UNIVERSIDADE FEDERAL DE MINAS GERAIS
Instituto de Ciências Exatas
Dissertação de Mestrado em Matemática

José Gustavo Coelho

CURVAS ELÍPTICAS SOBRE CORPOS FINITOS

BELO HORIZONTE
2020

José Gustavo Coelho

Curvas elípticas sobre corpos finitos

Versão final da dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais.

Orientador: Israel Vainsencher

Departamento de Matemática
Universidade Federal de Minas Gerais
Março de 2020

Coelho, José Gustavo

C672c Curvas elípticas sobre corpos finitos [manuscrito] / José Gustavo Coelho. – 2023.
1 recurso online (51 f. il. color.): pdf.

Orientador: Israel Vainsencher
Dissertação (mestrado) - Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática.
Referências: f.50-51.

1. Matemática – Teses. 2. Curvas elípticas – Teses. 3. Curvas algébricas –Teses. 4. Corpos finitos (Álgebra) –Teses. I. Vainsencher, Israel. II. Universidade Federal de Minas Gerais, Instituto de Ciências Exatas, Departamento de Matemática. III. Título.

CDU 51 (043)

Ficha catalográfica elaborada pela bibliotecária Belkiz Inez Rezende Costa
CRB 6/1510 Universidade Federal de Minas Gerais - ICEx

Universidade Federal de Minas Gerais
Departamento de Matemática
Programa de Pós-Graduação em Matemática

FOLHA DE APROVAÇÃO

Curvas Elípticas sobre Corpos Finitos

JOSÉ GUSTAVO COELHO

Dissertação defendida e aprovada pela banca examinadora constituída pelos Senhores:

Prof. Israel Vainsencher
UFMG

Prof. Lucas da Silva Reis
UFMG

Prof. Paulo Antônio Fonseca Machado
UFMG

Belo Horizonte, 09 de março de 2020.

Av. Antônio Carlos, 6627 – Campus Pampulha - Caixa Postal: 702
CEP-31270-901 - Belo Horizonte – Minas Gerais - Fone (31) 3409-5963
e-mail: pgmat@mat.ufmg.br - home page: http://www.mat.ufmg.br/pgmat

Agradecimentos

Agradeço ao meu orientador por aceitar conduzir o meu trabalho de pesquisa.

A todos os meus professores do curso de Matemática da Universidade Federal de Minas Gerais pela excelência da qualidade técnica de cada um.

Aos meus pais, que sempre estiveram ao meu lado me apoiando ao longo de toda a minha trajetória.

Aos meus colegas pela paciência.

Resumo

Muito é falado sobre curvas elípticas e suas aplicações na criptografia. Este texto trata de forma concisa do aspecto algébrico delas. Vemos a curva elíptica como uma curva plana projetiva com uma operação que torna o conjunto de seus pontos um grupo abeliano.

O primeiro capítulo trata de definir propriamente uma curva elíptica, as operações sobre ela e fórmulas concretas para seu cálculo. é mostrado como determinar a forma de Weierstrass e são apresentados resultados sobre a estrutura, como os Teoremas de Nagell-Lutz e Mordell.

O segundo capítulo começa a trabalhar especificamente com curvas elípticas sobre corpos finitos, com o propósito de expor brevemente como elas são usadas para a criptografia.

O capítulo final utiliza recursos algébricos mais sofisticados afim de se exibir resultados sobre a existência e estrutura dos grupos em curvas elípticas sobre corpos finitos.

Palavras-chave: *curvas elípticas, geometria algébrica, grupos.*

Abstract

Much has been said about elliptic curves and their applications in cryptography. This text regards their algebraic aspects. We shall approach elliptic curves as plane projective curves possessing an operation that turns the set of its points into an abelian group.

The first chapter deals with properly defining elliptic curves, their operations and concrete formulas for calculating in them. It is shown how to determine the Weierstrass form and results about the structure, like Nagell-Lutz's and Mordell's theorems are presented.

The second chapter begins the work on elliptic curves over finite fields, with the purpose of briefly exposing how they are used in cryptography.

The final chapter uses more sophisticated algebraic methods to display results about the existence and structure of the groups in elliptic curves over finite fields.

Keywords: *elliptic curves, algebraic geometry, groups.*

Conteúdo

1 Operações sobre curvas elípticas

Ainda é magia mesmo que você saiba como foi feita.
-Terry Pratchett

Curvas cúbicas não-singulares

Ao longo deste texto usamos vários conceitos da geometria algébrica, que podem ser encontrados em [1], [2] e [3]. Dado um corpo K, uma curva sobre o plano afim ou projetivo é o conjunto dos zeros de um polinômio com coeficientes em K neste plano, com o grau da curva sendo definido como o grau do polinômio. Neste texto estudamos as curvas elípticas de grau três, que consistem em todas as curvas de grau três, ou cúbicas, não-singulares.

A forma geral para o polinômio que define uma cúbica é

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

onde as constantes $a, b, c, d, e, f, g, h, i$ e j são tomadas sobre o corpo K.

Implicitamente sempre assumimos que a curva está no plano projetivo sobre este corpo, mas para denotar qualquer ponto específico usamos por simplicidade suas coordenadas afins sempre que possível.

Denotamos por $\overline{K}$ o fecho algébrico do corpo K. Escrevemos E/K para enfatizar que a curva elíptica E é definida por uma equação a coeficientes em K. Seja $K' \supseteq K$ uma extensão de corpos, a notação $E(K')$ denota o conjunto dos pontos de E com coordenadas em K', ditos pontos K'-racionais, ou simplesmente pontos racionais se não houver ambiguidade sobre o corpo.

Registramos para uso posterior o clássico Teorema de Bézout.

Proposição 1. *Sejam E e L curvas sem componentes em comum, de graus m e n respectivamente. Então a soma dos índices de interseção em todos os pontos é igual a mn.*

Demonstração. A demonstração do Teorema de Bézout pode ser encontrada em [1]. □

Seja E uma cúbica não-singular e L uma reta, as seguintes afirmações sobre índice e ordem de interseções de curvas são consequência do Teorema anterior:

i) Como E é não-singular, também é irredutível. Logo podemos sempre aplicar Bézout, porque a curva não pode ter a reta L como componente. Assim,

ii) $\sum_{P \in \mathbb{P}^2} I(P, F \cap L) = 3$, logo a reta intersecta a cúbica em no máximo três pontos.

iii) Por propriedades do índice de interseção, temos que se L é tangente a E no ponto P, então $I(P, E \cap L) \geq 2$. Portanto a tangente de um ponto só pode intersectar novamente a curva em no máximo outro ponto.

iv) Se P é um ponto tal que $I(P, E, L) = 3$, dito um ponto de inflexão, temos que a reta não intersecta a cúbica em nenhum outro ponto.

v) Em cúbicas não-singulares, P é um ponto de inflexão se e apenas se $I(P, E \cap L) = 3$, onde L é a tangente de E em P.

Seja E uma cúbica não-singular na qual sejam conhecidos dois pontos com coordenadas racionais P e Q. A equação da reta determinada por dois pontos tem coeficientes racionais, e é chamada uma reta racional. Pelo Teorema de Bézout ela deve se encontrar com a curva em mais um ponto, ou ser tangente à curva em algum dos dois. Como as constantes na equação da reta e da curva são racionais, ao resolver o sistema de modo a achar o ponto restante, constatamos que esse terceiro ponto também é racional. Isto nós dá um meio de calcular mais pontos racionais na cúbica a partir de pontos conhecidos: criamos retas passando por pontos que já identificamos e buscamos pontos novos na interseção com a cúbica.

Grupo definido sobre a curva

Um fato importante é que podemos definir um grupo abeliano sobre os pontos racionais de uma curva elíptica. Para este fim, definimos uma operação binária no conjunto E .

Definição 2. A aplicação $* : E \times E \to E$ associa a cada par de pontos $(P, Q) \in E \times E$ o ponto $P * Q := R \in E$, terceiro ponto da interseção da reta secante $\overline{PQ}$ com a curva. Se $P = Q$, tomamos a reta tangente à curva no ponto ao invés da secante. Fixamos também um ponto $\mathcal{O}$ da curva, e o chamamos de origem.

Notamos que esta operação é fechada quando restringida a pontos em $E(K)$, pois neste caso todos as constantes envolvidas estão em K, e o pontos resultantes da operação também devem ter coordenadas em K.

Proposição 3. *A operação $*$ satisfaz as seguintes propriedades:*

i) $P * Q = Q * P$.

ii) $P * (P * Q) = Q$.

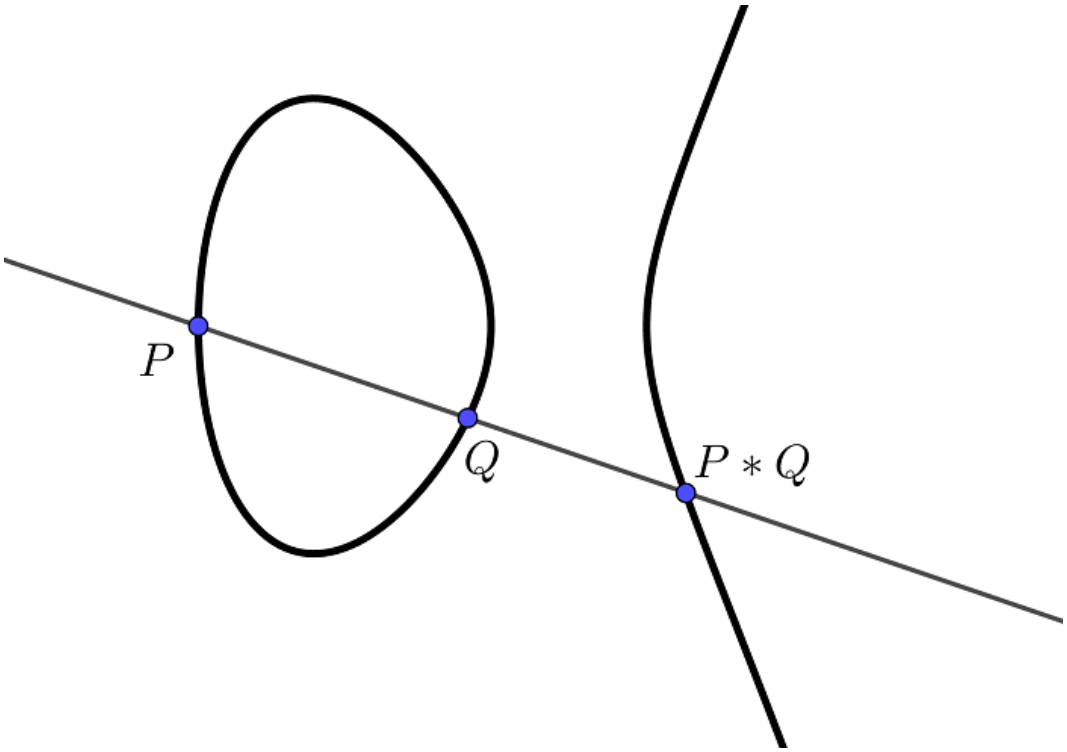
iii) Se P é um ponto de inflexão então $P * P = P$.

Demonstração.

i) Se $P = Q$ isso é trivial. Caso contrário, a reta ligando P a Q é a mesma reta ligando Q a P.

ii) No plano projetivo existem exatamente três pontos de interseção de uma cúbica com uma reta, contado com multiplicidade. Assim, a reta que passa por P, $P * Q$ e $P * (P * Q)$ é a mesma que passa por P, $P * Q$ e Q. Assim estes trios devem coincidir, e $P * (P * Q) = Q$.

iii) Como P é um ponto de inflexão, sua tangente tem apenas o ponto P em comum com a curva, com multiplicidade 3, e pela Proposição 1 não encontra nenhum outro ponto.



O nosso trabalho para definir um grupo ainda não acabou, visto que $*$ não define uma operação de grupo. Basta ver que como operação, a aplicação não é associativa. Porém, a operação $*$ pode ser usada para definir uma operação de grupo. □

Definição 4. Sejam $P, Q \in E$. A operação adição $+ : E \times E \to E$ é definida como

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

onde $\mathcal{O}$ é o ponto origem que escolhemos na curva. Notamos que desde que $\mathcal{O}$ esteja em $E(K)$ esta operação também é fechada quando restringida apenas a pontos racionais.

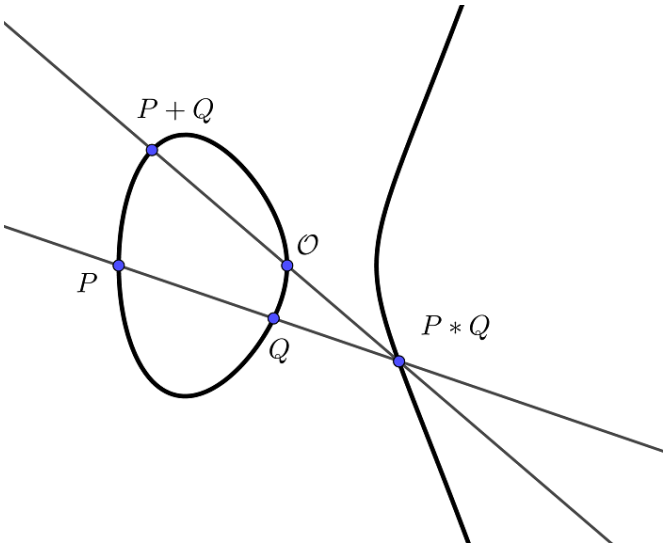
Verificaremos que esta operação é associativa, propriedade que faltava à operação $*$.

Proposição 5. *Seja E uma curva cúbica sobre um corpo qualquer. A operação $+$ sobre E é associativa, isto é, $P + (Q + R) = (P + Q) + R$ para $P, Q, R \in E$.*

Demonstração. Definimos $D_1 := P + (Q + R)$, $D_2 := (P + Q) + R$, $D_1' = D_1 * \mathcal{O}$ e $D_2' = D_2 * \mathcal{O}$ respectivamente.

Sejam $L_1 := \overline{QR(Q * R)}$, $L_2 := \overline{(P * Q)\mathcal{O}(P + Q)}$ e $L_3 := \overline{PD_1'(Q + R)}$ retas. A união dessas retas forma uma cúbica degenerada E_1. Analogamente temos que as retas $N_1 = \overline{R(P + Q)D_2'}$, $N_2 = \overline{PQ(P * Q)}$ e $N_3 = \overline{(Q * R)\mathcal{O}(Q + R)}$ formam uma cúbica E_2.

Observamos que E e E_1 se intersectam em nove pontos: $P, Q, R, Q * R, P * Q, Q + R, P + Q, D_1'$ e $\mathcal{O}$. Sabemos que a curva E_2 também também intersecta E em pelo menos oito dos pontos listados, salvo possivelmente D_1'. Então, o Teorema de Cayley-Bacharach[6] implica que E_2 também possui o ponto D_1'. Como duas cúbicas que não



possuem componentes em comum podem se intersectar em no máximo nove pontos, temos que $D_1' = D_2' \Rightarrow D_1 = D_2 \Rightarrow P + (Q + R) = (P + Q) + R$, provando a associatividade da operação $+$.

