, y)$ é um polinômio não constante em $\mathbb{K}[x, y]$. Neste caso teremos a seguinte definição:

Definição 1.1.5. *Seja $f(x, y)$ um polinômio não constante em $\mathbb{K}[x, y]$. A curva algébrica plana afim C_f sobre $\mathbb{K}$ determinada por $f(x, y)$ é o conjunto:*

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

Utilizaremos também a notação $C_f : f(x, y) = 0$.

Definimos o grau da curva C_f como sendo o grau do polinômio f, cuja notação é $grau(f)$. Curvas de graus 1, 2 e 3 são chamadas retas, cônicas e cúbicas, respectivamente.

Observação 1.1.6. *Como $\overline{\mathbb{K}}$ é algebricamente fechado e $f(x, y)$ é não constante, então C_f é infinito.*

Observação 1.1.7. *Se $f(x, y) = g(x, y)h(x, y)$ onde $g(x, y)$ e $h(x, y)$ são polinômios não constantes em $\mathbb{K}[x, y]$, então $C_f = C_g \cup C_h$.*

Definição 1.1.8. *Dizemos que a curva C_f é redutível se existem $g(x, y)$ e $h(x, y)$ polinômios não constantes em $\overline{\mathbb{K}}[x, y]$ tais que, $f(x, y) = g(x, y)h(x, y)$. Caso não exista uma decomposição dessa forma, a curva é dita irredutível.*

Daqui em diante denotaremos $f(x, y)$ simplesmente por f.

Lema 1.1.9. *(Lema de Gauss) Seja D um domínio de fatoração única e $\mathbb{K}$ seu corpo de frações. Seja $f \in D[x]$ um polinômio primitivo (i.é. o mdc dos coeficientes de f é igual a 1) e $g \in D[x]$ arbitrário. Então:*

i) f é irredutível em $D[x] \iff f$ é primitivo em $D[x]$ e irredutível em $K[x]$

ii) $f|g$ em $D[x] \iff f|g$ em $K[x]$.

Demonstração. Ver [3], Lema II.3.6, Pág. 54 □

Um dos teoremas centrais da geometria algébrica é o Teorema de Bézout, que nos mostra como calcular o número de interseções de duas curvas algébricas, levando em conta as interseções no infinito e as multiplicidades de interseções. Primeiramente definiremos o que significa as interseções no infinito e a multiplicidade de interseções, em seguida enunciaremos o Teorema de Bézout.

Por exemplo, sabemos que duas retas distintas têm um único ponto de interseção, a não ser que elas sejam paralelas. Neste caso, diremos que elas se encontram no infinito. Então devemos incorporar um ponto no infinito para cada direção do plano afim. Para visualizarmos o modo

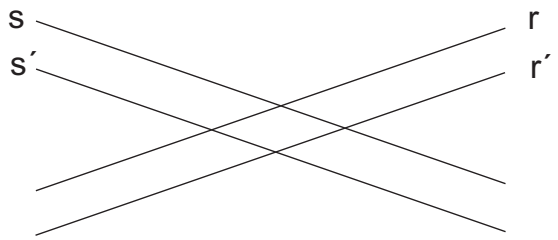

Figura 1.1: Pares de retas paralelas.

que devemos adicionar pontos no plano afim, consideremos r e s duas retas concorrentes e r' e s' retas paralelas a r e s respectivamente.

Se adicionarmos um único ponto no infinito, todo par de retas, concorrentes ou paralelas, se intersectariam nesse ponto. Por exemplo, as retas da figura anterior se intersectariam em dois pontos como na figura abaixo.

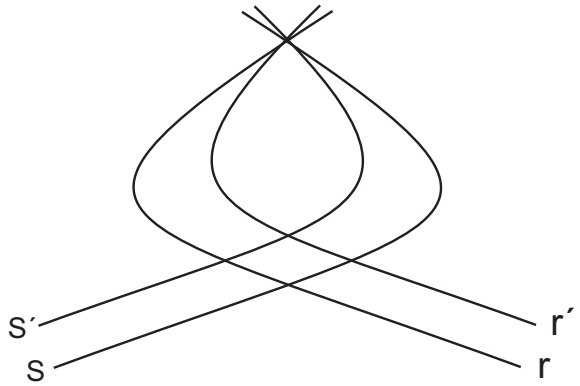

Figura 1.2: Pontos no infinito.

Convém então adicionar um ponto no infinito para cada direção do plano afim, ou equivalentemente, para cada reta contendo a origem.

Dessa forma poderiamos definir o plano projetivo como sendo

$$\mathbb{R}^2 \cup \{\text{Retas do plano que passam pela origem}\}.$$

Se identificarmos $\mathbb{R}^2$ com o plano $z = 1$, em $\mathbb{R}^3$, vemos que para cada ponto do plano $z = 1$, existe uma única reta que passa por esse ponto e a origem.

Isto nos permite definir o plano projetivo como sendo o conjunto de retas de $\mathbb{R}^3$ que passam pela origem.

As retas que se encontram no plano xy, são os "pontos no infinito" e as outras retas se identificam com pontos de $\mathbb{R}^2$.

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

Definição 1.1.10. *Considere a seguinte relação de equivalência entre os pontos de* $\mathbb{K}^3$*:*

$$(x_1, x_2, x_3) \sim (y_1, y_2, y_3) \Leftrightarrow \exists \lambda \in \mathbb{K}^* : \lambda(x_1, x_2, x_3) = (y_1, y_2, y_3).$$

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

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

ou ainda,

$$\mathbb{P}^2(\mathbb{K}) = \left\{\textit{Retas em } \mathbb{K}^3 \textit{ que passam pela origem}\right\}.$$

Notação 1.1.11. *: Se* $(x_1, x_2, x_3) \in \mathbb{K}^3$, $(x_1, x_2, x_3) \neq (0, 0, 0)$, *então, sua classe de equivalência será denotada por* $[x_1 : x_2 : x_3]$ *ou por* $l_{(x_1,x_2,x_3)}$.

Fazendo $\mathbb{K} = \mathbb{R}$ temos:

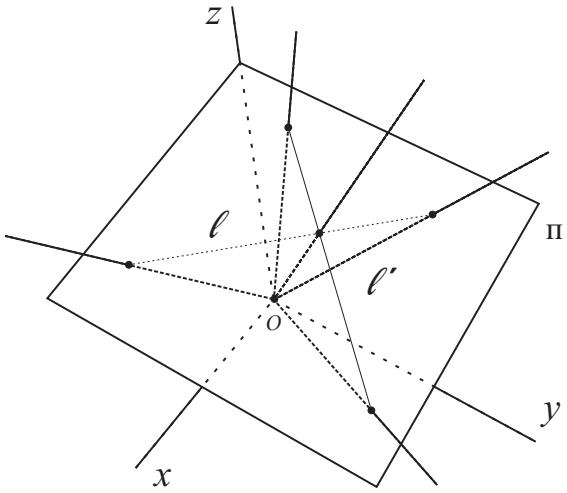

Figura 1.3: Plano Projetivo

Definiremos curvas planas projetivas, destacando o fato de que um ponto no plano projetivo é uma classe de equivalência, logo possui vários representantes. Portanto, para que a definição de curva plana projetiva seja consistente, trabalharemos com uma classe especifica de polinômios.

Definição 1.1.12. *Um polinômio* $f \in \mathbb{K}[x, y, z]$ *é dito homogêneo de grau* $n \geq 1$, *se cada um de seus monômios possui grau (total) n.*

Observemos que, se $f(x, y, z) \in \mathbb{K}[x, y, z]$ é um polinômio homogêneo de grau $n \geq 1$, então $f(\lambda x, \lambda y, \lambda z) = \lambda^n f(x, y, z), \forall \lambda \in \mathbb{K}$. E mais, se f se anula em um ponto (x, y, z), então f se anula em $(\lambda x, \lambda y, \lambda z)$.

Como antes, denotaremos f ao invés de $f(x, y, z)$.

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

Definição 1.1.13. *Seja* f *um polinômio homogêneo não constante em* $\mathbb{K}[x, y, z]$. *A curva algébrica plana projetiva* C_f *sobre* $\mathbb{K}$ *determinada por* f *é o conjunto:*

$$C_f = \{[x : y : z] \in \mathbb{P}^2\left(\overline{\mathbb{K}}\right) : f(x, y, z) = 0\}.$$

Seja $\mathbb{F}$ *uma extensão de* $\mathbb{K}$, *o conjunto de pontos de* C_f *definidos sobre* $\mathbb{F}$ *é*

$$C_f(\mathbb{F}) = \left\{[x : y : z] \in C_f : [x : y : z] \in \mathbb{P}^2(\mathbb{F})\right\}.$$

Definimos o grau de uma curva algébrica plana projetiva como sendo o grau do polinômio que a define. Curvas projetivas de graus 1, 2 e 3 são ditas, respectivamente, retas, cônicas e cúbicas projetivas.

Definição 1.1.14. *Dizemos que uma curva algébrica plana projetiva C_f é não singular, se para todo $P \in C_f$ vale:*

$$\frac{\partial f}{\partial x}(P) \neq 0 \qquad ou \qquad \frac{\partial f}{\partial y}(P) \neq 0 \qquad ou \qquad \frac{\partial f}{\partial z}(P) \neq 0.$$

Os casos mais interessantes ocorrem quando $\mathbb{K} = \mathbb{Q}$ e temos que:

$$C_f(\mathbb{Q}) \subseteq C_f(\mathbb{R}) \subseteq C_f(\mathbb{C}).$$

O interesse aritmético é conhecer $C_f(\mathbb{Q})$. Trataremos dos casos em que o grau do polinômio f é menor ou igual a 3, e nos capítulos seguintes, abordaremos os casos em que o grau de f é exatamente 3.

Seja a função injetora:

$$\mathbb{K}^2 \to \mathbb{P}^2(\mathbb{K})$$

$$(x, y) \mapsto [x : y : 1]$$

que identifica os pontos do plano afim, com os pontos do plano projetivo.

Chame de V_3 a imagem desta função, então $C_f \cap V_3$ pode ser visto como a curva plana afim definida por $f(x, y, 1)$.

Do mesmo modo, uma curva plana afim, dada por $g \in \mathbb{K}[x, y]$, pode ser estendida a uma curva plana projetiva definida pela funçao homogênea $\widetilde{g}(x, y, z) = z^n g(x/z, y/z)$ em que n é o grau do polinômio g.

De formar similar, definimos os planos afins V_1 e V_2 da seguinte forma: Seja a função injetora:

$$\mathbb{K}^2 \to \mathbb{P}^2(\mathbb{K})$$

$$(y, z) \mapsto [1 : y : z]$$

Chame de V_1 a imagem desta função, então $C_f \cap V_1$ pode ser vista como a curva plana afim dada por $f(1, y, z)$. Com respeito a variável y o procedimento é o mesmo. Este processo é chamado de desomogeneização de C_f.

1.2 O Teorema de Bézout

Considere a cônica dada por $C_f : y - x^2 = 0$ e as retas $l_0 : y = 0$, $l_1 : x = 0$, $l_2 : x = y$ e $l_3 : y = x + 1$.

Graficamente, vemos que l_0 intersecta o gráfico da curva C_f apenas na origem, o mesmo ocorrendo com a reta l_1. Já as retas l_2 e l_3 intersectam C_f em dois pontos.

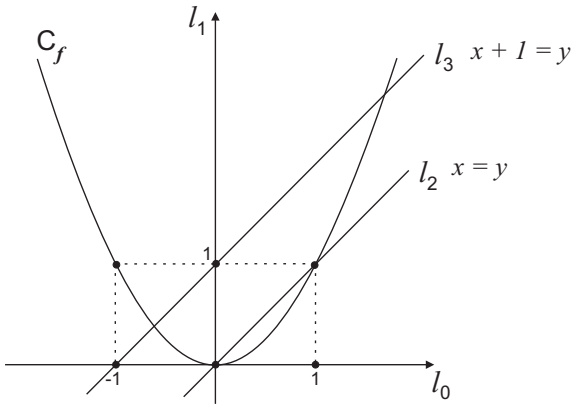

Figura 1.4: Visualizando o Teorema de Bézout

Note que l_0 é tangente a C_f no ponto $(0,0)$, assim, podemos imaginar que o ponto $(0,0)$ conte como se fosse um ponto de intersecção dupla. Isto motiva a idéia de defenir um "índice de intersecção" entre duas curvas.

Já a reta l_1 intersecta C_f em um único ponto. Precisamos introduzir a noção de "pontos no infinito" (trabalhando no plano projetivo), para encontrar um segundo ponto de intersecção.

Assim, a intersecção entre uma reta e uma cônica, no plano projetivo, contém dois pontos.

Intuitivamente, a interseção entre curvas de graus m e n deve conter mn pontos.

O teorema de Bézout mostra que este raciocínio pode ser generalizado, quando computamos de forma correta os pontos de interseção entre curvas planas projetivas. Estas curvas devem satisfazer uma outra hipótese (de não possuirem componentes em comum), derivada da definição 1.2.2.

Proposição 1.2.1. *Um polinômio homogêneo $f \in \mathbb{K}[x,y,z]$ pode ser fatorado como $f = f_1 f_2$, $f_1, f_2 \in \mathbb{K}[x,y,z]$ se, e somente se, cada polinômio f_j, $j = 1,2$, é homogêneo. Logo cada polinômio f_j define uma curva plana projetiva $C_{f_j} : f_j = 0$, $j = 1,2$.*

Demonstração. ($\Leftarrow$) É claro.

($\Rightarrow$) Por absurdo, suponha f_1 não homogêneo.

Seja $grau(f_1) = k$.

Então $f_1 = g_k + g_{k-1} + \cdots + g_0$, onde g_j é homogêneo de grau j, $j = 0, 1, \ldots, k$.

Seja $l = \min\{j : g_j \neq 0\}$. Por hipótese $l < k$, logo $f_1 = g_k + g_{k-1} + \cdots + g_l$, com $g_l \neq 0, g_k \neq 0$.

Considere agora, $f_2 = h_s + h_{s-1} + \cdots + h_t$, com $h_t \neq 0$, $h_s \neq 0$ e $t \leq s$.

Assim:

$$f = f_1 f_2 = g_k h_s + (g_k h_{s-1} + g_{k-1} h_s) + \ldots + g_l h_l,$$

onde $grau(g_k h_s) = k + s$ e $g_k h_s \neq 0$, pois $\mathbb{K}[x,y,z]$ é um domínio. Temos que, $grau(g_l h_t) = l + t$ e $h_l g_t \neq 0$ pelo mesmo motivo.

Também: $l < k$ e $t \leq s$, então $l + t < k + s$. E isto implica que f não é homogêneo. ABSURDO!

Portanto, f_1 é homogêneo.

□

Definição 1.2.2. *Seja $C_f : f(x, y, z) = 0$ uma curva plana projetiva e $f = f_1 \dots f_n$, a fatoração de f sobre $\overline{\mathbb{K}}$ em polinômios irredutíveis. Cada curva $C_{f_j} : f_j(x, y, z) = 0$, $j = 1, \dots, n$, é dita componente irredutível de C_f.*

Primeiramente, vamos mostrar que a interseção entre duas curvas planas afins é finita se os polinômios que as definem não possuem componente comum não constante.

Proposição 1.2.3. *Sejam f e g polinômios sem componentes comuns em $\mathbb{K}[x, y]$. Então a interseção entre as curvas planas afins $C_f : f(x, y) = 0$ e $C_g : g(x, y) = 0$ é finita.*

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

$$r(x)f + s(x)g = 1.$$

Isto implica, em particular, que f e g não possuem componentes em comum sobre $\overline{\mathbb{K}}$. Escrevendo $r(x) = \frac{r_1(x)}{r_2(x)}$, $s(x) = \frac{s_1(x)}{s_2(x)}$ onde $r_1, r_2, s_1, s_2 \in \mathbb{K}[x]$, obtemos:

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

Seja $P = (x_0, y_0) \in C_f \cap C_g$. Logo, $f(x_0, y_0) = g(x_0, y_0) = 0$, ou seja $r_2(x_0)\, s_2(x_0) = 0$.

Assim, vemos que existe um número finito de valores para x_0 limitado pelo número de raízes de $r_2(x)s_2(x) = 0$.

