Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

Dissertação de Mestrado

CRIPTOGRAFIA USANDO CURVAS HIPERELÍPTICAS

por

Alonso Sepúlveda Castellanos

Mestrado em Matemática - Campinas - SP

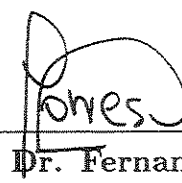
Orientador: **Prof. Dr. Fernando Eduardo Torres Orihuela**

Este trabalho contou com apoio financeiro do CNPq.

CRIPTOGRAFIA USANDO CURVAS HIPERELÍPTICAS

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Alonso Sepúlveda Castellanos** e aprovada pela comissão julgadora.

Campinas, 12 de Março de 2004.



Prof. Dr. Fernando E. Torres Orihuela

Banca examinadora:

Prof. Dr. Fernando E. Torres Orihuela.

Prof. Dr. Paulo Henrique Viana.

Prof. Dr. Paulo Roberto Brumatti.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP como requisito parcial para obtenção do título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Castellanos, Alonso Sepúlveda

C276c Criptografia usando curvas hiperelipticas/Alonso Sepúlveda
Se63c Castellanos-- Campinas, [S.P. :s.n.], 2004.

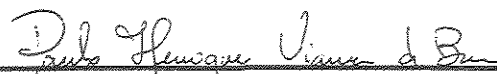
Orientador : Fernando Eduardo Torres Orihuela

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

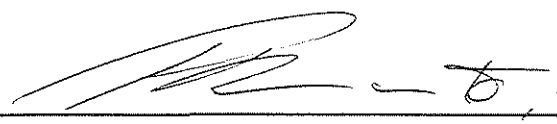
1.Criptografia. 2.Curvas algébricas. 3.Logaritmos. I. Torres Orihuela, Fernando Eduardo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Dissertação de Mestrado defendida em 12 de março de 2004 e aprovada pela Banca Examinadora composta pelos Profs. Drs.

Prof (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA



Prof (a). Dr (a). PAULO HENRIQUE VIANA DE BARROS



Prof (a). Dr (a). PAULO ROBERTO BRUMATTI

Ao meu DEUS

Aos meus pães JOSE ALONSO E YOLANDA

Ao $(0, 12, 14, 17)$

Agradecimentos

A toda minha familia na Colômbia.

Aos senhores da casa onde estou morando Mario e Lucia, pela companhia e ambente familiar que tem compartilhado comigo durante me estadia no Brasil.

A minha igreja por tudo o que tem-me ensinado.

Ao Thyago e Elder, duas pessoas que tem estado mais perto de mi, apoiandome e orientandome para fazer o melhor.

Ao meu orientador e amigo Fernando Torres pelo apoio para conseguir esta nova escada na vida.

Aos meus amigos da facultade Adriana, Germano, Rodolfo, Laercio e todos os que tem compartilhado comigo, directa ou indirectamente.

Aos Ednaldo, Cidinha e Tânia pelos seus relacionamentos implícitos comigo.

Aos professores que tive aula, pelo que aprendi ao igual que aos professores da banca por seus comentarios sobre a teses.

.....Todos fazem parte da minha lenda de vida, nunca os esquecere.....

Abstract

In 1989, Koblitz introduced by the first time the hyperelliptic cryptosystems, which based their security on the resolution of the discrete logarithm problem on the Jacobian of a hyperelliptic curve. In this article, Koblitz generalized the algorithm to add points in the Jacobian presented by Cantor in 1987.

At this dissertation, we study properties of the hyperelliptic curves and its Jacobians, looking at the implementation of public-key cryptosystems. Also, we present Cantor's algorithm to add points in the Jacobian (This is important to the efficiency of the cryptosystem) and we show an algorithm to attack the discrete logarithm problem on theses groups (The intractability of this problem is essential for the security of the cryptosystem).

Resumo

Em 1989, Koblitz introduziu pela primeira vez os criptossistemas hiperelípticos, os quais baseiam sua segurança na resolução do problema do logaritmo discreto sobre o Jacobiano de uma curva hiperelíptica. Neste artigo, Koblitz generalizou o algoritmo para somar pontos no Jacobiano apresentado por Cantor em 1987.

Nesta dissertação, estudamos propriedades das curvas hiperelípticas e seus Jacobianos, visando à implementação de criptossistemas de chave pública. Também apresentamos o algoritmo de Cantor para somar pontos no Jacobiano (isto é importante para efetividade do criptossistema) e mostramos um algoritmo para atacar o problema do logaritmo discreto sobre estes grupos (a intratabilidade deste problema é essencial para a segurança do criptossistema).

LISTA DE SÍMBOLOS

• K	Um corpo de característica $p \geq 0$
• $\bar{K}$	O fecho algébrico de K
• $G_{\bar{K}/K}$	Grupo de Galois de $\bar{K}/K$
• $\text{mdc}(a, b)$	Máximo divisor comum de a e b
• $\mathbb{Z}/n\mathbb{Z}$	Grupo aditivo dos inteiros módulo n
• $(\mathbb{Z}/n\mathbb{Z})^*$	Grupo multiplicativo dos inteiros módulo n
• $\mathbb{F}_q$	Corpo finito com q elementos
• $\mathbb{F}_q^*$	Corpo finito sem o zero
• $\mathbf{P}^2(K)$	Plano projetivo sobre K
• $\#(S)$	Cardinalidade do conjunto S
• $\mathbf{E}$	Curva elíptica
• $\mathbf{E}(K)$	Pontos racionais de $\mathbf{E}$ sobre K
• $\mathcal{O}$	Ponto no infinito
• $\Delta = \Delta(\mathbf{E})$	Discriminante da curva elíptica $\mathbf{E}$
• $P \oplus Q$	Soma de pontos da curva elíptica
• $\#\mathbf{E}(K)$	Número de pontos racionais de $\mathbf{E}$ sobre K

- ϕ Função de Euler
- $\log_b x$ Logaritmo em base b de x
- $GL_d(R)$ Conjunto de matrizes invertíveis com entradas no anel R
- $\det(A)$ Determinante da matriz A
- $\mathrm{Aut}_L(C)$ Grupo de automorfismos de C sobre L
- $\mathbf{H}$ Curva hiperelíptica
- n_L Número de pontos racionais de $\mathbf{H}$ sobre L
- D Divisor de H
- $\deg(D)$ Grau de um divisor D sobre $\mathbf{H}$
- $\mathrm{Sup}(D)$ Suporte de um divisor D
- $\mathrm{Div}_L(\mathbf{H})$ Grupo de divisores de $\mathbf{H}$ definidos sobre L
- $\mathrm{Div}_L^0(\mathbf{H})$ Grupo de divisores de grau zero definidos sobre L
- $L[\mathbf{H}]$ Anel de funções polinomiais de $\mathbf{H}$ sobre L
- $L(\mathbf{H})$ Corpo de funções racionais de $\mathbf{H}$ sobre L
- $\mathrm{div}(r)$ Divisor principal de uma função racional
- $v_P(r)$ Valoração ou ordem de $P \in \mathbf{H}$ em r
- $\mathcal{J}_L(\mathbf{H})$ Jacobiano de $\mathbf{H}$ sobre L
- $\#\mathcal{J}_L(\mathbf{H})$ Número de pontos do Jacobiano de $\mathbf{H}$ sobre L

LISTA DE FIGURAS

1.1 Diagrama de Comunicação 2

3.1 Curva Elíptica $\mathbf{E} : y^2 = x^3 - 4x$ Soma de P e Q 21
3.2 Duplicação dos pontos P e T 21

4.1 Curva Hiperelíptica 1 32
4.2 Curva Hiperelíptica 2 33
4.3 Curva Hiperelíptica 3 33

CONTEÚDO

Lista de Símbolos i

Lista de Figuras iii

Introdução vi

1 Aspectos Gerais 1

1.1 Criptoanálise 3

1.2 Criptografia de Chave Privada 5

1.3 Criptografia de Chave Pública 8

2 Criptossistemas Públicos Básicos 11

2.1 Diffie-Hellman 11

2.2 RSA 12

2.3 ElGamal 15

2.3.1 Ataque ao Problema do Logaritmo Discreto 16

3 Criptossistemas Elípticos 19

3.1 Noções da Teoria de Curvas Elípticas 19

3.2 Criptossistemas usando Curvas Elípticas 23

4 Criptossistemas Hiperelípticos 28

4.1 Conceitos Básicos de Curvas Hiperelípticas 29

4.1.1 Generalidades 29

4.1.2 Pontos racionais 31
4.1.3 Exemplos 32
4.1.4 Uma involução sobre **H** 34
4.1.5 Divisores sobre **H** 35
4.1.6 Corpo de funções racionais 35
4.1.7 Pontos regulares e pólos de uma função racional 36
4.1.8 Divisores principais. 36
4.1.9 Divisores semi-reduzidos 38
4.1.10 Divisores reduzidos 39
4.2 O Jacobiano de **H** 42
4.2.1 Pontos racionais do Jacobiano 42
4.2.2 Soma de Divisores no Jacobiano 43
4.2.3 Automorfismo de Frobenius 49
4.3 Criptossistemas usando Curvas Hiperelípticas 50
4.3.1 Ataque Index-Calculus para resolver o HECDLP 51

Comentários **53**

Apêndice **56**

A Preliminares Matemáticos **56**

B Complexidade Algoritmica **59**
B.1 Classes de Complexidade 62
Bibliografia 64

Introdução

Através dos anos a criptografia vem sendo usada para enviar mensagens ocultas com o objetivo de serem lidas somente por pessoas autorizadas. Entre os problemas que a criptografia resolve, referentes a segurança em uma comunicação, temos: privacidade, integridade, autenticidade e o não repudio das mensagens. Desde o início do último século, uma fonte permanente de algoritmos para a implementação de criptossistemas de chave pública são provenientes de Variedades Abelianas (veja [8, Milne, Cap. V]), em especial do Jacobiano de curvas algébricas. Este capítulo introdutório descreve o objetivo do presente trabalho, assim como a estrutura na qual foram desenvolvidos os demais capítulos, com o intuito de facilitar a compreensão da teoria aqui exposta.

Objetivo

O objetivo desta dissertação é o estudo de propriedades das Curvas Hiperelípticas e seus Jacobianos, visando a construção de criptossistemas de chave pública. Esta implementação foi introduzida pela primeira vez por Koblitz [19], baseado na intratabilidade do problema do Logaritmo Discreto em subgrupos do Jacobiano de curvas hiperelípticas. Aqui, surgem questões sobre a implementação deste tipo de criptossistemas e sua segurança frente ataques como o Index-Calculus[2].

[2]Um ataque para resolver o Problema do Logaritmo Discreto (DLP). No entanto, será visto com detalhe na subseção (2.3.1)

Dados Históricos

A palavra *criptografia* provém do grego *kryptós-grapho* que significa escritura oculta. Desde a antiguidade, a escrita oculta tem estado presente intrínsecamente no sistema de escrita hieroglífica dos egípcios. Os romanos, utilizavam-a para comunicar planos de batalha durante suas lutas; através dos anos, a escrita oculta manteve seu maior interesse no âmbito militar e tal é o fato que durante a Segunda Guerra Mundial, o exército alemão estabelecia comunicações ocultas via uma máquina, chamada *ENIGMA*[3], para orientar suas tropas contra o exército inimigo. Ao tempo, num lugar chamado Bletchley Park na Inglaterra, um grupo de cientistas, entre os que se encontrava Alan Turing[4], trabalhavam no projeto *ULTRA* tentando descobrir as mensagens ocultas enviadas pelo exército alemão. Como conseqüência, este grupo de cientistas construiu o primeiro computador da história, chamado *Colossus*.

Desde então, até hoje têm havido um crescimento enorme de estudos relacionados com a escrita oculta, chegando a converter esta arte em uma ciência de interesse para o avanço tecnológico, chamada de *Criptografia*. Os estudos feitos no início desta área estavam somente relacionados com informações militares secretas devido à conjuntura política do mundo; mais sobre a história da criptografia pode-se ver em [17].

A partir da década do 70, após um trabalho fundamental de Diffie e Hellman [10], a criptografia se torna uma ciência ao serviço do cidadão comum. Para ter uma escrita oculta se aplica um *Criptossistema* que simplesmente é um algoritmo que dá segurança e proteção em uma comunicação. A construção destes algoritmos é freqüêntemente realizado a partir de objetos matemáticos tais como: Números Primos, Grupos Finitos, Curvas Elípticas, Curvas Hiperelípticas, Jacobianos de Curvas e Variedades Abelianas [4], [21], [29], [40].

Em 1985, Victor Miler (IBM) e Neal Koblitz (Universidade de Washington) independentemente propuseram os Criptossistemas Elípticos [18] como implementação de criptossistemas de chave pública baseando sua segurança na resolução do Problema do Logaritmo Discreto (DLP) sobre grupos abelianos finitos. Devido à aparição de técnicas para abordar o problema do logaritmo discreto sobre o grupo de pontos de um tipo de curvas elípticas [36], [4]; se faz necessário o estudo de novos campos onde a implementação de criptossistemas de chave pública seja adequada para fins criptográficos.

[3]patenteada pelo engenheiro alemão Arthur Scherbius em 1923.

[4](1912-1954) Pioneiro na ciência da computação e na inteligência artificial.

Pelas considerações acima, em 1989, Neal Koblitz [19] introduziu os chamados criptossistemas hiperelípticos pela primeira vez, usando o Jacobiano de curvas hiperelípticas definidas sobre corpos finitos, baseado na intratabilidade computacional para o (DLP) sobre este tipo de grupos, isto é, baseado em um algoritmo de tempo exponencial para resolver este problema. As curvas hiperelípticas definidas sobre corpos de característica 2 são de maior interesse na implementação de sistemas criptográficos, pois a eficiência das operações neste tipo de corpos é melhor.

Estrutura da Dissertação

O presente trabalho está dividido da seguinte maneira:

- No capítulo 2 apresentamos a teoria elementar de criptografia de chave privada (ou simétrica) e de chave pública (ou assimétrica), assim como os tipos de técnicas usadas para tentar quebrar um criptossistema, fornecendo uma ampla visão no contexto criptográfico.

- No capítulo 3 estudamos os criptossistemas básicos de chave pública e fazemos alguns exemplos particulares (não práticos) para mostrar o funcionamento destes. Mencionamos métodos existentes para quebrar os criptossistemas, assim como considerações a levar na escolha dos parâmetros para ter maior segurança. Também mostramos um ataque eficiente para os criptossistemas implementados sobre corpos finitos.

- No capítulo 4 é inteiramente dedicado aos Criptossistemas Elípticos, mostramos os conceitos básicos de curvas elípticas e fazemos um exemplo de aplicação destas curvas em um criptossistema de chave pública (ElGamal).

- No capítulo 5 estudamos os Criptossistemas Hiperelípticos e definimos a estrutura de grupo sobre o qual estarão baseadas as operações do criptossistema. Mostramos um algoritmo para a soma de pontos do Jacobiano que foi introduzida pela primeira vez por Cantor [7], e que foi melhorada por Koblitz [19]; além de resultados como: o número de pontos deste grupo e o ataque index calculus implementado para este tipo criptossistemas.

- Finalmente comentamos alguns dos pontos mais relevantes observados ao longo do trabalho, resultados importantes de outros trabalhos obtidos nesta area, assim como propostas futuras de pesquisa a continuar.

CAPÍTULO 1

Aspectos Gerais

Como foi mencionado na introdução, a criptografia estuda criptossistemas que nada mais são algoritmos que fornecem segurança e proteção em uma comunicação. Os aspectos da segurança, estão relacionados com *a Privacidade*, *a Integridade*, *a Autenticidade* e *o não Repudio* das mensagens durante uma comunicação.

A privacidade faz referência ao fato que uma mensagem só pode ser lida por pessoas autorizadas. Por exemplo, se em uma ligação telefônica entre duas pessoas, se uma terceira escuta a conversa, então está violando a privacidade da comunicação.

A integridade está relacionada ao fato de ter certeza que a mensagem não foi alterada durante a comunicação. Por exemplo, utilizando alguns sites da internet podem-se fazer diversas compras. Se a informação que se utilizou para estas compras não fosse controlada e caso houvesse alguma violação desta, poderia causar prejuízo tanto ao consumidor como ao vendedor; assim se perderia a integridade da comunicação.

A autenticidade se tem quando podemos confirmar a identidade da pessoa que enviou a mensagem. Por exemplo, quando uma pessoa vai descontar um cheque, este passa por uma verificação de autenticação para saber se a assinatura esta correta, pois do contrário não poderá receber o dinheiro; em caso de uma mensagem, se esta não for confirmada sua autenticidade, a informação recebida não teria credibilidade.

O não repudio evita que alguma pessoa envolvida na comunicação tente negar o envio ou recebimento de uma mensagem.

Esquemáticamente a aplicação de um criptossistema durante uma comunicação está representada na Figura (1.1). Seja **A** um usuário que deseja enviar uma mensagem segreda (ou *texto plano*) **m** para um usuário **B**. Então **A** aplica uma função ε para cifrar a **m** (processo chamado de *cifrado* da mensagem), e obtém a mensagem cifrada (texto cifrado ou criptograma) **c**. Logo **A** envia **c** para **B** por uma linha de comunicação a qual não é necessariamente segura no sentido que um terceiro usuário não autorizado poderia ter acesso a **c**. Finalmente, **B** recupera **m** aplicando uma função d para decifrar a **c** (este processo é chamado de *decifrado* da mensagem).

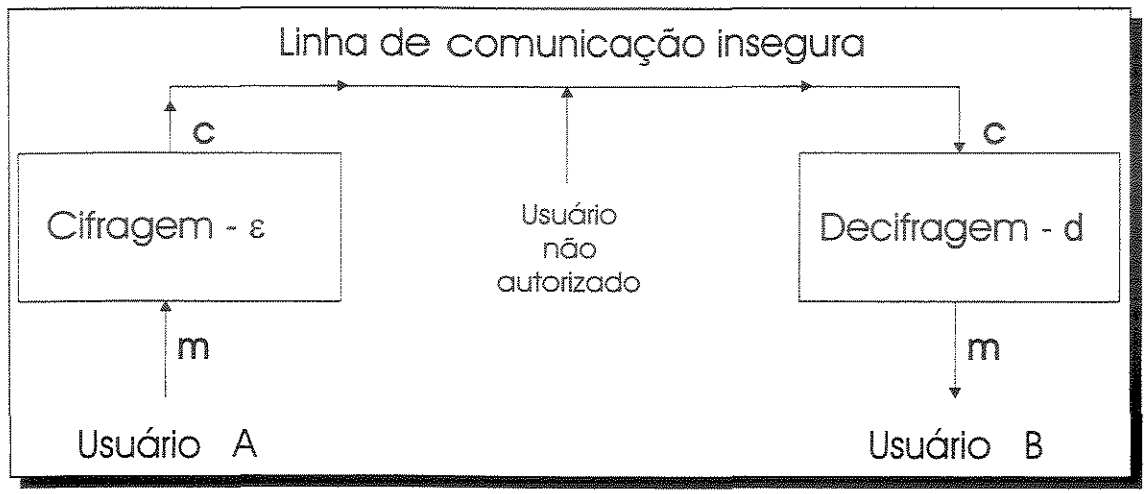


Figura 1.1: Diagrama de Comunicação

Formalmente um criptossistema é descrito por uma sêxtuple

$$(\mathcal{A}, \mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}), \tag{1.1}$$

em que:

- $\mathcal{A}$ é um conjunto finito, chamado o *alfabeto de entrada*;[1]
- $\mathcal{M}$ é um conjunto formado por cadeias finitas de comprimento constante; este conjunto é chamado o *espaço de mensagens básicas*;
- $\mathcal{C}$ é também um conjunto formado por cadeias finitas de elementos de $\mathcal{A}$, onde o comprimento de cada cadeia não é necessáriamente constante (ver Exemplo 2.3); este conjunto é chamado o *espaço de mensagens básicas cifrados*;

[1]Usualmente $\mathcal{A}$ é o alfabeto binário $\{0, 1\}$, o alfabeto inglês ou o alfabeto de alguma língua.

- $\mathcal{K}$ é um conjunto finito, cada elemento deste conjunto é chamado de *chave* e é uma ferramenta fundamental para manter oculta a informação;
- $\mathcal{E}$ é o espaço das funções $\varepsilon : \mathcal{M} \longrightarrow \mathcal{C}$; cada uma destas funções é chamada de *função de cifragem*;
- $\mathcal{D}$ é o espaço das funções $d : \mathcal{C} \longrightarrow \mathcal{M}$; cada uma destas funções é chamada de *função de decifragem*;

tal que, cada chave $k \in \mathcal{K}$ determina uma única função de cifragem $\varepsilon_k \in \mathcal{E}$ e uma única função de decifragem $d_k \in \mathcal{D}$ tais que $d_k \circ \varepsilon_k = \mathrm{id}|_{\mathcal{M}}$. Além disso, se as funções ε_k e d_k satisfazem $\varepsilon_k \circ d_k = \mathrm{id}|_{\mathcal{C}}$, então é possível assinar as mensagens enviadas ao outro usuário, para garantir a autenticidade das mensagens.

A criptografia está dividida em dois tipos:

(1) de *chave privada* (ou *simétrica*);

(2) de *chave pública* (ou *assimétrica*).

Em vários casos se usa uma combinação destes dois tipos, pois um criptossistema de chave pública apesar de ser mais seguro, é computacionalmente mais custoso; isto é, requer de mais recursos computacionais. Um fato importante que se deve ter ao construir um criptossistema é, por exemplo, os possíveis ataques que existem para o criptossistema e o tempo que estes demoram para descobrir a mensagem; considerações de este tipo são básicas para que o criptossistema não seja facilmente quebrado. Esta e outras questões motivaram o desenvolvimento de uma ciência paralela à criptografia, chamada *Criptoanálise*. A importância desta nova ciência é devida ao fato que a segurança de um criptossistema não pode ser garantida indeterminadamente, pois este mesmo criptossistema pode ser desvendado em um futuro não tão distante.

Como veremos a seguir, a criptoanálise estuda as formas possíveis (ou *ataques*) que uma pessoa não autorizada pode dispor para descobrir o conteúdo de uma mensagem cifrada ou o que é o mesmo, *quebrar o criptossistema* [29, p. 41], [30, p. 209], [40, p. 24].

1.1 Criptoanálise

O objetivo da criptoanálise é de descobrir o conteúdo de uma mensagem original a partir de uma mensagem cifrada sem conhecer a chave para decifrá-a. Um *criptoanalista* é uma

pessoa que faz criptoanálise; vulgarmente conhecida com o nome de intruso, usuário não autorizado, atacante, pirata ou hacker.

Os ataques que um criptoanalista pode fazer numa comunicação entre os usuários **A**, **B** estão classificados como segue:

(1) *Ativos*: aqui o criptoanalista faz ações indiretas para recuperar a mensagem original; por exemplo, se faz passar por uma pessoa autorizada ou tenta substituir uma mensagem de **A** para **B** por outra falsa, porém esta pessoa não é considerada um verdadeiro criptoanalista.

(2) *Passivos*: aqui o criptoanalista tenta recuperar a mensagem original **m** enviada por **A** a partir da correspondente mensagem cifrada **c** (isto também pode ser feito se ele descobre a chave k utilizada por **B** para decifrar **c**). Entre estes ataques temos:

   (2.1) *Mensagem cifrada (parcialmente) conhecida*: aqui o criptoanalista dispõe de pelo menos parte da mensagem cifrada;

   (2.2) *Mensagem básica conhecida*: aqui o criptoanalista conhece uma quantidade de mensagens básicas, todos eles enviados por **A**, e seus correspondentes mensagens cifrados;

   (2.3) *Mensagem básica escolhida*: aqui o criptoanalista conhece a função de cifragem da comunicação entre **A** e **B**.

Intuitivamente é claro que entre os três tipos de ataques passivos mencionados, o ataque (2.3) é o mais forte, isto é, o ataque com maior possibilidade dos três para quebrar o criptossistema; portanto se espera que um bom criptossistema seja difícil de ser quebrado para este tipo de ataque. Um criptoanalista que esteja nas condições (2.3), na maioria dos casos, se estaría enfrentando com um criptossistema que baseia sua segurança na dificuldade de resolver um problema matemático, computacionalmente inviável de abordar.

