UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

LEONARDO GARCIA DE CASTRO

Curvas Elípticas, Emparelhamentos e Uma Aplicação à Criptografia

Campinas

2023

Leonardo Garcia de Castro

Curvas Elípticas, Emparelhamentos e Uma Aplicação à Criptografia

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática.

Orientador: Saeed Tafazolian

Este trabalho corresponde à versão final da Dissertação defendida pelo aluno Leonardo Garcia de Castro e orientada pelo Prof. Dr. Saeed Tafazolian.

Campinas

2023

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

C279c

Castro, Leonardo Garcia de, 1998-
Curvas elípticas, emparelhamentos e uma aplicação à criptografia / Leonardo Garcia de Castro. – Campinas, SP : [s.n.], 2023.

Orientador: Saeed Tafazolian.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Curvas elípticas. 2. Teoria de emparelhamentos. 3. Protocolo Diffie-Hellman. I. Tafazolian, Saeed, 1978-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações Complementares

Título em outro idioma: Elliptic curves, pairings and an application to cryptography
Palavras-chave em inglês:
Elliptic curves
Matching theory
Diffie-Hellman protocol
Área de concentração: Matemática
Titulação: Mestre em Matemática
Banca examinadora:
Saeed Tafazolian [Orientador]
Pietro Speziali
Sajad Salami
Data de defesa: 05-04-2023
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0009-0006-7795-7355
- Currículo Lattes do autor: http://lattes.cnpq.br/1520512279956521

Dissertação de Mestrado defendida em 05 de abril de 2023 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SAEED TAFAZOLIAN

Prof(a). Dr(a). PIETRO SPEZIALI

Prof(a). Dr(a). SAJAD SALAMI

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

A todos que fazem ciência.

Agradecimentos

Primeiramente gostaria de agradecer à minha família, meu pai Elton; minha mãe Doralice; e aos meus irmãos Leandra e Lucas, que sempre me apoiaram e me incentivaram a seguir este caminho.

Gostaria também de agradecer ao Prof. Dr. Saeed Tafazolian por ter aceitado ser meu orientador.

Agradeço a todos os meus amigos que fiz durante o mestrado, em especial Mayara Duarte que teve a paciência de me ajudar quando precisei; Daniel Bernal que me ensinou várias coisas; Gabriela Gularte pelo apoio e preocupação; Juliana Calderon que sofreu junto comigo; Letícia Candido pela companhia e por me fazer rir e esquecer todo o estresse. Agradeço a todos dos nosso pequeno clube de leitura: Cassia; Gabriel; Melissa; Lucas; Matheus; Alejandro; Léo Silva; Pehuen; Robson; Samuel; Tiago; Walteir; Crystianne; Tenilson.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

"The Office, season 7
episode 19, minute 14:45"

Resumo

Em criptografia um dos desafios é garantir a troca segura de chaves, para isto algoritmos fazem uso do logaritmo discreto e da sua dificuldade de ser resolvidos em alguns grupos. As curvas elípticas tem uma estrutura de grupo abeliano quando munidas de uma operação soma, é um exemplo de grupo que dificulta o cálculo logaritmo discreto, por isto iremos estudar algumas propriedades dessas curvas. Além disso, os emparelhamentos de Weil e Tate definidos em pontos de uma curva elíptica se mostraram eficientes para resolver o protocolo tripartido de Diffie-Hellman, entre outras aplicações. Contudo sua implementação é cara computacionalmente, assim veremos uma melhora de ambos que facilitam seus cálculos.

Palavras-chave: Curvas Elípticas. Emparelhamento. Protocolo Diffei-Hellman.

Abstract

In cryptography, one of the challenges is to ensure the secure exchange of keys. This involves utilizing algorithms that leverage the discrete logarithm problem, which is known for its difficulty in certain groups. An example of such a group is the elliptic curve group. In this study, we will explore various properties of this curve. Additionally, the Weil and Tate pairings defined at points on the elliptic curve have proven to be efficient in solving the Diffie-Hellman tripartite protocol and have found applications in various other scenarios. However, their implementation is computationally expensive. Therefore, in this work, we will describe an improvement in both the Weil and Tate pairings that facilitates their calculations.

Keywords: Elliptic Curves. Pairing. Diffie-Hellman protocol.

Lista de ilustrações

Sumário

Introdução

Codificar mensagens para que terceiros não consigam entender seu conteúdo é uma método usada desde o antigo Egito. Atualmente, codificar um texto virou uma ciência que se preocupa muito mais do que apenas cifrar, mas também com a autentificação da mensagem, autentificação do remetente, etc... A Criptografia estuda meios eficientes para tornar um texto simples ilegível, mas também está sempre em busca de como quebrar o sistema.

Para cifrar um texto fazemos uso de algum algoritmo, existem alguns tipos diferentes, cada um utilizando uma técnica, contudo cada algoritmo precisa de uma "chave", que geralmente é um número ou uma lista de números, que vão determinar a regra da cifra. Por muitos anos, foram utilizados métodos de criptografia conhecidos como simétricos, nesses tipos havia somente uma chave, que era usada para cifrar e descifrar um texto. Contudo, esse método tinha um ponto falho, que é, duas pessoas não poderiam trocar mensagens de forma segura sem antes determinar uma chave.

Foi só na década de 70, quando Diffie e Hellman (DIFFIE; HELLMAN, 1976) propuseram um protocolo de troca de chaves, que a falha da criptografia simétrica foi resolvida, isto porque o protocolo garantia que duas pessoas, sem um contato prévio, pudessem trocar chaves de forma segura. Criptografias utilizando esse protocolo são conhecidas como assimétricas isto porque agora são utilizadas duas chaves, uma publica e uma privada. Ou seja, cada indivíduo tem duas chaves, e quando duas pessoas querem se comunicar, elas podem por meio dessas chaves combinar uma, de modo que só elas tenham acesso.

A segurança da criptografia assimétrica está ligada na dificuldade de se resolver o problema do Logaritmo Discreto. Inicialmente, era-se calculado sobre corpos finitos, mas Miller (MILLER, 1986) e Neal koblitz (KOBLITZ, 1987) propuseram (de modo independente) o cálculo utilizando os pontos de uma curva elíptica. Uma das vantagens de se trabalhar com o grupo das curvas elípticas é que o problema do logaritmo discreto fica mais difícil de ser resolvido.

Por conta da dificuldade de resolver o logaritmo discreto, no inicio dos anos 90 os autores (MENEZES; VANSTONE; OKAMOTO, 1991) propuseram um ataque, que transforma o problema do logaritmo discreto em uma curva elíptica, em um problema de logaritmo discreto em um corpo finito. Apesar deste feito, isso só se aplicava a algumas curvas, de modo que esse ataque contribui para fortalecer ainda mais a criptografia em curvas elípticas, pois expunha quais curvas não eram adequadas para se trabalhar em criptografia.

Umas das ferramentas utilizadas no ataque foi o Emparelhamento de Weil, que passou a ser aplicado em criptografias baseadas em identidade (BONEH; FRANKLIN, 2001) e em assinaturas curtas (JOUX, 2002). Além disso, foi proposto o uso do emparelhamento para resolver o problema do protocolo de Diffie e Hellman tripartido (JOUX, 2000). Com uso do Emparelhamento de Weil, também foram propostas aplicações do Emparelhamento de Tate que pode ser vista em (MENEZES, 2009).

Um dos problemas dos Emparelhamento é a sua implementação, pois geralmente são computacionalmente caros, por isso busca-se sempre maneiras alternativas de calculá-los. Miller (MILLER et al., 1986) propôs um algoritmo interativo que ainda é utilizado, e em (EISENTRÄGER; LAUTER; MONTGOMERY, 2004) é dado uma melhora tanto para o Emparelhamento de Weil quanto de Tate.

Desse modo, o objetivo desse trabalho é o estudo das curvas elípticas, e os emparelhamentos de Weil e Tate. Teremos como base o artigo (EISENTRÄGER; LAUTER; MONTGOMERY, 2004), onde estudaremos suas propostas e melhorias. A dissertação está organizada da seguinte maneira:

No Capítulo 1, vamos definir uma variedade afim, e também uma curva algébrica plana afim. Vamos introduzir a ideia do Espaço Projetivo e enunciaremos alguns resultados importantes. Por fim, definiremos alguns elementos estudados na geometria algébrica. No Capítulo 2, abordaremos As Curvas Elípticas, vamos introduzir a Equação de Weierstrass e também verificar que uma curva elíptica munida de uma operação soma é um grupo abeliano.

No Capítulo 3, vamos estudar os Emparelhamento de Weil e Tate, e também iremos definir novos emparelhamentos que são computacionalmente melhores. No Capítulo 4, daremos uma demonstração da melhoria. Por fim, no Capítulo 5, daremos uma aplicação dos emparelhamentos no protocolo tripartido de Diffie-Hellman.

1 Curvas Planas

Neste Capítulo vamos definir algumas estruturas estudadas na geometria algébrica essenciais para o entendimento das curvas elípticas, baseando-se nos livros (SILVERMAN, 2009), (FULTON, 1989) e (VAINSENCHER, 1979) como referencias. Ao longo dessa dissertação vamos considerar K um corpo e $\bar{K}$ seu fecho algébrico.

1.1 Curvas Algébricas

Vamos começar definindo o espaço onde vamos trabalhar, e também as variedades algébricas.

Definição 1. *Seja K um corpo e $\bar{K}$ seu fecho algébrico. O n-Espaço Afim (sobre K) é o conjunto denotado por:*

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{(x_1, x_2, ..., x_n); x_i \in \bar{K} i = 1, 2, ..., n\}.$$

De modo análogo, o conjunto dos pontos K-racionais de $\mathbb{A}^n$ é denotado por:

$$\mathbb{A}^n(K) = \{(x_1, x_2, ..., x_n) \in \mathbb{A}^n; x_i \in K \; i = 1, 2, ..., n\}.$$

Observação 1. *Podemos introduzir no n-espaço afim uma topologia, chamada topologia de Zariski (para mais detalhes ver (FULTON, 1989)). Contudo vamos considerar $\mathbb{A}^n$ apenas como sendo o lugar onde vão "morar"as curvas.*

Denote por $\bar{K}[X] = \bar{K}[x_1, ..., x_n]$ o anel de polinômios de n variáveis. Seja $S \subset \bar{K}[X]$, não vazio. Consideremos o conjunto

$$V_S = \{P \in \mathbb{A}^n; \; f(P) = 0 \; \forall f \in S\}$$

Chamaremos o conjunto da forma V_S de conjunto algébrico. Se um conjunto $V \subset \mathbb{A}^n$ é algébrico, podemos associa-lo a um ideal $I(V)$ de $\bar{K}[X]$ do seguinte modo,

$$I(V) = \{f \in \bar{K}[X]; \; f(P) = 0 \; \forall P \in V\}.$$

Se $I(V)$ é um ideal primo de $\bar{K}[X]$, dizemos então que V é uma variedade (afim). Daremos mais adiante uma definição de dimensão da variedade, contudo nesse trabalho estaremos interessados apenas nas variedade de dimensão um, as quais nomeamos como curvas algébricas.

1.1.1 Curvas Algébricas Planas Afim

Agora vamos definir de forma formal o que é uma curva algébrica plana e qual é a sua diferença com as demais curvas.

Definição 2. *Seja $I = \langle f \rangle \subset \bar{K}[x,y]$ um ideal, onde f é não constante. Chamaremos de* ***curva algébrica plana afim*** *o conjunto da forma*

$$V_I = \{P \in \mathbb{A}^2;\ h(P) = 0\ \forall h \in I\}.$$

Contudo, podemos apenas olhar para o polinômio f que geral o ideal para podermos definir a curva. Ou seja, se $V(f) = \{P \in \mathbb{A}^2 | f(P) = 0\}$, então $V_I = V(f)$. Logo, vamos denotar uma curva sempre por $V(f)$ (ou apenas por f)

Com essa definição estabelecemos classes de equivalências, i.e, f e λf são polinômios, tais que, os ideais gerados por eles são iguais, i.e, $\langle f \rangle = \langle \lambda f \rangle$, então ambos definem a mesma curva $V(f) = V(\lambda f)$. Outra observação é que, a definição distingue curvas do tipo $V(f)$ e $V(f^2)$, pois podemos notar que as curvas geradas por ambos são iguais, contudo no caso de f^2 é como se um ponto P tivesse um "peso"2, ou seja, essa multiplicidade deve ser considerada.

A partir daqui vamos simplificar e dizer apenas curva ao invés de curva algébrica.

Exemplo 1. *Um caso simples para ver que f e f^2 são curvas diferentes é considerar $f(x,y) = x$ e $f^2(x,y) = g(x,y) = x^2$. note que g é o limite de $g_t(x,y) = x^2 - t^2$, com $t \in \bar{K}$ quando $t \to 0$. Assim se traçarmos uma reta na altura $y = 1$ ela vai interceptar g_t em dois pontos distintos, e quando $t \to 0$ esses pontos convergem para um único ponto.*

Além disso, vamos dizer que $V(f) \subseteq \mathbb{A}^2$ está **definida** sobre K se $f \in K[x,y]$, f não constante. Vamos denotar por $V(f)/K$ se $V(f)$ é definida sobre K, e $V(K) = V(f) \cap \mathbb{A}^2(K)$ o **conjunto dos pontos K-racionais** de $V(f)$.

Definição 3. *Dizemos que uma curva algébrica plana $V(f) \subset \mathbb{A}^2$ é* ***redutível*** *se $f = g \cdot h$, onde $g, h \in \bar{K}[x,y]$ são polinômios não constantes e $V(f) = V(g) \cup V(h)$. Caso contrario, dizemos que a curva é* ***irredutível****.*

Exemplo 2. *Sejam $\langle f \rangle$ e $\langle g \rangle$ ideais com $f, g \in \bar{K}[x,y]$ não constantes. Se $\langle f \rangle \subseteq \langle g \rangle$ então $V(f) \supseteq V(g)$, pois dado $P \in V(g)$ como $f \in \langle g \rangle$, logo $f = g \cdot h$ para algum $h \in \bar{K}[x,y]$. Assim, $0 = g(P) \cdot h(P) = f(P)$, portanto $P \in V(f)$.*

Proposição 1. *Uma curva algébrica plana $V(f) \subset \mathbb{A}^2$ é irredutível se, e somente se, $\langle f \rangle$ é um ideal primo.*

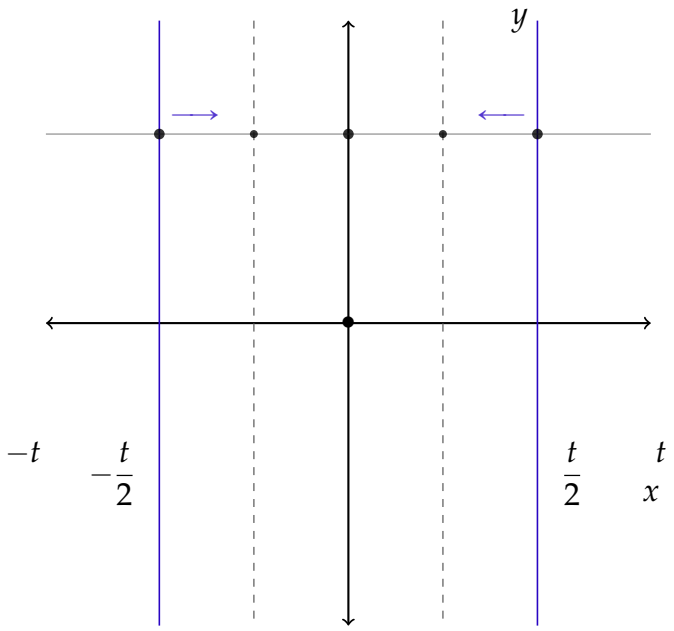

Figura 1 – Uma representação do Exemplo 1

Demonstração. Primeiramente, suponha $V(f)$ irredutível e que $\langle f \rangle$ não é primo. Seja $f_1 \cdot f_2 \in \langle f \rangle$ tal que $f_1, f_2 \notin \langle f \rangle$. Segue que

$$\langle f_1 \cdot f_2 \rangle \subset \langle f \rangle \Rightarrow V(f) \subset V(f_1.f_2)$$

Ou seja, $V(f) \subset V(f_1 \cdot f_2) = V(f_1) \cup V(f_2)$. Se $V(f) \subset V(f_1)$ (resp. $V(f_2)$), então $\langle f_1 \rangle \subset \langle f \rangle$ (resp. $\langle f_2 \rangle \subset \langle f \rangle$). Contradição, pois $f_1 \notin \langle f \rangle$ (resp. $f_2 \notin \langle f \rangle$).

Por outro lado, suponha que $\langle f \rangle$ é primo e $V(f)$ redutível. Como $V(f)$ é redutível podemos escrever $f = g \cdot h$ como $g, h \in \bar{K}[x, y]$. Então $g \cdot h \in \langle f \rangle$ contudo $g, h \notin \langle f \rangle$, contradição. □

No estudo de curvas, uma ferramenta importante são as afinidades (transformações afins), que podemos ver como uma mudança de coordenadas, isto porquê algumas propriedades importantes das curvas planas são invariantes pelas afinidades.

Definição 4. *Uma **transformação afim** ou **afinidade** em K^2 é uma aplicação*

$$T : K^2 \to K^2,$$

composta de uma translação com um isomorfismo linear.