Para cada x_0 fixado, existe um número finito de valores para y_0 tais que $f(x_0, y_0) = 0$, a menos que $(x - x_0)$ seja fator comum de f. Mas nesse caso, f não é fator comum de g. Assim, em todos os casos, para x_0 fixado, existe um número finito de valores de y_0 tais que f e g se anulam ao mesmo tempo, como queriamos demonstrar.

□

Este resultado pode ser estendido para curvas planas projetivas.

Se $f(x, y, z)$ e $g(x, y, z)$ são polinômios homogêneos em $\mathbb{K}[x, y, z]$, sem componentes em comum, então a interseção entre as curvas planas projetivas, definidas por estes polinômios, pode ser escrita como

$$\left\{[x : y : 1] \in \mathbb{P}^2(\mathbb{K}); f(x, y, 1) = g(x, y, 1) = 0\right\} \cup \left\{[x : y : 0] \in \mathbb{P}^2(\mathbb{K}); f(x, y, 0) = g(x, y, 0)\right\}.$$

Estes dois conjuntos são finitos pela proposição 1.2.3, pois os polinômios considerados se encontram em $\mathbb{K}[x, y]$.

Sejam $C_f : f(x, y, z) = 0$ e $C_g : g(x, y, z) = 0$ 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 C_f e C_g em um ponto fixo P.

Definição 1.2.4. *Sejam* $P = (a, b) \in \overline{\mathbb{K}}^2$ *e*

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

Definimos a aplicação $F(\mathbb{K}) \to \mathbb{N}$ *tal que o par* (C_f, C_g) *é enviado em um número* $(C_g, C_f)_P$ *satisfazendo as seguintes propriedades:*

1) $(C_f, C_g)_P = 1$, *se* $f(x, y) = x - a$ *e* $g(x, y) = y - b$;

2) $(C_f, C_g)_P$=$(C_g, C_f)_P$, *para todo* $(C_f, C_g) \in F(\mathbb{K})$;

3) $(C_f, C_{gh})_P = (C_f, C_g)_P + (C_f, C_h)_P$, *para todos* $(C_f, C_g), (C_f, C_h) \in F(\mathbb{K})$;

4) $(C_f, C_{g+fh})_P = (C_f, C_g)_P$, *para todos* (C_f, C_g) *e* (C_f, C_h) *em* $F(\mathbb{K})$;

5) $(C_f, C_g)_P = 0$, *se* $P \notin C_g$ *e* $(C_f, C_g) \in F(\mathbb{K})$.

Proposição 1.2.5. *A aplicação definida anteriormente existe e é única.*

Demonstração. Ver [2], proposição 1.8, pág 8-9. □

Observação 1.2.6. *O número* $(C_f, C_g)_P$ *é chamado de índice de intersecção das curvas* C_f *e* C_g

Exemplo 1.2.7. *Considere* $f(x, y) = x$ *e* $g(x, y) = y^2 - x^3 + x$. *A multiplicidade de interseção entre estas curvas no ponto* $P = (0, 0)$ *é dada por:*

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

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

Sejam C_f e C_g curvas projetivas e P um ponto que se encontra em V_3 (por exemplo). Sejam as curvas planas afins $C_{\overline{f}}$ e $C_{\overline{g}}$ 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 $P = [x : y : 1] \in C_f \cap C_g$, então $\overline{P} = (x, y) \in C_{\overline{f}} \cap C_{\overline{g}}$.

A interseção no plano projetivo está definida pela interseção no plano afim da seguinte forma:

$$(C_f, C_g)_P := (C_{\overline{f}}, C_{\overline{g}})_{\overline{P}}\,,$$

onde a interseção da direita está definida pela proposição 1.2.4 Construções similares podem ser feitas nos planos afins V_1 e V_2.

Finalmente, podemos enunciar o:

Teorema 1.2.8 (Teorema de Bézout)**.** *Sejam*

$$C_f : f(x, y, z) = 0,\ C_g : g(x, y, z) = 0$$

duas curvas planas projetivas sem componentes comuns de graus m *e* n *respectivamente. Então:*

$$\sum_{P \in C_f \cap C_g} (C_f, C_g)_P = mn.$$

Demonstração. Ver [1] Apêndice A, seção 4. □

1.3 Curvas Elípticas

Nesta seção (e nas próximas seções), $\mathbb{K}$ denota um corpo de característica diferente de 2 e 3.

Definição 1.3.1. *Uma curva elíptica E sobre $\mathbb{K}$ é uma curva plana projetiva não singular definida sobre $\mathbb{K}$ de grau 3, juntamente com um ponto racional $\mathcal{O} \in E$.*

Definição 1.3.2. *Um ponto P sobre uma curva elíptica E é dito ponto de inflexão, se a multiplicidade de interseção da reta tangente com a curva E no ponto P é ≥ 3.*

A proposição a seguir, mostra formas equivalentes de definir uma curva elíptica.

Proposição 1.3.3. *As seguintes definições de curvas elípticas são equivalentes:*

a) O mesmo que a definição 1.3.1, que $\mathcal{O}$ é um ponto de inflexão.

b) Uma curva plana projetiva não singular E sobre $\mathbb{K}$ da forma :

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_5z^3$$

cujos coeficientes estão em $\mathbb{K}$.

Demonstração. Ver [2], págs 45-46. □

Pelo teorema de Bézout, duas curvas cúbicas projetivas se intersectam em 9 pontos, contando as multiplicidades.

Um teorema muito importante da geometria algébrica, a qual daremos a prova (de um caso específico) nesta dissertação é o teorema de Mordell (Teorema 3.6.4) que diz que o grupo dos pontos racionais sobre uma curva elíptica é um grupo finitamente gerado.

Para demonstrar o Teorema de Mordell precisamos definir uma lei de grupo sobre o conjunto de pontos de uma curva elíptica. Para tal, definimos uma operação, que notaremos $*$, para encontrar um ponto a partir de dois outros. Esta operação será definida de forma geométrica.

Dados dois pontos P e Q na curva elíptica, considere a reta que passa por estes dois pontos. Por Bézout, esta reta intersecta a curva em um terceiro ponto que denotaremos $P * Q$.

Esta operação ainda não é uma lei de grupo, pois não possui elemento neutro, por exemplo.

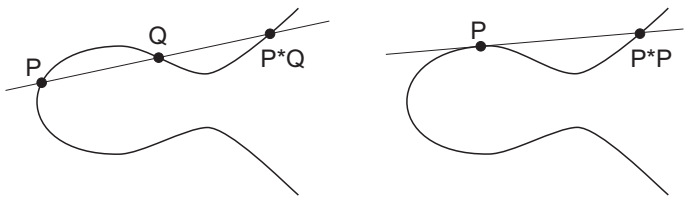

Figura 1.5: Composição de pontos em uma cúbica

No entanto podemos definir uma lei de grupo, com a seguinte regra: "Tome a reta que passa por P e Q, sendo $P * Q$ o terceiro ponto de interseção com a cúbica. A reta que passa por $\mathcal{O}$ e

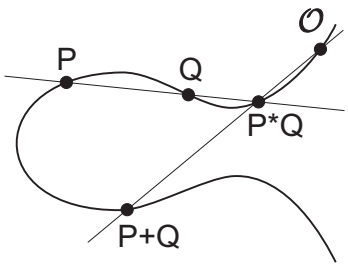

Figura 1.6: Lei de Grupo em uma cúbica.

por $P * Q$ intersecta a cúbica em um novo ponto, o qual será denotado por $P + Q$. Assim, por definição, $P + Q = \mathcal{O} * (P * Q)$"

Teorema 1.3.4. *Seja E uma curva elíptica sobre um corpo $\mathbb{K}$ com um ponto $\mathcal{O} \in E(\mathbb{K})$. Então $E(\mathbb{K})$ é um grupo abeliano com a lei $+$ definida acima.*

Demonstração. Esta operação é claramente comutativa, pois a reta que passa por P e Q é a mesma que passa por Q e P. Provemos que $P + \mathcal{O} = P$. Seja l a reta que pasa por P e $\mathcal{O}$. Por Bézout, existe um terceiro ponto $P * \mathcal{O}$ na interseção $E \cap l$. Note 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, daí, $P + \mathcal{O} = P$, ou seja, $\mathcal{O}$ é o elemento neutro da lei de grupo.

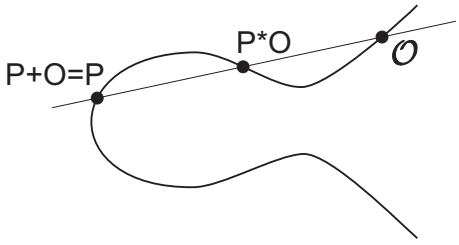

Figura 1.7: Verificação de que $\mathcal{O}$ é o elemento neutro.

Agora, 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 $E \cap l$ (observe que se $\mathcal{O}$ satisfaz (b) da proposição 1.3.5, então $S = \mathcal{O}$).

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

Por fim, mostremos que $+$ é associativa. Sejam P,Q e R três pontos sobre a curva E. Provar que $(P + Q) * R = P * (Q + R)$ é suficiente para provar que $(P + Q) + R = P + (Q + R)$.

Sejam l_1 a reta que passa por P e Q e $P * Q$, r_1 a reta que passa por $\mathcal{O}$, $P * Q$ e $P + Q$.

Sejam l_2 a reta que passa por $P + Q$, R e $(P + Q) * R$, r_2 a reta que passa por Q, R e $Q * R$.

Sejam l_3 a reta que passa por $\mathcal{O}$, $Q * R$ e $Q + R$, r_3 a reta que passa por P,$Q + R$ e $P * (Q + R)$.

Na figura 1.9 as retas r_1, r_2 e r_3 estão desenhadas por um traço continuo, e a retas l_1, l_2 e l_3 por um traçoo pontilhado.

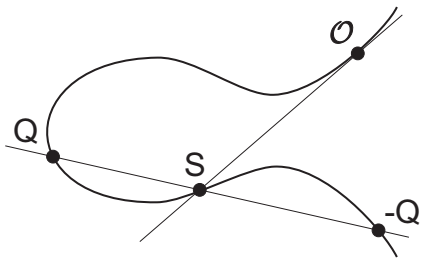

Figura 1.8: Inverso $-Q$ de um ponto Q

Considere também as cúbicas E_l definida pela união de l_1, l_2 e l_3 e E_r definida pela união de r_1, r_2 e r_3. Note que E e E_l se intersectam nos pontos P, Q, $P * Q$, R, $(P + Q) * R$, $\mathcal{O}$, $Q * R$ e $Q + R$. Note também que E e E_r se intersectam nos pontos $\mathcal{O}$, $P * Q$, $P + Q$, Q, R, $Q * R$, $Q + R$, P e $P * (Q + R)$. Assim, $E \cap E_l$ e $E \cap E_r$ possuem oito pontos em comum. Logo, pela proposição 1.3.5 a seguir, o nono ponto de interseção deve ser o mesmo. Isto é $(P + Q) * R = P * (Q + R)$.

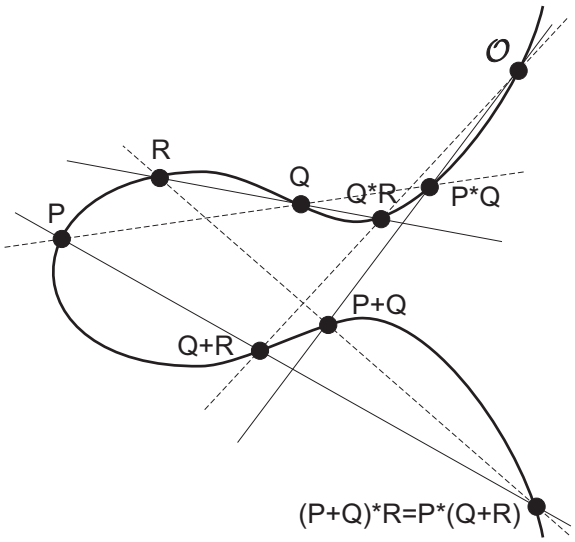

Figura 1.9: Verificando que a lei é associativa

□

Proposição 1.3.5. *Se duas curvas cúbicas em $\mathbb{P}^2(\mathbb{K})$ se intersectam em exatamente nove pontos, então toda curva cúbica que passa por oito desses pontos, também passará pelo nono ponto.*

Demonstração. Sejam C_f e C_g duas cúbicas. Pelo Teorema de Bézout, elas se intercectam em nove pontos.

Sejam eles $P_1, \ldots, P_9$ e seja h uma cúbica que passa pelos oito pontos $P_1, \ldots, P_8$. Queremos provar que $P_9 \in h$. Uma cúbica da forma: $f(x, y, z) = a_1x^3 + a_2x^2y + \cdots + a_{10}z^3$ tem 10 coeficientes $a_1, \ldots, a_{10}$.

A condição: C_f passa por um ponto $P = (x : y : z)$ é uma condição linear em $a_1, \ldots, a_{10}$, dada por $a_1x^3 + a_2x^2y + \cdots + a_{10}z^3 = 0$.

Os oito pontos

$$P_1 = (x_1 : y_1 : z_1), \ldots, P_8 = (x_8 : y_8 : z_8),$$

estão em "posição geral"se os vetores $(x_i^3, x_i^3 y_i, \ldots, z_i^3)$, $i = 1, \ldots, 8$, são linearmente independentes.

Considere

$$\Omega = \{ \text{ cúbicas que passam por } P_1, \ldots, P_8 \}.$$

Então $\dim \Omega = 2$ como espaço vetorial sobre $\mathbb{K}$.

Se $C_f \neq C_g$, então f e g são L.I e $\Omega = \langle f, g \rangle$. Então $h = \lambda f + \mu g$ com $\lambda, \mu \in \mathbb{K}$.

Como $f(P_9) = 0$ e $g(P_9) = 0$, então $h(P_9) = 0$. Quando os $P_i's$ não estão em posição geral, a prova completa é dada pelo estudo caso a caso (ver [8], III, 6.2.)

□

1.4 A Forma Normal de Weirstrass de uma Curva Elíptica

Provaremos o teorema de Mordell, utilizando fórmulas explícitas para a lei de grupo. Para tornar essas fórmulas tão simples quanto possível, é importante saber que, qualquer cúbica com um ponto racional pode ser transformada em uma nova forma especial, dita Forma Normal de Weierstrass. Não daremos uma prova completa disto, mas sim uma indicação da prova. Além disso, elaboraremos um exemplo específico para ilustrar a teoria geral. Em seguida, iremos restringir nossa atenção para cúbicas dadas sob a forma Normal de Weierstrass, o que classicamente consiste em uma equação do tipo: $y^2 = 4x^3 - b_2 x - b_3$.

Utilizaremos uma equação um pouco mais geral, que chamaremos forma de Weierstrass.

Seja E uma curva elíptica sobre $\mathbb{K}$, dada por;

$$E : y^2 z + a_1 xyz + a_2 yz^2 = x^3 + a_2 x^2 z + a_4 xz^2 + a_6 z^3.$$

Fazendo uma substituição de variáveis, em que $x = x^{'}$,$y = y^{'} - \frac{a_3}{2}x$ e $z = z^{'}$, eliminamos o termo xyz da 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:

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

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

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

que será a equação de Weierstrass usada neste trabalho.

Teorema 1.4.1. *Seja $\mathbb{K}$ um corpo de característica diferente de 2 e 3. Cada curva elíptica E é isomorfa a uma curva da forma:*

$$E(a, b, c) : y^2 z = x^3 + ax^2 z + bxz^2 + cz^3.$$

Demonstração. As contas feitas acima provam o teorema. □

1.5 Fórmulas Explícitas para a Lei de Grupo

No teorema 1.3.1, dados P e Q pertencentes a $E(\mathbb{K})$, nós temos um processo geométrico para determinar as coordenadas do ponto $P+Q$. Não seria então possível provar esta associatividade diretamente, estudando as coordenadas dos pontos $P+Q$ em função das coordenadas de P e Q? Sim! isto é possível.

Considere E 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 interseção $E \cap z = 0$. Assim ,este ponto é de inflexão da cúbica.

Desse modo, 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 E 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 1.11 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.