Um criptossistema que envolve a substituição sistemática de cada símbolo de seu alfabeto por outro qualquer, então podemos aplicar o ataque chamado de *análise de freqüências* que é um ataque do tipo (2.1). Por exemplo, se o alfabeto do criptossistema são os elementos do alfabeto de uma língua, para aplicar este ataque se calcula a freqüência média com que cada letra aparece no texto; esta freqüência tende a ser constante para textos com o mesmo número de letras.

A língua portuguessa tem as seguintes propriedades [9]:

- um monossílabo tem uma única letra a qual é necessáriamente uma vogal;
- as vogais são mais freqüentes que as consoantes;
- a vogal "a"é a mais freqüente;
- consoantes como o S e o M são mais freqüentes que as outras.

No entanto, este tipo de ataque só funciona para mensagens suficientemente longas, pois é possível construir uma mensagem curta cuja contagem de freqüências seja diferente da média geral. A distribuição de freqüências das letras do alfabeto em inglês pode ser encontrada em [29, p. 247]. Assim, apenas contando a freqüência de cada símbolo no texto cifrado, podemos descobrir qual letra correspondem aos símbolos mais freqüentes.

Um ataque do tipo (2.2) se mostra no Exemplo (1.4). Entre os ataques do tipo (2.3) estão aqueles chamados de *força bruta* onde o criptoanalista conhece o espaço de chaves e trata de obter a mensagem original aplicando em forma exaustiva todas as possíveis funções de decifrado à mensagem cifrada.

1.2 Criptografia de Chave Privada

Aqui manteremos a notação da Seção (1.1). Um criptossistema de chave privada é aquele onde para cada chave $k \in \mathcal{K}$, pode-se calcular d_k a partir de ε_k ou vice-versa. O interessante de algumas classes de criptossistemas deste tipo é somente teórica, no entanto, seu estudo permite entender melhor os criptossistemas de chave pública [29, p. 25]. A classe dos criptossistemas mencionada, não tem garantia de segurança em uma comunicação, pois são fácilmente quebrados, por exemplo, em um computador comum se pode implementar algoritmos que quebram rapidamente estes criptossistemas. Exemplos de criptossistemas que pertencem à classe mencionada acima são o *de César* (Exemplo 1.1), o *Vigenère* (Exemplo 1.2) e o criptossistema de *Hill* (Exemplo 1.3).

Para os exemplos a seguir, nosso alfabeto de entrada $\mathcal{A}$ será o inglês que tem 26 elementos. Identificamos este com o grupo finito $\mathbb{Z}/26\mathbb{Z}$ via a bijeção $\phi : \mathcal{A} \longrightarrow \mathbb{Z}/26\mathbb{Z}$ tal que $\phi(\mathrm{A}) = 0, \phi(\mathrm{B}) = 1, \cdots, \phi(\mathrm{Z}) = 25$. Aqui, ϕ é chamada uma *codificação* de $\mathcal{A}$, isto é, uma correspondência bijetiva que permite operar os elementos de $\mathcal{A}$ como elementos do grupo $\mathbb{Z}/26\mathbb{Z}$.

Exemplo 1.1. (Criptossistema de César) Seja $\mathcal{M} = \mathcal{C} = \mathcal{K} = \mathbb{Z}/26\mathbb{Z}$. Para cada $k \in \mathcal{K}$ definamos a função de cifragem $\varepsilon_k : \mathcal{M} \longrightarrow \mathcal{C}$, $x \mapsto x + k$ (aqui $+$ é a operação de soma no grupo $\mathbb{Z}/26\mathbb{Z}$). Logo, a função de decifragem será $d_k(y) = y - k$.

O nome deste criptossistema é devido a que o caso $k = 3$ foi usado pelo Imperador Romano Júlio César (45 A.C.) para comunicar-se com os generais do seu exército nas lutas (ele não confiava em seus mensageiros!) [17].

Exemplo 1.2. No século XVI, o exemplo anterior foi melhorado pelo criptografador francês Blaise Vigenère. Sua idéia consistiu em fixar uma palavra (seqüência finita de elementos do alfabeto de entrada) e aplicar, em base a esta, o criptossistema de César a cada elemento de $\mathcal{M}$; esta palavra será um elemento de $\mathcal{K}$. Neste criptossistema, para um inteiro $s \geq 2$ fixado, temos:

$$\mathcal{M} = \mathcal{C} = \mathbb{Z}/26\mathbb{Z}\,, \qquad \mathcal{K} = (\mathbb{Z}/26\mathbb{Z})^s\,.$$

Enviaremos mensagens formadas por cadeias finitas de elementos do alfabeto de entrada, digamos do tipo $(m_1, \ldots, m_\ell)$, que serão cifrados em mensagens similares como $(c_1, \ldots, c_\ell)$ (note que cada $m_i, c_i \in \mathcal{M} = \mathcal{C}$).

Agora, para cada $k = (k_1, \ldots, k_s) \in \mathcal{K}$, as funções de cifragem e decifragem estão definidas por $\varepsilon_k : \mathcal{M} \longrightarrow \mathcal{C}$, $\varepsilon_k(m_i) := m_i + k_{i \pmod s}$ e $d_k : \mathcal{C} \longrightarrow \mathcal{M}$, $d_k(c_i) = c_i - k_{i \pmod s}$, respectivamente. Observamos que s representa o número de caracteres da chave.

Para um exemplo numérico, tomemos $s = 6$. Queremos enviar a seguinte mensagem $(2, 17, 8, 15, 19, 14, 6, 17, 0, 5, 8, 0)$ (que significa CRIPTOGRAFIA de acordo a nossa codificação), utilizando a chave $(0, 11, 14, 13, 18, 14)$ (que significa ALONSO). Logo a mensagem cifrada será $(2, 2, 22, 2, 11, 2, 6, 2, 14, 18, 0, 14)$ (que representada no alfabeto inglês seria CCWCLCGCOSAO).

Observemos agora que no criptossistema de César uma letra da mensagem cifrada não pode corresponder a diferentes letras da respectiva mensagem enviada; no entanto, isto pode acontecer no criptossistema de Vigenère como se pode ver no exemplo acima. Note que isto não significa que a função de cifragem ε_k não seja injetiva, pois o decifragem é feita tendo presente a posição de cada letra. Para este criptossistema é possível um ataque de análise de freqüências por blocos de tamanho s, veja [29, p. 248].

Exemplo 1.3. (Criptossistema de Hill) Os criptossistemas nos exemplos anteriores só foram melhorados depois de muito tempo. De fato, em 1931 Lester S. Hill introduziu os chamados criptossistemas *lineares* ou *matriciais* [15]; os nomes se devem as correspondentes funções de

cifragem que representam automorfismos do grupo $(\mathbb{Z}/26\mathbb{Z})^s$, onde $s \geq 1$ é um inteiro fixo. Estes criptossistemas resultariam mais resistentes aos ataques por força bruta e análise de freqüências. Para descreve-os, sejam

$$\mathcal{M} = \mathcal{C} := (\mathbb{Z}/26\mathbb{Z})^s\,, \qquad \mathcal{K} := \{GL_s(\mathbb{Z}/26\mathbb{Z})\}\,.$$

Observe que $K \in \mathcal{K}$ se e somente se $\det(K)$ é uma unidade em $\mathbb{Z}/26\mathbb{Z}$. Os elementos de $\mathcal{M} = \mathcal{C}$ serão vistos como vetores de tamanho $1 \times s$. Logo, para cada $K \in \mathcal{K}$ a função de cifragem $\varepsilon_K : \mathcal{M} \to \mathcal{C}$ é dada por $\varepsilon(m) := m \cdot K$, e conseqüentemente a função de decifragem $d_K(c) : \mathcal{C} \to \mathcal{M}$ dada por $d_K(c) = c \cdot K^{-1}$. Para um exemplo numérico, tomemos $s = 2$. Queremos enviar a mensagem $\mathbf{m} := (0, 12, 14, 17)$ (que significa, de acordo a nossa codificação, AMOR). Para cifrar utilizaremos a chave

$$K = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix}.$$

A matriz inversa de K é a matriz com linhas $(25, 3)$ e $(2, 21)$. Como os elementos de $\mathcal{M}$ (mensagens básicas) são vetores 1×2, primeiro devemos decidir como particionar em blocos (de 1×2) a mensagem a ser enviada. Usualmente esta partição se faz da esquerda para direita. Assim, particionamos $\mathbf{m}$ em $\mathbf{m_1} := (0, 12)$ e $\mathbf{m_2} := (14, 17)$. Logo a mensagem cifrada será $(\mathbf{m_1}K, \mathbf{m_2}K) = (24, 12, 0, 7)$ (que, usando o alfabeto inglês, representa YMAH).

Se o comprimento ℓ de uma mensagem a cifrar $\mathbf{m} = (a_1, \ldots, a_\ell)$ não é múltiplo do comprimento s das mensagens básicas, então a mensagem a cifrar será $\mathbf{m} := (\mathbf{m}, a, \ldots, a) = (a_1, \ldots, a_\ell, a, \ldots, a)$. Aqui o símbolo a é um elemento previamente fixado do alfabeto de entrada, e a quantidade de a's é o mínimo possível tal que o comprimento de $\mathbf{m}$ seja múltiplo de s.

A seguir, mostramos um ataque do tipo (2.2) ao criptossistema de Hill.

Exemplo 1.4. No exemplo anterior tomemos $s = 3$; suponhamos conhecido as mensagens básicas $\mathbf{m_1} = (18, 14, 11) = SOL$, $\mathbf{m_2} = (8, 1, 12) = IBM$, $\mathbf{m_3} = (15, 0, 25) = PAZ$, assim como seus correspondentes cifrados $\mathbf{c_1} = (23, 20, 22) = XUW$, $\mathbf{c_2} = (17, 21, 17) = RVR$ e $\mathbf{c_3} = (3, 0, 15) = DAP$.

Então o criptoanalista pode achar a chave $K = (k_{ij})$ do criptossistema mediante a resolução de sistemas lineares de equações. De fato, de $\mathbf{m_i}K = \mathbf{c_i}$, $i = 1, 2, 3$ temos 3 sistemas de equações lineares com variáveis k_{1j}, k_{2j}, k_{3j} $(j = 1, 2, 3)$. Se pode ver que a chave que está

sendo usada para cifrar mensagens é:

$$K = \begin{pmatrix} 2 & 8 & 15 \\ 15 & 25 & 3 \\ 1 & 16 & 2 \end{pmatrix}$$

Este ataque é do tipo passivo (2.2) e é fácil implementar um algoritmo para executa-o.

Exemplo 1.5. (Criptossistema DES) O criptossistema *Data Encryption Standard* (DES) foi desenvolvido na década do 70 pelo National Bureau of Standards e o IBM. As chaves deste criptossistema são cadeias de 56 bits de comprimento e portanto para um criptoanalista tentar quebrar o criptossistema usando o ataque por força bruta, deverá analisar 2^{56} possibilidades (chaves); estes cálculos podem ser viáveis mediante o uso dos computadores atuais. Em meados de Julho de 1998, a empresa *Electronic Frontier Foundation* (EFF) mostrou um ataque ao DES o qual decifra mensagens em menos de três dias. Apesar disto, este criptossistema ainda continua sendo usado em transações bancárias. Para um tratamento mais detalhado deste criptossistema ver [29, p. 250], [40, p. 70].

Outros criptossistemas de chave privada que ainda se utilizam são: FEAL, IDEA, AES; ver [40], [29], [26]. Finalmente, citamos três desvantagens ao utilizar um criptossistema de chave privada.

(A) *A distribuição de chaves*: Se dois usuários desejam estabelecer uma comunicação, eles necessitam conhecer a priori uma chave do criptossistema; isto nem sempre é possível devido à insegurança da linha de comunicação.

(B) *A manipulação de chaves*: Em uma comunicação de n usuários, que se faz dois a dois, cada um deles tem que manipular $n(n-1)/2$ chaves, o qual não é pratico para um usuário.

(C) *A falta de assinatura digital*: Em uma comunicação usando este tipo de criptografia, não necessáriamente é possível ter certeza da procedência das mensagens cifradas.

1.3 Criptografia de Chave Pública

Nesta dissertação, por um cálculo *computacionalmente fácil* e *computacionalmente difícil* entenderemos como um cálculo que é realizado por um algoritmo de tempo polinomial ou respectivamente por um algoritmo de tempo exponencial (ver Apêndice B).

Com o objetivo de dar uma maior liberdade na hora de estabelecer uma comunicação segura e de cobrir as deficiências da criptografia de chave privada mencionadas em (A), (B), (C) da seção anterior, em 1976 nasce a *criptografia de chave pública* através de um trabalho fundamental de Diffie e Hellman [10]. Neste trabalho encontramos a descrição do primeiro sistema que permite a dois usuários compartilhar um segredo em comum, usando uma linha de comunicação que se supõe insegura; este é chamado de *Troca de Chaves Diffie-Hellman.* Uma característica relevante deste sistema está em que sua segurança depende da existência de funções *unidirecionais e unidirecionais com segredo* as quais serão definidas posteriormente. A saber, estas funções estão relacionadas com problemas matemáticos computacionalmente difíceis de resolver.

Uma das principais aplicações dos criptossistemas de chave pública foram em sistemas de comunicação electrônica, especialmente em redes de comunicação telefônica. Outra aplicação é com respeito a autenticação de mensagens, o que nos permite obter uma *firma digital* a partir da mensagem e assim garantir sua autenticidade (ver [29, p. 425]).

Com a notação de (1.1), definimos um criptossistema de chave pública como aquele onde conhecida a função de cifragem ε_k, é computacionalmente difícil achar a função de decifragem d_k. Para estes criptossistemas temos $k = (k_1, k_2) \in \mathcal{K}$ onde k_1 se utiliza para cifrar (*chave pública*) e k_2 para decifrar (*chave privada*) ou vice-versa. Assim, uma diferença notável entre a criptografia de chave privada e a criptografia de chave pública está no uso das chaves; além disso a chave para cifrar de cada usuário no criptossistema de chave pública é conhecida por qualquer usuário, o que não pode acontecer na criptografia de chave privada, pois como foi mencionado anteriormente, estes criptossistemas de chave privada conhecida uma das chaves pode ser encontrada a outra chave facilmente, implicando que qualquer pessoa poderia lê as mensagens cifradas. No que segui, introduzimos os conceitos de funções unidirecionais e unidirecionais com segredo.

Seja $f : X \to Y$ uma função entre dois conjuntos X e Y, f é dita *unidirecional* (*one-way-function*) se as seguintes condições são satisfeitas:

(1) Para todo $x \in X$, $f(x)$ é computacionalmente fácil de calcular;

(2) Para cada $y \in \mathrm{Im}(f)$, achar x tal que $f(x) = y$, é computacionalmente difícil de calcular.

Agora suponha que f é uma função unidirecional, f é dita *unidirecional com segredo* (*trapdoor-one-way-function*) se além das propriedades (1) e (2) acima ela satisfaz:

(3) O cálculo em (2) passa a ser computacionalmente fácil sempre que se conheça alguma informação adicional. A informação adicional é chamada *o segredo* (*trapdoor*) de f.

Em geral, é difícil determinar quando uma função dada satisfaz a propriedade (3) acima; isto se deve a que esta depende dos conceitos "computacionalmente fácil"e "computacionalmente difícil"que a sua vez estão ligados com o problema $NP = P$ da Teoria da Complexidade [30, p. 220], o qual ainda é um problema em aberto. Em particular, a existência de funções unidirecionais e respectivamente unidirecionais com segredo não está garantida. A seguir, damos três possíveis exemplos de funções unidericionais, ver [29, p. 115].

Exemplo 1.6. Fixemos p, q dois primos grandes (aproximadamente de 200 a 400 algarismos).

(1) **Exponencial módulo p.** Seja p um primo, α um gerador de $\mathbb{F}_p^*$, $X = Y = \mathbb{F}_p^*$ e $f : X \to Y$ dada por $f(x) = \alpha^x$. Esta f satisfaz a primeira propriedade para ser unidirecional, pois o cálculo de $f(x)$ é obtido em tempo polinomial. Ao respeito da segunda propriedade, dado y tentar calcular x tal que $y = \alpha^x$ é conhecido como o *Problema do Logaritmo Discreto* (PLD) sobre $\mathbb{F}_p^*$, veja Definição (2.1).

(2) **Fatoração inteira.** Seja $n := pq$, onde p, q são dois primos diferentes (não conhecidos) e $m \geq 1$ um inteiro co-primo com $(p-1)(q-1)$. Consideremos $X = Y = (\mathbb{Z}/n\mathbb{Z})^*$ e $f : X \to Y$ definida por $f(x) = x^m$. Aqui novamente o cálculo de $f(x)$ se faz em tempo polinomial. Dado $y \in Y$ tentar calcular x tal que $y = x^m$ (sem conhecer os valores de p e q) é equivalente ao problema da fatoração de inteiros grandes [6], [29, p. 89], [40, p. 150].

(3) **Função Rabin.** Sejam p e q primos diferentes e ambos congruentes a 3 módulo 4. Seja $n := pq$ e $X = Y$ igual ao conjunto de quadrados de $(\mathbb{Z}/n\mathbb{Z})^*$. Definamos $f : X \to Y$ por $f(x) = x^2$. As condições sobre p e q garante a injetividade de f, e o cálculo de x tal que $y = f(x)$ (para y dado) é o problema de calcular raízes quadráticas módulo n. [29, p. 115].

Exemplo 1.7. O item (2) do exemplo acima sería uma função unidirecional com segredo, pois uma informação adicional para que está satisfaça a condição (3) de função unidirecional com segredo seria que p e q fossem conhecidos.

CAPÍTULO 2

Criptossistemas Públicos Básicos

Neste capítulo estudamos o sistema de troca de chaves Diffie-Hellman e os primeiros criptossistemas de chave pública mais relevantes tais como **RSA** e **ElGamal**, assim como os problemas matemáticos nos quais estes criptossistemas baseiam sua seguraça. Mostramos um exemplo de cada um só para ilustrar sua aplicação, pois os dados com os quais trabalhamos não estão dentro dos parâmetros exigidos públicamente para garantir um nível de segurança específico, por exemplo, o tamanho dos parâmetros que definem as funções unidirecionais com segredo para implementar o criptossistema deveriam estar entre 200 e 400.

2.1 Diffie-Hellman

Como já foi mencionado na Seção (1.3), a criptografia de chave pública nasceu no primeiro artigo publicado por Whitfield Diffie e Martin Hellman [10] em 1976. Em este artigo, Diffie e Hellamn propuseram um sistema para trocas de chaves criptográficas entre dois usuários sobre uma linha de comunicação insegura, no entanto este não é um método para cifrar mensagens.

Para dois usuários **A** e **B** que desejam ter uma chave em comum, eles devem de escolher um número primo p e um elemento α, gerador de $(\mathbb{Z}/p\mathbb{Z})^*$, que serão parâmetros públicos. A seguir, os passos que cada usuário deve fazer para compartilhar o segredo.

- **A** escolhe um número aleatório x entre 1 e $p-2$ e envia a **B** o valor de $\alpha^x \pmod{p}$.

- B escolhe um número aleatório y, análogamente ao passo anterior, e envia a A o valor $\alpha^y \pmod p$.
- B calcula $\mathrm{k} = (\alpha^x)^y \pmod p$.
- A calcula $\mathrm{k} = (\alpha^y)^x \pmod p$.

Ao final, os usuários A e B compartilham o segredo k. Este processo é chamado *troca de chaves Diffie-Hellman.*

Problema Diffie-Hellman (DHP) O problema que se enfrenta um atacante interessado em saber o segredo que os usuários A e B compartilham, está relacionado com o *Problema do Logaritmo Discreto* (DLP) sobre um grupo G, que definimos a seguir:

Definição 2.1. Dados $\alpha, \beta \in G$, achar $x \in \mathbb{Z}$, se existe, tal que $\alpha^x = \beta$.

Para o sistema de troca de chaves de Diffie-Hellman o análogo a este problema podemos enunciar assim:

Definição 2.2. Dados um primo p, um gerador α de $(\mathbb{Z}/p\mathbb{Z})^*$ e os valores $\alpha^a \pmod p$, $\alpha^b \pmod p$ achar o valor de $\alpha^{ab} \pmod p$, é o que chamamos *Problema Diffie-Hellman* (DHP).

Observamos que se o DLP tivesse solução, então dados os valores p, α, α^a e α^b podemos achar o valor de a e assim calcular o valor α^{ab}, o que implicaria ter solução ao DHP. A recíproca nem sempre é verdadeira, ver [29, p. 113].

2.2 RSA

Este criptossistema foi criado por Ronald Rivest, Adi Shamir e Leonard Adleman (1978). O criptossistema pode ser usado para cifrar e assinar mensagens [29, p. 433], [29, p. 204]. O **RSA** baseia sua segurança na dificuldade de fatorar inteiros grandes. A seguir, os passos que dois usuários A e B (representados pela letra U) devem fazer para estabelecer uma comunicação usando o criptossistema **RSA**.

(1) O usuário U escolhe dois números primos p e q (se recomenda que estes números tenham entre 200 e 400 algarismos) e calcula $n_{\mathrm{U}} = pq$. Logo, o grupo a ser usado pelo usuário U será $(\mathbb{Z}/n_{\mathrm{U}}\mathbb{Z})^*$. A ordem do grupo é calculada usando a função ϕ de *Euler* $\phi(n_{\mathrm{U}}) = \phi(p \cdot q) = \phi(p) \cdot \phi(q) = (p-1)(q-1)$. É claro que o usuário U não tem problema de calcular a ordem do grupo, pois conhece os valores de p e q.

(2) Depois, $\mathbf{U}$ escolhe um inteiro $r_{\mathbf{U}}$ tal que $1 < r_{\mathbf{U}} < \phi(n_{\mathbf{U}})$ seja relativamente primo com a ordem do grupo.

(3) Usando o algoritmo estendido de Euclides, calculamos o inverso de $r_{\mathbf{U}}$, que chamaremos de $s_{\mathbf{U}}$; daí temos que $r_{\mathbf{U}} \cdot s_{\mathbf{U}} \equiv 1 \pmod{\phi(n_{\mathbf{U}})}$ com $1 < s_{\mathbf{U}} < \phi(n_{\mathbf{U}})$.

(4) A chave pública do usuário $\mathbf{U}$ será o par $(n_{\mathbf{U}}, r_{\mathbf{U}})$, enquanto sua chave privada será o número s_U; é claro que também devem de permanecer ocultos os números p, q e $\phi(n_{\mathbf{U}})$ por segurança do criptossistema.

Para o usuário $\mathbf{A}$ enviar uma mensagem ao usuário $\mathbf{B}$, usa a chave pública $(n_{\mathbf{B}}, r_{\mathbf{B}})$ de $\mathbf{B}$, e para cada mensagem básica $\mathbf{m} \in \mathcal{M} = \mathcal{C} = (\mathbb{Z}/n_{\mathbf{B}}\mathbb{Z})^*$ aplica a função de cifragem $\varepsilon_{\mathbf{B}}(\mathbf{m}) = \mathbf{m}^{r_{\mathbf{B}}} \equiv \mathbf{c} \pmod{n_{\mathbf{B}}}$ e envia para $\mathbf{B}$. Para o usuário $\mathbf{B}$ obter a mensagem original aplica sua função de decifragem $d_{\mathbf{B}}(\mathbf{c}) = \mathbf{c}^{s_{\mathbf{B}}} \equiv (\mathbf{m}^{r_{\mathbf{B}}})^{s_{\mathbf{B}}} \equiv \mathbf{m}^{r_{\mathbf{B}} s_{\mathbf{B}}} \equiv \mathbf{m} \pmod{n_{\mathbf{B}}}$. O espaço de chaves é o conjunto $\mathcal{K} = \{(r_{\mathbf{B}}, s_{\mathbf{B}}) \in \mathbb{Z} \times \mathbb{Z} \mid 1 < r_{\mathbf{B}} < \phi(n_{\mathbf{B}}), \text{mdc}(r_{\mathbf{B}}, \phi(n_{\mathbf{B}})) = 1 \text{ e } r_{\mathbf{B}} s_{\mathbf{B}} \equiv 1 \pmod{\phi(n_{\mathbf{B}})}\}$. Nem todo elemento de $\mathcal{K}$ serve para usar como chave em um criptossistema, pois existem ataques eficientes dependendo da escolha dos parâmetros p, q e $r_{\mathbf{B}}$.