□

Proposição 6. *$(E, +)$ é um grupo abeliano, e o ponto fixo $\mathcal{O}$ é seu elemento neutro.*

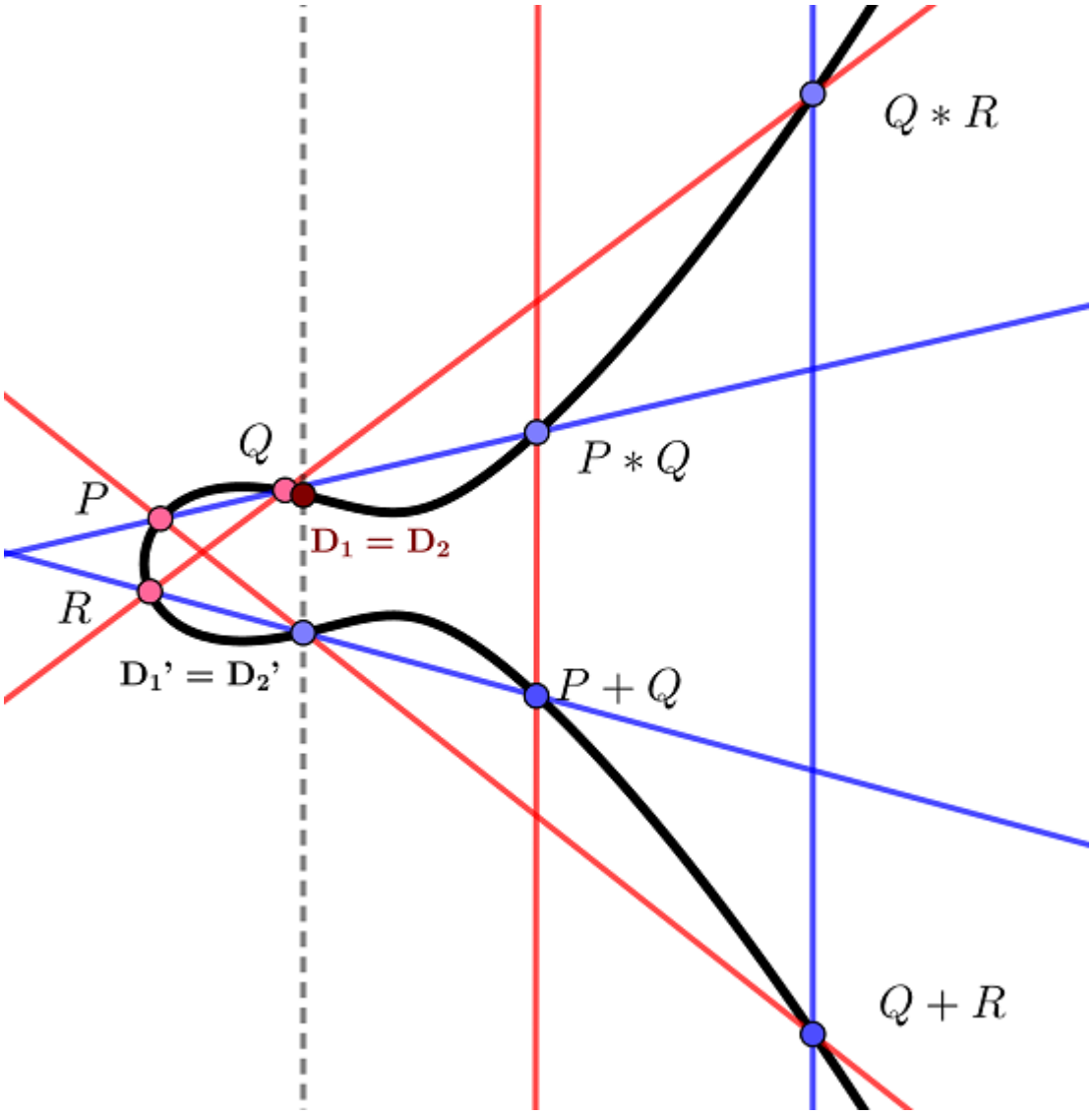
Demonstração. Já vimos que $+$ é uma operação associativa. Também é comutativa, pois da comutatividade da operação $*$ segue que $\mathcal{O} * (P * Q) = \mathcal{O} * (Q * P)$. Vamos então mostrar que $\mathcal{O}$ é o elemento neutro. Seja $P \in E$. $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * (\mathcal{O} * P) = P$, logo $\mathcal{O}$ é o elemento neutro. Por fim, para qualquer ponto P, o elemento $-P := P * \mathcal{O}$ é seu inverso, pois

$$\begin{aligned} P + (-P) &= \mathcal{O} * (P * (P * \mathcal{O})) \\ &= \mathcal{O} * \mathcal{O} = \mathcal{O}. \end{aligned}$$

□

Observamos que a soma nos permite encontrar pontos racionais em curvas elípticas. Seja E uma cúbica não-singular na qual sejam conhecidos dois pontos com coordenadas racionais P e Q. A equação da reta determinada por dois pontos tem coeficientes racionais, e é chamada uma reta racional. Pelo Teorema de Bézout ela deve se encontrar com a curva em mais um ponto, ou ser tangente à curva em algum dos dois. Como as constantes na equação da reta e da curva são racionais, ao resolver o sistema de modo a achar o ponto restante, constatamos que esse terceiro ponto também é racional. Isto nós dá um meio de calcular mais pontos racionais na curva a partir de pontos conhecidos: criamos retas passando por pontos que já identificamos e buscamos pontos novos na interseção com a cúbica.

Figura 0.1: As retas em azul e em vermelho formam as cúbicas degeneradas E_1 e E_2, respectivamente.



Forma Normal de Weierstrass

A equação completa

$$f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$$

para uma curva elíptica não é prática para fins de realização de cálculos, a grande quantidade de coeficientes deixa desnecessariamente complicado realizar operações explicitamente. Felizmente a equação de toda cúbica sobre um corpo de característica diferente de 2 pode ser reescrita através de transformações birracionais como

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

através de mudanças de variáveis, de forma que exista uma correspondência entre os pontos na cúbica original e na cúbica nova. Se além da característica do corpo ser diferente de 2 ela também for diferente de 3, então há como eliminar o termo x^2, deixando a equação na forma

$$y^2 = x^3 + dx + e$$

Qualquer que seja o caso, os tipos de equações descritas são chamadas de forma de Weierstrass da curva. Vamos descrever como realizar essa transformação para uma cúbica arbitrária, como mostrado em [9].

Iremos trabalhar especificamente sobre o plano projetivo para garantir uma bijeção entre os pontos da curva inicial e a curva na forma de Weierstrass. Suponha que conhecemos um ponto racional P numa cúbica E dada em um sistema de coordenadas (U, V, W) pela equação de terceiro grau

$$F(U,V,W) = aU^3 + bU^2V + cUV^2 + dV^3 + eU^2W + fUVW + gV^2W + \\ + hUW^2 + iVW^2 + jW^3 = 0.$$

O método de determinar a forma de Weierstrass da curva depende se P é um ponto de inflexão ou não.

Caso I) Se P é ponto de inflexão, vamos fixar ele como a origem $\mathcal{O}$, e fazer mudanças de coordenadas para levar este ponto em $(0 : 1 : 0)$, que será a escolha mais conveniente quando formos dar fórmulas explícitas para a operação $+$.

Seja l_P a tangente da curva em P. Podemos escolher um sistema de coordenadas (X, Y, Z) tal que a equação de l_P seja $Z = 0$. Dessa forma, o ponto que vai pra $(1 : 0 : 0) \in \mathbb{P}^2$, que denotaremos por Q, pode ser escolhido como qualquer ponto racional diferente de P sobre a reta. Sejam $(P_U : P_V : P_W)$ e $(Q_U : Q_V : Q_W) \in \mathbb{P}^2$ as coordenadas originais de P e Q sobre a curva; temos a correspondência linear $(U, V, W)^T = M(X, Y, Z)^T$ onde M é a matriz

$$\begin{bmatrix} Q_U & P_U & \cdot \\ Q_V & P_V & \cdot \\ Q_W & P_W & \cdot \end{bmatrix}$$

que representa a mudança de coordenadas projetivas $\alpha : (X, Y, Z) \to (U, V, W)$. Para determinar a última coluna escolhemos qual ponto $R \in \mathbb{P}^2$ vai corresponderá a $(0 : 0 : 1)$ no sistema de coordenadas (X, Y, Z). Podemos escolher qualquer ponto racional, desde que a matriz seja invertível. Tentamos então preencher a coluna com os valores $(1, 0, 0)^T, (0, 1, 0)^T$ ou $(0, 0, 1)^T$. Ela deve ser invertível com ao menos um deles, ou P e Q seriam linearmente dependentes, o que não acontece pois em coordenadas projetivas isto implicaria serem o mesmo ponto.

Completa a matriz, temos U, V e W como funções lineares das novas coordenadas X, Y e Z. A equação original nessas novas coordenadas é da forma

$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$$

Assim como desejado, $\mathcal{O} = (0 : 1 : 0)$ é o único ponto no infinito da curva, isto é, o único ponto sobre a reta $Z = 0$: fazendo $Z = 0$ na equação acima obtemos $X = 0$.

Desomogeneizando a equação da curva, temos

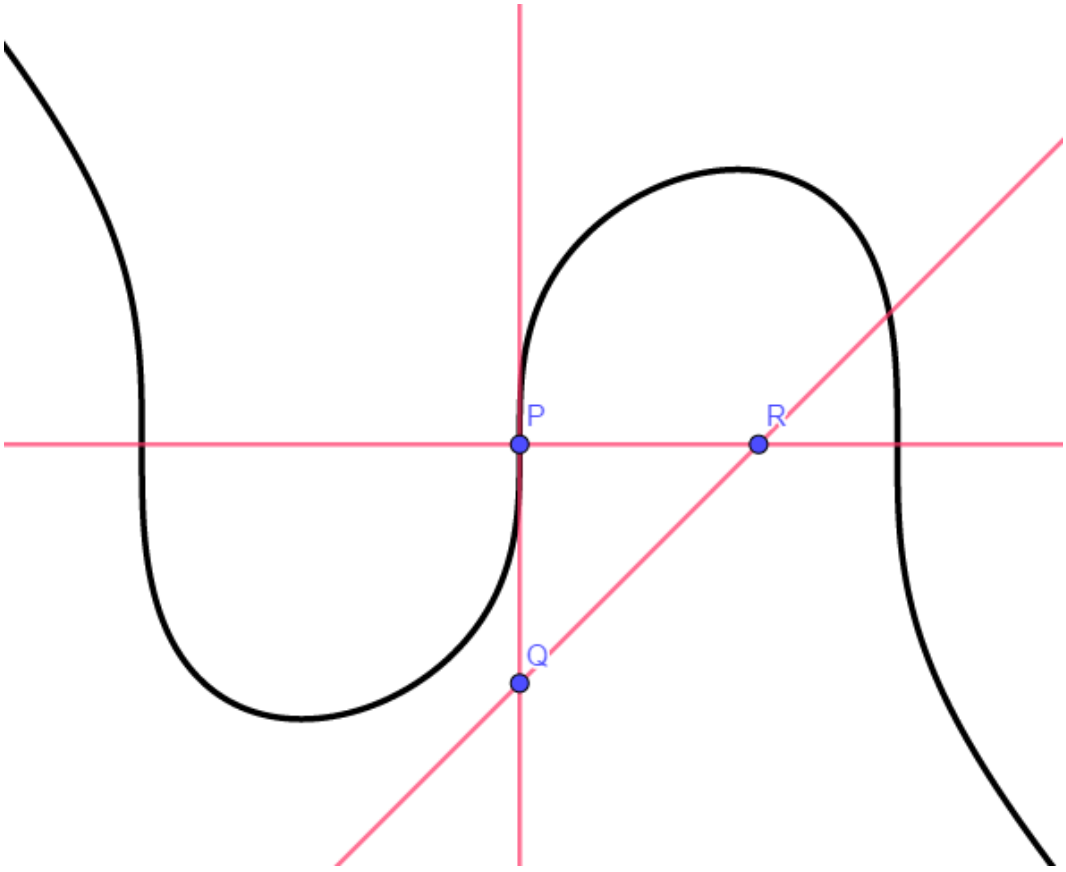
$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

O lado direito é um polinômio cúbico em x, mas precisamos fazer algumas mudanças de coordenada para que o lado esquerdo se torne y^2. Se a característica do corpo é diferente de 2, temos que $y^2 + a_1xy + a_2y = \left(y + \frac{a_1x+a_2}{2}\right)^2 - \frac{a_1^2x^2+2a_1a_2x+a_2^2}{4}$, então completamos quadrados com a substituição $y + \frac{a_1x+a_2}{2} \to y$:

$$y^2 = x^3 + \left(a_3 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_2}{2}\right)x + \left(a_5 + \frac{a_2^2}{4}\right)$$

Por fim, se a característica do corpo for diferente de 3 podemos eliminar o termo x^2 fazendo a substituição $x \to x - \frac{1}{3}\left(a_3 + \frac{a_1^2}{4}\right)$.

Figura 0.2: Exemplo da escolha de pontos quando P é ponto de inflexão



Exemplo 6.1. Começamos com a curva cúbica E dada for $g(u, v) = u^3 + v^3 - 1 = 0$ sobre um corpo de característica diferente de 3. Sua forma homogênea é $G(U, V, W) =$

$U^3 + V^3 - W^3$. Verificamos que o ponto $P = (1 : -1 : 0)$ está na curva. A tangente a esse ponto é dada por

$$\begin{aligned} 0 = \frac{\partial F}{\partial U}(P)(U-1) + \frac{\partial F}{\partial V}(P)(V+1) + \frac{\partial F}{\partial U}(P)(W) \\ = 3(U-1) + 3(V+1) + 0(W) \\ = 3U + 3V \end{aligned}$$

Simplificando, $U + V = 0$ é a reta tangente no ponto. Para encontrar as interseções da reta com a curva, substituímos $V = -U$, obtendo

$$\begin{aligned} &- U^3 + U^3 - W^3 = 0 \\ &\Rightarrow W = 0 \end{aligned}$$

Portanto P é um ponto de inflexão. Definimos uma mudança de coordenadas que o leva a $\mathcal{O} = (0 : 1 : 0)$. Isso significa fazer os eixos $Z = 0$ e $X = 0$ passarem por ele.

Tomamos então outro ponto Q sobre essa reta distinto de P, por exemplo $Q = (0 : 0 : 1)$. Escolhemos a transformação de forma que Q seja levado em $(1 : 0 : 0)$. Temos então uma matriz de mudança de coordenadas:

$$(U, V, W)^T = \begin{bmatrix} 0 & 1 & \cdot \\ 0 & -1 & \cdot \\ 1 & 0 & \cdot \end{bmatrix} (X, Y, Z)^T,$$

onde ainda iremos escolher a última coluna, que deve ser escolhida de forma que a matriz seja invertível. Escolhemos completá-la da seguinte maneira:

$$\begin{bmatrix} 0 & 1 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

Ou seja, $(U, V, W) \to (Y + Z, -Y, X)$. Substituindo na equação,

$$\begin{aligned} (Y+Z)^3 + (-Y^3) - X^3 = 0 \\ -X^3 + 3Y^2Z + 3YZ^2 + Z^3 = 0, \end{aligned}$$

realizando a desomogeneização $(x, y) = (X/Z, Y/Z)$,

$$1 + 3y + 3y^2 = x^3$$

dividindo por 3,

$$\frac{1}{3} + y + y^2 = \frac{x^3}{3}$$

completando quadrados,

$$\left(y + \frac{1}{2}\right)^2 = \frac{x^3}{3} - \frac{1}{12}$$

e renomeando $y + \frac{1}{2}$ como y, obtemos

$$y^2 = \frac{x^3}{3} - \frac{1}{12}.$$

Precisamos então que o coeficiente de x^3 seja 1. Então fazemos as mudanças $x \to \frac{x}{3}$, $y \to \frac{y}{9}$ e multiplicamos os dois lados da equação por 81, obtemos

$$y^2 = x^3 - \frac{27}{4}$$

Para conseguirmos todos os denominadores como números inteiros, fazemos a aplicação $x \to \frac{x}{4}$, $y \to \frac{y}{8}$ e multiplicamos a equação por 64 para chegar na forma de Weierstrass: $y^2 = x^3 - 432$.