Vamos então determinar as coordenadas de $P_1 + P_2$, a partir das coordenadas de P_1 e P_2 pertencentes a $E(\mathbb{K})$.

Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ pontos na cúbica E e seja $P_1 * P_2 = (x_3, y_3)$.

Então $P_1 + P_2 = (x_3, -y_3)$.

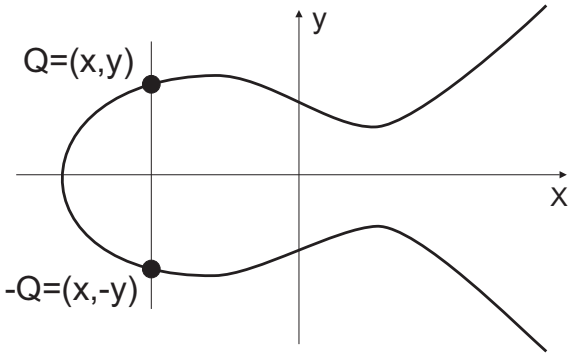

Figura 1.10: O inverso de um ponto na cúbica de Weierstrass.

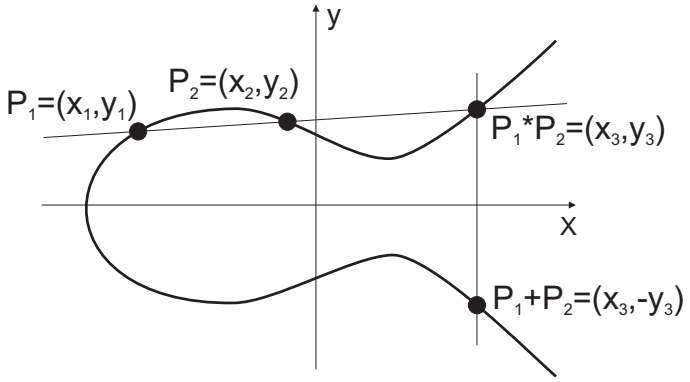

Figura 1.11: Lei da adição na cúbica de Weirstrass.

Assumiremos que $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ são dados e calcularemos (x_3, y_3). Observe que a equação da reta que passa por P_1 e P_2 tem como equação, $y = \lambda x + \upsilon$, onde $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ e $\upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Pelo teorema de Bézout, esta reta corta a cúbica nos pontos P_1, P_2 e $P_1 * P_2$. Para obtermos este terceiro ponto de interseção basta substituir a equação da reta na cúbica:

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

Daí,

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

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

Assim, obtemos uma cúbica em x, cujas raízes são as abscissas x_1, x_2 e x_3 dos pontos P_1, P_2 e $P_1 * P_2$, respectivamente.

Logo:

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

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

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

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

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

Portanto:

$$x_3 = \lambda^2 - a - x_1 - x_2 \quad \text{e} \quad y_3 = \lambda x_3 + \upsilon,$$

que são as fórmulas para o cálculo de $P_1 + P_2 = (x_3, -y_3)$.

Vejamos um exemplo.

Exemplo 1.5.1. *Seja a curva elíptica $y^2 = x^3 + 17$ e os pontos $P_1 = (-1, 4)$ e $P_2 = (2, 5)$ pertencentes a curva.*

Calcularemos $P_1 + P_2$ utilizando as fórmulas anteriores.

Como,

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

e

$$\upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2 = \frac{13}{3},$$

então

$$y = \frac{1}{3}x + \frac{13}{3}.$$

Então,

$$x_3 = \lambda^2 - a - x_1 - x_2 = \left(\frac{1}{3}\right)^2 - 0 - (-1) - (2) = -\frac{8}{9}$$

e

$$y_3 = \lambda x_3 + \upsilon = \frac{1}{3}\left(-\frac{8}{9}\right) + \frac{13}{3} = \frac{109}{27}.$$

Portanto,

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

As fórmulas utilizadas para o cálculo de $P_1 + P_2$ envolvem a inclinação da reta que passa pelos pontos P_1 e P_2, a saber λ. E o caso em que os dois pontos coincidem? Neste caso, suponhamos que temos $P_0 = (x_0, y_0)$ e encontraremos $P_0 + P_0 = 2P_0$. Precisamos encontrar a reta tangente à curva passando por P_0. Como as coordenadas x e y são iguais, não podemos utilizar a mesma formula para λ. Sendo assim, a partir da relação $y^2 = f(x)$ encontramos por derivação que:

$$\lambda = \frac{dy}{dx} = \frac{f^{'}(x_0)}{2y_0},$$

que é a fórmula de λ quando queremos duplicar um ponto. É conveniente ter uma expressão explicita para $2P$ em termos das coordenadas de $P = (x, y)$.

Para isso, substituiremos $\lambda = \frac{dy}{dx} = \frac{f^{'}(x)}{2y}$ nas fórmulas anteriores, ou seja:

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

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

$$x_3 = \left(\frac{f^{'}(x)}{2y}\right)^2 - a - 2x$$

$$x_3 = \left(\frac{(3x^2 + 2ax + b)^2}{4y^2}\right) - a - 2x$$

$$x_3 = \frac{(9x^4 + 12ax^3 + 6bx^2 + 4abx + b^2) + (-8x^4 - 12ax^3 - 4a^2x^2 - 8bx^2 - 4abx - 4cx - 4ac)}{4x^3 + 4ax^2 + 4bx + 4c}$$

$$x_3 = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}.$$

Esta é a fórmula para encontrar a abscissa x de $2P$.

Note que $y_3 = \frac{f^{'}(x)}{2y}x_3 + \upsilon$, é a fórmula para encontrar a coordenada y de $2P$.

Muitas vezes estas fórmulas são chamadas de fórmulas de duplicação do ponto. Estas são as fórmulas básicas aplicáveis a adição de pontos sobre uma cúbica, quando a mesma, está na forma normal 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

Nos próximos capítulos estudaremos curvas elípticas definidas sobre o corpos dos racionais. Dizemos que um elemento P de um grupo tem ordem m se

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

mas $nP \neq O$, para todo inteiro $1 \leq n < m$. Caso m exista, então P tem ordem finita, se não, P é de ordem infinita. Neste capítulo faremos um estudo sobre os pontos de ordem finita de $E(\mathbb{Q})$. A curva elíptica E será dada por:

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

com $a, b, c \in \mathbb{Z}$ e $\Delta = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 \neq 0$. O o modelo afim desta curva é:

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

Denotaremos por $E(\mathbb{Q})_{tors}$ o subgrupo de torção de $E(\mathbb{Q})$, ou seja, o grupo dos pontos racionais de ordem finita e $E[m](\mathbb{Q})$ o subgrupo de $E(\mathbb{Q})$,de pontos P tais que $mP = \mathcal{O}$.

Observe que:

$$E(\mathbb{Q})_{tors} = \bigcup\nolimits_{m\geq 1} E[m](\mathbb{Q}).$$

Se $P = (x, y)$ então suas coordenadas afins são denotadas por $x(P)$ e $y(P)$.

2.1 Pontos de Ordem 2 e de Ordem 3

Proposição 2.1.1. *Seja E uma curva cúbica não singular, definida por:*

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

Então:

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

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

Demonstração. a) Por definição um ponto $P = (x, y)$ em E de ordem 2 é tal que

$$2P = \mathcal{O} \Leftrightarrow P + P = \mathcal{O} \Leftrightarrow P + \mathcal{O} = -P \Leftrightarrow P = -P \Leftrightarrow (x, y) = (x, -y) \Leftrightarrow y = 0,$$

como queríamos.

b) Primeiro procuraremos quantos pontos de ordem 2 a curva E possui. Do item a) temos que se $P = (x, y) \neq \mathcal{O} \in E$ tem ordem 2, então $y = 0$, isso implica que $x^3+ax^2+bx+c = 0$. Assim esta equação tem três raizes em $\overline{\mathbb{Q}}$. Como f é não singular, estas três raizes são distintas. Logo existem três pontos de ordem 2. Desse modo $E[2](\mathbb{Q}) = \{\mathcal{O}, P_1, P_2, P_3\}$ no qual cada P_i é diferente de $\mathcal{O}$. Como $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ é o único grupo a quatro elementos que não possui elementos de ordem 4 (isto segue da teoria dos grupos), então

$$E[2] \cong \{\mathcal{O}, P_1, P_2, P_3\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} .$$

□

Proposição 2.1.2. *Seja E uma curva cúbica não singular, definida por:*

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

Então:

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

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

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

Demonstração. a) Seja $P = (x, y) \neq \mathcal{O}$ em E, então:

$$3P = \mathcal{O} \Leftrightarrow 2P = -P \Leftrightarrow x(2P) = x(-P) = x(P) \tag{2.1}$$

pela fórmula de duplicação de um ponto, temos que:

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

que é equivalente a,

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

Reciprocamente, se x é raiz do polinômio

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

temos que,

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

ou seja, $x(2P) = x(P) = x(-P)$. Portanto por (2.1), segue que P tem ordem três.

b) Seja $P = (x, y)$ um ponto de ordem 3. Pelo item (a), temos que $\psi(x) = 0$.

Através de cálculos simples, observa-se que:

$$\psi'(x) = 12f(x)$$

e

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

Então, ψ tem raíz múltipla se, e somente se, $12f(x) = 0$ e $2f(x)f''(x) - f'(x)^2 = 0$. Isso implica que, $f(x) = f'(x) = 0$, o que é impossível. Assim, ψ possui quatro raízes distintas.

Sejam β_1, β_2, β_3 e β_4 tais raízes, então para cada valor de x temos dois valores para y em nossa cúbica.

Para cada raiz de x, existem dois pontos sobre a cúbica E. Logo, a curva E tem exatamente 8 pontos de ordem três.

Desse modo, $E[3] = \{\mathcal{O}, P_1, P_2, \ldots P_8\}$ onde cada P_i é diferente de $\mathcal{O}$.

Como $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ é o único grupo (abeliano), a menos de isormorfismo, com nove elementos tais que cada elemento tem ordem 3, então

$$E[3] \cong \{\mathcal{O}, P_1, P_2, \ldots P_8\} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

□

2.2 Teorema de Nagell-Lutz e o Teorema de Mazur

Teorema 2.2.1 (Teorema de Nagell-Lutz). *Sejam $a, b, c \in \mathbb{Z}$ e seja E 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 neste caso P é de ordem 2) ou y^2 divide Δ.

Demonstração. Ver Proposições 2.2.2 e 2.2.4. □

O teorema nos fornece um algorítmo para encontrar todos os pontos racionais de torção sobre uma curva elíptica E, 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 $P = [x : y : 1] \in E(\mathbb{Q})$ é um ponto de torção.

A recíproca do teorema não é válida: um ponto $P = [x : y : 1] \in E(\mathbb{Q})$ 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 $P \in E(\mathbb{Q})$ é de ordem finita. Mostraremos um exemplo desta aplicação, no último cápitulo. O teorema de Nagell-Lutz segue dos dois próximos resultados:

Proposição 2.2.2. *Seja $P = [x_1 : y_1 : 1] \in E(\mathbb{Q})$. 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 $E(\mathbb{Q})$, com coordenadas inteiras; suponha ainda $y_1 \neq 0$.

Pela fórmula de duplicação, temos:

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

Façamos,

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

Assim,

$$x_2 = \frac{g(x_1)}{4f(x_1)} \in \mathbb{Z}.$$

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 2.2.3. *Os polinômios*

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

foram obtidos utilizando o sistema de álgebra computacional Máxima.

Proposição 2.2.4. *Se $P = [x : y : 1] \in E(\mathbb{Q})_{tors}$, então $x, y \in \mathbb{Z}$.*

Demonstração. Ver [1], Capítulo II, Seção 4. □

Teorema 2.2.5 (Teorema de Mazur)**.** *Seja E uma curva elíptica, definida sobre os racionais, e suponha que $E(\mathbb{Q})$ 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 $E(\mathbb{Q})$ formam um grupo isomorfo a um dos grupos seguintes

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

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

Demonstração. Ver [6] e [7]. □

CAPÍTULO 3

O TEOREMA DE MORDELL

O objetivo principal deste capítulo é a demonstração do Teorema de Mordell, o qual afirma que o grupo de pontos racionais de uma curva elíptica é finitamente gerado. Este teorema foi conjecturado primeiramente por Poincaré em 1901 e demonstrado em 1922 por Louis Mordell.

3.1 Altura de um Ponto

Definição 3.1.1. *Seja um número racional* $x = \frac{m}{n}$, $mdc(m,n) = 1$. *Definimos a altura* $H(x)$ *como sendo o máximo valor absoluto do numerador e do denominador, ou seja:*

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

A altura de um ponto racional mede o quanto o ponto é complexo do ponto de vista da Teoria dos Números; esta altura 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 $\frac{999}{1000}$. Ambos tem aproximadamente o mesmo valor absoluto, mas o segundo é mais "complicado" que o primeiro, pelo menos do ponto de vista da Teoria dos Números. Se esta razão não for convincente, então possivelmente a seguinte propriedade de altura, explicará por que é uma noção tão útil.

3.2 Propriedades da Altura

Proposição 3.2.1. *Seja* M *um número real positivo. O Conjunto,*

$$\left\{x = \frac{m}{n} \in \mathbb{Q} : H(x) \leq M\right\}$$

é finito.

Demonstração. Se a altura de $x = \frac{m}{n}$ é menor que alguma constante fixada, então $|m|$ e $|n|$ são menores que esta constante, por isso há somente um número finito de possibilidades para m e n. □

Se

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

é uma curva cúbica não singular com coeficientes inteiros a, b, c e se $P = (x, y)$ é um ponto racional na curva, definimos a altura de P sendo simplesmente a altura da abscissa x, isto é, $H(P) = H(x)$.

Veremos que a altura se comporta como se fosse uma função multiplicativa. Por exemplo, compararemos $H(P + Q)$ com o produto $H(P)H(Q)$.

Por razão de notação, é mais conveniente ter uma função que possui um comportamento aditivo, então definimos a função h como altura tomando o logaritmo de H, ou seja,

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

Assim, $h(P)$ é sempre um numero real não negativo, pois

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

A altura para o ponto no infinito é definida por: $H(\mathcal{O}) = 1$ ou, equivalentemente, $h(\mathcal{O}) = 0$.

Nosso objetivo neste capítulo, é provar que o grupo dos pontos racionais $E(\mathbb{Q})$ é finitamente gerado; tal fato seguirá dos lemas 3.2.2, 3.2.3, 3.2.4 e 3.2.6, os quais vamos enunciar, demonstrar e utilizar para demonstrar o Teorema de Mordell.

Lema 3.2.2. *Para todo número real positivo M, o conjunto $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ é finito.*

Demonstração. Considere $P \in E(\mathbb{Q})$ tal que $h(P) \leq M$. Se $P \neq \mathcal{O}$, então $P = (x, y)$, onde (x, y) satisfaz a equação $y^2 = x^3 + ax^2 + bx + c$.

Por definição temos que $h(P) = h(x) = \log H(x) \leq M$, isto é, $1 \leq H(x) \leq e^M$.

Pela proposição 3.2.1, existem no máximo $k(2k + 1)$ valores possíveis para x, onde k é a parte inteira de e^M.

Como para cada valor de x, existem no máximo dois valores possíveis para y, então o conjunto $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ é finito.

□

Lema 3.2.3. *Seja P_0 um ponto racional em*

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

fixado. Existe uma constante k_0, dependendo de P_0 e de a,b,c tal que:

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

Demonstração. Ver seção 3.3. □

Lema 3.2.4. *Existe uma constante k, dependendo de a,b,c tal que:*

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

Demonstração. Ver seção 3.4. □

Observação 3.2.5. *Os lemas 3.2.3 e 3.2.4 relacionam a lei de grupo em E, que é definida geometricamente, com a altura dos pontos que é uma ferramenta da Teoria dos Números.*

Assim, de certa forma pode-se pensar na altura, como uma ferramenta para traduzir informações geométricas em informações aritméticas.