Exemplo 2.3. Tomemos o alfabeto inglês codificado como nos exemplos dados no capítulo anterior de criptossistemas de chave privada sendo o alfabeto de entrada. O usuário $\mathbf{A}$ deseja enviar a mensagem $\mathbf{m} = \mathbf{NOTA}$ para o usuário $\mathbf{B}$, para isso, vejamos como o usuário $\mathbf{B}$ escolhe sua chave pública e privada.

O usuário $\mathbf{B}$ escolhe dois números primos $p_{\mathbf{B}} = 73$ e $q_{\mathbf{B}} = 89$, calcula $n_{\mathbf{B}} = 73 \cdot 89 = 6497$ e considera o grupo $(\mathbb{Z}/6497\mathbb{Z})^*$. A ordem do grupo é $\phi(6497) = 72 \cdot 88 = 6336$. Suponhamos que $\mathbf{B}$ escolhe o número $r_{\mathbf{B}} = 299$ e prova que $\text{mdc}(299, 6336) = 1$. Acha o inverso de $r_{\mathbf{B}}$ módulo 6336, logo $s_{\mathbf{B}} = 5891$. Portanto, a chave pública de $\mathbf{B}$ será $(n_{\mathbf{B}}, r_{\mathbf{B}}) = (6497, 299)$, deixando em secreto os outros valores.

Para enviar a mensagem a $\mathbf{B}$ devemos determinar o comprimento[1] dos blocos em que será dividido a mensagem original, de tal forma que sejam elementos de $\mathcal{M}$, para isto, devemos ter em conta que as mensagens básicas devem ser elementos do grupo $(\mathbb{Z}/6497\mathbb{Z})^*$, então o comprimento destes não deve ser maior a $n_B = 6497$. Assim, como $26^2 = 676 < n_B < 17576 = 26^3$, então a mensagem básica deverá ter no máximo **duas** letras. Para enviar mensagens maiores se divide em blocos de duas letras (completando o último bloco com

[1]por exemplo, o comprimento da palavra PAZ no alfabeto inglês é $P \times 26^2 + A \times 26 + Z = 15 \times 26^2 + 0 \times 26 + 25 = 686$.

símbolos previamente estabelecidos, no caso quando o comprimento da mensagem original não fosse um múltiplo do comprimento das mensagens básicas). Na prática o comprimento das mensagens básicas é maior, pois a ordem do grupo também é maior. Primeiro codificamos cada bloco de tal forma que seja um elemento de $\mathcal{M}$.

$$NO = N \cdot 26 + O = 13 \cdot 26 + 14 = 352 = m_1 \; TA = T \cdot 26 + A = 19 \cdot 26 + 0 = 494 = m_2.$$

Ciframos $m_1, m_2 \in \mathcal{M} = (\mathbb{Z}/6497\mathbb{Z})^*$ com a chave pública de $\mathbf{B}$.

$$c_1 \equiv m_1^{r_\mathbf{B}} \pmod{n_\mathbf{B}} \equiv 5324 \pmod{6497}, c_2 \equiv m_2^{r_\mathbf{B}} \pmod{n_\mathbf{B}} \equiv 335 \pmod{6497}.$$

Decodificamos a mensagem cifrada

$$c_1 = 5324 = 7 \cdot 26^2 + 22 \cdot 26 + 20 = HWU \; c_2 = 335 = 0 \cdot 26^2 + 12 \cdot 26 + 23 = AMX.$$

Portanto, a mensagem a enviar para $\mathbf{B}$ é (HWU, AMX). Para que $\mathbf{B}$ possa recuperar a mensagem, primeiro codifica os dados recebidos.

$$HWU = 5324 = c_1 \; AMX = 335 = c_2 \; .$$

Agora, recupera a mensagem calculando,

$$m_1 \equiv c_1^{s_\mathbf{B}} \pmod{n_\mathbf{B}} \equiv 5324^{5891} \pmod{6497} \equiv 352 \pmod{6497} \text{ e}$$

$$m_2 \equiv c_2^{s_\mathbf{B}} \pmod{n_\mathbf{B}} \equiv 335^{5891} \pmod{6497} \equiv 494 \pmod{6497}.$$

Logo, o usuário $\mathbf{B}$ decodifica m_1 e m_2 para obter o mensagem original,

$$m_1 = 352 = 13 \cdot 26 + 14 = NO \; m_2 = 494 = 19 \cdot 26 + 0 = TA \; .$$

A tarefa a fazer de um criptoanalista é recuperar a mensagem $\mathbf{m}$ correspondente ao texto cifrado $\mathbf{c}$, tendo uma informação pública (n, r) do destinátario $\mathbf{B}$, é o que se chama o problema RSA. Uma possível forma que o criptoanalista usaria para resolver o problema RSA, seria fatorando n, pois assim poderia calcular $\phi(n)$ e s. Como s é obtido, o criptoanalista pode decifrar a mensagem enviada pelo usuário $\mathbf{A}$. Em caso contrário, se o criptoanalista de alguma forma consegui calcular s, então poderia também fatorar n como segui. Notemos que $rs \equiv 1 \pmod{\phi(n)}$, então existe $k \in \mathbb{Z}$ tal que $rs - 1 = k\phi(n)$. Logo, pelo Teorema de Euler[2] temos que $a^{rs-1} \equiv 1 \pmod{n}$ para todo $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Seja $rs - 1 = 2^u t$, onde t é um inteiro ímpar; então existe $i \in [1, u]$ tal que $a^{2^{i-1}t} \not\equiv \pm 1 \pmod{n}$ e $a^{2^i t} \equiv 1 \pmod{n}$. Se

[2]Se $a \in (\mathbb{Z}/n\mathbb{Z})^*$ então $a^{\phi(n)} \equiv 1 \pmod{n}$.

a, i satisfazem a condição anterior, então o $\mathrm{mdc}(a^{2^{i-1}t} - 1, n)$ é um fator não trivial de n, ver [29, p. 287].

Do feito acima, podemos concluir que o problema RSA e o problema de fatorar n são computacionalmente equivalentes. Ao construir este criptossistema devemos evitar um tipo de chaves $k \in \mathcal{K}$, tal que ao aplicar a função de cifragem a mensagem não muda, isto é, $\varepsilon(\mathbf{m}) = \mathbf{m}$. Este tipo de chaves são chamadas de *chaves fracas*. Sempre há alguma mensagem para as quais acontece isto, seja qual for o valor de n. O objetivo é reduzir ao mínimo o número deste tipo de chaves. Temos para $n = p \cdot q$ e r o expoente para cifrar que:

$$\sigma_n = [1 + \mathrm{mdc}(r - 1, p - 1)] \cdot [1 + \mathrm{mdc}(r - 1, q - 1)]$$

representa o número de valores de $\mathbf{m} \in \mathcal{M}$ que não mudam ao ser cifrados. Como $r - 1$, $p - 1$, $q - 1$ são números pares, então no mínimo $\sigma_n = 9$ [29, p. 290].

2.3 ElGamal

Este criptossistema foi criado inicialmente para produzir assinaturas digitais, mas depois se estendeu para cifrar mensagens. O criptossistema ElGamal propõe um esquema de chave pública baseado no problema do logaritmo discreto sobre um grupo (finito e cíclico) G fixado; ver Definição (2.1). Suponha que o usuário **A** deseja enviar uma mensagem $\mathbf{m}$ ao usuário **B**, usando este criptossistema; logo **A** tem que fazer o seguinte:

- Obter os parâmetros públicos de **B**, a saber, (p, α, α^b) onde p é um número primo grande e α um gerador do grupo multiplicativo $G = (\mathbb{Z}/p\mathbb{Z})^*$ dos inteiros módulo p;
- Escolher aleatóriamente um inteiro k tal que $1 \leq k \leq p - 2$;
- Representar as mensagens $\mathbf{m}$ como inteiros entre $\{0, 1, \ldots, p - 1\}$;
- Calcular $\gamma = \alpha^k \pmod{p}$ e $\delta = \mathbf{m}(\alpha^b)^k \pmod{p}$;
- Enviar o texto cifrado $\mathbf{c} = (\gamma, \delta)$ para **B**. Agora, para o usuário **B** recuperar a mensagem,
- Usa sua chave privada para calcular $\gamma^{p-1-b} = \alpha^{-kb} \pmod{p}$;
- Obtêm a mensagem $\mathbf{m}$ calculando $\gamma^{p-1-b}\delta \pmod{p}$.

Os grupos mais usados no criptossistema ElGamal são os grupos multiplicativos de corpos finitos.

Exemplo 2.4. Considere o primo $p = 15485863$, $G = (\mathbb{Z}/15485863\mathbb{Z})^*$ e um gerador $\alpha = 7$. O usuário **B** escolhe o inteiro $b = 21702$ e calcula $\alpha^b = 7^{21702} \equiv 8890431 \pmod{15485863}$, que são suas respectivas chave privada e pública. Suponhamos que o usuário **A** deseja enviar a **B** a mensagem $\mathbf{m} = JOSE$. Então, para isto se escolhe uma codificação do alfabeto usando o mesmo análise feito para o exemplo do criptossistema RSA.

$$\mathbf{m} = JOSE = 9 \cdot 26^3 + 14 \cdot 26^2 + 18 \cdot 26 + 4 = 168120$$

O usuário **A** escolhe o inteiro $k = 480$ e calcula

$$(\gamma^k) = 7^{480} \equiv 12001315 \pmod{15485863} \text{ e,}$$

$$\delta = \mathbf{m}(\alpha^b)^k \pmod{15485863} \equiv 168120 \cdot 9846598 \equiv 2272786 \pmod{15485863}.$$

Depois decodifica a mensagem cifrada:

$$\gamma = 12001315 = 1 \cdot 26^5 + 0 \cdot 26^4 + 6 \cdot 26^3 + 21 \cdot 26^2 + 11 \cdot 26 + 1 = BAGVLB,$$

$$\delta = 2272786 = 4 \cdot 26^4 + 25 \cdot 26^3 + 8 \cdot 26^2 + 2 \cdot 26 + 22 = EZICW.$$

Portanto a mensagem a enviar a **B** é (BAGVLB,EZICW). Vejamos como o usuário **B** recupera a mensagem. Primeiro **B** codifica a mensagem cifrada recebida; então $BAGVLB = 12001315 = \alpha^a$ e $EZICW = 2272786 = \mathbf{m} \cdot \alpha^{ab}$. Depois calcula:

$$\gamma^{p-1-b} = 12001315^{15464160} \equiv 14823281 \pmod{15485863}.$$

Finalmente,

$$\mathbf{m} = \gamma^{p-1-b} \cdot \delta \equiv 168120 \pmod{15485863},$$

assim,

$$\mathbf{m} = 168120 = 9 \cdot 26^3 + 14 \cdot 26^2 + 18 \cdot 26 + 4 = JOSE.$$

2.3.1 Ataque ao Problema do Logaritmo Discreto

A seguir descreveremos um ataque para resolver o problema do logaritmo discreto chamado de *index-calculus*. Este é um ataque do tipo (2.3), ver Seção (1.1) e seu fundamento é similar ao método de fatorar números inteiros chamado *Base Fator* ver [20, p.148]. A seguir

descreveremos este ataque para um grupo G em geral. Seja $G =< g >$ o grupo base, $\#(G) = n$ e $B = \{P_1, \ldots, P_r\} \subseteq G$ a base fator. O ataque está dividido em três passos, nos passos (1) e (2) se quer achar o logaritmo discreto de cada elemento da base fator em base g. Por último, usando a informação obtida construímos um sistema equações onde os elementos da base fator apareçam, relacionando o elemento a achar o logaritmo discreto. Assim,

(1) Se procuram igualdades do tipo

$$\prod_{i=1}^{r} P_i^{a_i} = g^t \, t \in \mathbb{Z},$$

ou equivalentemente

$$\sum_{i=1}^{r} a_i \mathrm{ind}_g(P_i) \equiv t \pmod{n}, \tag{2.1}$$

onde $\mathrm{ind}_g(x) = s$ se $x = g^s$.

(2) Uma vez obtidas suficientes equações da forma (2.1) se calculam os $\mathrm{ind}_g(P_i)$.

(3) Dado $a \in G$ calcular o $\mathrm{ind}_g(a)$ é o mesmo que resolver o problema do logaritmo discreto. Se procurão equações da forma

$$\prod_{i=1}^{r} P_i^{\alpha_i} = a g^{\alpha},$$

onde $\alpha \in \mathbb{Z}$; pelo item (2) temos que $\mathrm{ind}_g(a) = \sum_{i=1}^{r} \mathrm{ind}_g(P_i) - \alpha$.

Observação 2.5. A eficiência do método está em achar o conjunto B para que existam as equações do tipo (2.1).

Exemplo 2.6. Seja $G = \mathbb{F}_{19}^*$ e $g = 3$ um gerador do grupo. Temos que $\#(\mathbb{F}_{19}^*) = 18$ e escolhamos $B = \{2, 3, 5\}$. Claramente $\mathrm{ind}_3(3) = 1$; para achar os logaritmos dos outros elementos da base, definimos relações do tipo (2.1) e as resolvemos. Logo,

$$5 \equiv 3^4 \pmod{19} \Rightarrow \mathrm{ind}_3(5) = 4 \pmod{18},$$

$$2^2 \cdot 5 \equiv 3^{18} \pmod{19} \Rightarrow 2\mathrm{ind}_3(2) + \mathrm{ind}_3(5) \equiv 0 \pmod{18} \Rightarrow \mathrm{ind}_3(2) = 7 \pmod{18}$$

Suponhamos que queremos achar o logaritmo discreto de $a = 11$ no grupo G. Então,

$$11 \equiv 2 \cdot 3 \cdot 5 \pmod{19} \text{ logo}$$

$$\mathrm{ind}_3(11) = \mathrm{ind}_3(2) + \mathrm{ind}_3(3) + \mathrm{ind}_3(5) \equiv 12 \pmod{18}.$$

Nos últimos anos tem-se achado algoritmos computacionais cada vez mais eficientes para resolver os problemas matemáticos nos quais estes criptossistemas de chave pública baseiam sua segurança, tendo colocado em dúvida a confiança depositada nestes, que alguns anos atrás eram uma coisa distante, mas devido ao avanço tecnológico isto se faz cada vez mais provável. Portanto, é indispensável a procura de novas estruturas matemáticas nas quais se possa implementar os criptossistemas para uma maior segurança. Para isso, nos seguintes capítulos foram consideradas estruturas relacionadas com o Jacobiano de curvas algébricas.

CAPÍTULO 3

Criptossistemas Elípticos

Neste capítulo apresentamos uma formalização matemática de curvas elípticas e mostramos algumas propriedades importantes destas que são usados para a escolha conveniente dos parâmetros que definem os criptossistemas elípticos. Com este capítulo queremos entrar em um contexto particular à utilização de *Curvas Algébricas* e a partir destas introduzir o Jacobiano de curvas algébricas para a implementação de criptossistemas de chave pública. O nome de curvas elípticas é devido a que elas foram utilizadas no passado para medir o perímetro de elipses e encontrar o comprimento das ôrbitas planetárias. Contudo, o nome não é conveniente, pois de fato estas curvas não são elipses.

Nos últimos anos, o estudo das curvas elípticas tem aumentado por suas diversas aplicações em diferentes áreas, como por exemplo, na Teoria dos Números e Ciências da Computação; além disso, propriedades destas curvas jogam um papel importante na demonstração do famoso **Último Teorema de Fermat**. Para mais detalhes sobre a teoria de curvas elípticas ver [4], [37], [38].

3.1 Noções da Teoria de Curvas Elípticas

Fixemos K um corpo de característica $p \geq 0$ e seja $\bar{K}$ seu fecho algébrico.

Definição 3.1. Uma curva elíptica $\mathbf{E}$ sobre K são os zeros no plano projetivo $\mathbf{P}^2(\bar{K})$ de um

polinômio da forma

$$F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3\,, \tag{3.1}$$

onde $a_1, a_2, a_3, a_4, a_6 \in K$,[1] são tais que

$$\Delta = \Delta(\mathbf{E}) := -b_1^2b_4 - 8b_2^3 - 27b_3^2 + 9b_1b_2b_3 \neq 0\,,$$

com

$$b_1 = a_1^2 + 4a_2 \quad b_2 = a_1a_3 + 2a_4\,,$$
$$b_3 = a_3^2 + 4a_6 \quad b_4 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2\,.$$

Temos que a curva $\mathbf{E}$ é não singular (veja Apêndice A) pois Δ (chamado o *discriminante* da curva) é diferente de zero. Observamos que a curva $\mathbf{E}$ intercepta à reta $Z = 0$ em um único ponto, a saber

$$\mathcal{O} := (0:1:0)\,.$$

Agora, consideramos as funções racionais $x := X/Z$ e $y := Y/Z$ restritas a $\mathbf{E}$. Logo de (3.1) podemos tomar a $\mathbf{E}$ como sendo simplesmente o ponto $\mathcal{O}$ e os zeros em $\bar{K} \times \bar{K}$ da equação afim:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,, \tag{3.2}$$

onde os a_i's são tomados como em (3.1). Se a característica p de K é diferente de 2, por médio de mudanças afines de coordenas podemos supor que $\mathbf{E}$ está descrita por

$$y^2 = x^3 + c_1x^2 + c_2x + c_3\,, \tag{3.3}$$

onde $c_1, c_2, c_3 \in K$ são tais que $\Delta = -4c_1^3c_3 - c_1^2c_2^2 - 16c_2^3 - 108c_3^2 + 72c_1c_2c_3 \neq 0$. Se mais ainda, $p \neq 3$ podemos reduzir a equação anterior a:

$$y^2 = x^3 + d_1x + d_2\,, \tag{3.4}$$

onde $d_1, d_2 \in K$ e $\Delta = -16(4d_1^3 + 27d_2^2) \neq 0$.

Pontos racionais Seja L um corpo tal que $K \subseteq L \subseteq \bar{K}$. O conjunto dos pontos racionais sobre L da curva $\mathbf{E}$, denotado por $\mathbf{E}(L)$, é o ponto $\mathcal{O}$ junto os pares $(x,y) \in L \times L$ que satisfazem a equação (3.2). Existe uma estrutura de grupo comutativo sobre $\mathbf{E}(L)$

[1] A explicação da enumeração destes elementos se encontra em [21, p. 118].

definida por uma operação binária $\oplus$, que pode ser descrita geometricamente da seguinte forma. Sejam $P, Q \in \mathbf{E}(K)$ e $L \subset \mathbf{P}^2(K)$ a reta que passa através destes dois pontos. Pelo *Teorema de Bezout* (veja [11, p. 112]) temos que esta reta intercepta a curva em outro ponto R (notemos que para $P = Q$, L é tangente em $\mathbf{E}(K)$). Seja L' a reta que une R e $\mathcal{O}$, logo o terceiro ponto que esta reta intercepta $\mathbf{E}(K)$ é $P \oplus Q$ (Veja Figura 3.1 e 3.2).

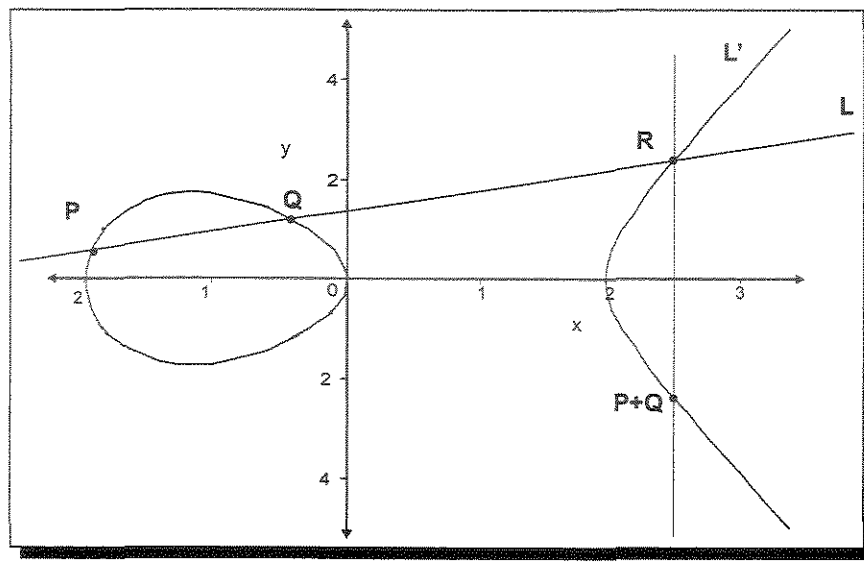


Figura 3.1: Curva Elíptica $\mathbf{E} : y^2 = x^3 - 4x$ Soma de P e Q

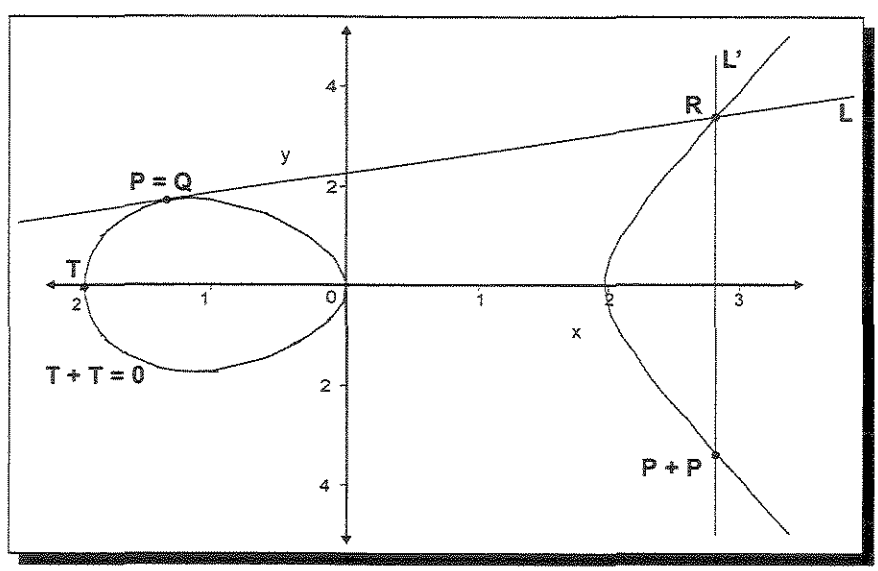


Figura 3.2: Duplicação dos pontos P e T

Usando a idéia geométrica da soma de pontos na curva elíptica, podemos escrever analiticamente as fórmulas para calcular está, da seguinte forma: O elemento identidade vai estar dado por $\mathcal{O}$ e dados $P = (a, b), Q = (c, d) \in \mathbf{E}(L)$ temos que $-P := (a, -b - a_1 a - a_3)$ e $P \oplus Q := (e, f)$, onde

$$\begin{aligned} e :=& \lambda^2 + a_1\lambda - a_2 - a - c\,, \\ f :=& -(\lambda + a_1)e - \mu - a_3\,, \end{aligned}$$

sendo

$$\lambda = \frac{3a^2 + 2a_2 a + a_4 - a_1 b}{2b + a_1 a + a_3}\,, \qquad \mu = \frac{-a^3 + a_4 a + 2a_6 - a_3 b}{2b + a_1 a + a_3}\,;$$

quando $a = c$ e $Q \neq -P$, e

$$\lambda = \frac{d - b}{c - a}, \qquad \mu = \frac{bc - ad}{c - a}$$

quando $a \neq c$.

Uma prova de que $(\mathbf{E}(L), \oplus)$ é um grupo pode ser vista por exemplo em [37, p. 55]. Para uma prova intrínseca deste fato (é dizer sem o uso de coordenadas) veja [11, p. 125].

Exemplo 3.2. Seja $T = (-2, 0), P = (-1, \sqrt{3})$ pertencente a $\mathbf{E}$ uma curva elíptica definida pela equação $y^2 = x^3 - 4x$ sobre $\mathbb{R}$ (ver figura 3.2). Usando as formulas para somar pontos sobre a curva, obtemos que $2T = \mathcal{O}$ e $2P = (25/12, -35\sqrt{3}/72)$.

