



UNIVERSIDADE ESTADUAL DA PARAÍBA  
CAMPUS I  
CENTRO DE CIÊNCIAS E TECNOLOGIA  
DEPARTAMENTO DE MATEMÁTICA  
CURSO DE LICENCIATURA EM MATEMÁTICA

LINDOMAR ROBSON ALVES DE LIMA

CRIPTOGRAFIA EM CURVAS ELÍPTICAS

CAMPINA GRANDE  
2021

LINDOMAR ROBSON ALVES DE LIMA

**CRIPTOGRAFIA EM CURVAS ELÍPTICAS**

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

**Área de concentração:** Álgebra

**Orientador:** Prof. Msc. Vilmar Vaz da Silva

CAMPINA GRANDE

2021

É expressamente proibido a comercialização deste documento, tanto na forma impressa como eletrônica. Sua reprodução total ou parcial é permitida exclusivamente para fins acadêmicos e científicos, desde que na reprodução figure a identificação do autor, título, instituição e ano do trabalho.

L732c Lima, Lindomar Robson Alves de.  
Criptografia em curvas elípticas [manuscrito] / Lindomar Robson Alves de Lima. - 2021.  
52 p.

Digitado.  
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2021.  
"Orientação : Prof. Me. Vilmar Vaz da Silva, Coordenação do Curso de Matemática - CCT."

1. Criptografia. 2. Algoritmo. 3. Curvas elípticas. I. Título  
21. ed. CDD 511.8

**LINDOMAR ROBSON ALVES DE LIMA**

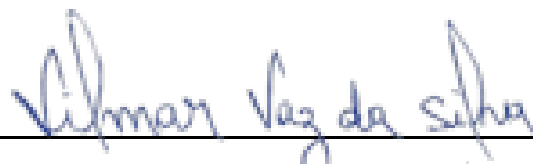
**CRIPTOGRAFIA EM CURVAS ELÍPTICAS**

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática do Centro de Ciências e Tecnologia da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de Licenciado em Matemática.

Área de concentração: Álgebra

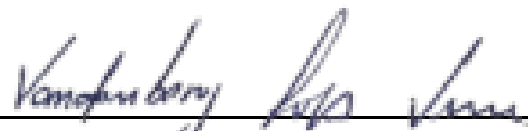
Aprovado em: 19/03/2021.

**BANCA EXAMINADORA**



---

Prof. Msc. Vilmar Vaz da Silva (Orientador)  
Universidade Estadual da Paraíba (UEPB)



---

Prof. Dr. Vanderberg Lopes Vieira  
Universidade Estadual da Paraíba (UEPB)



---

Prof<sup>ª</sup>. Dr<sup>ª</sup>. Emanuela Régia de Souza Coelho  
Universidade Estadual da Paraíba (UEPB)

À minha querida  
família, DEDICO.

## AGRADECIMENTOS

Agradeço a Deus pelo dom da vida, pela capacidade da aprendizagem e da criatividade matemática que dia após dia procuro exercitar e desenvolver. Agradeço a Deus pela saúde e pela longevidade, para finalizar esse período inicial da minha vida universitária, concluindo assim o fechamento de um ciclo e a abertura de outro.

Agradeço a minha família, em especial aos meus pais, Antônio Isidorio de Lima e Maria das Dores Alves de Lima, pelo incentivo incessante, a meus irmãos e irmã, Antônio, Nazareno e Lidiane, que apesar da distância nunca esqueceram de mim. Agradeço a minha esposa Edvanda Luiz Diniz Lima, pelo companheirismo nas situações mais complexas, as minhas filhas Livia Diniz Lima e Larissa Diniz Lima, pelos momentos de lazer inesquecíveis.

Agradeço aos professores que tanto influenciaram o estudante que sou hoje, pelo profissional que me tornei e pelo amadurecimento intelectual e pela formação acadêmica. Reservo aqui um agradecimento especial ao professor orientador Vilmar Vaz da Silva que ajudou na minha formação como professor, nas orientações primeiras acerca das definições de Álgebra Linear e, principalmente, pela excelente orientação na realização desse trabalho.

## RESUMO

Através da história, é notório o uso da criptografia para codificação e decodificação de mensagens que, por sua importância, são protegidas por intrincados métodos e técnicas, que visam dificultar a interceptação de informações por entes que buscam a decodificação não autorizada. Contudo com o avanço computacional e sua crescente influência nos métodos de comunicação, fez-se necessário o desenvolvimento de novos algoritmos de mensagens. Dada a necessidade de aumentar o nível de segurança nas trocas de informação e no compartilhamento de conteúdos no espaço virtual (internet) é que a criptografia em curvas elípticas traz uma proposta para aumentar o nível de segurança dos códigos e conseqüentemente um acréscimo na dificuldade de conversão das mensagens cifradas. Nesse sentido, este trabalho apresenta o estudo do protocolo Diffie-Hellman (ECDH), que tem a finalidade de possibilitar a troca de chaves por dois ou mais usuários. O objetivo é fornecer as ferramentas matemáticas necessárias para o entendimento da forma como codificamos e decodificamos mensagens através da criptografia em curvas elípticas.

**Palavras-chave:** Criptografia. Algoritmo. Curvas Elípticas.

## ABSTRACT

Through history, it's notorious the cryptography's use for codification and decodification of messages that, for it's importance, are protected by intricate methods and techniques that aim difficult the interception of informations by beings who seek non-authorized decodification. However, with the computacional advance and it's increasing influence in the communication methods, the development of new messages algorithms became needed. Due the need of increase the security level in information's exchange and in the sharing of contents in online space (internet), cryptography in elliptic curves bring a propose to increase the security level and, hence, enhance the encrypted messages decodification complexity. In that regard, this paper presents the study of Diffie-Hellman protocol, whom aims to enable the keys exchange by two or more users. The goal is to provide the required mathematical tools for understanding about the method we use to codificate and decodificate messages through cryptography in elliptic curves.

**Keywords:** Cryptography. Algorithm. Elliptic Curves.



## LISTA DE FIGURAS

3.1	Exemplos de cúbicas . . . . .	33
3.2	Adição dos pontos $P$ e $Q$ com $P \neq Q$ . . . . .	38
3.3	Adição dos pontos $P$ e $Q$ com $P = Q$ . . . . .	38
3.4	Associatividade da Operação de Adição com Pontos de Curvas Elípticas . . . . .	40
4.1	Sistema Criptográfico . . . . .	42
4.2	Sistema de chave simétrica reduzido . . . . .	43
4.3	Sistema de chave pública . . . . .	44

## LISTA DE TABELAS

3.1	Adição para $E : y^2 = x^3 + x + 1$ sobre $\mathbb{Z}_7$ . . . . .	41
3.2	Possibilidades de Curvas Elipticas em $\mathbb{Z}_7$ pelo Teorema de Hasse. . . . .	41
4.1	Algoritmo Dobra - Adiciona . . . . .	46
4.2	Parâmetros em ECDH. . . . .	49
4.3	Descrição do Protocolo ECDH. . . . .	49

## LISTA DE SÍMBOLOS

$(G : H)$	Índice do subgrupo $H$ no grupo $G$
$\mathbb{K}[x, y, z]$	Anel de polinômios em 3 variáveis com coeficientes em $\mathbb{K}$
$\text{disc}(F)$	Discriminante do polinômio $F$
$*$	Operação binária
$E(\mathbb{Z}_p)$	Curva elíptica sobre $\mathbb{Z}_p$
$U(A)$	Unidades do conjunto $A$
$V(P)$	Conjunto de zeros do polinômio $P$
$(a, b)$	Máximo divisor comum entre $a$ e $b$
$\bar{a}$	Classe de equivalência do inteiro $a$
$\equiv_n$	Relação de congruência módulo o inteiro $n$
$\mathbb{K}$	Corpo
$\mathbb{N}$	Conjunto dos números naturais
$\mathbb{P}_{\mathbb{K}}^2$	Plano projetivo de dimensão 2
$\mathbb{Q}$	Conjunto dos números racionais
$\mathbb{Z}$	Conjunto dos números inteiros
$\mathbb{Z}_n$	Conjunto dos inteiros módulo $n$
$\mathcal{O}$	Identidade do grupo $E(\mathbb{Z}_p)$
$O(a)$	Ordem do elemento $a$ em um grupo
$\sim$	Relação de equivalência
$a \mid b$	Inteiro $a$ divide inteiro $b$
$G$	Grupo
$H < G$	$H$ é subgrupo de $G$
$H = \langle a \rangle$	Subgrupo cíclico gerado por $a$
$\log_P(Q)$	Logaritmo discreto elíptico de $Q$ com respeito a $P$
ECDLP	Problema do Logaritmo Discreto em Curva Elíptica

# SUMÁRIO

	Página
<b>1</b>	<b>INTRODUÇÃO</b> <span style="float: right;"><b>11</b></span>
<b>2</b>	<b>PRELIMINARES</b> <span style="float: right;"><b>12</b></span>
<b>2.1</b>	<b>Teoria dos Números</b> . . . . . 12
<i>2.1.1</i>	<i>Princípio da Boa Ordem e Indução Finita</i> . . . . . 12
<i>2.1.2</i>	<i>Divisibilidade</i> . . . . . 13
<i>2.1.3</i>	<i>Congruência</i> . . . . . 17
<i>2.1.4</i>	<i>Resíduos Quadráticos</i> . . . . . 20
<b>2.2</b>	<b>Estruturas Algébricas</b> . . . . . 20
<i>2.2.1</i>	<i>Grupos</i> . . . . . 21
<i>2.2.2</i>	<i>Subgrupos</i> . . . . . 23
<i>2.2.3</i>	<i>Grupos Cíclicos</i> . . . . . 25
<i>2.2.4</i>	<i>Homomorfismo de Grupos</i> . . . . . 27
<b>3</b>	<b>CURVAS ELÍPTICAS</b> <span style="float: right;"><b>29</b></span>
<b>3.1</b>	<b>Espaço Projetivo</b> . . . . . 29
<b>3.2</b>	<b>Cúbicas</b> . . . . . 32
<b>3.3</b>	<b>Curvas Elípticas Sobre <math>\mathbb{Z}_p</math></b> . . . . . 34
<b>3.4</b>	<b>Operação com Pontos de uma Curva Elíptica</b> . . . . . 37
<b>4</b>	<b>SISTEMA CRIPTOGRÁFICO UTILIZANDO CURVAS ELÍPTICAS</b> <span style="float: right;"><b>42</b></span>
<b>4.1</b>	<b>Fundamentos Básicos da Criptografia</b> . . . . . 42
<b>4.2</b>	<b>Tipos de Sistemas Criptográficos</b> . . . . . 43
<i>4.2.1</i>	<i>Desvantagem do Uso da Criptografia por Chave Simétrica</i> . . . . . 44
<i>4.2.2</i>	<i>Vantagem do Uso da Criptografia por Chave Pública</i> . . . . . 44
<b>4.3</b>	<b>Aplicações de Curvas Elípticas à Criptografia</b> . . . . . 44
<i>4.3.1</i>	<i>Curva Elíptica e o Problema do Logaritmo Discreto</i> . . . . . 44
<b>4.4</b>	<b>Protocolo Diffie-Hellman (ECDH)</b> . . . . . 48
<i>4.4.1</i>	<i>Descrição do Protocolo (ECDH)</i> . . . . . 48
<b>5</b>	<b>CONSIDERAÇÕES FINAIS</b> <span style="float: right;"><b>51</b></span>
	<b>REFERÊNCIAS</b> <span style="float: right;"><b>52</b></span>

## 1 INTRODUÇÃO

Criptografia é uma área da Criptologia que trata do estudo das técnicas de escrever mensagens em cifra ou em código, de modo que somente o indivíduo autorizado possa decifrar e ler as mensagens. A criptografia é tão antiga quanto a própria escrita. Já verificava-se sua presença no sistema de escrita hieroglífica egípcia. Os romanos utilizavam códigos secretos para comunicar planos de guerra. Depois da Segunda Guerra Mundial, com a invenção dos sistemas computacionais eletrônicos, a área recebeu um enorme impulso incorporando complexos algoritmos matemáticos. Desde 1948, a criptografia passa a ser considerada uma ciência aplicada que se encarrega do estudo das técnicas matemáticas relacionadas com os aspectos da segurança da informação, tais como:

- **A confidencialidade**, que é usada para assegurar o conteúdo da informação, onde só pessoas autorizadas poderão sabê-lo.
- **A integridade dos dados**, que refere-se à alteração não autorizada dos dados.
- **A autenticação de dados**, que é relacionada com a identificação.
- **O não-repúdio**, que impede a uma entidade negar as ações acima.

No presente trabalho serão estudados os aspectos fundamentais da Criptografia em Curvas Elípticas, e, para tanto, o mesmo está organizado da seguinte maneira: no Capítulo 2, são apresentados os resultados básicos da Teoria dos Números e Estruturas Algébricas, necessários para o desenvolvimento deste trabalho; no Capítulo 3 é feito um breve estudo sobre a teoria das Curvas Elípticas; no Capítulo 4, são apresentados alguns fundamentos básicos da Criptografia e o Sistema Criptográfico utilizando Curvas Elípticas e, por fim, no Capítulo 5, são apresentadas as Considerações Finais do trabalho.

## 2 PRELIMINARES

Neste capítulo serão explorados conceitos e resultados básicos da Teoria dos Números seguindo as referências Santos (2009) e Vieira (2015) e estruturas algébricas seguindo a referência Vieira (2013), importantes para a construção dos pontos da curva elíptica necessários para o desenvolvimento do trabalho.

### 2.1 Teoria dos Números

A Teoria dos Números se dedica ao estudo das propriedades dos números inteiros  $\mathbb{Z}$ . Esta seção apresenta algumas definições e resultados vinculados a estas propriedades, dando ênfase ao estudo da divisão euclidiana e da relação de congruência.

#### 2.1.1 Princípio da Boa Ordem e Indução Finita

À seguir, listemos os axiomas:

$A_0$  : Princípio da Boa Ordem (PBO). Todo conjunto não vazio de inteiros positivos contém um elemento mínimo.

$A_1$  : Primeira Forma do Princípio de Indução Finita. Seja  $B$  um subconjunto dos inteiros positivos. Se  $B$  possui as duas seguintes propriedades:

- (i)  $1 \in B$
  - (ii)  $k + 1 \in B$  sempre que  $k \in B$
- então  $B$  contém todos os inteiros positivos.

$A_2$ : Segunda Forma do Princípio de Indução Finita. Seja  $B$  um subconjunto dos inteiros positivos. Se  $B$  possui as duas seguintes propriedades:

- (i)  $1 \in B$
  - (ii)  $k + 1 \in B$  sempre que  $1, 2, \dots, k \in B$
- então  $B$  contém todos os inteiros positivos.