Lema 3.2.6. *O índice* $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ *é finito.*

Demonstração. Ver seção 3.6. □

Usamos a notação $2E(\mathbb{Q})$ para denotar o subgrupo de $E(\mathbb{Q})$ que consiste dos pontos que são o dobro dos pontos de $E(\mathbb{Q})$. Para qualquer grupo abeliano G, a multiplicação por m:

$$G \xrightarrow{m} G, \;\; P \mapsto \underbrace{P + \cdots + P}_{m\ termos} = mP,$$

é um homomorfismo, e a imagem deste homomorfismo é o subgrupo mG de G. O lema 3.2.6 afirma que, para $G = E(\mathbb{Q})$, o subgrupo $2G$ tem índice finito em G.

Esses lemas estão em ordem crescente de dificuldade. O lema 3.2.2 já foi provado. Os lemas 3.2.3 e 3.2.4 estão relacionados à teoria das alturas e números racionais.

Já o lema 3.2.6 é mais sutil, e como queremos nos restringir ao trabalho com números racionais, provaremos o lema apenas para uma classe de curvas cúbicas. Provaremos o teorema de Mordell para curvas elípticas da forma $y^2 = f(x) = x^3 + ax^2 + bx + c$ que possuem pelo menos um ponto de ordem 2, isto é, $f(x)$ deve ter pelo menos 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 $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado. Podemos esquecer completamente os pontos racionais de uma curva e supor somente que temos um grupo comutativo G, escrito aditivamente, e a função altura $h : G \to [0, \infty]$. Suponha também que G e h satisfazem os quatro lemas. Apresentaremos agora de novo nossas hipóteses e provaremos que G precisa ser finitamente gerado.

Teorema 3.2.7. *Seja G um grupo comutativo. Suponha que existe uma função* $h : G \to [0, \infty]$ *com as três propriedades abaixo:*

1) Para cada número real positivo M, o conjunto $\{P \in G : h(P) \leq M\}$ *é finito.*

2) Para cada $P_0 \in G$ *existe uma constante* k_0 *tal que*

$$h(P + P_0) \leq 2h(P) + k_0, \forall\, P \in G.$$

3) Existe uma constante k tal que: $h(2P) \geq 4h(P) - k$, $\forall\, P \in G$.

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

Demonstração. Seja $[G : 2G] = n$ e considere $\{Q_1, \cdots, Q_n\} \subset G$, um conjunto de representantes de $G/2G$.

Seja $P \in G$, $\exists\, i_1$ tal que $P \in 2G + Q_{i_1}$ logo $\exists\, P_1 \in G$ tal que

$$P = 2P_1 + Q_{i_1} \Rightarrow P - Q_{i_1} = 2P_1.$$

Também, $\exists\, i_2$ tal que $P_1 \in 2G + Q_{i_2}$ logo $\exists\, P_2 \in G$ tal que

$$P_1 = 2P_2 + Q_{i_2} \Rightarrow P_1 - Q_{i_2} = 2P_2.$$

Repetindo este processo obtemos uma sequência de pontos $(P_m)_{m\geq 1}$ tais que,

$$\begin{aligned} P &= 2P_1 + Q_{i_1}; \\ P_1 &= 2P_2 + Q_{i_2}; \\ &\vdots \\ P_m &= 2P_{m+1} + Q_{i_{m+1}} \end{aligned} \tag{3.1}$$

onde $Q_{i_1}, \ldots, Q_{i_m}$ são escolhidos no conjunto de representantes das classes laterais $\{Q_1, \ldots, Q_n\}$ e $P, P_1, \ldots$ são elementos de G.

Vemos então que para todo $m \in \mathbb{N}$,

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m. \tag{3.2}$$

Do item 2) temos que, para $-Q_j$ existe k_j tal que, para todo $P \in G$ temos,

$$h\left(P - Q_j\right) \leq 2h(P) + k_j.$$

Comparemos as alturas de P_j e P_{j-1}. De (3.2), temos que

$$P_{j-1} = Q_{i_j} + 2P_j\,.$$

Tome $k' = \max\{k_j\}$. Assim,

$$\forall\ P \in G:\ h(P - Q_j) \leq 2h(P) + k_j \leq 2h(P) + k'\,.$$

Aplicando os itens 2) e 3) em (3.1)

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

$$\Rightarrow 4h\left(P_j\right) - k \leq 2h\left(P_{j-1}\right) + k'$$

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

Como $\frac{1}{2} = \frac{3}{4} - \frac{1}{4}$, então:

$$h\left(P_j\right) \leq \frac{3}{4}h\left(P_{j-1}\right) - \underbrace{\frac{1}{4}h\left(P_{j-1}\right) + \frac{k+k'}{4}}_{-\frac{1}{4}(h(P_{j-1})-(k+k'))}$$

Afirmação: $\exists\, m \in \mathbb{N} : h\left(P_m\right) < k + k'$

Por absurdo suponha:

$$\forall\ m \geq 0 : h\left(P_m\right) \geq k + k',$$

então,

$$h\left(P_{j-1}\right) - k - k' \geq 0,$$

ou seja,

$$-\frac{1}{4}\left(h\left(P_{j-1}\right) - k - k'\right) \leq 0.$$

Daí,

$$h\left(P_j\right) \leq \frac{3}{4}h\left(P_{j-1}\right) \underbrace{-\frac{1}{4}\left(h\left(P_{j-1}\right) - k - k'\right)}_{\leq 0} \leq \frac{3}{4}h\left(P_{j-1}\right) \Rightarrow h\left(P_j\right) \leq \frac{3}{4}h\left(P_{j-1}\right).$$

Assim:

$$h\left(P_1\right) \leq \frac{3}{4}h\left(P\right)$$

e

$$h\left(P_2\right) \leq \frac{3}{4}h\left(P_1\right) \leq \left(\frac{3}{4}\right)^2 h\left(P\right).$$

Por indução:

$$h\left(P_j\right) \leq \left(\tfrac{3}{4}\right)^j h\left(P\right).$$

Como $\lim\limits_{j\to\infty}\left(\frac{3}{4}\right)^j = 0$, então existe $m \geq 0$ tal que $\left(\frac{3}{4}\right)^m < \frac{k+k'}{h(P)}$

Logo, $h\left(P_m\right) \leq \left(\frac{3}{4}\right)^m h\left(P\right) < k + k'$, o que contradiz nossa suposição. Logo,

$$\exists\, m \in \mathbb{N} : h\left(P_m\right) < k + k'.$$

Assim, cada ponto $P \in G$, se escreve como combinação linear de elementos do conjunto

$$\left\{Q_1, \ldots, Q_n\right\} \cup \left\{P \in G : h(P) \leq k + k'\right\}.$$

Pelo item 1) este conjunto é finito. Logo G é finitamente gerado.

□

Este teorema é chamado de Teorema da Descida, haja vista que sua demonstração é feita no estilo do método de Fermat de descida finita. Começamos com um ponto arbitrário, em nosso caso o ponto $P \in E(\mathbb{Q})$, e com algumas manipulações produzimos um ponto de altura menor.

É preciso ter uma forma de mensurar o tamanho do ponto, para isso usamos a altura. Com sorte, a aplicação repetida deste processo leva a uma das conclusõs seguintes. Em nosso caso,

repetimos o processo até achar um ponto que se encontra, em um conjunto finito. Em outros casos, se chega a uma contradição, usualmente a existência e um inteiro estritamente entre zero e um. Então podemos concluir que não existe solução. Este método usado por Fermat, mostra que $x^4 + y^4 = 1$ não tem solução racional com $xy \neq 0$; ele queria utilizar o mesmo raciocínio para provar que $x^n + y^n = 1$ não tem solução para todo $n \geq 3$.

Infelizmente complicações adicionais surgiram quando o n aumenta. Tendo em vista o Teorema da Descida, e a demonstração do lema 3.2.2 acima, resta-nos provar os lemas 3.2.3, 3.2.4 e 3.2.6.

3.3 A Altura de $P + P_0$

Nesta seção será feita a prova do lema 3.2.3, que nos dá uma relação entre a altura de P, P_0 e $P + P_0$. Para isso façamos antes algumas observações.

Primeiramente, se $P = (x, y)$ é um ponto racional em nossa curva, então x e y têm 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 numero cujo cubo é o denominador de y.

Com efeito, 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:

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

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

$$\frac{n^2M^3}{N^2M^3} = \frac{m^3 + am^2M + bmM^2 + cM^3}{M^3}$$

$$\frac{n^2M^3}{N^2M^3} = \frac{m^3N^2 + aN^2m^2M + bN^2mM^2 + cN^2M^3}{N^2M^3}$$

$$n^2M^3 = m^3N^2 + aN^2m^2M + bN^2mM^2 + cN^2M^3. \tag{3.3}$$

Veja que N^2 é um fator comum de todos os termos do lado direito da igualdade (3.3), então $N^2|n^2M^3$.

Como $mdc(n, N) = 1$ então $N^2|M^3$.

Agora mostraremos que $M^3|N^2$.

De fato, pela equação (3.3) vemos que $M|N^2m^3$ e como $mdc(m, M) = 1$, obtemos $M|N^2$. Ou seja,

$$M^2|n^2M^3,\ aN^2m^2M,\ bN^2mM^2,\ cN^2M^3.$$

De (3.3) temos: $N^2m^3 = n^2M^3 - (aN^2m^2M + bN^2mM^2 + cN^2M^3)$, logo $M^2|N^2m^3$.

Como $mdc(m, M) = 1$ temos $M^2|N^2$, ou seja, $M|N$.

Isso implica que

$$M^3|n^2M^3 - (aN^2m^2M + bN^2mM^2 + cN^2M^3).$$

Novamente por (3.3) seque se que $M^3|N^2m^2$ e como $mdc(m, M) = 1$, então $M^3|N^2$.

Conclui-se que $M^3 = N^2$, pois $M, N > 0$.

Como $M|N$, seja $e = \frac{N}{M} \in \mathbb{N}$, então,

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

Portanto

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

com m,n inteiros, $e > 0$ e $mdc(m, e) = mdc(n, e) = 1$.

Nossa segunda observação diz respeito sobre 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, mostremos que há uma constante $K > 0$, dependendo de a,b,c tal que $|n| \leq KH(P)^{3/2}$.

Provaremos isto usando o fato de que o ponto P satisfaz a equação da curva. De fato, substituiremos o ponto na equação e multiplicando por e^6 e excluiremos o denominador:

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

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

$$|n^2| \leq |m^3| + |am^2e^2| + |bme^4m| + |ce^6|$$

$$\leq H(P)^3 + |a|H(P)^3 + |b|(H(P)^3 + |c|H(P)^3)$$

$$= H(P)^3(1 + |a| + |b| + |c|).$$

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

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

Provaremos agora o Lema 3.2.3.

Demonstração. Observe que o lema é trivial se $P_0 = \mathcal{O}$, pois para qualquer $P \in E(\mathbb{Q})$ tem se

$$h(P+P_0) = h(P) \leq 2h(P) < 2h(P) + k_0.$$

para qualquer $k_0 > 0$.

Seja então $P_0 \neq \mathcal{O}$, $P_0 = (x_0, y_0)$.

Observação 3.3.1. *Note que é suficiente provar que a desigualdade vale para todo P exceto para P em algum conjunto finito.*

Isto é verdade pois se P pertence a um conjunto finito, existe somente um número finito de diferenças $h(P+P_0) - 2h(P)$. Isto é, acharemos $k_0' > 0$, tal que $h(P+P_0) < 2h(P) + k_0'$, para $P \neq \pm P_0$, pois considerando $k_0'' = \max\{h(P+P_0) - 2h(P),\ com\ P \in \{\mathcal{O}, \pm P_0\}\}$, teremos então $k_0 = \max\{k_0', k_0''\}$.

Seja então $P \in E(\mathbb{Q})$, $P \notin \{-P_0, \mathcal{O}, P_0\}$.

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

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

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

Da seção 1.5 temos: $\zeta = \lambda^2 - a - x - x_0$, com $\lambda = \frac{y-y_0}{x-x_0}$.

Assim:

$$\zeta = \frac{(y-y_0)}{(x-x_0)} - a - x - x_0$$

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

$$\zeta = \frac{(y^2 - 2yy_0 + {y_0}^2) - (x^2 - 2xx_0 + {x_0}^2)(x+x_0+a)}{(x-x_0)^2}$$

$$\zeta = \frac{(y^2 - 2yy_0 + {y_0}^2) - (x^3 + x^2x_0 + x^2a - 2x^2x_0 - 2x{x_0}^2 - 2axx_0 + {x_0}^2x + {x_0}^3 + a{x_0}^2)}{(x-x_0)^2}.$$

Fazendo $y^2 - x^3 = ax^2 + bx + c$ (pois o ponto P está na curva) temos:

$$\zeta = \frac{ax^2 + bx + c - 2y_0y + {y_0}^2 + x^2x_0 + {x_0}^2x - ax^2 - a{x_0}^2 - {x_0}^3 + 2axx_0}{(x-x_0)^2}$$

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

Podemos escrever a expressão acima da seguinte maneira:

$\zeta = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$ com A,B,C,D,E,F e G números racionais que podem ser expressos em termos de a,b,c,x e x_0.

Mas se multiplicarmos o numerador e o denominador pelo mínimo denominador comum de $A, \ldots, G$ podermos assumir que $A, \ldots, G$ são inteiros.

Em resumo: temos inteiros $A, \ldots, G$ que dependem de a,b,c,x_0 e y_0 de modo que para todo ponto $P = (x, y)$ não pertencente a $\{-P_0, \mathcal{O}, P_0\}$ a coordenada x de $P + P_0$ é igual a $\zeta = \frac{Ay+Bx^2+Cx+D}{Ex^2+Fx+G}$.

É importante ressaltar 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 a constante k depende de $A, \ldots, G$ contanto que não dependa de x e y. Agora substituindo $x = \frac{m}{e^2}$ e $y = \frac{n}{e^3}$ e multiplicando a fração por $\frac{e^4}{e^4}$ encontramos

$$\zeta = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fne^2 + Ge^4}.$$

Logo temos uma expressão para ζ com um inteiro dividido por outro inteiro.

Não conhecemos esta expressão na forma irredutível, mas por cancelamento do fator comum a altura é menor que o máximo entre estes números.

Daí, por um lado temos que

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

Por outro lado, temos as seguintes estimativas:

$|e| \leq H(P)^{1/2}$, $|n| \leq K^{'} H(P)^{3/2}$,$|m| \leq H(P)$ onde $k^{'}$ depende somente de a,b,c. Usando estas desigualdades e a desigualdade triangular temos:

$$\begin{aligned} |Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq \left(|Ak^{'}| + |B| + |C| + |D|\right) H(P)^2 \end{aligned}$$

e

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

Portanto:

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

Aplicando logaritmo em ambos os lados obtemos:

$$h(P + P_0) \leq 2h(P) + k_0^{'},$$

onde a constante

$$k_0'' = \log \max\left\{|Ak^{'}| + |B| + |C| + |D|,\, |E| + |F| + |G|\right\}$$

e $k_0' = \max\{k', k''\}$ depende somente de a,b,c,x_0 e y_0 e independe de $P = (x, y)$.

A observação 3.3.1 completa a demonstração. □

3.4 A Altura de $2P$

Na seção anterior provamos que:

"Se P_0 é um ponto racional em E fixado, existe uma constante k_0, dependendo de P_0 e de a,b e c tal que: $h(P+P_0) \leq 2h(P) + k_0$, $\forall\, P \in E(\mathbb{Q})$".

Nesta seção daremos a prova do Lema 3.2.4, que nos diz:

"Existe uma constante k dependendo de a,b e c tal que $h(2P) \geq 4h(P) - k$ para todo P em $E(\mathbb{Q})$".

Da mesma forma que na prova do Lema 3.2.3, podemos ignorar qualquer conjunto finito de pontos, haja vista que pode-se escolher k maior $4h(P)$ para todos pontos desse conjunto.

Então descartamos o conjunto finito de pontos que satisfazem $2P = \mathcal{O}$.

Seja $P = (x, y)$ e escreva $2P = (\zeta, \eta)$.

A fórmula de duplicação é: $\zeta + 2x = \lambda^2 - a$ onde $\lambda = \frac{f'(x)}{2y}$, logo:

$$\zeta = \frac{f'(x)}{4y^2} - a - 2x.$$

Colocando tudo sobre um denominador comum e usando $y^2 = f(x) = x^3 + ax^2 + bx + c$ obtemos a seguinte expressão para ζ:

$$\zeta = \frac{\left(f'(x)\right)^2 - (8x + 4a)\, f(x)}{4\,(f(x))} = \frac{x^4 \cdots}{4x^3 \cdots}.$$

Note que $f(x) \neq 0$ pois $2P \neq \mathcal{O}$. Assim, ζ é o quociente de dois polinômios em x com coeficientes em $\mathbb{Z}$.