Dado um inteiro m, temos uma aplicação $[m] : \mathbf{E}(L) \to \mathbf{E}(L)$ definida pela soma de $|m|$ pontos, a saber $P \mapsto P \oplus \ldots \oplus P$ ou $P \mapsto (-P) \oplus \ldots \oplus (-P)$, se $m \geq 0$ respectivamente se $m < 0$. Esta aplicação é a base para realizar as operações nos criptossistemas baseados em curvas elípticas (ver Seção 3.2) e pode ser calculada em tempo polinomial. Entretanto, não se conheçe um algoritmo determinístico eficiente para calcular o valor de m dados os pontos P e mP. Este problema, formalmente definido abaixo, é o chamado *Problema do Logaritmo Discreto sobre Curvas Elípticas* (ECDLP).

Definição 3.3. Sejam $\mathbf{E}$ uma curva elíptica definida sobre o corpo K, $Q, P \in \mathbf{E}(K)$. O problema do logaritmo discreto sobre $\mathbf{E}$ (em base Q), é o de encontrar um inteiro $m \in \mathbb{Z}$, se existe, tal que $P = mQ$.

A seguir consideramos curvas elípticas definidas sobre corpos finitos, pois estas são de interesse nas aplicações criptográficas ([4, p. 34], [37, p. 130]). Seja L um corpo finito tal

que $\#(L) = q = p^r$. Uma primeira questão a ser considerada ao trabalhar com este tipo de corpos é sobre o número de pontos de $\mathbf{E}(L)$. A priori uma cota superior é $q^2 + 1$, que pode ser melhorada consideravelmente. De fato, Hasse (1933) demonstrou que (veja [37, V.1.1]):

$$|\#\mathbf{E}(L) - (q+1)| \leq 2\sqrt{q}\,. \tag{3.5}$$

Por um resultado de Serre [39, p. 180], podemos escrever então

$$\#\mathbf{E}(L) = q + 1 - t\,, \qquad \text{onde } |t| \leq 2\lfloor\sqrt{q}\rfloor\ ,.$$

Aqui $t = t(\mathbf{E}(L))$ é chamada a *traça de Frobenius* de $\mathbf{E}(L)$. Reciprocamente, dados $q = p^m$ e t tais que

- $|t| \leq \lfloor\sqrt{q}\rfloor$,
- Se $p|t$, então $p^h|t$ com $h := \lfloor(m+1)/2\rfloor$,

então existe uma curva elíptica $\mathbf{E}$ definida sobre $\mathbb{F}_q$ tal que $\#\mathbf{E}(\mathbb{F}_q) = q + 1 - t$.

Exemplo 3.4. Considere a curva $\mathbf{E}$ com equação afim $y^2 = x^3 - 7x + 2$ sobre $K = \mathbb{F}_{23}$. Ela tem um único ponto na sua projetivização e é elíptica pois seu discriminante Δ é $-64((-7)^3 - 2^2) = 2^7 \neq 0$ ver (3.4). Esta curva tem 26 pontos racionais sobre $\mathbb{F}_{23}$. Logo $t = -2$.

Exemplo 3.5. Seja o corpo finito $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4 + x + 1)$ e $\alpha \in \mathbb{F}_{2^4}$ uma raiz primitiva do polinômio irredutível $x^4 + x + 1$ em $\mathbb{F}_2[x]$. As potências de α são dadas na tabela (3.1). Consideremos a curva elíptica $\mathbf{E} : y^2 + xy = x^3 + x^2 + 1$ sobre o corpo finito $\mathbb{F}_{2^4}$. O conjunto de ponto racionais de $\mathbf{E}$ sobre $\mathbb{F}_{2^4}$ são: $\mathbf{E}(\mathbb{F}_{2^4}) = \{\mathcal{O}, (0,1), (1,\alpha^5), (1,\alpha^10), (\alpha^3,\alpha), (\alpha^3,\alpha^9), (\alpha^5,1), (\alpha^5,\alpha^{10}), (\alpha^6,\alpha^2), (\alpha^6,\alpha^3), (\alpha^9,\alpha^8), (\alpha^9,\alpha^{12}), (\alpha^{10},1), (\alpha^{10},\alpha^5), (\alpha^{12},\alpha^4), (\alpha^{12},\alpha^6)\}$. Logo, $\#(\mathbf{E}(\mathbb{F}_{2^4})) = 16$ e daqui que $t = 1$.

Outra questão fundamental a considerar é sobre a estrutura do grupo de $(\mathbf{E}(L), \oplus)$. Este grupo não é necessáriamente cíclico, mas pode-se mostrar que é o produto de dois grupos cíclicos, ver [4, p.].

3.2 Criptossistemas usando Curvas Elípticas

Criptossistemas baseados em curvas elípticas foram propostos pela primeira vez e independentemente em 1985 por Victor Miller (IBM) e Neal Koblitz (Universidade de Washington). Estes são implementações de criptossistemas de chave pública que baseiam sua

n	α^n	n	α^n
0	1	8	α^2+1
1	α	9	$\alpha^3+\alpha$
2	α^2	10	$\alpha^2+\alpha+1$
3	α^3	11	$\alpha^3+\alpha^2+\alpha$
4	$\alpha+1$	12	$\alpha^3+\alpha^2+\alpha+1$
5	$\alpha^2+\alpha$	13	$\alpha^3+\alpha^2+1$
6	$\alpha^3+\alpha^2$	14	α^3+1
7	$\alpha^3+\alpha+1$	15	1

Tabela 3.1: Potências de α em $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/(x^4+x+1)$

segurança na resolução do problema do logaritmo discreto para grupos abelianos finitos. A implementação dos criptossistemas de chave pública sobre uma curva elíptica $\mathbf{E}$ se faz em forma natural. A questão a resolver é mais que todo a codificação do alfabeto de entrada como pontos racionais da curva $\mathbf{E}$ sobre um corpo finito L.

Exemplo 3.6. Para o sistema de troca de chaves Diffie-Hellman (2.1), suponha que temos uma curva elíptica $\mathbf{E}$ definida sobre $L = \mathbb{F}_q$ e um ponto $Q \in \mathbf{E}(L)$. O usuário $\mathbf{A}$ escolhe um inteiro aleatório k_A, calcula o ponto k_AQ, o qual envia para o usuário $\mathbf{B}$. Da mesma forma, $\mathbf{B}$ envia k_BQ para $\mathbf{A}$. Agora, os dois usuários tem um segredo em comum que será $k_A(k_BQ) = k_B(k_AQ)$. Um atacante que está interessado neste segredo entre os usuários $\mathbf{A}$ e $\mathbf{B}$ deverá determinar o valor de $P = k_Ak_BQ$ conhecendo somente Q, k_AQ e k_BQ. Logo, o atacante está enfrentando o chamado *problema Diffie-Hellman para Curvas Elípticas.*

Exemplo 3.7. Análogamente ao exemplo acima, podemos definir o criptossistema ElGamal (2.3) sobre curvas elípticas. Os usuários $\mathbf{A}$ e $\mathbf{B}$ devem de conhecer o corpo $L = \mathbb{F}_q$, a curva elíptica $\mathbf{E}$ sobre L e um ponto base[2] $G \in \mathbf{E}(L)$, que serão parâmetros de domínio público. Assim, se o usuário $\mathbf{A}$ deseja enviar o ponto $P_{\mathbf{m}}$ (associado à mensagem $\mathbf{m}$) ao usuário $\mathbf{B}$; este escolhe um inteiro aleátorio k_A, e envia para $\mathbf{B}$ o par $(k_AG, P_{\mathbf{m}} \oplus k_A(r_BG))$. $\mathbf{B}$ recebe esta mensagem e calcula o ponto $r_B(k_AG)$ usando a primeira coordenada da mensagem cifrada e sua chave privada. Logo, subtrai da segunda coordenada este valor e recupera a mensagem $P_{\mathbf{m}}$.

[2]Este será o ponto base sobre o qual se calcula o logaritmo discreto no grupo $\mathbf{E}(L)$.

Para implementar um criptossistema baseado em curvas elípticas, implica uma série de escolhas, por exemplo:

(1) Tipo de corpo base ($\mathbb{F}_p$ ou $\mathbb{F}_{2^m}$);

(2) Representação dos elementos do corpo base (polinomial, normal, entre outras);

(3) Equação da curva;

(4) Representação dos pontos da curva.

Ao tempo há fatores que influenciam nestas escolhas, as quais devem ser consideradas simultaneamente para ter o melhor criptossistema. Dentre destes fatores temos:

- Considerações de segurança;
- Disponibilidade de métodos para otimizar a aritmética no corpo;
- Disponibilidade de métodos para otimizar a aritmética na curva elíptica;
- Restrições do ambiente no computador.

Como foi mencionado no começo da seção, para a implementação de criptossistemas sobre curvas elípticas é necessário dispor um método para identificar cada mensagem básica $\mathbf{m}$ com um ponto $P_{\mathbf{m}} \in \mathbf{E}(L)$. Reciprocamente, se requer que o processo para recuperar $\mathbf{m}$ a partir de $P_{\mathbf{m}}$ seja computacionalmente rápido (um algoritmo de tempo polinômial). Normalmente, se usam métodos probabilísticos [18], [30, p. 233], que permitam fazer a identificação com um grau de erro pequeno. A seguir, descreveremos dois métodos para isto.

(1) Para corpos de característica diferente de 2 e 3, a curva elíptica é dada pela equação (3.4). Suponhamos que as mensagens básicas $\mathbf{m}$ são números naturais tais que $0 \leq \mathbf{m} \leq R$ com $R \in \mathbb{Z}$. Fixamos t um número natural (do qual dependerá a probabilidade de erro do método) e escolhemos um corpo $\mathbb{F}_q$, tais que $q > Rt$. Os inteiros entre 1 e Rt podem ser escritos da forma $\mathbf{m} \cdot t + j$ com $j = 1, \ldots, t-1$, assim podemos identificá-los como elementos de $\mathbb{F}_q$. Dado uma mensagem $\mathbf{m}$, tomemos $mt = x \in \mathbb{F}_q$ e calculamos o valor de $f(x) = x^3 + d_1 x + d_2$. Se $f(x)$ fosse um quadrado em $\mathbb{F}_q$, então tomamos $P_{\mathbf{m}} = (x, y)$ com $y = \sqrt{f(x)}$; em caso contrário tomamos $x = mt + 1$ e calculamos $f(x)$ e determinamos se é um quadrado em $\mathbb{F}_q$. Em geral, se para algum valor $j < t$, temos que $f(x)$ é um quadrado, então tomamos $P_{\mathbf{m}} = (x, \sqrt{f(x)})$. Para recuperar a

mensagem original $\mathbf{m}$ aplicamos a formula $m = \lfloor x/t \rfloor$. A probabilidade de falhar este procedimento para codificar é aproximadamente de $1/2^t$.

(2) Suponhamos $q = p^n$ e $n = 2n'$, além, que as mensagens básicas são inteiros $\mathbf{m}$ tais que $0 \leq m < p^{n'}$ onde $\mathbf{m}$ está escrito da forma $\mathbf{m} = m_0 + m_1 p + \ldots + m_{n'-1} p^{n'-1}$, $0 \leq m_j < p$. Para $\{b_0, \ldots, b_{n'-1}\}$ uma base de $\mathbb{F}_{p^{n'}}$ como espaço vetorial sobre $\mathbb{F}_p$ tomamos $x(\mathbf{m}) = m_0 b_0 + m_1 b_1 + \ldots + m_{n'-1} b_{n'-1}$ e $y(\mathbf{m})$ é uma solução da equação da curva (notemos que como equação tem grau 2 em y, então esta solução sempre existe em $\mathbb{F}_{p^n}$), logo $P_{\mathbf{m}} = (x(m), y(m))$.

Uma implementação eficiente de um criptossistema baseado em Curvas Elípticas, por exemplo, pode ver-se em [25]. A seguir mostramos uma forma de implementar o criptossistema ElGamal baseado em curvas elípticas, com o objetivo de dar uma idéia do uso das curvas elípticas na criptografia.

Exemplo 3.8. Consideramos a curva elíptica $\mathbf{E}$ definida por $Y^2 = X^3 - 7X + 2$ definida sobre o corpo $(\mathbb{Z}/751\mathbb{Z})^*$ e ponto base $G = (741, 152) \in \mathbf{E}((\mathbb{Z}/751\mathbb{Z})^*)$. Para codificar a mensagem identificamos as letras do alfabeto com o conjunto $\{10, 11, \ldots, 35\}$, respectivamente. O usuário **A** deseja enviar o mensagem $\mathbf{m} =$ **CURVASELIPTICAS** para o usuário **B**, que usando o método (1) acima, codifica as letras como pontos da curva elíptica. Assim, $0 \leq \mathbf{m} \leq 35 = R$, escolhemos $t = 20$ então $q = 751 \geq Rt = 700$. Codificando cada letra da mensagem temos: $P_C = (241, 372), P_U = (601, 172), P_R = (541, 104), P_V = (621, 324)$, $P_A = (202, 32), P_S = (565, 269), P_E = (282, 101), P_L = (423, 301), P_I = (361, 82), P_P = (501, 53), P_T = (581, 283)$. O usuário **B** escolhe sua chave privada $r_B = 7$ e calcula o ponto $7G = (739, 164)$, que será sua chave pública. Logo, o usuário **A** usa a chave pública de **B** para cifrar cada mensagem básica, por exemplo, o ponto $P_C = (241, 372)$. **A** escolhe o número $k = 3$ e calcula $3G$, $3 \cdot 7G$ e $P_C + 3 \cdot 7G = (576, 100)$. Então **A** envia o par de pontos $(kG, P_C + kr_BG) = ((76, 623), (576, 100))$. Desta forma o usuário **A** envia o seguinte mensagem cifrada (M.C.):
$M.C. = \{(76, 623), (576, 100), (59, 506), (109, 172), (365, 335), (392, 297), (132, 458), (742, 350), (458, 351), (149, 682), (357, 312), (171, 58), (149, 682), (576, 100), (392, 297), (132, 458)\}$.

O usuário **B** recupera a mensagem original multiplicando o primeiro dos números recebidos por sua chave privada, obtendo o valor de $r_BkG = (0, 113)$ e depois subtrai este dos outros pontos, i.e., $(576, 100) - (0, 113) = (241, 372) = P_C$ e assim com todos os pontos da

mensagem cifrada, por último o usuário $\mathbf{B}$ decodifica esta mensagem como foi dito no item (1).

A seguir, alguns fatos interessantes que estão relacionados com os criptossistemas elípticos:

- A proposta de usar curvas elípticas para implementar criptossistemas de chave pública, baseados no problema do logaritmo discreto foi motivada pelo avanço em ataques, como o index calculus, feito aos criptossistemas construídos a partir de corpos finitos [1].

- Um trabalho de Menezes, Okamoto e Vanstone [28], mostram como dada uma curva elíptica $\mathbf{E}$ definida sobre $\mathbb{F}_q$, o DLP sobre esta curva pode ser reduzido (usando um algoritmo de tempo polinomial), ao problema do logaritmo discreto sobre o corpo $\mathbb{F}_{q^k}$ onde o valor de k dependia da curva elíptica. Isto implica que para valores pequenos de k, o criptossistema era quebrado; Menezes, Okamoto e Vanstone provaram que este fato acontecia com as curvas elípticas *supersingulares*. Uma curva elíptica $\mathbf{E}$ definida sobre $\mathbb{F}_q$ é chamada de supersingular se $\#(\mathbf{E}) \equiv 1 \pmod{p}$.

- Existe outro tipo de curvas elípticas não adequadas para criptografia chamadas de anômalas, isto é, uma curva elíptica $\mathbf{E}$ definida sobre $\mathbb{F}_q$ tal que $\#(\mathbf{E}) = q$, pois Satoh e Araki mostraram um algoritmo de tempo polinomial para o DLP sobre este tipo particular de curvas elípticas, ver [36].

- O algoritmo mais rápido que se conheçe, até hoje, para a multiplicação de pontos em curvas elípticas definidas sobre corpos finitos de característica 2 da forma $\mathbb{F}_{2^m}$ foi desenvolvido por Julio López e Ricardo Dahab [24].

- Devido à existência de ataques eficientes para certos tipos de curvas elípticas, se faz necessário procurar novos grupos onde a resolução do problema de logaritmo discreto tenha complexidade de tempo exponencial. Este é o tema que queremos abordar no próximo capítulo, introduzindo os Jacobianos de curvas Hiperelípticas.

- Existem algoritmos propostos para gerar os parâmetros públicos para os criptossistemas elípticos, ver [14], [31].

- O passado 24 de Agosto do 2003, a Agência de Segurança Nacional (NSA) em Maryland, adquiriu os direitos exclusivos a *Certicom* para usar os Criptossistemas de Curvas Elípticas, fato que nos leva a pensar na importância para o estudo deste tipo de criptossistemas.

CAPÍTULO 4

Criptossistemas Hiperelípticos

Atualmente, a resolução do DLP sobre curvas elípticas é de tempo exponencial salvo certas curvas tais como as Supersingulares e as Anómalas. Porém, esta segurança poderia ser quebrada no sentido que a complexidade da resolução do DLP se torne de tempo sub-exponencial; isto é factível devido, por exemplo, ao avanço das Ciência Matemática, Computacional e Física respectivamente. Assim, se faz necessário o estudo de novos grupos onde o DLP tenha uma resolução de tempo exponencial (veja [16]). Devido a que uma curva elíptica coincide com seu *Jacobiano*, é natural tentar obter tais grupos como subgrupos do Jacobiano de uma curva arbitraria.

Geralmente, pode-se tentar estudar subgrupos de *Variedades Abelianas* sobre corpos finitos (por exemplo Jacobianos). Fatos teóricos destes objetos se encontram em [8, Milne, Cap. V]. Em esta generalidade, o uso destas variedades ainda parece estar longe de concretizar-se, pois não é claro como implementar algorítmos que permitam operar eficientemente com seus elementos. No caso de que a Variedade Abeliana seja o Jacobiano de uma curva, então a eleição do grupo está ligada com a estrutura da curva em questão. Se deve ter presente pelo menos duas propriedades básicas da curva: (i) que tenha um modelo plano simples e (ii) que o tempo de operar no Jacobiano seja polinomial. A seguir nos referimos a algumas de tais curvas.

- Curvas hiperelípticas (veja Equação 4.1); Koblitz [19] foi o primeiro que propôs usar grupos do Jacobiano destas curvas (definidas sobre corpos finitos) onde se es-

pera que o DLP tenha complexidade de tempo exponencial. Para operar os elementos do Jacobiano, Koblitz melhorou e generalizou o algoritmo de Cantor [7];

- Curvas de Picard: Sejam $t \geq 1$ um inteiro, $a_1, \ldots, a_t \in \mathbb{F}_q$ distintos dois a dois e $m_1, \ldots, m_t$ inteiros no negativos tal que $\sum_{i=1}^{t} m_i = 4$. Então esta curva são os zeros (x, y) junto com $\mathcal{O}$ (ponto no infinito) tal que $y^3 = a\prod_{i=1}^{t}(x - a_i)^{m_i}$ para $a \in \mathbb{F}_q$. Se a curva admite certos automorfismos, J.P Cherdieu, J. Estrada e E. Reinaldo implementaram um algoritmo em tempo polinomial para a soma no Jacobiano. Estas curvas são um caso particular de curvas *Superelípticas*, as quais tem sido sugeridas para construir criptossistemas de chave pública por Galbraith, Paulus e Smart em [13].

- Curvas $C_{ab} \subseteq \bar{K}^2$, a saber do tipo $C : \alpha_{b,0}x^b + \alpha_{0,a}y^a + \sum_{ia+jb<ab} \alpha_{i,j}x^i y^j = 0$, onde $\alpha_{i,j} \in K$, $\alpha_{b,0} \neq$, $\alpha_{0,a} \neq$ e a, b são inteiros positivos co-primos. Este tipo de curvas tem sido sugeridas também na construção de códigos algébrico geométricos, ver [27]).

Neste capítulo estudamos o Jacobiano de curvas hiperelípticas e a aplicação destes em criptossistemas chamados *Criptossistemas hiperelípticos*. Nos últimos anos tem aumentado o interesse pelo estudo destas curvas as quais em particular foram utilizadas, por exemplo, para o desenho de códigos corretores de erros [5] e algoritmos de fatoração [22].

4.1 Conceitos Básicos de Curvas Hiperelípticas

Nesta seção, introduzimos a teoria básica de curvas hiperelípticas e seus Jacobianos com o fim de propor grupos que sirvam para implementar criptossistemas de chave pública.

Fixemos K um corpo perfeito de característica $p \geq 0$ e seja $\bar{K}$ seu fecho algébrico e g um inteiro positivo.

4.1.1 Generalidades

As curvas hiperelípticas são uma classe especial de curvas algébricas e podem ser vistas como uma generalização das curvas elípticas.

Definição 4.1. Uma curva hiperelíptica $\mathbf{H}$ sobre K são os zeros no plano projetivo $\mathbf{P}^2(\bar{K})$ de uma equação da forma

$$Y^2Z^{2g-1} + h(X/Z)YZ^{2g} = f(X/Z)Z^{2g+1}, \tag{4.1}$$

onde,

(1) $f \in K[X]$, mónico e de grau $2g+1$;

(2) $h \in K[X]$, $h = 0$ ou de grau no máximo g;

(3) A curva $\mathbf{H}$ é não singular em todo ponto $P = (x : y : 1) \in \mathbf{H}$.

O número g é chamado o gênero da curva (veja [11, p. 196]).
Da equação (4.1) temos que a curva $\mathbf{H}$ intercepta a reta $Z = 0$ no ponto

$$\mathcal{O} = (0 : 1 : 0),$$

e assim podemos considerar a $\mathbf{H}$ como sendo a união deste ponto com os zeros $(X, Y) \in \bar{K} \times \bar{K}$ do polinômio:

$$F = F(X, Y) := Y^2 + h(X)Y - f(X). \tag{4.2}$$

Fácilmente se prova que F é irredutível em $\bar{K}[X, Y]$, i.e., F é absolutamente irredutível (ver Apêndice A). A condição (3) acima é equivalente a que o sistema

$$\begin{aligned} Y^2 + h(X)Y - f(X) &= 0 \\ 2Y + h(X) &= 0 \\ h(X)'Y - f'(X) &= 0 \end{aligned}$$

não tenha solução em $\bar{K} \times \bar{K}$. Mais ainda, da equação (4.1) podemos mostrar que $\mathbf{H}$ é não singular em $\mathcal{O}$ se e somente se $g = 1$. De fato, des-homogeneizando esta equação com respeito a Y temos

$$Z^{2g-1} + h(X/Z)Z^{2g} = f(X/Z)Z^{2g+1},$$

e daqui a curva é não singular em $\mathcal{O}$ se e somente se $2g - 1 = 1$. Se a característica p é maior que dois, então o polinômio (4.2) pode ser considerado como

$$F = Y^2 - f(X), \qquad \text{com } f(X) \text{ um polinômio mônico de grau } 2g+1, \tag{4.3}$$

fazendo a mudança de variáveis: $Y \mapsto Y - h(X)/2$.