*Observação 2.1.* Os princípios  $A_0$ ,  $A_1$  e  $A_2$  são equivalentes. Para detalhes ver (Santos, 2009, Apêndice A).

**Exemplo 2.1.** Considere o conjunto:

$$B = \left\{ n \in \mathbb{Z} : n > 0 \text{ e } 1 + x + x^2 + \dots + x^{n-1} = \frac{x^n - 1}{x - 1}, x \neq 1 \right\}.$$

Demonstrar-se-á que o conjunto  $B$  é formado por todos os inteiros positivos. Observe que:

- (i)  $1 \in B$ , pois,

$$x^0 = 1 = \frac{x^1 - 1}{x - 1}.$$

(ii) Suponha que  $n \in B$ , ou seja,

$$1 + x + x^2 + \dots + x^{n-1} = \frac{x^n - 1}{x - 1}.$$

(iii) Para  $n + 1$ , utilizando a hipótese de indução, tem-se:

$$\sum_{i=0}^{n-1} x^i + x^n = \frac{x^n - 1}{x - 1} + x^n = \frac{x^n - 1 + x^{n+1} - x^n}{x - 1} = \frac{x^{n+1} - 1}{x - 1}.$$

Pelo Princípio de Indução Finita (1ª forma),  $B$  contém todos os inteiros positivos.

### 2.1.2 Divisibilidade

**Definição 2.1.** Se  $a$  e  $b$  são inteiros, diz-se que  $a$  divide  $b$ , denotado por  $a \mid b$ , se existir um inteiro  $c$  tal que  $b = ac$ . Se  $a$  não divide  $b$ , escreve-se  $a \nmid b$ .

**Proposição 2.1.** Se  $a, b$  e  $c$  são inteiros,  $a \mid b$  e  $b \mid c$ , então  $a \mid c$ .

*Demonstração.* Como  $a \mid b$  e  $b \mid c$ , existem inteiros  $k_1$  e  $k_2$  com  $b = k_1a$  e  $c = k_2b$ . Substituindo o valor de  $b$  na equação  $c = k_2b$  tem-se  $c = k_2k_1a$  o que implica  $a \mid c$ .  $\square$

**Proposição 2.2.** Se  $a, b, c, m$  e  $n$  são inteiros,  $c \mid a$  e  $c \mid b$  então  $c \mid (ma + nb)$ .

*Demonstração.* Sejam  $c \mid a$  e  $c \mid b$ ,  $a = k_1c$  e  $b = k_2c$

$$a = k_1c, b = k_2c, \text{ logo}$$

$$ma = mk_1c, nb = nk_2c, \text{ daí } ma + nb = (mk_1 + nk_2)c \text{ portanto } c \mid (ma + nb).$$

$\square$

*Observação 2.2.* Seja  $a, b$  pertencentes ao conjunto dos números inteiros, com  $b \neq 0$ , então  $n/d$  nada mais é do que  $n$  ser divisível por  $d$ .

**Teorema 2.1.** Para  $a, d, n \in \mathbb{Z}$  divisão tem as seguintes propriedades:

- (i)  $n \mid n$ ;
- (ii)  $d \mid n \Rightarrow ad \mid an$ ;
- (iii)  $ad \mid an$  e  $a \neq 0 \Rightarrow d \mid n$ ;
- (iv)  $1 \mid n$ ;
- (v)  $n \mid 0$ ;
- (vi)  $d \mid n$  e  $n \neq 0 \Rightarrow |d| \leq |n|$ ;
- (vii)  $d \mid n$  e  $n \mid d \Rightarrow |d| = |n|$ ;
- (viii)  $d \mid n$  e  $d \neq 0 \Rightarrow (n/d) \mid n$ .

*Demonstração.* (i) Como  $n = 1 \cdot n$  segue da definição que  $n \mid n$ , inclusive para  $n = 0$ .

(ii) Se  $d \mid n$  então  $n = cd$  para algum inteiro  $c$ . Logo  $an = cad$ , o que conclui a prova do item.

(viii) Se  $d \mid n$  então  $n = k_1d$  e portanto  $n/d$  é um inteiro. Como  $(n/d) \cdot d = n$  segue da definição que  $(n/d) \mid n$ . Os demais itens também são consequências imediatas da definição.  $\square$

**Lema 2.1.** (*Propriedade Arquimediana*) *Considere dois inteiros  $a$  e  $b$ , com  $b \neq 0$ . Então, existe  $n \in \mathbb{Z}$  tal que  $nb \geq a$ .*

*Demonstração.* Ver (Vieira, 2013, Lema 2.2).  $\square$

**Teorema 2.2.** (*Eudoxius*) *Dados  $a$  e  $b$  inteiros com  $b \neq 0$  então  $a$  é um múltiplo de  $b$  ou se encontra entre dois múltiplos consecutivos de  $b$ , isto é, correspondendo a cada par de inteiros de  $a$  e  $b \neq 0$  existe um inteiro  $q$  tal que, para  $b > 0$ ,*

$$qb \leq a < (q + 1)b,$$

e para  $b < 0$

$$qb \leq a < (q - 1)b.$$

*Demonstração.* Seja  $A = \{(x + 1)b : xb \geq a, x \in \mathbb{Z}\}$ . Pelo Lema 2.1 tal conjunto é não vazio. Pelo Princípio da Boa Ordem ele possui um menor elemento da forma  $(q_0 + 1)b$ . Note que  $q_0b \notin A$ , pois,  $q_0b < (q_0 + 1)b$  e  $(q_0 + 1)b$  é elemento mínimo. Ou seja:

$$(q_0 - 1)b < a \leq q_0b.$$

$\square$

**Teorema 2.3.** (*Algoritmo da Divisão*) *Dados dois inteiros  $a$  e  $b$ ,  $b > 0$ , existe um único par de inteiros  $q$  e  $r$  tais que*

$$a = qb + r, \text{ com } 0 \leq r < b \text{ (} r = 0 \Leftrightarrow b \mid a \text{)}, \quad (2.1)$$

em que  $q$  é chamado de quociente e  $r$  de resto da divisão de  $a$  por  $b$ .

*Demonstração.* Pelo Teorema de Eudoxius, como  $b > 0$ , existe  $q$  satisfazendo:

$$qb \leq a < (q + 1)b. \quad (2.2)$$

De (2.2) segue que  $0 \leq a - qb$  e  $a - qb < b$ . Desta forma, definindo  $r = a - qb$ , tem-se garantida a existência. A fim de mostrar a unicidade, suponha a existência de outro par  $q_1$  e  $r_1$  verificando:



$$a = q_1b + r_1 \text{ com } 0 \leq r_1 < b. \quad (2.3)$$

Das Igualdades (2.1) e (2.3) segue que  $(qb + r) - (q_1b + r_1) = 0$ , daí  $b(q - q_1) = r_1 - r$ , o que implica  $b \mid (r_1 - r)$ . Mas, como  $r_1 < b$  e  $r < b$ , tem-se  $|r_1 - r| < b$  e, portanto, como  $b \mid (r_1 - r)$  deve-se ter  $r_1 - r = 0$  o que implica  $r = r_1$ . Logo  $q_1b = qb$ , então  $q_1 = q$ , uma vez que  $b \neq 0$ .  $\square$

*Observação 2.3.* O máximo divisor comum de dois inteiros  $a$  e  $b$ , com  $a$  ou  $b$  diferentes de zero e denotados por  $(a, b)$ , é o maior inteiro que divide  $a$  e  $b$ .

**Teorema 2.4.** *Seja  $d$  o máximo divisor comum de  $a$  e  $b$ , então existem inteiros  $n_0$  e  $m_0$  tais que  $d = n_0a + m_0b$ .*

*Demonstração.* Seja  $B$  o conjunto de todas as combinações lineares  $\{na + nb\}$ , onde  $n$  e  $m$  são inteiros. Este conjunto contém, claramente, números negativos, positivos e também o zero. Escolha  $n_0$  e  $m_0$  tais que  $c = n_0a + m_0b$  seja o menor inteiro positivo pertencente ao conjunto  $B$ . Provar-se-á que  $c \mid a$  e  $c \mid b$ .

Como as demonstrações são similares, mostrar-se-á apenas que  $c \mid a$ . A prova é por contradição. Suponha que  $c \nmid a$ . Neste caso, pelo Teorema 2.3, existem  $q$  e  $r$  tais que  $a = qc + r$  com  $0 < r < c$ . Portanto,  $r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b$ . Isto mostra que  $r \in B$ , pois  $(1 - qn_0)$  e  $(-qm_0)$  são inteiros, o que é uma contradição, uma vez que  $0 < r < c$  e  $c$  é o menor elemento positivo de  $B$ . Logo  $c \mid a$  e de forma análoga se prova que  $c \mid b$ .

Como  $d$  é um divisor comum de  $a$  e  $b$ , existem inteiros  $k_1$  e  $k_2$  tais que  $a = k_1d$  e  $b = k_2d$  e, portanto,  $c = n_0a + m_0b = n_0k_1d + m_0k_2d = d(n_0k_1 + m_0k_2)$ , o que implica  $d \mid c$ . Do Teorema 2.1 (vi), tem-se que  $d \leq c$  (ambos são positivos) e como  $d < c$  não é possível, uma vez que  $d$  é o máximo divisor comum, concluímos que  $d = n_0a + m_0b$ .  $\square$

**Teorema 2.5.** *Se  $a \mid bc$  e  $(a, b) = 1$ , então  $a \mid c$ .*

*Demonstração.* Como  $(a, b) = 1$ , pelo Teorema 2.4, existem inteiros  $n$  e  $m$  tais que  $na + mb = 1$ . Multiplicando-se os dois lados desta igualdade por  $c$  tem-se:  $n(ac) + m(bc) = c$ . Como  $a \mid ac$  e, por hipótese,  $a \mid bc$  então, pela Proposição 2.2,  $a \mid c$ .  $\square$

**Teorema 2.6.** *Se  $a$  e  $b$  são inteiros e  $a = qb + r$  em que  $q$  e  $r$  são inteiros, então  $(a, b) = (b, r)$ .*

*Demonstração.* Da relação  $a = qb + r$  pode-se concluir que todo divisor de  $b$  e  $r$  é um divisor de  $a$  (Proposição 2.2). Esta mesma relação, escrita na forma  $r = a - qb$ , diz que todo divisor de  $a$  e  $b$  é um divisor de  $r$ . Logo o conjunto dos divisores comuns de  $a$  e  $b$  é igual ao conjunto dos divisores comuns de  $b$  e  $r$ , o que garante o resultado de  $(a, b) = (b, r)$ .  $\square$

**Teorema 2.7.** *Sejam  $r_0 = a$  e  $r_1 = b$  inteiros não negativos com  $b \neq 0$ . Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_j = q_{j+1}r_{j+1} + r_{j+2}, \quad 0 \leq r_{j+2} < r_{j+1},$$

para  $j = 0, 1, 2, \dots, n-1$  e  $r_{n+1} = 0$  então  $(a, b) = r_n$ , o último resto não nulo.

*Demonstração.* Pelo Algoritmo de Euclides, inicialmente aplica-se o Teorema 2.3 para dividir  $r_0 = a$  por  $r_1 = b$  obtendo  $r_0 = q_1r_1 + r_2$ , em seguida divide-se  $r_1$  por  $r_2$  obtendo  $r_1 = q_2r_2 + r_3$  e assim sucessivamente, até a obtenção do resto por  $r_{n+1} = 0$ . Como a cada passo o resto é sempre menor do que o anterior e opera-se com números inteiros positivos, é claro que após um número finito de aplicações do Teorema 2.3, obter-se-á resto nulo. Tem-se, pois, a seguinte sequência de equações:

$$\begin{aligned} r_0 &= q_1r_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= q_2r_2 + r_3, & 0 < r_3 < r_2 \\ r_2 &= q_3r_3 + r_4, & 0 < r_4 < r_3 \\ &\vdots & \vdots \\ r_{n-2} &= q_{n-1}r_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0. \end{aligned}$$

A última dessas equações diz, pelo Teorema 2.6, que o máximo divisor comum de  $r_n$  e  $r_{n-1}$  é  $r_n$ . A penúltima, que este número é igual a  $(r_{n-1}, r_{n-2})$  e, prosseguindo desta maneira têm-se-á, por repetidas aplicações do Teorema 2.6, a sequência:

$$r_n = (r_{n-2}, r_n) = (r_{n-2}, r_{n-1}) = \dots = (r_1, r_2) = (r_0, r_1) = (a, b).$$

Portanto, o máximo divisor comum de  $a$  e  $b$  é o último resto não-nulo da sequência de divisões descrita.  $\square$

**Definição 2.2.** (Número Primo) Um número inteiro  $n$  ( $n > 1$ ) possuindo somente dois divisores positivos  $n$  e  $1$  é chamado primo. Se  $n > 1$  não é primo diz-se que  $n$  é composto.

**Proposição 2.3.** *Se  $p \mid ab$ ,  $p$  primo, então  $p \mid a$  ou  $p \mid b$ .*

*Demonstração.* Se  $p \nmid a$ , então  $(a, p) = 1$ , o que implica, pelo Teorema 2.5,  $p \mid b$ .  $\square$

**Teorema 2.8.** (Teorema Fundamental da Aritmética) *Todo inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.*

*Demonstração.* Se  $n$  é primo, não há nada a ser demonstrado. Suponha, pois,  $n$  composto. Seja  $p_1$  ( $p_1 > 1$ ) o menor dos divisores positivos de  $n$ . Afirma-se que  $p_1$  é primo. Isto é verdade, pois, caso contrário existiria  $p, 1 < p < p_1$  com  $p \mid n$ , contradizendo a escolha

de  $p_1$ . Logo,  $n = p_1 n_1$ . Se  $n_1$  for primo a prova está completa. Caso contrário, seja  $p_2$  o menor fator de  $n_1$ . Pelo argumento anterior,  $p_2$  é primo e tem-se que  $n = p_1 p_2 n_2$ .