Observação 2. *Se tomarmos um isomorfismo linear composto com uma translação, ainda será uma transformação afim, contudo não necessariamente a mesma.*

Definição 5. *Seja T uma afinidade. O $\bar{K}$-automorfismo do anel de polinômios em 2 variáveis associado a T é dado por*

$$\overline{T} : \bar{K}[x, y] \to \bar{K}[x, y]$$

onde $\left(\overline{T} \cdot f\right)(x,y) = f\left(T^{-1}(x,y)\right)$

Proposição 2. *Sejam $V(f)$ uma curva e T uma afinidade. Então $V(\overline{T} \cdot f) = T(V(f))$.*

Demonstração. Ver (VAINSENCHER, 1979). □

Exemplo 3. *Considere a curva definida por $E : y^2 + a_1xy + a_3y = x^3a_2x^2 + a_4x + a_6$, vamos encontrar a única família de mudanças de coordenadas que preservam a equação. Dada T uma afinidade, temos que,*

$$x = ax' + by' + c,$$

$$y = a'x' + b'y' + c'.$$

Ou seja, reescrevemos x e y como função das novas variáveis. Fazendo a substituição em E, vamos olhar para os termos x^3 e y^2

$$x^3 = (ax' + by' + c)^3,$$

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

Concluímos que $b = 0$, (pois não queremos que apareça um y'^3), e $a^3 = b'^2$ (para que mantenha a forma da equação). Com os demais termos não iremos ter nenhum problema. Definimos por fim,

$$u = \frac{b'}{a} \qquad \text{e} \qquad s = \frac{a'}{u}$$

Com essas mudanças, obtemos que

$$x = u^2x' + c,$$

$$y = u^2sx' + u^3y + c.$$

Definição 6. *Dizemos que uma propriedade* P *relativa a curvas é* ***invariante*** *ou* ***independente do referencial*** *se, para toda afinidade T, uma curva $V(f)$ satisfaz* P *se, e só se $V(T_\bullet f)$ satisfaz* P.

Exemplo 4. *O grau de uma curva é uma propriedade invariante; se duas curvas se interceptam num ponto P então suas afinidades vão se interceptar no ponto $T(P)$ para alguma afinidade T.*

1.1.2 Curvas Singulares

Vamos agora introduzir uma noção de ponto suave, uma das características desses pontos é a unicidade de retas tangentes, tal importância ficará mais evidente no Capítulo 2, quando formos definir uma operação de grupo nos pontos de uma curva elíptica.

Definição 7. *Seja $V(f)$ uma curva plana afim e $P \in V(f)$. Dizemos que P é um* ***ponto singular*** *se*

$$\frac{\partial f}{\partial x}(P) = 0 = \frac{\partial f}{\partial y}(P).$$

Caso contrário, dizemos que P é um ponto ***não singular*** *(ou* ***suave****).*

Se $P = (a, b) \in V(f)$ é um ponto suave, definimos a **reta tangente** a $V(f)$ em P por

$$T_P f := \frac{\partial f}{\partial x}(P)(x - a) + \frac{\partial f}{\partial y}(P)(y - b)$$

Exemplo 5. *Seja $f \in \bar{K}[x, y]$ um polinômio não constante de grau d, seja também $P = (a, b) \in V(f)$. Podemos considerar uma afinidade T, tal que $T(P) = (0, 0)$ e $T \cdot f(x, y) = g(x, y)$. Podemos escrever*

$$g(x, y) = g_m(x, y) + g_{m+1}(x, y) + \cdots + g_d(x, y) \text{ com } g_i \text{ homogêneo de grau i e } g_m \neq 0$$

Temos então que:

Definição 8. *A* ***multiplicidade*** *de $P \in V(f)$ é definida por $\text{mult}_P f := m$. Além disso, se $m \geqslant 2$ dizemos que P é um* ***ponto múltiplo ordinário*** *se existem exatamente m retas tangentes distintas a $V(f)$ em P.*

Pontos duplos ordinários, ou seja $m = 2$, são ditos **nós**, e pontos duplos com uma única tangente são ditos **cúspides**.

Exemplo 6. *O ponto $P = (0, 0)$ na curva $V(y^2 - x^3 - x^2)$ é um ponto de nó, pois podemos escrever $y^2 - x^3 - x^2 = (y^2 - x^2) - x^3$, note que $y^2 - x^2$ é homogêneo de grau dois e $y^2 - x^2 = (x + y)(x - y)$ tendo assim duas retas tangente em P.*

Agora, considerando $P = (0, 0)$ em $V(y^2 - x^3)$ temos que P é um ponto de cúspide, pois $y^2 = (y - 0x)^2$ é o termo homogêneo de menor grau, logo teremos apenas um reta tangente dada por $r : y$.

Proposição 3. *Uma curva algébrica plana afim possui um numero finito de pontos singulares.*

Demonstração. (SILVERMAN, 2009) □

1.2 Plano Projetivo

O Plano Projetivo é uma particularização do Espaço Projetivo, fazemos uso de tal espaço para podermos definir de modo formal o que seria os pontos no infinito. Vamos, primeiramente, definir o Espaço Projetivo, e em seguida, olhar para o Plano Projetivo.

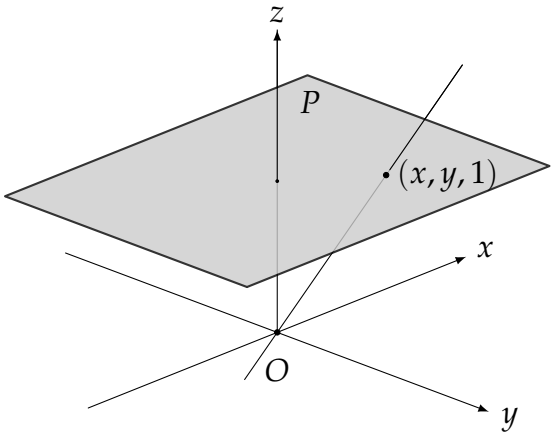

Figura 2 – Plano Projetivo

Definição 9. *O n-**espaço projetivo** definido sobre um corpo K, denotado por* $\mathbb{P}^n$ *(ou* $\mathbb{P}^n(\overline{K})$ *para ressaltar que estamos olhando para o fecho algébrico de K) é definido como*

$$\mathbb{P}^n := \frac{\bar{K}^{n+1}}{\sim},$$

onde $\sim$ *é a relação de equivalência dada por*

$$P_1 \sim P_2 \iff \exists \lambda \in \bar{K}^*, \text{ tal que, } P_1 = \lambda P_2.$$

Os pontos em $\mathbb{P}^n$*, denotados por* $[x_0 : x_1 : \cdots : x_n]$*, são classes de equivalência*

$$[x_0 : x_1 : \cdots : x_n] = \{(\lambda x_0, ..., \lambda x_n) \in \mathbb{A}^{n+1}; \lambda \in \overline{K}^*\}$$

O Plano Projetivo é um caso particular quando $n = 2$, ou seja, o plano projetivo $\mathbb{P}^2 = \mathbb{P}^2(\overline{K})$ é dado por

$$\mathbb{P}^2 := \frac{\overline{K}^3 \backslash (0,0,0)}{(x,y,z) \sim \lambda(x,y,z)}.$$

Pode ser visto também como o conjunto das retas de $\bar{K}^3$ que passam pela origem (ex. figura 2).

Exemplo 7. *O espaço afim* $\mathbb{A}^2$ *pode ser mergulhado em* $\mathbb{P}^2$ *através do seguinte mapa*

$$\phi : \mathbb{A}^2 \hookrightarrow \mathbb{P}^2 \text{ dado por } \phi(x,y) = [x : y : 1].$$

Consideremos $U = \phi(\mathbb{A}^2) = \{[x : y : 1] \in \mathbb{P}^2\}$. Se pegarmos $[x : y : z] \in \mathbb{P}^2$, tal que, $z \neq 0$ podemos dividir todas as entradas por z. Logo teremos

$\left[\frac{x}{z} : \frac{y}{z} : 1\right]$ que é equivalente a $[x : y : z]$ no plano projetivo. Desse modo, conseguimos recuperar/encontrar o ponto em $\mathbb{A}^2$ que leva em $[x : y : z]$. Concluímos assim que todo ponto de $\mathbb{P}^2$ tal que $z \neq 0$ está na imagem da ϕ.

Agora, considere $\mathbb{P}^2 \backslash U = \{[x : y : 0] \in \mathbb{P}^2\} = \{$ retas em $z = 0$ passando pela origem $\}$. Cada reta no plano é um ponto em $\mathbb{P}^2$, desse modo, para cada direção do plano afim vamos agregar um ponto, a esses pontos damos o nome de **pontos no infinito**.

Observação 3. *A maneira que mergulhamos $\mathbb{A}^2$ em $\mathbb{P}^2$ não é única, por exemplo, poderíamos enviar $(x, z) \longmapsto [x : 1 : z]$ e com isso, poderíamos também tomar os pontos no infinito como sendo os pontos da forma $[x : 0 : z]$. Para simplificar, vamos sempre considerar os pontos no infinito como sendo os que tem $z = 0$.*

Observação 4. *A noção de pontos no infinito pode ser estendida para espaços projetivos de dimensão maiores.*

1.2.1 Variedades projetivas

Vamos definir uma variedade projetiva em $\mathbb{P}^n$, contudo nosso foco será nas curvas, que são variedades de dimensão um. Em seguida vamos ver alguns resultados para curvas projetivas que estão em $\mathbb{P}^2$.

Definição 10. *Um polinômio $F \in \bar{K}[X]$ é dito **homogêneo de grau** d se $F(\lambda x_0, \lambda x_1, ..., \lambda x_n) = \lambda^d F(x_0, x_1, ..., x_n)$.*

Consideramos polinômios homogêneos, já que no espaço projetivo estamos trabalhando com representantes de classes de equivalências, assim o zero de um polinômio não pode depender do representante escolhido. Ficará mais claro quando estivermos trabalhando com curvas projetivas planas.

Um ideal I em $\bar{K}[X]$ é dito **homogêneo**, se é gerado por polinômios homogêneos. Considere

$$V_I = \{P \in \mathbb{P}^n; f(P) = 0 \forall f \in I, f \text{ homogêneo}\}.$$

Definição 11. *$V \in \mathbb{P}^n$ é dito um **conjunto algébrico projetivo** se é da forma V_I. Além disso, dado um conjunto algébrico projetivo associamos ao seu ideal homogêneo $I(V)$ em $\bar{K}[X]$*

$$I(V) = \{f \in \bar{K}[X]; f \text{ homogêneo}, f(P) = 0 \forall P \in V\}.$$

Definição 12. *Um conjunto algébrico projetivo é dito uma **variedade** se seu ideal I(V) de polinômios homogêneos é primo.*

Variedades de dimensão um são ditas curvas. Enunciaremos alguns resultados de curvas projetivas planas, i.e, curvas contidas em $\mathbb{P}^2$ que serão uteis no próximo capítulo.

1.2.2 Curvas Projetivas

Como fizemos no espaço afim, vamos definir uma curva no plano projetivo (que chamaremos de curva projetiva). Primeiramente, vamos tomar o polinômio $F : x^2 + y + z$ em $\bar{K}[x, y, z]$, note que o ponto $[1 : 0 : -1]$ é um zero de F, contudo $[2 : 0 : -2] = 2[1 : 0 : -1]$ não zera F, mas no plano projetivo ambos são equivalente. Então se quiser definir uma curva como sendo zeros de um polinômio, temos que tomar o cuidado de que F se anule independente do representante. Para contornar esse problema, vamos trabalhar com polinômios homogêneos.

Logo, se F é homogêneo e $[x : y : z]$ é um ponto que anula F, então $\lambda[x : y : z]$ também anula F para qualquer λ. Sendo assim, vamos trabalhar com polinômios homogêneos quando estivermos no espaço projetivo.

Para simplificar, denotaremos por f quando estivermos no plano afim ($f \in \bar{K}[x, y]$) e por F quando estivermos no caso projetivo ($F \in \bar{K}[x, y, z]$).

Definição 13. *Seja $I = \langle F \rangle \subset \bar{K}[x, y, z]$ um ideal gerado por um polinômio homogêneo. Definimos uma curva plana projetiva como sendo*

$$C_I := \{P \in \mathbb{P}^2; F(P) = 0 \quad \forall F \in I, F \text{ homogêneo}\}.$$

Como já discutido para o caso afim, basta olhar os pontos que anulam o polinômio gerador. Daqui em diante, quando nos referirmos a curvas, estamos falando de uma curva plana projetiva, e também vamos denotar por $C(F)$ a curva associada ao polinômio homogêneo F. Vamos definir para o caso projetivo o que já foi definido para o caso afim.

Definição 14. *Seja $C(F)$ uma curva e $P \in C(F)$. Dizemos que P é um* ***ponto singular*** *se*

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial Z}(P) = 0.$$

Caso contrário, dizemos que P é um ponto ***não singular (ou suave)****.*

Seja $P \in C(F)$ um ponto suave definimos a reta tangente a $C(F)$ em P por

$$T_P F : \frac{\partial F}{\partial x}(P)x + \frac{\partial F}{\partial y}(P)y + \frac{\partial F}{\partial z}(P)z.$$

Definição 15. *Seja $C(F)$ uma curva. Dizemos que é redutível se existem polinômios homogêneos $G, H \in \bar{K}[x, y, z]$ não constantes, tal que, $F = G \cdot H$, assim $C(F) = C(G) \cup C(H)$. Caso contrário, dizemos que $C(F)$ é irredutível.*

Se $C(F)$ é uma curva, podemos escrever $C(F) = C(F_1) \cup \ldots \cup C(F_n)$, onde cada F_i é um fator irredutível do polinômio F, ou seja, cada $C(F_i)$ é uma curva irredutível. Nosso objetivo é contar a interseção de curvas que não tem componentes irredutíveis em comum, para isto, vamos primeiro definir o que é uma projetividade (mudança de coordenadas projetivas).

As transformações lineares invertíveis em $\bar{K}^3$ formam um grupo, denotado por $Gl_3(\bar{K})$. Dado $\varphi \in Gl_3(\bar{K})$, note que, φ leva retas que passam pela origem (em $\bar{K}^3$), em retas que passam pela origem. Ou seja, φ induz uma bijeção em $\mathbb{P}^2$, tomando o cuidado de que, φ e $\lambda\varphi$ ($\lambda \in \bar{K}$) são equivalentes quando olhadas como aplicações de $\mathbb{P}^2$ em $\mathbb{P}^2$, definimos

$$PGl_2(\bar{K}) := \frac{Gl_3(\bar{K})}{\bar{K}^*}$$

como sendo o conjunto das projetividades, PGl_2 é um grupo com respeito a composição, logo a composta de duas projetividade ainda é uma projetividade, como também, a inversa de uma projetividade é uma projetividade.

De maneira análoga ao caso afim, uma projetividade induz um K- isomorfismo, i.e, seja $\varphi \in PGl_2(\bar{K})$

$$\varphi_\bullet : \bar{K}[x,y,z] \to \bar{K}[x,y,z]$$

para todo $(x,y,z) \in \bar{K}^3$ e $F \in \bar{K}[x,y,z]$

$$(\varphi_\bullet F)(x,y,z) = F(\varphi^{-1}(x,y,z))$$

Definição 16. *Duas curvas F e G são ditas projetivamente equivalentes, se existe um projetividade $\varphi \in PGl_2(\bar{K})$, tal que, $F = \varphi_\bullet G$.*

Um resultado importante no estudo da Geometria Algébrica é o teorema de Bézout, que afirma que, se duas curvas F e G não tem componentes irredutíveis em comum, então o número de pontos em $C(F) \cap C(G)$, contando suas devidas multiplicidades, é $grau(F).grau(G)$.

Teorema 1 (Propriedades característica do índice de interseção)**.** *Seja χ_k o conjunto das curvas projetivas planas em $\mathbb{P}^2$. Então existe uma única aplicação*

$$I : \mathbb{P}^2 \times \chi_k \times \chi_k \longrightarrow \mathbb{Z}_{\geqslant 0} \cup \{\infty\}$$

$$(P,F,G) \longmapsto I(P,G,F)$$

Satisfazendo as seguintes propriedades :

1. $I(P,F,G) = I(P,G,F)$
2. $I(P,F,G) = \infty \Leftrightarrow P$ *pertence a uma componente comum de F e G*

3. $I(P,F,G) = 0 \Leftrightarrow P \notin F \cap G$
4. $\forall \phi \in PGL_2\ I(P,F,G) = I(\phi(P), \phi F, \phi G)$
5. $I([0:0:1], X, Y) = 1$
6. $I(P,F,GH) = I(P,F,G) + I(P,F,H)$
7. $I(P,F,G) = I(P,F,G+FH)$, *onde* H *é homogêneo de grau* $deg(G) - deg(F) \geqslant 1$

Demonstração. (VAINSENCHER, 1979) □

Exemplo 8. *Considere a curva dada por* $E : F(X,Y,Z) = Y^2Z + a_1XYZ - a_2X^2Z + a_3YZ^2 - a_4XZ^2 - a_6Z^3 - X^3$. *A equação da reta tangente à E no ponto O é dada por*

$$L : \frac{\partial F}{\partial x}(O)x + \frac{\partial F}{\partial y}(O)y + \frac{\partial F}{\partial Z}(O)z = 0$$

É fácil ver que apenas o termo $\frac{\partial F}{\partial Z}(O)$ *será diferente de zero, sendo* $\frac{\partial F}{\partial Z}(O) = 1$. *Logo,* $L : z$.

Vamos calcular o grau de interseção de L e E utilizando o Teorema do índice de interseção. Primeiramente considere $H : Y^2 + a_1XY + a_xYZ - a_2X^2 - a_4XZ - a_6Z^2$. *Agora, temos que*

$$I(O,L,E) = I(O,L,E-HL) \Longrightarrow I(O,L,E) = I(O,Z,X^3)$$

utilizando a propriedade 6, $I(O,Z,X^3) = 3I(O,Z,X) = 3.1 = 3$.