Caso II) Caso o ponto P não seja um ponto de inflexão, a reta tangente l_P intersecta a curva em um outro ponto Q. Tomamos a reta tangente l_Q nesse ponto da curva neste ponto. Definimos então um ponto R tomando qualquer reta r distinta de l_P passando por P, e encontrando a sua interseção com l_Q, que é a reta tangente à curva em Q.

Definimos as novas coordenadas X, Y e Z de forma que l_P, l_Q e r se tornem as retas $Z = 0$, $X = 0$ e $Y = 0$. Isso é equivalente à aplicação $P \to (1 : 0 : 0)$, $Q \to (0 : 1 : 0)$ e $R \to (0 : 0 : 1)$. Temos então a correspondência

$$(U, V, W)^T = \begin{bmatrix} P_U & Q_U & R_U \\ P_V & Q_V & R_V \\ P_W & Q_W & R_W \end{bmatrix} (X, Y, Z)^T.$$

Esta matriz é sempre invertível porque os pontos não são colineares. Temos então as coordenadas originais U, V e W como funções lineares de X, Y e Z:

$$\begin{aligned} U &= P_U X + Q_U Y + R_U Z \\ V &= P_V X + Q_V Y + R_V Z \\ W &= P_W X + Q_W Y + R_W Z. \end{aligned}$$

Substituindo essas relações na equação $F(U, V, W) = 0$, obtemos a equação da curva E', que corresponde à curva E nas novas coordenadas e é dado por uma equação

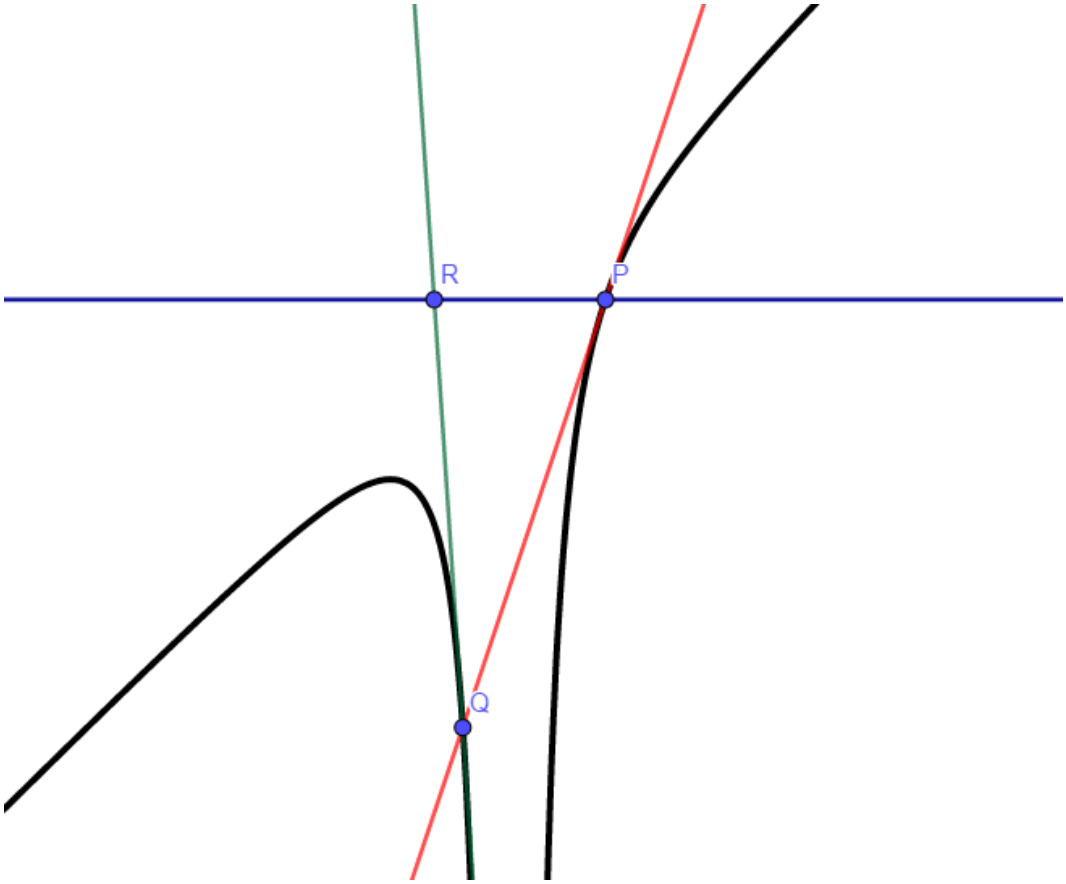
$$F'(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eZ \cdot G(X, Y, Z) = 0,$$

onde $G(X, Y, Z)$ é um polinômio homogêneo de grau 2. Nesta equação a, b e d são nulos, pois

i) $P = (1 : 0 : 0) \in E'$, logo $F'(1, 0, 0) = a = 0$.

ii) $Q = (0 : 1 : 0) \in E'$, logo $F'(0, 1, 0) = d = 0$.

Figura 0.3: Exemplo da escolha de pontos quando P não é ponto de inflexão



iii) A interseção da reta $Z = 0$ com a curva E' são os pontos P, com multiplicidade 2, e Q. Esses pontos devem ser as raízes da equação $F'(X, Y, 0) = 0$. Como já sabemos que $a = d = 0$, podemos escrever $F'(X, Y, 0) = XY(bX + cY) = 0$, onde cada fator linear corresponde a um ponto de interseção. Como Q satisfaz $X = 0$, P deve satisfazer $Y = 0$ e $bX + cY = 0$. Isto implica $b = 0$.

Portanto, a equação assume a forma

$$cXY^2 + eZ \cdot G(X, Y, Z) = 0,$$

que ao ser desomogeneizada, pode ser rescrita como

$$xy^2 + (a'x + b')y = c'x^2 + d'x + e'.$$

Multiplicando os dois lados por x, obtemos

$$(xy)^2 + (a'x + b')xy = \text{polinômio cúbico em } x,$$

onde usando a aplicação birracional $xy \mapsto y$, temos

$$y^2 + (ax + b)y = \text{cúbica em } x.$$

Finalmente, substituindo y por $y - \frac{1}{2}(ax+b)$ e completando o quadrado do lado esquerdo chegamos a

$$y^2 = \text{cúbica em } x.$$

Se por acaso o termo x^3 no lado direito tiver um coeficiente $\lambda \neq 1$, só precisamos trocar x e y por λx e $\lambda^2 y$, respectivamente, e depois simplificar. Se a característica do corpo for diferente de 3, então também é possível sumir com o termo x^2 substituindo x por $x - \alpha$ para um α apropriado.

Exemplo 6.2. Para um exemplo do segundo caso, tomamos a cúbica $u^3 - u^2 v - 1 = 0$, que corresponde à curva projetiva $U^3 - U^2V - W^3 = 0$. Observe que o ponto racional $P = (1:0:1)$ pertence à curva. A reta tangente nesse ponto é $3U - V - 3W = 0$. O ponto P não é de inflexão, pois essa tangente intersecta a curva no ponto $Q = (-\frac{1}{2} : -\frac{9}{2} : 1)$.

A tangente à curva em Q é $15U + V + 12W = 0$. Escolhemos $R = (-\frac{4}{5} : 0 : 1)$ sobre essa reta.

Definimos então a transformação

$$(U,V,W)^T = \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{4}{5} \\ 0 & -\frac{9}{2} & 0 \\ 1 & 1 & 1 \end{bmatrix} (X,Y,Z)^T.$$

Da qual obtemos a correspondência linear $(U,V,W) = (X - \frac{Y}{2} - \frac{4Z}{5}, -\frac{9Y}{2}, X + Y + Z)$. Substituindo as expressões em $U^3 - U^2V - W^3 = 0$, obtemos

$$\left(X - \frac{Y}{2} - \frac{4Z}{5}\right)^3 - \left(X + \frac{Y}{2} - \frac{4Z}{5}\right)^2 \left(-\frac{9Y}{2}\right) - (X+Y+Z)^3 = 0,$$

$$-\frac{27}{4}XY^2 - \frac{27}{5}X^2Z - \frac{54}{5}XYZ - \frac{27}{25}XZ^2 - \frac{27}{25}YZ^2 - \frac{189}{125}Z^3 = 0.$$

Desomogeneizamos para obter

$$\begin{aligned} xy^2 + \frac{4}{5}x^2 + \frac{8}{5}xy + \frac{4}{25}x + \frac{4}{25}y + \frac{28}{125} &= 0, \\ xy^2 + \left(\frac{8}{5}x + \frac{4}{25}\right)y &= -\frac{4}{5}x^2 - \frac{4}{25}x - \frac{28}{125}, \\ (xy)^2 + \left(\frac{8}{5}x + \frac{4}{25}\right)xy &= -\frac{4}{5}x^3 - \frac{4}{25}x^2 - \frac{28}{125}x. \end{aligned}$$

Fazendo a aplicação $xy \to y$, temos

$$y^2 + \left(\frac{8}{5}x + \frac{4}{25}\right)y = -\frac{4}{5}x^3 - \frac{4}{25}x^2 - \frac{28}{125}x.$$

Somamos $\frac{1}{4}\left(\frac{8}{5}\,x+\frac{4}{25}\right)^2$ de ambos os lados e completamos quadrados para obter

$$\left(y+\frac{1}{2}\left(\frac{8}{5}\,x+\frac{4}{25}\right)\right)^2=-\frac{4}{5}\,x^3+\frac{12}{25}\,x^2-\frac{12}{125}\,x+\frac{4}{625}.$$

Substituimos $y+\frac{1}{2}\left(\frac{8}{5}\,x+\frac{4}{25}\right)\to y$ e obtemos

$$y^2=-\frac{4}{5}\,x^3+\frac{12}{25}\,x^2-\frac{12}{125}\,x+\frac{4}{625}.$$

Em seguida trocamos x e y por $-\frac{4}{5}x$ e $\frac{16}{25}y$ respectivamente, e depois simplificamos:

$$y^2=x^3+\frac{3}{4}\,x^2+\frac{3}{16}\,x+\frac{1}{64}.$$

Podemos simplificar removendo o termo x^2 ao substituir x por $x-\frac{1}{4}$. Temos então simplesmente $y^2=x^3$, a cúspide.

Fórmulas para a operação na forma de Weierstrass

Afirmamos anteriormente que a forma de Weierstrass facilita o cálculo explicito de somas de pontos, e agora veremos como estes cálculos são feitos. Começamos pelo problema de somar dois pontos em uma curva elíptica dada por uma equação da forma $y^2=x^3+ax^2+bx+c$. Para facilitar o cálculos escolhemos uma origem $\mathcal{O}$ que torne a operação $(P*Q)*\mathcal{O}$ trivial. Para isso homogeneizamos a curva no espaço projetivo, obtendo a equação

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

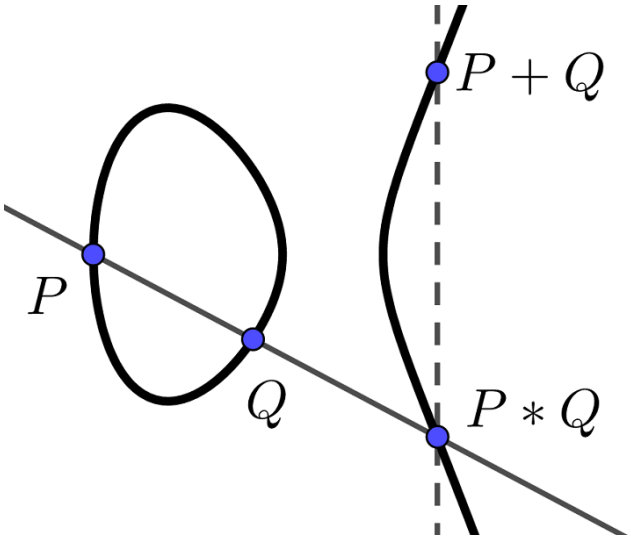
Podemos então fazer a escolha de $\mathcal{O}$ como $(0:1:0)$, que satisfaz a equação acima. A vantagem dessa escolha é que para qualquer ponto P sobre a curva, $P*\mathcal{O}$ será apenas uma reflexão pelo eixo x. Assim, para calcular uma soma $P+Q$, só precisamos encontrar $P*Q$ e depois inverter o sinal da sua ordenada.

Para encontrar uma fórmula explícita para a soma, tomamos dois pontos $P_1=(x_1,y_1)$ e $P_2=(x_2,y_2)$, com $x_1\neq x_2$. A reta que liga os dois é dada por $y=\lambda x+\delta$, onde $\lambda=\frac{y_2-y_1}{x_2-x_1}$ e $\delta=y_1-\lambda x_1$. Para encontrar os pontos de interseção dessa reta com a curva, substituímos y por $y=\lambda x+\delta$ na equação da curva, obtendo a seguinte equação em x:

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

Sejam x_1, x_2 e x_3, possivelmente com repetição, as soluções desta equação, sendo x_1 e x_2 as abscissas de P e Q respectivamente, e x_3 a abscissa da soma que procuramos. Temos então,

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



Algumas operações (confira a seção 1.4 de [4]) nos levam à seguinte solução:

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

$$y_3 = \lambda x_3 + \delta$$

Notamos que esta fórmula só funciona se os pontos são diferentes. No caso em que somamos um ponto com ele mesmo, então usamos a reta tangente à curva no ponto ao invés da secante entre dois pontos. Escrevendo $y^2 = f(x)$, temos que a inclinação da reta tangente da curva no ponto $P = (x, y)$ é dada por

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

Fazendo um processo análogo ao usado anteriormente, mas substituindo $\lambda = \frac{f'(x)}{2y}$ em $x_3 = \lambda^2 - x_1 - x_2$, encontramos a abscissa do ponto $2P$, através da expressão, chamada fórmula da duplicação:

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

Grupo dos pontos racionais

Anteriormente vimos que a operação + definida torna o conjunto dos pontos de uma curva elíptica um grupo abeliano. Queremos agora provar que o conjunto dos pontos racionais $E(\mathbb{Q})$ é finitamente gerado. Para isto provaremos um resultado mais forte sobre uma classe de grupos à qual $E(\mathbb{Q})$ pertence.

Grupos normados e geração finita

Seja G um grupo abeliano e normado. Adotando uma notação aditiva, para cada n natural temos uma aplicação de grupos

$$\begin{aligned}[n] : G &\to G \\ g &\to ng.\end{aligned}$$

onde $ng = g + \cdots + g$ somado n vezes.

Definição 7. Um grupo G é dito normado se existe uma função $h : G \to \mathbb{R}_{\geq 0}$ com as seguintes propriedades:

i) Para cada $r \in \mathbb{R}_{\geq 0}$ o conjunto $H(r) := \{P \in G | h(P) \leq r\}$ é finito.

ii) $h(mP) = |m|^2 h(P)$ para todo $P \in G$ e $m \in \mathbb{Z}$.

iii) $h(P+Q) + h(P-Q) = 2h(P) + 2h(Q)$, também conhecida como de regra do paralelogramo.

A função h que satisfaz essas condições é chamada de função altura em G.

Teorema 8. *Seja G um grupo abeliano. Suponha que G é um grupo normado e que $[G : 2G]$ é finito. Então G é finitamente gerado.*

Demonstração. Seja h a função altura de G. Denotamos o subgrupo de torção de G por $G_{tor} := \{g \in G : ng = 0, n \in \mathbb{Z}\}$. Para qualquer $g \in G_{tor}$, como $ng = 0$ temos que $0 = h(0) = h(ng) = |n|h(g)$. Isto implica que $h(g) = 0$ e portanto $G_{tor} \subseteq H(0)$. Pelo item (i) da definição de um grupo normado, temos que $\#H(0)$ é finito. Logo, $\#G_{tor} < \infty$.