Repetindo este procedimento, obtêm-se uma sequência decrescente de inteiros positivos  $n_1, n_2, \dots, n_r$ . Como todos eles são inteiros maiores do que 1, este processo deve terminar. Como os primos na sequência  $p_1, p_2, \dots, p_k$  não são necessariamente distintos,  $n$  terá, em geral, a seguinte forma:

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}.$$

Para mostrar a unicidade, usa-se indução ( $2^{\text{a}}$  forma) em  $n$ . Para  $n = 2$  a afirmação é verdadeira. Suponha, então, que ela se verifica para todos os inteiros maiores do que 1 e menores do que  $n$ . Se  $n$  é primo, não há nada a provar. Suponha, então, que  $n$  seja composto e que tenha duas fatorações:

$$n = p_1 p_2 \dots p_s = q_1 q_2 \dots q_r.$$

Provar-se-á que  $s = r$  e que cada  $p_i$  é igual a algum  $q_j$ . Como  $p_1$  divide o produto  $q_1 q_2 \dots q_r$  ele divide pelo menos um dos fatores  $q_j$ . Sem perda de generalidade pode-se supor que  $p_1 \mid q_1$ . Como são ambos primos, isto implica  $p_1 = q_1$ . Logo,  $n/p_1 = p_2 \dots p_s = q_2 \dots q_r$ . Como  $1 < n/p_1 < n$ , a hipótese de indução diz que as duas fatorações são idênticas, isto é,  $s = r$ , a menos da ordem, as fatorações  $p_1 p_2 \dots p_s$  e  $q_1 q_2 \dots q_s$  são iguais.  $\square$

### 2.1.3 Congruência

Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ . Diz-se que  $a$  e  $b$  são congruentes módulo  $n$ , em símbolos  $a \equiv b \pmod{n}$ , quando  $a - b$  é divisível por  $n$ . Caso contrário, diz-se que  $a$  não é congruente a  $b$  módulo  $n$  e denota-se por  $a \not\equiv b \pmod{n}$ .

*Observação 2.4.* Usar-se-á também a notação mais simples  $\equiv_n$  para representar a relação de congruência módulo o inteiro  $n$ .

**Exemplo 2.2.**  $9^4 \equiv 1 \pmod{5}$ , pois

$$9^4 - 1 = (9^2 - 1)(9^2 + 1) = 5 \times 1.312.$$

**Teorema 2.9.** *Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ . Então  $a \equiv b \pmod{n}$  se, e somente se,  $a$  e  $b$  possuem o mesmo resto quando divididos por  $n$ .*

*Demonstração.* Suponha que  $a \equiv b \pmod{n}$ . Então existe  $k \in \mathbb{Z}$  tal que

$$a - b = kn.$$

Agora, sabe-se pelo algoritmo da divisão que dados  $a, b \in \mathbb{Z}$ , existem  $q_1, q_2, r_1, r_2 \in \mathbb{Z}$  tais que:

$$\begin{cases} a = q_1 \cdot n + r_1, & 0 \leq r_1 < n \\ b = q_2 \cdot n + r_2, & 0 \leq r_2 < n \end{cases} . \quad (2.4)$$

Das igualdades em (2.4), tem-se:

$$a - b = (q_1 - q_2) \cdot n + r_1 - r_2, \text{ com } |r_1 - r_2| < n. \quad (2.5)$$

Por fim, sendo  $a - b$  um múltiplo de  $n$ , segue de (2.5) que

$$r_1 - r_2 = 0 \Rightarrow r_1 = r_2.$$

Reciprocamente, suponhamos que

$$a = q_1 \cdot n + r \text{ e } b = q_2 \cdot n + r, \text{ com } 0 \leq r < n.$$

Então,

$$a - b = (q_1 - q_2) \cdot n,$$

isto é,  $n \mid (a - b)$ . Portanto,  $a \equiv b \pmod{n}$ .  $\square$

**Teorema 2.10.** *Sejam  $a, b, c, d, x, \in \mathbb{Z}$  e  $n \in \mathbb{N}$ . Então as seguintes condições são satisfeitas:*

1. *Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , então  $a + c \equiv b + d \pmod{n}$  e  $ac \equiv bd \pmod{n}$ .*
2. *Se  $a \equiv b \pmod{n}$ , então  $ax \equiv bx \pmod{n}$ .*
3. *Se  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ , então  $ax \equiv c \pmod{n} \Leftrightarrow bx \equiv d \pmod{n}$ .*
4. *Se  $a \equiv b \pmod{n}$ , então  $a^k \equiv b^k \pmod{n}$ ,  $\forall k \in \mathbb{N}$ .*

*Demonstração.* Serão provados apenas os itens 1 e 4. Para 1, suponha que  $a \equiv b \pmod{n}$  e  $c \equiv d \pmod{n}$ . Então existe  $m, y \in \mathbb{Z}$  tais que

$$a - b = xn \text{ e } c - d = yn.$$

Logo,

$$(a + c) - (b + d) = (a - b) + (c - d) = (x + y)n,$$

isto é,  $a + c \equiv b + d \pmod{n}$ . Por outro lado,

$$ac - bd = (b + xn)(d + yn) - bd = (by + dx + xyn)n,$$

isto é,  $ac \equiv bd \pmod{n}$ .

Agora, provar-se-á (4). Suponha que  $a \equiv b \pmod{n}$  e seja

$$X = \{k \in \mathbb{N} : a^k \equiv b^k \pmod{n}\}.$$

Então:

1.  $1 \in X$ .
2. Suponha, como hipótese de indução, que o resultado seja válido para algum  $k \in X$ , ou seja,  $a^k \equiv b^k \pmod{n}$ .

Como  $a \equiv b \pmod{n}$  e  $a^k \equiv b^k \pmod{n}$  tem-se, pelo ítem 1 do Teorema 2.10 que  $a^{k+1} \equiv b^{k+1} \pmod{n}$ . Logo,  $k+1 \in X$ . Portanto,  $X = \mathbb{N}$ .  $\square$

**Teorema 2.11.** *Seja  $n$  um inteiro positivo. A relação  $\equiv_n$  é uma relação de equivalência no conjunto dos inteiros.*

*Demonstração.* Seja  $n$  um inteiro positivo. Provar-se-á que  $\equiv_n$  é reflexiva, simétrica e transitiva.

I -  $\equiv_n$  é reflexiva. Seja  $x$  um inteiro arbitrário. Como  $0 \cdot n = 0$ , tem-se que  $n \mid 0$ , ou seja,  $n \mid (x - x)$ . Portanto,  $x \equiv_n x$ .

II -  $\equiv_n$  é simétrica. Sejam  $a$  e  $b$  inteiros e suponha que  $a \equiv_n b$ . Isto significa que  $n \mid (a - b)$ . Assim, existe um inteiro  $k$  tal que  $(a - b) = kn$ . Mas então  $(a - b) = (-k)n$ . Assim,  $n \mid (b - a)$  e, portanto,  $b \equiv_n a$ .

III -  $\equiv$  é transitiva. Sejam  $a$ ,  $b$  e  $z$  inteiros tais que  $a \equiv_n b$  e  $b \equiv_n z$ , ou seja,  $n \mid (a - b)$  e  $n \mid (b - z)$ . Logo  $a - b = k_1n$  e  $b - z = k_2n$ . Somando-se membro a membro as igualdades anteriores, tem-se  $a - z = (k_1 + k_2)n$  e, portanto,  $n \mid (a - z) \rightarrow a \equiv_n z$ .  $\square$

Sejam  $a$  e  $n$  inteiros com  $n \neq 0$ . Pelo algoritmo da divisão, existem únicos inteiros  $q$  e  $r$  tais que  $a = q \cdot n + r$ , com  $0 \leq r < n$ . Daí tem-se:

$$1) \text{ Se } r = 0 \implies a - 0 = q \cdot n \implies n \mid (a - 0) \implies a \equiv 0 \pmod{n}.$$

$$2) \text{ Se } r = 1 \implies a - 1 = q \cdot n \implies n \mid (a - 1) \implies a \equiv 1 \pmod{n}.$$

⋮

$$n - 1) \text{ Se } r = n - 1 \implies a - (n - 1) = q \cdot n \implies n \mid (a - (n - 1)) \implies a \equiv (n - 1) \pmod{n}.$$

Ou seja, qualquer que seja  $a \in \mathbb{Z}$ ,

$$a \equiv_n 0 \text{ ou } a \equiv_n 1 \text{ ou } a \equiv_n 2 \text{ ou } \dots \text{ ou } a \equiv_n (n - 1).$$

Portanto,  $\equiv_n$  possui  $n$  classes de equivalência, são elas  $\bar{0}$ ,  $\bar{1}$ ,  $\bar{2}$ ,  $\dots$ ,  $\overline{n-1}$ . Daí, considerando o conjunto  $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ ; tal conjunto é uma partição dos inteiros e será denominado conjunto dos inteiros módulo  $n$ .

### 2.1.4 Resíduos Quadráticos

Nesta subseção será estudada as soluções para a congruência  $x^2 \equiv a \pmod{n}$  em que  $(a, n) = 1$ . Esse estudo será iniciado com o teorema a seguir.

**Teorema 2.12.** *Para  $p$  um primo ímpar e  $a$  um inteiro não-divisível por  $p$ , a congruência  $x^2 \equiv a \pmod{p}$ , caso tenha uma solução, tem exatamente duas soluções incongruentes módulo  $p$ .*

*Demonstração.* Caso esta congruência tenha uma solução  $x_1$ , claramente  $-x_1$  também será solução, uma vez que

$$(-x_1)^2 = x_1^2 \equiv a \pmod{p}.$$

Mostrar-se-á que estas soluções  $x_1$  e  $-x_1$  são incongruentes módulo  $p$ . Se  $x_1 \equiv -x_1 \pmod{p}$ , então ter-se-ia  $2x_1 \equiv 0 \pmod{p}$  e, como  $p$  é ímpar e  $p \nmid x_1$  (pois  $p \mid (x_1^2 - a)$  e  $p \nmid a$ ), isto é impossível. Precisa-se mostrar que só existem duas soluções incongruentes. Seja  $y$  uma solução de  $x^2 \equiv a \pmod{p}$ , i.e.,  $y^2 \equiv a \pmod{p}$ . Como  $x_1$  é solução tem-se  $x_1^2 \equiv y^2 \equiv a \pmod{p}$  e, portanto,  $x_1^2 - y^2 = (x_1 + y)(x_1 - y) \equiv 0 \pmod{p}$ . Logo,  $p \mid (x_1 + y)$  ou  $p \mid (x_1 - y)$ , o que implica  $y \equiv -x_1 \pmod{p}$  ou  $y \equiv x_1 \pmod{p}$ .  $\square$

**Definição 2.3.** Sejam  $a$  e  $n$  inteiros com  $(a, n) = 1$ . Diz-se que  $a$  é um resíduo quadrático módulo  $n$  se a congruência  $x^2 \equiv a \pmod{n}$  tiver solução. Caso a mesma não tenha solução, diz-se que  $a$  não é um resíduo quadrático módulo  $n$  ou que  $a$  é um resíduo não-quadrático.

**Exemplo 2.3.** Como  $5^2 \equiv 1 \pmod{8}$ , então 1 é um resíduo quadrático módulo 8.

**Teorema 2.13.** *Seja  $p$  um primo ímpar. Dentre os números  $1, 2, \dots, p-1$ , metade desses números são resíduos quadráticos e metade resíduos não-quadráticos*

*Demonstração.* Considere os quadrados dos números de 1 a  $p-1$ . Como  $1^2 \equiv 1 \pmod{p}$  sabe-se pelo Teorema 2.12 que  $-1$  também é a solução de  $x^2 \equiv 1 \pmod{p}$ , mas  $-1 \equiv p-1 \pmod{p}$ . Logo, 1 e  $p-1$  são as únicas soluções de  $x^2 \equiv 1 \pmod{p}$ . Tome, agora,  $2^2$  que será congruente a algum número  $k$  diferente de 1. Como  $-2 \equiv p-2 \pmod{p}$ , 2 e  $p-2$  são as únicas soluções incongruentes de  $x^2 \equiv k \pmod{p}$ . É claro que se  $p > 3$ ,  $k$  será igual a 4. Já tem-se, portanto, dois pares  $(1, p-1)$  e  $(2, p-2)$ , cada par sendo as duas únicas soluções de uma congruência do tipo  $x^2 \equiv a \pmod{p}$ . Procedendo desta maneira ter-se-á, ao final,  $(p-1)/2$  pares, cada um solução para uma dentre  $(p-1)/2$  congruências  $x^2 \equiv a_i \pmod{p}$  associados a exatamente  $(p-1)/2$  dos números  $1, 2, 3, \dots, p-1$ . Os  $(p-1)/2$  números  $a_i$ 's são os  $(p-1)/2$  resíduos quadráticos. Os restantes  $(p-1)/2$  não são resíduos quadráticos.  $\square$

## 2.2 Estruturas Algébricas

Nesse sentido esta seção é importante pois, como foi trabalhado com curvas elípticas de cardinalidade prima, nota-se a formação de grupos cíclicos finitos e, portanto, todo o

ponto da curva é um ponto gerador dela mesma. Observar-se-á com maior profundidade operações definidas sobre conjuntos e suas propriedades algébricas. Será apresentada, inicialmente, uma definição formal de operação.

### 2.2.1 Grupos

**Definição 2.4.** (Operação binária) Seja  $A$  um conjunto não vazio. Uma função  $\star : A \times A \rightarrow A$  chama-se operação binária sobre  $A$ .

**Proposição 2.4.** *Seja  $n$  um número natural. Então:*

$$\begin{aligned} + : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\longmapsto \bar{a} + \bar{b} = \overline{a + b} \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{Z}_n \times \mathbb{Z}_n &\longrightarrow \mathbb{Z}_n \\ (\bar{a}, \bar{b}) &\longmapsto \bar{a} \cdot \bar{b} = \overline{a \cdot b} \end{aligned}$$

definem duas operações de adição e multiplicação sobre  $\mathbb{Z}_n$ .

*Demonstração.* Sejam  $\bar{a}_1, \bar{a}_2, \bar{b}_1, \bar{b}_2 \in \mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$  tais que  $\bar{a}_1 = \bar{a}_2$  e  $\bar{b}_1 = \bar{b}_2$ .

Logo, por definição,  $a_1 \equiv a_2 \pmod{n}$  e  $b_1 \equiv b_2 \pmod{n}$ . Do Teorema 1.10, segue que

$$(a_1 + b_1) \equiv (a_2 + b_2) \pmod{n} \text{ e portanto } \overline{a_1 + b_1} = \overline{a_2 + b_2}.$$

Por isso,

$$\bar{a}_1 + \bar{b}_1 = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \bar{a}_2 + \bar{b}_2.$$

Desse modo, pelo Teorema 1.10,

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}, \text{ portanto, } \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2}.$$

E assim,

$$\bar{a}_1 \cdot \bar{b}_1 = \overline{a_1 \cdot b_1} = \overline{a_2 \cdot b_2} = \bar{a}_2 \cdot \bar{b}_2.$$

□

As operações sobre  $\mathbb{Z}_n$  dadas na Proposição 2.4 se valem de importantes propriedades conforme destacadas no teorema à seguir.