A cúbica $y^2 = f(x)$ é não singular por suposição, portanto, sabemos que $f(x)$ e $f'(x)$ não tem raízes em comum.

Sabendo que $h(P) = h(x)$ e $h(2P) = h(\zeta)$ estamos tentando provar que $h(\zeta) = 4h(x) - k$. O seguinte lema conclui a demonstração.

Lema 3.4.1. *Sejam $\phi(x)$ e $\psi(x)$ polinômios com coeficientes inteiros e raízes não comuns.*

Seja d o máximo dos graus de $\phi(x)$ e $\psi(x)$. Então:

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

2) Existem k_1 e k_2, dependendo de $\phi(x)$ e $\psi(x)$, tal que para todo racional $\frac{m}{n}$ que não são raízes de ψ temos:

$$dh\left(\frac{m}{n}\right) - k_1 \leq h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + k_2.$$

Demonstração. 1) Primeiro observe que $\phi(x)$ e $\psi(x)$ têm grau menor ou igual a d, logo o número $n^d\phi\left(\frac{m}{n}\right)$ é inteiro inteiros pois:

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

$$\phi\left(\frac{m}{n}\right) = a_d\frac{m^d}{n^d} + a_{d-1}\frac{m^{d-1}}{n^{d-1}} + \ldots + a_0.$$

Logo $n^d\phi\left(\frac{m}{n}\right) \in \mathbb{Z}$.

De maneira inteiramente análoga $n^d\psi\left(\frac{m}{n}\right) \in \mathbb{Z}$.

Então faz sentido encontrar maximo divisor comum de $n^d\phi\left(\frac{m}{n}\right)$ e $n^d\psi\left(\frac{m}{n}\right)$.

O resultado que mostraremos é que não há muito a simplificar quando realizamos o quociente destes dois números. O que devemos simplificar está limitado por R.

Sem perda de generalidade suponhamos que $grau\,\phi \geq grau\,\psi$ pois:

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

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

Assim podemos escrever:

$$n^d\phi\left(\frac{m}{n}\right) = n^d\left(a_d\frac{m^d}{n^d} + a_{d-1}\frac{m^{d-1}}{n^{d-1}} + \cdots + a_0\right) = a_d m^d + a_{d-1}m^{d-1}n + \cdots + a_0 n^d$$

e

$$n^d\psi\left(\frac{m}{n}\right) = n^d\left(b_e\frac{m^e}{n^e} + b_{e-1}\frac{m^{e-1}}{n^{e-1}} + \cdots + e_0\right) = b_e m^e n^{d-e} + b_{e-1}m^{e-1}n^{d-e-1} + \cdots + b_0 n^d.$$

Para simplificar a notação faremos:

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

Precisamos achar uma estimativa para $mdc\left(\Phi(m,n), \Psi(m,n)\right)$ que independa de m ou n.

Como $\phi(x)$ e $\psi(x)$ não tem raízes em comum, 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 tais que

$$F(x)\phi(x) + G(x)\psi(x) = 1(*).$$

Seja A um inteiro grande o suficiente tal que $AF(x)$ e $AG(x)$ tenham coeficientes inteiros. Mas seja $D = \max\{grau\,F(x),\, grau\,G(x)\}$.

Note que A e D independem de m ou n. Substituindo $x = \frac{m}{n}$ em $(*)$ e multiplicando ambos os lados por An^{D+d}, temos,

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

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

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

Como os números $n^D AF\left(\frac{m}{n}\right)$ e $n^D AG\left(\frac{m}{n}\right)$ são inteiros então $\gamma | An^{D+d}$.

Isto não é bom o suficiente pois devemos mostrar que γ divide um número fixo que independe de n. Na realidade o que vamos mostrar é que γ divide $Aa_d{}^{D+d}$ onde a_d é o coeficiente dominante de $\phi(x)$.

Provemos isto observando que γ divide $\Phi(m,n)$ e certamente divide $An^{D+d}\Phi(m,n)$.

Como,

$$An^{D+d-1}\Phi(m,n) = An^{D+d-1}n^d\phi\left(\frac{m}{n}\right) = An^{D+d-1}\left(a_d m^d + a_{d-1}m^{d-1}n + \cdots + a_0 n^d\right)$$

$$An^{D+d-1}\Phi(m,n) = a_d An^{D+d-1}m^d + a_{d-1}An^{D+d-1}nm^{d-1} + \cdots + a_0 An^{D+2d-1}. \quad (3.4)$$

Como γ divide o primeiro membro de (3.4) temos que γ também dividirá o segundo membro de (3.4) pois são iguais, assim temos que todos os termos, exceto o primeiro possuem An^{D+d} como fator, e, já provamos que $\gamma \mid An^{D+d}$, então segue que γ dividirá o primeiro termo do segundo membro de (3.4). Logo $\gamma \mid a_d Am^d n^{D+d-1}$.

Agora, como $\gamma \mid An^{D+d}$ e $\gamma \mid a_d Am^d n^{D+d-1}$ então,

$$\gamma \mid mdc\left(An^{D+d}, a_d m^d n^{D+d-1}\right) = An^{D+d-1}mdc\left(n, a_d m^d\right).$$

Temos que $mdc(m,n) = 1$ isso implica que,

$$mdc\left(n, a_d m^d\right) = mdc\left(n, a_d\right) \text{ e } mdc\left(n, a_d\right) \mid a_d, \text{ então } \gamma \mid Aa_d n^{D+d-1}.$$

Por indução podemos conseguimos provar que

$$\gamma \mid Aa_d^2 n^{D+d-2}, \gamma \mid Aa_d^3 n^{D+d-3}, \cdots, \gamma \mid Aa_d^{D+d} n^{D+d-(D+d)} = Aa_d^{D+d}.$$

Façamos isto, ou seja provaremos que,

$$\gamma \mid Aa_d^k n^{D+d-k} \Rightarrow \gamma \mid Aa_d^{k+1} n^{D+d-(k+1)}.$$

Suponha que $\gamma \mid Aa_d^k n^{D+d-k}$. Então,

$$Aa_d^{k+1} n^{D+d-(k+1)}\Phi(m,n) =$$

$$= Aa_d^{k+1} m^d n^{D+d-(k+1)} + Aa_d^k a_{d-1} m^{d-1} n^{D+d-k} + \cdots + Aa_d^k a_0 n^{D+2d-(k+1)}.$$

Daí,

$$\gamma \mid Aa_d^{k+1} m^d n^{D+d-(k+1)} \Rightarrow$$

$$\Rightarrow \gamma \mid mdc\left(Aa_d^{k+1}m^d n^{D+d-(k+1)}, Aa^k{}_d n^{D+d-k}\right) =$$

$$= Aa^k{}_d n^{D+d-(k+1)} mdc\left(m^d, n\right)$$

De $mdc(m,n) = 1$ temos $mdc\left(m^d.n\right) = 1$.

Portanto $\gamma \mid Aa_d^{k+1} n^{D+d-(k+1)}$ como queriamos.

Concluimos por indução que $\gamma \mid Aa_d^{D+d}$, e tomando $R = Aa^{D+d}$ encerramos a demonstração do item 1) do lema.

2) Mostraremos que existem constantes K_1 e K_2, dependendo de $\phi(x)$ e $\psi(x)$ tais que para todo $\frac{m}{n} \in Q$ que são raízes de ψ tem-se:

$$dh\left(\frac{m}{n}\right) - k_1 \leq h\left(\frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)}\right) \leq dh\left(\frac{m}{n}\right) + k_2$$

Como antes, excluiremos um conjunto finito de números racionais.

Assuma que o número racional $\frac{m}{n}$ não é raiz de ϕ. Pela definição de altura, temos que se é um número racional não-nulo então $H(r) = H\left(\frac{1}{r}\right)$. Com efeito, se $r = \frac{a}{b} \in \mathbb{Q}^*$, então $H(r) = h\left(\frac{a}{b}\right) = \max\{|a|, |b|\}$ e $H\left(\frac{1}{r}\right) = h\left(\frac{b}{a}\right) = \max\{|b|, |a|\}$

Novamente, podemos supor sem perda de generalidade que $grau\phi = d$ e $grau\psi = e$, com $e \leq d$. Continuando com a notação utilizada em 1), o número racional cusa altura pretende-se estimar é;

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

Em 1), mostramos que existe um inteiro $R \geq 1$, independente de m e n, de modo que o $mdc\left(\Phi(m,n), \Psi(m,n)\right| R$.Assim, utilizando a desigualdade trivial $\max\{a,b\} \geq \frac{1}{2}(a+b)$ temos que:

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

e

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

logo:

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

Queremos comparar $H(\xi)$ á quantidade $H\left(\frac{m}{n}\right)^d = \max\{|m|^d, |n|^d\}$, dessa forma considere o seguinte quociente:

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

$$= \frac{1}{2R}\frac{|n^d|\left(|\phi\left(\frac{m}{n}\right)| + |\psi\left(\frac{m}{n}\right))|}{\max\{|m|^d, |n|^d\}} = \frac{1}{2R}\frac{\left(|\phi\left(\frac{m}{n}\right)| + |\psi\left(\frac{m}{n}\right)|\right)}{\max\{|\frac{m}{n}|^d, 1\}}. \tag{3.5}$$

Isto sugere que devemos estudar a função $p(t) = \frac{|\phi(t)|+|\psi(t)|}{\max\{|t|,1\}}$.

Vamos analisar tal limite.

Se $|t| \leq 1 \Rightarrow p(t) = |\phi(t)| + |\psi(t)|$.

Como ϕ e ψ são polinômios, então são funções contínuas.

Logo, no intervalo $[-1, 1]$, $p(t)$ possui mínimo.

Seja $t_0 \in [-1, 1]$. Temos que $p(t) \geq p(t_0)$ para todo t em $[-1, 1]$.

Se $p(t_0) = 0$ então $\phi(t_0) = 0$ e $\psi(t_0) = 0$ o que implica que que ϕ e ψ tem raiz comum. Absurdo ! Logo $\phi(t_0) > 0$, o que implica que para $|t| \leq 1$ tem-se $p(t) \geq c_2 > 0$ para algum $c_2 > 0$

Se $|t| > 1$, então

$$p(t) = \frac{|\phi(t) + \psi(t)|}{|t|^d}.$$

Daí,

$$\lim_{t\to+\infty} p(t) = \lim_{t\to+\infty} |a_d + \frac{a_{d-1}}{|t|} + \cdots + \frac{a_0}{|t|^d}| + |b_e + \frac{b_{e-1}}{|t|} + \cdots + \frac{b_0}{|t|^e}|$$

Lembrando que $d \geq e$. Logo, $\lim_{t\to+\infty} p(t) = |a_d| + |b_e| > 0$ e por definição de limite, existe $M > 0$ tal que, para todo $|t| \geq M$: $0 < \frac{|a_d|+|b_e|}{2} \leq p(t) \leq \frac{3(|a_d|+|b_e|)}{2}$.

Como $p(t)$ é contínuo, então para $|t| \leq M$ $p(t)$ possui máximo e mínimo, isto é, existe t_0 com $|t_0| \leq M$ tal que $p(t) \geq p(t_0)$ o que implica que, para todo $t \in \mathbb{R}$, $p(t) \geq \min\{p(t_0), \frac{|a_d|+|b_e|}{2}\}$

Em resumo: existe c_1 tal que $p(t) \geq c_1$ para todo $t \in \mathbb{R}$

Utilizando este fato na desigualdade (3.4) temos que $H(\xi) \geq \frac{c_1}{2R} H\left(\frac{m}{n}\right)^d$.

As constantes c_1 e R independem de m e n, assim aplicando logaritmo temos a seguinte desigualdade:

$h(\xi) = \log H(\xi) \geq \log \frac{c_1}{2R} H\left(\frac{m}{n}\right)^d = \log \frac{H\left(\frac{m}{n}\right)^d}{\frac{2R}{c_1}} = \log H\left(\frac{m}{n}\right)^d - \log \frac{2R}{c_1} = dh\left(\frac{m}{n}\right) - k_1$ em que $k_1 = \log \frac{2R}{c_1}$.

Resta mostrar a outra desigualdade; continuaremos com a mesma notação.

Temos:

$$\Phi(m, n) = a_d m^d + a_{d-1} m^{d-1} n + \cdots + a_0 n^d$$

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

e

$$\Psi(m, n) = b_e m^e + b_{e-1} m^{e-1} n + \cdots + b_0 n^e$$

$$|\Psi(m,n)| \leq (|b_e| + \cdots + |b_0|)\max\{|m|^e, |n|^e\} \leq (|b_e| + \cdots + |b_0|)\max\{|m|^d, |n|^d\}$$

com $e \leq d$.

Seja $C = \max\{|a_d| + \cdots + |a_0|, |b_e| + \cdots + |b_0|\}$. Assim,

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

Aplicando logaritmo novamente, temos que:

$h(\xi) \leq dh\left(\frac{m}{n}\right) + \log C$. Tomando $k_2 = \log C$, obtemos

$$h(\xi) \leq dh\frac{m}{n} + k_2.$$

Isto conclui a prova do item 2) do lema.

□

3.5 Um Homomorfismo Importante

Lembrando que, para provarmos o teorema de Mordell, resta provar o lema 3.2.6 que nos diz que o índice $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ é finito. Esta é a parte mais técnica da demonstração. Infelizmente, não podemos provar o lema 3.2.6 para todas as curvas cúbicas sem utilizar ferramentas da teoria álgebrica dos números, além disso nós trabalharemos somente com os números racionais, por esse motivo, vams supor que o polinômio $f(x)$ tem pelo menos uma raiz racional x_0, o que é equilalente a dizer que a curva tem pelo menos um ponto racional de ordem dois. Desenvolveremos nesta seção algumas ferramentas necessarias para demonstrar o lema 3.2.6.

Como $f(x_0) = 0$, e f é um polinômio com coeficientes inteiros e coeficiente dominante 1, então 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 $E(\mathbb{Q})$. A nova equação terá coeficientes inteiros e a curva terá a forma:

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

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

A fórmula do discrimanante neste caso é: $\Delta = b^2(a^2 - 4b)$.Assuma que nossa curva é não singular, isto é, $\Delta \neq 0$, assim $b \neq 0$ e $a^2 - 4b \neq 0$.

Estamos interessados no índice $[E(\mathbb{Q}) : 2(\mathbb{Q})]$ ou equivalentemente na ordem do grupo quociente $E(\mathbb{Q})/2E(\mathbb{Q})$, é extremamente útil saber que a função de duplicação $P \to 2P$ pode ser dividida em duas operações.

A função de duplicação de um ponto, é de alguma forma de grau quatro pois, a função racional dada pela coordenada x de $2P$ é de grau quatro na coordenada x de P. Escreveremos a função $P \mapsto 2P$ como a composição de duas funções de grau dois, as quais serão mais fáceis de manusear. Entretanto, as duas funções não serão de E em E, mas sim de E para outra curva $\overline{E}$ e novamente para E. A outra curva $\overline{E}$ que consideraremos é a curva dada pela equação:

$$\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x \quad \text{em que} \quad \overline{a} = -2a \quad \text{e} \quad \overline{b} = a^2 - 4b$$

As curvas E e $\overline{E}$ estão intimamente relacionadas, então é natural estudar-las comparando-as.

Aplicando novamente o procedimento e olhando para

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

onde $\overline{\overline{a}} = -2\overline{a} = 4a$ e $\overline{\overline{b}} = \overline{a}^2 - 4\overline{b} = (-2a)^2 - 4(a^2 - 4b) = 16b$, temos que a curva é dada por $\overline{\overline{E}} : y^2 = x^3 + 4ax^2 + 16bx$.

A curva $\overline{E}$ é essencialmente a mesma curva que E, basta trocarmos y por $8y$ e x por $4x$, e dividir a equação por 64. Desse modo, o grupo $\overline{\overline{E(\mathbb{Q})}}$ de pontos racionais em $\overline{\overline{E}}$ é isomorfo ao grupo $E(\mathbb{Q})$ de pontos racionais em E.