Teorema 2 (Bézout)**.** *Seja F,G duas curvas planas projetivas. Se F e G não tem componentes irredutíveis em comum, então* $\#F \cap G = deg(F)deg(G)$ *contando as devidas multiplicidades de interseções.*

Demonstração. (VAINSENCHER, 1979) □

1.2.3 Homogenezação de Curvas

Sabemos que podemos mergulhar $\mathbb{A}^2$ em $\mathbb{P}^2$, então dada uma curva plana afim, quando aplicamos ϕ a sua imagem vai ser uma curva plana projetiva.

Exemplo 9. *Considere em* $\mathbb{A}^2$ *a seguinte curva plana* $V(f : ax + by + c)$ *(vamos supor* $a, b, c \neq 0$*). Quando aplicamos* ϕ *em* $V(ax+by+c)$ *temos como imagem os pontos* $\left[x : \frac{-ax-c}{b} : 1\right]$, *olhando* $\mathbb{P}^2$ *como sendo* $\bar{K}^3$, *que cada ponto é uma reta saindo de* $(0,0,0)$ *passando por* $\left[x : \frac{-ax-c}{b} : 1\right]$. *Vamos ter assim um plano de equação* $ax + by + cz = 0$, *onde* $F : ax + by + c$ *é um polinômio homogêneo. Agora a curva projetiva* $C(F)$ *pode ser vista como sendo*

$$C(F) = \{[x:y:z] \in \mathbb{P}^2; ax+by+cz = 0\} = \{[x:y:1] \in \mathbb{P}^2; ax+by+c = 0\}$$
$$\cup \{[x:y:0] \in \mathbb{P}^2; ax+by = 0\} = V(f) \cup \left\{\left[x : \frac{-ax}{b} : 0\right]\right\}$$

Note que podemos multiplicar $\left[x : \frac{-ax}{b} : 0\right]$ *por* b/x *e obtemos o representante* $[b : -a : 0]$. *Logo,* $C(F) = V(F) \cup \{[b : -a : 0]\}$, *podemos interpretar que* $V(f)$ *tem um ponto no infinito.*

Vamos definir o resultado acima para o caso geral.

Definição 17. *Seja* $f = \sum_{i=0}^{d} f_i$ *onde cada* $f_i \in \bar{K}[x,y]$ *é homogêneo de grau i,* $f_d \neq 0$. *A* ***homogenização*** *de* f *é o polinômio homogêneo de grau d*

$$F(x,y,z) = \sum_{i=0}^{d} z^{d-i} f_i(x,y)$$

Exemplo 10. *Seja* $f = \sum_{i=0}^{d} f_i$ *onde cada* $f_i \in \bar{K}[x,y]$ *é homogêneo de grau i,* $f_d \neq 0$, *é fácil ver que os pontos no infinito estão determinados por* f_d, *pois tomando* $z = 0$ *em* $F(x,y,z) = \sum_{i=0}^{d} z^{d-i} f_i(x,y)$, *ficamos apenas com* $f_d(x,y) = \prod_{j=1}^{l} (a_j x + b_j y)^{m_j}$ *com* $\sum_{j=1}^{l} m_j = d$, *ou seja* $[b_i : -a_i : 0]$ *são os pontos e* m_j *é dito a multiplicidade de interseção de F e z em* $[b_j : -a_j : 0]$.

1.3 Mapas Entre Curvas

Vamos definir e enunciar alguns resultados que auxiliam na construção do emparelhamento de Weil. Os resultados presentes nessa seção podem ser encontrado em (SILVERMAN, 2009)

Definição 18. *Sejam* C_1 *e* C_2 *curvas projetivas em* $\mathbb{P}^n$. *Um mapa racional de* C_1 *para* C_2 *é dado na forma*

$$\phi : C_1 \longrightarrow C_2 \quad \text{tal que} \quad \phi = [f_0, ..., f_n],$$

de modo que, se as funções $f_0, ..., f_n \in \bar{K}(C_1)$ *são todas definidas em* $P \in C_1$, *então*

$$\phi(P) = [f_0(P), ..., f_n(P)] \in C_2.$$

Um mapa onde as funções são definidas em todos os ponto de C_1 é dito uma **morfismo**. Além disso, vamos dizer que C_1 e C_2 são isomorfas, se existirem mapas $\phi : C_1 \to C_2$ e $\psi : C_2 \to C_1$, tal que, $\phi \circ \psi$ e $\psi \circ \phi$ são a identidade.

Exemplo 11. *Considere* $C : Z^2 = X^2 + Y^2$ *e o mapa* $\phi : C_1 \longrightarrow \mathbb{P}^1$ *dado por* $\phi = [X + Y, Y]$. *Verifica-se que* ϕ *é regular em todos os pontos, e mais, que C é isomorfa a* $\mathbb{P}^1$.

Teorema 3. *Seja* $\phi : C_1 \longrightarrow C_2$ *um morfismo de curvas, então ou* ϕ *é constante ou* ϕ *é sobrejetiva.*

1.3.1 Isogenia

Definição 19. *Sejam E_1 e E_2 curvas elípticas. Uma **isogenia** de E_1 para E_2 é um morfismo ϕ satisfazendo $\phi(O) = O$*

*Duas curvas elípticas são **isogênicas** se existir uma isogênia, tal que, $\phi(E_1) \neq \{O\}$.*

Exemplo 12. *Seja E uma curva elíptica e $m > 0$ um numero inteiro. Definimos a isogenia multiplicação por m*

$$[m] : E \longrightarrow E \quad \text{tal que} \quad [m](P) = P \oplus P \oplus \cdots \oplus P.$$

De maneira similar, definimos para o caso $m < 0$.

Definição 20. *Sejam E uma curva elíptica e $m > 1$ um inteiro. O **subgrupo** $m-$**torção** de E, denotado por $E[m]$ é definido como*

$$E[m] = \{P \in E; [m](P) = O\}.$$

2 Curvas Elípticas

Neste capitulo vamos abordar as curvas elípticas e trabalharemos com algumas propriedades particulares que essa família de curvas satisfazem.

2.1 Equação de Weierstrass

Uma curva da forma

$$Y^2Z + a_1XYZ - a_2X^2Z + a_3YZ^2 - a_4XZ^2 - a_6Z^3 - X^3 = 0 \tag{2.1}$$

onde $a_1, ..., a_6 \in \bar{K}$, é dita uma curva elíptica. Note que,tendo o plano $Z = 0$ como sendo os pontos no infinito, $O = [0 : 1 : 0]$ será o único ponto no infinito dessa família de curvas. Uma segunda observação, é que essa família de curva é suave. Assim nosso primeiro passo é tentar simplificar o máximo a equação obtida a partir da afinização de (2.1).

Vamos denotar por E a curva elíptica plana afim, obtida quando tomamos $Z = 1$, ou seja,

$$E : y^2 + a_1xy - a_2x^2 + a_3y - a_4x - x^3 - a_6 = 0$$

Com $O = [0 : 1 : 0]$ sendo o ponto no infinito, essa equação é chamada de Equação de Weierstrass. Supondo que $char(K) \neq 2$, podemos fazer a seguinte mudança de variável

$$y \longmapsto \frac{1}{2}(y - a_1x - a_3)$$

logo,

$$E : \left(\frac{1}{2}(y - a_1x - a_3)\right)^2 + a_1x\left(\frac{1}{2}(y - a_1x - a_3\right) + a_3\left(\frac{1}{2}(y - a_1x - a_3)\right) = x^3 + a_2x^2 + a_4x + a_6$$

Multiplicando por 4 ambos os lados vamos ter:

$$E : (y^2 + a_1^2x^2 - 2a_1xy + 2a_1a_3x - 2a_3y + a_3^2) + (2a_1xy - 2a_1^2x^2 - 2a_1a_3x) + (2a_3y - 2a_3a_1x - 2a_3^2) = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6$$

$$\Updownarrow$$

$$E : y^2 - a_1^2x^2 - 2a_1a_3x = 4x^3 + 4a_2x^2 + 4a_4x + 4a_6$$

$$\Updownarrow$$

$$E : y^2 = 4x^3 + x^2(4a_2 + a_1^2) + x(4a_4 + 2a_1a_3) + (4a_6 + a_3^2).$$

Defina

$$b_2 = 4a_2 + a_1^2, \qquad 2b_4 = 4a_4 + 2a_1a_3, \quad \text{e} \quad b_6 = 4a_6 + a_3^2, \text{ então,}$$

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.$$

Se $char(\bar{K}) \neq 2, 3$ podemos "simplificar"ainda mais a equação de Weierstrass fazendo a seguinte mudança de coordenadas

$$(x, y) \longmapsto \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right),$$

$$E : \left(\frac{y}{108}\right)^2 = 4\left(\frac{x - 3b_2}{36}\right)^3 + b_2\left(\frac{x - 3b_2}{36}\right)^2 + 2b_4\left(\frac{x - 3b_2}{36}\right) + b_6$$

$$\Updownarrow$$

$$E : y^2 = (x^3 - 9b_2x^2 + 27b_2^2x - 27b_2^3) + (9b_2x^2 - 54b_2^2x + 3^4b_2^3) + (2^33^4b_4x - 2^33^5b_2b_4) + 108^2b_6$$

$$\Updownarrow$$

$$E : y^2 = x^3 + x(-27b_2^2 + 27(24b_4)) + (54_2^3 - 54(36b_2b_4) + 54(216b_6))$$

Defina

$$c_4 = b_2^2 - 24b_4 \quad \text{e} \quad c_6 = -b_2^3 + 36b_2b_6 - 216b_6.$$

Logo temos a expressão

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

O que fizemos é uma mudança particular do Exemplo 3, além disso, a partir da equação de Weierstrass definimos:

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_5 + a_2a_3^2 - a_4^2$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

$$j = \frac{c_4^3}{\Delta}$$

Definição 21. *Δ é o Discriminante da equação de Weierstrass. j é dito $j-$invariante da curva elíptica.*

Se tomarmos um curva elíptica E dada pela equação de Weierstrass, já temos que,

$$x = u^2x' + r \qquad \text{e} \qquad y = u^3y' + u^2sx' + t \tag{2.2}$$

com $u, r, s, t \in \bar{K}$, é a única mudança de coordenadas que preserva a equação de Weierstrass. Através de cálculos encontramos os valores do discriminante e do j-invariante da curva elíptica após aplicarmos a mudança

$$u^{12}\Delta' = \Delta \qquad j' = j$$

Perceba que, apos aplicarmos uma mudança de coordenadas, o j-invariante não se altera, veremos adiante que duas curvas elípticas são isomorfas, se e somente se, tem os mesmo j-invariante.

Supondo que $char(K) \neq 2, 3$ temos nossa curva elíptica dada pela equação

$$y^2 = x^3 + Ax + B, \qquad \text{com } A, B \in \bar{K}.$$

Nessa condições, temos

$$\Delta = -16(4A^3 + 27B^2) \qquad \text{e} \qquad j = -1728\frac{(4A)^3}{\Delta}$$

Lema 1. *Seja $p(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ um polinômio de grau três, temos que $p(x)$ possui raiz dupla se, e somente se $\Delta = 0$. Onde $\Delta = 18a_0a_1a_2 - 4a_0a_2^3 + a_1^2a_2^2 - 4a_1^3 - 27a_0^2$*

Além disso, temos o seguinte resultado

Proposição 4. *Uma curva elíptica E dada pela equação de Weierstrass satisfaz:*

(i) E é não-singular $\Leftrightarrow \Delta \neq 0$;

(ii) E é nodal $\Leftrightarrow \Delta = 0$ e $c_4 \neq 0$;

(iii) E é uma cúspide $\Leftrightarrow \Delta = c_4 = 0$

Demonstração. Vamos fazer a demonstração para o caso $char(K) \neq 2, 3$.

(i) Podemos supor $E : y^2 = x^3 + Ax + B$.

$\Longrightarrow$: Suponha $\Delta = 0$, i.e, $-4A^3 - 27B^2 = 0$. Logo teremos uma raiz dupla para $p(x) = x^3 + Ax + B$. Se x_0 é a raiz dupla, então para o ponto $(x_0, 0)$ temos que $\frac{\partial f}{\partial x}(x_0, 0) = 0$ e $\frac{\partial f}{\partial y}(x_0, 0) = 0$. Logo E é singular.

$\Longleftarrow$: Suponha E singular, então $P = (x_0, y_0)$ é um ponto singular se satisfaz

$$2y_0 = 3x_0^2 + A = 0.$$

Assim, x_0 é uma raiz dupla de $x^3 + AX + B$, ou seja $\Delta = 0$.

Faremos os itens (ii) e (iii) simultaneamente, considere a curva elíptica

$$E : y^2 + a_1xy - a_2x^2 + a_3y - a_4x - x - a_6 = 0$$

Primeiramente, se E é singular no ponto $P = (x_0, y_0)$, pelo item (i) já temos que $\Delta = 0$. Agora, note que, fazendo uma mudança de variável

$$x = x' + x_0 \qquad y = y' + y_0$$

satisfaz (2.2), tendo $u = 1$ e $s = 0$. Nessas condições tanto Δ como c_4 são invariantes. Podemos assim, sem perda de generalidade supor $P = (0, 0)$. Então

$$a_6 = f(0,0) = 0 \qquad a_4 = \frac{\partial f}{\partial x}(0,0) = 0 \qquad a_3 = \frac{\partial f}{\partial y}(0,0) = 0$$

ou seja,

$$E : y^2 = x^3 + a_2x^2 - a_1xy.$$

Temos também que $c_4 = a_1^2 + 4a_2$. Agora temos $f_2(x, y) = y^2 + a_1xy - x^2$ fator homogêneo de menor grau, pela Definição 8 P é um ponto de nó se, e só se, f_2 pode ser escrito em dois fatores, isto ocorre se, e somente se, $a_1^2 + 4a_2 \neq 0$ (discriminante considerando f_2 apenas na variável y) Analogamente, P é um cúspide $\Leftrightarrow a_1^2 + 4a_2 = 0$ □

Proposição 5. *Duas curvas elípticas são isomorfas sobre $\bar{K}$ se, e somente se ambas tem o mesmo j-invariante.*

Demonstração. Primeiramente, se duas curvas elípticas são isomorfas, temos que só há uma família de mudanças de variáveis que mantém a equação de Weierstrass, e como vimos os j-invariantes serão iguais. Agora, sejam E_1 e E_2 curvas elípticas com os mesmos j-invariantes. Por simplicidade, vamos supor $char(K) \geqslant 5$ e escrevemos

$$E_1 : y^2 = x^3 + A_1x + B_1 \qquad E_2 : y^2 = x^3 + A_2x + B_2$$

Pela hipótese de $j(E_1) = j(E_2)$ segue que

$$\frac{(4A_1)^3}{4A_1^3 + 27B_1^2} = \frac{(4A_2)^3}{4A_2^3 + 27B_2^2}$$

$$\Rightarrow (4A_1)^3(4A_2^3 + 27B_2^2) = (4A_2)^3(4A_1^3 + 27B_1^2)$$

Simplificando a expressão obtemos

$$A_1^3B_2^2 = A_2^3B_1^2 \tag{2.3}$$

Vamos verificar que E_1 e E_2 são isomorfas através do isomorfismo

$$(x, y) \longmapsto (u^2x', u^3y')$$

Temos os seguintes casos:

A) Se $j = 0$, então $A_1 = A_2 = 0$, devemos ter B_1 e B_2 diferentes de zero.

$$E_1 : y^2 = x^3 + B_1 \qquad E_2 : y^2 = x^3 + B_2$$

Saindo de E_1, vamos encontrar u de modo a termos o isomorfismo,

$$(u^3y)^2 = (u^2x)^3 + B_1 \Rightarrow u^6y^2 = u^6x^3 + B_1 \Rightarrow y^2 = x^3\frac{B_1}{u^6}$$

Logo, $B_2 = \frac{B_1}{u^6}$, então $u = \left(\frac{B_1}{B_2}\right)^{1/6}$

B) Se $j = 1728$, logo $B_1 = B_2 = 0$ e $A_1, A_2 \neq 0$. Desta forma, obtemos

$$E_1 : y^2 = x^3 + A_1x \qquad E_2 : y^2 = x^3 + A_2x$$

De modo análogo ao que foi feito em A),

$$(u^3y)^2 = (u^2x)^3 + A_1x \Rightarrow y^2 = x^3 + \frac{A_1}{u^6} \Rightarrow u = \left(\frac{A_1}{A_2}\right)^{1/4}.$$

C) Se $j \neq 0, 1728$ nesse caso, $A_1B_1 \neq 0$, ou seja, $A_2B_2 \neq 0$, isso porque, caso um deles fosse por conta da igualdade (2.3) o outro também deveria ser.

$$E_1 : y^2 = x^3 + A_1x + B_1 \qquad E_2 : y^2 = x^3 + A_2x + B_2$$

Repetindo os passou feitos em A) e B), vamos obter, u = $\left(\frac{B_1}{B_2}\right)^{1/6}$ e $u = \left(\frac{A_1}{A_2}\right)^{1/4}$, contudo de (2.3) temos que são iguais, então u está bem definido.

□

Definição 22. *Uma equação de Weierstrass é da forma de Legendre se ela pode ser escrita como*

$$y^2 = x(x-1)(x-\lambda)$$

$\lambda \in \bar{K}$

Se $char(K) \neq 2$, então podemos reescrever a equação de Weierstrass na forma de Legendre.