**Teorema 2.14.** *As operações de adição e multiplicação sobre  $\mathbb{Z}_n$  têm as propriedades:*

$$(1) \bar{a} + (\bar{b} + \bar{c}) = (\bar{a} + \bar{b}) + \bar{c}, \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n \text{ (a adição é associativa).}$$

- (2)  $\bar{a} + \bar{b} = \bar{b} + \bar{a}$ ,  $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n$  (a adição é comutativa).
- (3)  $\bar{a} + \bar{0} = \bar{0} + \bar{a}$ ,  $\forall \bar{a} \in \mathbb{Z}_n$  (existência de elemento neutro da adição).
- (4) Dado  $\bar{a} \in \mathbb{Z}_n$ , existe  $\bar{b} \in \mathbb{Z}_n$ , tal que  $\bar{a} + \bar{b} = \bar{0}$  (existência do inverso aditivo para cada elemento em  $\mathbb{Z}_n$ ).
- (5)  $\bar{a} \cdot (\bar{b} \cdot \bar{c}) = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$ ,  $\forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$  (a multiplicação é associativa).
- (6)  $\bar{a} \cdot \bar{b} = \bar{b} \cdot \bar{a}$ ,  $\forall \bar{a}, \bar{b} \in \mathbb{Z}_n$  (a multiplicação é comutativa).
- (7)  $\bar{a} \cdot \bar{1} = \bar{a}$ ,  $\forall \bar{a} \in \mathbb{Z}_n$  (existência de elemento neutro da multiplicação).
- (8)  $\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$  (a multiplicação é distributiva sobre a adição).
- (9) Dado  $\bar{a} \in \mathbb{Z}_n$ , existe  $\bar{b} \in \mathbb{Z}_n$ , tal que  $\bar{a} \cdot \bar{b} = \bar{1}$  se, e somente se,  $\text{mdc}(a, n) = 1$  ( $\bar{a}$  tem inverso multiplicativo).

*Demonstração.* Demonstrar-se-á apenas os itens (1) e (4).

- (1) Considerando  $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ , e o fato de a adição em  $\mathbb{Z}$  ser associativa, obtêm-se

$$\bar{a} + (\bar{b} + \bar{c}) = \bar{a} + \overline{b+c} = \overline{a+(b+c)} = \overline{(a+b)+c} =$$

$$\overline{a+b+c} = \overline{(a+b)+c} = (\bar{a} + \bar{b}) + \bar{c},$$

ou seja, a adição é associativa.

- (4) Dado  $\bar{a} \in \mathbb{Z}_n$ , existe  $\bar{x} \in \mathbb{Z}$  tal que  $\bar{a} + \bar{x} = \bar{0}$  se, e somente se,  $\overline{a+x} = \bar{0}$ . Ou seja,  $\bar{a} + \bar{x} = \bar{0}$  se, e somente se,  $\overline{a+x} = \bar{n}$ , pois  $n \equiv 0 \pmod{n}$ . Mas,

$$a + x \in \bar{n} \Leftrightarrow a + x = nk \text{ para algum } k \in \mathbb{Z}.$$

Em particular, para  $k = 1$ ,  $x = n - a$ . Portanto,  $\bar{x} = \overline{n-a} \in \mathbb{Z}_n$  é o inverso aditivo de  $\bar{a}$ . □

**Definição 2.5.** Seja  $G$  um conjunto não vazio munido de uma operação binária  $\star$ , diz-se que o par  $(G, \star)$  é um grupo se satisfaz as seguintes condições:

- i)  $\star$  é associativa, ou seja,

$$a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in G.$$

- ii) Existe um elemento neutro  $e$  pertencente a  $G$  tal que:

$$a \star e = e \star a = a \quad \forall a \in G.$$

- iii) Todo elemento em  $G$  possui inverso, ou seja,

$$\forall a \in G, \exists a' \in G \text{ tal que } a \star a' = e.$$



O elemento  $a'$  inverso de  $a$  será denotado por  $a^{-1}$ .

Indica-se um grupo por  $(G, \star)$  ou simplesmente por  $G$ , se não houver dúvidas acerca da operação.

**Exemplo 2.4.** Tem-se que o conjunto  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$  munido com a operação de multiplicação é um grupo. De fato, o produto em  $\mathbb{R}$  é associativo e sabe-se que o número 1 é o neutro multiplicativo dos reais e dado  $a \in \mathbb{R}^*$  então  $\frac{1}{a}$  é o inverso de  $a$  e  $\frac{1}{a} \in \mathbb{R}^*$ . Logo,  $(\mathbb{R}^*, \cdot)$  é grupo.

**Exemplo 2.5.** Dado  $n \geq 2$ , o conjunto  $\mathbb{Z}_n$  com a multiplicação definida na Proposição 2.4 não é um grupo, pois  $\bar{0}$  não possui inverso. Além disso, pelo item (9) do Teorema 2.14, dado  $\bar{a} \in \mathbb{Z}_n$ , existe  $\bar{b} \in \mathbb{Z}_n$  tal que  $\bar{a} \cdot \bar{b} = \bar{1}$  se, e somente se,  $\text{mdc}(a, n) = 1$ . No entanto, pelo mesmo teorema, considerando o fato da multiplicação ser associativa, segue que o subconjunto próprio de  $\mathbb{Z}_n$

$$U(\mathbb{Z}_n) = \{\bar{a} \in \mathbb{Z}_n : \text{mdc}(a, n) = 1\},$$

é um grupo multiplicativo. Quando  $n$  for primo, é claro que

$$U(\mathbb{Z}_n) = \{\bar{1}, \bar{2}, \dots, \overline{n-1}\}.$$

Para  $n = 4$ , por exemplo,  $U(\mathbb{Z}_4) = \{\bar{1}, \bar{3}\}$ ; e com  $n = 7$ ,  $U(\mathbb{Z}_7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ .

### 2.2.2 Subgrupos

**Definição 2.6.** Seja  $G$  um grupo. Um subconjunto não vazio  $H$  de  $G$  é um subgrupo de  $G$  quando, munido com a operação de  $G$ , também é um grupo. Para indicar que  $H$  é um subgrupo de  $G$ , usaremos a seguinte notação:  $H < G$ .

**Exemplo 2.6.** De acordo com o Teorema 2.14,  $G = (\mathbb{Z}_4, +)$  em que  $+$  é a operação de adição definida na Proposição 2.4 é um grupo. Tem-se  $H = \{\bar{0}, \bar{2}\}$  é um subgrupo de  $G$ . De fato, note que a soma é bem definida em  $H$  e como a soma em  $\mathbb{Z}_n$  é associativa, então em  $H$  a soma é associativa, pois  $H$  é um subconjunto de  $\mathbb{Z}_4$ . Note também que  $\bar{0} \in H$  e sabe-se que  $\bar{0}$  é o neutro de  $\mathbb{Z}_n$ . Ademais tem-se que todos os elementos de  $H$  possuem seus inversos em  $H$ , pois o inverso de  $\bar{0}$  é o próprio e o inverso de  $\bar{2}$  também é o próprio. Logo,  $H$  também é um grupo, portanto por definição  $H < G$ .

**Proposição 2.5.** *Sejam  $G$  um grupo e  $H$  um subconjunto não-vazio de  $G$ . Então,*

$$H < G \Leftrightarrow h_1 h_2^{-1} \in H, \forall h_1, h_2 \in H.$$

*Demonstração.* ( $\Rightarrow$ ) Suponha que  $H < G$ . Sejam  $h_1, h_2 \in H$ . Como  $H < G$  então,  $H$  com a operação herdada de  $G$  é também um grupo e, portanto, existe  $h_2^{-1} \in H$  e sendo a operação fechada para os elementos de  $H$  segue que  $h_1 h_2^{-1} \in H$ .

( $\Leftarrow$ ) Suponha que  $h_1 h_2^{-1} \in H, \forall h_1, h_2 \in H$ . Como  $H$  é subconjunto de  $G$  e herda a operação do mesmo, então a propriedade associativa para os elementos de  $H$  é automaticamente satisfeita. Como  $H \neq \emptyset$  então existe  $h \in H$ . Por hipótese tem-se que  $hh^{-1} = e \in H$ . Por fim, se  $h \in H$  então  $eh^{-1} = h^{-1} \in H$ . Logo,  $H < G$ .  $\square$

**Definição 2.7.** Seja  $G$  um grupo. Dados  $a \in G$  e  $n \in \mathbb{Z}$ , define-se a  $n$ -ésima potência de  $a$  em símbolos  $a^n$ , da seguinte forma:

$$a^n = \begin{cases} e, & \text{se } n = 0 \\ a^{n-1}a, & \text{se } n > 0 \\ (a^{-1})^{-n}, & \text{se } n < 0 \end{cases}$$

ou seja, se  $n \in \mathbb{N}$ , então

$$a^n = \underbrace{a \ a \ \cdots \ a}_n, \text{ } n \text{ vezes}$$

e, se  $n < 0$ , então

$$a^n = \underbrace{a^{-1} \ a^{-1} \ \cdots \ a^{-1}}_n.$$

*Observação 2.5.* Se  $(G, +)$  é um grupo, então a definição anterior pode ser escrita da seguinte forma:

$$na = a^n = \begin{cases} e, & \text{se } n = 0 \\ (n-1)a + a, & \text{se } n > 0 \\ (-n)(-a), & \text{se } n < 0 \end{cases}$$

**Proposição 2.6.** *Seja  $G$  um grupo. Dados  $a \in G$  e  $n, m \in \mathbb{Z}$  são válidos:*

$$a^n a^m = a^{n+m} \quad e \quad (a^n)^m = a^{(nm)}.$$

*Demonstração.* Apenas o primeiro tópico será demonstrado. Mantendo  $m \geq 0$  fixo e usando indução em  $n$ , têm-se para  $n = 0$

$$a^0 a^m = ea^m = a^m = a^{0+m}.$$

Portanto, o resultado é válido para  $n = 0$ . Agora, suponha verdade para  $n$ , ou seja,

$$a^n a^m = a^{n+m}.$$

Com  $(n+m) \geq 0$ , provar-se-á que o resultado continua válido para  $n+1$  com  $(n+1+m) \geq 0$ .

Recorde que, por definição,

$$a^{n+1} = a^n a, \text{ e } a^{n+1+m} = a a^{n+m}$$

para  $n, n+m \geq 0$ . Assim, se  $n+1+m > 0$ , então  $n+m \geq 0$  e

$$a^{n+1} a^m = a a^n a^m = a a^{n+m} = a^{n+m+1},$$

em que a segunda igualdade segue da hipótese de indução. Se  $n+1+m = 0$ , então  $m = -(n+1)$ ; logo

$$a^{n+1} a^m = a^{n+1} a^{(-n-1)} = a^{n+1} (a^{-1})^{n+1} = e = a^0 = a^{n+1-(n+1)} = a^{n+1+m}.$$

E o resultado é válido para  $n+1$ , logo, por indução, é válida para  $n \in \mathbb{N}$  com  $n+m \geq 0$ . De modo geral, se  $n, m, \in \mathbb{Z}$  são quaisquer, escolha  $r > 0$  tal que

$$r+m > 0, \quad r+n > 0 \text{ e } r+m+n > 0.$$

Logo,

$$a^{m+n} = a^{m+n} e = a^{m+n} (a^r a^{-r}) = (a^{m+n} a^r) a^{-r} = a^{m+n+r-r} = a^{m+(n+r)} a^{-r} \implies$$

$$\text{e o resultado segue } a^m a^{n+r} a^{-r} = a^m a^n a^r a^{-r} = a^m a^n.$$

□

### 2.2.3 Grupos Cíclicos

**Definição 2.8.** Sejam  $G$  um grupo e  $a \in G$ . Considere  $H$  o conjunto de todas as potências de  $a$  (ou múltiplos de  $a$ , se a operação for adição), ou seja,

$$H = \{a^n, n \in \mathbb{Z}\}. \quad (2.6)$$

Portanto,  $H$  é um subgrupo de  $G$  denominado de subgrupo cíclico gerado por  $a$  e é denotado por  $H = \langle a \rangle$  ou  $H = [a]$ . Diz-se também que  $a$  é o gerador de  $H$ . O subgrupo  $H = \langle a \rangle$  é o menor subgrupo de  $G$  que contém  $a$ .

**Definição 2.9.** Um grupo  $G$  é dito cíclico quando existir  $a \in G$  tal que  $G = \langle a \rangle$ .

**Exemplo 2.7.** Para cada  $n \in \mathbb{N}$ ,  $n > 2$ , o grupo  $(\mathbb{Z}_n, +)$  é cíclico. De fato, dado  $\bar{a} \in \mathbb{Z}_n$ ,

$$\bar{a} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{a \text{ vezes}} = \underbrace{\bar{1} + \bar{1} + \cdots + \bar{1}}_{a \text{ vezes}}, \quad a\bar{1},$$

ou seja,  $\bar{a} = a\bar{1}$ , de modo que  $\bar{a} \in \langle \bar{1} \rangle$ . Isso mostra que  $\mathbb{Z}_n \subset \langle \bar{1} \rangle$ , e como  $\langle \bar{1} \rangle \subset \mathbb{Z}_n$ , então  $\langle \bar{1} \rangle = \mathbb{Z}_n$ .

**Proposição 2.7.** *Todo grupo cíclico é abeliano.*

*Demonstração.* Sejam  $G$  um grupo cíclico e  $a \in G$  tal que  $G = \langle a \rangle$ . Dados,  $x_1, x_2 \in G$ , tem-se  $x_1 = a^{n_1}$  e  $x_2 = a^{n_2}$ . Daí,

$$x_1 \cdot x_2 = a^{n_1} \cdot a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} \cdot a^{n_1} = x_2 \cdot x_1,$$

ou seja,  $G$  é abeliano. □

**Definição 2.10.** Sejam  $G$  um grupo e  $a \in G$ . Se existe  $n \in \mathbb{N}$  tal que  $a^n = e$ , diz-se que o elemento  $a$  tem ordem finita (ou é de ordem finita). Neste caso, o menor inteiro positivo  $m$  tal que  $a^m = e$  chama-se ordem de  $a$  e denota-se por  $O(a)$ . Caso não exista nenhum  $n \in \mathbb{N}$  satisfazendo tal propriedade, então o elemento  $a$  é dito de ordem infinita.

*Observação 2.6.* Em um grupo  $G$ , tem-se sempre

$$O(a) = 1 \Leftrightarrow a = e.$$

**Exemplo 2.8.** Pelo Exemplo 2.5,  $U(\mathbb{Z}_7) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$  com a operação de multiplicação definida na Proposição 2.4 é um grupo. Observe que

$$(\bar{2})^3 = \bar{8} = \bar{1} \text{ e } (\bar{5})^6 = \overline{15625} = \bar{1}.$$

Portanto,  $O(\bar{2}) = 3$  e  $O(\bar{5}) = 6$ .