Seja $G/2G = \{P_1, \ldots, P_k\}$. Denote $\alpha := \max\{h(\bar{P_1}), \ldots, h(\bar{P_k})\} + 1$. Pela primeira propriedade de um grupo normado, temos que $H(\alpha)$ é um conjunto finito. Seja S o subgrupo gerado pelos pontos de $H(\alpha)$. Afirmamos que $S = G$, isto é, $H(\alpha)$ gera G.

Suponhamos por absurdo que esta afirmação não seja verdade. Há então um $P \in G \setminus S$. Seja $\beta := h(P)$ e tomemos $R \in H(\beta) \cap (G \setminus S)$ com $h(R) \leq h(P) \quad \forall P \in H(\beta)$. Podemos assim supor que o P é o elemento com menor altura que não está em S. Mas $\bar{P} = \bar{P_j}$ para algum $\bar{P_j}$ em $G/2G$. Portanto $\exists Q \in G$ tal que $P = P_j + 2Q$ e $2Q = P_j - P$. Daí,

$$\begin{aligned}4h(Q) &= h(2Q) \\ &= h(P_j - P) \\ &= 2h(P_j) + 2h(P) - h(P_j + P) \\ &\leq 2\alpha + 2h(P) < 4h(P),\end{aligned}$$

o que implica que $h(Q) < h(P)$ e contradiz a minimalidade de P, completando a demonstração. □

Estando provado que grupos normados são finitamente gerados, resta mostrar que o grupo $E(\mathbb{Q})$ possui uma função que o torna normado. Para isto, vamos definir explicitamente uma função que satisfaça as condições mencionadas na definição 7.

Definição 9.

a) Seja $a/b \in \mathbb{Q}^*$ uma fração reduzida. Definimos sua "pseudo-altura"por $H(a/b) := \max(|a|, |b|)$, e sua altura logarítmica por $h(a/b) := \log(H(a/b))$.

b) Seja $P \in E(\mathbb{Q})$. Se $P \neq \mathcal{O}$, então P pode ser representado por $(x : y : 1)$ a função altura logarítmica $\widetilde{h}$ em $E(\mathbb{Q})$ será definida por:

$$\widetilde{h}(\mathcal{O}) = 0 \quad e \quad \widetilde{h}(P) = h(x)$$

c) Seja G um grupo abeliano. Dizemos que uma aplicação $f : G \longrightarrow \mathbb{R}_{\geq 0}$ é **discreta** se $\forall r \in \mathbb{R}$ o conjunto $\{\alpha \in G | f(\alpha) < r\}$ é finito.

Para cada $n \in \mathbb{R}$ o conjunto $\{\alpha \in \mathbb{Q} | h(\alpha) < n\}$ é finito, pois existe um número finito de naturais m tais que $m < n$. Segue que

$$\{P \in E(\mathbb{Q}) | \tilde{h}(P) < n\}$$

também é finito. Portanto a função $\tilde{h}$ em $E(\mathbb{Q})$ é discreta.

Lema 10. *Existe uma constante $c \in \mathbb{R}_{\geq 0}$ tal que para qualquer $P, Q \in E(\mathbb{Q})$ temos*

$$|\tilde{h}(P+Q) + \tilde{h}(P-Q) - 2\tilde{h}(P) - \tilde{h}(Q)| \leq c$$

Demonstração. Veja [7, pág. 218]. □

Proposição 11. *Seja E uma curva elíptica sobre $\mathbb{Q}$. Existe uma função $\sigma : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$ que satisfaz as seguintes propriedades:*

i) $\sigma(P) \geq 0 \quad \forall P \in E(\mathbb{Q})$.

ii) Existe uma constante $r \in \mathbb{R}_{\geq 0}$ tal que $\left|\sigma(P) - \frac{1}{2}\tilde{h}(P)\right| < r$.

iii) σ é discreta.

iv) $\sigma(P+Q) + \sigma(P-Q) = 2\sigma(P) + 2\sigma(Q) \quad \forall P, Q \in E(\mathbb{Q})$.

v) $\sigma(mP) = m^2\sigma(P) \quad \forall P \in E(\mathbb{Q})$.

vi) $\sigma(P) = 0$ *se e apenas se* $P \notin E(\mathbb{Q})_{tor}$.

E portanto σ é uma norma sobre $E(\mathbb{Q})$.

Demonstração. Definimos a função

$$\delta(P) := \lim_{n \to \infty} \frac{\tilde{h}(2^n P)}{4^n}.$$

Queremos provar que $\sigma(P) := \frac{1}{2}\delta(P)$ é uma norma para $E(\mathbb{Q})$. O primeiro passo é mostrar que o limite na definição de δ existe para qualquer ponto. Aplicando o item (a) da Definição 9 temos a igualdade.

$$\frac{\tilde{h}(2^n P)}{4^n} = \tilde{h}(P) + \sum_{k=1}^{n} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))$$

Fazendo $P = Q$ no Lema 10, temos que $\exists c \in \mathbb{R}_{\geq 0}$ tal que $|\tilde{h}(2P) - 4\tilde{h}(P)| < c$ para todo ponto $P \in E(\mathbb{Q})$. Consequentemente,

$$\begin{aligned} \frac{1}{4^k}\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P) &\leq \frac{1}{4^k}\left|\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P)\right| \\ &< \frac{1}{4^k}c, \end{aligned}$$

e portanto a expressão $\sum_{k=1}^{n} \frac{1}{4^k}\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P)$ converge pelo teste da comparação e a função é bem definida. Vamos agora provar que a função atende a todas as propriedades do enunciado.

i) Por definição, $\sigma(P) = \frac{1}{2}\delta(P)$. Por sua vez $\delta(P)$ é definido como o limite de uma sequência de valores positivos, o que implica $\sigma(P) \geq 0$ para todo $P \in E(\mathbb{Q})$.

ii) Temos

$$\left|\sigma(P) - \frac{1}{2}\tilde{h}(P)\right| = \frac{1}{2}|\delta(P) - \tilde{h}(P)|.$$

Como $\frac{\tilde{h}(2^n P)}{4^n} = \tilde{h}(P) + \sum_{k=1}^{n} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))$, então

$$\begin{aligned} \left|\delta(P) - \tilde{h}(P)\right| &\leq \left|\sum_{k=1}^{\infty} \frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))\right| \\ &\leq \sum_{k=1}^{\infty} \left|\frac{1}{4^k}(\tilde{h}(2^k P) - 4\tilde{h}(2^{k-1}P))\right| \\ &\leq \sum_{k=1}^{n} \frac{1}{4^k}c \\ &< \frac{c}{3}, \end{aligned}$$

e portanto $\left|\sigma(P) - \frac{1}{2}\tilde{h}(P)\right| < c/6$.

iii) Suponhamos que $\sigma(P) < r$ para algum $r \in \mathbb{R}$. Usando o resultado anterior, temos

$$\frac{1}{2}\tilde{h}(P) < \sigma(P) + \frac{c}{6} < r + \frac{c}{6}.$$

Como $\tilde{h}$ é uma função discreta, os valores de P que satisfazem a condição são finitos, e portanto a função σ também é discreta.

iv) Pelo Lema 10 afirmamos que

$$\frac{1}{4^n}\left|\tilde{h}(2^n(P+Q)) + \tilde{h}(2^n(P-Q)) - 2\tilde{h}(2^nP) - 2\tilde{h}(2^nQ)\right| < \frac{c}{4^n}.$$

O limite desta expressão quando $n \to \infty$ nos dá a regra do paralelogramo

$$\sigma(P+Q) + \sigma(P-Q) = 2\sigma(P) + 2\sigma(Q).$$

v) Faremos indução sobre m. Para $m = 2$ temos

$$\begin{aligned}\delta(2P) &= \lim_{k\to\infty} \frac{1}{4^k}\tilde{h}(2^{k+1}P) \\ &= 4 \cdot \lim_{k\to\infty} \frac{1}{4^{k+1}}\tilde{h}(2^{k+1}P) \\ &= 4\delta(P).\end{aligned}$$

Assim $\sigma(2P) = 4\sigma(P)$. Então seja $m \in \mathbb{N}$ e suponha por hipótese de indução que $\sigma(kP) = k^2\sigma(P)$ para todo k natural menor ou igual a m. Pela regra do paralelogramo temos que

$$\sigma((m+1)P) = \sigma(mP + P) = 2\sigma(mP) + 2\sigma(P) - \sigma((m-1)P),$$

e então pela hipótese de indução temos

$$\begin{aligned}2\sigma(mP) + 2\sigma(P) - \sigma((m-1)P) &= 2m^2\sigma(P) + 2\sigma(P) - (m-1)^2\sigma(P) \\ &= (2m^2 + 2 - (m-1)^2)\sigma(P) \\ &= (m+1)^2\sigma(P).\end{aligned}$$

vi) Seja $P \in E(\mathbb{Q})_{tor}$, $P \neq \mathcal{O}$. Isto é, $nP = \mathcal{O}$ para algum $n > 1$. Temos

$$n^2\sigma(P) = \sigma(nP) = 0 \Rightarrow \sigma(P) = 0.$$

Reciprocamente suponha que $\sigma(P) = 0$ e considere o conjunto dos múltiplos de P,

$$S := \{nP : n \in \mathbb{N}\}.$$

Já que $\sigma(nP) = 0$, então $S \subset \{P' \in E(\mathbb{Q}) : \sigma(P') = 0\}$. Como a função σ é discreta, então S é finito. Isto implica que P tem ordem finita.

Concluímos que a função σ define uma norma no grupo $E(\mathbb{Q})$. □

Corolário 12. ***Teorema de Mordell.*** *Seja E uma curva elíptica sobre $\mathbb{Q}$. A operação $+$ de soma torna $E(\mathbb{Q})$ um grupo abeliano finitamente gerado.*

Demonstração. Há uma prova de que $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ é finito na seção 2.4 do livro [4]. Assim, como a Proposição 11 nos diz que $E(\mathbb{Q})$ é normado, o corolário vem aplicação do Teorema 8. □

A demonstração anterior serve para curvas elípticas definidas sobre $\mathbb{Q}$. Para uma curva elíptica $E/\mathbb{F}_q$, o grupo $E(\mathbb{F}_q)$ é claramente finitamente gerado, pois é finito.

Teorema da estrutura dos grupos abelianos finitamente gerados

Agora que foi mostrado que o grupo dos pontos racionais de uma curva elíptica é abeliano e finitamente gerado, veremos como último resultado deste capítulo um resultado importante que nos permite representar esse grupo como somas diretas de grupos cíclicos.

Teorema 13. *Todo grupo abeliano finitamente gerado é isomorfo a um grupo da*

$$\mathbb{Z}^r \bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{(p_i^{e_i})}, \quad k, e_1, \ldots, e_k \in \mathbb{Z}_{>0},$$

onde cada p_i é um número primo, possivelmente com repetição entre eles. Esta representação é única a menos da ordem das somas.

Demonstração. Veja o Teorema B.4 em [7]. □

Em particular este Teorema se aplica às estruturas de grupo de curvas elípticas sobre $\mathbb{Q}$ ou corpos finitos, já que o grupo dos pontos racionais sobre estes corpos é finitamente gerado. Observamos ainda que se o grupo abeliano é finito, então os primos p_i são os primos que dividem a cardinalidade do grupo.

2 Pontos racionais e criptografia

De agora em diante iremos trabalhar com curvas elípticas sobre corpos finitos. Implicitamente sempre assumiremos que a curva está em um plano projetivo sobre este corpo, mas para denotar qualquer ponto iremos usar as suas coordenadas afins, a menos que ele esteja na reta do infinito. Além disso, a origem será sempre o ponto projetivo $\mathcal{O} = (0 : 1 : 0)$.

Corpos finitos sempre têm cardinalidade igual a uma potência de um primo. Denotamos por p o primo, $q = p^n$ a cardinalidade do corpo, onde n é um inteiro positivo, e por $\mathbb{F}_q$ o corpo finito com q elementos, que é uma extensão de grau n de $\mathbb{F}_p$. Ao operar sobre corpos finitos, perdemos a capacidade de visualizar a equação cúbica como uma "curva", como estamos acostumados. O gráfico dos pontos racionais se torna um conjunto finito de pontos, mas as propriedades de grupo se preservam.

Definição 14. Seja $E/\mathbb{F}_q$ a curva elíptica sobre $\mathbb{F}_q$ definida por uma equação $F(x, y) = 0$. Denotamos os seus pontos racionais, isto é, a valores em $\mathbb{F}_q$ por

$$E(\mathbb{F}_q) := \{(x, y) : x, y \in \mathbb{F}_q, F(x, y) = 0\}.$$

Como estamos trabalhando sobre corpos finitos, surge a possibilidade de listar todos os pontos racionais. Algoritmos que tenham execução rápida em um computador, de preferência sem ultrapassar a capacidade de memória do aparelho, são preferíveis. O método de força bruta para listar pontos racionais é simplesmente pegar cada ponto com coordenadas em $\mathbb{F}_q$ e testar se $F(x, y) = 0$. Na proposição a seguir mostramos um método que faz o mesmo com menos cálculos.

Proposição 15. *Seja $E : y^2 = f(x)$ uma curva elíptica sobre $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, onde $p \neq 2$ e α é um elemento algébrico de grau n. Todo elemento de $\mathbb{F}_q$ pode ser escrito como $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ onde os a_i's estão em $\mathbb{F}_p$. O seguinte algoritmo nos permite encontrar todos os pontos racionais diferentes da origem $\mathcal{O}$ na curva.*

i) Fazemos duas listas A e B. Na lista A colocamos y^2 para todo $y = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$ onde $0 \leq a_0 \leq \lfloor \frac{p}{2} \rfloor$ e os demais a_i's assumem todos os valores em $\mathbb{F}_p$. Na lista B colocamos o valor de $f(x)$ para cada $x \in \mathbb{F}_q$.

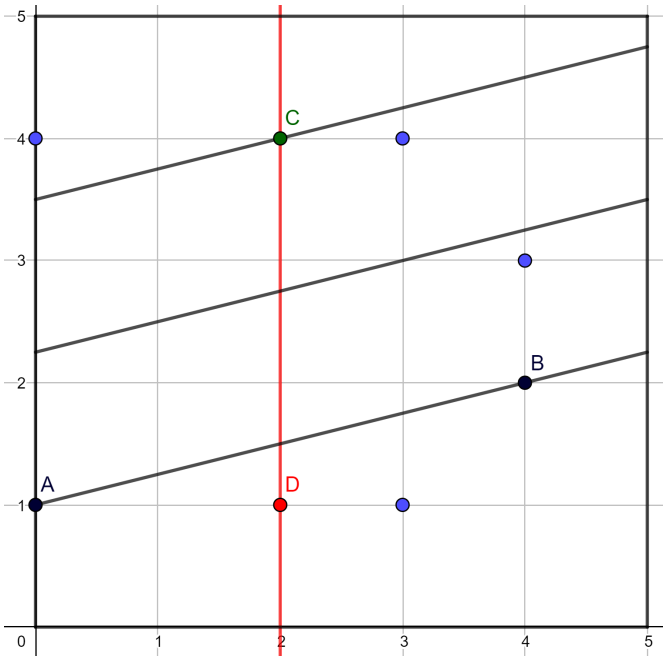
ii) Comparamos os valores em A e B. Cada coincidência nos dá um y e um x tais que $y^2 = f(x)$. Adicionamos o ponto (x, y) aos nossos resultados, e se $y \neq 0$ adicionamos também $(x, -y)$.

Demonstração. Achar todas as correspondências de y^2 e $f(x)$ para valores de x e y em $\mathbb{F}_q$ é evidentemente suficiente. A escolha de iterar os a_0 apenas entre 0 e $\lfloor \frac{p}{2} \rfloor$ vem do fato de que se (x, y) satisfaz $y^2 = f(x)$, então $(x, -y)$ também satisfaz. Podemos então calcular apenas metade dos valores de y e usar esta simetria para diminuir o número de comparações pela metade.