Proposição 6. *Toda curva curva elíptica suave é isomorfa a uma curva dada pela forma de Legendre*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

com $\lambda \in \bar{K}$ *e* $\lambda \neq 0, 1$.

Demonstração. Supondo que $char(K) \neq 2$ podemos escrever a curva elíptica por

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

Fazendo a mudança $(x, y) \longmapsto (x, 2y)$, obtemos

$$E : 4y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \Rightarrow y^2 = (x - e_1)(x - e_2)(x - e_3)$$

para alguns $e_1, e_2, e_3 \in \bar{K}$.

A mudança de coordenadas realizadas foi,

$$x = x \quad \text{e} \quad y = y - (a_1/2)x - a_3/2$$

assim, $u = 1$, logo $\Delta' = \Delta$. Pela hipótese de E ser não-singular, $\Delta \neq 0$, segue então que $\Delta' \neq 0 \Rightarrow e_1, e_2, e_3$ são distintos.

Fazendo a mudança,

$$x = (e_2 - e_1)x' + e_1 \quad \text{e} \quad y = (e_2 - e_1)^{3/2}y'$$

temos que,

$$E : (((e_2 - e_1)^{3/2}y')^2 = [(e_2 - e_1)x' + e_1 - e_1][(e_2 - e_1)x' + e_1 - e_2][(e_2 - e_1)x' + e_1 - e_3]$$

$$E : (e_2 - e_1)^3(y')^2 = x'(e_2 - e_1)[(e_2 - e_1)x' + (e_1 - e_2)][(e_2 - e_1)x' + (e_1 - e_3)]$$
$$= x'(e_2 - e_1)[(e_2 - e_1)^2x'^2 + (e_2 - e_1)x'(e_1 - e_3) + (e_1 - e_2)(e_2 - e_1)x' + (e_1 - e_2)(e_1 - e_3)]$$

dividindo por $(e_2 - e_1)^3$, temos

$$E : y'^2 = x'\left(x'^2 + \frac{x'(e_1 - e_3)}{(e_2 - e_1)} + \frac{x'(e_1 - e_2)}{(e_2 - e_1)} - \frac{(e_1 - e_3)}{(e_2 - e_1)}\right)$$
$$= x'\left(x'^2 + \frac{x'(e_1 - e_3)}{(e_2 - e_1)} - x' - \frac{(e_1 - e_3)}{(e_2 - e_1)}\right).$$

Nomeando $\lambda = \dfrac{e_3 - e_1}{e_2 - e_1}$ e substituindo na expressão (por um abuso de notação vamos escrever y e x ao invés de y' e x') obtemos

$$E : y^2 = x(x^2 - \lambda x - x + \lambda) = x(x - 1)(x - \lambda)$$

Como não podemos ter raízes duplas, $\lambda \neq 0, 1$ □

Proposição 7. *Seja E uma curva elíptica e $D = \sum_{P \in E} n_p(P) \in Div(E)$. Então, D é um divisor principal se, e somente se,*

$$\sum_{P \in P} n_p = 0 \qquad e \qquad \sum_{P \in E} [n_p]P = O.$$

Demonstração. (SILVERMAN, 2009) □

2.2 A Lei dos Grupos

Veremos nessa seção que é possível definir uma operação de grupo sobre os pontos de uma curva elíptica, daremos primeiro uma representação geométrica e em seguida, com o uso da equação de Weierstrass obteremos um algoritmo para o cálculo da operação de modo explícito.

2.2.1 Operação do Grupo

Seja E uma curva elíptica (a curva está no plano afim) dada pela equação de Weierstrass, com $O = [0 : 1 : 0]$ sendo o ponto no infinito, além disso, vamos supor que $\Delta \neq 0$, essa hipótese garante a unicidade retas tangentes. Se L é uma reta, o teorema de Bézout nos dá que L vai intersectar E em três pontos, ou caso L seja tangente a E em dois pontos. Contudo a soma dos graus das intersecções vai ser três.

Definição 23 (Ideia geométrica)**.** *Seja $P, Q \in E$. Seja também L a reta passando por P e Q (se $P = Q$, então L vai ser tangente a E). Denote por R o terceiro (ou segundo caso $P = Q$) ponto de interseção de E e L. Tome agora L' a reta passando por $O = [0 : 1 : 0]$ e R, assim L' vai interceptar E em mais um ponto, denotado por $P \oplus Q$.*

Vamos verificar que E munida da operação acima é um grupo abeliano.

Proposição 8. *A lei da **Definição 23** tem as seguintes propriedades:*

1. *Seja $P, Q, R \in E$, então $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*
2. *Temos que $P \oplus O = O \oplus P = P$, $\forall P \in E$.*
3. *Dado $P \in E$, existe um ponto em E denotado por $\ominus P$, tal que, $P \oplus (\ominus P) = O$*
4. *$P \oplus Q = Q \oplus P$ $\forall P, Q \in E$.*
5. *Se L é uma reta que intercepta E nos pontos P, Q, R (não necessariamente distintos), então $(P \oplus Q) \oplus R = O$.*
6. *Suponha que E está definida sobre K, então $E(K) = \{(x, y) \in K^2; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$ é um subgrupo de E.*

Demonstração do item 5 da Proposição 8. Primeiro vamos calcular $P \oplus Q$. Temos que L é a reta passando por P, Q e R. Considere L' passando por O e R, assim o terceiro ponto chamamos de $P \oplus Q$. Agora para o cálculo de $(P \oplus Q)$ e R, já temos a reta L' passando por eles e interceptando E em O, podemos olhar $R' = O$, agora queremos uma reta L'' passando por $R' = O$ e O, ou seja, L'' deve tangenciar E em O. Vimos no Exemplo 8 que o grau de interseção é três, por Bézout temos que $L'' \cap E = \{O\}$. Logo $(P \oplus Q) \oplus R = O$. □

A seguir enunciamos algumas ferramentas que serão importantes para demonstrar o item 1.

Definição 24. *Sejam F e G curvas projetivas sem componentes comuns, definimos o Divisor da interseção por*

$$F_\bullet G = \sum_{P \in \mathbb{P}^2} I(P, G, F) \cdot P$$

Suponha F, G e H curvas, e $H_\bullet F \geqslant G_\bullet F$, i.e, H tem um divisor de interseção maior do que G. Quando existe uma curvas B, tal que, $B_\bullet F = H_\bullet F - G_\bullet F$? Para uma B satisfazendo essa igualdade devemos ter $deg(B) = deg(H) - deg(G)$.

Condição de Max Noether : Sejam $P \in \mathbb{P}^2$, F, G curvas sem componentes em comum, passando por P. Seja H uma outra curva, dizemos que a condição de Max Noether é satisfeita em P (com respeito a F, G e H) se

$$h \in \langle f, g \rangle \subseteq \bar{K}[\mathbb{P}^2]_P$$

i.e, existem $a, b \in \bar{K}[\mathbb{P}^2]_P$, tal que, $h = af + bG$. h, f e g são as homegenezação de H, F e G, respectivamente.

Teorema 4 (Teorema fundamental de Max Noether)**.** *Seja F, G e H curvas planas projetivas. Assuma que F e G não tem componentes em comum. Então existe uma equação $H = AF + BG$ (com A, B polinômios de graus $deg(H) - deg(F)$ e $deg(H)deg(G)$, respectivamente) se, e somente se, a condição de Noether e satisfeita em todo ponto $P \in F \cap G$.*

Demonstração. Livro (FULTON, 1989) □

Proposição 9. *Sejam F, G e H curvas planas, e $P \in F \cap G$. Então a condição de Noether é satisfeita em P se vale alguns dos itens:*

1. *F e G se encontram transversalmente em P e $P \in H$;*
2. *P é um ponto simples em F e $I(P, H, F) \geqslant I(P, G, F)$;*
3. *F e G tem tangentes distintas em P e $m_P(H) \geqslant m_P(F) + m_P(G) - 1$.*

Demonstração. (FULTON, 1989) □

Corolário 1. *Se é válido algum dos itens acima, temos*

1. *F e G se encontram em $deg(F)deg(G)$ pontos distintos, e H passa por esses pontos. Ou*
2. *todos os pontos de $F \cap G$ são pontos simples de F e $H_\bullet F \geqslant G_\bullet F$, então existe uma curva B,tal que $B_\bullet F = H_\bullet F - G_\bullet F$.*

Vamos agora demonstrar o item 1.

Demonstração do item 1 da Proposição 8. Sejam $P, Q, R \in E$. Vamos calcular primeiro $(P \oplus Q) \oplus R$. Considere

1. L_1 a reta passando por P, Q e S' ,
2. M_1 a reta passando por O, S' e S, aqui $S = P \oplus Q$,
3. L_2 a reta passando por S, R e T',

então, $(P \oplus Q) \oplus R$ será o terceiro ponto de interseção da reta passando por O e T'.

Agora vamos encontrar $P \oplus (Q \oplus R)$, considere

1. M_2 a reta passando por Q, R e U',
2. L_3 a reta passando por O, U', U, aqui $U = Q \oplus R$,
3. M_3 a reta passando por P, U e T'',

então, $P \oplus (Q \oplus R)$ será o terceiro ponto de interseção da reta passando por O e T''. Assim, basta verificar que $T' = T''$.

Defina $C_1 = L_1 L_2 L_3$ e $C_2 = M_1 M_2 M_3$, é fácil ver que

$$E \bullet C_1 = P + Q + R + S + S' + U + U' + T'$$

$$E \bullet C_2 = P + Q + R + S + S' + U + U' + T''$$

Defina agora, L a reta passando por T' mas não por T''. Temos $L \bullet E = T' + P_1 + P_2$. Assim, $LC_2 \bullet E = C_1 \bullet E + T'' + P_1 + P_2$. Tomando $F = E, G = C_1$ e $H = LC_2$, pelo item 2 do corolário, temos que existe B, tal que $B = T'' + P_1 + P_2$ e $deg(B) = deg(H) - deg(G) = 4 - 3 = 1$. Ou seja, existe uma reta passando por P_1, P_2 e T'', i.e, $L = B$ e portanto $T' = T''$. □

Demonstração do item 2 da Proposição 8. Tomando $Q = O$ na definição, então seja L a reta passando por P e O, temos que ela deve interceptar E em R. Portanto, L' deve passar por R e O, logo vai coincidir com L e assim $P \oplus O = P$. Análogo para $O \oplus P$. □

Demonstração do item 3 da Proposição 8. Usando os itens 2 e 5, temos que

$$O = (P \oplus O) \oplus R = P \oplus R.$$

Basta definir $R = \ominus P$. □

Demonstração do item 4 da Proposição 8. Note que, a reta passando por P e Q é a mesma passando por Q e P (a construção é simétrica). Portanto obteremos os mesmo resultados em ambos os casos. □

Exemplo 13. *Suponha E definida sobre K e $P, Q \in E$ pontos racionais. Se $L : aX + bY + cZ$ é a reta ligando os dois ponto, então a, b, c devem pertencer a K, pois se $P = (p_1, p_2, p_3)$ e $Q = (q_1, q_2, q_3)$, temos*

$$\begin{cases} ap_1 + bp_2 + cp_3 = 0, \\ aq_1 + bq_2 + cq_3 = 0, \end{cases}$$

então, $c = \dfrac{-ap_1 - bp_2}{p_3}$. Substituindo na segunda equação do sistema, obtemos

$$aq_1 + bq_2 + \frac{(-ap_1 - bp_2)q_3}{p_3} = 0 \Rightarrow a(q_1p_3 - p_{q_3}) + b(q_2p_3 - p_2q_3) = 0$$

$$\Rightarrow \frac{a}{b} = \frac{-(q_2p_3 - p_2q_3)}{(q_1p_3 - p_{q_3})} \in K$$

assim, $a, b \in K$, e logo $c \in K$. Portanto, L está definida sobre K.

Agora, se L intercepta E em um terceiro ponto, então esse deve ser racional. Para ver isto, podemos supor que $[0 : 1 : 0]$ não é o ponto de interseção, logo podemos olhar para os pontos da forma $[X : Y : 1]$, (vamos fazer $Z = 1$ na equação da reta e da curva elíptica), assim

$$E : y^2 + a_1xy - a_2x^2 + a_3y - a_4x - x^3 - a_6 = 0 \quad \text{e} \quad L : y = ax + b$$

Substituindo na equação da curva elíptica vamos obter algo do tipo

$$(x - x_1)(x - x_2)(x - x_3) = 0 \tag{2.4}$$

Sem perda de generalidade, podemos supor que x_1 e x_2 são coordenadas de P e Q. Vamos olhar na equação de E (após feita a substituição de y) e na equação (2.4) o coeficiente do termo x^2. Com simples cálculos, obtemos que são:

$$a^2 + aa_1 - a_2 \quad \text{e} \quad x_1 + x_2 + x_3$$

como

$$a^2 + aa_1 - a_2 = x_1 + x_2 + x_3 \Rightarrow x_3 = a^2 + aa_1 - a_2 - x_1 - x_2 \in K$$

Portanto, todas as coordenadas do terceiro ponto estão em K.

Demonstração do item 6 da Proposição 8. Como consequência deste exemplo, podemos tomar dois pontos em $K(E)$ e realizar a operação no espaço projetivo, obtendo um ponto que quando afinizado estará em $K(E)$. □

2.2.2 Formula explícita

Vamos através da equação de Weierstrass obter um algoritmo para somar dois pontos da curva.

Seja E uma curva elíptica dada pela equação de Weierstrass

$$E : f(x,y) = y^2 + a_1xy - a_2x^2 + a_3y - a_4x - x^3 - a_6 = 0$$

então

1. Seja $P = (x_0, y_0) \in E$. Então $\ominus P = (x_0, -y_0 - a_1x_0 - a_3)$, pois

   $\ominus P$ é o ponto, tal que, se L é a reta passando por P e $\ominus P$, então L' é tangente à E em O, isso só ocorre se L intercepta o ponto O. Assim, considere L a reta passando por P e O, temos que $L : x - x_0 = 0$. Substituindo em E, obtemos

   $$f(x_0, y) = (y - y_0)(y - y_1).$$

   Uma das raízes deve ser coordenada de P, assim como feito no último exemplo, vamos olhar para o coeficiente de y, na equação de E quando fizermos a mudança de variável e em $(y - y_0)(y - y_1)$, como ambos devem ser iguais obtemos

   $$a_1x_0 + a_3 = -y_0 - y_1 \Rightarrow y_1 = -y_0 - a_1x_0 - a_3.$$

2. Sejam $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$. Seja também $L : y = \lambda x + b$ a reta passando por P_1 e P_2. Vamos definir os valores dos coeficientes da reta para os casos $P_1 = P_2$ e $P_1 \neq P_2$, e por fim, encontrar o resultado da soma.

   Se $x_1 = x_2$ e $y_2 = -y_1 - a_1x_1 - a_3$, então $P_1 \oplus P_2 = O$ (caso $P_1 = \ominus P_2$.

   Se $P_1 = P_2$, a equação da reta tangente é dada por

   $$L : \frac{\partial f}{\partial x}(P)(x - x_1) + \frac{\partial f}{\partial y}(P)(y - y_1) = 0$$
   $$\Rightarrow L : (-3x_1^2 + a_1y_1 - 2a_2x_1 - a_4)(x - x_1) + (2y_1 + a_1x_1 + a_3)(y - y_1) = 0$$
   $$\Rightarrow L : y = \frac{3x_1^2 + 2a_2x_1 + a_4 + a_1y_1}{2y_1 + a_1x_1a_3}x + \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1a_3}.$$

   Se $P_1 \neq \pm P_2$, então $L : y = \lambda x + b$ deve satisfazer

   $$\begin{cases} y_1 = \lambda x_1 + b, \\ y_2 = \lambda x_2 + b, \end{cases}$$

   resolvendo o sistema obtemos $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ e $b = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1}$.

   Agora que já temos os valores dos coeficientes, para calcular $P_1 \oplus P_2$, vamos encontrar o terceiro ponto de interseção usando a mesma lógica do exemplo 14,

pois o item 5 da proposição 10 nos dá que $(P_1 \oplus P_2) \oplus P_3 = O$, então $P_1 \oplus P_2 = \ominus P_3$. Logo, se $P_3 = (x_3, y_3)$ é o terceiro ponto, então $x_3 = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2$ e $y_3 = x_3\lambda + b$. Basta usar o item 1 para encontrar o $\ominus P$, ou seja

$$\ominus P_3 = (\lambda^2 + \lambda a_1 - a_2 - x_1 - x_2, -(\lambda + a_1)x^3 - b - a_3).$$

Exemplo 14. *Vamos supor que* $char(\bar{K}) \neq 2, 3$*, logo uma curva elíptica E é dada na forma reduzida por* $E : y^2 - x^3 - Ax - B$*. Considerando O como o ponto no infinito, vamos verificar a lei do grupo. Considere* $P_1 = (x_1, x_2)$ *e* $P_2 = (x_2, y_2)$

Se $P_1 = P_2$ *a equação da reta tangente a E em* P_1 *é*

$$L : (-3x_1^2 - A)(x - x_1) + (2y_1)(y - y_1) = 0$$

$$\Rightarrow L : y = \frac{x(3x_1^2 + A)}{2y_1} + \frac{-3x_1^3 - Ax_1 + 2y_1^2}{2y_1},$$

podemos simplificar para

$$L : y = x\lambda - x_1\lambda + y_1.$$

Se $P_1 \neq \pm P_2$*, podemos supor* $L : y = \lambda x + b$ *a equação da reta passando por ambos, para esse caso já temos o valor de* λ *e b. Vamos reescrever b de modo a facilitar os cálculos, ou seja,*

$$b = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} = \frac{y_1x_2 - y_2x_1 + (y_1x_1) - (y_1x_1)}{x_2 - x_1} = -x_1\frac{y_2 - y_1}{x_2 - x_1} + y_1$$

Logo $L : y = \lambda(x - x_1) + y_1$.