**Proposição 2.8.** *Seja  $G$  um grupo.*

1. *Dado  $a \in G$ ,  $a \neq e$ , tem-se que  $O(a) = 2 \Leftrightarrow a = a^{-1}$ .*
2.  *$O(a) = O(a^{-1}) \quad \forall a \in G$ .*
3. *Se  $O(a) = 2$  para todo  $a \in G - \{e\}$ , então  $G$  é abeliano.*
4. *Se  $O(a) = mn$ , então  $O(a^m) = n$ .*

*Demonstração.* (1) Se  $O(a) = 2$ , então  $a^2 = e$ . Assim,

$$a^{-1}a^2 = a^{-1} \Leftrightarrow a = a^{-1}.$$

Reciprocamente, se  $a = a^{-1}$ , então  $aa = aa^{-1}$ , ou seja,  $a^2 = e$ , o que implica em  $O(a) = 2$ , pois  $a \neq e$ .

(2) Se  $a \in G$  tem ordem finita, então existe  $n \in \mathbb{N}$  tal que  $a^n = e$ . Mas,

$$a^n = e \Leftrightarrow a^{-n} = e \Leftrightarrow (a^{-1})^n = e.$$

Por isso, o menor  $m \in \mathbb{N}$  satisfazendo  $a^m = e$  é o menor que satisfaz  $(a^{-1})^m = e$ . Portanto,  $O(a) = O(a^{-1})$ . Por outro lado, se  $a$  tem ordem infinita, então pela digressão acima, a ordem de  $a^{-1}$  também é infinita.

(3) Por hipótese,  $O(a) = 2$  para todo  $a \in G - \{e\}$ . Logo, pelo item (1),

$$a = a^{-1}, \quad \forall a \in G.$$

Agora, dados  $a, b \in G$ , tem-se que  $ab \in G$ . Desse modo,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

o que mostra que  $G$  é abeliano.

(4) Inicialmente,

$$O(a) = nm \Rightarrow a^{nm} = e \Rightarrow (a^m)^n = e.$$

Só resta mostrar que  $n$  é o menor inteiro positivo satisfazendo  $(a^m)^n = e$ . Se  $r \in \mathbb{N}$  e  $r < n$  é tal que  $(a^m)^r = e$ , então

$$\begin{cases} a^{mr} = e, \\ mr < mn \end{cases}$$

Isso contradiz o fato de  $mn$  ser a ordem de  $a$ . Portanto,  $O(a^m) = n$ . □

**Teorema 2.15.** (Teorema de Lagrange) *Sejam  $G$  um grupo finito e  $H$  um subgrupo de  $G$ . Então, a ordem de  $H$  divide a ordem de  $G$ .*

*Demonstração.* Ver (Vieira, 2013, Teorema 3.12) □

**Corolário 2.1.** *Todo grupo  $G$  de ordem prima é cíclico. Em particular,  $G$  é abeliano.*

*Demonstração.* Seja  $|G| = p$  com  $p$  primo; assim, existe  $a \in G$  tal que  $a \neq e$ . Pelo Teorema de Lagrange,  $|\langle a \rangle|$  divide  $|G| = p$ . Sendo  $p$  um número primo, então  $|\langle a \rangle| = 1$  ou  $|\langle a \rangle| = p$ . Mas, como  $a \neq e$ , segue que  $|\langle a \rangle| = p$ , ou seja,  $\langle a \rangle = G$ , o que mostra que  $G$  é cíclico. Pela Proposição 1.6, tem-se que  $G$  é abeliano. □

### 2.2.4 Homomorfismo de Grupos

**Definição 2.11.** Sejam  $(G_1, \star)$  e  $(G_2, \cdot)$  grupos. Uma função  $f : G_1 \rightarrow G_2$  chama-se homomorfismo de  $G_1$  em  $G_2$  quando

$$f(a \star b) = f(a) \cdot f(b), \quad \forall a, b \in G_1$$

**Proposição 2.9.** *Seja  $f : G_1 \rightarrow G_2$  um homomorfismo de grupos. Se  $f$  é sobrejetor e  $G_1$  for abeliano, então  $G_2$  é necessariamente abeliano.*

*Demonstração.* Para  $a_1, b_1 \in G_2$ , mostremos que  $a_1 \cdot b_1 = b_1 \cdot a_1$ . Como  $f$  é sobrejetor, existem  $a, b \in G_1$  tais que  $f(a) = a_1$  e  $f(b) = b_1$ . Desde que  $G_1$  é abeliano, então  $a \star b = b \star a$ . Logo,

$$a_1 \cdot b_1 = f(a) \cdot f(b) = f(a \star b) = f(b \star a) = f(b) \cdot f(a) = b_1 \cdot a_1,$$

ou seja,  $a_1 \cdot b_1 = b_1 \cdot a_1$ , o que mostra que  $G_2$  é também abeliano.  $\square$

*Observação 2.7.* Nas condições da definição anterior, se  $e_1$  e  $e_2$  são os elementos neutros de  $G_1$  e  $G_2$ , respectivamente e  $a \in G_1$ , então

$$(i) \quad f(e_1) = e_2$$

$$(ii) \quad f(a^{-1}) = f(a)^{-1}.$$

De fato, para (i), tem-se:

$$e_1 \star e_1 = e_1 \Rightarrow f(e_1 \star e_1) = f(e_1) \Rightarrow f(e_1) \cdot f(e_1) = f(e_1) \Rightarrow f(e_1) = e_2.$$

Para (ii), tem-se:

$$a^{-1} \star a = e_1 \Rightarrow f(a^{-1} \star a) = f(e_1) \Rightarrow f(a^{-1}) \cdot f(a) = e_2 \Rightarrow f(a^{-1}) = f(a)^{-1}.$$

**Proposição 2.10.** *Seja  $f : G_1 \rightarrow G_2$  um homomorfismo de grupos. Então,  $Im(f) = \{f(a) : a \in G_1\}$  é subgrupo de  $G_2$ , chamado de imagem de  $f$ .*

*Demonstração.* Sendo  $f(e_1) = e_2$ , então  $Im(f) \neq \emptyset$ . Agora, dados  $x, y \in Im(f)$ , existem  $a, b \in G_1$  tais que  $f(a) = x$  e  $f(b) = y$ . Por isso,

$$x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \star b^{-1})$$

de maneira que  $x \cdot y^{-1} \in Im(f)$  e, pela Proposição 2.5,  $Im(f) < G_2$ .  $\square$

### 3 CURVAS ELÍPTICAS

Este capítulo apresenta um breve estudo sobre geometria algébrica e a teoria das curvas elípticas Vainsencher (2005), Hoffstein (2008) e Salehyan (2014), dando maior destaque as curvas elípticas definidas sobre corpos finitos.

#### 3.1 Espaço Projetivo

Nos cursos elementares de Geometria Analítica, quando estuda-se o problema de interseção de retas no plano cartesiano, observa-se que retas paralelas não possuem ponto em comum. Em outras palavras, o sistema dado pelas equações de retas paralelas não possui solução. Este problema se repete ao estudar a interseção da reta dada pela equação  $x = 0$  e a hipérbole dada pela equação  $xy = 1$ . Esta falha do plano cartesiano pode ser resolvida com o estudo destes problemas no plano projetivo construído a seguir.

**Definição 3.1.** Um conjunto não-vazio  $A$  munido de duas operações de adição  $+$  e multiplicação  $\cdot$  chama-se anel quando as propriedades seguintes são satisfeitas:

- $(A, +)$  é um grupo abeliano;
- A multiplicação é associativa, ou seja,  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ ,  $\forall x, y, z \in A$ ;
- A multiplicação é distributiva sobre a adição, isto é:  $x \cdot (y + z) = x \cdot y + x \cdot z$  e  $(x + y) \cdot z = x \cdot z + y \cdot z$ ,  $\forall x, y, z \in A$

**Definição 3.2.** Um anel  $\mathbb{K}$ , comutativo com unidade, chama-se corpo quando todo elemento não-nulo de  $\mathbb{K}$  tem inverso multiplicativo, ou seja, dado  $a \in \mathbb{K}$ ,  $a \neq O_{\mathbb{K}}$ , existe  $b \in \mathbb{K}$  tal que  $a \cdot b = 1_{\mathbb{K}}$ .

Seja  $\mathbb{K}$  um corpo e seja  $\mathbb{K}^3 = \{(a_0, a_1, a_2) ; a_i \in \mathbb{K}\}$ . Em  $\mathbb{K}^3 \setminus \{(0, 0, 0)\}$  defina a seguinte relação:

$$(a_0, a_1, a_2) \sim (b_0, b_1, b_2) \Leftrightarrow \exists \lambda \in \mathbb{K} \setminus \{0\}; (a_0, a_1, a_2) = \lambda(b_0, b_1, b_2). \quad (3.1)$$

Em suma, dois pontos distintos da origem estão relacionados, se pertencem a mesma reta que passa pela origem.

**Proposição 3.1.** A relação  $\sim$  definida em (3.1) é uma relação de equivalência.

*Demonstração.* [1]  $\sim$  é reflexiva, pois

$$(a_0, a_1, a_2) = 1(a_0, a_1, a_2), \text{ para } \lambda = 1.$$

Daí,

$$(a_0, a_1, a_2) \sim (a_0, a_1, a_2).$$

[2]  $\sim$  é simétrica. De fato, se

$$(a_0, a_1, a_2) \sim (b_0, b_1, b_2) \implies \exists \lambda \in \mathbb{K} \setminus \{0\} \text{ tal que } (a_0, a_1, a_2) = \lambda(b_0, b_1, b_2).$$

Como  $\mathbb{K}$  é um corpo e  $\lambda \neq 0$ , então  $\exists \lambda^{-1} \in \mathbb{K}$  tal que  $\lambda \cdot \lambda^{-1} = 1$ . Daí segue que

$$\lambda^{-1}(a_0, a_1, a_2) = \lambda\lambda^{-1}(b_0, b_1, b_2),$$

ou seja,

$$\lambda^{-1}(a_0, a_1, a_2) = 1(b_0, b_1, b_2),$$

logo,

$$(b_0, b_1, b_2) = \lambda^{-1}(a_0, a_1, a_2) \implies (b_0, b_1, b_2) \sim (a_0, a_1, a_2).$$

[3]  $\sim$  é transitiva. De fato, suponha

$$(a_0, a_1, a_2) \sim (b_0, b_1, b_2) \text{ e } (b_0, b_1, b_2) \sim (c_0, c_1, c_2).$$

Daí, existem  $\lambda_1, \lambda_2 \in \mathbb{K} \setminus \{0\}$  tais que

$$\begin{cases} (a_0, a_1, a_2) = \lambda_1(b_0, b_1, b_2) & (3) \\ (b_0, b_1, b_2) = \lambda_2(c_0, c_1, c_2) & (4) \end{cases}$$

Substituindo (4) em (3), tem-se

$$(a_0, a_1, a_2) = \lambda_1 [\lambda_2(c_0, c_1, c_2)] = \lambda_1\lambda_2(c_0, c_1, c_2)$$

e, como  $\lambda_1\lambda_2 \in \mathbb{K} \setminus \{0\}$ , segue que

$$(a_0, a_1, a_2) \sim (c_0, c_1, c_2).$$

□

Dessa forma, pode-se considerar o conjunto quociente:

$$\mathbb{P}_{\mathbb{K}}^2 := \frac{\mathbb{K}^3 \setminus \{(0, 0, 0)\}}{\sim}.$$

Tal conjunto é chamado de plano projetivo. Geometricamente,  $\mathbb{P}_{\mathbb{K}}^2$  é o conjunto de todas as retas em  $\mathbb{K}^3$  que passam pela origem. A classe de  $(a_0, a_1, a_2)$  ou um ponto de  $\mathbb{P}_{\mathbb{K}}^2$  é denominado por  $(a_0 : a_1 : a_2)$  e  $a_0, a_1$  e  $a_2$  serão denominados de coordenadas homogêneas de  $(a_0 : a_1 : a_2)$ .



A seguir será explicado como o plano projetivo resolve as falhas do plano cartesiano.

**Proposição 3.2.** *A aplicação*

$$\begin{aligned} \varphi : \mathbb{K}^2 &\longrightarrow \mathbb{P}_{\mathbb{K}}^2 \\ (a_0, a_1) &\longmapsto (a_0 : a_1 : 1) \end{aligned} ,$$

é injetiva.

*Demonstração.* Sejam  $(a_0, a_1), (b_0, b_1) \in \mathbb{K}^2$  tais que  $\varphi(a_0, a_1) = \varphi(b_0, b_1)$ . Daí, para algum  $\lambda_i \in \mathbb{K}$ :

$$(a_0 : a_1 : 1) = (b_0 : b_1 : 1) \Leftrightarrow \begin{cases} (a_0, a_1, 1) = \lambda_1 \cdot (b_0, b_1, 1) \Leftrightarrow 1 \cdot \lambda_1 \Leftrightarrow \lambda = 1 \\ (b_0, b_1, 1) = \lambda_2 \cdot (a_0, a_1, 1) \end{cases} \Rightarrow \lambda_1 = \lambda_2 = 1$$

$\Rightarrow (a_0, a_1) = (b_0, b_1)$ . Logo,  $\varphi$  é injetiva.  $\square$

Pela Proposição 3.2, ao identificar  $\mathbb{K}^2$  com sua imagem em  $\mathbb{P}_{\mathbb{K}}^2$ , pode-se considerar o plano cartesiano como um subconjunto do plano projetivo, em outras palavras,  $\mathbb{P}_{\mathbb{K}}^2$  possui uma cópia de  $\mathbb{K}^2$ . Lembrando a definição da relação de equivalência em 3.1, pode-se escrever

$$\varphi(\mathbb{K}^2) = \{(a_0 : a_1 : a_2) \mid a_2 \neq 0\}.$$

**Definição 3.3.** Os pontos do conjunto

$$H_{\infty} := \mathbb{P}_{\mathbb{K}}^2 \setminus \varphi(\mathbb{K}^2) = \{(a_0 : 1 : 0) \mid a_0 \in \mathbb{K}\} \cup \{(1 : 0 : 0)\},$$

são chamados de pontos no infinito.

*Observação 3.1.* Têm-se que,

$$\mathbb{P}_{\mathbb{K}}^2 = \varphi(\mathbb{K}^2) \cup H_{\infty}.$$

**Exemplo 3.1.** A hipérbole e a reta dadas pelas equações  $xy = 1$  e  $x = 0$  não se interceptam em  $\mathbb{K}^2$ . A hipérbole em  $\mathbb{P}_{\mathbb{K}}^2$  é dada pela equação  $xy = z^2$  e a reta por  $x = 0$ . A primeira possui dois pontos no infinito:  $(1 : 0 : 0)$  e  $(0 : 1 : 0)$ , e a segunda apenas um:  $(0 : 1 : 0)$ . Portanto  $(0 : 1 : 0)$  é o ponto de interseção entre a hipérbole e a reta.