Notamos que esta simetria só é perfeita se o primo p é diferente de 2. No caso em que $p = 2$ o algoritmo é semelhante, mas a_0 assume todos os valores em $\mathbb{F}_p$ e ao achar uma correspondência adicionamos apenas o ponto encontrado. □

Para somar dois pontos $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, assim como no caso geral definimos $P+Q$ como (x_3, y_3), onde $x_3 = \lambda^2 - a - x_1 - x_2$, $y_3 = -\lambda x_3 - \delta$, com coeficientes calculados sobre $\mathbb{F}_q$. Em todas as aplicações que serão apresentadas nesta parte usaremos apenas corpos da forma $\mathbb{F}_p$ identificados com o conjunto dos inteiros módulo p, simplificando os cálculos.

Figura 0.4: Na curva $E : y^2 = x^3 + 1$ sobre $\mathbb{F}_5$, a soma dos pontos A e B é o ponto D.



Exponenciação e soma rápidas

Nas aplicações que serão descritas nos deparamos com um problema: em alguns momentos temos que calcular o valor de uma potência módulo algum número, algo do tipo $a^k \bmod n$, sendo que k e n podem ser muito grandes. Tentar calcular a^k e depois tirar o módulo é ineficiente, pois o valor de a^k cresce de maneira exponencial. Tentar a cada etapa multiplicar por a e depois tirar o módulo evita este crescimento, mas também não é um algoritmo eficiente, pois o número de operações é linear com k, que pode ser muito grande.

Vamos apresentar um método que opera em tempo logarítmico com o tamanho de k. Primeiro representamos k na forma binária:

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \cdots + k_{s-1} \cdot 2^{s-1} + k_s \cdot 2^s$$

onde cada k_i é igual a 0 ou 1. Em seguida calculamos as constantes $A_0 := a, A_1 := A_0^2, A_2 := A_1^2, \ldots, A_s := A_{s-1}^2$ módulo n. Por fim, $a^k \bmod n$ é obtido como

$$a^k = \prod_{i=0,\, k_i=1}^{s} A_i.$$

Um problema análogo é calcular kP numa curva, os seja, como somar um ponto com ele mesmo k vezes. Como antes, primeiro calculamos a representação binária $k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \cdots + k_{s-1} \cdot 2^{s-1} + k_s \cdot 2^s$ de k. Usamos a fórmula de dobrar pontos para calcular $P_0 = P, P_1 = 2P_0, P_2 = 2P_1, \ldots, P_s = 2P_{s-1}$. Por fim só precisamos somar os pontos:

$$kP = \bigoplus_{i=0,\, k_i=1}^{s} P_i.$$

Algoritmo de Cipolla

Consideremos o conjunto dos pontos racionais $E(\mathbb{F}_p)$ de uma curva elíptica sobre $\mathbb{F}_p$, dada por um equação na forma de Weierstrass $y^2 = f(x)$.

Para uma abscissa $x \in \mathbb{F}_p$ podemos nos perguntar se existe alguma ordenada y tal que (x, y) está em $E(\mathbb{F}_p)$, e se existe, quantas e quais são. Seja $c := f(x_0)$ para um x_0 fixo, o problema de determinar a existência de uma ordenada se reduz a encontrar um y tal que

$$y^2 \equiv c \bmod p.$$

Para saber se isso é possível usamos o símbolo de Legendre:

Definição 16. Para cada $c \in \mathbb{F}_p$ definimos seu símbolo de Legendre como

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{se } c \text{ é um quadrado,} \\ -1 & \text{se } c \text{ não é um quadrado,} \\ 0 & \text{se } c = 0. \end{cases}$$

Proposição 17. *Para $c \in \mathbb{F}_p$, a fórmula explícita do símbolo de Legendre é*

$$\left(\frac{c}{p}\right) = c^{(p-1)/2}.$$

Demonstração. Veja [7, § 5.3.2] □

Desta forma, para saber se x_0 existe como a abscissa de um ponto só precisamos calcular o símbolo de Legendre de $c = f(x_0)$. Notamos que se $c = 0$ a única escolha para y é 0, mas se $y^2 = c$ com $c \neq 0$, então temos uma segunda raiz distinta $-y$. Solucionada a questão da existência ou não da raiz, resta saber como encontrá-la quando ela existe. Disto se trata o algoritmo de Cipolla.

Teorema 18. ***Algoritmo de Cipolla.*** *Suponhamos que a congruência*

$$y^2 \equiv c \ mod \ p$$

admita solução. O seguinte algoritmo calcula os possíveis valores para y:

i) Por tentativa e erro encontre um $a \in \mathbb{F}_p$ tal que $a^2 - c$ não seja um quadrado.

ii) As soluções possíveis são $y = \pm(a + \sqrt{a^2 - c})^{(p+1)/2}$.

Demonstração. Observamos que apesar do passo (i) consistir em achar um valor não quadrado através de tentativa e erro, este passo geralmente é bem rápido. O número de elementos de $\mathbb{F}_p$ com símbolo de Legendre -1 é $(p-1)/2$, logo a probabilidade de que um a qualquer satisfaça a condição é $\frac{p-1}{2p} \sim \frac{1}{2}$. Devemos então esperar uma média de 2 tentativas para achar um a que sirva.

Vamos provar que $(a + \sqrt{a^2 - c})^{(p+1)/2}$ é uma solução. Denotando $w := \sqrt{a^2 - c}$, observamos que este valor está na extensão $\mathbb{F}_{p^2} = \mathbb{F}_p(w)$. Então para qualquer valor $b \in \mathbb{F}_p$ temos em característica p que

$$\begin{aligned}(b + w)^p &= b^p + w^p \\ &= b + w^p \\ &= b - w,\end{aligned}$$

pois como $w^2 = a^2 - c$ não é um quadrado em $\mathbb{F}_p$, então $\left(\frac{w^2}{p}\right) = w^{p-1} = -1$. Assim,

$$\begin{aligned}((a + \sqrt{a^2 - c})^{(p+1)/2})^2 &= (a + \sqrt{a^2 - c})^{p+1} \\ &= (a + \sqrt{a^2 - c}) \cdot (a + \sqrt{a^2 - c})^p \\ &= (a + \sqrt{a^2 - c}) \cdot (a - \sqrt{a^2 - c}) \\ &= a^2 - a^2 + c \\ &= c.\end{aligned}$$

Portanto $y = (a + \sqrt{a^2 - c})^{(p+1)/2}$ é uma solução. A outra solução é exatamente $-y$. □

Sistema ElGamal

Nesta seção descrevemos um sistema criptográfico que utiliza curvas elípticas sobre corpos finitos. Seja E uma curva elíptica dada por uma equação na forma de Weierstrass $y^2 = f(x)$ sobre o corpo finito $\mathbb{F}_p$, onde p é um primo. Escolhemos um ponto $P \in E(\mathbb{F}_p)$ que gere um subgrupo grande de $E(\mathbb{F}_p)$. No sistema criptográfico ElGamal a chave pública é o par $(E(\mathbb{F}_p), P)$, e cada pessoa torna público o ponto $C = cP$, onde $c \in \mathbb{Z}$ é sua chave privada.

Vamos enumerar os passos de uma troca de mensagens através deste sistema. Suponha que Ana queira mandar uma mensagem criptografada para Bernardo. O processo ElGamal é o seguinte:

i) Ana e Bernardo escolhem chaves privadas $a, b \in \mathbb{Z}$ respectivamente, e cada um calcula os pontos $A = aP$ e $B = bP$ e os revela ao outro.

ii) Ana codifica sua mensagem como um ponto $M \in E(F_p)$.

iii) Ana calcula $S = M + aB$ e envia para Bernardo.

iv) Bernardo calcula

$$\begin{aligned} S - bA &= M + aB - bA \\ &= M + abP - baP \\ &= M. \end{aligned}$$

v) Bernardo decifra a mensagem que corresponde ao ponto M.

Observamos que é necessária uma maneira de transformar uma mensagem de texto em um ponto da curva para executar este algoritmo. Para isso usamos o **método de Koblitz** [8]:

i) Ana e Bernado concordam em uma constante $\lambda \in \mathbb{Z}$.

ii) Seja M uma mensagem em linguagem natural, consistindo de uma sequência de caracteres $c_0c_1 \dots c_s$. Seja a_i o código ASCII correspondente a cada c_i, concatenamos os códigos correspondentes a cada caractere para ter obter número $m = a_0a_1 \dots a_s$.

iii) Para determinar a abscissa do ponto, Ana testa o símbolo de Legendre de

$$f(m\lambda + 1),\ f(m\lambda + 2),\ f(m\lambda + 3) \dots$$

até achar um $f(m\lambda + i)$ que seja um quadrado módulo p, e define $x = f(m\lambda + i)$.

iv) Ana usa o algoritmo de Cipolla para encontrar um valor de y tal que o ponto $P = (x, y)$ esteja na curva. Ela então envia este ponto para Bernado usando o algoritmo ElGamal.

v) Quando chega a vez de Bernardo extrair a mensagem do ponto $P = (x, y)$, ele pega a abscissa x e calcula $m = \left\lfloor \frac{x}{\lambda} \right\rfloor$. Finalmente, ele consulta a tabela ASCII para decifrar a mensagem.

Observamos que se $m \geq p$ então simplesmente dividimos sua representação binária em pedaços menores e enviamos vários pontos. Notamos ainda que no passo (iii), o inteiro i em $f(m\lambda + i)$ não pode ultrapassar λ, pois isso criaria ambiguidade no passo (v). Se λ for grande é quase impossível que nenhuma das tentativas resultem em símbolo de Legendre 1. Se por acaso isto acontecer, é só dividir a representação binária de m em dois pedaços menores e tentar de novo.

Exemplo 18.1. Ana e Bernardo já tinham previamente concordado em usar a curva elíptica $E(\mathbb{F}_p)$ dada por $y^2 = x^3+x+1$ onde p é o primo 10000000000000000000000000000319. Tomaram sobre este corpo o ponto público $P = (0, 1) \in E(\mathbb{F}_p)$ depois de terem checado por meio de um programa que o ponto é um gerador de $E(\mathbb{F}_p)$. Após isso Ana e Bernardo escolheram respectivamente as chaves privadas

$$a = 33471323420154298930316972633 \text{ e } b = 63293600728932886663226907583,$$

e publicaram os pontos

$$\begin{aligned} A &= 334713234201542989303169726 33 \cdot P \\ &= (138697934672336062777949550 20, 985038696550980436767859592 91), \\ B &= 632936007289328866632269075 83 \cdot P \\ &= (485012431341346546896318822 09, 684915321240078712481535964 98). \end{aligned}$$

Agora Ana quer enviar para Bernardo a mensagem PATO. O primeiro passo é transformar esta mensagem em um ponto. Vamos então representar cada letra pelo seu número ASCII decimal e concatená-los para formar a ordenada de um ponto

P	A	T	O
080	065	084	079

obtendo $m = 80065084079$. Eles combinam usar uma constante $\lambda = 10000$, e Ana tenta usar o método de Cipolla para encontrar uma ordenada para $x = m\lambda + 1 = 800650840790001$. Ela encontrou o valor $y = 188941920745560132774507280 37$, obtendo o ponto

$$M = (800650840790001, 188941920745560132774507280 37),$$

que tem a mensagem m mergulhada. Ana calcula então o ponto

$$S = M + aB = (105805162811874752431816110 75, 857542255586350341439999283 03),$$

e o envia para Bernardo. Bernardo ao receber o ponto calcula

$$S - bA = M = (800650840790001, 188941920745560132774507280 37).$$

Então para obter m ele pega a abscissa $x = 800650840790001$ e calcula

$$\left\lfloor \frac{x}{\lambda} \right\rfloor = \left\lfloor \frac{800650840790001}{10000} \right\rfloor = 80065084079$$

e por fim checa a tabela ASCII decimal para desvendar a mensagem decodificada PATO.

3 Curva elípticas sobre corpos finitos

Iremos fazer uma discussão detalhada sobre a estrutura de grupo de curvas elípticas sobre corpos finitos. Neste capítulo $\mathbb{F}_q$ sempre irá se referir a um corpo finito de q elementos, onde $q = p^n$ é potência de algum primo p. O objetivo final é conseguir classificar as estruturas dos grupos de pontos racionais como no Teorema 13. Daqui pra frente conceitos de teoria algébrica dos números, que podem ser encontrados em [10], [11] e [13], serão usados com frequência.

Preliminares

Começamos apresentando definições necessárias da teoria algébrica dos números.

Corpos numéricos e ordens

Definição 19. Um corpo numérico algébrico, ou simplesmente corpo numérico, é uma extensão finita de corpo de $\mathbb{Q}$. O corpo é dito **quadrático** se a extensão é de grau 2. Um corpo quadrático é dito **complexo** se é da forma $\mathbb{Q}(\sqrt{d})$ com $d \in \mathbb{Z}_{<0}$.

Definição 20. O **anel de inteiros** em um corpo numérico algébrico $\mathcal{K}$ é o anel $O_\mathcal{K}$ dos elementos de $\mathcal{K}$ que são inteiros sobre $\mathbb{Z} \subset \mathcal{K}$, isto é, consiste nos elementos de $\mathcal{K}$ que são raízes de polinômios mônicos com coeficientes em $\mathbb{Z}$. Chamamos os elementos de $O_\mathcal{K}$ de **inteiros numéricos**. Em outras palavras, $O_\mathcal{K} = \mathcal{K} \cap \overline{\mathbb{Z}}$, onde $\overline{\mathbb{Z}}$ é o fecho algébrico de $\mathbb{Z}$.

Definição 21. Seja $\mathcal{K}$ uma álgebra finitamente gerada sobre $\mathbb{Q}$. Uma **ordem** O de $\mathcal{K}$ é um subanel de $\mathcal{K}$ finitamente gerado como $\mathbb{Z}$-módulo tal que o produto tensorial $O \otimes_\mathbb{Z} \mathbb{Q}$ seja igual a $\mathcal{K}$.

Observamos que como o próprio anel de inteiros satisfaz a condição de uma ordem e contém todas as outras ordens por ter todos os inteiros algébricos, ele é a única ordem maximal em um corpo numérico. Definimos então uma classe de ideais contidas em corpos numéricos ou suas ordens.

Definição 22.

a) Um **ideal fracionário** é um $O_\mathcal{K}$-submódulo de $\mathcal{K}$ finitamente gerado.

b) Um **ideal fracionário de uma ordem** O é um submódulo de $\mathcal{K}$ finitamente gerado como um O-módulo.

Proposição 23. *O conjunto dos ideais fracionários diferentes de zero do anel de inteiros de um corpo numérico é um grupo abeliano pela operação de multiplicação.*

Demonstração. Consequência direta das Proposições 6.1.4 e 6.1.6 em [10] e [10]. □

Proposição 24. *Seja I um ideal fracionário de $O_{\mathcal{K}}$. Então I pode ser escrito como um produto de ideais*

$$I = \prod_i \mathfrak{p}_i^{\varepsilon_i}, \quad \text{onde cada } \mathfrak{p}_i \text{ é um ideal primo de } O_{\mathcal{K}} \text{ e cada } \varepsilon_i \text{ é } 1 \text{ ou } -1,$$

e este produto é único a menos da ordem de seus fatores.

Demonstração. Veja Corolário 6.1.10 de [10]. □

Teorema 25. *Sejam $\mathcal{K}/\mathcal{K}'$ uma extensão galoisiana de corpos numéricos, p um primo de $O_{\mathcal{K}'}$, $pO_{\mathcal{K}} = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}$ a decomposição do ideal gerado por p em ideais primos distintos, e $f_i = [O_{\mathcal{K}}/\mathfrak{p}_i : O_{\mathcal{K}'}/p]$ para $1 \leq i \leq g$. Então,*

$$e_1 = \cdots = e_g, \quad f_1 = \cdots = f_g,$$

e $[\mathcal{K} : \mathcal{K}'] = efg$, onde e é o valor comum dos e_i's e f é o valor comum dos f_i's.