Lema 4.2. *Seja F o polinômio em (4.2). Se $p = 2$ então $h(X) \neq 0$.*

Demonstração. Suponha que $h(X) = 0$; derive F com respeito a X e seja $x \in \bar{K}$ uma raíz de $f(X)'$. Seja $y \in \bar{K}$ raiz de $Y^2 = f(x)$. Logo o ponto $(x, y) = (x : y : 1)$ é um ponto singular da curva, contradição com a hipótese (3) da definição de curva hiperelíptica. □

4.1.2 Pontos racionais

De forma análoga ao caso elíptico, podemos definir o conjunto de pontos racionais para um corpo L tal que $K \subseteq L \subseteq \bar{K}$. O conjunto $\mathbf{H}(L)$ de *pontos racionais de* $\mathbf{H}$ *sobre* L está formado pelo ponto $\mathcal{O}$ e os zeros $(x, y) \in L \times L$ do polinômio F em (4.2). Para $K = \mathbb{F}_q$ e $L = \mathbb{F}_{q^n}$, seja n_L o número de pontos racionais de $\mathbf{H}$ sobre L, então

$$n_L = q^n + 1 - \sum_{i=1}^{g} (\alpha_i + \bar{\alpha}_i)\,, \tag{4.4}$$

onde os α_i's são inteiros algébricos[1] de módulo $\sqrt{q^n}$.[2] Temos que

$$\alpha_i = \beta_i^n\,, \qquad \text{para } i = 1, \ldots, g \tag{4.5}$$

onde os β_i's e seus conjugados são raízes de um polinômio com coeficientes em $\mathbb{Z}[t]$ da forma:

$$h(t) = t^{2g} + a_1 t^{2g-1} + \ldots + a_g t^g + q a_{g-1} t^{g-1} + q^2 a_{g-2} t^{g-2} + \ldots + q^{g-1} a_1 t + q^g\,. \tag{4.6}$$

De (4.4) obtemos a chamada cota de Hasse-Weil para $\mathbf{H}(L)$, a saber

$$|n_L - (q^n + 1)| \leq 2\sqrt{q^n}\, g\,.$$

Agora seja $S_i := \#\mathbf{H}(\mathbb{F}_{q^i}) - (q^i + 1)$. Por (4.4) e (4.5) aplicados com $n = i$, temos

$$S_i = -\sum_{j=1}^{g} (\beta_j^i + \bar{\beta}_j^i)\,, \qquad \text{para } i \geq 1\,.$$

Assim por exemplo da Equação (4.6), $a_1 = S_1$, $2a_2 = S_2 + S_1 a_1$, e em geral temos as seguintes fórmulas de recorrência (por exemplo, utilizando as fórmulas de Newton, ver [39, Cor. V.1.17]),

$$i a_i = S_i + \sum_{j=1}^{i-1} S_{i-j} a_j\,.$$

Vemos então que o polinômio $h(t)$ em (4.6) se determina completamente se e somente se conhecemos S_i para $i = 1, \ldots, g$. Em particular, com esta informação se calcula $\#\mathbf{H}(\mathbb{F}_{q^i})$ para $i \geq g + 1$.

---

[1] Um número complexo α é chamado um *inteiro algébrico* se este satisfaz um polinômio da forma $x^m + a_{m-1}x^{m-1} + \ldots + c_1 x + c_0 = 0$ com $c_i \in \mathbb{Z}$.

[2] Esta é a hipótese de Riemann para curvas sobre corpos finitos [8, Milne, Cap. 7, §11], [39, Cap. 5].

4.1.3 Exemplos

Exemplo 4.3. *Seja $K = \mathbb{F}_2$ e consideremos a curva* $\mathbf{H}$ *definida por:*

$$F(X,Y) = Y^2 + Y - X^5 - X^3 - X = 0\,.$$

Temos $\partial_Y F(X,Y) = 1$ e pelo tanto $\mathbf{H}$ *é hiperelíptica de gênero 2. Determinaremos $n_r := \#\mathbf{H}(\mathbb{F}_{2^r})$. Pelo mencionada acima, será suficiente calcular n_1 e n_2. Por processo exaustivo temos que $n_1 = 3$ e $n_2 = 9$. Então $a_1 = 0$ e $a_2 = 2$. Logo, $h(t) = t^4 + 2t^2 + 4$, daqui $\alpha_1 = (\sqrt{2} + \sqrt{6}i)/2$ e $\alpha_2 = (-\sqrt{2} + \sqrt{6}i)/2$. Finalmente temos que*

$$n(\mathbb{F}_{2^r}) = \begin{cases} 2^r + 1 & se \quad r \equiv 1,3,5 \pmod 6 \\ 2^r + 1 + 2^{r/2+1} & se \quad r \equiv 2,4 \pmod 6 \\ 2^r + 1 - 2^{r/2+2} & se \quad r \equiv 0 \pmod 6 \end{cases}$$

Exemplo 4.4. As curvas deste exemplo são hiperelípticas como pode ser verificado usando somente a definição. Todas estas tem gênero dois. Seja a curva $\mathbf{H}$ definida por:

$$Y^2 = (X+1)(X^2+1)(X^2+3)\,.$$

Então o seu gráfico em $\mathbb{R} \times \mathbb{R}$ é:

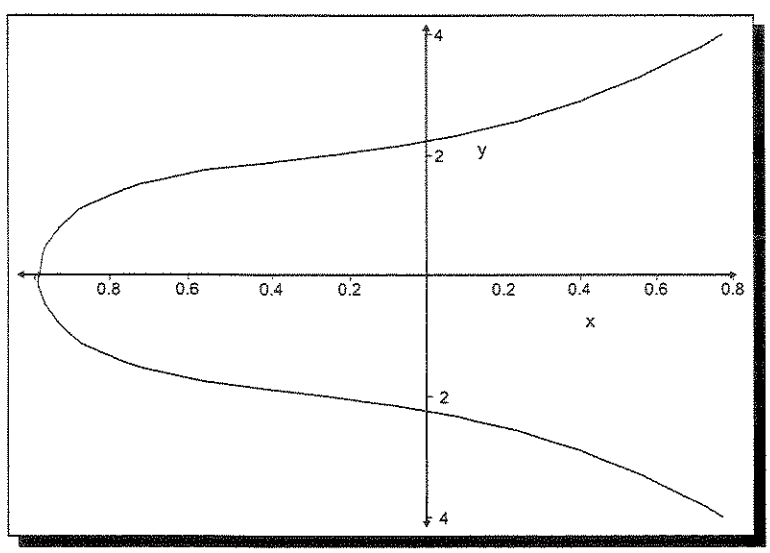


Figura 4.1: Curva Hiperelíptica 1

Agora suponha que $\mathbf{H}$ está definida por:

$$Y^2 = X(X^2-1)(X^2+5)\,.$$

Então o seu gráfico em $\mathbb{R} \times \mathbb{R}$ é:

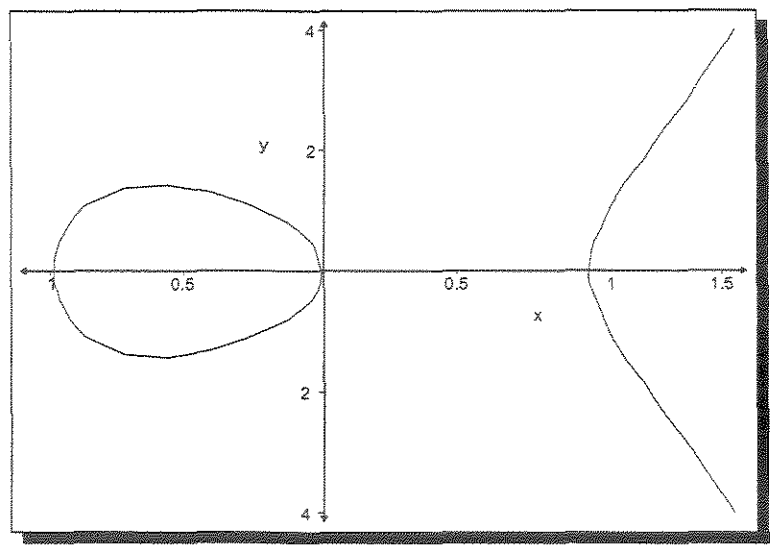


Figura 4.2: Curva Hiperelíptica 2

Finalmente considere a curva $\mathbf{H}$ definida por

$$Y^2 = X(X+1)(X-1)(X+2)(X-2)\,.$$

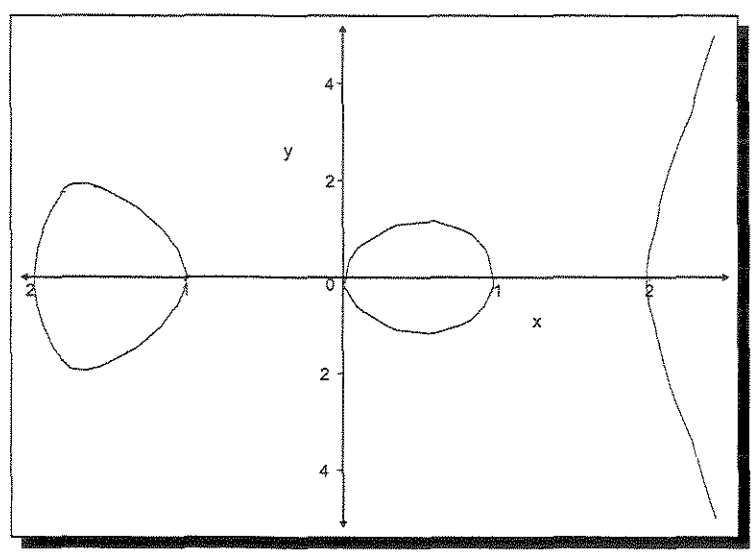


Figura 4.3: Curva Hiperelíptica 3

4.1.4 Uma involução sobre H

Sobre $\mathbf{H}$ e de forma natural está definida uma *involução* $\sigma : \mathbf{H} \to \mathbf{H}$ definida por $(x, y) \mapsto (x, -y - h(x))$ e $\sigma(\mathcal{O}) = \mathcal{O}$; observe que σ é um automorfismo de $\mathbf{H}$ tal que $\sigma \circ \sigma$ é a identidade sobre $\mathbf{H}$ (alguns autores chamam a $\sigma(x, y)$ e $\sigma(\mathcal{O})$ o *oposto* de (x, y) e de $\mathcal{O}$ respectivamente). Lembramos que podemos supor $h(X) = 0$ se $p > 2$. Os pontos fixos de σ são chamados de *Pontos Especiais*, caso contrário, de *Ordinários*. No caso $p > 2$ e $h(X) = 0$, os pontos especiais diferentes de $\mathcal{O}$ são da forma $(a, 0)$ onde a é raiz de $f(X)$ no corpo considerado.

Exemplo 4.5. Considere a curva $\mathbf{H}$ sobre $\mathbb{F}_7$ definida por:

$$Y^2 + XY = f(X) := X^5 + 5X^4 + 6X^2 + X + 3\,.$$

Afirmamos que esta curva é hiperelíptica de gênero $g = 2$. Com efeito, temos que o grau de $f(X) = 2g + 1$, o grau de $h(X) := X$ é menor o igual que 2 e verifiquemos que o sistema $Y^2 + XY = f(X)\,(1)$, $2Y + X = 0\,(2)$, $Y = 5X^4 + 6X^3 + 5X + 1\,(3)$ não tem solução em $\bar{\mathbb{F}}_7 \times \bar{\mathbb{F}}_7$. De (2) temos que $Y = 3X$; e substituindo em (3), $5X^4 + 6X^3 + 2X + 1 = 0\,(4)$; em (1): $X^5 + 5X^4 + X^2 + X + 3 = 0\,(5)$. Logo, as raízes de (4) são $\{1, 2, 3, 4\}$ e nenhuma destas é raiz de (5), logo concluímos que a curva definida acima é uma curva hiperelíptica. Fazendo a mudança de coordenadas $Y \mapsto Y + 4X$ e $X \mapsto X$, a equação acima fica equivalente à equação :

$$Y^2 = X^5 + 5X^4 + X^2 + X + 3\,.$$

Logo os pontos especiais de $\mathbf{H}$ sobre $\mathbb{F}_7$ são $\mathcal{O}$ e os pontos $(a, 0)$ onde a é uma raiz em $\mathbb{F}_7$ de $X^5 + 5X^4 + 6X^2 + X + 3 = 0$. Este polinômio só tem uma raiz em $\mathbb{F}_7$, a saber $\{6\}$. Daí que o único ponto especial da curva é $P = (6, 4)$. Temos que os pontos racionais de $\mathbf{H}$ sobre $\mathbb{F}_7$ são:

$$\mathbf{H}(\mathbb{F}_7) = \{\mathcal{O}, (1,1), (1,5), (2,2), (2,3), (5,3), (5,6), (6,4)\}\,.$$

Exemplo 4.6. Consideremos a curva hiperelíptica $\mathbf{H}$ definida por $Y^2 + (X^2 + X)Y = X^5 + X^3 + 1$, de gênero 2 sobre o corpo $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$, onde o polinômio $X^5 + X^2 + 1$ é irredutível em $\mathbb{F}_2[X]$. O conjunto de pontos racionais desta curva é:
$\mathbf{H}(\mathbb{F}_{2^5}) = \{\mathcal{O}, (0,1), (1,1), (\alpha^5, \alpha^{15}), (\alpha^5, \alpha^{27}), (\alpha^7, \alpha^4), (\alpha^7, \alpha^{25}), (\alpha^9, \alpha^{27}), (\alpha^9, \alpha^{30}), (\alpha^{10}, \alpha^{30}),$
$(\alpha^{14}, \alpha^8), (\alpha^{14}, \alpha^{19}), (\alpha^{15}, 0), (\alpha^{15}, \alpha^8), (\alpha^{18}, \alpha^{23}), (\alpha^{18}, \alpha^{29}), (\alpha^{19}, \alpha^2), (\alpha^{19}, \alpha^{28}), (\alpha^{20}, \alpha^{15}),$
$(\alpha^{20}, \alpha^{29}), (\alpha^{23}, 0), (\alpha^{23}, \alpha^4), (\alpha^{25}, \alpha), (\alpha^{25}, \alpha^{14}), (\alpha^{27}, 0), (\alpha^{27}, \alpha^2), (\alpha^{28}, \alpha^7), (\alpha^{28}, \alpha^{16}), (\alpha^{29}, 0),$
$(\alpha^{29}, \alpha), (\alpha^{30}, 0), (\alpha^{30}, \alpha^{16})\}$. Os pontos $(0, 1)$ e $(1, 1)$ são pontos fixos da curva.

4.1.5 Divisores sobre H

Um *divisor* D sobre $\mathbf{H}$ é uma soma formal de pontos de $\mathbf{H}$, $D = \sum_P v_P(D)P$, onde cada $v_P(D)$ é um inteiro e diferente de zero somente para um número finito de pontos (pelo tanto podemos identificar D com um elemento do grupo abeliano livre gerado pelos pontos de $\mathbf{H}$). O conjunto $\mathrm{Sup}(D)$ dos pontos P onde $v_P(D) \neq 0$ é chamado de *suporte* de D. O conjunto de divisores de $\mathbf{H}$ será denotado por $\mathrm{Div}(\mathbf{H})$ e este é um grupo comutativo com a operação :

$$D_1 + D_2 = \sum_P v_P(D_1)P + \sum_P v_P(D_2)P := \sum_P (v_P(D_1) + v_P(D_2))P\,.$$

O *grau* de um divisor D está definido por $\deg(D) := \sum_P v_P(D)$; logo temos um homomorfismo sobrejetivo de grupos dado por $\deg : \mathrm{Div}(\mathbf{H}) \to \mathbb{Z}$, $D \mapsto \deg(D)$. Para $D \in \mathrm{Div}(\mathbf{H})$ e τ um automorfismo de $\mathbf{H}$, definimos $D^\tau := \sum_P v_P(D)\tau(P)$. Para um corpo L tal que $K \subseteq L \subseteq \bar{K}$, dizemos que D *está definido sobre* L, se para todo automorfismo τ de $\mathbf{H}$ definido sobre L temos que $D^\tau = D$. Dizemos que τ está definido sobre L se $\tau(P) = P$ para todo $P \in \mathbf{H}(L)$. O conjunto de tais divisores será denotado por $\mathrm{Div}_L(\mathbf{H})$ e este é um subgrupo de $\mathrm{Div}(\mathbf{H})$. Para dois divisores $D_1 = \sum_P v_P(D_1)P$, $D_2 = \sum_P v_P(D_2)P \in \mathrm{Div}_L(\mathbf{H})$, definimos (de acordo com [21, p. 167])

$$\mathrm{mdc}(D_1, D_2) := \sum_{P \neq \mathcal{O}} \min\{v_P(D_1), v_P(D_2)\}P - m\mathcal{O}\,,$$

com $\deg(\mathrm{mdc}(D_1, D_2)) = 0$. Definamos $\mathrm{Div}^0_L(\mathbf{H}) := \mathrm{Div}_L(\mathbf{H}) \cap \mathrm{Kernel}(\deg)$; este conjunto é um subgrupo de $\mathrm{Div}_L(\mathbf{H})$ e desempenhará um papel relevante no que segue.

4.1.6 Corpo de funções racionais

Os elementos do anel $L[\mathbf{H}] := L[X,Y]/(F)$, onde (F) é o ideal de $L[X,Y]$ gerado por F, podem ser considerados *funções polinomiais* $p : \mathbf{H} \to \mathbf{P}^1(\bar{K})$ com $p(P) = \infty$ se e somente se $P = \mathcal{O}$. Este anel quociente de fato é isomorfo ao conjunto de funciones polinomiais para $L = \bar{K}$.

Sendo F absolutamente irredutível, $L[\mathbf{H}]$ é um domínio de integridade e portanto está definido seu corpo quociente $L(\mathbf{H})$; este é chamado o *Corpo de Funções Racionais de* $\mathbf{H}$ *sobre* L. Para $R \in L[X,Y]$, denotemos por $\bar{R}$ a sua classe em $L[\mathbf{H}]$. Consideremos o homomorfismo de anéis $L[X] \to L[\mathbf{H}]$, $R(X) \mapsto \bar{R}(X)$. Logo este é injetivo pois $\deg_Y(R(X)) = 0$ para $R(X) \neq 0$. Em particular, podemos identificar cada constante $a \in L$ con $\bar{a}$ e X com $\bar{X}$. Seja

$y := \bar{Y}$. Então tomando classes, temos $F(X, y) = 0$, isto é,

$$y^2 + h(X)y - f(X) = 0\,.$$

Desta forma, cada elemento de $L[\mathbf{H}]$ pode ser reduzido de maneira única há

$$A(X) + B(X)y\,.$$

Observe que isto significa que $L[\mathbf{H}]$ é um módulo livre de posto dois sobre $L[X]$. Finalmente, temos que $L(\mathbf{H}) = L(X, y)$ pois $[L(\mathbf{H}) : L(X)] = 2$ e $[L(\mathbf{H}) : L(y)] = 2g + 1$.

4.1.7 Pontos regulares e pólos de uma função racional

Aqui será conveniente assumir $L = \bar{K}$. Seja $r \in \bar{K}(\mathbf{H})$, $P \in \mathbf{H}$, $P \neq \mathcal{O}$. Dizemos que r *está definida* em P ou que r é *regular* em P, se existem funções polinomiais R, S tais que $r = R/S$ e $S(P) \neq 0$; neste caso $r(P) := R(P)/S(P)$. Esta definição independe da representação de r mediante R e S; de fato se $R/S = R_1/S_1$, então F divide $(RS_1 - R_1S)$ e se segue a boa definição de $r(P)$.

No caso de que r não possa ser definido em P, este ponto é dito um *pólo* de r e definimos $r(P) := \infty$ (desta forma r induz uma função racional $\mathbf{H} \to \mathbf{P}^1(\bar{K})$). Se r está definido em P e $r(P) = 0$, P é chamado de *zero* de r. Observamos que $r \neq 0$ tem um número finito de pólos e zeros. Com efeito, os zeros $P = (a_P, b_P)$ de r são os zeros de uma função polinomial da forma $A(X) + B(X)y$, onde $A, B \in \bar{K}[X]$. Podemos supor $\mathrm{mdc}(A(X), B(X)) = 1$; agora $(A(X) + B(X)y)(A(X) - B(X)(y + h(X))$ é uma função polinomial em X e portanto o número de coordenadas a_P para P é finito. Como $A(a_P) + B(a_P)b_P = 0$ e $B(a_P) \neq 0$ (do contrário $(X - a_P)$ é um divisor de $A(X)$ e $B(X)$) então $b_P = -A(a_P)/B(a_P)$. O mesmo raciocínio serve para os pólos.

4.1.8 Divisores principais.

A cada função racional não nula r associaremos o seguinte divisor sobre $\mathbf{H}$, chamado de *principal*,

$$\mathrm{div}(r) := \sum_{P \in \mathbf{H}} v_P(r)P\,,$$

onde $P \in \mathrm{Sup}(\mathrm{div}(r))$ se e somente se P é um zero ou P é um polo de r. Para $P \in \mathbf{H}$ e $r = 0$, $v_P(0) := +\infty$. Em $\bar{K}(\mathbf{H}) \setminus \{0\}$ se espera que v_P satisfaça as seguintes propriedades:

(1) $v_P(rr_1) = v_P(r) + v_P(r_1)$;

(2) $v_P(r + r_1) \geq \min\{v_P(r), v_P(r_1)\}$ (e temos a igualdade se $v_P(r) \neq v_P(r_1)$), neste caso v_P é chamada de *valoração* ou de *ordem* em P.

Para $r = R/S \in \bar{K}(\mathbf{H})$, $r \neq 0$, $v_P(r)$ será por definição $v_P(R) - v_P(S)$. Logo é suficiente definir $v_P(R)$ para uma função polinomial $R = A(X) + B(X)y$.
Caso 1. O ponto $P = (a, b) \neq \sigma(P)$ onde σ é a involução de $\mathbf{H}$. Seja ℓ a maior potência de $(X - a)$ que divide a A e B; logo $R = (X - a)^{\ell} R_1$, onde $R_1 = A_1(X) + B_1(X)y \in \bar{K}[\mathbf{H}]$.

- Se $R_1(P) \neq 0$, $v_P(R) := \ell$;
- Se $R_1(P) = 0$. Usando $F(X, y) = 0$, obtemos

$$R_1(X, y)R_1(\sigma(X, y)) = N(X) := A_1^2 - A_1 B_1 h - B_1^2 f \in \bar{K}[X]\,. \tag{4.7}$$

  Logo $v_P(R) := \ell + \ell_1$, onde ℓ_1 é a maior potência de $(X - a)$ que divide o polinômio $N(X)$ acima.

Exemplo 4.7. Seja $P = (a, b) \neq \sigma(P)$. Para $R = X - a$, temos $v_P(R) = v_{\sigma(P)}(R) = 1$. Para $S = y - b$, consideramos $S(X, y) \cdot S(X, -y - h(X)) = N(X) = b^2 + bh(X) - f(X)$. Logo $v_P(y - b) = \ell_1 \geq 1$ onde ℓ_1 é a maior potência de $(X - a)$ que divide $N(X)$. Pode acontecer que $v_P(y - b) > 1$. Por exemplo considere a característica $p > 2$, $a \in K^*$ e as curvas $\mathbf{H}_a$ definidas por

$$F_a(X, Y) := Y^2 - a^2 - (X - a)^2 - (X - a)^3\,.$$

Temos que os possíveis pontos singulares de $\mathbf{H}_a$ em $K \times K$ satisfazem $Y = 0$, $2+3(X-a) = 0$; neste caso a deve satisfazer a condição $27a^2 = -4$. Logo concluímos que $\mathbf{H}_a$ é hiperelíptica de gênero 1, salvo possívelmente dois valores de a. Logo considerando $P = (a, a)$, temos $v_P(y - b) = v_P(y - a) = 2$. Agora, seja $p = 2$, $a \in K$ e as curvas $\mathbf{H}_a$ definidas por

$$F_a(X, Y) := Y^2 + Y - (X - a)^3 - (X - a)^5\,.$$

Para qualquer valor de a temos que $\mathbf{H}_a$ é uma curva hiperelíptica de gênero 2. Logo considerando $P = (a, 1)$ temos que $v_P(y - b) = v_P(y + 1) \geq 3$.

Caso2: O ponto $P = (a, b) = \sigma(P)$. Sejam R_1, ℓ, ℓ_1 como no caso anterior. Então se $R_1(P) \neq 0$, $v_P(R) := 2\ell$; caso contrário, $v_P(R) = 2\ell + \ell_1$.
Case 3: $P = \mathcal{O}$. Aqui $v_{\mathcal{O}}(R) := -\max\{2\deg(A(X)), 2\deg(B(X)) + 2g + 1\}$.

onde R é P ou $\sigma(P)$.

Se $P = \sigma(P)$, e n_P é um inteiro par, temos $n_P P \sim n_P \mathcal{O}$; caso contrário se $n_P = 2n+1$, $n_P P \sim 2n\mathcal{O} + P$. Isto termina a prova. □

4.1.10 Divisores reduzidos

O objetivo desta sub-seção é mostrar que todo divisor de grau zero é linearmente equivalente a um único divisor de um certo tipo (Teorema 4.11) o qual será importante para fazer as operações sobre o Jacobiano da curva.
Fixemos D um divisor semi-reduzido,

$$D = \sum_{P=\sigma(P), P\neq\mathcal{O}} P + \sum_{P\neq\sigma(P)} v_P(D)P - m\mathcal{O}\,.$$

D é chamado *reduzido* se $\sum_{P\neq\mathcal{O}} v_P(D) = m \leq g$, onde g é o gênero de $\mathbf{H}$.