Considere agora a seguinte aplicação:

$$\begin{aligned} \tilde{\varphi} : \varphi(\mathbb{K}^2) &\longrightarrow \mathbb{K}^2 \\ (a_0 : a_1 : a_2) &\longmapsto \left( \frac{a_0}{a_2}, \frac{a_1}{a_2} \right) . \end{aligned}$$

*Observação 3.2.* As aplicações  $\varphi$  e  $\tilde{\varphi}$  são tais que

$$\varphi \circ \tilde{\varphi} = Id_{\varphi(\mathbb{K}^2)} \quad \text{e} \quad \tilde{\varphi} \circ \varphi = Id_{\mathbb{K}^2}.$$

De fato,

$$\left\{ \begin{array}{l} [\varphi \circ \tilde{\varphi}](a_0, : a_1 : a_2) = \varphi\left(\frac{a_0}{a_2}, \frac{a_1}{a_2}\right) = \left(\frac{a_0}{a_2} : \frac{a_1}{a_2} : 1\right) = (a_0 : a_1 : a_2) \\ \text{e} \\ [\tilde{\varphi} \circ \varphi](a_0, a_1) = \tilde{\varphi}(\varphi(a_0, a_1)) = \tilde{\varphi}(a_0, : a_1 : 1) = (a_0, a_1) \end{array} \right.$$

Utilizando  $\varphi$  e  $\tilde{\varphi}$  é possível visualizar os objetos de  $\mathbb{K}^2$  em  $\mathbb{P}_{\mathbb{K}}^2$  e também olhar para os objetos no plano projetivo como união de seus pontos no infinito e o complementar destes pontos que é chamado de sua parte afim. Esta idéia será esclarecida através do exemplo a seguir.

**Exemplo 3.2.** Seja

$$C = \{(x : y : z) \mid x^2 - y^2 - z^2 = 0\} \subset \mathbb{P}_{\mathbb{K}}^2.$$

Ao substituir  $z = 0$ , obtêm-se  $x^2 - y^2 = 0$  ou  $x = \pm y$ . Então os pontos no infinito de  $C$  são  $(1 : \pm 1 : 0)$ . Sua parte afim é dada pela equação  $x^2 - y^2 = 1$ , uma hipérbole. Então pode-se pensar em  $C$  como a união de uma hipérbole e dois pontos no infinito.

### 3.2 Cúbicas

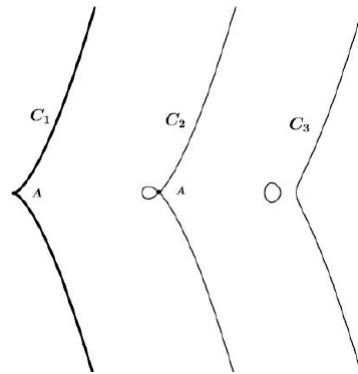
**Definição 3.4.** Sejam  $\mathbb{K}$  um corpo e  $P$  um elemento de  $\mathbb{K}[x, y, z]$  (Anel de Polinômios nas indeterminadas  $x, y$  e  $z$  com coeficientes em  $\mathbb{K}$ ) homogêneo de grau 3. O conjunto dos zeros de  $P$ , denotado por  $V(P)$ , é chamado de uma cúbica plana projetiva ou simplesmente uma cúbica.

**Exemplo 3.3.** Considere as cúbicas:  $C_1 : y^2z = x^3$ ,  $C_2 : y^2z = x^2(x + z)$  e  $C_3 : y^2z = x(x - z)(x - 2z)$ . Todas possuem um único ponto no infinito  $(0 : 1 : 0)$ . Suas partes afins, ou seja, as cúbicas afins correspondentes são  $y^2 = x^3$ ,  $y^2 = x^2(x + 1)$  e  $y^2 = x(x - 1)(x - 2)$ .

*Observação 3.3.* As curvas do Exemplo 3.3 são tais que em todos os pontos de  $C_3$  é possível escrever a equação da reta tangente à curva, o que não acontece nos casos de  $C_1$  e  $C_2$ . Isto ocorre pelo fato das funções implícitas  $y^2 = x^3$  e  $y^2 = x^2(x + 1)$  não possuírem derivadas no ponto  $A(0, 0)$ . Se calcular as derivadas parciais destas funções neste ponto, veremos que todas se anulam, o que não ocorre com  $C_3$ , pois, em cada ponto, pelo menos uma das derivadas parciais não é nula, o que nos leva à seguinte definição.

**Definição 3.5.** Um ponto  $(a : b : c) \in C = V(P)$  é dito um ponto singular se  $\frac{\partial}{\partial x}P(a : b : c) = \frac{\partial}{\partial y}P(a : b : c) = \frac{\partial}{\partial z}P(a : b : c) = 0$ . Se  $C$  tiver pelo menos um ponto singular, será chamada de uma curva singular. Caso contrário, será chamada curva suave.

*Observação 3.4.* Se uma curva é suave então ela não possui nós ou cúspides e, geometricamente, isto significa que o traço da curva não possui auto intersecções ou vértices.

**Figura 3.1** – Exemplos de cúbricas

**Exemplo 3.4.** As curvas  $C_1$  e  $C_2$  do Exemplo 3.3 são singulares, seus pontos singulares são  $(0 : 0 : 1)$  e  $(1 : 0 : 1)$  respectivamente; no entanto,  $C_3$  é uma curva suave. A Figura 3.1 mostra a representação geométrica dessas curvas.

**Definição 3.6.** Uma mudança de coordenadas projetiva de  $\mathbb{P}_{\mathbb{K}}^2$  é uma aplicação dada por  $P \mapsto AP$ , onde  $A$  é uma matriz invertível de ordem 3 e  $P(x : y : z) \in \mathbb{P}_{\mathbb{K}}^2$  é representado da forma  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ .

Diz-se que  $X_1, X_2 \subset \mathbb{P}_{\mathbb{K}}^2$  são projetivamente equivalentes, se existe uma mudança de coordenadas projetiva  $T$  tal que  $T(X_1) = X_2$ .

**Exemplo 3.5.** As cônicas  $C_1, C_2 \subset \mathbb{P}_{\mathbb{C}}^2$  dadas pelas equações

$$x^2 + y^2 + z^2 = 0 \quad \text{e} \quad y^2 = xz$$

são projetivamente equivalentes por meio da mudança de coordenadas dada por

$$\begin{pmatrix} i & 0 & -1 \\ 0 & 1 & 0 \\ i & 0 & 1 \end{pmatrix}, \text{ isto é, } (x : y : z) \mapsto (ix - z : y : ix + z).$$

De fato, observe que:

$$y^2 = (ix - z) \cdot (ix + z) = (ix)^2 - z^2 = -x^2 - z^2 \Rightarrow x^2 + y^2 + z^2 = 0.$$

**Teorema 3.1.** Uma cúbrica suave é projetivamente equivalente à cúbrica

$$y^2 z = x(x - z)(x - \lambda z),$$

em que  $\lambda \in \mathbb{C} \setminus \{0, 1\}$ .

*Demonstração.* Ver (Vainsencher, 2005, p.153). □

*Observação 3.5.* O único ponto no infinito de uma cúbica projetiva suave dada no Teorema 3.1 é  $\mathcal{O} = (0 : 1 : 0)$ , e sua parte afim é dada pela equação  $y^2 = f(x)$ , em que  $f$  é um polinômio de grau 3 em uma variável com raízes distintas. Esta forma de apresentar uma cúbica afim suave é conhecida por sua *forma de Weierstrass*.

Para finalizar esta seção, será apresentada a importante definição de curva elíptica.

**Definição 3.7.** Uma cúbica suave definida sobre o corpo  $\mathbb{K}$  é chamada de uma curva elíptica sobre  $\mathbb{K}$ .

### 3.3 Curvas Elípticas Sobre $\mathbb{Z}_p$

Em virtude das aplicações na criptografia, esta seção aborda o estudo das curvas elípticas sobre corpos finitos, ou seja, adotar-se-á  $\mathbb{K} = \mathbb{Z}_p$  com  $p$  um número primo, pois, neste caso,  $\mathbb{Z}_p$  com as operações definidas na Proposição 2.4 é um corpo ((Vieira, 2013, Proposição 5.7)).

A seguir será apresentada a importante definição de discriminante de um polinômio, que será utilizada na definição de curvas elípticas sobre corpos finitos. Mais detalhes ver Endler (1986).

**Definição 3.8.** (Discriminante) Sejam  $\mathbb{K}$  um corpo e  $F(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{K}[x]$ . O discriminante de  $F$  é definido por

$$\text{disc}(F) = \prod_{i=1}^n \prod_{j=i+1}^n (\alpha_j - \alpha_i)^2,$$

em que  $\alpha_1, \alpha_2, \dots, \alpha_n \in V(F)$ .

*Observação 3.6.* Analisando a definição do discriminante se pode concluir facilmente que se  $\text{disc}(F) \neq 0$  então  $F$  possui todos os zeros distintos, o que significa para o caso das cúbicas, que as mesmas são suaves.

**Proposição 3.3.** Para a cúbica  $F(x) \in \mathbb{K}[x]$  dada por  $F(x) = x^3 + ax + b$  tem-se que  $\text{disc}(F) = -4a^3 - 27b^2$ .

*Demonstração.* Pela Definição 3.8 têm-se,

$$\text{disc}(F) = (x_2 - x_1)^2 \cdot (x_3 - x_1)^2 \cdot (x_3 - x_2)^2, \quad (3.2)$$

em que  $x_1, x_2$  e  $x_3$  são os zeros de  $F$  em  $\mathbb{K}$ . Desenvolvendo a igualdade em (3.2) obtêm-se:

$$\begin{aligned}
disc(F) &= (x_2^2 - 2x_1x_2 + x_1^2) \cdot (x_3^2 - 2x_1x_3 + x_1^2) \cdot (x_3^2 - 2x_2x_3 + x_2^2) \\
&= (x_2^2x_3^2 - 2x_1x_2^2x_3 + x_1^2x_2^2 - 2x_1x_2x_3^2 + 4x_1^2x_2x_3 - 2x_1^3x_2 + x_1^2x_3^2 - 2x_1^3x_3 + x_1^4) \\
&\quad \cdot (x_3^2 - 2x_2x_3 + x_2^2) \\
&= -6(x_1x_2x_3)^2 + 2x_1x_2^2x_3^3 + 2x_1x_2^3x_3^2 + 2x_1^2x_2^3x_3 + 2x_1^2x_2x_3^3 + 2x_1^3x_2x_3^2 + 2x_1^3x_2^2x_3 \\
&\quad - 2x_1x_2^4x_3 - 2x_1x_2x_3^4 - 2x_1^4x_2x_3 - 2[(x_1x_2)^3 + (x_1x_3)^3 + (x_2x_3)^3] \\
&\quad + x_1^2x_2^2(x_1^2 + x_2^2) + x_1^2x_3^2(x_1^2 + x_3^2) + x_2^2x_3^2(x_2^2 + x_3^2). \tag{3.3}
\end{aligned}$$

Das relações de Girard para  $F$ , têm-se:

$$\begin{cases} x_1 + x_2 + x_3 &= 0 & (I) \\ x_1x_2 + x_1x_3 + x_2x_3 &= a & (II) \\ x_1x_2x_3 &= -b & (III) \end{cases} . \tag{3.4}$$

Utilizando a igualdade (II) em (3.4), obtêm-se:

$$(x_1x_2 + x_1x_3 + x_2x_3)^3 = a^3. \tag{3.5}$$

Segue do desenvolvimento da igualdade em (3.5) que

$$\begin{aligned}
&(x_1x_2)^3 + 3x_1^3x_2^2x_3 + 3x_1^3x_2x_3^2 + (x_1x_3)^3 + 3x_1^2x_2^3x_3 \\
&+ 6(x_1x_2x_3)^2 + 3x_1^2x_2x_3^3 + 3x_1x_2^3x_3^2 + 3x_1x_2^2x_3^3 + (x_2x_3)^3 = a^3. \tag{3.6}
\end{aligned}$$

Substituindo  $x_1x_2x_3 = -b$  em (3.6), têm-se:

$$\begin{aligned}
(x_1x_2)^3 + (x_1x_3)^3 + (x_2x_3)^3 &= a^3 + 3bx_1x_2(x_1 + x_2) + 3bx_1x_3(x_1 + x_3) \\
&\quad + 3bx_2x_3(x_2 + x_3) - 6b^2 \tag{3.7}
\end{aligned}$$

Agora, da igualdade (I) em (3.4), segue

$$x_1 + x_2 = -x_3, \quad x_1 + x_3 = -x_2 \quad \text{e} \quad x_2 + x_3 = -x_1. \tag{3.8}$$

Substituindo as igualdades dadas por (3.8) em (3.7) e novamente usando o fato de que  $x_1x_2x_3 = -b$ , têm-se:

$$\begin{aligned}
(x_1x_2)^3 + (x_1x_3)^3 + (x_2x_3)^3 &= a^3 + 3b^2 + 3b^2 + 3b^2 - 6b^2 \\
&= a^3 + 3b^2. \tag{3.9}
\end{aligned}$$

Substituindo as igualdades (III) de (3.4) e (3.9) em (3.3), têm-se:

$$\begin{aligned} \text{disc}(F) &= -6b^2 - 2bx_2x_3(x_2 + x_3) - 2bx_1x_2(x_1 + x_2) - 2bx_1x_3(x_1 + x_3) \\ &\quad + 2b(x_1^3 + x_2^3 + x_3^3) - 2(a^3 + 3b^2) + x_2^2x_3^2(x_2^2 + x_3^2) \\ &\quad + x_1^2x_2^2(x_1^2 + x_2^2) + x_1^2x_3^2(x_1^2 + x_3^2). \end{aligned} \quad (3.10)$$

Ainda das relações de Girard, utilizando novamente (I), têm-se:

$$x_1^2 + x_2^2 = x_3^2 - 2x_1x_2, \quad x_1^2 + x_3^2 = x_2^2 - 2x_1x_3 \quad \text{e} \quad x_2^2 + x_3^2 = x_1^2 - 2x_2x_3 \quad (3.11)$$

e,

$$(x_1 + x_2)^3 = -x_3^3 \Rightarrow x_1^3 + x_2^3 + x_3^3 = -3x_1x_2(x_1 + x_2).$$

Daí, segue que

$$x_1^3 + x_2^3 + x_3^3 = -3b. \quad (3.12)$$

Substituindo as igualdades em (3.8), em (3.11) e (3.12) na igualdade (3.10), têm-se:

$$\begin{aligned} \text{disc}(F) &= -6b^2 - 2b^2 - 2b^2 - 2b^2 - 6b^2 - 2a^3 - 6b^2 + b^2 + b^2 + b^2 - 2(a^3 + 3b^2) \\ &= -4a^3 - 27b^2 \end{aligned}$$

□

**Exemplo 3.6.** É possível verificar através do  $\text{disc}(F)$  quando uma curva é boa para se encriptar. Isso ocorre quando o  $\text{disc}(F) \neq 0$ . Daí

$$-4a^3 - 27b^2 \neq 0, \quad \text{então} \quad 4a^3 + 27b^2 \neq 0$$

. Usando a cúbica  $y^2 = x^3 + x + 1$ , tem-se que:

$$4(1)^3 + 27(1)^2 = 31 \neq 0.$$

A partir da Observação 3.6 e da Proposição 3.3, seguirá a definição de curva elíptica sobre  $\mathbb{Z}_p$ .