Demonstração. Veja o Teorema 13.2.2 de [10]. □

Definição 26. Seja $\mathcal{K} = \mathbb{Q}(\sqrt{d})$ um corpo numérico quadrático, d livre quadrados, e sejam $O_{\mathcal{K}}$ seu anel de inteiros e $O \subset O_{\mathcal{K}}$ uma de suas ordens quadráticas.

a) O **discriminante do corpo** $\mathcal{K}$ é definido como

$$D_{\mathcal{K}} = \begin{cases} d & \text{se } d \equiv 1 \bmod 4, \\ 4d & \text{se } d \equiv 2, 3 \bmod 4. \end{cases}$$

b) O índice $c = [O_{\mathcal{K}} : O]$ é chamado de **condutor** de O.

c) O **discriminante da ordem** O é $D(O) = c^2 D_{\mathcal{K}}$.

d) Uma ordem em um corpo numérico é dita **complexa** se o corpo for complexo.

Observamos para cada inteiro $c \in \mathbb{Z}_{>0}$, o anel $O_{\mathcal{K}}$ tem precisamente um subanel D de índice c e discriminante $D(O) = c^2 D_{\mathcal{K}}$. Isso implica que as ordens complexas quadráticas são determinadas por seus discriminantes, e podemos então nos referir sem ambiguidade à ordem O de discriminante D como $O(D)$, sem nem mesmo especificar em qual corpo quadrático a ordem está (veja a Seção 2 de [15]).

Proposição 27. *Seja $\mathcal{K}$ um corpo numérico quadrático com discriminante $D_{\mathcal{K}}$. Então seu anel de inteiros é*

$$\mathbb{Z}\left[\frac{D_{\mathcal{K}} + \sqrt{D_{\mathcal{K}}}}{2}\right].$$

Demonstração. Veja o Corolário 2 do Teorema 1 em [12]. □

Notamos que todo corpo númerico quadrático é uma extensão galoisiana por ser de grau dois. Há então um número bem limitado de possibilidades para os valores de e, f e g.

Definição 28. Seja $\mathcal{K}/\mathbb{Q}$ uma extensão quadrática de corpos. Como seu grau é 2, a extensão $\mathcal{K}/\mathbb{Q}$ é galoisiana, e portanto para cada primo $p \in \mathbb{Z}$ temos $efg = 2$. Existem três possibilidades para a decomposição do ideal $pO_{\mathcal{K}}$ gerado por p em $O_{\mathcal{K}}$ como produto de ideais primos:

i) Ele é dito **ramificado** se $e = 2$, $f = g = 1$. Isto é, $pO_{\mathcal{K}} = \mathfrak{p}^2$ onde $\mathfrak{p}$ é um primo em $O_{\mathcal{K}}$.

ii) Ele é dito **inerte** se $e = 1$, $f = 2$, $g = 1$. Neste caso $pO_{\mathcal{K}} = \mathfrak{p}$, significando que o ideal gerado por p é primo.

iii) Ele é dito **decomposto** se $e = f = 1$, $g = 2$. Neste caso $pO_{\mathcal{K}} = \mathfrak{p}_0\mathfrak{p}_1$ se decompõe no produto de dois primos distintos.

Daqui pra frente em vez de dizer que o ideal $pO_{\mathcal{K}}$ ramifica, decompõe ou é inerte em $O_{\mathcal{K}}$, diremos por simplicidade que o primo p têm essas propriedades.

Proposição 29. *Seja $\mathcal{K}$ um corpo quadrático de discriminante $D_{\mathcal{K}}$, e seja p um inteiro primo. Então*

a) p ramifica se $p \mid D_{\mathcal{K}}$.

b) p decompõe se o símbolo de Legendre $\left(\frac{D_{\mathcal{K}}}{p}\right)$ for igual a 1.

c) p é inerte se $\left(\frac{D_{\mathcal{K}}}{p}\right)$ for -1.

Demonstração. Veja o Corolário 5.17 de [13]. □

Formas quadráticas e classes de equivalência

Definição 30. Dada uma ordem O, definimos como $I(O)$ o conjunto dos ideais fracionários invertíveis de O, dados como na Definição 22, e definimos $P(O)$ como o conjunto dos ideais fracionários principais de $O_{\mathcal{K}}$.

Temos que $I(O)$ é um grupo para a operação de multiplicação de ideais dado pelo Lema 23, assim como $P(O)$. O grupo quociente $C(O) = I(O)/P(O)$ é chamado o **grupo de classe** de O. Por fim, definimos o **número de classe** $h(O)$ como a cardinalidade de $C(O)$.

Determinar a cardinalidade $h(O)$ é importante pois mais a frente veremos que este valor é relevante para a determinação da estrutura do grupo de pontos racionais em curvas elípticas. Para determinar esta cardinalidade introduzimos o conceito de formas quadráticas.

Definição 31.

a) Uma **forma quadrática binária**, é um polinômio da forma $f(x, y) = ax^2 + bxy + cy^2$ com coeficientes $a, b, c \in \mathbb{Z}$.

b) O **discriminante** de uma forma quadrática f é definido como

$$\Delta(f) = b^2 - 4ac.$$

c) A forma quadrática é dita positiva definida se $\Delta(f) < 0$ e $a > 0$.

d) A forma é dita primitiva se mdc $(a, b, c) = 1$.

Observamos que para qualquer forma f temos $\Delta(f) \equiv 0$ ou 1 mod 4, porque se $a, b, c \in \mathbb{Z}$, então $b^2 - 4ac \equiv b^2 \equiv 0$ ou 1 mod 4.

Definição 32. Seja $\Delta \in \mathbb{Z}_{<0}$ com $\Delta \equiv 0$ ou 1 mod 4. Definimos então

$$B(\Delta) = \{ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y] : a > 0 \text{ e } b^2 - 4ac = \Delta\}$$

como sendo o conjunto formas binárias quadráticas positivas definidas de discriminante Δ. Analogamente, definimos

$$b(\Delta) = \{ax^2 + bxy + cy^2 \in B(\Delta) : \text{ mdc } (a, b, c) = 1\}$$

como as formas primitivas de discriminante Δ.

Proposição 33. *Sejam $SL_2(\mathbb{Z})$ o grupo especial linear 2×2 de $\mathbb{Z}$, $f(x, y) = ax^2+bxy+cy^2$ uma forma em $B(\Delta)$ e $\rho = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z})$. Definimos a operação*

$$f \circ \rho = a(px + qy)^2 + b(px + qy)(rx + sy) + c(rx + sy)^2.$$

Temos que as seguintes propriedades são satisfeitas:

a) A operação descrita nos dá uma ação do grupo especial linear $SL_2(\mathbb{Z})$ sobre $B(\Delta)$ e $b(\Delta)$.

b) As cardinalidades de $B(\Delta)/SL_2(\mathbb{Z})$ e de $b(\Delta)/SL_2(\mathbb{Z})$ são finitas.

Demonstração. Veja a Proposição 5.4.2 de [11]. □

Definição 34. Sejam $CL(\Delta) = B(\Delta)/SL_2(\mathbb{Z})$ e $Cl(\Delta) = b(\Delta)/SL_2(\mathbb{Z})$ os conjuntos quocientes pela relação de órbita. As cardinalidades de $CL(\Delta)$ e $Cl(\Delta)$ são chamadas respectivamente de **número de classe de Kronecker**, denotado $H(\Delta)$, e **número de classe ordinário**, $h(\Delta)$.

Teorema 35. *Seja O uma ordem em um corpo quadrático. O seu número de classe como ordem é igual ao número de classe de seu discriminante $\Delta(O)$ em termos de formas binárias. Isto é, $h(O) = h(\Delta(O))$.*

Demonstração. Veja o Teorema 7.7 de [13].

□

Este resultado é importante pois é muito mais fácil contar $h(\Delta(O))$ do que contar $h(O)$, e é assim que os resultados que determinam número de classe de ordens em corpos quadráticos são obtidos (veja a Seção 2 de [13]). Sabendo que existem métodos concretos para calcular o número de classe ordinário, usaremos esses valores como quantias conhecidas quando necessário.

Isogenias

Definição 36. Seja K um corpo fixo.

a) Uma **isogenia** é um morfismo $\phi : E \to E'$ entre curvas elípticas $E/K, E'/K$ tal que $\phi(\mathcal{O}) = \mathcal{O}$, onde $\mathcal{O}$ é o elemento neutro dos grupos.

b) Seja E/K uma curva elíptica. Um endomorfismo é uma isogenia $\phi : E \to E$.

c) $\overline{K}(E)$ é o corpo de funções de E sobre o fecho algébrico de K.

Observamos que uma isogenia $\phi : E \to E'$ induz uma aplicação injetiva

$$\begin{aligned} \phi^* : \overline{K}(E') &\to \overline{K}(E) \\ f &\mapsto f \circ \phi. \end{aligned}$$

Um morfismo entre duas curvas irredutíveis é ou constante ou sobretivo (Veja Proposição II.6.8 em [3]), isto é $\phi(E) = \mathcal{O}$ ou $\phi(E) = E'$. Em geral não há sobrejetividade quando nos restringimos apenas aos pontos racionais. Uma das propriedades importantes das isogenias é que quando vemos as curvas elípticas como grupos as isogenias são homomorfismos.

Proposição 37. *Sejam E/K e E'/K curvas elípticas. Qualquer isogenia $\phi : E \longrightarrow E'$ é um homomorfismo sobre as curvas vistas como grupos.*

Demonstração. Veja o Teorema III.4.8 em [5].

□

Isogenias de uma curva para ela mesma são portanto endomorfismos, assim como somas e composições desses endomorfismos. Desta forma obtemos uma definição equivalente de isogenia que geralmente é mais útil: é um homomorfismo dado por funções racionais nas coordenadas dos pontos.

Definição 38.

a) Duas curvas elípticas são ditas **isógenas** se existir uma isogenia (não nula) entre elas.

b) Dizemos que duas curvas elípticas E_1, E_2 sobre $\mathbb{F}_q$ são **isomorfas** se existem duas isogenias $\phi : E_1 \to E_2$ e $\psi : E_2 \to E_1$ tais que $\phi \circ \psi = \mathrm{id}_{E_1}$ e $\psi \circ \phi = \mathrm{id}_{E_2}$. Esta é uma relação de equivalência. Podemos tomar as classes de equivalência das curvas por esta relação.

c) $I(t) :=$ conjunto das classes de isomorfismo de curvas elípticas, sobre um corpo $\mathbb{F}_q$ fixo, com exatamente $q + 1 - t$ pontos racionais.

d) $N(t) :=$ quantidade de classes de isomorfismo em $I(t)$.

Recordamos que em uma extensão de corpos L/K, um elemento $\alpha \in L$ é dito separável sobre K se ele é algébrico sobre K e seu polinômio minimal é separável. O conjunto de todos os elementos de L separáveis sobre K forma um subcorpo chamado fecho separável de K em L, e o fecho separável de K em $\overline{K}$ é simplesmente chamado fecho separável de K.

Uma extensão L/K é **separável** se L é igual ao fecho separável de K em L, e **inseparável** caso contrário. Seja S o fecho separável de K em L, então $[L : K]$ é o produto dos graus $[S : K]$ e $[L : S]$, que são chamados respectivamente de grau separável e grau de inseparabilidade da extensão L/K.

Definição 39. Sejam K um corpo e $E_1/K, E_2/K$ curvas elípticas. Para uma isogenia $\phi : E_1 \to E_2$ definimos,

a) $\deg(\phi)$ como o grau da extensão finita $\overline{K}(E_1)/\phi^*\overline{K}(E_2)$, isto é,

$$\deg(\phi) = [\overline{K}(E_1) : \phi^*\overline{K}(E_2)].$$

De forma similar, definimos $\deg_s(\phi)$ e $\deg_i(\phi)$ como sendo os graus das extensões separáveis e inseparáveis da extensão, respectivamente.

b) O grau da isogenia constante $E_1 \mapsto \mathcal{O}$ é 0 por convenção.

c) A isogenia é dita **separável** se $\deg(\phi) = \deg_s(\phi)$.

Teorema 40. *Seja $\phi : E_1 \to E_2$ uma isogenia não constante de curvas elípticas. Então,*

a) para todos os pontos $Q \in E_2$ temos $\#\phi^{-1}(Q) = \deg_s(\phi)$;

b) se ϕ é separável temos $\#\ker\phi = \deg(\phi)$.

Demonstração.

a) As Proposições II.6.8 e II.6.9 de [3] nos garantem que $\#\phi^{-1}(Q) = \deg_s(\phi)$ para todos menos um número finito de pontos em E_2. Porém, para quaisquer $Q, Q' \in E_2$ e $R \in E_1$ de tal que $\phi(R) = Q - Q'$, como ϕ é um homomorfismo, temos uma bijeção

$$\begin{aligned} \phi^{-1}(Q) &\to \phi^{-1}(Q') \\ P &\mapsto P + R, \end{aligned}$$

e portanto $\#\phi^{-1}(Q)$ é o mesmo para todo $Q \in E_2$.

b) Se ϕ é separável, pelo item (a) temos que $\#\phi^{-1}(Q) = \deg(\phi)$ para qualquer $Q \in E_2$. Em particular para $Q = \mathcal{O}$ temos $\#\ker\phi = \#\phi^{-1}(\mathcal{O}) = \deg(\phi)$.

□

Observamos que este resultado implica que, com exceção da isogenia constante, todo ponto na imagem de uma isogenia tem um número finito de pontos na pré-imagem.

Proposição 41. *Para qualquer cadeia de isogenias* $E_1 \xrightarrow{\psi} E_2 \xrightarrow{\phi} E_3$*, temos* $\deg(\psi \circ \phi) = \deg(\psi) \cdot \deg(\phi)$.

Demonstração. Por definição,

$$\begin{aligned}\deg(\psi \circ \phi) &= [\overline{k}(E_1) : (\phi \circ \psi)^* K(E_3)] \\ &= [\overline{k}(E_1) : \psi^* \overline{k}(E_2)] \cdot [\overline{k}(E_2) : \phi^* K(E_3)] \\ &= \deg(\psi) \cdot \deg(\phi).\end{aligned}$$

□

Definição 42. Para cada $m \in \mathbb{Z}$ podemos definir a isogenia "vezes m", $[m] : E \to E$ de forma natural:

1. Se $m > 0$, $[m](P) = \underbrace{P + \cdots + P}_{m \text{ vezes}}$.
2. Se $m < 0$, $[m](P) = -[-m](P)$.
3. A isogenia $[0]$ é a isogenia constante $E \mapsto \mathcal{O}$.

Para todo $m \in \mathbb{Z}$, temos que $[m]$ comuta com qualquer $\phi \in \mathrm{End}(E)$ isogenia de E para E. De fato, para $m \geq 0$ temos

$$\phi \circ [m](P) = \phi(\underbrace{P + \cdots + P}_{m \text{ vezes}}) = \underbrace{\phi(P) + \cdots + \phi(P)}_{m \text{ vezes}} = [m] \circ \phi(P),$$

e o caso para $m < 0$ é análogo. Interessa saber quando essa isogenia é separável.

Proposição 43. *Seja* E/K *uma curva elíptica e* $m \in \mathbb{Z}$*,* $m \neq 0$ *em* K*. Então o endomorfismo* $[m]$ *é separável.*

Demonstração. Veja o Corolário III.5.4 em [5]. □

Observamos que se o corpo é $\mathbb{F}_q$, $q = p^n$ onde p é primo, então esta proposição é equivalente a dizer que se $p \nmid m$ então $[m]$ é separável.