Supondo que $P_3 = (x_3, y_3)$ *é o ponto onde a reta passando por* P_1 *e* P_2 *intercepta E, então temos que*

$$(\lambda(x - x_1))^2 = x^3 + Ax + B \qquad e \qquad (x - x_1)(x - x_2)(x - x_3) = 0$$

Olhando para o coeficiente do termo x^2 *na primeira e segunda equação, vamos obter que*

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

e substituindo na equação da reta temos que $y_3 = \lambda(x_3 - x_1) + y_1$*. Ou seja,* $P_3 = (\lambda^2 - x_1 - x_2, \lambda(x_3 - x_1) + y_1)$*, pelo item 5 da proposição 10, temos que*

$$P_1 \oplus P_2 = \ominus P_3 \Rightarrow P_1 \oplus P_2 = ((\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1)$$

Para o caso $P_1 = P_2$*, vemos de maneira análoga que*

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{e} \quad y_3 = x_3\lambda - x_1\lambda + y_1.$$

Logo,

$$P_1 \oplus P_1 = (\lambda^2 - x_1 - x_2, -x_3\lambda + x_1\lambda - y_1).$$

Vamos fazer uma observação que será utilizado no capitulo 4, note que, para o caso $P_1 \neq \pm P_2$, *para realizar a soma dos dois ponto devemo fazer duas multiplicações* (λ^2 *e* $\lambda(x_1 - x_3)$) *e uma divisão* $\left(\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}\right)$. *Já no caso* $P_1 = P_2$, *é necessário uma divisão (a do próprio lambda) e 4 multiplicações* λ^2 , $-x_3\lambda$, $x_1\lambda$ *e* $\lambda = \dfrac{(3x_1^2 + A)}{2y_1}$

2.2.3 Isogenia

Definição 25. *Sejam* E_1 *e* E_2 *curvas elípticas. Uma* ***isogenia*** *de* E_1 *para* E_2 *é um morfismo* ϕ *satisfazendo* $\phi(O) = O$

Duas curvas elípticas são ***isogênicas*** *se existir uma isogênia, tal que,* $\phi(E_1) \neq \{O\}$.

Exemplo 15. *Seja* E *uma curva elíptica e* $m > 0$ *um numero inteiro. Definimos a isogenia multiplicação por* m

$$[m] : E \longrightarrow E \quad \text{tal que} \quad [m](P) = P \oplus P \oplus \cdots \oplus P.$$

De maneira similar, definimos para o caso $m < 0$.

Definição 26. *Sejam* E *uma curva elíptica e* $m > 1$ *um inteiro. O* ***subgrupo*** $m-$***torção*** *de* E, *denotado por* $E[m]$ *é definido como*

$$E[m] = \{P \in E; [m](P) = O\}.$$

Proposição 10. *Sejam* E *uma curva elíptica e* $m \in \mathbb{Z}$ *com* $m \neq 0$. *Se* $char(K) = 0$ *ou* $p = char(K)$ *e* p *não divide* m, *então*

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

Demonstração. (SILVERMAN, 2009) □

3 Emparelhamentos

Neste capítulo estudaremos os emparelhamento de Weil e Tate, para ambos os caso vamos está sempre considerando uma curva elíptica plana.

3.1 Emparelhamento de Weil

Nessa seção vamos definir o emparelhamento de Weil, ferramenta utilizada em varias áreas, o qual foi primeiramente proposto por Weil numa primeira demonstração da Hipótese de Riemann em corpos finitos. Atualmente é utilizada na criptografia, contudo a implementação de modelos que fazem uso do emparelhamento são caros computacionalmente, assim uma boa parte dos estudos buscam uma maneira de otimizar o calculo do emparelhamento.

Para esta seção vamos fixar um inteiro $m \geqslant 2$, o qual é vamos assumir ser primo com $p = char(K)$ (no caso de $p > 0$). Vamos denotar também $E[m]$ o grupo dos pontos de $m-$torção.

Seja $T \in E[m]$, então pela proposição 7 existe uma função $f \in \bar{K}(E)$ satisfazendo $\text{div}(f) = m(T) - m(O)$. Agora, tome $T' \in E$, tal que, $[m]T' = T$. Analogamente, existe uma função $g \in \bar{K}(E)$ satisfazendo

$$\text{div}(g) = \sum_{R \in E[m]} (T' \oplus R) - (R).$$

Note que,

$$\sum_{R \in E[m]} (T' \oplus R) - (R) = m^2 T' + \sum_{R \in E[m]} (R) - (R) = O.$$

Na penúltima igualdade usamos o fato de que $\#E[m] = m^2$ e que $m^2 T' = O$. Vamos verificar os divisores das funções $f \circ [m]$ e g^m.

Primeiro, note que se P é zero de ordem 1 de uma função g, então para g^2, P será um zero de ordem 2, logo o $\text{div}(g^m) = m \sum_{R \in E[m]} (T' \oplus R) - (R)$. Agora para $f \circ [m]$, os zeros serão os pontos da forma $(T' + R)$ com $R \in E[m]$ e $T = mT'$, cada $(T' \oplus R)$ é um zero de ordem m (construção análoga para os polos), logo $\text{div}(f \circ [m]) = m \sum_{R \in E[m]} (T' \oplus R) - (R)$.

Como os divisores são iguais, então elas se diferenciam por um escalar do corpo, ou seja, multiplicando f por um escalar conveniente, podemos assumir que $f \circ [m] = g^m$. Agora, seja $S \in E[m]$, outro ponto de m-torção (podemos ter $S = T$), então

para qualquer ponto $X \in E$, temos

$$g(S \oplus X)^m = f([m]S + [m]X) = f([m]X) = g(X)^m. \tag{3.1}$$

Olhando para

$$\frac{g(X \oplus S)}{g(X)}$$

como sendo uma função de X, verifica-se que ela apenas assume valores finitos, sendo uma raiz m-ésima da unidade. Em particular, o morfismo

$$E \longrightarrow \mathbb{P}^1 \qquad S \longmapsto \left[\frac{g(X \oplus S)}{g(X)} : 1\right]$$

não é sobrejetivo, pela Teorema 3 temos que é constante. Assim, vamos definir o emparelhamento de Weil por

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

onde, $e_m(S,T) = \dfrac{g(X \oplus S)}{g(X)}$

em que $X \in E$ é qualquer ponto que não anule ambas funções. μ_m é denotado como sendo o grupo das m-ésima raízes da unidade. Notemos que nossa função g está bem definida a menos de uma multiplicação por escalar, mas e_m não depende da escolha de g, pois no passo 3.1 o escalar não vai interferir.

Proposição 11. *O emparelhamento de Weil e_m tem as seguintes propriedades:*

1. *É bilinear, ou seja*

$$e_m(S_1 \oplus S_2, T) = e_m(S_1, T)e_m(S_2, T),$$
$$e_m(S, T_1 \oplus T_2) = e_m(S, T_1)e_m(S, T_2).$$

2. *É alternado, isto é, $e_m(T,T) = 1$. Em particular $e_m(S,T) = e_m(T,S)^{-1}$.*

3. *É não degenerada, ou seja, se $e_m(S,T) = 1 \forall S \in E[m]$, então $T = O$.*

4. *É compatível, isto é, $e_{mm'}(S,T) = e_m([m']S, T)$ $\forall S \in E[mm']$ com $T \in E[m]$.*

Demonstração. **Item 1**

Vamos verificar a linearidade de cada termo separadamente, para o primeiro fator termos que,

$$e_m(S_1 \oplus S_2, T) = \frac{g(X \oplus (S_1 \oplus S_2))}{g(X)} = \frac{g(X \oplus (S_1 \oplus S_2))}{g(X)} \frac{g(X \oplus S_1)}{g(X \oplus S_1)}.$$

Como
$$\frac{g(X \oplus S_1)}{g(X))} = e_m(S_1, T) \qquad e \qquad \frac{g((X \oplus S_1) \oplus S_2)}{g(X \oplus S_1)} = e_m(S_2, T),$$
segue que $e_m(S_1 \oplus S_2, T) = e_m(S_1, T)e_m(S_2, T)$.

Agora para o segundo fator, dado os pontos $T_1, T_2, T_3 = T \oplus T_2 \in E[m]$, considere as funções $f_1, f_2, f_3 \in \bar{K}(E)$, tais que

$$\operatorname{div}(f_i) = m(T_i) - m(O), \qquad i = 1, 2, 3.$$

A partir das f's vamos tomar $g_1, g_2, g_3 \in \bar{K}(E)$ onde

$$g_i^m = f_i \circ [m], \qquad i = 1, 2, 3.$$

Observe que até aqui estamos tomando funções da mesma forma que fizemos na construção emparelhamento, ou seja, para cada T_i temos o valor de $e_m(S, T_i)$. Para finalizar, tomemos uma última função $h \in \bar{K}(E)$, tal que,

$$\operatorname{div}(h) = (T_1 \oplus T_2) - (T_1) - (T_2) + (O).$$

Perceba que,
$$\operatorname{div}\left(\frac{f_3}{f_1 f_2}\right) = m \operatorname{div}(h).$$
Assim concluímos que $f_3 = c f_1 f_2 h^m$ para algum $c \in \bar{K}^*$. Fazendo composição com $[m]$ em ambos os lados, temos que

$$f_3 = c f_1 f_2 h^m \Rightarrow g_3^m = c g_1^m g_2^m (h \circ [m])^m.$$

tomando a m-ésima raiz, obtemos $g_3 = g_1 g_2 (h \circ [m])$. Vamos agora ao cálculo:

$$e_m(S, T_1 \oplus T_2) = \frac{g_3(X + S)}{g_3(X)} = \frac{c g_1(X + S) g_2(X + S) h([m]X + [m]S)}{c g_1(X) g_2(X) h([m]X)} = e_m(S, T_1) e_m(S, T_2).$$

Item 2

Exemplo 16. *Seja E uma curva elíptica definida em K, e $Q \in E$, então definimos o mapa translação por Q*

$$\tau_Q : E \longrightarrow E \qquad \tau_Q(P) = P \oplus Q$$

É fácil verificar que $\tau_{\ominus Q}$ é a inversa, logo temos um isomorfismo.

Vamos mostrar que $e_m(T, T) = 1 \forall T \in E[m]$. Consideramos as funções $f, g \in \bar{K}(E)$ como anteriormente, também considere os mapas de translações $\tau_{[i]T}$ para $i = 0, 1, ..., m - 1$. Considere o divisor da seguinte função $f \circ \tau_{[i]T}$, dada por

$$\operatorname{div}(f \circ \tau_{[i]T}) = m([1 - i]T) - m(-[i]T),$$

segue que,

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m \sum_{i=0}^{m-1} [([1-i]T) - (-[i]T)].$$

Olhando como soma de pontos, temos $m \sum_{i=0}^{m-1} [([1-i]T) - (-[i]T)] = O$, ou seja, $\prod_{i=0}^{m-1} f \circ \tau_{[i]T}$ é constante. De modo análogo, verificamos que

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$$

também é constante. Segue que

$$\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}(X) = \prod_{i=0}^{m-1} g \circ \tau_{[i]T'}(X \oplus T') \Rightarrow \prod_{i=0}^{m-1} g(X \oplus [i]T') = \prod_{i=0}^{m-1} g(X \oplus [1+i]T',$$

cancelando os fatores, obtemos

$$g(X) = g(X \oplus [m]T') = g(X \oplus T).$$

Pela definição temos que

$$e_m(T,T) = \frac{g(X \oplus T)}{g(X)} = 1.$$

Agora, pelo item (a) temos que

$$e_m(T \oplus S, T \oplus S) = e_m(T,T)e_m(T,S)e_m(S,T)e_m(S,S) \Rightarrow e_m(T,S)e_m(S,T) = 1.$$

Item 3

Se $e_m(S,T) = 1 \ \forall S \in E[m]$, temos que

$$\frac{g(X \oplus S)}{g(X)} = 1 \Leftrightarrow g(x) = g(X \oplus S) \forall S \in E[m].$$

Assim, $g = h \circ [m]$ para alguma função $h \in \bar{K}(E)$. Por construção temos que

$$(h \circ [m])^m = g^m = f \circ [m].$$

Logo, $f = h^m$, mas assim

$$m \operatorname{div}(h) = \operatorname{div}(f) = m(T) - m(O) \Rightarrow \operatorname{div}(h) = (T) - (O).$$

Lema 2. *Seja C uma curva de gênero um, e $P, Q \in C$, então $(P) \sim (Q) \Leftrightarrow P = Q$.*

Pelo lema, temos $T = O$.

Item 4

Dado $T \in E[m]$, vamos tomar $f, g \in \bar{K}(E)$, da maneira usual, i.e,

$$\text{div}(f) = m(T) - m(O) \quad \text{e} \quad g^m = f \circ [m].$$

Vamos através dele construir funções para o cálculo de $e_{mm'}$. Temos que

$$\text{div}(f^{m'}) = m.m'(T) - mm'(O),$$

e também

$$\begin{aligned} g^m = f \circ [m] \Rightarrow g^m \circ [m'] = f \circ [mm'] &\Rightarrow (g^m \circ [m'])^{m'} = f^{m'} \circ [mm'] \\ &\Rightarrow (g^{\circ}[m'])^{mm'} = f^{m'} \circ [mm']. \end{aligned}$$

Logo

$$e_{mm'}(S,T) = \frac{(g \circ [m'])(X \oplus S)}{(g \circ [m'])(X)} = \frac{g([m']X \oplus [m']S)}{g([m']X} = \frac{g(Y \oplus [m']S)}{g(Y)} = e_m([m']S, T).$$

□

A maneira como foi definida o emparelhamento de Weil é útil quando se trabalha de maneira algébrica, contudo para a implementação em algoritmos devemos encontrar uma outra forma de expressar o emparelhamento. Nesse intuito, considere a definição a seguir.

Definição 27. *Seja E uma curva elíptica, definimos os emparelhamentos*

$$\tilde{e}_m : E[m] \times E[m] \longrightarrow \mu_m$$

do seguinte modo: Para $P, Q \in E[m]$, escolha divisores $D_P, D_Q \in Div^0(E)$, tais que, $D_P \sim (P) - (O)$ e $D_Q \sim (Q) - (O)$. Assumindo que D_P e D_Q tem suportes disjuntos, e como a ordem de P e Q é m, então existem funções f_P e f_Q de modo que

$$\text{div}(f_P) = mD_P \quad \text{e} \quad \text{div}(f_Q) = mD_Q,$$

assim,

$$\tilde{e}_m(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)}.$$

Vamos verificar que mapa acima está bem definido. Primeiramente, como os suportes dos divisores são disjuntos então não teremos problemas em aplicar as funções. Agora, tomando divisores diferentes, mas que ainda são equivalentes à $(P) - (O)$ e $(Q) - (O)$ não interferiram no resultado, pois suponha

$$\tilde{D}_P \sim (P) - (O) \quad \text{e} \quad \tilde{D}_Q \sim (Q) - (O).$$

Tomemos as funções $\tilde{f}_P, \tilde{f}_Q \in \bar{K}(E)$ tais que

$$\operatorname{div}(\tilde{f}_P) = m\tilde{D}_P \quad \text{e} \quad \operatorname{div}(\tilde{f}_Q) = m\tilde{D}_Q.$$

Podemos reescrever os divisores como

$$\tilde{D}_P = D_P + \operatorname{div}(h_P) \quad \text{e} \quad \tilde{D}_Q = D_Q + \operatorname{div}(h_Q),$$

onde $h_P, h_Q \in K(E)$ são funções. Antes de mostrarmos a igualdade, note que,

$$\operatorname{div}(\tilde{f}_P) = m\tilde{D}_P = mD_P + m\operatorname{div}(h_P),$$

ou seja, a menos de uma multiplicação por escalar, podemos supor $\tilde{f}_P = f_P h^m$. Análogo para $\tilde{f}_Q$, temos

$$\frac{\tilde{f}_P(\tilde{D}_Q)}{\tilde{f}_Q(\tilde{D}_P)} = \frac{f_P(\tilde{D}_Q)h_P(m\tilde{D}_Q)}{\tilde{f}_Q(D_P + \operatorname{div}(h_P))} = \frac{f_P(\tilde{D}_Q)h_P(m\tilde{D}_Q)}{\tilde{f}_Q(D_P)\tilde{f}_Q\operatorname{div}(h_P))} = \frac{f_P(\tilde{D}_Q)h_P(m\tilde{D}_Q)}{\tilde{f}_Q(D_P)h_P(\operatorname{div}(\tilde{f}_Q))}.$$

Na última igualdade utilizamos a Reciprocidade de Weil, segue que

$$\frac{f_P(\tilde{D}_Q)h_P(m\tilde{D}_Q)}{\tilde{f}_Q(D_P)h_P(\operatorname{div}(\tilde{f}_Q))} = \frac{f_P(\tilde{D}_Q)h_P(m\tilde{D}_Q)}{\tilde{f}_Q(D_P)h_P(m\tilde{D}_Q))} = \frac{f_P(\tilde{D}_Q)}{\tilde{f}_Q(D_P)}.$$