Seja D_1 um divisor de grau zero; logo pelo Lema 4.8 podemos supor que $D_1 \sim D$. Para $P \in \mathrm{Sup}(D) \setminus \{\mathcal{O}\}$, $P = (a_P, b_P)$, definamos

$$A = A(X) := \prod_P (X - a_P)^{v_P(D)} \in \bar{K}[X]\,.$$

Lema 4.9. *Existe um único polinômio $B = B(X) \in \bar{K}[X]$ tal que:*

(1) $\deg(B) < \deg(A)$;

(2) *Para $P \in \mathrm{Sup}(D) \setminus \{\mathcal{O}\}$, $B(a_P) = b_P$;*

(3) $B^2 + Bh(X) - f(X) \equiv 0 \pmod{A}$.

Além disso, $D = \mathrm{div}(A, B) := \mathrm{mdc}(\mathrm{div}(A), \mathrm{div}(B - y))$. Para $r \in \bar{K}(\mathbf{H})$, observamos que a notação $r \equiv 0 \pmod{A}$ significa que $r = As$ onde $v_P(s) \geq 0$.

Demonstração. Primeiro mostramos uma versão "local" do lemma.
Afirmação 1. Para $P \in \mathrm{Sup}(D)$, $P \neq \mathcal{O}$, existe um único polinômio $R = R_P(X)$ tal que (i) $\deg(R) < v_P(D)$, (ii) $R(a_P) = b_P$, (iii) $R^2 + Rh(X) - f(X) \equiv 0 \pmod{(X - a_P)^{v_P(D)}}$.
Caso $P \neq \sigma(P)$. Como $v_P((y - b_P)/(X - a_P)) \geq 0$, $y = b_P + (X - a_P)A$, com único $A \in \bar{K}(\mathbf{H})$ tal que $v_P(A) \geq 0$. Repetindo este processo por substituições do tipo $A = (A - A(P)) + A(P)$, obtemos uma única representação para y do tipo

$$y = b_P + c_1(X - a_P) + \ldots + c_{v_P(D)-1}(X - a_P)^{v_P(D)-1} + (X - a_P)^{v_P(D)} R_1\,,$$

onde $v_P(R_1) \geq 0$. Logo definimos:

$$R = R_P(X) := b_P + c_1(X - a_P) + \ldots + c_{v_P(D)-1}(X - a_P)^{v_P(D)-1}.$$

Este polinômio claramente satisfaz (i), (ii); a propriedade (iii) segue do fato que $y \equiv R \pmod{(X-a_P)^{v_P(D)}}$ (observe que $v_P((R-y)/(x-a_P)^{v_P(D)}) \geq 0$ pois $R-y = (x-a_P)^{v_P(D)}R_1$). **Caso** $P = \sigma(P)$. Aqui $v_P(D) = 1$; logo $R = R_P := b_P$.

Para a versão global aplicamos o Teorema Chinês dos Restos para A e os R_P; pelo tanto existe um único polinômio $B = B(X)$ tal que $\deg(B) < \deg(A)$ e $B(X) \equiv R_P \pmod{(X - a_P)^{v_P(D)}}$. Este B claramente satisfaz (1) e (2); (3) é devido ao fato de que os fatores de A são co-primos entre si. A unicidade segue-se da prova. Finalmente mostramos que D é o mdc dos divisores $\mathrm{div}(A)$ e $\mathrm{div}(B - y)$.

Seja $P = (a, b)$ tal que $P = \sigma(P)$; temos que $v_P(B - y) \geq 1$ por (2) e que $v_P(A) = 2$. Para mostrar que de fato $v_P(B-y) = 1$ consideremos a função $N = N(X) := B^2 + Bh(X) - f(X) = (B-y)(B+y+h)$; logo (2) implica $v_P(N) \geq 1$. Afirmamos que $v_P(N) = 1$; para isto, bastará mostrar que $N'(a) \neq 0$. Temos $N'(X) = 2BB' + B'h(X) + Bh(X)' - f(X)'$. Logo avaliando em P, usando (2) e o fato que $b = -b - h(a)$, obtemos $N'(a) = bh'(a) - f'(a) \neq 0$, pois $\mathbf{H}$ é não singular em P. Obtemos assim que $v_P(D) = 1$.

Seja P agora tal que $P \neq \sigma(P)$. De (3), $(R-y)(R+y+h(X)) = R^2 + Rh(X) - f(X) = Ar$ onde $v_P(r) \geq 0$. Logo $v_P(B-y) = v_P(A) + v_P(r)$, pois P não é ponto fixo. Então $v_P(D) = n_P$ e portanto, o $\mathrm{mdc}(\mathrm{div}(A), \mathrm{div}(B - y)) = \sum_{P \neq \mathcal{O}} n_P P - m\mathcal{O} = D$. □

Observação 4.10. *Sejam A e B dois polinômios satisfazendo as condições (1) e (3) do lema anterior. Então o divisor $D := \mathrm{mdc}(\mathrm{div}(A), \mathrm{div}(B - y))$ é semi-reduzido.*

Demonstração. Seja $P = (a_P, b_P) \in \mathrm{Sup}(\mathrm{div}(A))$. Para $P \neq \sigma(P)$ e de (3) temos que $v_P(B - y) = v_P(A) + v_P(s)$ onde $v_P(s) \geq 0$, logo $v_P(B - y) \geq v_P(A)$ e $v_{\sigma(P)}(B - y) = 0$. Para $P = \sigma(P)$ e da condição (3) segue-se $(B - y)(P) = 0$, logo $v_P(B - y) \geq 1$. Afirmamos que $v_P(B-y) = 1$. Dado $N(X) = (B - y)(B + y + h) = B^2 + Bh - f$; temos que $N(a_P) = 0$ e $N'(a_P) \neq 0$, pois $P \neq \mathcal{O}$ não é ponto singular da curva. □

Teorema 4.11. *Existe um único divisor reduzido D_1 tal que $D \sim D_1$.*

Demonstração. **Existência.** Podemos supor $D = D_0 := D_0^0 - m\mathcal{O}$ semi-reduzido (Lema 4.8) tal que $\sum_{P \neq \mathcal{O}} v_P(D_0) \geq g+1$ onde g é o gênero de $\mathbf{H}$. Assim, podemos escolher $P_1, \ldots, P_{g+1}$ do suporte de D (não necessariamente diferentes) e considerar o divisor semi-reduzido:

$$E = E_0 := P_1 + \ldots + P_{g+1} - (g+1)\mathcal{O}.$$

Pelo lema anterior, existem polinômios $A = A_0$ e $B = B_0$ tal que $\mathrm{div}(B - y) = P_1 + \ldots + P_{g+1} + Q_1 + \ldots + Q_g - (2g+1)\mathcal{O}$. Seja $D = F_0 + P_1 + \ldots + P_{g+1} - m\mathcal{O}$. Logo

$$D - \mathrm{div}(B - y) = F_0 - Q_1 - \ldots - Q_g - (m - 2g - 1)\mathcal{O} \sim D_1 := D_0^1 - (m-1)\mathcal{O}\,,$$

sendo que D_1 pode ser assumido semi-reduzido. Agora a prova de existência termina por indução sobre m, pois o grau do novo divisor construído, no mínimo diminui em 1.

Unicidade. Sejam $D_1 \neq D_2$ divisores reduzidos tal que $D \sim D_1$ e $D \sim D_2$. Como $\deg(D_1 - D_2) = 0$, pelo Lema (4.8), $D_1 - D_2 \sim D_3$ onde D_3 é o divisor semi-reduzido obtido da prova do lema. Seja $P \in \mathbf{H}$ tal que $m := v_P(D_1) \neq n := v_P(D_2)$; considerando $D_1 - D_2$ ou $D_2 - D_1$, podemos supor que $m \geq 1$ e que algum dos seguintes casos podem ocorrer:

(1) $n = 0$ e $v_{\sigma(P)}(D_2) = 0$;

(2) $1 \leq n < m$;

(3) $1 \leq v_{\sigma(P)}(D_2) \leq m$.

Logo pela escolha de D_3 temos que $v_P(D_3) \geq 1$ para todos os casos acima. De fato, nos Casos (1) e (2) $v_P(D_3) = (m - n) \geq 1$; no caso (3) $\sigma(P) \neq P$; logo da propriedade $P + \sigma(P) \sim 2\mathcal{O}$ e da contrução de D_3 segue-se a afirmação. Agora como $D_3 \sim 0$, existe $r \in \bar{K}(\mathbf{H})$ tal que $D_3 = \mathrm{div}(r)$; pela definição de D_3, o único polo de r é $\mathcal{O}$ e assim $r = A(X) + B(X)y$ onde $A(X), B(X) \in \bar{K}[X]$. Para $i = 1, 2, 3$ escrevamos $D_i = \sum_{P \neq \mathcal{O}} v_{P(i)}(D_i)P - d_i\mathcal{O}$, onde $d_i := (\sum_{P \neq \mathcal{O}} v_{P(i)}(D_i))$. Pela definição de divisor reduzido, $d_1 \leq g$ e $d_2 \leq g$; pelo tanto fica claro que $d_3 \leq 2g$.

Afirmação : $B(X) = 0$. Suponha que $B(X) \neq 0$; como $v_{\mathcal{O}}(A(X) \neq v_{\mathcal{O}}(B(X)y)$, então $v_{\mathcal{O}}(r) = \min\{v_{\mathcal{O}}(A(X)), v_{\mathcal{O}}(B(X)y\}$. Temos que $v_{\mathcal{O}}(B(X)y) < v_{\mathcal{O}}(A(X))$, pois do contrário, $-2\deg(B(X)) - (2g+1) > v_{\mathcal{O}}(A(X)) = v_{\mathcal{O}}(r) = -d_3 \geq -2g$ o qual é uma contradição. Portanto temos, $v_{\mathcal{O}}(B(X)) - (2g+1) = v_{\mathcal{O}}(r) = -d_3$ e assim $d_3 \geq 2g + 1 + 2\deg(B(X))$. Logo $r = A(X)$ com $\deg(A(X)) \geq 1$. Tome $Q = (a, b) \in \mathbf{H}$ tal que $A(a) = 0$; logo pela definição de $\sigma(Q)$, temos que $Q, \sigma(Q) \in \mathrm{Sup}(D_3)$ o qual é contraditório com a definição de D_3. □

4.2 O Jacobiano de H

Nesta seção definiremos o Jacobiano de uma curva hiperelíptica $\mathbf{H}$. O *Jacobiano* $\mathcal{J} = \mathcal{J}_{\mathbf{H}}$ de $\mathbf{H}$ é o grupo

$$\mathcal{J} = \mathrm{Div}^0/P\,,$$

onde $\mathrm{Div}^0 = Div^0_K(\mathbf{H})$ é o grupo de divisores de grau zero sobre $\mathbf{H}$ e $P = P_K(\mathbf{H})$ é o subgrupo de divisores principais de Div^0. A maneira de comentário, $\mathcal{J}$ pode ser munido de uma estrutura de variedade algébrica de dimensão g onde as operações de soma e inversa de $\mathcal{J}$ sejam compatíveis com a estrutura algébrica. Assim, podemos considerar $\mathcal{J}$ como uma variedade Abeliana.

4.2.1 Pontos racionais do Jacobiano

Para aplicações criptográficas usando o método Diffie-Hellman ou ElGamal, é de interesse o estudo de subgrupos finitos do Jacobiano da curva hiperelíptica escolhida. Em nosso caso, consideraremos subgrupos finitos do Jacobiano da curva definida sobre $K = \mathbb{F}_q$. É um fato que $\mathcal{J}$ está também definido sobre K. Seja L uma extensão finita de K e D um divisor de grau zero definido sobre L. Pelo Teorema (4.11) existe um único divisor reduzido $D_1 = \sum_P v_P(D_1)P$ tal que $D \sim D_1$ e pela denifinição de divisor reduzido temos que $\sum_P v_P(D_1) \leq g$ onde g é o gênero da curva. Assim, existe um número finito de possibilidades para obter divisores reduzidos, logo obtemos um número finito de elementos do Jacobiano; existem também as fórmulas explícitas para calcular este. Seja $K := \mathbb{F}_q$, $L = \mathbb{F}_{q^n}$ e $N_L := \#\mathcal{J}_{\mathbf{H}}(L)$. Se sabe que N_L pode-se calcular a partir dos inteiros α_i em (4.4). De fato temos [39, Teorema V1.15]

$$N_L = \prod_{i=1}^{g}(1-\beta_i^n)(1-\bar{\beta}_i^n)\,. \tag{4.8}$$

Logo, usando que $|\alpha_i| = q^{n/2}$ se obtém:

$$(q^{n/2}-1)^{2g} \leq N_L \leq (q^{n/2}+1)^{2g}\,.$$

Em particular, N_L se comporta assintóticamente como q^{ng}.

Exemplo 4.12. Escolhendo a curva do Exemplo (4.3) temos que: Para $L = \mathbb{F}_{q^n}$,

$$N_L := \#\mathcal{J}_{\mathbf{H}}(L) = \begin{cases} 2^{2n} + 2^n + 1 & \text{se } n \equiv 1,5 \pmod 6 \\ (2^n + 2^{n/2} + 1)^2 & \text{se } n \equiv 2,4 \pmod 6 \\ (2^n - 1)^2 & \text{se } n \equiv 3 \pmod 6 \\ (2^{n/2} - 1)^4 & \text{se } n \equiv 0 \pmod 6 \end{cases}$$

Seja $L = \bar{K}$. Pelo Teorema 4.11 a cada classe $[D] \in \mathcal{J}_{\mathbf{H}}(\bar{K})$, lhe corresponde um único divisor reduzido D_R. De fato, o mapa $[D] \longmapsto D_R$ define um sistema completo de representantes para os elementos de $\mathcal{J}_{\mathbf{H}}(\bar{K})$.

4.2.2 Soma de Divisores no Jacobiano

Aqui apresentaremos o algoritmo de Koblitz [19], que como foi dito na introdução, este apresenta uma generalização dos algoritmos de Cantor [7] para computar eficientemente a soma de dois divisores reduzidos no $\mathcal{J}_{\mathbf{H}}(L)$, o qual só fez para o caso em que a característica do corpo era diferente de dois e $h(X) = 0$. A seguir descrevemos em forma geral estes algoritmos.

- **Algoritmo 1** Dados dois divisores $[D_1], [D_2] \in \mathcal{J}_{\mathbf{H}}(K)$ semi-reduzidos, ao aplicar o algoritmo este devolve um divisor D_0 semi-reduzido, equivalente ao divisor $D_1 + D_2$.
- **Algoritmo 2** Dado um divisor semi-reduzido D_0 de grau ℓ_0, ao aplicar o algoritmo, este devolve um divisor D semi-reduzido tal que $D_0 \sim D$ e $\ell \leq \ell_0$, onde ℓ é o grau de D. Aplicando sucessivamente este algoritmo achamos um divisor reduzido equivalente a D_0.

A seguir os passos a efetuar para cada algoritmo:

Algoritmo 1. Sejam $D_1 = \text{div}(A_1, B_1)$ e $D_2 = \text{div}(A_2, B_2)$ divisores semi-reduzidos sobre a curva $Y^2 + h(X)Y = f(X)$ definidos sobre K, onde $h, f \in K[X]$ e $A_1, B_1, A_2, B_2 \in K[X]$. A seguir, descrevemos os passos formalmente para aplicar este algoritmo.

(1) Usando o algoritmo de Euclides sobre $K[X]$, achamos $d_1, e_1, e_2 \in K[X]$ tal que:

$$d_1 = \text{mdc}(A_1, A_2) \text{ e } d_1 = e_1 A_1 + e_2 A_2 \,,$$

(2) Usando outra vez o algoritmo de Euclides, achamos $d, c_1, c_2 \in K[X]$ tal que:

$$d = \text{mdc}(d_1, B_1 + B_2 + h) \text{ e } d = c_1 d_1 + c_2(B_1 + B_2 + h) \,,$$

(3) Sejam $s_1 = c_1 e_1$, $s_2 = c_2 e_2$ e $s_3 = c_2$, então temos que:

$$d = s_1 A_1 + s_2 A_2 + s_3(B_1 + B_2 + h)\,, \tag{4.9}$$

(4) O divisor $D' = \mathrm{div}(A', B')$ é o divisor semi-reduzido equivalente a $D_1 + D_2$, tal que:

$$A' = A_1 A_2 / d^2\,, \text{e} \tag{4.10}$$

$$B' = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d} \pmod{A}\,. \tag{4.11}$$

A seguir, mostramos que o divisor D' acima, é um divisor semi-reduzido e equivalente a $D_1 + D_2$, a prova está dividida em três partes:

- Mostremos que A' e B' são funções polinomiais. Claramente A' é uma função polinomial, pois d divide A_1 e A_2, então d^2 divide $A_1 A_2$. Usando a equação (4.9), podemos escrever $B' = \dfrac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d}$ como sendo

$$\frac{B_2(d - s_2 A_2 - s_3(B_1 + B_2 + h)) + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d} =$$

$$B_2 + \frac{s_2 A_2(B_2 - B_1) - s_3(B_2^2 + B_2 h - f)}{d}\,.$$

  Pela definição de D_2 temos que A_2 divide $B_2^2 + B_2 h - f$, logo B' é também uma função polinomial.

- Agora mostramos que $D' = \mathrm{div}(A', B')$ é um divisor semi-reduzido. Seja

$$B' = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f)}{d} + sA'$$

  com $s \in K[X]$. Subtraindo y a cada lado temos que

$$(B' - y) = \frac{s_1 A_1 B_2 + s_2 A_2 B_1 + s_3(B_1 B_2 + f) - yd}{d} + sA' =$$

$$\frac{s_1 A_1(B_2 - y) + s_2 A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y)}{d} + sA'\,,$$

  e como $(B' - y)\sigma(B' - y) = (B' - y)(B' + y + h) = B'^2 + B'h - f$, então podemos ver que para A' dividir $B'^2 + B'h - f$, é suficiente mostrar que o produto $A_1 A_2$ divide o produto de $s_1 A_1(B_2 - y) + s_2 A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y)$ com $\sigma(s_1 A_1(B_2 - y) + s_2 A_2(B_1 - y) - s_3(B_1 - y)(B_2 - y))$; isto é imediato, pois A_1 divide $B_1^2 + B_1 h - f = (B_1 - y)\sigma(B_1 - y)$ e A_2 divide $B_2^2 + B_2 h - f = (B_2 - y)\sigma(B_2 - y)$. Portanto, pela Observação (4.10) o $\mathrm{div}(A', B')$ é um divisor semi-reduzido.

- Por último, mostramos que $D' \sim D_1 + D_2$. Seja $P = (a, b) \in \mathbf{H}(L)$, temos dois casos a considerar:

  (1) Se $P = (a, b) \neq \sigma(P)$;

  (1.a) Suponhamos que $v_P(D_1) = m_1, v_{\sigma(P)}(D_1) = 0$, $v_P(D_2) = m_2$ e $v_{\sigma(P)}(D_2) = 0$, onde $m_1, m_2 \geq 0$. Logo, $v_P(B_1 - y) \geq m_1$ e $v_P(B_2 - y) \geq m_2$. Se $m_1 = 0$ ou $m_2 = 0$, então $v_P(d_1) = 0$, implicando que $v_P(d) = 0$ e $v_P(A') = m_1 + m_2$. Se $m_1, m_2 \geq 1$, então desde que $(B_1 + B_2 + h)(a) = 2b + h(a) \neq 0$ temos $v_P(d) = 0$ e $v_P(A') = m_1 + m_2$; da equação (4.11) segue que $v_P(B' - y) \geq \min\{m_1 + m_2, m_2 + m_1, m_1 + m_2\} = m_1 + m_2$. Portanto, $v_P(D') = m_1 + m_2$.

  (1.b) Suponha que $v_P(D_1) = m_1$ e $v_{\sigma(P)}(D_2) = m_2$, onde $m_1 \geq m_2 \geq 1$. Nós temos que $v_P(A_1) = m_1$, $v_P(A_2) = m_2$, $v_P(d_1) = m_2$, $v_P(B_1 - y) \geq m_1$, $v_P(B_2 - y) = 0$ e $v_{\sigma(P)}(B_2 - y) \geq m_2$. A última desigualdade implica que $v_P(B_2 + h + y) \geq m_2$ e daqui $v_P(B_1 + B_2 + h) \geq m_2$ ou $(B_1 + B_2 + h) = 0$. Logo, $v_P(d) = m_2$ e $v_P(A') = m_1 - m_2$. Da equação (4.11) temos $v_P(B' - y) \geq \min\{m_1 + 0, m_2 + m_1, m_1 + 0\} - m_2 = m_1 - m_2$. Portanto $v_P(D') = m_1 - m_2$.

  (2) Se $P = \sigma(P)$;

  (2.a) Suponhamos que $v_P(D_1) = 1$ e $v_P(D_2) = 1$. Então, $v_P(A_1) = 2$, $v_P(A_2) = 2$ e $v_P(d_1) = 2$. Temos que $(B_1 + B_2 + h)(a) = 2b + h(a) = 0$, logo $v_P(B_1 + B_2 + h) \geq 2$ ou $(B_1 + B_2 + h) = 0$, então $v_P(d) = 2$ e $v_P(A') = 0$. Portanto $v_P(D') = 0$

  (2.b) Suponhamos que $v_P(D_1) = 1$ e $v_P(D_2) = 0$, logo $v_P(A_1) = 2$, $v_P(A_2) = 0$. Daqui temos $v_P(d_1) = v_P(d) = 0$ e $v_P(A') = 2$. Como $v_P(A_2) = 0$ e da equação (4.11) temos $v_P(B' - y) \geq 1$. Da equação (4.11) podemos dizer que $v_P(B' - y) \geq 2$ só se $v_P(s_2 A_2 + s_3(B_2 - y)) \geq 1$. Se isto acontece, então $v_P(s_2 A_2 + s_3(B_2 + h + y)) \geq 1$ (ou $s_2 A_2 + s_3(B_1 + B_2 + h) = 0$). Isto implica que da equação (4.9) $v_P(d) \geq 1$, contradição. Logo $v_P(B' - y) = 1$ e portanto $v_P(D') = 1$

Exemplo 4.13. Consideremos a curva hiperelíptica $\mathbf{H}$ definida por $Y^2 + (X^2 + X)Y = X^5 + X^3 + 1$, de gênero 2 sobre o corpo $\mathbb{F}_{2^5} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$, ver Exemplo (4.6).

(1) Sejam $P = (\alpha^{30}, 0)$, $\sigma(P) = (\alpha^{30}, \alpha^{16})$, $Q_1 = (0, 1)$ e $Q_2 = (1, 1)$. Definamos os divisores reduzidos $D_1 = P + Q_1 - 2\mathcal{O}$ e $D_2 = \sigma(P) + Q_2 - 2\mathcal{O}$. Primeiro achamos os polinômios $A_1, B_1, A_2, B_2 \in \mathbb{F}_{2^5}[X]$ tais que $D_1 = \mathrm{div}(A_1, B_1)$ e $D_2 = \mathrm{div}(A_2, B_2)$.

Então temos que $A_1 = \prod_{P \in \mathrm{Sup}(D_1)}(X - a_P)^{v_P(D_1)}$, logo $A_1 = X(X + \alpha^{30})$. Usando as condições do lema 4.9, obtemos $B_1 = \alpha X + 1$. Análogamente, temos que $A_2 = (X + \alpha^{30})(X + 1)$ e $B_2 = \alpha^{23}X + \alpha^{12}$. A seguir, aplicamos o Algoritmo (1) para achar o divisor semi-reduzido equivalente à soma de D_1 e D_2. Logo, calculamos $d_1 = \mathrm{mdc}(A_1, A_2) = X + \alpha^{30}$ tal que $d_1 = A_1 + A_2$ e $d = \mathrm{mdc}(d_1, B_1 + B_2 + h) = X + \alpha^{30}$, assim $d = d_1$. Então,

$$A' = A_1A_2/d^2 = X(X + 1)\,, \text{e } B' \equiv 1 \pmod{A'}\,.$$

Dos polinômios acima, segue-se

$$\mathrm{div}(A') = 2Q_1 + 2Q_2 - 4\mathcal{O}\,, \text{e}$$

$$\mathrm{div}(B' - y) = \mathrm{div}(y + 1) = Q_1 + Q_2 + \sum_{i=1}^{3} P_i - 5\mathcal{O}\,;$$

tal que $P_i \in \mathbf{H}(\bar{\mathbb{F}}_2) \neq Q_1, Q_2$. Portanto, $D' = \mathrm{div}(A', B') = Q_1 + Q_2 - 2\mathcal{O}$.