Definição 44. Sejam E/K, E_1/K e E_2/K curvas elípticas.

a) Definimos $\mathrm{Hom}(E_1, E_2)$ como o conjunto de todas as isogenias de E_1 para E_2.

b) Definimos $\mathrm{End}(E)$ como o conjunto de todos os endomorfismos de E.

Proposição 45. *Sejam* E/K*,* E_1/K *e* E_2/K *curvas elípticas.*

a) A soma de duas isogenias $\phi, \psi : E_1 \to E_2$ *é uma nova isogenia* $(\phi + \psi) : E_1 \to E_2$ *dada por* $(\phi + \psi)(P) = \phi(P) + \psi(P)$ *para todo* $P \in E_1$ *e* $Hom(E_1, E_2)$ *é um grupo com esta operação.*

b) Dadas isogenias $\phi, \psi : E \to E$, a composição $(\psi \circ \phi)(P) = \psi(\phi(P))$ também é uma isogenia. Definindo a multiplicação como a composição e a soma como no item anterior, temos uma estrutura de anel para $Hom(E, E)$.

Demonstração.

a) A operação está bem definida porque a soma de dois morfismos também é um morfismo, e $\phi(\mathcal{O}) + \psi(\mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}$.

   Essa operação tem $[0]$ como elemento neutro. Para qualquer $\phi \in \mathrm{Hom}(E_1, E_2)$, temos o inverso aditivo $[-1] \circ \phi$. A operação também é comutativa, pois $\phi(P), \psi(P) \in E_2$ para todo $P \in E_1$, e a soma de pontos em curvas elípticas é comutativa.

b) A composição de endomorfismos de grupos é também um endomorfismo. A identidade da multiplicação em $\mathrm{End}(E)$ é $[1]$. A associatividade e distributividade da composição com a soma vêm do fato das isogenias serem homomorfismos.

□

A existência dessa estrutura de anel nos permite chamar os conjuntos $\mathrm{Hom}(E_1, E_2)$ e $\mathrm{End}(E)$ de **grupo de homomorfismos** e **anel de endomorfismos**, respectivamente.

Aplicação de Frobenius

Definição 46. Dada uma curva elíptica $E/\mathbb{F}_q$, o **endomorfismo de Frobenius** $\pi : E \to E$ é a aplicação

$$\pi(x, y) = (x^q, y^q),$$

que eleva as coordenadas dos pontos à q-ésima potência. O valor de $\pi(\mathcal{O})$ é definido como $\mathcal{O}$ para garantir que π seja uma isogenia. Observamos que como o grupo de Galois da extensão $\overline{\mathbb{F}}_q/\mathbb{F}_q$ é gerado pelo automorfismo $x \mapsto x^q$ (veja o Teorema V.1.1 de [5]) então $\pi(P) = P$ se e apenas se $P \in E(\mathbb{F}_q)$.

Proposição 47. *Seja $E/\mathbb{F}_q$ uma curva elíptica e π seu endomorfismo de Frobenius. Então,*

a) π é uma isogenia separável.

b) $\deg(\pi) = q$.

Demonstração. Veja a Proposição II.2.11 em [5]. □

Proposição 48. *Seja $E/\mathbb{F}_q$ uma curva elíptica e $\pi : E \longrightarrow E$ seu endomorfismo de Frobenius. Então*

a) $E(\mathbb{F}_q) = \{P \in E : P = \pi(P)\}$.

b) $E(\mathbb{F}_q) = \ker([1] - \pi)$.

Demonstração.

a) Seja $P = (a, b) \in E$. Temos,

$$\begin{aligned}\pi(P) = P &\Leftrightarrow a^q = a,\ b^q = b,\\ &\Leftrightarrow a, b \in \mathbb{F}_q,\\ &\Leftrightarrow P \in E(\mathbb{F}_q).\end{aligned}$$

b) Temos que $([1] - \pi)(P) = P - \pi(P)$, o que pelo item anterior é $\mathcal{O}$ se e somente se $P \in E(\mathbb{F}_q)$.

□

Proposição 49. *Seja E uma curva elíptica definida sobre $\mathbb{F}_q$ onde $q = p^n$, p primo. Sejam π o endomorfismo de Frobenius, e $m, n \in \mathbb{Z}$. Então a isogenia*

$$[m] + ([n] \circ \pi) : E \to E$$

é separável se e apenas se $p \nmid m$. Em particular, $[1] - \pi$ é separável.

Demonstração. Veja corolário III.5.5 em [5]. □

O anel de endomorfismos

Proposição 50. *Sejam E, E' curvas elípticas sobre um corpo K.*

a) A aplicação $[m] : E \longrightarrow E$ é não constante para $m \neq 0$.

b) O grupo de isogenias $Hom(E, E')$ é um $\mathbb{Z}$-módulo livre de torção.

c) $End(E)$ é um anel de característica 0 e sem divisores de zero (domínio integral).

Demonstração.

a) Veja a Proposição III.4.2 em [5].

b) É um $\mathbb{Z}$-módulo por ser um anel contendo $\mathbb{Z}$. Sejam $\phi \in \mathrm{Hom}(E_1, E_2)$ e $m \in \mathbb{Z}$ satisfazendo $[m] \circ \phi = [0]$. Tomamos o grau de ambos os lados da igualdade usando a Proposição 41 obtendo

$$\deg([m]) \cdot \deg(\phi) = 0 \Rightarrow \deg([m]) = 0 \text{ ou } \deg(\phi) = 0$$

Portanto ou $m = 0$ ou $\phi = [0]$, provando que o anel é livre de torção.

c) Notemos que o item anterior mostra que a característica é 0. Sejam $\phi, \psi \in \mathrm{End}(E)$ tais que $\phi \circ \psi = [0]$, tomando o grau de ambos os lados temos

$$\deg(\phi) \cdot \deg(\psi) = \deg(\phi \circ \psi) = \deg([0]) = 0.$$

Assim, $\phi = [0]$ ou $\psi = [0]$. Concluímos que $\mathrm{End}(E)$ é um domínio integral.

□

Proposição 51. *Sejam $E_1/K, E_2/K$ curvas elípticas sobre um corpo K e $\phi : E_1 \to E_2$ uma isogenia. Existe uma única* ***isogenia dual*** $\hat{\phi} : E_2 \longrightarrow E_1$ *tal que $\hat{\phi} \circ \phi = [m]$, onde $m = deg\ \phi$.*

Demonstração. Veja o Teorema III.6.1 em [5]. □

Teorema 52. *Sejam $E_1/K, E_2/K$ curvas elípticas sobre um corpo K e $\phi : E_1 \to E_2$ uma isogenia. Então,*

a) se $\psi : E_1 \longrightarrow E_2$ é outra isogenia. Então $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$

b) se $m = \deg(\phi)$, temos $\hat{\phi} \circ \phi = [m]$ em E_1 e $\phi \circ \hat{\phi} = [m]$ em E_2.

c) seja $\lambda : E_2 \longrightarrow E_1$ é outra isogenia, temos $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$.

d) $\forall m \in \mathbb{Z}$, $\widehat{[m]} = [m]$ e $\deg[m] = m^2$.

Demonstração. Veja o Teorema III.6.2 em [5].

□

Definição 53. Seja $\phi \in \mathrm{End}(E)$ um endomorfismo de uma curva elíptica. Então definimos seu **traço** como sendo a soma

$$T(\phi) = \hat{\phi} + \phi,$$

e sua **norma** como a composição

$$N(\phi) = \hat{\phi} \circ \phi.$$

Percebemos que pela definição de morfismo dual dada na Proposição 51, que a norma sempre é a multiplicação por um inteiro $m > 0$. Podemos então associar a norma de qualquer isogenia com um inteiro positivo. De forma similar, temos a igualdade

$$\begin{aligned} T(\phi) &= \hat{\phi} + \phi \\ &= \hat{\phi} \circ \phi - \hat{\phi} \circ \phi + [1] - [1] + \hat{\phi} + \phi \\ &= [1] + \hat{\phi} \circ \phi - (\hat{\phi} - [1]) \circ (\phi - [1]) \\ &= [1] + N(\phi) - N(\phi - [1]). \end{aligned}$$

Como isto é a soma de isogenias de multiplicação por inteiros, então o traço é a isogenia de multiplicação por um inteiro, possivelmente negativo.

A estrutura

A pergunta mais básica a se fazer quanto à estrutura do grupo de pontos racionais é quantos pontos racionais existem em uma curva elíptica sobre $\mathbb{F}_q$.

Ao colocarmos sua equação na forma $y^2 = f(x)$ fica claro que só podemos ter no máximo dois valores de y para cada valor de x, e exatamente um se o corpo finito tem característica 2. Contando com $\mathcal{O}$, isso nos dá uma cota superior de $2q + 1$ pontos. Veremos que esta cota pode ser melhorada, e que a quantidade de pontos racionais sempre é algo em torno de $q + 1$ pontos.

Teorema 54. *Seja $E/\mathbb{F}_q$ uma curva elíptica, então*

a) $\#E(\mathbb{F}_q) = q + 1 - t$, *onde t é o traço do endomorfismo de Frobenius;*

b) $|t| \leq 2\sqrt{q}$.

Demonstração.

a) Consideremos o endomorfismo de Frobenius π. A Proposição 48 nos diz que $E(\mathbb{F}_q) = \ker(1 - \pi)$. Usando então o Teorema 40 e a Proposição 49 temos que $\#E(\mathbb{F}_q) = \#\ker(1 - \pi) = \deg(1 - \pi)$. Então pelo item (b) do Teorema 52 e pelo fato da Proposição 49 implicar $N(\pi) = q$ por π ser separável,

$$\begin{aligned}\deg(1 - \pi) &= \widehat{(1 - \pi)} \circ (1 - \pi) \\ &= 1 - (\hat{\pi} + \pi) + \hat{\pi} \circ \pi \\ &= 1 - T(\pi) + N(\pi) \\ &= q + 1 - t, \text{ onde } t = T(\pi).\end{aligned}$$

b) A desigualdade é consequência direta da cota de Hasse-Weil (veja o Teorema 9.18 em [2]), levando em conta que curvas elípticas têm gênero 1 por serem curvas não-singulares de grau 3.

□

Sabendo que o número de pontos está nesta faixa, iremos determinar quais são os possíveis valores que a quantidade de pontos racionais de curvas sobre $\mathbb{F}_q$ pode assumir. Da relação (a) do Teorema 54 temos que a quantidade de pontos racionais está diretamente ligada ao traço t do endomorfismo de Frobenius.

Seja $I(t)$ como na Definição 38, o seguinte teorema nos fala da existência ou não de curvas com cardinalidades específicas:

Teorema 55. ***Existência.*** *Considere as curvas elípticas sobre um corpo finito $\mathbb{F}_q$, $q = p^n$. Para qualquer inteiro t com $|t| \leq \lfloor 2\sqrt{q} \rfloor$, o conjunto $I(t)$ é não vazio se e somente se uma das seguintes condições é satisfeita:*

i) $mdc\ (t, p) = 1$.

ii) n é ímpar e uma das seguintes condições é satisfeita:

a) $t = 0$.

b) $t^2 = 2q$ *e* $p = 2$.

c) $t^2 = 3q$ *e* $p = 3$.

iii) n é par e uma das seguintes condições é satisfeita:

a) $t^2 = 4q$.

b) $t^2 = q$ *e* $p \not\equiv 1 \ mod\ 3$.

c) $t = 0$ *e* $p \not\equiv 1 \ mod\ 4$.

Demonstração. Veja o Teorema 4.1 em [14].

□

Isto nos dá para quais constantes t existe alguma curva elíptica sobre $\mathbb{F}_q$ com $q+1-t$ pontos racionais. Mas também interessa saber quantas classes de isomorfismo existem para curvas com $q+1-t$ pontos racionais quando elas existem. Vamos introduzir uma definição que será usada para este fim.

Definição 56. Uma álgebra de quatérnions é uma álgebra da forma

$$Q = \{a + b\alpha + c\beta + d\alpha\beta : a, b, c, d \in \mathbb{Q}\},$$

onde $\alpha^2, \beta^2 \in \mathbb{Q}$, $\alpha^2, \beta^2 < 0$ e $\alpha\beta = -\beta\alpha$.

Em tal álgebra todo elemento diferente de zero tem um inverso multiplicativo. Dizemos que Q se ramifica em um primo p se quando estendemos os coeficientes a, b, c, d de Q ao corpo dos p-ádicos todo elemento continua invertível. De igual forma dizemos que Q se ramifica em ∞ se quando estendemos os coeficientes de Q a $\mathbb{R}$ todo elemento continua invertível. Denotamos por $Q_{\infty,p}$ a álgebra de quatérnions que só se ramifica em ∞ e em p.

O resultado a seguir nos dá o número de classes de isomorfismo:

.

Teorema 57. *Seja $N(t)$ como na Definição 38. Consideramos curvas elípticas sobre $\mathbb{F}_q$.*

a) Seja O uma ordem quadrática que ocorre como um anel de endomorfismos de uma curva em $I(t)$. Denotemos então

$$g = \begin{cases} 2, & \text{se } p \text{ não ramifica em } O, \\ 1, & \text{se } p \text{ ramifica.} \end{cases}$$

Então $N(t) = g \cdot h(O)$.

b) Seja O uma ordem maximal em $\mathbb{Q}_{\infty,p}$ que ocorre como um anel de endomorfismos de uma curva elíptica em $I(t)$. O número $N(t)$ é igual 1 ou 2, sendo 1 se o menor primo contendo p em O é principal e 2 caso contrário.

Demonstração. Veja [15, Teo. 4.5.]. □

Uma consequência direta disto é que o número de classes em $I(t)$ com qualquer anel de endomorfismos O é finito pois $h(O)$ é finito.

Teorema 58. ***Anéis de endomorfismo possíveis.*** *Consideremos curvas elípticas sobre $\mathbb{F}_q$, onde $q = p^n$, p é primo, e t é um dos números listados no Teorema 55. Seja $I(t)$ como na Definição 38. Temos ao menos uma curva em $I(t)$, e os seguintes anéis são os que ocorrem como anéis de endomorfismo de curvas nas classes de isomorfismo inclusas em $I(t)$:*

i) Se $p \nmid t$, todas as ordens quadráticas complexas contendo $O(t^2 - 4q)$

ii) Se $t = \pm 2\sqrt{q}$, todas as ordens maximais em $\mathbb{Q}_{\infty,p}$.

iii) Se $p \mid t$ e $t \neq \pm 2\sqrt{q}$, todas as ordens complexas quadráticas contendo $O(t^2 - 4q)$ tais que $p \nmid [O_{\mathcal{K}} : O]$.

Demonstração. Veja o Teorema 4.2 de [14]. □

Provado isto, podemos nos referir às isogenias pelos seus números algébricos correspondentes na estrutura da ordem como um anel. Seja $\varphi : \mathrm{End}(E) \to O$ o isomorfismo entre o anel de endomorfismos e a sua ordem correspondente. Pela definição de isogenia,

$$\varphi([0]) \to 0, \quad \varphi([1]) \to 1$$

e $\varphi([m]) = \overbrace{\varphi([1]) + \cdots + \varphi([1])}^{m \text{ vezes}} = m$. Portanto os inteiros são correspondentes às isogenias de multiplicação de pontos por inteiros.

Esta identificação dos inteiros será usada implicitamente daqui pra frente: toda vez que uma equação envolvendo isogenias tiver coeficientes inteiros, eles são as aplicações de multiplicação pelo inteiro em questão. Dizer que uma isogenia está em $\mathbb{Z}$ será o mesmo que dizer que a isogenia é uma multiplicação por um inteiro.

O que resta a fazer é determinar explicitamente qual a estrutura de grupo, assim como vista no Teorema 13, tem o grupo de pontos racionais de cada curva elíptica. Para isto vamos introduzir alguns resultados auxiliares que permitem estudar subgrupos do grupo de endomorfismo.