Agora defina a função $\phi : E \to \overline{E}$. Desse modo, ϕ será homomorfismo de grupos e levará os pontos racionais de $E(\mathbb{Q})$ nos pontos racionais de $\overline{E(\mathbb{Q})}$. Em seguida, procedendo da mesma forma, definiremos a função $\psi : \overline{E} \to \overline{\overline{E}}$. Tendo em vista o isomorfismo $\overline{\overline{E}} \cong E$ a composição $\psi \circ \phi$,, é um homomorfismo de E em E, que será a multiplicação por dois.

A função $\phi : E \to \overline{E}$ é definida da seguinte forma:

Se $P = (x, y) \in E$ 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

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

Assim, ϕ está bem definida, resta-nos checar se $\overline{x}$ e $\overline{y}$ satisfazem a equação de $\overline{E}$ o que é simples; substituindo $\overline{x}$ em $y^2 = x^3 + ax^2 + bx$, chegamos que:

$$\overline{x}^3 + \overline{a}\overline{x}^2 + \overline{b}\overline{x} = \overline{x}\left[\overline{x}^2 + \overline{a}.\overline{x} + \overline{b}\right] = \overline{x}\left[\overline{x}^2 - 2a\overline{x} + (a^2 - 4b)\right] =$$

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

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

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

$$= \frac{y^2}{x^6}(x^3 - bx)^2 = \left(\frac{y(x^3 - bx)}{x^3}\right)^2 = \left(\frac{y(x^2 - b)}{x^2}\right)^2 = \overline{y}^2$$

Proposição 3.5.1. *Sejam E e $\overline{E}$ curvas elípticas dadas pelas equações:*

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

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

1. *Existe um homomorfismo* $\phi : E \to \overline{E}$ *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* $\overline{E}$ *temos a função* $\overline{\phi} : \overline{E} \to \overline{\overline{E}}$. *A curva* $\overline{\overline{E}}$ *é isomorfa a* E *pela função* $(x,y) \mapsto \left(\frac{x}{4}, \frac{y}{8}\right)$. *Existe assim um homomorfismo* $\psi : \overline{E} \to E$ *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 $\psi \circ \phi : E \to E$ *é a multiplicação por dois:*

$$\psi \circ \phi(P) = 2P.$$

Demonstração. Vimos anteriormente que a função ϕ leva pontos de E em pontos de $\overline{E}$ e supondo que ϕ é um homomorfismo, segue que o núcleo de ϕ são os pontos $\mathcal{O}$ e T, pois $\phi(\mathcal{O}) = \overline{\mathcal{O}}$ e $\phi(T) = \overline{\mathcal{O}}$ e $\phi(P) \neq \overline{\mathcal{O}} \quad \forall \quad P \neq \mathcal{O}$ e $P \neq T$. Logo precisamos provar que ϕ é um homomorfismo, ou seja,

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \quad \forall \quad P_1, P_2 \in E.$$

Observe que o primeiro sinal $+$ é adição em E e o segundo é adição em $\overline{E}$

Analisemos os seguintes casos:

Se $P_1 = \mathcal{O}$ e $P_2 = P \neq \mathcal{O}, \in E$,

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

Se $P_1 = T = P_2 \in E$,

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

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

Note que $2T$ tem ordem dois pois $y = 0$ logo $2T = \mathcal{O}$

Se $P_1 = T\,(x_2, y_2)$ e $P_2 = P = (x_1, y_1) = (x, y) \in E$ com $x \neq 0$, temos, pela fórmula de duplicação de pontos que: $P + T = (x_3, -y_3)$ onde:

$$x_3 = \lambda^2 - a - x_1 - x_2 \quad \text{onde,} \quad \lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$y_3 = \lambda x_3 + v$, onde v é o coeficiente linear da reta que passa por P e T.

Assim,

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

$$y_3 = \frac{y}{x}\frac{b}{x} + 0 = \frac{by}{x^2}.$$

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

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

Então:

$$\overline{x}(P+T) = \left(\frac{y(P+T)}{x(P+T)}\right)^2 = \frac{\left(\frac{-by}{x^2}\right)^2}{\left(\frac{b}{x}\right)^2} = \frac{b^2y^2}{x^4}\frac{x^2}{b^2} = \frac{y^2}{x^2} = \overline{x}(P).$$

$$\overline{y}(P+T) = \left(\frac{y(P+T)\left[(x(P+T))^2 - b\right]}{(x(P+T))^2}\right) = \frac{\frac{-by}{x^2}\left(\left(\frac{b}{x}\right)^2 - b\right)}{\left(\frac{b}{x}\right)^2} =$$

$$= \left[\frac{-by}{x^2}\frac{b^2 - bx^2}{x^2}\right]\frac{x^2}{b^2} = \frac{b^2(-by + x^2y)}{x^2b^2} = y\left(\frac{x^2 - b}{x^2}\right) = \overline{y}(P).$$

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

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 finalizar a prova de que ϕ é um homomorfismo, resta mostrar que se

$$P_1 + P_2 + P_3 = \mathcal{O} \text{ então } \phi(P_1) + \phi(P_2) + \phi(P_3) = \overline{\mathcal{O}},$$

pois, $P_3 = -(P_1 + p_2)$ e sabemos que $\phi(P_1 + P_2) = \phi(-P_3) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$. Daí, 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. Da 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). Provaremos que $\phi(P_1), \phi(P_2), \phi(P_3)$ são a interseção de algumas retas com $\overline{E}$. Observe que $v \neq 0$, pois se $v = 0$ significaria que a reta $y = \lambda x + v$ passaria por T, contrariando a nossa suposição de que P_1, P_2, P_3 são distintos de T.

A reta de interseção com $\overline{E}$ que pegamos é:

$$y = \overline{\lambda}x + \overline{v} \quad \text{onde,}$$

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

Para verificar que $\phi(P_1) = \phi(x_1, y_1) = (\overline{x_1}, \overline{y_1})$ esta na reta $y = \overline{\lambda}x + \overline{v}$, faremos as seguites operações:

$$y_1 = \overline{\lambda}x_1 + \overline{v} = \frac{v\lambda - b}{v}\left(\frac{y_1}{x_1}\right)^2 + \frac{v^2 - av\lambda + b\lambda^2}{v} = \frac{(v\lambda - b)(y_1)^2 + (v^2 - av\lambda + b\lambda^2)x_1^2}{vx_1^2} =$$

$$= \frac{(v\lambda(y_1)^2 - b(y_1)^2 + v^2x_1^2 - av\lambda x_1^2 + b\lambda^2 x_1^2)}{vx_1^2} = \frac{v\lambda\left(y_1^2 - ax_1^2\right) - b\left(y_1^2 - \lambda^2 x_1^2\right) + v^2x_1^2}{vx_1^2} =$$

$$= \frac{v\lambda\left(y_1^2 - ax_1^2\right) - b\left(y_1 + \lambda x_1\right)\left(y_1 - \lambda x_1\right) + v^2x_1^2}{vx_1^2}.$$

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

$$\frac{v\lambda\left(x_1^3 + bx_1\right) - bv\left(y_1 + \lambda x_1\right) + v^2x_1^2}{vx_1^2} = \frac{\lambda\left(x_1^3 + bx_1\right) - b\left(y_1 + \lambda x_1\right) + vx_1^2}{x_1^2} =$$

$$= \frac{\lambda x_1^3 + \lambda b x_1 - by_1 - b\lambda x_1 + vx_1^2}{x_1^2} = \frac{x_1^2\overbrace{(\lambda x_1 + v)}^{y_1} - by_1}{x_1^2} = \frac{y_1(x_1^2 - b)}{x_1^2} = \overline{y_1}.$$

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

O cálculo para $\phi(P_2)$ e $\phi(P_3)$ é exatamente o mesmo.

Observe 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 para isto, teriamos 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 note que ϕ é contínua como uma função de E em $\overline{E}$, 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 $\overline{\overline{E}}$ é dada pela equação $\overline{\overline{E}} : y^2 = x^3 + 4ax^2 + 16bx$ por isso é claro que a função $(x, y) \mapsto \left(\frac{x}{4}, \frac{y}{8}\right)$ é um isomorfismo de $\overline{\overline{E}}$ para E. Do item (1) temos um homomorfismo $\overline{\phi} : \overline{E} \to \overline{\overline{E}}$ definido pela mesma equação que define ϕ, mas trocando $\overline{a}$ e $\overline{b}$ por a e b. Uma vez que a função $\psi : \overline{E} \to E$ é a composta de $\overline{\phi} : \overline{E} \to \overline{\overline{E}}$ com o isomorfismo $\overline{\overline{E}} \to E$, obtemos de forma imediata que ψ é um homomorfismo (como composição de homomorfismos) bem definido de $\overline{E}$ para E. Resta provar que $\psi \circ \phi$ é multiplicação por dois. Usando um pouco de álgebra e resultados anteriores temos, por um lado:

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

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,

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

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

$$\psi \circ \phi(x,y) = \psi\left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) = \left(\frac{\left(\frac{y(x^2-b)}{x^2}\right)^2}{4\left(\frac{y^2}{x^2}\right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2}\right)^2 - (a^2-4b)\right)}{8\left(\frac{y^2}{x^2}\right)^2}\right) =$$

$$= \left(\frac{y^2(x^2-b)^2}{x^4}.\frac{x^4}{4y^4}, \frac{y(x^2-b)}{x^2}.\left(\frac{y^4}{x^4}.\frac{-x^4(a^2-4b)}{x^4}\right)\frac{x^4}{8y^4}\right) =$$

$$= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4-(a^2-4b)x^4)}{8y^3x^2}\right).$$

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.

$$= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(y^4-(a^2-4b)x^4)}{8y^3x^2}\right) =$$

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

$$= \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)x^2\left[(x^2+ax+b)^2-x^2a^2-4bx^2\right]}{8y^3x^2}\right) =$$

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

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

De maneira análoga teríamos, $\phi \circ \psi(\overline{x},\overline{y}) = 2(\overline{x},\overline{y})$. Podemos argumentar também da seguinte forma: como ϕ é um homomorfismo, sabemos que:

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

Por outro lado, o homomorfismo $\phi : E \to \overline{E}$ visto sobre $\overline{\mathbb{Q}}$, é sobrejetor. Ou seja, dado $\overline{P} \in \overline{E}(\overline{\mathbb{Q}})$, existe $P \in E(\overline{\mathbb{Q}})$, tal que $\phi(P) = \overline{P}$. Assim, $\phi(\psi(\overline{P})) = \phi(\psi(\phi(P))) = \phi(2P) = 2\phi(P) = 2\overline{P}$

Apenas provamos que $2P = \psi \circ \phi(P)$, sendo $\phi \circ \psi(\phi(P)) = 2(\phi(P))$. Agora $\phi : E \to \overline{E}$ é uma função de pontos complexos, então para qualquer $\overline{P} \in \overline{E}$ nós podemos achar $P \in E$ com $\phi(P) = \overline{P}$. 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 3.2.6

Nesta seção completaremos a prova do lema 3.2.6 e com isso, chegaremos a demonstração do Teorema de Mordell.

Vamos continuar com as mesmas notações utilizadas anterioremente.

Temos duas curvas $E : y^2 = x^3 + ax^2 + bx$ e $\overline{E} : y^2 = x^3 + \overline{a}x^2 + \overline{b}x$ onde $\overline{a} = -2a$ e $\overline{b} = a^2 - 4b$ e também temos os homomorfismos $\phi : E \to \overline{E}$ e $\psi : \overline{E} \to E$ de tal forma que as composições $\phi \circ \psi : \overline{E} \to \overline{E}$ e $\psi \circ \phi : E \to E$ 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.

Claramente, dado qualquer ponto $P \in \overline{E}\left(\overline{Q}\right)$, existe um ponto $P \in E\left(\overline{Q}\right)$ tal que $\phi(P) = \overline{P}$. Em outras palavras, trabalhando sobre o fecho algébrico dos racionais, o homomorfismo ϕ é sobrejetor. Examinaremos agora, o que acontece sobre o corpo dos racionais.

Fica claro, a partir da definição, que o homomorfimo ϕ restrito a $\mathbb{Q}$ define um homomorfismo de $E(\mathbb{Q})$ para $\overline{E}(\mathbb{Q})$. Se aplicarmos o homomorfimo ϕ em $E(\mathbb{Q})$ obteremos um subgrupo de $\overline{E}(\mathbb{Q})$ denotado por $\phi\left(\overline{E}(\mathbb{Q})\right)$. A seguir, faremos três afirmações que juntas, fornecem uma boa descrição da imagem:

(i) $\overline{\mathcal{O}} \in \phi(E\mathbb{Q})$

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

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

Demonstração. (i) É óbvio pois $\overline{\mathcal{O}} = \phi(\mathcal{O})$ e $\mathcal{O} \in \mathbb{Q}$.

(ii A partir da lei de formação de ϕ temos que $\overline{T} \in \phi(\mathbb{Q})$ se, e somente se, existe um ponto racional $(x, y) \in \mathbb{Q}$ tal que $\frac{y^2}{x^2} = 0$. Note que $x \neq 0$, pois caso $x = 0$, significa que $(x, y) = T$ e $\phi(T) = \overline{\mathcal{O}} \neq \overline{T}$. Então $\overline{T} \in \phi(\mathbb{Q})$ se, e somente se existe um ponto racional $(x, y) \in \mathbb{Q}$ com $x \neq 0$ e $y = 0$. Pondo $y = 0$ na equação de $E(\mathbb{Q})$ 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 $(\overline{x}, \overline{y}) \in \phi(\mathbb{Q})$ é um ponto com $\overline{x} \neq 0$, então pela definição de ϕ segue que $\overline{x} = \frac{y^2}{x^2}$, que é o quadrado de um número racional $w = \frac{y}{x}$.

Reciprocamente, queremos encontrar um ponto racional sobre E que é enviado em $(\overline{x}, \overline{y})$ onde x é o quadrado de um número racional. O núcleo do homomorfismo ϕ é $\{\mathcal{O}, T\}$. suponha que $\overline{x} = w^2$, onde $w \in \mathbb{Q}$.

Defina

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

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

Afirmamos que $P_1 = (x_1, y_1), P_2 = ((x_2, y_2) \in \mathbb{Q}$ e $\phi(x_i, y_i)$,para $i = 1, 2$. Primeiro provemos que $(x_1, y_1), (x_2, y_2) \in \mathbb{Q}$.

Com efeito, temos que

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

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

$$\frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{y}^2}{\overline{x}}\right) = \frac{1}{4}\left(\frac{\overline{x}^3 - 2a\overline{x}^2 + a^2\overline{x} - \overline{x}^3 + 2a\overline{x}^2 - a^2\overline{x} + 4b\overline{x}}{\overline{x}}\right) = b$$

Mostrar que $P_i = (x_i, y_i) \in E$ 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 provarmos 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 imediata 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:

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

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

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

Isto completa a verificação da afirmação (iii).

Observação 3.6.1. *A menos de manipulações algébricas, tudo o que provamos para o homomorfismo ϕ vale também para o homomorfismo ψ.*

□

Lembre-se que o nosso objetivo nesta seção é provar o Lema 3.2.6, que diz que $2E(\mathbb{Q})$ tem índice finito em $E(\mathbb{Q})$.

Veremos em breve que isto é consequência de poder provar que os índices $[\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))]$ e $[E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q}))]$ são finitos. Na verdade, mostraremos que $[\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] \leq 2^{s+1}$, onde s é o número de fatores primos distintos de $\overline{b} = a^2 - 4b$ e também que $[E(\mathbb{Q}) : \psi(\overline{E}(\mathbb{Q}))] \leq 2^{r+1}$, onde r é o número de fatores primos distintos de b.

Como observamos anteriormente, a partir das afirmações (i),(ii) e (iii) sabemos que $\psi(\overline{E}(\mathbb{Q}))$ é o conjunto de pontos $(x, y) \in E(\mathbb{Q})$ tal que x é o quadrado de um número racional diferente de zero, juntamente com o ponto $\mathcal{O}$, e também T, se b é um quadrado perfeito.