(2) Sejam $D_1 = P + Q_1 - 2\mathcal{O}$ e $D_2 = Q_1 + Q_2 - 2\mathcal{O}$. Então $D_1 = \mathrm{div}(A_1, B_1)$ e $D_2 = \mathrm{div}(A_2, B_2)$ onde $A_1 = X(X + \alpha^{30})$, $B_1 = \alpha X + 1$, $A_2 = X(X + 1)$ e $B_2 = 1$. Logo, como $d = d_1 = X$ obtemos

$$A' = (X + \alpha^{30})(X + 1)\,, \text{e } B' \equiv \alpha^{14}X + \alpha^{13} \pmod{A'}\,.$$

Daqui,

$$\mathrm{div}(A') = 2Q_2 + P + \sigma(P) - 4\mathcal{O}\,, \text{e}$$

$$\mathrm{div}(B' - y) = Q_2 + P + \sum_{i=1}^{3} P_i - 5\mathcal{O}\,, \text{tal que } P_i \neq Q_2, P, \sigma(P) \text{ e } P_i \in \mathbf{H}(\bar{\mathbb{F}}_2)$$

portanto, $D' = \mathrm{div}(A', B') = Q_2 + P - 2\mathcal{O}$.

Exemplo 4.14. Consideremos a curva hiperelíptica $\mathbf{H}$ definida por $Y^2 + XY = X^5 + 5X^4 + 6X^2 + X + 3$, de gênero 2 sobre o corpo $\mathbb{F}_7$. O conjunto de pontos racionais desta curva é:

$$\mathbf{H}(\mathbb{F}_7) = \{\mathcal{O}, (1,1), (1,5), (2,2), (2,3), (5,3), (5,6), (6,4)\}\,,$$

onde o ponto $(6,4)$ é um ponto fixo.

(1) Sejam $D_1 = \mathrm{div}(A_1, B_1)$ e $D_2 = \mathrm{div}(A_2, B_2)$ onde $A_1 = X^2 + 6 = (X+1)(X-1)$, $B_1 = 2X + 6$, $A_2 = X^2 + 4X + 2 = (X-1)(X+5)$, $B_2 = 4X + 1$. Calculemos o divisor D' equivalente à soma de D_1 e D_2. Então, $d_1 = \mathrm{mdc}(A_1, A_2) = X - 1$, logo $d_1 = 5A_1 + 2A_2$ e $d = \mathrm{mdc}(d_1, B_1 + B_2 + h) = \mathrm{mdc}(X-1, 0) = X - 1 = d_1$. Assim,

$$A' = (X+1)(X+5)\,, \text{e}\, B' \equiv 4X + 1 \pmod{A'}\,;$$

logo,

$$\mathrm{div}(A') = 2(6,4) + (2,2) + (2,3) - 4\mathcal{O}\,, \text{e}$$

$$\mathrm{div}(B' - y) = (6,4) + (2,2) + (1,5) + \sum_{i=1}^{2} P_i - 5\mathcal{O}\,.$$

Portanto $D' = \mathrm{div}(A', B') = Q + P - 2\mathcal{O}$

Algoritmo 2 Seja $D' = \mathrm{div}(A', B')$ um divisor semi-reduzido; o procedimento a seguir acha um divisor $D = \mathrm{div}(A, B)$ reduzido e equivalente a D' tal que $\deg(A) < \deg(A')$. Aplicando sucessivamente este algoritmo, achamos um divisor reduzido $\widetilde{D} = \mathrm{div}(\widetilde{a}, \widetilde{b})$ equivalente a D' tais que $\deg(\widetilde{a}) \leq g$. Então,

$$A = (f - hB' - B'^2)/A'\,, \text{e} \tag{4.12}$$

$$B = (-h - B') \pmod{A}\,, \tag{4.13}$$

se c é o coeficiente líder de A, então $A = c^{-1}A$. A seguir, mostramos que o Algoritmo (2) devolve um divisor equivalente a D' e de menor grau.

(1) Mostremos que $\deg(A) \leq \deg(A')$. Seja $m = \deg(A')$ e $n = \deg(B')$ onde $m > n$ e $m \geq g+1$. Logo $\deg(A) = \max\{2g+1, 2n\} - m$. Se $m = g+1$ então $\deg(A) = g < \deg(A')$. Se $m > g+1$ então $\max\{2g+1, 2n\} \leq 2(m-1)$, logo $\deg(A) \leq (m-2) \leq \deg(A')$.

(2) $D = \mathrm{div}(A, B)$ é um divisor semi-reduzido. De (4.12) $f - B'h - B'^2 = AA'$, então passando módulo A a ambos lados e aplicando (4.13) temos que $f + (B+h)h - (B+h)^2 \equiv 0 \pmod{A}$. Simplificando fica $f - Bh - B^2 \equiv \pmod{A}$. Portanto A divide $(f - Bh - B^2)$ e aplicando o lema (4.9) concluímos que $D = \mathrm{div}(A, B)$ é um divisor semi-reduzido.

(3) Escrevamos o divisor D' da seguinte forma:

$$D' = \sum_{P \neq \sigma(P)} n_P P + \sum_{P = \sigma(P)} P - m\mathcal{O}$$

Pela prova do lema (4.9) podemos escrever

$$\operatorname{div}(A') = \sum_{P\neq\sigma(P)} n_P P + \sum_{P\neq\sigma(P)} n_P\sigma(P) + \sum_{P=\sigma(P)} 2P - (*)\mathcal{O},$$

$$\operatorname{div}(B'-y) = \sum_{P\neq\sigma(P)} m_P P + \sum_{P=\sigma(P)} P + \sum_{P\in\mathbf{H}'} s_P P - (*)\mathcal{O},$$

onde $m_P \geq n_P$, $s_P \geq 1$ e $\mathbf{H}' = \mathbf{H} \setminus (\operatorname{Sup}(D') \cup \{\sigma(P) : P \in \operatorname{Sup}(D')\} \cup \{\mathcal{O}\})$. Como $(B'^2 + B'h - f) = (B'-y)(B'+y+h)$ temos que:
$\operatorname{div}(B'^2 + B'h - f) =$

$$\sum_{P\neq\sigma(P)} m_P P + \sum_{P\neq\sigma(P)} m_P\sigma(P) + \sum_{P=\sigma(P)} 2P + \sum_{P\in\mathbf{H}'} s_P P + \sum_{P\in\mathbf{H}'} s_P\sigma(P) - (*)\mathcal{O},$$

assim, usando a equação (4.12) temos

$$\operatorname{div}(A) = \operatorname{div}(B'^2 + B'h - f) - \operatorname{div}(A') =$$

$$\sum_{P\neq\sigma(P)} t_P P + \sum_{P\neq\sigma(P)} t_P\sigma(P) + \sum_{P\in\mathbf{H}'} s_P P + \sum_{P\in\mathbf{H}'} s_P\sigma(P) - (*)\mathcal{O},$$

onde $t_P = m_P - n_P$. Como $B = -h - B' + sA$ onde $s \in K[X]$. Para $P = (a,b) \in \operatorname{Sup}(\operatorname{div}(A))$, temos que $B(a) = -h(a) - B'(a) + s(a)A(a) = -h(a) - b$. Então

$$\operatorname{div}(B-y) = \sum_{P\neq\sigma(P)} r_P\sigma(P) + \sum_{P\in\mathbf{H}'} w_P\sigma(P) + \sum_{P\in\tilde{\mathbf{H}}} z_P P - (*)\mathcal{O},$$

onde $r_P \geq t_P$, $w_P \geq s_P$ e $\tilde{\mathbf{H}}$ é o conjunto $\mathbf{H} \setminus \operatorname{Sup}(\operatorname{div}(B-y))$. Logo,
$\operatorname{div}(A,B) =$

$$\sum_{P\neq\sigma(P)} t_P\sigma(P) + \sum_{P\in\mathbf{H}'} s_P\sigma(P) - (*)\mathcal{O} \sim -\sum_{P\neq\sigma(P)} t_P P - \sum_{P\in\mathbf{H}'} s_P P - (*)\mathcal{O} = D - \operatorname{div}(B'-y).$$

Portanto $D \sim D'$. Notemos que o divisor $D = \operatorname{div}(A,B)$ é reduzido se e somente se $\deg(A) \leq g$, onde g é o gênero da curva.

Exemplo 4.15. Seja a curva $H : Y^2 + (X^2+X)Y = X^5 + X^3 + 1$ de gênero 2 definida sobre $\mathbb{F}_{2^5}$. Consideremos o divisor semi-reduzido $D' = (0,1) + (1,1) + (\alpha^5, \alpha^{15}) - 3\mathcal{O}$. Então $D' = \operatorname{div}(A', B')$ onde $A' = X(X+1)(X+\alpha^5)$ e $B' = \alpha^{17}X^2 + \alpha^{17}X + 1$. Agora, calculamos os polinômios A e B tais que $D = \operatorname{div}(A,B)$ é o divisor reduzido equivalente a D'. Então,

$$A = (X+\alpha^{28})(X+\alpha^{29}), \text{e } B \equiv \alpha^{23}X + \alpha^{21} \pmod{A}.$$

Logo,

$$\mathrm{div}(A) = (\alpha^{28}, \alpha^7) + (\alpha^{28}, \alpha^{16}) + (\alpha^{29}, 0) + (\alpha^{29}, \alpha) - 4\mathcal{O}\,\mathrm{e}$$

$$\mathrm{div}(B + y) = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) + \sum_{i=1}^{3} P_i - 5\mathcal{O}\,.$$

Portanto $D = \mathrm{div}(A, B) = (\alpha^{28}, \alpha^7) + (\alpha^{29}, 0) - 2\mathcal{O}$.

Exemplo 4.16. Considerando a mesma curva do Exemplo (4.14); seja o divisor semi-reduzido $D' = \mathrm{div}(A', B') = \mathrm{div}(X^7 + 2X^6 + 3X^5 + 6X^3 + 4X + 5, 5X^6 + 5X^5 + 6X^4 + 4X^3 + 5X^2 + 4)$. Achemos o divisor reduzido D equivalente a D'. Aplicando o Algoritmo (2) a D' obtemos o divisor $D'_1 = \mathrm{div}(A'_1, B'_1) = \mathrm{div}(x^5 + 6x^3 + 6x^2 + 6x + 1, 3x^4 + 6x^2 + 6x + 1)$. Como o grau de A'_1 e $5 \geq g = 2$ o gênero da curva, então continuamos aplicando o algoritmo até ter um divisor reduzido. Assim,

$$D = \mathrm{div}(A, B) = \mathrm{div}(x^2 + x + 5, 4x + 4)\,.$$

4.2.3 Automorfismo de Frobenius

O automorfismo de Frobenius pode ser eficientemente usado para realizar operações com os elementos no Jacobiano. A saber, seja

$$\phi : \bar{\mathbb{F}}_q \longrightarrow \bar{\mathbb{F}}_q \text{ tal que } x \mapsto x^q\,,$$

o automorfismo de Frobenius. Este automorfismo pode ser estendido sobre o Jacobiano de uma curva hiperelíptica definida sobre $\mathbb{F}_q$. Assim, para $P = (x, y) \in \mathbf{H}(\bar{\mathbb{F}}_q)$ seja $P^\phi = (x^q, y^q)$ e $\mathcal{O}^\phi = \mathcal{O}$. Para um divisor $D = \sum_{P \in \mathbf{H}} v_P(D)P$ de $\mathbf{H}$ definimos $D^\phi = \sum_{P \in \mathbf{H}} v_P(D)P^\phi$. A seguir, mostramos uma propriedade importante da ação do Frobenius sobre divisores semi-reduzidos.

Teorema 4.17. *Seja D um divisor semi-reduzido de $\mathbf{H}$ definido sobre $\mathbb{F}_{q^n}$, então o divisor D^ϕ é semi-reduzido e está definido sobre $\mathbb{F}_{q^n}$. Além disso, se $D = \mathrm{div}(A, B)$ com $A, B \in \mathbb{F}_{q^n}[X]$ então $D^\phi = \mathrm{div}(A^\phi, B^\phi)$.*

Demonstração. Seja $D = \sum_{P \neq \mathcal{O}} v_P(D)P - m\mathcal{O}$ onde $m = \sum_{P \neq \mathcal{O}} v_P(D)$ um divisor semi-reduzido definido sobre $\mathbb{F}_{q^n}$. Como ϕ é automorfismo e D é um divisor semi-reduzido, então D^ϕ é semi-reduzido. Como ϕ comuta com todo $\gamma \in \mathrm{Aut}(\bar{\mathbb{F}}_q : \mathbb{F}_{q^n})$, segui que $(D^\phi)^\gamma = (D^\gamma)^\phi = D^\phi$, isto é, D^ϕ está definido sobre $\mathbb{F}_{q^n}$. Seja $A(X) = \prod_{P \in \mathrm{Sup}(D)} (X - a_P)^{n_P} \in \mathbb{F}_{q^n}[X]$, onde

$n_P = v_P(D)$ e $B(X)$ é o único polinômio que satisfaz as condições do Lema (4.9) tal que $D = \mathrm{mdc}(\mathrm{div}(A(X)), \mathrm{div}(B(X) - y)) = \mathrm{div}(A, B)$. Então

$$D^\phi = \sum_{P \neq \mathcal{O}} v_P(D) P^\phi - m\mathcal{O} = \mathrm{div}(\bar{A}, \bar{B}),$$

onde $\bar{A} = \prod_{P \in \mathrm{Sup}(D)} (X - a_P^q)^{n_P} \in \mathbb{F}_{q^n}[X]$ e $\bar{B} \in \mathbb{F}_{q^n}[X]$ é o único polinômio satisfazendo o Lema (4.9). Podemos observar que $A^\phi = \prod_{P \in \mathrm{Sup}(D)} (X - a_P^q)^{n_P} = \bar{A}$, logo resta mostrar que $B^\phi = \bar{B}$. Como $\deg(B) < \deg(A)$ então $\deg(B^\phi) < \deg(A^\phi) = \deg(\bar{A})$, além disso, $B^\phi(a_P^q) = (B(a_P))^q = b_P^q$ para cada $P \in \mathrm{Sup}(D)$. Por último, A^ϕ divide $(B^2 + Bh - f)^\phi$, pois A divide $B^2 + Bh - f$ e $h, f \in \mathbb{F}_q[X]$. Como $\bar{B}$ é o único polinômio com essas três propriedades para D^ϕ e $\bar{A} = A^\phi$, então $B^\phi = \bar{B}$. □

Como conseqüência do Teorema, dado $D = \mathrm{div}(A, B) \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$ um divisor reduzido, então a ação do Frobenius sobre D é dada por $D^\phi = \mathrm{div}(A^\phi, B^\phi)$ um divisor reduzido. Assim, sejam $A = \sum_{i=0}^{k} a_i X^i \in \mathbb{F}_{q^n}[X]$ e $B = \sum_{i=0}^{k'} b_i X^i \in \mathbb{F}_{q^n}[X]$ representações explícitas de A e B, então $A^\phi = \sum_{i=0}^{k} a_i^q X^i$ e $B^\phi = \sum_{i=0}^{k'} b_i^q X^i$. Na prática, se representamos os elementos de $\mathbb{F}_{q^n}$ usando Base Normal (ver Apêndice A), então A^ϕ e B^ϕ podem ser determinados por simples *shifting* (desplazamento) na representação da base normal de cada coeficiente a_i, b_i para calcular D^ϕ. Desta forma o custo para operar elementos do Jacobiano é menor, implicando maior eficiência do algoritmo.

4.3 Criptossistemas usando Curvas Hiperelípticas

Como já foi mencionado, a implementação de novos grupos em criptossistemas de chave pública que baseiam a segurança no problema do logaritmo discreto (por exemplo, Diffie-Hellman e ElGamal) é cada vez mais importante para lograr um nível maior de segurança. O Jacobiano de curvas hiperelípticas é sugerido por Koblitz [19] como um grupo com as características adequadas para aplicar na criptografia. Uma das características está relacionada com a intratabilidade computacional do logaritmo discreto sobre este grupo, que definiremos a seguir.

Definição 4.18. O *Problema do logaritmo Discreto sobre o Jacobiano de Curvas Hiperelípticas* $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$ (HECDLP) é definido em forma análoga ao ECDLP (problema do logaritmo discreto sobre uma curva elíptica); assim, dados dois divisores D_1 e D_2 definidos sobre $\mathbb{F}_{q^n}$,

determinar um inteiro m, se existe, tal que $[D_2] = m[D_1]$ em $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$, ou equivalentemente, $mD_1 - D_2 \in P_{\mathbf{H}}(\mathbb{F}_{q^n})$ é o que se chama o HECDLP.

Assim, podemos definir em forma natural o sistema de troca de chaves Diffie-Hellman entre os usuários **A** e **B**, sobre o Jacobiano de uma curva hiperelíptica definida em um corpo finito. Os parâmetros públicos são: o corpo finito $\mathbb{F}_{q^n}$, a equação da curva hiperelíptica **H** e um elemento base $D_0 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$. **A** escolhe um inteiro $m_{\mathbf{A}}$, sua chave privada e envia para **B** o ponto $m_{\mathbf{A}}D_0$; análogamente, **B** envia $m_{\mathbf{B}}D_0$, onde $m_{\mathbf{B}}$ é sua chave privada. Logo o segredo compartilhado será o divisor $m_{\mathbf{A}}m_{\mathbf{B}}D_0 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$.

Uma condição importante para a escolha de uma curva hiperelíptica está relacionada com a dificuldade de resolver o problema do logaritmo discreto sobre seu Jacobiano. Assim, a seguir mostramos o ataque index-calculus para o problema do logaritmo discreto, visto na Subseção (2.3.1) para corpos finitos, implementado para o Jacobiano de curvas hiperelípticas [41].

4.3.1 Ataque Index-Calculus para resolver o HECDLP

No 2000, Gaudry, Hess e Smart [12] mostraram como o problema do logaritmo discreto (DLP) em curvas elípticas definidas sobre $\mathbb{F}_{2^n}$ se podia reduzir ao DLP no Jacobiano de uma curva hiperelíptica **H** definida sobre um subcorpo de $\mathbb{F}_{2^n}$. Assim, o estudo dos criptossistemas hiperelípticos e o HECDLP, poderiam ser usados para atacar os criptossistemas elípticos.

O index-calculus tem sido aplicado satisfatoriamente em vários problemas criptográficos interessantes, incluindo o DLP para corpos finitos (ver Subseção 2.3.1). Esta mesma idéia pode ser usada para o DLP no Jacobiano $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n})$ de uma curva hiperelíptica **H** de gênero g definida sobre $K = \mathbb{F}_q$. No que segue, $D_1 \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$, $D_2 \in < D_1 >$ e queremos determinar m tal que $[D_2] = m[D_1]$ ou $m = \log_{D_1} D_2$.

(1) O primeiro passo é computar a estrutura de $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ como soma direta de subgrupos cíclicos e se procurão representações de D_1 e D_2 sobre esta soma direta, logo para resolver o DLP simplesmente aplicamos o Teorema Chinês dos Restos Generalizado. Para descrever o método, introduzimos algumas definições .

Definição 4.19. Seja $D = \mathrm{div}(A, B)$ um divisor semi-reduzido sobre **H**. Dizemos que D é um divisor *primo* se o polinômio A é irredutível sobre $\mathbb{F}_q[X]$, o corpo base de **H**.

Seja $A \in K[X]$ um polinômio irredutítivel e α uma raiz de A. Dizemos que $Y^2 + h(X)Y - f(X)$ é separável $\pmod{A}$ se $Y^2 + h(\alpha)Y - f(\alpha)$ tem duas raízes distintas em $K(\alpha)$.

Definição 4.20. O polinômio A é dito separável se A não divide $f(X)$ e $Y^2+h(X)Y-f(X)$ é separável $\pmod{A}$.

Definição 4.21. O polinômio A é dito ramificado se A divide $f(X)$.

Para $D \in \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ tal que $D = \mathrm{div}(A, B)$, podemos escrever este como a soma de divisores primos da forma $D_i = \mathrm{div}(A_i, B_i)$, onde os A_i são fatores primos de A. Seja t um inteiro chamado a cota de smooth-ness.

Definição 4.22. Um divisor é dito t-smooth se todos seus divisores primos são de grau menor ou igual a t.

Quando $t = 1$, um divisor 1-smooth será um divisor para o qual o polinômio A é completamente separável sobre $\mathbb{F}_q$.

Seja $S = \{P_1, \ldots, P_n\}$ a *base fator* onde $P_i = \mathrm{div}(A_i, B_i)$ são todos os divisores primos ramificados e separáveis tal que $\deg(A_i) \leq t$ para algum $t \in \mathbb{Z}$. Se A_i é sepáravel, então unicamente um dos divisores primos sobre A_i, $\mathrm{div}(A_i, B_i)$ ou $\mathrm{div}(A_i, -B_i - h)$, está em S.

O primeiro método procura achar $m > n$ t-smooth divisores principais tal que se tenha a relação $\sum_j \alpha_j P_j \sim \mathcal{O}$. Se S gera $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ então a aplicação

$$\phi : \mathbb{Z}^n \to \mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \,\text{onde}\, \phi(\alpha_1, \ldots, \alpha_n) \mapsto \sum_j \alpha_j P_j \,,$$

é um homomorfismo sobrejetivo, logo $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \cong \mathbb{Z}^n/\mathrm{Ker}(\phi)$. Cada relação é um elemento $\alpha_i' = (\alpha_{i1}, \ldots, \alpha_{in}) \in \mathrm{Ker}(\phi)$, e se o conjunto de m relações forma um sistema completo de geradores do $\mathrm{Ker}(\phi)$, então $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$ tal que $(d_1, \ldots, d_n)$ são os elementos da *forma normal de Smith* (SNF) (ver Apêndice A) da matriz relação $A = (\alpha_1' \ldots \alpha_m')$ onde α_i' estão escritos como colunas. Geradores X_i de cada subgrupo $\mathbb{Z}/d_i\mathbb{Z}$ podem ser calculados achando as matrizes $P = (p_{ij})$ e $Q = (q_{ij})$ tal que $P^{-1}AQ = SNF(A)$ e fazemos $X_i = \sum_{j=1}^{n} p_{ij} P_j$.

O segundo passo do algoritmo é achar representações de D_1 e D_2 em $Z/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$. Se D_1 e D_2 podem ser fatorados sobre S como $D_1 \sim \sum r_i P_i$ e $\sum s_i P_i$, então

$D_1 \sim \sum r'_i X_i$ e $D_2 \sim \sum s'_i X_i$ onde $(r'_1, \ldots, r'_n) = P^{-1}(r_1, \ldots, r_n)^T$ e $(s'_1, \ldots, s'_n) = P^{-1}(s_1, \ldots, s_n)^T$. Finalmente damos as representações de $D_1 = (r'_1, \ldots, r'_n)$ e $D_2 = (s'_1, \ldots, s'_n)$ em $\mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_n\mathbb{Z}$, logo o DLP pode ser resolvido usando o Teorema Chinês dos Restos generalizado para achar $m \in \mathbb{Z}$ tal que as congruências $r'_i \equiv m s'_i \pmod{d_i}$ onde $1 \leq i \leq n$ sejam simultaneamente satisfeitas.