Repetindo o mesmo processo, obtemos

$$\frac{f_P(D_Q)}{f_Q(D_P)}$$

Aplicando a Reciprocidade de Weil, garantimos ainda que $\dfrac{f_P(D_Q)}{f_Q(D_P)}$ é uma m-ésima raiz da unidade e

$$f_P(\operatorname{div}(f_Q) = f_Q(\operatorname{div}(f_P) \Leftrightarrow f_P(mD_Q) = f_Q(mD_P) \Leftrightarrow \left(\frac{f_P(D_Q)}{f_Q(D_P)}\right)^m = 1.$$

Teorema 5. *Os emparelhamentos e_m e $\tilde{e}_m$ são equivalentes, ou seja,$\tilde{e}_m(P,Q) = e_m(P,Q)$ para todo $(P,Q) \in E[m] \times E[m]$.*

Demonstração. Primeiramente escolha pontos $P', Q', R \in E$, de modo que

$$[m]P' = P, \qquad [m]Q' = Q, \qquad [2]R = P' - Q \quad \text{e} \quad P' \neq \pm Q'.$$

Agora, defina os divisores D_P, D_Q, tais que $D_P = (P) - (O)$ e $D_Q = (Q \oplus [m]R) - ([m]R)$, tome também funções $f_P, f_Q, g_P, g_Q \in \bar{K}(E)$ satisfazendo

$$\operatorname{div}(f_P) = mD_P, \qquad \operatorname{div}(f_Q) = mD_Q,$$

$$f_P \circ [m] = g_P^m \quad \text{e} \quad f_Q \circ [m] = g_Q^m.$$

Como feito anteriormente, verifica se que

$$\operatorname{div}(g_P) = \sum_{T\in E[m]} [(T \oplus P') - (T)] \quad \text{e} \quad \operatorname{div}(g_Q) = \sum T \in E[m][(T \oplus Q' \oplus R) - (T \oplus R)]$$

Considere,

$$i) \quad \frac{g_P(X \oplus Q' \oplus R)g_Q(X)}{g_P(X \oplus R)g_Q(X \oplus P')} \in \bar{K}(E)$$

como uma função na variável X. Verificamos facilmente que

$$\begin{aligned}
\operatorname{div}(g_P(X \oplus Q' \oplus R)) &= \sum_{T\in E[m]} [(T \oplus R) - (T \ominus Q' \ominus R)],\\
\operatorname{div}(g_Q(X)) &= \sum_{T\in E[m]} [(T \oplus Q' \oplus R) - (T \oplus R)],\\
\operatorname{div}(g_P(X \oplus R)) &= \sum_{T\in E[m]} [(T \oplus P' \ominus R) - (T \ominus R)],\\
\operatorname{div}(g_Q(X \oplus P')) &= \sum_{T\in E[m]} [(T \ominus R) - (T \oplus R \ominus P')].
\end{aligned}$$

Segue que,

$$\begin{aligned}
&\operatorname{div}\left(\frac{g_P(X \oplus Q' \oplus R)g_Q(X)}{g_P(X \oplus R)g_Q(X \oplus P')}\right)\\
&\quad = \operatorname{div}(g_P(X \oplus Q' \oplus R)) + \operatorname{div}(g_Q(X)) - \operatorname{div}(g_P(X \oplus R)) - \operatorname{div}(g_Q(X \oplus P'))\\
&\qquad = \sum_{T\in E[m]} [(T \oplus Q' \oplus R) - (T \ominus Q' \ominus R) + (T \oplus R \ominus P') - (T \oplus P' \ominus R)],
\end{aligned}$$

note que,

$$\begin{aligned}
(T \oplus Q' \oplus R) &= (T \oplus P' \ominus P' \oplus Q' \oplus R) = (T \oplus P' \ominus [2]R \oplus R) = (T \oplus P' \ominus R),\\
(T \ominus Q' \ominus R) &= (T \oplus P' \ominus P' \ominus Q' \ominus R) = (T \ominus P' \oplus [2]R \ominus R) = (T \ominus P' \oplus R).
\end{aligned}$$

Logo,

$$\operatorname{div}\left(\frac{g_P(X \oplus Q' \oplus R)g_Q(X)}{g_P(X \oplus R)g_Q(X \oplus P')}\right) = 0.$$

Pelo Corolário 1, temos que a função é constante. Com um raciocínio parecido, verifica se para

$$ii) \quad \prod_{i=0}^{m-1} g_Q(X \oplus [i]Q') \in \bar{K}(E)$$

que

$$\operatorname{div}\left(\prod_{i=0}^{m-1} g_Q(X \oplus [i]Q')\right) = 0,$$

ou seja, também é constante. Com essas informações vamos ao cálculo de $\tilde{e}_m(P, Q)$, temos que

$$\tilde{e}_m(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)} = \frac{f_P(Q \oplus [m]R) f_P([m]R)^{-1}}{f_Q(P) f_Q(O)^{-1}} = \frac{f_P([m]Q' \oplus [m]R) f_Q([m]O)}{f_P([m]R) f_Q([m]P')}.$$

Utilizamos a definição de $\tilde{e}_m$ e o modo de como foi tomado os pontos P' e Q', nas igualdes anteriores. Agora, usando o fato de que $g_P^m = f_P \circ [m]$ e $g_Q^m = f_Q \circ [m]$, segue que

$$\frac{f_P([m]Q' \oplus [m]R) f_Q([m]O)}{f_P([m]R) f_Q([m]P')} = \left(\frac{g_P(Q' \oplus R) g_Q(O)}{g_P(R) g_Q(P')} \right)^m.$$

Como a função $i)$ é constante, então para $X = [i]Q'$ com $i = 0, 1, ..., m-1$, temos

$$\left(\frac{g_P(Q' \oplus R) g_Q(O)}{g_P(R) g_Q(P')} \right) \left(\frac{g_P([2]Q' \oplus R) g_Q(Q')}{g_P(R \oplus Q') g_Q(P' \oplus Q')} \right) \cdots$$
$$\cdots \left(\frac{g_P([m]Q' \oplus R) g_Q([m-1]Q')}{g_P(R \oplus [m-1]Q') g_Q(P' \oplus [m-1]Q')} \right)$$
$$= \left(\frac{g_P(Q' \oplus R) g_Q(O)}{g_P(R) g_Q(P')} \right)^m.$$

Assim,

$$\prod_{i=0}^{m-1} \frac{g_P([i+1]Q' \oplus R) g_Q([i]Q')}{g_P(R \oplus [i]Q') g_Q(P' \oplus [i]Q')} = \frac{g_P(R \oplus [m]Q')}{g_P(R)} \prod_{i=0}^{m-1} \frac{g_Q([i]Q')}{g_Q(P' \oplus [i]Q')}.$$

A última igualdade sai do fato de que o produto é telescópico para g_P. Agora, como $ii)$ é constante, para $X = P'$ e $X = O$ temos

$$\prod_{i=0}^{m-1} g_Q(P' \oplus [i]Q') = \prod_{i=0}^{m-1} g_Q(O \oplus [i]Q'),$$

então,

$$\prod_{i=0}^{m-1} \frac{g_Q(O \oplus [i]Q')}{g_Q(P' \oplus [i]Q')} = 1,$$

logo,

$$\frac{g_P(R \oplus [m]Q')}{g_P(R)} \prod_{i=0}^{m-1} \frac{g_Q([i]Q'}{g_Q(P' \oplus [i]Q')} = \frac{g_P(R \oplus [m]Q')}{g_P(R)} = \frac{g_P(R \oplus Q)}{g_P(R)} = e_m(P,Q).$$

□

Vamos agora exibir um "melhoramento"do emparelhamento de Weil, o qual vamos chamar de **Emparelhamento de Weil Quadrado**.

Lema 3. *Seja $f : E \longrightarrow K$ uma função racional em E com um zero de ordem m (ou um polo de ordem $-m$) em O. Defina $g : E \longrightarrow K$ por $g(X) = f(X)/f(\ominus X)$. Então $g(O)$ é finito e $g(O) = (-1)^m$.*

Demonstração. A função racional $h = x/y$ tem zero de ordem 1 em O, pois x tem polo de ordem 2 em O e y tem polo de ordem 3 em O. Agora, definindo $f_1 = f/h^m$, é fácil ver que f_1 não tem nem zero nem polo em O, logo $f_1(O)$ é um valor finito não nulo. Seja $\phi(X) = h(X)/h(\ominus X)$, então

$$\phi(P) = h(P)/h(\ominus P) = \frac{x(P)}{y(P)}\frac{y(\ominus P)}{x(\ominus P)} = -1.$$

Portanto,

$$g(P) = \frac{f(P)}{f(\ominus P)}\frac{f_1 h^m(P)}{f_1 h^m(\ominus P)}\frac{\phi^m(P) f_1(P)}{f_1(\ominus P)} = (-1)^m \frac{f_1(P)}{f_1(\ominus P)}.$$

Fazendo $P = O$, obtemos $g(O) = (-1)^m$. □

Considerando $f_{m,P}$ a função com divisor dado por $\mathrm{div}(f_{m,P}) = m(P) - m(O)$ e $f_{m,Q}$, tal que $\mathrm{div}(f_{m,Q}) = m(Q) - m(O)$, temos o seguinte resultado.

Teorema 6. *Seja m um inteiro positivo. Suponha P e Q pontos de m-torção em E, sem ser a identidade (O) e $P \neq \pm Q$. Então o emparelhamento de Weil Quadrado satisfaz*

$$(-1)^m e_m(P,Q)^2 = \frac{f_{m,P}(Q) f_{m,Q}(\ominus P)}{f_{m,P}(\ominus Q) f_{m,Q}(P)}.$$

Demonstração. Sejam $R_1, R_2 \in E$, tais que, os divisores definidos por $D_P = (P \oplus R_1) - (R_1)$ e $D_Q = (Q \oplus R_2) - (R_2)$ tenham suportes disjuntos. Defina também $D_{\ominus Q} = (\ominus Q \oplus R_2) - (R_2)$. Considere f_P e $f_Q \in \bar{K}(E)$ com $\mathrm{div}(f_P) = mD_P$ e $\mathrm{div}(f_Q) = mD_Q$.

$$e_m(P,Q) = \frac{f_P(D_Q)}{f_Q(D_P)} = \frac{f_P((Q \oplus R_2) - (R_2))}{f_Q((P \oplus R_1) - (R_1))} = \frac{f_P(Q \oplus R_2) f_Q(R_1)}{f_P(R_2) f_Q(P \oplus R_1)}. \tag{3.2}$$

Agora, considere $f_{m,P}$ a função com divisor dado por $\mathrm{div}(f_{m,P}) = m(P) - m(O)$. Assim, defina

$$g(X) = f_{m,P}(X \ominus R_1) \Longrightarrow \mathrm{div}(g) = m(P \oplus R_1) - m(R_1).$$

Como $\mathrm{div}(g) = \mathrm{div}(f_P)$ segue que elas se diferem por um escalar, ou seja, $\dfrac{g(X)}{f_P(X)}$ é constante e

$$\frac{g(X)}{f_P(X)} = \frac{g(X \oplus Q)}{f_P(X \oplus Q)}.$$

Para $X = R_2$,

$$\frac{g(R_2)}{f_P(R_2)} = \frac{g(R_2 \oplus Q)}{f_P(R_2 \oplus Q)} \Rightarrow \frac{f_P(Q \oplus R_2)}{f_P(R_2)} = \frac{g(Q \oplus R_2)}{g(R_2)} = \frac{f_{m,P}(Q \oplus R_2 \ominus R_1)}{f_{m,P}(R_2 \ominus R_1)}.$$

Tomando $f_{m,Q}$, tal que, $\mathrm{div}(f_{m,Q}) = m(Q) - m(O)$, chegamos de modo análogo que

$$\frac{f_Q(R_1)}{f_Q(P \oplus R_1)} = \frac{f_{m,Q}(R_1 \oplus R_2)}{f_{m,Q}(P \oplus R_1 \ominus R_2)}.$$

Voltando em 3.2, e substituindo os valores obtemos

$$e_m(P,Q) = \frac{f_{m,P}(Q \oplus R_2 \ominus R_1) f_{m,Q}(R_1 \ominus R_2)}{f_{m,P}(R_2 \ominus R_1) f_{m,Q}(P \oplus R_1 \ominus R_2)}. \tag{3.3}$$

Com o mesmo raciocínio, obtemos

$$\begin{aligned} e_m(P,\ominus Q) &= \frac{f_{m,P}(\ominus Q \oplus R_2 \ominus R_1) f_{m,\ominus Q}(R_1 \ominus R_2)}{f_{m,P}(R_2 \ominus R_1) f_{m,\ominus Q}(P \oplus R_1 \ominus R_2)} \\ &= \frac{f_{m,P}(\ominus Q \oplus R_2 \ominus R_1) f_{m,Q}(\ominus R_1 \oplus R_2)}{f_{m,P}(R_2 \ominus R_1) f_{m,Q}(\ominus P \ominus R_1 \oplus R_2)}. \end{aligned} \tag{3.4}$$

Sabemos que

$$e_m(P,O) = 1, \quad \forall P \in E[m]$$

logo,

$$1 = e_m(P,O) = e_m(P, Q \ominus Q) = e_m(P,Q) e_m(P,\ominus Q) \Rightarrow e_m(P,Q) = \frac{1}{e_m(P,\ominus Q)}.$$

Agora, podemos reescrever e_m^2 da seguinte maneira

$$e_m^2(P,Q) = e_m(P,Q) e_m(P,Q) = e_m(P,Q) \frac{1}{e_m(P,\ominus Q)} = \frac{e_m(P,Q)}{e_m(P,\ominus Q)}.$$

Utilizando (3.3) e (3.4) temos que

$$\begin{aligned} \frac{e_m(P,Q)}{e_m(P,\ominus Q)} &= \frac{f_{m,P}(Q \oplus R_2 \ominus R_1) f_{m,Q}(R_1 \ominus R_2)}{f_{m,P}(R_2 \ominus R_1) f_{m,Q}(P \oplus R_1 \ominus R_2)} \frac{f_{m,P}(R_2 \ominus R_1) f_{m,Q}(\ominus P \ominus R_1 \oplus R_2)}{f_{m,P}(\ominus Q \oplus R_2 \ominus R_1) f_{m,Q}(\ominus R_1 \oplus R_2)} \\ &= \frac{f_{m,P}(Q \oplus R_2 \ominus R_1) f_{m,Q}(R_1 \ominus R_2)}{f_{m,Q}(P \oplus R_1 \ominus R_2)} \frac{f_{m,Q}(\ominus P \ominus R_1 \oplus R_2)}{f_{m,P}(\ominus Q \oplus R_2 \ominus R_1) f_{m,Q}(\ominus R_1 \oplus R_2)}, \end{aligned}$$

por simplicidade, tomemos $R = R_2 \ominus R_1$, então

$$e_m^2(P,Q) = \frac{f_{m,P}(Q \oplus R) f_{m,Q}(\ominus R)}{f_{m,Q}(P \ominus R)} \frac{f_{m,Q}(\ominus P \oplus R)}{f_{m,P}(\ominus Q \oplus R) f_{m,Q}(R)}.$$

Fixando os pontos P e Q, podemos olhar a expressão do lado direito da igualdade como sendo uma função de R. Denotando por $\psi(R)$ tal função, como $f_{m,P}$ e $f_{m,Q}$ tem zeros em P e Q, respectivamente, e polos em O, então $\psi(R)$ só deve ter zeros o polos para $R = P, Q, \ominus Q, P \oplus Q, P \ominus Q$. Através de cálulos simples vemos que $\operatorname{div}(\psi(R)) = 0$, ou seja, $\psi(R)$ é constante. Concluímos que

$$\psi(R) = e_m^2(P,Q), \quad \forall R$$

Pegando em particular $R = O$, i.e, $R_1 = R_2$, temos

$$\frac{f_{m,P}(Q) f_{m,Q}(O)}{f_{m,Q}(P)} \frac{f_{m,Q}(\ominus P)}{f_{m,P}(\ominus Q) f_{m,Q}(O)} = \frac{f_{m,P}(Q) f_{m,Q}(\ominus P)}{f_{m,P}(\ominus Q) f_{m,Q}(P)} (-1)^m.$$

A última igualdade é consequência do Lema 3. Portanto,

$$e_m^2(P,Q) = (-1)^m \frac{f_{m,P}(Q) f_{m,Q}(\ominus P)}{f_{m,P}(\ominus Q) f_{m,Q}(P)}.$$

□

3.2 Emparelhamento de Tate

John Tate propôs o emparelhamento para variedades abelianas, contudo Stephen Lichtenbaum mostrou uma maneira eficiente de calculá-lo sobre variedades jacobianas de curvas algébricas. Nesse trabalho, vamos nos basear no trabalho de (FREY; RÜCK, 1994) que adaptou o emparelhamento para curvas elípticas. Não iremos fazer uma construção detalhada do Emparelhamento de Tate.