A idéia da demonstração é achar um homomorfismo a partir do grupo quociente $E(\mathbb{Q})/\psi(\overline{E}(\mathbb{Q}))$ 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 $\mathbb{Q}^*$, isto é:

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

Proposição 3.6.2. *Seja α uma função definida de $\mathbb{Q}$ para $\mathbb{Q}^*/\mathbb{Q}^{*2}$ definida por:*

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

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

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

$$\overline{\alpha} : \mathbb{Q}/\psi(\overline{E}(\mathbb{Q})) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$

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:

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

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

Demonstração. a) Provaremos que α é um homomorfismo. Como α envia elementos inversos de E em elementos inversos de $\mathbb{Q}^*/\mathbb{Q}^{*2}$, pois:

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

resta-nos provar que

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

onde $+$ é adição em $E(\mathbb{Q})$ e $\bullet$ multiplicação em $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

Os casos em que $P_1, P_2, P_3 := \{\mathcal{O}, \mathcal{O}, \mathcal{O}\}, \{T, T, \mathcal{O}\}$ são imediatos; o caso $\{P, -P, \mathcal{O}\}$ também é imediato pois já provamos que $\alpha(-P) = \alpha(P)^{-1} \pmod{\mathbb{Q}^{*2}}$.

Para provarmos 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:

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

Daí,

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

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

$$x_1x_2x_3 = v^2 - c$$

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

A útima 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 diferentes de $\mathcal{O}$ e T.

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. Logo: $\alpha(T)\alpha(-P)\alpha(T - P) = x_1 \bullet b \bullet x_2 = b \bullet b = b^2 = 1 \pmod{\mathbb{Q}^{*2}}$

b) Note que:

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

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

c) Seja $P = (x, y) \in E(\mathbb{Q})$, $P \neq \mathcal{O}$, $P \neq T$. Vimos 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:

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

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

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

Esta equação, expressa n^2 como o produto de dois inteiros.

Seja $d = mdc(m, m^2 + ame^2 + be^4)$; assumindo que x está na forma irredutivel, temos

$$d = mdc(m, m^2 + ame^2 + be^4) = mdc(m, be^4) = mdc(m, b),$$

já que $mdc(m, e) = 1$.

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

Ou seja, 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 $\alpha(P) = b \pmod{\mathbb{Q}^{*2}}$. Portanto a tese do item c) está provada.

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

□

Temos agora, as ferramentas necessárias para provar o lema 3.2.6 que decorre do seguinte lema.

Lema 3.6.3. *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. Temos que $\phi(A)$ tem índice finito em B e que $\psi(B)$ tem índice finito em A.

Em outros termos,

$$A/\psi(B) = \{a_1 + \psi(B), a_2 + \psi(B), \cdots, a_n + \psi(B)\}$$

$$B/\phi(A) = \{b_1 = \phi(A), b_2 + \phi(A), \cdots, b_m + \phi(A)\}$$

Veja que:

$$a_i + \psi(b_j) \in A \ \ \text{e} \ \ a_i + \psi(b_j) + 2A \in A/2A.$$

Vamos provar que

$$A/2A \subseteq \{a_i + \psi(b_j) + 2A/1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$$

Seja $a \in A$ então devemos provar que existem i,j tais que $a \in a_i + \psi(b_j) = 2A$

Seja $a + \psi(B) \in A/\psi(B)$ então existe i tal que $a \in a_i + \psi(B)$ o que implica que existe $b \in B$ tal que $a = a_i + \psi(b)$.

Agora, $b + \phi(A) \in B/\phi(A)$, ou seja, existe j tal que $b \in b_j + \phi(A)$, o que implica que existe $a' \in A$ tal que $b = b_j + \phi(a')$.

Daí, $a = a_i + \psi(b_j + \phi(a')) = a_i + \psi(b_j) + \psi \circ \phi(a') = a_i + \psi(b_j) + 2a'$.

Assim, $a \in a_i + \psi(b_j) + 2A$ e, portanto:

$$A/2A \subseteq \{a_i + \psi(b_j) + 2A/1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m\}$$

e

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

□

Podemos enfim, enunciar e concluir a demonstração do:

Teorema 3.6.4. *(Teorema de Mordell) Seja E uma curva elíptica dada pela equação*

$$E : y^2z = x^3 + ax^2z + bxz^2 + cz^3,$$

onde a,b,c são inteiros e seja $E(\mathbb{Q}) = \{[x : y : z] \in E : x, y, z \in \mathbb{Q}\}$. Então $E(\mathbb{Q})$ é um grupo abeliano finitamente gerado.

Demonstração. Tendo em vista os lemas 3.2.1, 3.2.2, 3.2.3 e 3.2.6, segue que as condições do Teorema 3.2.1 são satisfeitas. Portanto, $E(\mathbb{Q})$ é finitamente gerado. □

Precisamos também do seguinte teorema sobre grupos abelianos finitamente gerados, a saber:

Teorema 3.6.5. *Seja G um grupo abeliano finitamente gerado e G_{tors} seu subgrupo de torção.*

a) Existem um inteiro $r \geq 0$ e um subgrupo $L \cong \mathbb{Z}^r$ tais que $G = G_{tors} \oplus L$.

b) Existem inteiros unicamente determinados $r \geq 0$ e ${p_1}^{v_1}, \ldots, {p_u}^{v_u}$ com $p_1 \leq \ldots \leq p_u$ números primos e com $v_1 \geq 1, \ldots, v_u \geq 1$ tais que

$$G \cong \frac{\mathbb{Z}}{{p_1}^{v_1}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{{p_u}^{v_u}\mathbb{Z}} \times \mathbb{Z}^r$$

Finalizamos este capítulo com uma observação, que será muito útil no próximo capitulo:

Observação 3.6.6. *a) Tendo em vista o teorema anterior segue que:*

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

b) O inteiro r é o posto da curva elíptica E.

c) Note que: O grupo $E(\mathbb{Q})$ é finito se, e só se, o posto de E é igual a zero.

CAPÍTULO 4

NÚMEROS CONGRUENTES

4.1 Introdução

Definição 4.1.1. *Um número inteiro $n \geq 1$ é dito um número congruente se existir um triângulo retângulo cujos lados sejam números racionais e cuja área seja n*

Uma definição mais geral inclui todos os racionais positivos com esta propriedade.

Antes de estendermos esta noção, observemos que um inteiro n é dito livre de quadrados se n puder ser escrito da forma $\prod_{i=1}^{r} p_i$ onde os p_i's são números primos distintos.

Definição 4.1.2. *Um número racional positivo n é dito congruente se existem $x, y, z \in \mathbb{Q}$ positivos tais que*

$$\begin{cases} x^2 + y^2 = z^2 \\ \\ n = \dfrac{xy}{2} \end{cases}$$

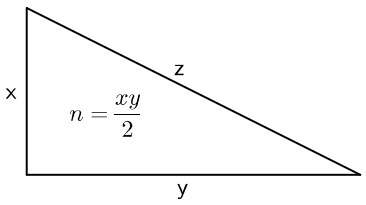

Tabela 4.1: Número Congruente

Observação 4.1.3. *Se $n \in \mathbb{Q} - \{0\}$, então existe $s \in \mathbb{Q} - \{0\}$ tal que $s^2 n$ é um número inteiro livre de quadrados.*

Se n for um número congruente, área de um triângulo retângulo de lados x, y, z, então a área do triângulo retângulo de lados sx, sy, sz é igual a $s^2 n$.

Em resumo: n é congruente $\Leftrightarrow$ $s^2 n$ é congruente. Assim, podemos sempre supor que n seja um inteiro positivo livre de quadrados.

Em um resumo de algum de seus trabalhos sobre teoria dos números que enviou a Huygens em 1959, Fermat afirma ter demonstrado, por um método singular que ele denomina método descenso infinito, entre outros teoremas, que não existe um triângulo retângulo com lados números inteiros cuja área seja o quadrado de um inteiro. Nesta carta, Fermat dá apenas uma idéia geral do método de descenso infinito, pois para um maior detalhamento, a carta ficaria muito grande. Felizmente, os detalhes da prova deste resultado, podem ser encontrados na margem do livro a Aritmética de Diofanto, junto à última proposição desta obra. Essencialmente, o argumento pode variar, provando primeiro que a equação $x^4 - y^4 = z^2$ não têm soluções inteiras não triviais, um resultado que Fermat demonstra usando o método do descenso infinito, de forma análoga a como se demonstra equação $x^4 + y^4 = z^2$ não têm soluções inteiras não triviais e logo usa-se esta equação para concluir que a equação $x^4 + y^4 = z^4$ não têm soluções não triviais.

Teorema 4.1.4. *Nenhum quadrado de um número inteiro pode ser escrito como a área de um triângulo retângulo cujos lados sejam números inteiros.*

Demonstração. Suponhamos que a área de um triângulo retângulo (a, b, c) com lados inteiros tenha como área o quadrado de um número inteiro m, ou seja, que $m^2 = \frac{ab}{2}$. Então,

$$(a + b)^2 = a^2 + b^2 + 2ab = c^2 + 4m^2$$

e

$$(a - b)^2 = a^2 + b^2 - 2ab = c^2 - 4m^2$$

donde segue que

$$(a^2 - b^2)^2 = (a - b)^2(a + b)^2 = c^4 - (2m)^4.$$

Assim a equação $z^2 = x^4 - y^4$ teria a solução não trivial $x = c$, $y = 2m$, $z = a^2 - b^2$, o que contradiz o resultado de Fermat, mencionado anteriormente. □

Exemplo 4.1.5. *a) Segue do teorema anterior que $n = 1, 4$ não são congruentes. Posteriormente obteve-se que $n = 2, 3$, também não são congruentes, mas, 5 é um número congruente, pois, é a área do triângulo retângulo cujos lados são $x = \frac{20}{3}$, $y = \frac{3}{2}$ e $z = \frac{41}{6}$.*

b) 6 é o menor número congruente tal que existe um triângulo retângulo cujos lados têm como comprimento números naturais, a saber: 3,4 e 5. De fato, no item anterior vimos que 5 é um número congruente, porém, seus lados não são números naturais.

A questão de determinar se um determinado número é congruente é chamado de "O problema do número congruente".

O Teorema de Tunnel fornece um critério que pode ser testado para determinar se um número é congruente (ver [2], página 3). O problema é que o resultado depende da conjectura de Birch e Swinnerton-Dyer (ver [2], capítulo IV, seção 10), um problema em aberto no campo da teoria dos números, que faz parte dos sete problemas do milênio.

Veremos agora um resultado elementar para caracterizar um número congruente.

Proposição 4.1.6. *Seja $n \geq 1$ um número inteiro livre de quadrados. Sejam $x, y, z \in \mathbb{Q}$ tais que $0 < x < y < z$. Então existe uma bijeção entre o conjunto de triângulos retângulos de lados x,y,z e área n e o conjunto de números racionais w tais que*

$$w - n, w, w + n \in \mathbb{Q}^2$$

dada por

$$(x, y, z) \longmapsto w = \left(\frac{z}{2}\right)^2$$

com inversa

$$w \longmapsto \left(\sqrt{w+n} - \sqrt{w-n}, \sqrt{w+n} + \sqrt{w-n}, 2\sqrt{n}\right).$$

Em particular, n é um número congruente se e somente se existir um número racional w tal que

$$w, w + n, w - n \in \mathbb{Q}^2.$$

Demonstração. Se $x^2 + y^2 = z^2$ e $n = \frac{xy}{2}$, então $(x \pm y)^2 = z^2 \pm 4n(*)$.

Logo

$$\left(\frac{x \pm y}{2}\right)^2 = \left(\frac{z}{2}\right)^2 \pm n.$$

Tome $w = \frac{z}{2}^2$ temos que $w, w + n, w - n \in \mathbb{Q}^2$.

Reciprocamente, dado w tal que $w, w + n, w - n \in \mathbb{Q}^2$ então $x = \sqrt{w+n} - \sqrt{w-n}$, $y = \sqrt{w+n} + \sqrt{w-n}$ e $z = 2\sqrt{w}$ satisfazem a $0 < x < y < z$, $xy = 2n$ e $x^2 + y^2 = z^2$. □

4.2 Equações Cúbicas

Nesta seção, associaremos a um número congruente n uma solução de uma certa equação cúbica.

Considere n um número congruente e $x, y, z \in \mathbb{Q}$ tais que $0 < x < y < z$, $n = \frac{xy}{2}$. Por (2) temos que

$$\left(\frac{x^2 - y^2}{4}\right)^2 = \left(\frac{z}{2}\right)^2 - n^2.$$

Em outros termos, encontramos soluções racionais $u = \frac{z}{2}$ e $v = \frac{x^2-y^2}{4}$ para a equação $u^4 - n^2 = v^2$. Multiplicando ambos os membros desta equação por u^2 obtemos

$$(u^2)^3 - n^2u^2 = (uv)^2.$$

Logo, $a = u^2$ e $b = uv$ fornece uma solução racional (a, b) para a equação cúbica $y^2 = x^3 - n^2x$. Reciprocamente, dada uma solução racional (a, b) da equação cúbica $y^2 = x^3 - n^2x$, será que (a, b) provém de um triângulo retângulo como acima? Nem sempre isto ocorre ! Para que isto aconteça, devemos ter $a \in \mathbb{Q}^2$, e, além disto, o denominador de a tem que ser par. Com efeito, dado um terno pitagórico $x < y < z$, seja s o *mmc* dos denominadores de x,y e z. Então, $x' = sx$, $y' = sy$, $z' = sz$ são números inteiros primos entre si. Neste caso x' e y'

têm paridades distintas, digamos que x' seja ímpar e y' seja par. Em particular z' é ímpar. Portanto $a = \left(\frac{z}{2}\right)^2 = \left(\frac{z'}{2s}\right)^2$ tem o denominador par. Sejam x_1,y_1 e z_1 os denominadores de x,y e z respectivamente. Denote por $2^{x'_1}$,$2^{x'_2}$ e $2^{z'_1}$ as maiores potências de 2 dividindo x_1,y_1 e z_1. Seja 2^{s_1} a maior potência de 2 dividindo s. Como sx e sz são ímpares e sy é par, conclui-se que $s_1 = x'_1 = z'_1$ e $s_1 < y'_1$. Estas condições nem sempre são satisfeitas. Basta pegar por exemplo a solução $\left(\left(\frac{41}{7}\right)^2, \frac{29520}{7^3}\right)$ da equação $y^2 = x^3 - (31)^2x$ que não provém de nenhum triângulo retângulo.

Observação 4.2.1. *Um terno de inteiros positivos (x, y, z) onde $x^2 + y^2 = z^2$ é chamada de terno pitagórico.*

Um terno pitagórico x,y e z tal que $mdc(x, y, z) = 1$ é dita terno pitagórico primitivo.

Se (x, y, z) é uma terno pitagórico primitivo então z é ímpar e x ou y é par.

Lema 4.2.2. *Seja (x, y, z) uma terno pitagórico primitivo, com y par. Então existem $\alpha, \beta \in \mathbb{Z}$ com $mdc\,(\alpha, \beta) = 1$ tais que*

$$\begin{aligned} x &= \alpha^2 - \beta^2, \\ y &= 2\alpha\beta, \\ z &= \alpha^2 + \beta^2. \end{aligned}$$

Demonstração. Como y é par então existe $C \in \mathbb{Z}$ tal que $y = 2C$.