Definição 59. Considere uma curva elíptica E/K. Denotamos por $E[m]$ o subconjunto $\{P \in E : [m]P = \mathcal{O}\}$.

Evidentemente $E[m]$ é o mesmo que $\ker[m]$. Como isogenias são também homomorfismos, este conjunto é um subgrupo de E, chamado **subgrupo de m-torção** de E.

Proposição 60. *Sejam E/K uma curva elíptica e m um inteiro diferente de 0. Então,*

a) se $char(K) = 0$ ou se $char(K) = p > 0$ onde $p \nmid m$, então

$$E[m] = \frac{\mathbb{Z}}{(m)} \times \frac{\mathbb{Z}}{(m)}.$$

b) se $char(K) = p > 0$ então uma das seguintes identidades é verdadeira:

i) $E[p^i] = \{\mathcal{O}\}$ para todo inteiro positivo i.

ii) $E[p^i] = \frac{\mathbb{Z}}{(p^i)}$ para todo inteiro positivo i.

Demonstração.

a) Se $\text{char}(K) = 0$ ou $\text{char}(K) = p > 0$ e $p \nmid m$, a Proposição 47 nos diz que $[m]$ é separável. Assim o item (d) do Teorema 52 implica que $\#E[m] = m^2$. Além disso, $\deg[d] = d^2$ para todo d que divide m. Portanto $\#E[m] = m^2$ e $\#E[d] = d^2$ para todo $d \mid m$.

Logo a única estrutura abeliana possível para $E[m]$ é $\frac{\mathbb{Z}}{(m)} \times \frac{\mathbb{Z}}{(m)}$.

b) Veja a Proposição 6.4 em [5, Cap. III].

□

Lema 61. *Seja E uma curva elíptica sobre $\mathbb{F}_q$, $q = p^n$. Seja m um inteiro positivo tal que $p \nmid m$, e t o traço do endomorfismo de Frobenius π de E. Os seguintes itens são equivalentes:*

i) $E[m] \subset E(\mathbb{F}_q)$,

ii) $m^2 \mid q + 1 - t, \quad m \mid q - 1$, e ou $\pi \in \mathbb{Z}$ ou $O\left(\frac{t^2-4q}{m^2}\right) \subset End(E)$.

Demonstração. Veja Proposição 3.7 em [15]. □

Lema 62. *Seja $E/\mathbb{F}_q$ uma curva elíptica tal que $\#E(\mathbb{F}_q) = q + 1 - t$. Então,*

a) se $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$ *é um subgrupo de* $E(\mathbb{F}_q)$*, então* $m^2 \mid \#E(\mathbb{F}_q)$*.*

b) se para todo $2 \leq m \in \mathbb{Z}$ *temos* $m^2 \nmid \#E(\mathbb{F}_q)$*, então o grupo* $E(\mathbb{F}_q)$ *é cíclico.*

c) se E *contém* $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$ *temos*

i) $m \mid q-1$*,*

ii) $m \mid 2-t$*,*

iii) $p \nmid m$*.*

Demonstração.

a) A ordem de $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$ é m^2 e a ordem de qualquer subgrupo divide a ordem do grupo.

b) Se a ordem de $E(\mathbb{F}_q)$ é livre de quadrados, pelo Teorema 13 temos que $E(\mathbb{F}_q)$ é isomorfo a um
$$\bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{(p_i)},$$
onde cada p_i é um número primo distinto, o que é um grupo cíclico.

c) Suponhamos que E contenha $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$.

i) Pela Proposição 60 sabemos que $E[m] = \mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$. Como $E[m] \subset E(\mathbb{F}_q)$, temos pelo Lema 61 que $m \mid q-1$.

ii) Como $m \mid q+1-t$ e $m \mid q-1$, então $m \mid (q+1-t)-(q-1) = 2-t$.

iii) $m \mid q-1$ implica que $\mathrm{mdc}(m,q) = 1$, e portanto $p \nmid m$.

□

Podemos agora classificar as estruturas dos grupos de pontos racionais.

Teorema 63. *(Lema 4.8 em [15]) Seja* $t \in \mathbb{Z}$*.*

i) Se $t^2 = q, 2q$ *ou* $3q$*, então toda curva* E *em* $I(t)$ *tem* $E(\mathbb{F}_q)$ *cíclico.*

ii) Se $t^2 = 4q$*, então toda curva* E *em* $I(t)$ *tem* $E(\mathbb{F}_q) \cong \dfrac{\mathbb{Z}}{(\sqrt{q} \pm 1)} \oplus \dfrac{\mathbb{Z}}{(\sqrt{q} \pm 1)}$*, com sinais de menos se* $t = 2\sqrt{q}$ *e de mais se* $t = -2\sqrt{q}$*.*

iii) Se $q \not\equiv -1 \bmod 4$ *então toda curva* E *em* $I(0)$ *tem* $E(\mathbb{F}_q)$ *cíclico. Se* $q \equiv -1 \bmod 4$ *então exatamente* $h(-4p)$ *classes de isomorfismo em* $I(0)$ *possuem* $E(\mathbb{F}_q)$ *cíclico e as outras* $h(-p)$ *possuem* $E(\mathbb{F}_q) \cong \frac{\mathbb{Z}}{(2)} \oplus \frac{\mathbb{Z}}{((q+1)/2)}$*.*

Demonstração. Pelo Teorema 55 temos que existe ao menos uma curva elíptica para cada uma dessas condições enumeradas. Vamos encontrar as estruturas possíveis caso a caso:

i) Suponha que $t^2 = \alpha q$, $\alpha = 1, 2$ ou 3. Pelo item (b) do Lema 62, para mostrar que $E(\mathbb{F}_q)$ é cíclico só precisamos mostrar que não existe inteiro $m \geq 2$ tal que $m^2 \mid \#E(\mathbb{F}_q)$. Suponhamos então que existe tal m. Pelo item (c) do Lema 62 temos $m^2 \mid q + 1 - t$ e $m \mid q - 1$. Fazendo a substituição $q = t^2/\alpha$ obtemos $m^2 \mid \frac{t^2 - \alpha t + \alpha}{\alpha}$ e $m \mid \frac{t^2 - \alpha}{\alpha}$. Notamos então que

$$4 - \alpha = (t + 2) \cdot \frac{t^2 - \alpha t + \alpha}{\alpha} + (\alpha - t - 2) \cdot \frac{t^2 - \alpha}{\alpha},$$

e por isso $m \mid 4 - \alpha$. Verificamos o valor que m assume para cada α:

- Se $\alpha = 3$, então $m \mid 1$ e portanto $m = 1$.
- Se $\alpha = 2$ então $m \mid 2$. Suponhamos por absurdo que $m = 2$. Como $q = t^2/\alpha = t^2/2$, temos que t é múltiplo de 2 e q é uma potência de 2. Portanto $p = 2$, contradizendo o item (c) do Lema 62. Portanto, $m = 1$.
- Se $\alpha = 1$ temos $m \mid 3$ e $t = \pm\sqrt{q}$. Porém se m fosse 3, teríamos pelo item (c) do Lema 62 que $m^2 = 9 \mid q + 1 - t = q + 1 \pm \sqrt{q}$. Ao testar todas as congruências $\mod 9$ possíveis para $\sqrt{q}$, vemos que isso não pode acontecer. Portanto temos $m = 1$.

Isto contradiz a suposição de que $m \geq 2$, e implica que $E(\mathbb{F}_q)$ é cíclico.

ii) Seja $t = 2\sqrt{q}$. Como t é o traço do endomorfismo de Frobenius e o traço sempre é inteiro, temos que $\sqrt{q}$ também é inteiro. Portanto, a quantidade de pontos racionais é $\#E(\mathbb{F}_q) = q + 1 - t = q + 1 - 2\sqrt{q} = (\sqrt{q} - 1)^2$.

Tomemos então $m = \sqrt{q} - 1$. Assim $m \mid q - 1$ e $m^2 \mid q + 1 - t$, e então pelo Lema 61 temos

$$E[\sqrt{q} - 1] \subseteq E(\mathbb{F}_q).$$

No entanto, a cardinalidade de ambos os conjuntos é a mesma:

$$\begin{aligned} \#E[\sqrt{q} - 1] &= \#\ker[\sqrt{q} - 1] \\ &= (\sqrt{q} - 1)^2 \\ &= q + 1 - t \\ &= \#E(\mathbb{F}_q), \end{aligned}$$

logo $E(\mathbb{F}_q) = E[\sqrt{q} - 1]$. Assim, pela Proposição 60, $E(\mathbb{F}_q) = \mathbb{Z}/(\sqrt{q} - 1) \oplus \mathbb{Z}/(\sqrt{q} - 1)$. O caso $t = -2\sqrt{q}$ é análogo.

iii) Seja $t = 0$. Suponha que $E(\mathbb{F}_q)$ contenha um grupo da forma $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$. Pelo item (c) do Lema 62 temos que $m^2 \mid q + 1$, $m \mid q - 1$ e $m \mid 2$, logo $m = 2$ ou $m = 1$.

Consideramos primeiro o caso $q \not\equiv -1 \mod 4$. Supomos por absurdo que $m = 2$, implicando que $m^2 \mid q + 1 \Rightarrow q + 1 \equiv 0 \mod 4$. Isto contradiz a condição de que $q \not\equiv -1 \mod 4$. Concluímos que $m = 1$, e portanto $E(F_q)$ é cíclico.

Agora examinamos o caso em que $q \equiv -1 \bmod 4$, o que implica que q não é quadrado. Observamos que como $t = 0$, o Teorema 58 nos diz que o anel de endomorfismo da curva é uma ordem quadrática $\mathrm{End}(E)$ em um corpo quadrático complexo $\mathcal{K}$ tal que $p \nmid [O_{\mathcal{K}} : \mathrm{End}(E)]$ e que contém $O(-4q)$. Como $q \equiv -1 \bmod 4$ implica que $-p \equiv 1 \mod 4$, e o discriminante de uma ordem é o índice ao quadrado dela com o anel de inteiros vezes o discriminante do anel de inteiros, pela Definição 26 temos que $O_{\mathcal{K}} = O(-p)$. Agora, como $O(-4q) \subset \mathrm{End}(E) \subset O(-4p)$ e $p \nmid [O(-4p) : \mathrm{End}(E)]$, então $\mathrm{End}(E)$ é $O(-4p)$ ou $O(-p)$.

Verificamos se $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ é um subgrupo em $\mathrm{End}(E)$. Pela Proposição 47 o grau de π é q. Como q não é quadrado, sabemos pelo item (d) do Teorema 52 que $\pi \notin \mathbb{Z}$, e como $E[2] = \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ temos pelo Lema 61 que $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2) \subset E(\mathbb{F}_q)$ se e apenas se $O\left(\frac{t^2-4q}{m^2}\right) = O(-q) \subset \mathrm{End}(E)$.

Como $O(-q) \subset O(-p)$ e $O(-q) \not\subset O(-4p)$, pelo Lema 61 temos que $E(\mathbb{F}_q)$ contém $\mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ se e apenas se $\mathrm{End}(E) = O(-p)$. Portanto para as curvas com anel de endomorfismos $O(-p)$ sabemos que $E(\mathbb{F}_q) = \frac{\mathbb{Z}}{(2)} \oplus \frac{Z}{((q+1)/2)}$. Já para as curvas com anel de endomorfismos $O(-4p)$, o conjunto dos pontos racionais $E(\mathbb{F}_q)$ é cíclico, pois $E(\mathbb{F}_q)$ não contém nenhum subgrupo da forma $\mathbb{Z}/(m) \oplus \mathbb{Z}/(m)$ neste caso.

Dado que p ramifica em $O(-p)$ e $O(-4p)$ pela Proposição 29, o Teorema 57 implica que exatamente $h(-p)$ classes de isomorfismo têm $O(-p)$ como seu anel de endomorfismos e $h(-4p)$ classes de isomorfismo têm anel de endomorfismos $O(-4p)$.

□

Finalmente temos um resultado mais fraco para o caso onde o traço de Frobenius t e a ordem q são coprimos:

Teorema 64. *Seja $E/\mathbb{F}_q$ uma curva elíptica com traço de Frobenius t, onde $q = p^n$, p primo. Suponha que $mdc(t, q) = 1$ e $U := \#E(\mathbb{F}_q) = q + 1 - t$ se decomponha em primos como $p^{v_p(U)} \prod_{i=1}^{k} p_i^{v_{p_i}(U)}$ onde $v_{p_i}(U)$ denota o expoente da maior potência de p_i a dividir U. Então $E(\mathbb{F}_q)$ é da forma*

$$\frac{\mathbb{Z}}{(p^{v_p(U)})} \oplus \bigoplus_{i=1}^{k} \left(\frac{\mathbb{Z}}{(p_i^{r_i})} \oplus \frac{\mathbb{Z}}{(p_i^{s_i})} \right),$$

onde r_i, s_i são inteiros positivos tais que $r_i + s_i = v_{p_i}(N)$ para todo primo $p_i \neq p$ que divide N.

Demonstração. Pela Proposição 60 temos que $E[p^{v_p(U)}] = \mathbb{Z}/(p^{v_p(U)})$ se p divide U e $\mathcal{O}$ caso contrário, e que $E[p_i] = \mathbb{Z}/(p_i) \oplus \mathbb{Z}/(p_i)$. Assim a estrutura do grupo $E(F_q)$ é da forma

$$\frac{\mathbb{Z}}{(p^{v_p(U)})} \oplus \bigoplus_{i=1}^{k} \left(\frac{\mathbb{Z}}{(p_i^{r_i})} \oplus \frac{\mathbb{Z}}{(p_i^{s_i})} \right).$$

□

Referências

[1] FULTON, William. *Algebraic Curves: An Introduction to Algebraic Geometry.* (2008).

[2] HIRSCHFIELD, J.W.P; KORCHMÁROS, G. e TORRES, F. *Algebraic Curves over a Finite Field.* Princeton University Press (2008).

[3] HARTSHORNE, Robin. *Algebraic Geometry.* Graduate Texts in Mathematics, Springer (1977).

[4] SILVERMAN, Joseph H. e TATE, John T. *Rational Points on Elliptic Curves.* Undergraduate Texts in Mathematics, Springer (2015).

[5] SILVERMAN, Joseph H. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics, Springer (2009).

[6] EISENBUD, D; GREEN, M. e HARRIS, J. *Cayley-Bacharach Theorems and Conjectures.* Bulletin of AMS (new series), v. 33 n. 3, (1996).

[7] WASHINGTON, Laurence C. *Elliptic Curves: Number Theory and Cryptography.* Segunda Edição. Discrete mathematics and its aplications. CRC Press, (2008).

[8] ANDRIA, Sally; GONDIM, Rodrigo e SALOMÃO, Rodrigo. *Introdução à Criptografia com Curvas Elípticas.* IMPA (2019).

[9] *How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form.* Disponível em `http://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/Matsuura-projective_transformation.pdf`

[10] STEIN, William. *A Brief Introduction to Classical and Adelic Algebraic Number Theory.* Semantic Scholar, (2004).

[11] BUCHMANN, Johannes e VOLLMER, Ulrich. *Binary Quadratic Forms: An Algorithmic Approach.* Springer (2007).

[12] MARCUS, Daniel A. *Number Fields.* Springer (1977).

[13] COX, David A. *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication.* 2nd ed., John Wiley & Sons (2013).

[14] WATERHOUSE, William C. *Abelian varieties over finite fields.* Annales scientifiques de L'É.N.S. 4e série, volume 2, no 4 (1969).

[15] SCHOOF, René. *Nonsingular Plane Cubic Curves over Finite Fields.* Journal of Combinatorial Theory, Series A 46, 183-211 (1987).