Definição 28. *Seja E uma curva elíptica sobre um corpo finto $\mathbb{F}_p$ (O é o ponto no Infinito). Sejam m e k números inteiro positivos, tais que, m é coprimo com p ($mdc(p,m) = 1$) e $\mathbb{F}_{p^k}$ contêm a m-ésima raiz da unidade ($m|p^k - 1$). Seja $G = E(\mathbb{F}_{p^k})$, $G[m]$ os subgrupo formado pelos pontos de m-torção e G/mG o grupo quociente. O Emparelhamento de Tate é um mapa da forma*

$$\phi : G[m] \times G/mG \longrightarrow \frac{\mathbb{F}^*_{p^k}}{(\mathbb{F}^*_{p^k})^m}.$$

Dados $P \in G[m]$ e $Q \in G/mG$. O divisor $m(P) - m(O)$ é principal, logo existe $f_{m,P} \in E(\mathbb{F}_p)$ como $div(f) = m(P) - m(O)$. Tome D um divisor como suporte disjunto de $div(f)$, mas de modo que seja equivalente a $(Q) - (O)$. Calculamos o Emparelhamento de Tate no par (P, Q)

$$\phi_m(P, Q) = f_{m,P}(D).$$

Vamos verificar que está bem definido (para simplificar vamos considerar a função acima com f). Dado $(P, Q) \in G[m] \times G/mG$, então se D_1, D_2 são divisores com suporte disjunto de $\text{div}(f)$ e $D_1 \equiv D_2 \equiv (Q) - (O)$ Podemos escrever $D_2 = D_1 + div(h)$ com $h \in E(\mathbb{F}_p)$. Logo

$$F(D_2) = f(D_1 + \text{div}(h)) = f(D_1)f(\text{div}(h)),$$

usando a reciprocidade de Weil, temos

$$f(D_1)f(\text{div}(h)) = f(D_1)h(\text{div}(f)) = f(D_1)h(m(P) - m(O)) = f(D_1)\left(\frac{h(P)}{h(O)}\right)^m.$$

Como $\left(\frac{h(P)}{h(O)}\right)^m \in (\mathbb{F}_p)^m$, logo pertencerá a classe de equivalência da unidade. Logo $f(D_2) = f(D_1)$.

Como D deverá ter grau zero, a escolha de um função f diferente não irá interferir nos cálculos. Na verdade, podemos tomar qualquer função tal que $\text{div}(f) \sim (P) - (O)$.

Proposição 12. *O Emparelhamento de Tate satisfaz as seguintes propriedades:*

1. *(Bilinear) Para $P_1, P_2 \in G[m]$ e $Q_1, Q_2 \in G$,*

$$\phi_m(P_1 \oplus P_2, Q_1) = \phi_m(P_1, Q_1)\phi_m(P_2, Q_1),$$

$$\phi_m(P_1, Q_1 \oplus Q_2) = \phi_m(P_1, Q_1)\phi_m(P_1, Q_2).$$

2. *(Não degenerado) Seja $P \in G[m]$. Se $\phi_m(P, Q) = 1$ para todo $Q \in G$, então $P = O$ Seja $Q \in G$, se $\phi_m(P, Q) = 1$ para todo $P \in G[m]$, então $Q \in mG$.*

Vamos agora dar um melhoramento para o Emparelhamento de Tate. Para isto, vamos antes elevar $f(D)$ à $\frac{q-1}{m}$, pois caso contrário o resultado é um elemento da classe de equivalência, e com essa adaptação não teremos esse problemas, mais que isso, o resultado será uma m-ésima raiz da unidade.

Teorema 7. *Seja m um inteiro positivo. Suponha que $P \in G[m]$ e $Q \in G$, tal que, $P \neq \pm Q$. Então definimos o Emparelhamento de Tate Quadrado como*

$$\phi_m^2(P, Q) = \left(\frac{f_{m,P}(Q)}{f_{m,P}(\ominus Q)}\right)^{\frac{q-1}{m}}.$$

Demonstração. Tome $R_1, R_2 \in G$, tais que os divisores $D_P = (P \oplus R_1) - (R_1)$ e $D_Q = (Q \oplus R_2) - (R_2)$. Segue que,

$$\phi_m(P, Q) = (f_{D_P}(D_Q))^{q-1/m} = (f_{D_P}((Q \oplus R_2) - (R_2))^{q-1/m} = \frac{f_{D_P}(Q \oplus R_2)^{(q-1)/m}}{f_{D_P}(R_2)^{(q-1)/m}}. \quad (3.5)$$

Tomando $f_{m,P} \in E(\mathbb{F}_q)$ uma função com divisor $m(P) - m(O)$, definimos

$$g(X) = f_{m,P}(X \ominus R_1) \Rightarrow \text{div}(g) = m(P \oplus R_1) - m(R_1).$$

Como no Emparelhamento de Weil, concluímos que

$$\frac{f_{D_P}(X \oplus Q)}{f_{D_P}(X)} = \frac{g(X \oplus Q)}{g(x)} = \frac{f_{m,P}(X \oplus Q \ominus R_1)}{f_{m,P}(X \ominus R_1)}$$

Considerando $X = R_2$, e voltando em (3.5), temos que

$$\phi_m(P, Q) = \left(\frac{f_{m,P}(R_2 \oplus Q \ominus R_1)}{f_{m,P}(R_2 \ominus R_1)}\right)^{q-1/m}$$

Para o ponto $\ominus Q$, definimos $D_{\ominus Q} = (\ominus Q \oplus R_2) - (R_2)$. E de maneira similar, obtemos que

$$\phi_m(P, \ominus Q) = \left(\frac{f_{m,P}(R_2 \ominus Q \ominus R_1)}{f_{m,P}(R_2 \ominus R_1)}\right)^{q-1/m}$$

De modo similar ao que foi feito no Emparelhamento de Weil, concluímos que

$$\phi_m^2(P, Q) = \frac{\phi_m(P, Q)}{\phi_m(P, \ominus Q)} = \frac{f_{m,P}(Q \oplus R_2 \ominus R_1)}{f_{m,P}(\ominus Q \oplus R_2 \ominus R_1)}$$

Definindo $R = R_2 \ominus R_1$, e olhando a ultima expressão como uma função de R, verifica-se que ela é constante, logo para $R = O$

$$\phi_m^2(P, Q) = \frac{f_{m,P}(Q)}{f_{m,P}(\ominus Q)}$$

□

4 Calculo do Emparelhamento

Neste capítulo, vamos fazer uma comparação dos emparelhamento, tal comparação será baseada na quantidade de operações necessárias para realizar o cálculo de cada emparelhamento. Para tal comparação faremos uso do algoritmo de Miller, que é bastante utilizado para a implementação de emparelhamentos.

4.1 Cadeia de Adição-Subtração

Para a implementação do emparelhamento devemos buscar por técnicas que otimizem o cálculo, isto porque, resolver um emparelhamento é trabalhoso. Sendo assim, vamos definir nesse capitulo a cadeia de adição-subtração, umas das diversas técnicas presentes na literaturas que facilitam a exponenciação. Por fim, vamos verificar que utilizando a cadeia de adição-subtração, o emparelhamento quadrado é melhor.

Vamos começar com um situação simples, suponha que pedimos para um computador calcular x^8, de modo lógico, ele vai resolver fazendo oito multiplicações, isto é, $x^8 = x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x \cdot x$. Sabe-se que, computacionalmente, a multiplicação é cara, logo um método de resolver exponenciação que diminua a quantidade de operações diminuirá drasticamente o tempo computacional gasto em um algoritmo. Na literatura são propostos algumas técnicas diferentes, contudo vamos focar apenas na que usa uma cadeia de adição-subtração.

Definição 29. *Uma sequência de números inteiros positivos $C = \{1 = a_0, a_1, ..., a_r = n\}$ é dita uma **Cadeia de Adição-Subtração** para n se, e somente se, $a_0 = 1$, $a_r = n$ e para cada $a_i \in C$ $0 < i \leqslant r$ existem j, s inteiros $0 < j, s \leqslant i$, tal que, $a_i = a_j + a_s$.*

Nesse contexto, vamos dizer que a cadeia tem comprimento r.

Exemplo 17. *Para cada inteiro positivo n, $C = \{1, 2, 3, ..., n\}$ é uma cadeia de adição-subtração.*

Contudo o interesse é sempre tentar buscar cadeia que tenham comprimento mínimo, pois considere o problema do início, para o número 8 considere a seguinte cadeia $C = \{1, 2, 4, 8\}$. Assim, para o cálculo de x^8 podemos operar da seguinte maneira: note que $x^8 = x^{4+4} = x^4 \cdot x^4 = x^{2+2} \cdot x^{2+2} = x^2.x^2.x^2.x^2$

Primeiro se calcula $x \cdot x = x^2$ e armazena esse valor; Em seguida $x^4 = x^2 \cdot x^2$ e armazena esse valor Por fim, $x^8 = x^4 \cdot x^4$

Perceba que foram necessária apenas 3 multiplicações, que é exatamente o comprimento da cadeia de oito. Isso se dá porque uma cadeia de adição-subtração é

um caminho que podemos seguir para obter um numero através de soma e subtração. Também podemos calcular x^7 do seguinte modo

$$x^7 = \frac{x^8}{x}.$$

Logo, sabemos que podemos resolver esse exponenciação com 3 multiplicações e 1 divisão. Aqui ficar mais claro do porque escolher cadeias de adição-subtração já que calcular o inverso de um ponto na curva elíptica é simples (lembre que se $P = (x, y) \Rightarrow \ominus P = (x, -y)$), ou seja, dividir na curva é barato computacionalmente. Esse fato também dificulta alguns ataques, mas não abordaremos.

4.2 Comparando os Emparelhamentos

Para essa seção vamos supor que $\text{char}(\bar{K}) \neq 2, 3$, ou seja, vamos supor que a equação da curva elíptica E é dada na forma reduzida. Vamos fixar um inteiro positivo m, e também, P, Q pontos de m-torção. Vamos definir também, para cada inteiro positivo j, a função racional $f_{j,A_p} \in \bar{K}(E)$ tal que $\text{div}(f_{j,P}) = jA_P - (jP) + (O)$. Onde A_P é um divisor equivalente á $(P) - (O)$. Note que, se P um ponto de m-torção, então $\text{div}(f_{m,A_P}) = mA_P$, isto é, $f_{m,A_P} = f_P$ (como definimos no emparelhamento). A construção de $f_{1,P}$ depende de A_P (a construção dada por Miller pode ser vista com mais detalhes em (AFTUCK, 2011)). Dados $f_{i,P}$ e $f_{j,P}$ podemos obter $f_{(i+j),P}$ do seguinte modo

$$f_{(i+j),P} = f_{i,P} f_{j,P} \frac{g_{iP,jP}}{g_{(i+j)P}}, \tag{4.1}$$

onde $g_{iP,jP}$ é a reta passando por iP e jP, e $g_{(i+j)P}$ é reta vertical passando por $(i + j)P$ e $\ominus(i + j)P$.

4.2.1 Algoritmo de Miller

O algoritmo proposto por Miller escolhe aleatoriamente dois pontos R_1, R_2 em E, e então define os divisores $A_P = (P + R_1) - (R_1)$ e $A_Q = (Q + R_2) - (R_2)$. Como acima, defini-se $f_{j,P}$ a função racional com $\text{div}(f_{j,A_P}) = j(P + R_1) - j(R_1) - (jP) + (O)$, de modo similar definimos $f_{j,Q}$.

Para o cálculo do Emparelhamento de Weil vamos precisar

$$e_m(P, Q) = \frac{f_{A_P}(A_Q)}{f_{A_Q}(A_P)} = \frac{f_{A_P}((Q \oplus R_2) - (R_2))}{f_{A_Q}((P \oplus R_1) - (R_1))} = \frac{f_{A_P}(Q \oplus R_2)}{f_{A_P}(R_2)} \frac{f_{A_Q}(R_1)}{f_{A_Q}(P \oplus R_1)}.$$

Lembremos que,

$$\frac{f_{A_P}(Q \oplus R_2)}{f_{A_P}(R_2)} \frac{f_{A_Q}(R_1)}{f_{A_Q}(P \oplus R_1)} = \frac{f_{m,A_P}(Q \oplus R_2)}{f_{m,A_P}(R_2)} \frac{f_{m,A_Q}(R_1)}{f_{m,A_Q}(P \oplus R_1)}.$$

Tomando uma cadeia de adição-subtração para m, para cada inteiro j construímos a tupla $t_j = [jP, jQ, n_j, d_j]$ onde n_j e d_j satisfazem

$$\frac{n_j}{d_j} = \frac{f_{j,A_P}(Q \oplus R_2)}{f_{j,A_P}(R_2)} \frac{f_{j,A_Q}(R_1)}{f_{j,A_Q}(P \oplus R_1)}.$$

Partindo de t_i e t_j, para calcular t_{i+j} devemos obter o valor de

$$\frac{n_{i+j}}{d_{i+j}} = \frac{f_{i+j,A_P}(Q \oplus R_2)}{f_{i+j,A_P}(R_2)} \frac{f_{i+j,A_Q}(R_1)}{f_{i+j,A_Q}(P \oplus R_1)},$$

utilizando (4.1) podemos reescrever como

$$\frac{n_{i+j}}{d_{i+j}} = \frac{n_i}{d_i}\frac{n_j}{d_j} \frac{g_{iP,jP}(Q \oplus R_2)}{g_{iP,jP}(R_2)} \frac{g_{(i+j)P}(R_2)}{g_{(i+j)P}(Q \oplus R_2)} \frac{g_{iQ,jQ}(R_1)}{g_{iQ,jQ}(P \oplus R_1)} \frac{g_{(i+j)Q}(P \oplus R_1)}{g_{(i+j)Q}(R_1)}. \tag{4.2}$$

Agora, vamos contar quantas operações de multiplicações são necessárias para resolver cada termo. A primeira coisa a se fazer é a soma dos pontos, i.e, $iP \oplus jP = (i + J)P$, do exemplo do capitulo 2, vemos que serão necessárias duas multiplicações e uma divisão. Análogo para $iQ \oplus jQ$, logo já foram gastas quatro multiplicações e duas divisões.

Vamos agora para a expressão $\frac{g_{iP,jP}(Q \oplus R_2)}{g_{(i+j)P}(R_2)}$, a reta $g_{iP,jP} = y - y(iP) - \lambda(x - x(iP))$ (como vista no Capítulo 2), logo para avaliar $g_{iP,jP}(Q \oplus R_2) = y(Q \oplus R_2) - y(iP) - \lambda(x(Q \oplus R_2) - x(iP))$ precisamos apenas de uma multiplicação (o valor de λ já foi calculado), o mesmo para $g_{iP,jP}(R_2)$.

Não é necessário nenhuma multiplicação para avaliar o termo $\frac{g_{(i+j)P}(R_2)}{g_{(i+j)P}(Q \oplus R_2)}$, pois $g_{(i+j)P} = x - x((i + j)P)$. Portanto, para as duas frações foram necessárias duas multiplicações. Para as frações restante, resolvemos de modo análogo sendo também utilizadas duas multiplicações. Por fim, para as seis frações, vamos precisar de dez multiplicações. Somando tudo temos que são necessárias dezoito multiplicações e duas divisões.

4.2.2 Algoritmo Emparelhamento quadrado

Assim, como feito anteriormente, fixada uma cadeia de adição-subtração para m, construímos para cada inteiro j a tupla $t_j = [jP, jQ, n_j, d_j]$ onde n_j e d_j satisfazem

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q) f_{j,Q}(\ominus P)}{f_{j,P}(\ominus Q) f_{j,Q}(P)}.$$

Comece com $t_1 = [P, Q, 1, 1]$, e dado t_i,t_j obtemos t_{i+j} prosseguindo:

1. Some na curva elíptica os pontos $iP \oplus jP = (i + j)P$ e $iQ \oplus jQ = (i + j)Q$.
2. Encontre os coeficientes da reta $g_{iP,jP}(X) = y(X) - y(iP) - \lambda(x(X) - x(iP))$.

3. Encontre os coeficientes da reta $g_{iQ,jQ}(X) = y(X) - y(iQ) - \lambda(x(X) - x(iQ))$.

4. Defina
$$\frac{n_{i+j}}{d_{i+j}} = \frac{n_i n_j}{d_i d_j} \frac{g_{iP,jP}(Q)}{g_{iP,jP}(\ominus Q)} \frac{g_{iQ,jQ}(\ominus P)}{g_{iQ,jQ}(P)}. \tag{4.3}$$

De modo similar, definimos t_{i-j}. Note que, nesse algoritmo não fazemos uso das linha verticais, pois $g_{(i+j)P}(Q) = g_{(i+j)P}(\ominus Q)$ (o mesmo vale para o ponto P). Quando $i + j = m$ podemos simplificar $n_{i+j}/d_{i+j} = n_i n_j / d_i d_j$, pois como os pontos são de m-torção a reta deverá ser vertical, e com isso apenas a coordenada x de cada ponto terá importância, fazendo com que as frações se simplifiquem.

Quando os termos n_m e d_m não são zeros, então o cálculo
$$\frac{n_m}{d_m} = \frac{f_{m,P}(Q) f_{m,Q}(\ominus P)}{f_{m,P}(\ominus Q) f_{m,Q}(P)} \tag{4.4}$$
foi um sucesso. Caso contrário, se n_m ou d_m zerarem, significa que $g_{iP,jP}(Q) = 0$ ou $g_{iQ,jQ}(P) = 0$ para algum i. Sem perda generalidade, suponha que o ocorreu o primeiro caso, $g_{iP,jP}$ passa pelos ponto iP, jP e $(-i - j)P$, assim $Q = iP, jP, (-i - j)P$. Em qualquer um dos caso Q seria um múltiplo de P, logo $e_m(P, Q) = 1$.

Dados t_i e t_j, vamos contar a quantidade de operações necessárias para o calculo de t_{i+j}. Como no algoritmo de Miller, vamos iniciar fazendo a soma de $iP \oplus jP = (i + j)P$ e $iQ \oplus jQ = (i + j)Q$. Já sabemos que para essa duas somas é preciso de 4 multiplicações e 2 divisões. Temos que
$$\frac{g_{iP,jP}(Q)}{g_{iP,jP}(\ominus Q)} = \frac{y(Q) - y(iP) - \lambda(x(Q) - x(iP))}{y(\ominus Q) - y(iQ) - \lambda(x(\ominus Q) - x(iQ))}.$$
Como $x(Q) = x(\ominus Q)$ só precisamos resolver uma multiplicação para obtermos os valores do numerador e denominador. O mesmo vale para a segundo fração. Por fim, vamos precisar de 6 multiplicações para multiplicar as 4 frações de (4.3). Somando tudo, é preciso 12 multiplicações e 2 divisões.