**Definição 3.9.** A curva elíptica sobre  $\mathbb{Z}_p$ ,  $p > 3$ , denotada por  $E(\mathbb{Z}_p)$ , é o conjunto de todos os pares  $(\bar{x}, \bar{y}) \in \mathbb{Z}_p^2$  que satisfazem

$$y^2 \equiv (x^3 + a \cdot x + b) \pmod{p},$$

junto com o ponto imaginário no infinito  $\mathcal{O}$ , em que  $\bar{a}, \bar{b} \in \mathbb{Z}_p$  e  $4 \cdot a^3 + 27 \cdot b^2 \neq 0 \pmod{p}$ .

**Exemplo 3.7.** Considere a Curva Elíptica

$$E : y^2 = x^3 + x + 1 \text{ sobre o corpo } \mathbb{Z}_7.$$

Sabe-se do Teorema 2.13 que dentre os números  $1, 2, \dots, 6$ , metade são resíduos quadráticos e metade não são. Nesse caso, têm-se:

$$1^2 \equiv 1 \pmod{7}, \quad 2^2 \equiv 4 \pmod{7}, \quad 3^2 \equiv 2 \pmod{7}.$$

Observe agora que substituindo o valor de  $x$  por 0 na equação que descreve  $E$ , têm-se:

$$y^2 \equiv 1 \pmod{7}. \quad (3.13)$$

Pelo Teorema 2.12, a congruência em (3.13) possui exatamente duas soluções que são 1 (que é resíduo quadrático) e  $-1$ ; porém,  $-1 \equiv 6 \pmod{7}$ . Daí, os pontos  $(0, 1), (0, 6) \in E$ . Por outro lado, fazendo  $x = 2$  na equação que descreve  $E$ , têm-se:

$$y^2 \equiv 4 \pmod{7}. \quad (3.14)$$

Novamente pelo Teorema 2.12, a congruência em (3.14) possui exatamente duas soluções que são 2 (que é resíduo quadrático) e  $-2$ ; porém,  $-2 \equiv 5 \pmod{7}$ . Daí, os pontos  $(2, 2), (2, 5) \in E$ . Logo, o conjunto  $E(\mathbb{Z}_7)$  possui cinco elementos e é dado por,

$$E(\mathbb{Z}_7) = \{\mathcal{O}, (0, 1), (0, 6), (2, 2), (2, 5)\}.$$

*Observação 3.7.* Para os valores de  $x = 1, 3, 4, 5$  e  $6$ , não existe valores para a variável  $y$  tais que o par  $(x, y)$  satisfaça a equação da curva.

### 3.4 Operação com Pontos de uma Curva Elíptica

Nesta seção será definida uma operação entre pontos de uma curva elíptica que a transformará em um grupo abeliano finito.

**Definição 3.10.** Sejam  $E$  uma Curva Elíptica e  $P, Q \in E$ . Define-se:

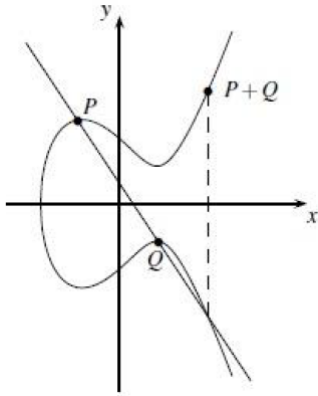
$$P \oplus Q = \text{Reflex}_X \{ \{r_{P,Q} \cap E\} \setminus \{P, Q\} \},$$

em que  $\text{Reflex}_X A$  é o reflexo do ponto  $A$  em relação ao eixo  $X$  e  $r_{P,Q}$  é a reta que contém os pontos  $P$  e  $Q$ .

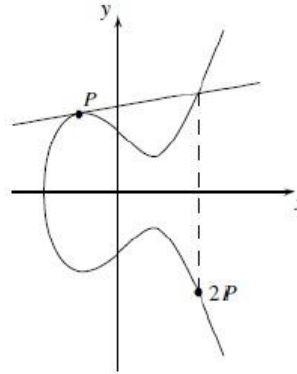
*Observação 3.8.* Para tornar mais simples, utiliza-se a notação aditiva usual, ou seja,  $P \oplus Q = P + Q$ .

As Figuras 3.2 e 3.3 apresentam uma interpretação geométrica para a soma de dois

**Figura 3.2** – Adição dos pontos  $P$  e  $Q$  com  $P \neq Q$ .



**Figura 3.3** – Adição dos pontos  $P$  e  $Q$  com  $P = Q$ .



Fonte: (Paar, 1998, p.243).

pontos de uma curva elíptica nos casos em que esses pontos são distintos ou iguais, respectivamente.

*Observação 3.9.* (a) Se  $P \neq Q$  e  $Q = \text{Reflex}_X(P)$ , então  $P + Q = \mathcal{O}$ .

(b) Se a reta tangente a  $E$  passando por  $P$  for vertical, então  $2P = \mathcal{O}$ .

(c) O reflexo de  $P = (x_P, y_P)$  é o ponto  $R = (x_P, -y_P)$  que denotar-se-á por  $R = -P$ .

(d)

$$nP = \underbrace{P + P + P + \dots + P}_{n \text{ cópias}}$$

**Teorema 3.2.** *Sejam,*

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

*uma curva elíptica e  $P_1, P_2 \in E$ .*

(a) *Se  $P_1 = \mathcal{O}$ , então  $P_1 + P_2 = P_2$ ;*

(b) *Se  $P_2 = \mathcal{O}$ , então  $P_1 + P_2 = P_1$ ;*

(c) *Se  $P_1 = (x_1, y_1)$  e  $P_2 = (x_2, y_2)$  e  $x_1 = x_2$  e  $y_1 = -y_2$ , então  $P_1 + P_2 = \mathcal{O}$ ;*

(d) *Caso contrário, defina  $\lambda$  por*

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{se } P_1 \neq P_2 \\ \frac{3 \cdot x_1^2 + a}{2y_1}, & \text{se } P_1 = P_2 \end{cases}$$

*e sejam*

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

*Então,  $P_1 + P_2 = (x_3, y_3)$ .*

*Demonstração.* (a), (b) e (c) seguem diretamente da definição da Operação e da sua



interpretação geométrica. (d) Da definição da operação, têm-se:

$$P_1 + P_2 = -\{\{r_{P_1, P_2} \cap E\} \setminus \{P_1, P_2\}\}. \quad (3.15)$$

Sabe-se do cálculo que:

$$r_{P_1, P_2} : y = \lambda \cdot x + n. \quad (3.16)$$

Se em (3.16),  $P_1 \neq P_2$  então  $r_{P_1, P_2}$  é secante à curva  $E$  e

$$\lambda = \frac{\Delta y}{\Delta x} = \frac{y_2 - y_1}{x_2 - x_1}.$$

Por outro lado, se  $P_1 = P_2$  então  $r_{P_1, P_2}$  é tangente à curva  $E$  e  $\lambda$  é o coeficiente angular dessa reta, que é obtido através da derivada da função  $y(x)$  definida implicitamente pela equação  $y^2 = x^3 + a \cdot x + b$ . Mas, têm-se que:

$$2 \cdot y \cdot y' = 3 \cdot x^2 + a \Rightarrow y'(x) = \frac{3 \cdot x^2 + a}{2y}.$$

Portanto,

$$\lambda = y'(x_1) = \frac{3 \cdot x_1^2 + a}{2y(x_1)} = \frac{3 \cdot x_1^2 + a}{2y_1}.$$

Agora, substituindo (3.16) na equação de  $E$ , têm-se

$$x^3 - \lambda^2 \cdot x^2 + (a - 2 \cdot n \cdot \lambda) \cdot x + b - n^2 = 0. \quad (3.17)$$

Das relações de Girard, segue que:

$$x_1 + x_2 + x_3 = \lambda^2 \Rightarrow x_3 = \lambda^2 - x_1 - x_2. \quad (3.18)$$

Como  $P_1 \in r_{P_1, P_2}$ , então:

$$y_1 = \lambda \cdot x_1 + n \Rightarrow n = y_1 - \lambda \cdot x_1. \quad (3.19)$$

Substituindo (3.18) e (3.19) em (3.16), obtêm-se:

$$y'_3 = \lambda \cdot x_3 + y_1 - \lambda \cdot x_1 \Rightarrow y'_3 = \lambda \cdot (x_3 - x_1) + y_1.$$

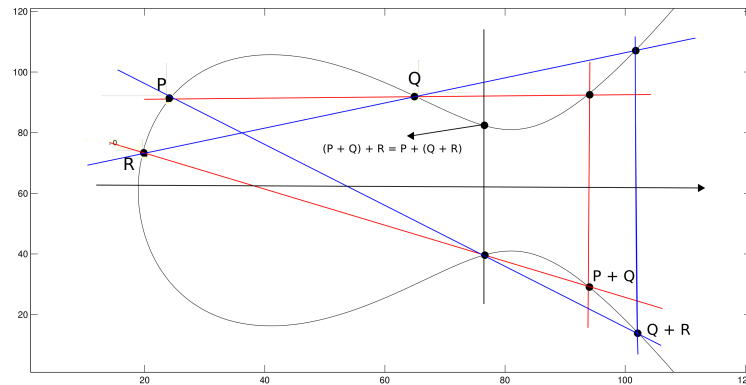
Logo,

$$P_1 + P_2 = -\{\{r_{P_1, P_2} \cap E\} \setminus \{P_1, P_2\}\} = -(x_3, y'_3) = (x_3, y_3).$$

□

**Teorema 3.3.** *Seja  $E$  uma curva elíptica sobre um corpo  $\mathbb{K}$ . Então a operação de adição sobre  $E$  tem as seguintes propriedades:*

**Figura 3.4** – Associatividade da Operação de Adição com Pontos de Curvas Elípticas



Fonte: O Autor (2020).

- (a)  $P + \mathcal{O} = \mathcal{O} + P = P, \forall P \in E$ ; [Identidade]
- (b)  $P + (-P) = \mathcal{O}, \forall P \in E$ ; [Inverso]
- (c)  $(P + Q) + R = P + (Q + R), \forall P, Q, R \in E$ ; [Associatividade]
- (d)  $P + Q = Q + P, Q \in E$  [Comutatividade]

*Demonstração.* (a), (b) e (d) são consequências imediatas da definição. A Figura 3.4 apresenta uma prova geométrica de (c). □

**Corolário 3.1.** A curva elíptica  $E(\mathbb{Z}_p)$  munida com a operação "+" forma um grupo abeliano finito. □

**Teorema 3.4.** O grupo  $E(\mathbb{Z}_p)$  possui subgrupos cíclicos. Se  $\#E(\mathbb{Z}_p) = q$ , com  $q$  primo, então  $E(\mathbb{Z}_p)$  é cíclico.

*Demonstração.* Seja  $P \in E(\mathbb{Z}_p)$ . Da Definição 2.8,  $H = \langle P \rangle$  é um subgrupo de  $E(\mathbb{Z}_p)$  denominado grupo cíclico gerado por  $P$ . Daí, se  $\#E(\mathbb{Z}_p) = q$ , com  $q$  primo segue, do Corolário 2.1 que  $E(\mathbb{Z}_p)$  é cíclico, em particular, pela Proposição 2.7, é abeliano. □

**Exemplo 3.8.** Considere a Curva Elíptica  $E : y^2 = x^3 + x + 1$  sobre o corpo  $\mathbb{Z}_7$ . Do Exemplo 3.7 têm-se que  $\#(E) = 5$  e, pelo Teorema 3.4,  $E$  é um grupo cíclico.

Ainda do Exemplo 3.7 têm-se  $E(\mathbb{Z}_7) = \{\mathcal{O}, (0, 1), (0, 6), (2, 2), (2, 5)\}$ . A Tabela 3.1 mostra a adição de pontos em  $E(\mathbb{Z}_7)$  dada pelo Exemplo 3.7.

**Teorema 3.5** (Teorema de Hasse). *Seja  $E$  uma curva elíptica sobre  $\mathbb{Z}_p$ . Então,  $\#(E) = p + 1 - t_p$ , com  $t_p$  satisfazendo  $|t_p| \leq 2\sqrt{p}$ .*

*Demonstração.* Ver (Silverman, 1992, p.110). □

**Tabela 3.1** – Adição para  $E : y^2 = x^3 + x + 1$  sobre  $\mathbb{Z}_7$ .

+	$\mathcal{O}$	(0,1)	(0,6)	(2,2)	(2,5)
$\mathcal{O}$	$\mathcal{O}$	(0,1)	(0,6)	(2,2)	(2,5)
(0,1)	(0,1)	(2,5)	$\mathcal{O}$	(0,6)	(2,2)
(0,6)	(0,6)	$\mathcal{O}$	(2,2)	(2,5)	(0,1)
(2,2)	(2,2)	(0,6)	(2,5)	(0,1)	$\mathcal{O}$
(2,5)	(2,5)	(2,2)	(0,1)	$\mathcal{O}$	(0,6)

Fonte: O Autor (2020).

**Exemplo 3.9.** Seja  $p = 7$  e  $E$  uma curva elíptica em  $\mathbb{Z}_7$ . Pelo Teorema de Hasse, têm-se:

$$7 + 1 - 2\sqrt{7} \leq \#(E) \leq 7 + 1 + 2\sqrt{7} \Rightarrow 3 \leq \#(E) \leq 13.$$

A Tabela 3.2 mostra curvas elípticas para cada valor de  $\#E$ .

*Observação 3.10.* O Teorema de Hasse afirma que o número de pontos de uma curva elíptica é aproximadamente da ordem do primo  $p$ .

*Observação 3.11.* As curvas elípticas de cardinalidade prima são consideradas boas curvas para fins criptográficos, pois, as mesmas formam grupos cíclicos finitos e, portanto, todo ponto da curva é um ponto gerador da mesma. Daí, pelo Exemplo 3.9, as possíveis curvas elípticas sobre  $\mathbb{Z}_7$  consideradas boas para criptografar são as de cardinalidades iguais à 3, 5, 7, 11 e 13.

**Tabela 3.2** – Possibilidades de Curvas Elípticas em  $\mathbb{Z}_7$  pelo Teorema de Hasse.

#E	(a,b)	#E	(a,b)	#E	(a,b)
3	(0,4)	7	(0,5)	11	(1,6)
4	(0,6)	8	(1,0)	12	(5,1)
5	(1,1)	9	(0,2)	13	(0,3)
6	(1,3)	10	(1,4)		

Fonte: O Autor (2020).