Da equação $x^2+y^2 = z^2$ vemos que x e z têm mesma paridade (pois $2|y$), como $mdc(x, y, z) = 1$, então x e z são ímpares, portanto $z+x$ e $z-x$ são pares. Sejam $A, B \in \mathbb{Z}$ tais que $z+x = 2A$ e $z-x = 2B$. Observemos que $mdc(A, B) = 1$ pois se $x = A-B$, $z = A+B$, logo $mdc(A, B)|x$ e $mdc(A, B)|z$. Como $(z-x)(z+x) = y^2$, então $mdc(A, B)^2|y^2$. Isto é $mdc(A, B)|mdc(x, y, z) = 1$. Da equação $z^2-x^2 = y^2$ obtemos $4AB = 4C^2$, ou seja, $AB = C^2$, com $mdc(A, B) = 1$. Portanto A e B devem ser quadrados perfeitos. Logo, existem $\alpha, \beta \in \mathbb{Z}$ tais que $A = \alpha^2$, $B = \beta^2$. Em particular, $x = \alpha^2 - \beta^2$; $z = \alpha^2 + \beta^2$ e $y^2 = z^2 - x^2 = 4AB = 4\alpha^2\beta^2$ □

Proposição 4.2.3. *Seja $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ uma solução de $y^2 = x^3 - n^2x$ tal que $a \in \mathbb{Q}^2$ com denominador par. Então, existe um triângulo retângulo de área n e lados $\sqrt{a+n} - \sqrt{a-n}$, $\sqrt{a+n} + \sqrt{a-n}$ e $\sqrt{2a}$.*

Demonstração. Seja $u = \sqrt{a} \in \mathbb{Q}$, $u > 0$ e $v = \frac{b}{u}$. Então $v^2 = \frac{b^2}{a} = a^2 - n^2$. Seja t o denominador de u. Daí, os denominadores de v^2 e a^2 são iguais a t^4, em particular,

$$(t^2v, t^2n, t^2a)$$

é uma terno pitagórico com t^2n par e $mdc(t^2v, t^2n, t^2a) = 1$. Segue do lema anterior que existem inteiros positivos α,β tais que $t^2v = \alpha^2-\beta^2$, $t^2n = 2\alpha\beta$ e $t^2a = \alpha^2+\beta^2$. Desse modo, o triângulo retângulo de lados

$$\left(\frac{2\alpha}{t}, \frac{2\beta}{t}, 2v\right)$$

tem área $\frac{2\alpha\beta}{t^2} = n$. Pela Proposição 4.1.1. temos que este terno corresponde a $\left(\frac{2u}{2}^2\right) = u^2 = a$. Portanto, existe um triângulo retângulo de lados $\sqrt{a+n} - \sqrt{a-n}$, $\sqrt{a+n} + \sqrt{a-n}$ e $2\sqrt{a}$ de área n.

□

4.3 Redução Módulo p

Seja p um número primo, $\mathbb{F}_p$ o corpo finito de p elementos, $\mathbb{P}^2(\mathbb{F}_p)$ e $\mathbb{P}^2(\mathbb{Q})$ os planos projetivos definidos sobre $\mathbb{F}_p$ e $\mathbb{Q}$ respectivamente. Dado $[a : b : c] \in \mathbb{P}^2(\mathbb{Q})$ podemos sempre escolher inteiros a_0, b_0, c_0 de tal forma que $mdc(a_0, b_0, c_0) = 1$. Para isto, basta multiplicar a, b, c pelo mmc dos denominadores. Dessa forma podemos definir a aplicação

$$\begin{array}{rccc} \Phi: & \mathbb{P}^2(\mathbb{Q}) & \longrightarrow & \mathbb{P}^2(\mathbb{F}_p) \\ & P = [a_0, b_0, c_0] & \longmapsto & \overline{P} = \left[\overline{a_0} : \overline{b_0} : \overline{c_0}\right]. \end{array}$$

Observe agora que, dada uma curva elíptica

$$E : y^2 = x^3 + ax + b,$$

sempre podemos escolher um modelo dela, de tal forma que seus coeficientes sejam inteiros e, reduzindo estes coeficientes módulo p, podemos considerar a curva reduzida $\widetilde{E} : y^2 = x^3 + \overline{a}x + \overline{b}$, definida agora, sobre o corpo finito $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Podem ocorrer dois casos:

- $\widetilde{E}$ continua sendo não singular, portanto é uma curva elíptica. Neste caso, dizemos que E tem uma boa redução módulo p.
- $\widetilde{E}$ é singular; neste caso dizemos que E não tem uma boa redução módulo p.

Em particular, se $P \in E(\mathbb{Q})$, então $\Phi(P) = \overline{P} \in \widetilde{E}(\mathbb{F}_p)$.

Note que, se $y^2 = x^3 + ax + b$ é uma equação com coeficientes inteiros, que define a curva E e, se Δ é o discriminante do polinômio $x^3 + ax + b$, o fato de E ser não singular é equivalente a dizer que $\Delta \neq 0$. Assim sendo, o discriminante $\overline{\Delta}$ do polinômio $x^3 + \overline{a}x + \overline{b}$ que define a curva $\widetilde{E}$ é a redução módulo p de Δ. Isto é, $\widetilde{E}$ é não singular se, e somente se, p não divide Δ. Neste caso podemos provar que $\Phi : E(\mathbb{Q}) \longrightarrow \widetilde{E}(\mathbb{F}_p)$ é um homomorfismo. Observe que $p|\Delta$ apenas para um número finito de primos p. A seguinte proposição identifica seu núcleo.

Proposição 4.3.1. *Seja $i \in 1, 2$ e $P_i = (x_i, y_i, z_i) \in \mathbb{P}^2(\mathbb{Q})$. A igualdade $\Phi(P_1) = \Phi(P_2)$ ocorre se, e somente se, p dividir simultaneamente os números $(y_1z_2 - y_2z_1)$, $(x_2z_1 - x_1z_2)$ e $(x_1y_2 - x_2y_1)$, que são as coordenadas provenientes do produto vetorial $P_1 \times P_2$.*

Demonstração. Sejam $\Phi(P_1) = (\overline{x_1}, \overline{y_1}, \overline{z_1})$ e $\Phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2})$. Suponhamos que $\Phi(P_1) = \Phi(P_2)$.

Então,

$$x_1 - x_2 = \lambda_1 p,$$
$$y_1 - y_2 = \lambda_2 p,$$
$$z_1 - z_2 = \lambda_3 p.$$

Provaremos que p divide $(y_1 z_2 - y_2 z_1)$. Temos que:

$$(y_1 z_2 - y_2 z_1) = (y_1 - y_2) z_2 + y_2 z_2 - y_2 z_1 = (y_1 - y_2) z_2 + y_2 (z_2 - z_1).$$

Substituindo as igualdades $y_1 - y_2 = \lambda_2 p$ e $z_1 - z_2 = \lambda_3 p$ na igualdade anterior obtemos que $(y_1 z_2 - y_2 z_1) = \lambda_2 p z_2 + y_2 \lambda_3 p = p(\lambda_2 z_2 + y_2 \lambda_3)$ e portanto p divide $(y_1 z_2 - y_2 z_1)$. De forma análoga, prova-se que p também divide $(x_2 z_1 - x_1 z_2)$ e $(x_1 y_2 - x_2 y_1)$.

Reciprocamente, suponhamos que p divide simultaneamente os números os números $(y_1 z_2 - y_2 z_1)$, $(x_2 z_1 - x_1 z_2)$ e $(x_1 y_2 - x_2 y_1)$.

Como $mdc(x_1, y_1, z_1) = 1$ então $p \nmid x_1$ ou $p \nmid y_1$ ou $p \nmid z_1$. Podemos supor, sem perda de generalidade, que $p \nmid x_1$. Assim,

$$\Phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2}) = (\overline{x_1 x_2}, \overline{x_1 y_2}, \overline{x_1 z_2}).$$

Como $p \mid (x_1 y_2 - x_2 y_1)$, então $\overline{x_1 y_2} = \overline{x_2 y_1}$ e, como $p \mid (x_2 z_1 - x_1 z_2)$, então $\overline{x_1 z_2} = \overline{x_2 z_1}$. Daí,

$\Phi(P_2) = (\overline{x_2}, \overline{y_2}, \overline{z_2}) = (\overline{x_1 x_2}, \overline{x_1 y_2}, \overline{x_1 z_2}) = (\overline{x_1 x_2}, \overline{x_2 y_1}, \overline{x_2 z_1})$.

Se $p | x_2$ então $\Phi(P_2) = (0, 0, 0)$, o que é impossível. Logo, multiplicando o terno $(\overline{x_1 x_2}, \overline{x_2 y_1}, \overline{x_2 z_1})$, pelo inverso de $\overline{x_2}$, concluimos que

$$\Phi(P_2) = (\overline{x_1}, \overline{y_1}, \overline{z_1}) = \Phi(P_1)$$

□

Corolário 4.3.2. *Seja E uma curva elíptica definida sobre $\mathbb{Z}$ e suponhamos que p é um primo suficientemente grande de tal forma que não divide as coordenadas de todos os produtos vetoriais dos pontos em $E(\mathbb{Q})_{tors}$ nem o discriminante de E. Então, a restrição do morfismo de redução*

$$\phi_p : E(\mathbb{Q})_{tors} \to \widetilde{E}(\mathbb{F}_p)$$

é injetora.

Demonstração. Sejam $P_1 \neq P_2 \in E(\mathbb{Q})_{tors}$. Como p é um primo suficientemente grande, tal que p não divide as coordenadas de todos os produtos vetoriais em $E(\mathbb{Q})$, e nem o discriminante de E, segue do lema anterior que $\phi_p(P_1) \neq \phi_p(P_2)$ e, portanto, ϕ_p é injetora.

□

Lema 4.3.3. *Para a curva elíptica $E_A : y^2 = x^3 - A^2 x$, se p é um número primo tal que $p \nmid \Delta_A = 4A^6$, $p \geq 7$ e $p \equiv 3 \pmod 4$, então $\widetilde{E}_A(\mathbb{F}_p)$ tem exatos $p + 1$ pontos.*

Demonstração. Primeiramente, $\widetilde{E}_A(\mathbb{F}_p)$ contém os quatro pontos $(0,0)$, $(-A,0)$, $(A,0)$ e $\mathcal{O}$. Observemos agora que, se $x \neq 0, A, -A$, considerando o par $x, -x$ notamos que, como $f(x) = x^3 - A^2x$ é uma função ímpar e $p \equiv 3 \pmod 4$ segue que -1 não é um quadrado módulo p, então exatamente um dos elementos $f(x)$ ou $f(-x)$ é um quadrado em $\mathbb{F}_p$. Portanto tem-se duas raízes quadradas que dão lugar aos pontos $\left(x, \pm\sqrt{f(x)}\right)$ ou $\left(-x, \pm\sqrt{f(-x)}\right)$, a qual nos dá um total de $p-3$ pontos extras em $\widetilde{E}_A(\mathbb{F}_p)$ que, juntamente com os 4 pontos óbvios, nos dão os $p+1$ pontos desejados. □

Teorema 4.3.4. $|E_A(\mathbb{Q})_{tors}| = 4$

Demonstração. Basta mostrar que $|E_A(\mathbb{Q})_{tors}|$ divide 4.

Seja p um primo suficientemente grande. Pelo teorema de Lagrange, a ordem de $E_A(\mathbb{Q})_{tors}$ divide a ordem de $E(\mathbb{F}_p)$ e pelo lema anterior a ordem de $E_A(\mathbb{F}_p)$ é $p+1$, se $p \equiv 3 \pmod 4$.

Pelo teorema de Dirichlet (Ver [9], Capítulo 7), existem infinitos primos p da forma $8n+3$. Assim, existe um primo $p \equiv 3 \pmod 8$, satisfazendo as condições do lema 4.3.3, e portanto, $|\widetilde{E}_A(\mathbb{F}_p)| = p+1$. Pelo corolário 4.3.1, $|E_A(\mathbb{Q})_{tors}|$ divide $p+1$ e como $p+1 \equiv 4 \pmod 8$, então 8 não divide $|E_A(\mathbb{Q})_{tors}|$.

Novamente pelo teorema de Dirichlet, existem infinitos primos da forma $12n+7$. Por um raciocínio similar ao anterior, 3 não divide $|E_A(\mathbb{Q})_{tors}|$, pois $3 \nmid p+1 \equiv 12n+8$. Analogamente, se $q > 3$ é um primo qualquer, existem infinitos primos $p \equiv 3 \pmod{4q}$. Escolhemos tal primo que não divida o discriminante de $E_A(\mathbb{Q})$, logo este primo satisfaz as condiçõees do lema 4.3.3, portanto $|\widetilde{E}_A(\mathbb{F}_p)| = p+1$. Como $p+1 \equiv 4 \pmod{4q}$, então $q \nmid p+1$, o que implica pelo corolário 4.3.1 que $q \nmid |E_A(\mathbb{Q})_{tors}|$.

Portanto, os únicos divisores de $|E_A(\mathbb{Q})_{tors}|$ são 1, 2 ou 4 e como $E_A(\mathbb{Q})_{tors}$ contém os quatro pontos óbvios, então sua ordem é exatamente 4.

□

4.4 Relação entre Curvas Elípticas e Números Congruentes

Considerando os resultados anteriores, podemos enunciar e demonstrar o resultado mais importante do nosso trabalho, que relaciona números congruentes e curvas elípticas.

Teorema 4.4.1. *Um número n é congruente se, e somente se, o posto da curva elíptica E : $y^2 = x^3 - n^2x$ é positivo.*

Demonstração. Suponha que n seja um número congruente e seja $(a,b) \in E(\mathbb{Q})$ a solução da equação cúbica obtida pelo argumento anterior a Proposição 4.2.1. Desse modo, $a \in \mathbb{Q}^2$, com denominador par. Se (a,b) tiver ordem finita, segue do Teorema anterior que (a,b) é necessariamente um ponto de ordem 2. Logo, sua primeira coordenada só pode ser 0, n ou $-n$. Temos que $0, -n \notin \mathbb{Q}^2$. Além disto para determinar se um inteiro positivo n é congruente, basta considerar sua classe módulo $\mathbb{Q}^2$. Assim, podemos supor sempre que n é livre de quadrados.

Portanto $n \notin \mathbb{Q}^2$. Pelo teorema de Mordell-Weil concluimos que (a, b) tem que ser um ponto de ordem infinita de $E(\mathbb{Q}^2)$, em particular, o posto de E é positivo.

Reciprocamente, dado um ponto $P = (x, y) \in E(\mathbb{Q})$ de ordem infinita então pela fórmula de duplicação de um ponto temos que:

$$x = \frac{x^4 + 2n^2x^2 + n^4}{(2y)^2}$$

satisfaz as condições da Proposição 4.2.1, e portanto, n é um número congruente.

□

Vejamos agora, um exemplo para fixar as idéias.

Já vimos anteriormente que $n = 5$ é um número congruente. Verificaremos este resultado utilizando o Teorema anterior. De fato, temos a seguinte curva elíptica associada a $n = 5$:

$$y^2 = x^3 - 5^2x = x(x^2 - 5^2) = x(x + 5)(x - 5).$$

Observe que $P = (45, 300)$ satisfaz a equação que define a curva elíptica. Alem disso, $y \neq 0$ e $y^2 = 90000 \nmid 62500 = \Delta$. Logo pelo teorema Nagell-Lutz temos que P é de ordem infinita. o que implica, pelo Teorema anterior, que 5 é um número congruente.

O mais interessante, é que, além de verificarmos que $n = 5$ é congruente, conseguimos encontrar através do ponto $P = (45, 300)$ os lados do triângulo retângulo que tornam $n = 5$ congruente.

Temos pela fórmula de duplicação de um ponto que $2P = \left(\left(\frac{41}{12}\right)^2, \frac{62279}{12^2}\right)$.

Pelos cálculos utilizados no argumento da demonstração do Teorema anterior, chame $w = \left(\frac{41}{12}\right)^2$ então os lados do triângulo retângulo serão

$$\sqrt{w + n} - \sqrt{w - n} = \frac{3}{2},$$

$$\sqrt{w + n} + \sqrt{w - n} = \frac{20}{3}$$

e

$$2\sqrt{w} = \frac{41}{6}.$$

REFERÊNCIAS BIBLIOGRÁFICAS

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

[2] Milne J.S, Elliptic Curves, *Booksurge Publishing*, 2006.

[3] Garcia A., Lequain I., Elementos de Álgebra, *Projeto Euclides-IMPA* 5.ed, 2010

[4] Vainsercher, I., Curvas Álgebricas Planas, *Coleção Matemática Universitária*, 1996

[5] Pacheco, A., Números Congruentes e Curvas Elípticas, *Matemática Universitária* nº22/23 (1997), pp 18-29

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

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

[8] Walker, R. J. 1950. Algebraic Curves. Princeton Mathematical Series, Vol. 13. Princeton University Press, Princeton, N. J. Reprinted by Dover 1962.

[9] T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag 1976.