Estimando que cada divisão corresponde a 5 multiplicações, então o para o Emparelhamento de Weil Quadrado, temos uma economia de aproximadamente 20%.

4.3 Emparelhamento de Tate Quadrado

Nessa seção vamos definir um algoritmo para o emparelhamento de Tate Quadrado.

Vamos fixar uma curva elíptica E e um inteiro $m > 0$, satisfazendo as hipóteses do emparelhamento. Dados um ponto P de m-torção e um ponto Q na curva

E, vamos calcular $p_m(P, Q)$. Primeiramente, definimos uma cadeia de adição-Ssbtração para m, para cada elemento j na cadeia, definimos a tupla $t_j = [jP, n_j, d_j]$, de modo que

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q)}{f_{j,P}(\ominus Q)}.$$

Começamos com $t_1 = [P, 1, 1]$, dados t_j e t_i, obtemos t_{j+i} seguindo os passos abaixo:

1. Realizamos uma soma de pontos,i.e, $jP \oplus iP = (j + i)P$.
2. Defina a reta $g_{jP,iP} = ax + by + c$.
3. Defina
$$\frac{n_{j+i}}{d_{j+i}} = \frac{n_j}{d_j}\frac{n_i}{d_i}\frac{g_{jP,iP}(Q)}{g_{jP,iP}(\ominus Q)}.$$
De modo similar se constrói t_{j-i}.

As retas verticais não aparecem, pois como no Emparelhamento de Weil, vão ser simplificadas. Quando $j + i = m$, assim como no Weil, vamos simplificar $n_{j+i} = n_j n_i$, o mesmo para n_{j+i}. Caso n_m/d_m não for zero, então elevando ele a $(q-1)/m$ potência e obtemos o resultado. Se o resultado for zero, significa que alguma das retas $g_{jP,iP}(Q)$ (ou para $\ominus Q$) deu zero, isso só é possível se $Q = ip, Q = jP$ ou $Q = (-j - i)P$.

Vamos agora verificar quantas operações são necessárias para calcular t_{j+i} partindo de t_j e t_i. Primeiramente, fazemos a multiplicação na curva, $jP \oplus iP = (j + i)P$, que vai gastar 2 multiplicações e 1 divisão. Para resolver

$$\frac{g_{jP,iP}(Q)}{g_{jP,iP}(\ominus Q)} = \frac{y(Q) - y(iP) - \lambda(x(Q) - x(iP))}{y(\ominus Q) - y(iP) - \lambda(x(\ominus Q) - x(iP))}$$

é necessário apenas 1 multiplicação, já que $x(Q) = x(\ominus Q)$. Por fim, para combinar os itens das 3 frações, vamos precisar de 4 multiplicações. Portanto, é necessário 7 multiplicações 1 divisão para obtermos t_{j+i}.

4.3.1 Algoritmo de Miller para Emparelhamento de Tate

Para o cálculo de

$$\phi_m(P, Q) = f(D_Q)$$

vamos tomar $R \in E$, e definir $D_Q = (Q \oplus R) - (R)$. Também, vamos fixar um inteiro $m > 0$ e tomar uma cadeia de adição-subtração. Por fim, definimos a tripla $t_j = [jP, n_j, d_j]$, tal que,

$$\frac{n_j}{d_j} = \frac{f_{j,P}(Q \oplus R)}{f_{j,P}(R)}.$$

Partindo de t_j e t_i, construímos t_{j+i} seguindo os passos a seguir:

1. Fazer a soma na curva $jP \oplus iP = (j+i)P$.
2. Definir a reta passando por iP e jP i.e, $g_{iP,jP} = ax + by + c$.
3. Defina
$$\frac{n_{j+i}}{d_{j+i}} = \frac{n_j}{d_j}\frac{n_i}{d_i}\frac{g_{iP,jP}(Q \oplus R)}{g_{i+j}(Q \oplus R)}\frac{g_{i+j}(R)}{g_{iP,jP}(R)}.$$

Nesse algoritmo, partindo de t_j e t_i, para calcular t_{j+i}, vão ser necessárias 10 multiplicações e 1 divisão. Pois, vai ser necessário uma soma na curva, que gasta 2 multiplicações e 1 divisão. Para o calculo de $g_{iP,jP}(R)$ e $g_{iP,jP}(Q \oplus R)$ vão ser necessárias uma multiplicação para cada. Por fim, para calcular as 4 frações é necessário 6 multiplicações. Logo, para o cáculo de t_{i+j} são necessárias 10 multiplicações e 1 divisão.

Temos um econima de 20% para o Tate quadrado, caso consideremos que cada divisão equivale a 5 multiplicações.

5 Aplicação no Protocolo de Diffie-Hellman

Neste capítulo daremos um breve aplicação dos emparelhamentos, mais especificamente, vamos dar uma solução para o problema do protocolo tripartido de Diffie-Hellman, para um entendimento mais profundo veja (JOUX, 2000).

5.1 Problema do Logaritmo Discreto

Conhecemos a função logarítmica como sendo $\log_b a = n$, onde o expoente n é tal que, $a = b^n$. Geralmente, trabalhamos como o log nos número reais, de modo que, a função é contínua. Vamos agora definir a ideia do logaritmo para grupos cíclicos finitos (e por esse motivo damos o nome de Logaritmo Discreto ou LD).

Seja $G = \langle g \rangle$ um grupo cíclico, então dado $a \in G$, temos que, $a = g^n$, $n \in \mathbb{Z}$. Caso g tenha uma ordem finita, sabemos que n não é único.

Definição 30. *Seja $G = \langle g \rangle$ e $a \in G$. Definimos o logaritmo discreto de a na base g, como sendo o menor inteiro n que satisfaz a igualdade $a = b^n$.*

Note que, caso $|g| = n$, então $g^n = g^j$, se e somente se, $n \equiv j \mod n$. Logo, $\log_g a$ é determinado módulo a ordem de g.

O Logaritmo Discreto tem algumas propriedades semelhantes ao log convencional, i.e,

$$\log_g ac = \log_g a + \log_g c \quad \text{e} \quad \log_g a^i = i \log_g a.$$

Vamos analisar agora a dificuldade de calcular o LD em diferentes grupos. Primeiro considere $G = (\mathbb{Z}_{p-1}, +)$ (grupo aditivo, p é primo). Considere $y \in G$. Supondo que $y \neq 1$ (caso trivial), podemos escreve $y = g + g + ... + g = xg$ (onde g é um gerador do grupo)

$$xg \equiv y \mod (p-1) \Rightarrow x \equiv yg^{-1} \mod (p-1)$$

Fácil de computar.

Agora considere $G = (\mathbb{Z}_p^*, \cdot)$ (grupo multiplicativo). Analogamente, considere $y \in G$, de modo que, $y = g^x$. Temos

$$g^n \equiv y \mod (p-1).$$

Resolver essa congruência não é algo trivial, de modo que, até um computador pode ter dificuldades caso p seja muito grande. Para mais detalhes, há dois algoritmos bem

famosos na literatura que facilitam o calculo do LD, algoritmos de Shanks e Pollard. Um outro algoritmo bem conhecido é o de Pohlig e Hellman, o algoritmo proposto por eles calcula LD em tempos significativos quando a ordem do grupo é produto de primos pequenos.

5.2 Protocolo Diffie-Helman

Temos registro do uso de técnicas para codificar mensagens desde o antigo Egito. Atualmente, criptografia, tornou-se uma ciência que se preocupa mais do que embaralhar uma mensagem, preocupações como autenticidade da mensagem, autenticidade de quem envio, etc. São sempre tópicos abordadas no estudo de criptografia. Contudo nesse texto, não abordaremos nenhum desses temas, tão pouco, iremos dar a implementação de um algoritmo de criptografia. Nosso estudo vai se basear em um problema da criptografia que é a troca de chaves.

Para ficar mais claro, a criptografia computacional consiste no embaralhamento de dados, existem vários algoritmos que fazem esse embaralhamento utilizando diferentes técnicas. Contudo, apenas o algoritmo não é suficiente para manter uma segurança adequado, pois, bisbilhoteiros podem descobri qual algoritmo esta sendo usado e recuperar os dados criptografados. Para contornar esse problema, cada algoritmo tem uma "chave", que geralmente é um número ou uma lista de números, que vai de uma certa forma ser responsável pela ordem do embaralhamento.

Suponha que Antônio e Bob desejam se comunicar utilizando um canal público, de modo que ninguém consiga saber sobre o que eles estão falando. Para isso, eles vão escolher algum método de criptografar, e também combinar uma chave. Tal chave é responsável por criptografar é descriptografar. Para essa configuração, damos o nome de criptografia simétrica.

Continue com Antônio e Bob querendo trocar informações. Contudo, suponha que eles não tenham combinado antes uma chave, e a única forma que eles tem para se comunicar é um canal público. A questão de como eles poderiam combinar uma chave através de um canal público sem que nenhum bisbilhoteiro também a obtivesse, levou bastante tempo para ser respondida, contudo Whitfield Diffie e Martin Hellman propuseram um protocolo para resolver esse problema(conhecido como Diffie-Helman ou DH).

Assim, com o uso do protocolo de DH surgiram técnicas de criptografia, conhecidas como criptografia assimétrica. Nesse caso, cada indivíduo tem um par de chaves, a chave publica, e a chave privada. E através dessas duas chaves duas pessoas conseguem combinar uma chave de maneira segura.

Vale lembra que o método DH não é para criptografar, ele funciona como uma troca de chaves em um meio público de forma segura.

Vamos agora a um exemplo de como Antônio e Bob poderiam combinar uma chave utilizando o DH.

- Antônio e Bob combinam uma curva elíptica sobre um corpo $\mathbb{F}_p$, tal que, o problema do logaritmo discreto seja difícil de resolver. Além disso, devem escolher um ponto P, de modo que, o subgrupo gerado por P tenha ordem grande.
- Antônio escolher um inteiro a (chave privada) e computa $aP = P_a$ e torna P_a publico (chave pública).
- Bob escolher um inteiro b e computa $bP = P_b$ e o torna publico.
- Antônio calula $aP_b = abP$.
- Bob calcula $bP_a = baP = abP$.
- Antônio e Bob escolhem uma forma de extrair uma chave de abP.

Perceba que, um bisbilhoteiro teria acesso a curva elíptica e aos ponto P, aP e bP. Tendo que calcular abP apenas com essas informações. Não há ainda conhecimento de alguma técnica para obter tal ponto, sem antes resolver logaritmo discreto , i.e, encontra a de através de aP e P

5.3 Protocolo Diffie-Helman Tripartido

Suponha agora que três pessoas queiram se comunicar, ou seja, combinar uma chave em comum utilizando um canal público. Note que, o método acima é um pouco falho, pois, suponha que Antônio, Bob e Carlos, cada um escolha um inteiro a, b e c. E então cada um vai publicar aP, bP e cP. Vamos nos colocar no lugar de Carlos, a chave em comum deverá ser $abcP$, contudo só teremos acesso à aP e bP, desse modo, para termos abP devemos resolver o PLD.

Uma maneira de contornar esse problema é repetir o protocolo duas vezes, i.e, Antônio divulga aP para Bob, este divulga bP para Carlos, que divulga cP para Antônio. Na segunda rodada, Antônio divulga acP para Bob, que divulga abP para Carlos, que divulga bcP para Antônio.

Assim, no final do processo todos terão condições de calcular $abcP$. Contudo, essa solução não é muito viável, pois repetir o processo gasta um tempo. Assim, vamos tentar obter uma função F, tal que,

$$F(a, bP, cP) = F(b, aP, cP) = F(c, aP, bP).$$

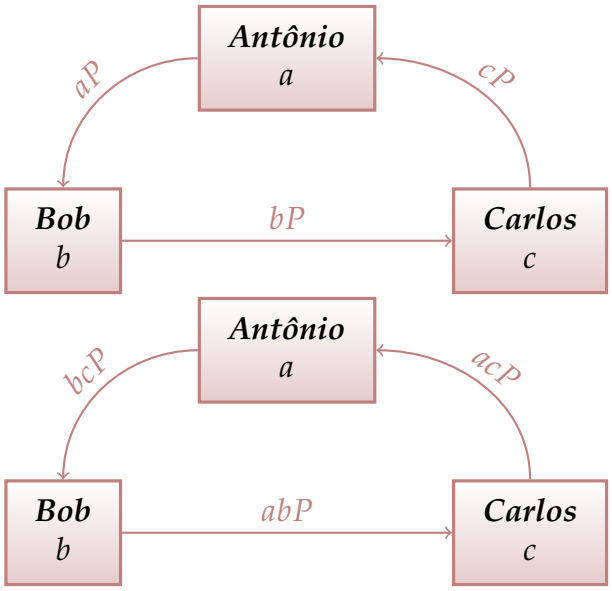

Figura 3 – A divulgação das informações na primeira e na segunda rodada.

Por conta da propriedade de ser bilinear, podemos tomar o emparelhamento e_m para assumir esse papel, assim

$$F(a, bP, cP) = e_m(bP, cP)^a = e_m(aP, cP)^b = e_m(aP, bP)^c = e_m(P, P)^{abc}.$$

Contudo, $e_m(P, P) = 1$, então é necessário que peguemos outro ponto $Q \in E[m]$, e portando cada indivíduo vai divulgar um par de pontos (P_x, Q_x). Carlos, por exemplo, terá acesso aos pares (P_a, Q_a) e (P_b, Q_b) e então, computará $\phi_m(P_a, Q_b)^c = \phi_m(aP, bQ)^c = \phi_m(P, Q)^{abc}$ (ou $\phi_m(P_b, Q_a)^c = \phi_m(P, Q)^{abc}$). Realizando este processo, todos obtém o mesmo resultado.

Utilizando um par de ponto (P, Q), podemos utilizar o Emparelhamento de Tate. Definimos os divisores $D_P = (P) - (O)$ e $D_Q = (Q \oplus R) - (R)$. E assim o algoritmo pode ser visto na tabela a seguir

Antônio Escolher a	Bob Escolher b	Carlos Escolher c
Divulga o par (P_a, Q_a)	Divulga o par (P_b, Q_b)	Divulga o par (P_c, Q_c)
Calcula o emparelhamento $\phi_m(P_b, Q_c)^a$	Calcula o emparelhamento $\phi_m(P_a, Q_c)^b$	Calcula o emparelhamento $\phi_m(P_a, Q_b)^c$
Todos obtem o mesmo valor $\phi_m(P, Q)^{abc}$		

Referências

AFTUCK, A. E. The weil pairing on elliptic curves and its cryptographic applications. UNF Digital Commons, 2011. Citado na página 53.

BONEH, D.; FRANKLIN, M. Identity-based encryption from the weil pairing. In: SPRINGER. *Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings*. [S.l.], 2001. p. 213–229. Citado na página 13.

DIFFIE, W.; HELLMAN, M. New directions in cryptography. *IEEE transactions on Information Theory*, v. 22, n. 6, p. 644–654, 1976. Citado na página 12.

EISENTRÄGER, K.; LAUTER, K.; MONTGOMERY, P. L. Improved weil and tate pairings for elliptic and hyperelliptic curves. In: SPRINGER. *Algorithmic Number Theory: 6th International Symposium, ANTS-VI, Burlington, VT, USA, June 13-18, 2004, Proceedings 6*. [S.l.], 2004. p. 169–183. Citado na página 13.

FREY, G.; RÜCK, H.-G. A remark concerning -divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of computation*, v. 62, n. 206, p. 865–874, 1994. Citado na página 49.

FULTON, W. *Algebraic curves*. [S.l.]: Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. xxii+226 p. (Advanced Book Classics). An introduction to Algebraic Geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original. ISBN 0-201-51010-3. Citado 2 vezes nas páginas 14 e 33.

JOUX, A. *A One Round Protocol for Tripartite Diffie–Hellman*. [S.l.], 2000. 385–393 p. Citado 2 vezes nas páginas 13 e 58.

_____. The weil and tate pairings as building blocks for public key cryptosystems. In: SPRINGER. *ANTS*. [S.l.], 2002. v. 2369, p. 20–32. Citado na página 13.

KOBLITZ, N. *A Course in Number Theory and Cryptography*. [S.l.]: Springer Science & Business Media, 1987. Citado na página 12.

MENEZES, A. An introduction to pairing-based cryptography. *Recent trends in cryptography*, AMS, v. 477, p. 47–65, 2009. Citado na página 13.

MENEZES, A.; VANSTONE, S.; OKAMOTO, T. Reducing elliptic curve logarithms to logarithms in a finite field. In: *Proceedings of the twenty-third annual ACM symposium on Theory of computing*. [S.l.: s.n.], 1991. p. 80–89. Citado na página 12.

MILLER, V. et al. Short programs for functions on curves. *Unpublished manuscript*, Citeseer, v. 97, n. 101-102, p. 44, 1986. Citado na página 13.

MILLER, V. S. *Use of Elliptic Curves in Cryptography*. [S.l.]: Springer, 1986. Citado na página 12.

SILVERMAN, J. H. *The Arithmetic of Elliptic Curves*. [S.l.]: Springer, 2009. v. 106. Citado 5 vezes nas páginas 14, 18, 24, 31 e 38.

VAINSENCHER, I. *Introdução às Curvas Algébricas Planas*. [S.l.]: Impa, 1979. Citado 3 vezes nas páginas 14, 17 e 23.