(2) O segundo método melhora o primeiro quando $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ é conhecido. Como acima, seja $S = \{P_1, \ldots, P_n\}$ a base fator com todos os divisores primos de grau menor o igual que t. As relações são achadas por tentativas para fatorar divisores da forma $rD_1 + sD_2$ sobre S. Cada divisor t-smooth leva a uma relação da forma $r_i D_1 + s_i D_2 \sim Q_i = \sum_j \alpha_{ij} P_j$. Quando tem sido achados $n+1$ relações diferentes, aplicamos o módulo $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ para encontrar uma combinação linear não trivial da forma $\sum_{i=1}^{n+1} \gamma_i \alpha'_i = (0, \ldots, 0)$, onde $\alpha'_i = (\alpha_{i_1}, \ldots, \alpha_{1_n})$ o qual implica que $\sum_{i=1}^{n+1} \gamma_i Q_i = 0$. Logo, $\sum_{i=1}^{n+1} \gamma_i (r_i D_1 + s_i D_2) = 0$ e $\log_{D_1} D_2 = -(\sum \gamma_i r_i)/(\sum \gamma_i s_i) \pmod{\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)}$

A eficiência do método depende bastante da escolha da base fator S, pois seus elementos, os divisores primos, devem de gerar $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$.

Existem various outros algoritmos apresentados na literatura para atacar o problema do logaritmo discreto sobre o Jacobiano de curavs hiperelípticas, ver [16].

Comentários

Esta dissertação teve como objetivo estudar as curvas Hiperelípticas e seus Jacobianos para o desenvolvimento de criptossistemas de chave pública que baseiam sua segurança na resolução do Problema do Logaritmo Discreto (DLP).

Diante destes estudos observamos que:

- Para implementações criptográficos se deseja que o número de pontos do Jacobiano $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{q^n}) := N_n$ seja divisível por um número primo grande. Neste sentido, existem curvas hiperelípticas que atingem a cota máxima de Hasse-Weil para o número de pontos chamadas de *curvas maximais* [39, p. 202]. Por exeplo, a curva hiperelíptica $Y^2+Y = X^5$ de gênero $g = 2$ é maximal sobre o corpo $\mathbb{F}_{2^4}$. Assim podemos considerar pontos racionais sobre extensões de $\mathbb{F}_{2^4}$, isto é, sobre corpos da forma $\mathbb{F}_{2^{4s}}$; mas para que a curva continue sendo maximal é necessário que o número s seja par; desta forma se tem suficientes pontos racionais para valores grandes de s. Além disso, se conhece que a estrutura do Jacobiano para este tipo de curvas é da forma $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_{\ell^2}) \cong (\mathbb{Z}/(\ell+1)\mathbb{Z})^{2g}$. Assim, com estas propriedades do grupo para fazer criptografia, estas curvas a priori são um *bom tipo* de curvas para implementar criptossistemas. O termo bom tipo, faz referencia à informação que obtemos do número de pontos e a estrutura do Jacobiano a partir destas curvas.

- O gênero g de curvas hiperelípticas adequadas para implementações criptográficas é de fundamental importância que seja pequeno (2 e 3), pois para $g \geq 4$ existe um algoritmo de tempo sub-exponencial que resolve o Problema do Logaritmo Discreto (DLP) sobre

o Jacobiano deste tipo de curvas [2].

- Analogamente ao caso de curvas elípticas anómalas, temos que se $\mathbf{H}$ é uma curva hiperelíptica tal que $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q) = q+1$, então o DLP em $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ pode ser eficientemente resolvido [36].

- Para uma curva hiperelíptica definida sobre um corpo finito $\mathbb{F}_q$, existe uma eficiente redução do DLP no $\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ para o DLP no grupo multiplicativo de um corpo de extensão $\mathbb{F}_{q^k}$, onde k é o inteiro mais pequeno tal que $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ divide $q^k - 1$, ou o maior fator primo de $\#\mathcal{J}_{\mathbf{H}}(\mathbb{F}_q)$ que divide $q^k - 1$.

APÊNDICE A

Preliminares Matemáticos

Planos Projetivo $\mathrm{P}^2(K)$ É o conjunto de classes de equivalência de triplas $(a_1, a_2, a_3) \in K \times K \times K$, não todos zero, onde duas triplas são equivalentes $(a_1, a_2, a_3) \sim (b_1, b_2, b_3)$ se $(a_1, a_2, a_3) = (\lambda b_1, \lambda b_2, \lambda b_3)$ para algum $\lambda \in K$. Cada classes de equivalência é chamada de *ponto projetivo*. Se um ponto projetivo (a_1, a_2, a_3) tem $a_3 \neq 0$, então esta classe de equivalência pode ser representada por uma tripla da forma $(a_1', a_2', 1)$ fazendo $a_1' = a_1/a_3$ e $a_2' = a_2/a_3$. Logo, podemos identificar o plano projetivo com os pontos $(x, y) \in K \times K$ do plano ordinário (ou afim) junto com os pontos para o qual $a_3 = 0$. O conjunto de pontos com a última coordenada nula são chamados de *reta no infinito*.

Função Zeta É uma ferramenta básica para calcular o número de pontos racionais de uma curva hiperelíptica. Seja $\mathbf{H}$ uma curva hiperelíptica definida sobre $K = \mathbb{F}_q$, e n_r o número de pontos racionais de $\mathbf{H}$ sobre $L = \mathbb{F}_{q^r}$. Então a *função zeta* de $\mathbf{H}$ é a série de potências

$$Z(\mathbf{H}/\mathbb{F}_q; t) = e^{\sum_{r \geq 1} n_r t^r / r}.$$

O seguinte teorema da função zeta provado por A. Weil é a justificativa da equação dada em (4.4).

Teorema A.1. *Seja* $\mathbf{H}$ *uma curva hiperelíptica de gênero* g *definida sobre* $\mathbb{F}_q$ *e* $Z(\mathbf{H}/\mathbb{F}_q; t)$ *sua função zeta. Então*

(1)

$$Z(\mathbf{H}/\mathbb{F}_q; t) = \frac{P(t)}{(1-t)(1-qt)},$$

onde $P(t)$ é um polinômio de grau $2g$ com coeficientes inteiros da forma

$$P(t) = 1 + a_1 t + \ldots + a_{g-1}t^{g-1} + a_g t^g + q a_{g-1} t^{g-1} + \ldots + q^g t^{2g}.$$

(2) *$P(t)$ pode-se fatorar da seguinte forma*

$$P(t) = \prod_{i=1}^{g} (1 - \beta_i t)(1 - \bar{\beta}_i t),$$

onde cada β_i é um número complexo de módulo $|\sqrt{q}|$ e $\bar{\beta}_i$ denota o complexo conjugado de β_i.

Definição A.2. Uma curva Elíptica $\mathbf{E}$ como na Definição (3.1) é *não singular* se e somente se o sistema $\partial(F)/\partial(X) = 0$, $\partial(F)/\partial(Y) = 0$, $\partial(F)/\partial(Z) = 0$ não tem solução para qualquer ponto $P \in \mathbf{E}$.

Mostremos que o polinômio F em (4.1) com $Z = 1$ é absolutamente irredutível em $\bar{K}[X, Y]$, onde g representa o gênero da curva. Suponhamos que o polinômio é redutível, então existem $G, H \in \bar{K}[X, Y]$ não constantes tais que $F = GH$. O grau de Y em G e H é 1 e G, H são não constantes, pois do contrário teríamos uma contradição já que o coeficiente de Y^2 é 1. Então $F = GH = (AY + B)(CY + D)$ e daqui temos as seguintes equações : $AC = 1$, $AD + BC = h(X)$ e $BD = f(X)$. Logo A e C são inversos e portanto constantes, o grau de $h(X)$ é menor o igual que g então o grau B e D são menores o iguais que g e daqui que o grau de $BD \leq 2g$ absurdo, pois o grau de $f(X)$ é $2g + 1$.

Base Normal. Seja $K = \mathbb{F}_q$ e $L = \mathbb{F}_{q^n}$ uma extensão finita. Uma base de L sobre K da forma $(\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}})$ para um adequado $\alpha \in L$, é chamada de *Base Normal* de L sobre K.

Teorema A.3. *Para qualquer corpo finito K e qualquer extensão finita L de K, existe uma Base Normal de L sobre K.*

Uma prova deste Teorema pode ser vista em [23, p. 60].

Forma Normal de Smith. Foi provado por Smith (1861) que qualquer matriz $A \in M_{m\times n}(\mathbb{Z})$ é equivalente a uma única matriz diagonal $S \in M_{m\times n}(\mathbb{Z})$ fazendo transformações unimodulares. Isto é, existem matrizes $P \in M_{m\times m}(\mathbb{Z})$ e $Q \in M_{n\times n}(\mathbb{Z})$ com $\det(P), \det(Q) =$

± 1, tal que

$$S = PAQ = \begin{pmatrix} s_1 & & & & & \\ & \ddots & & & & \\ & & s_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix} = \text{diag} = (s_1, \ldots, s_r, 0, \ldots, 0) \in M_{m \times n}(\mathbb{Z})$$

onde r determina o rango da matriz A e $s_i | s_{i+1}$ para $1 \leq i \leq r-1$. A matriz S é chamada a forma Normal de Smith de A e os elementos não nulos da diagonal de S são chamados os elementos invariantes de A. Como foi mencionado em na Subseção (4.3.1), computar a SNF pode ser aplicada para achar a estrutura canônica de grupos Abelianos.

APÊNDICE B

Complexidade Algoritmica

Quando projetamos um criptossistema pretendemos gerar um problema que seja difícil de ser decifrado por qualquer criptoanalista. Mas, dado que condições pode-se garantir que um problema seja intratável? O assunto frente a esta pergunta é como medir a capacidade necessária de calculo que se deve fazer ao abordar um problema. Nesta seção daremos uma breve introdução nas ferramentas formais que permitirão dar resposta a este tipo de questionamento.

Os criptossistemas de chave pública estão baseados na *Teoria de Complexidade Algorítmica*, que estuda a forma de construir algoritmos para resolver diferentes problemas. Entenderemos por algoritmo uma sequência finita e ordenada de etapas que finalizam em algum momento e devolve a solução. Nos criptossistemas, além de procurar segurança, também é importante que estes sejam rápidos de-se aplicar. Neste sentido, esta teoria nos da ferramentas para decidir quando um algoritmo é melhor que outro.

Na maioria dos casos, o tempo de execução de um algoritmo depende dos dados de entrada. Por exemplo, para ordenar a sequência $\{1, 2, 3, 4, 6, 5\}$ de menor a maior, se necessitam menos operações elementares que para ordenar $\{6, 5, 3, 2, 4, 1\}$. Isto nos leva a considerar três opções :

- Melhor caso: É o número de operações feitas no algoritmo quando os dados estão da melhor forma possível. Este caso não é prático, pois o algoritmo pode ter um melhor caso e os demais não.

- Pior caso: É o número de operações feitas quando a distribuição dos dados de entrada é a mais pessimista. Este nos permitirá obter uma cota para o tempo de execução necessária do algoritmo.

- Caso médio: Muitas vezes acontece que os algoritmos no pior dos casos não funcionam bem, mas na maioria dos outros casos seu comportamento é provavelmente efetivo.

Resulta impossível calcular o tempo exato de execução de um algoritmo, para isto utilizaremos um tipo de notação assintótica, que nos permitirá cotar sua magnitude. Normalmente consideramos o tempo de execução de um algoritmo como uma função $f(n) \in \mathbb{R}^+$ onde n é o tamanho do dado de entrada.

Dada a função $f(n)$, definimos:

- *Limite superior assintótico*: $f(n) = O(g(n))$ se existe uma constante positiva c e um número inteiro positivo n_0 tal que $0 \leq f(n) \leq cg(n)$ para todo $n \geq n_0$.

- *Limite inferior assintótico*: $f(n) = \Omega(g(n))$ se existe uma constante positiva c e um número inteiro positivo n_0 tal que $0 \leq cg(n) \leq f(n)$ para todo $n \geq n_0$.

- *Limite exato assintótico*: $f(n) = \Theta(g(n))$ se existem duas constantes positivas c_1, c_2 e um número inteiro positivo $n_0 > 0$ tal que $c_1 g(n) \leq f(n) \leq c_2 g(n)$ para todo $n \geq n_0$.

- *Notação o*: $f(n) = o(g(n))$ se para qualquer constante positiva c existe um número inteiro positivo $n_0 > 0$ tal que $0 \leq f(n) \leq cg(n)$ para todo $n \leq n_0$.

Sejam $f(n)$ e $g(n)$ funções positivas para $n \geq n_0$. Se

$$\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1$$

dizemos que f é assintóticamente igual a g para valores grandes de n, e denotamos por $f \asymp g$. Intuitivamente, $f(n) = O(g(n))$ significa que $f(n)$ cresce assintóticamente mais lento que $g(n)$ multiplicada por uma constante. Analogamente $f(n) = \Omega(g(n))$ quer dizer que $f(n)$ cresce assintóticamente no mínimo tão rápido como $g(n)$ multiplicada por uma constante. Definiremos agora algumas propriedades da notação acima:

a) $f(n) = O(g(n))$ se e somente se $g(n) = \Omega(f(n))$.

b) $f(n) = \Theta(g(n))$ se e somente se $f(n) = O(g(n))$ e $f(n) = \Omega(g(n))$.

c) Se $f(n) = O(h(n))$ e $g(n) = O(h(n))$, então $(f+g)(n) = O(h(n))$.

d) Se $f(n) = O(h(n))$ e $g(n) = O(l(n))$, então $(f \cdot g)(n) = O(h(n)l(n))$.

e) $f(n) = O(f(n))$.

f) Se $f(n) = O(g(n))$ e $g(n) = O(h(n))$, então $f(n) = O(h(n))$.

Para algumas funções bastante usadas, podemos definir diretamente a ordem de complexidade:

- *Funções polinomiais*: Se $f(n)$ é um polinômio de grau k, e o coeficiente da maior potência positivo, então $f(n) = \Theta(n^k)$.
- *Funções logarítmicas*: Para qualquer constante $c > 0$, $\log_c(n) = \Theta(\ln(n))$.
- *Fatoriais*: $n! = \Omega(2^n)$.
- *Logaritmo de um fatorial*: $\ln(n!) = \Theta(n \ln(n))$.

O tempo para executar um algoritmo depende das operações elementares que envolve e do comprimento dos dados de entrada. Podemos considerar como operação elementar aquela que se executa sempre em um tempo constante. Este conceito também depende das características concretas do computador em que estejamos trabalhando. Por exemplo, um computador que opera unicamente com números de 16 bits, não pode considerar-se elemental uma operação com números de 32 bits. Para medir este tempo é necessário uma unidade de medida, e como o computador faz qualquer calculo como somas binárias elementares, damos a seguinte definição.

Dizemos que um algoritmo é *polinomial* se o pior caso de execução é de ordem $O(n^k)$, onde n é o tamanho de entrada e k é uma constante. Além disso, qualquer algoritmo que não possa ser cotado por uma função polinomial, se conhece como *exponencial*. Em geral, os algoritmos polinomiais se consideram eficientes, enquanto os que são exponenciais se consideram ineficientes. Um algoritmo se denomina *sub-exponencial* se no pior dos casos, a função de execução é da forma $\exp^{o(n)}$, onde n é o tamanho da entrada. Estes são assintóticamente mais rápidos que os exponenciais puros, no entanto mais lentos que os polinomiais.

É usual classificar o tempo estimado entre o tempo polinomial e o exponencial. Seja n um inteiro positivo grande, $\gamma \in \mathbb{R}$ tal que $0 \leq \gamma \leq 1$ e $c > 0$ uma constante. Logo,

$$L_n(\gamma; c) = O(e^{((c+o(1))(lnn)^{\gamma}(lnlnn)^{1-\gamma})}).$$

Dizemos que um algoritmo é $L(\gamma)$ se o algoritmo aplicado a um inteiro n, tem um tempo estimado de execução da forma $L_n(\gamma; c)$ para alguma constante c. Em particular, um algoritmo de tempo polinomial é da forma $L(0)$, e um algoritmo de tempo exponencial da forma $L(1)$. Uma outra definição para um algoritmo sub-exponencial é um algoritmo de tempo $L(\gamma)$ onde $0 < \gamma < 1$.

B.1 Classes de Complexidade

Em ocasiões se reduzem os problemas de complexidade algoritmica a um simples problema de decisão, de forma que se considera um algoritmo como um mecanismo que permite obter uma resposta sem ou não a um problema.

- A classe de complexidade **P** é o conjunto de todos os problemas de decisão que podem ser resolvidos em tempo polinomial.
- A classe de complexidade **NP** é o conjunto de todos os problemas para os quais uma resposta afirmativa pode ser verificada em tempo polinomial, usando uma informação extra, chamada *certificado*.
- A classe de complexidade **co-NP** é o conjunto de todos os problemas para os quais uma resposta negativa pode ser verificada em tempo polinomial, usando um certificado apropriado.

Notemos que o fato de que um problema seja **NP**, não quer dizer que o certificado correspondente é fácil de obter, no entanto, dado este pode ser dada uma resposta positiva em um tempo polinomial. Esta observação pode ser feita também para os problemas **co-NP**.

Dentro da classe dos problemas **NP**, existe um subconjunto chamado **NP**-completos que denotamos **NPC**. Estes problemas se caracterizam porque todos eles são equivalentes, i.e., se podem reduzir um em outros, e se lograrmos resolver algum em tempo polinomial, então teremos resolvido todos no mesmo tempo.

Até agora só temos mencionado algoritmos determinísticos, isto é, algoritmos que sempre tem o mesmo caminho de execução, e que sempre dão uma resposta (se existe) para a mesma solução. Contudo, existem problemas para os quais é melhor usar algoritmos probabilísticos ou aleatórios. Estes algoritmos usa parâmetros aleatótrios de tal forma que para duas aplicações do algoritmo ao mesmo dado de entrada podem ser diferentes. Em alguns

casos este tipo de algoritmos pode obter melhores soluções em comparação com os algoritmos determinísticos.

Em geral, o fato de não se conhecer um algoritmo eficiente para resolver um problema não quer dizer que este não exista; por isso é importante a Teoria de Algoritmos para Criptografia. A contínua redução do tempo de execução necessária para resolver certos problemas, dada pelo aparecimento de algoritmos mais eficientes, junto com o avanço dia a dia do computador na parte de *hardware* disponível, impõe uma relativa frequência a atualizar as previsões de segurança dos criptossistemas. Para maiores detalhes ver [21, p. 18], [29, p. 57].

BIBLIOGRAFIA

[1] L. Adleman and J. Marrais: A subexponential algorithm for discrete logarithms over all finite fields, *Mathematics of Computation* **61**, 1993, 1-15.

[2] L. Adleman, J. DeMarris and M. Huang: A Subexponential Algorithm for Discrete Logaritms over Hypereliptic Curves of Large Genus over $GF(q)$, *Theorical Computer Science* **226**, 1999, 7-18.

[3] L. Adleman and M. Huang: Counting Points on Curves and Abelian Varieties over Finite Fields, *Journal Symbolic Computation* **32**, 2001, 171-189.

[4] I. Blake, G. Seroussi and N. Smart: *Elliptic Curves in Cryptgraphy*, London Mathematical Society Lecture Notes Series **265**, Cambrigde University Press, 1999.

[5] D. Le Brigand: Decoding of codes on hyperelliptic curves, *Eurocode '90*. Lectures Notes Computation Science **514**, Springer-Verlag, 1991, 126-134.

[6] J. Buchmann: Factorización de números grandes, *Revista de Investigacion y Ciencia*, Abril, 1999, 44-51.

[7] D. Cantor: Computing in the jacobian of a hiperelliptic curve, *Mathematics of Computation* 48, 1987, 95-101.

[8] G. Cornell and J.H. Silverman: *Arithmetic Geometry*, Springer-Verlag, New York, 1986.

[9] S.C. Coutinho: *Números Inteiros e Criptografia RSA*, SBM/IMPA, Rio de Janeiro, 2000.

[10] W.D. Diffie, M.E. Hellman: New Directions in Cryptography, *IEEE Transactions on information Theory* **22**, 1976, 644-654.

[11] W. Fulton: *Algebric Curves*, Benjamin, New York, 1969.

[12] P. Gaudry, F. Hess and N. Smart: Constructive and destructive facets of Weil decent on elliptic curves, *Journal of Cryptology* **15**, 2002, 9-46.

[13] S.D. Galbraith, S.M. Paulus and N.P. Smart: Arithmetic on Superelliptic Curves, *Mathematics of Computation* **71**, 2000, 393-405.

[14] GEC 1: "Recommended elliptic curve domain parameters". Standards for Efficient Cryptography Group, September, 1999. Working draft. Available at http://www.secg.org/.

[15] L.S. Hill: Concerning certain linear transformation apparatus of cryptography, *American Mathatematical Monthly* **38**, 1931, 135-154.

[16] M. Jacobson, A. Menezes and A. Stein: Hyperelliptic Curve and Cryptography (update), 2003. http://www.cacr.mayh.uwaterloo.ca. Technical report.

[17] D. Kahn: *The Codebreakers, The Story of Secret Writing*, Macmillan Publishing Co. N.Y. 1967.

[18] N. Koblitz: Elliptic curve cryptosystems, *Mathematical of Computation* **48**, 1987, 203-209.

[19] N. Koblitz: Hyperelliptic cryptosystems, *Journal Criptology* **1**, 1989, 139-150.

[20] N. Koblitz: *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 2nd edition, 1994. Criptology 1, 1989, 139-150.

[21] N. Koblitz: *Algebraic Aspects of Cryptography*, Springer-Verlag, Berlin-Heidelberg-New York, 1998.

[22] H.W. Lenstra, J. Pila, and C. Pomerance: A hyperelliptic smoothness test. I, *Philos. Trans. Royal Society London* **345**, 1993, 397-408.

[23] R. Lidl and H. Niederreiter: *Finite Fields, in Encyclopedia of Mathematics and its Applications*, G.-C. Rota, editor, Addison-Wesley, 1983.

[24] J. López and R. Dahab: Fast Multiplication on Elliptic Curves over $GF(2^m)$. *In CHES'99* number 1717 in LCNS. Springer-Verlag, 1999.

[25] J. López Hernández: *Implementação Eficiente em Software de Criptossistemas de Curvas Elípticas*. PhD thesis, Universidade Estadual de Campinas - UNICAMP, 2000.

[26] M.J. Lucena Lopez: *Criptografia y Seguridad en Computadores*. Tercera edicion, 2003. http://wwwdi.ujaen.es/ mlucena/lcripto.html

[27] R. Matsumoto: Constructing Algebraic Geometry Codes on the Normalization of a Singular C_{ab} Curve, *IEICE Transactions on Communications/Electronics/Information and Systems*, 1999. (available at http://citeseer.nj.nec.com/matsumoto99constructing.html)

[28] A.J. Menezes, T. Okamoto and S. Vanstone: Reducing elliptic curve logarithm in a finite field, *IEEE Transactions on Information Theory* **39**, 1993, 1639-1646.

[29] A.J. Menezes, P.C.van Oorschot and S.A.Vanstone: *Handbook of applied Cryptography*, CRC Press, 1996.

[30] C. Munuera y J. Tena: *Codificación de la Información*, Universidad de Valladolid, Valladolid, 1997.

[31] National Institute of Standards and Technology: Digital Signature Standard, FIPS Publication 186(2), 2000; available at http://csrc.nist.gov/fips.

[32] A.M. Odlyzko: Discrete logarithms and their cryptographic significance, Advances in Cryptography, Proceding of Eurocrypt 84, Springer-Verlag, New York, 1985, 224-314.

[33] J. Pelzl, T. Wollinger, J. Guajardo and C. Paar: Hyperelliptic curve cryptosystem Closing the performance gap to elliptic curve (update), Cryptology Print Archive: Report 2003/026, 2003. http://eprint.iacr.org/.

[34] G. Purdy: A high-security log-in procedure, *Communications of the ACM* **17**, 1974, 442-445.

[35] J.E. Sarlabous, E. R. Barreiro, J.A. Piñeiro: On the Jacobian Varieties of Picard Curves, Addition Law and Algebraic Structure. ICIMAF, Ministry of Sciences, Habana, Cuba, 1996.

[36] T. Satoh and K. Araki: Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Commentarii Mathematici Universitatis Sancti Pauli* **47**, 1998, 81-92.

[37] J.H. Silverman: *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1986.

[38] J.H. Silverman and J. Tate: *Rationals Points on Elliptic Curves*, Springer-Verlag, 1992.

[39] H. Stichtenoth: *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, Heidelberg, 1993.

[40] D.R. Stinson: *Cryptography (Theory and Practice)*, CRC Press, 1995.

[41] N. Thériault: Index calculus attack for hyperelliptic curves of small genus, 2003. Available at http://www.math.toronto.edu/ganita/publications.html