## 4 SISTEMA CRIPTOGRÁFICO UTILIZANDO CURVAS ELÍPTICAS

Neste capítulo são apresentados, de forma sucinta, alguns fundamentos básicos da criptografia e a aplicação das curvas elípticas em sistemas criptográficos de chave pública Stallings (2015) e Paar (1998), em particular, será apresentado o protocolo Diffie-Hellman (ECDH).

### 4.1 Fundamentos Básicos da Criptografia

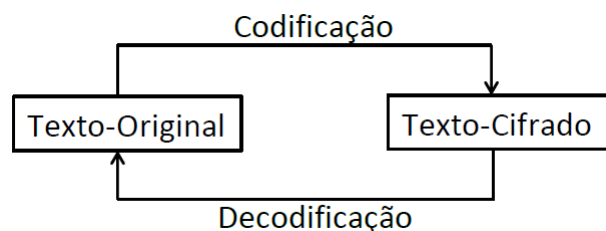
Para compreender o esquema de encriptação, deve-se atentar à cinco itens:

- **Texto claro:** diz respeito à mensagem ou dados originais que servem como entrada do algoritmo de encriptação;
- **Algoritmo de encriptação:** responsável por substituições e transformações no texto claro;
- **Chave secreta:** um outro tipo de entrada para o algoritmo de encriptação, sendo independente do texto claro e do algoritmo. A saída produzida pelo algoritmo, as substituições e transformações realizadas pelo mesmo dependem da chave que está sendo utilizada;
- **Texto cifrado** um conjunto de dados ininteligíveis, embaralhados, resultado da saída do algoritmo de encriptação, cuja decifração da mensagem depende do texto claro e da chave secreta;
- **Algoritmo de decifração:** algoritmo capaz de produzir o texto claro original, com base no texto cifrado e na chave secreta.

A Figura 4.1 mostra, de forma geral, como se processa um sistema criptográfico.

Existem três dimensões independentes que servem para caracterizar os sistemas criptográficos. São eles:

**Figura 4.1** – *Sistema Criptográfico*



Fonte: O Autor (2020).

- **O tipo das operações usadas para transformar texto claro em texto cifrado.** Existem dois princípios gerais que baseiam os algoritmos de encriptação: substituição (onde os elementos do texto claro, sejam eles quais forem, são mapeados em outros elementos) e a transposição (o rearranjo dos elementos no texto claro), além de ser fundamentalmente necessário que as operações sejam reversíveis, afim de que todas as informações possam ser extraídas. As várias sequências de substituições e transposições realizadas neste âmbito são chamadas de sistemas de produto;
- **O número de chaves usadas.** Quando um emissor e um receptor utilizam a mesma chave, chamamos o sistema de encriptação simétrica, sendo de chave única, chave secreta ou convencional. Para o caso de serem utilizadas chaves diferentes, o sistema é dito de encriptação assimétrica, com duas chaves ou de chave pública;
- **O modo em que o texto claro é processado.** Em uma cifra de bloco, há a entrada de um bloco de elementos por vez, criando uma saída para cada entrada. No caso de uma cifra de fluxo, todos os blocos de elementos são processados continuamente, permitindo a saída dos elementos por vez.

## 4.2 Tipos de Sistemas Criptográficos

Os sistemas criptográficos se dividem em dois tipos:

- **Chave Simétrica:** A Segurança depende do remetente e do destinatário possuírem algum segredo comum que é desconhecido do criptoanalista inimigo. A Figura 4.2 mostra a forma mais simples do sistema criptográfico de chave simétrica.
- **Chave Pública:** A Segurança depende do remetente e do destinatário que possuam alguma informação confiável comum, o que assume-se o criptoanalista inimigo também conhecer. A Figura 4.3 mostra o esquema geral de um sistema de chave pública.

**Figura 4.2** – Sistema de chave simétrica reduzido

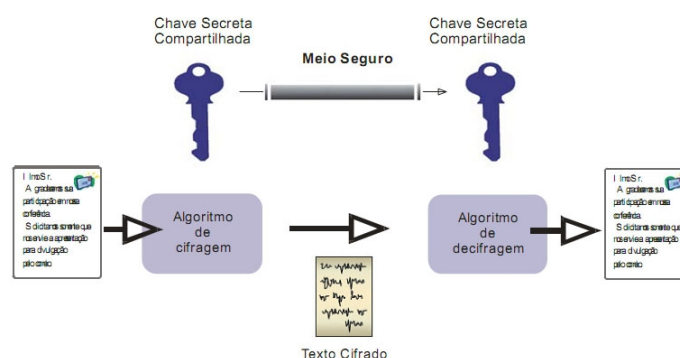
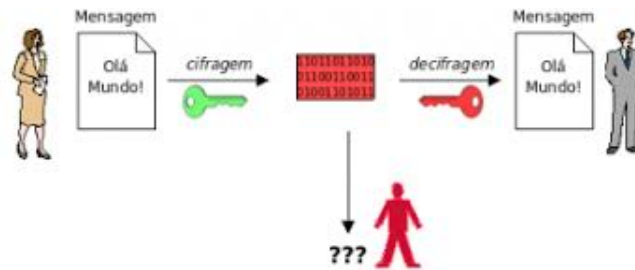


Figura 4.3 – Sistema de chave pública



Fonte: [http://www.cristiantm.com.br/\\_/rsrc/1472781891962/artigos/criptografia/criptografia-para-leigos/parte-ii-criptografia-assimtrica/cifragem-ass.png](http://www.cristiantm.com.br/_/rsrc/1472781891962/artigos/criptografia/criptografia-para-leigos/parte-ii-criptografia-assimtrica/cifragem-ass.png).

#### 4.2.1 Desvantagem do Uso da Criptografia por Chave Simétrica

A Encriptação por Chave Simétrica, também chamada de Encriptação Convencional ou Encriptação de Chave Única, possui uma limitação que é a utilização de uma única chave de encriptação e descriptação que é compartilhada pelo emissor e pelo receptor da mensagem codificada. Nesse caso, o uso da encriptação por chave simétrica limita o compartilhamento de informação, diminuindo o fluxo de mensagens e, conseqüentemente, reduz o alcance da informação pelos usuários.

#### 4.2.2 Vantagem do Uso da Criptografia por Chave Pública

A criptografia de chave pública oferece uma mudança radical de tudo o que foi feito antes. Por um lado, os algoritmos de chave pública são baseados em funções matemáticas, em vez de substituição e permutação. Mais importante, a criptografia de chave pública é assimétrica, envolvendo o uso de duas chaves separadas, ao contrário da criptografia simétrica, que utiliza apenas uma chave. O uso de duas chaves tem profundas conseqüências nas áreas de confidencialidade, distribuição de chave e autenticação.

### 4.3 Aplicações de Curvas Elípticas à Criptografia

Nesta seção, será estudado o sistema criptográfico utilizando curvas elípticas. Tal sistema é de chave pública e se baseia no problema do logaritmo discreto, apresentado à seguir.

#### 4.3.1 Curva Elíptica e o Problema do Logaritmo Discreto

**Definição 4.1.** Sejam  $E(\mathbb{Z}_p)$  uma curva elíptica e  $P, Q \in (\mathbb{Z}_p)$ . O Problema do Logaritmo Discreto utilizando Curva Elíptica (ECDLP) é o problema de encontrar um inteiro  $n$  tal que  $Q = nP$ . Por analogia com o Problema do Logaritmo Discreto para  $\mathbb{Z}_p^*$ , denotar-se-á este inteiro por  $n = \log_P(Q)$  e  $n$  será chamado o logaritmo discreto elíptico de  $Q$  com respeito a  $P$ .

*Observação 4.1.* Nem sempre o Logaritmo Discreto Elíptico existe, ou seja, podem existir  $P, Q \in E(\mathbb{Z}_p)$  tal que não exista um inteiro  $n$  tal que  $Q = nP$ .

*Observação 4.2.* Se existe um valor de  $n$  satisfazendo  $Q = nP$ , então existem vários. Daí, se  $s$  é a ordem de  $P$  e se  $n_0$  é algum inteiro tal que  $Q = n_0P$ , então as soluções para  $Q = nP$  são os inteiros  $n = n_0 + is$  com  $i \in \mathbb{Z}$ ; ou seja,  $\log_p(Q) \in \mathbb{Z}_s$ .

**Proposição 4.1.** *Seja  $P \in E(\mathbb{Z}_p)$  e  $s = O(P)$ . Então, a aplicação*

$$\begin{aligned} \log_P : E(\mathbb{Z}_p) &\longrightarrow \mathbb{Z}_s \\ Q &\longmapsto n = \log_P(Q) \end{aligned}$$

*está bem definida e é um homomorfismo de grupos.*

*Demonstração.* Para mostrar que  $\log_P$  está bem definida, sejam  $Q, R \in E(\mathbb{Z}_p)$  tais que  $\log_P(Q) \neq \log_P(R)$ . Deve-se mostrar que  $Q \neq R$ . Suponha que não, ou seja,  $Q = R$  e sejam  $m, n$  inteiros tais que

$$\bar{m} = \log_P(Q) \quad \text{e} \quad \bar{n} = \log_P(R). \quad (4.1)$$

Das igualdades em (4.1) segue que  $Q = \bar{m}P$  e  $R = \bar{n}P$ . Como  $Q = R$  têm-se:

$$\bar{m}P = \bar{n}P \Rightarrow (m - n)P = \mathcal{O}. \quad (4.2)$$

Como  $s = O(P)$ , segue que  $s \mid (m - n)$ , ou seja,

$$\bar{m} = \bar{n} \Rightarrow \log_P(Q) = \log_P(R) \text{ (contradição!)}$$

Portanto,  $Q \neq R$  e  $\log_P$  está bem definida.

Seja  $t \in \mathbb{Z}$  tal que  $\log_P(Q + R) = \bar{t}$ . Daí, segue que

$$tP = Q + R = mP + nP = (m + n)P \Rightarrow \bar{t} = \overline{m + n} = \bar{m} + \bar{n}. \quad (4.3)$$

Finalmente, de (4.3) têm-se:

$$\log_P(Q + R) = \bar{t} = \bar{m} + \bar{n} = \log_P(Q) + \log_P(R).$$

Logo,  $\log_P$  é um homomorfismo de grupos. □

**Exemplo 4.1.** Considere a curva elíptica

$$E : y^2 = x^3 + x + 3 \text{ sobre } \mathbb{Z}_7.$$

**Tabela 4.1** – Algoritmo Dobra - Adiciona

	<b>Entrada.</b> Ponto $P \in E(\mathbb{Z}_p)$ e inteiro $n \geq 1$ .
<b>1.</b>	Defina $Q = P$ e $R = \mathcal{O}$ .
<b>2.</b>	Loop enquanto $n > 0$ .
<b>3.</b>	Se $n \equiv 1 \pmod{2}$ , defina $R = R + Q$ .
<b>4.</b>	Defina $Q = 2Q$ e $n = \lfloor n/2 \rfloor$ .
<b>5.</b>	Se $n > 0$ , continue com o loop na Etapa <b>2</b> .
<b>6.</b>	Retorne o ponto $R$ , que é igual a $nP$ .

Fonte: (Hoffstein, 2008, p.293).

De acordo com a Tabela 3.2 têm-se  $\#E = 6$  e, é fácil concluir que

$$E(\mathbb{Z}_7) = \{\mathcal{O}, (4, 1), (4, 6), (5, 0), (6, 1), (6, 6)\}.$$

Agora, para os pontos  $P = (4, 1)$  e  $Q = (5, 0)$ , têm-se:

$$3P = Q.$$

Porém, não existe  $n \in \mathbb{Z}$  tal que  $nQ = P$ , pois,  $O(Q) = 2$ .

A seguir será visto o Algoritmo Dobra-Adiciona que otimiza a operação entre pontos de uma Curva Elíptica.

#### Algoritmo Dobra - Adiciona

Etapas do algoritmo:

- Inicialmente escreve-se  $n$  na forma binária como:

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \dots + n_r \cdot 2^r, \text{ com } n_0, n_1, \dots, n_r \in \{0, 1\}.$$

Nessa etapa, assumir-se-á  $n_r = 1$ .

- Calcula-se as seguintes quantidades:

$$Q_0 = P, Q_1 = 2Q_0, Q_2 = 2Q_1, \dots, Q_r = 2Q_{r-1}.$$

Note que  $Q_i = 2^i P$ .

- Calcula-se  $nP$  da seguinte forma:

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + \dots + n_r Q_r.$$

A implementação do Algoritmo é apresentado na Tabela 4.1.



*Observação 4.3.* O número total de operações realizadas no algoritmo é dado por  $r$  duplicidades de pontos na segunda etapa com mais  $r$  adições de pontos na terceira etapa, ou seja,  $2r$  operações no total. Agora, observe que  $n \geq 2^r \Rightarrow r \leq \log_2 n \Rightarrow 2r \leq 2 \log_2 n$ .

O resultado seguinte mostra que é possível reduzir ainda mais o número de operações entre pontos de uma curva elíptica, dando uma estimativa de  $\frac{3}{2}k$  operações, em que  $k = \lfloor \log n \rfloor + 1$ .

**Proposição 4.2.** *Sejam  $n$  um inteiro positivo e  $k = \lfloor \log n \rfloor + 1$ , o qual significa que  $2^k > n$ . Então nós podemos sempre escrever*

$$n = u_0 + u_1 \cdot 2 + u_2 \cdot 2^2 + u_3 \cdot 2^3 + \dots + u_k \cdot 2^k \quad (4.4)$$

com  $u_0, u_1, \dots, u_k \in \{-1, 0, 1\}$  e, no máximo,  $\frac{1}{2}k$  dos  $u_i$  não nulos.

*Demonstração.* Escreve-se inicialmente  $n$  na forma binária como:

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \dots + n_{k-1} \cdot 2^{k-1}, \quad \text{com } n_0, n_1, \dots, n_{k-1} \in \{0, 1\}.$$

Trabalhando da esquerda para a direita, observa-se a primeira ocorrência de dois ou mais coeficientes não-nulos  $n_i$ . Por exemplo, suponha que:

$$n_s = n_{s+1} = \dots = n_{s+t-1} = 1 \quad \text{e} \quad n_{s+t} = 0,$$

para algum  $t \geq 1$ . Em outras palavras, a quantidade

$$2^s + 2^{s+1} + \dots + 2^{s+t-1} + 0 \cdot 2^{s+t} \quad (4.5)$$

aparece na expansão binária de  $n$ . Observa-se que:

$$2^s + 2^{s+1} + \dots + 2^{s+t-1} + 0 \cdot 2^{s+t} = 2^s \cdot (1 + 2 + 2^2 + \dots + 2^{t-1}) = 2^s \cdot (2^t - 1).$$

Daí, é possível representar (4.5) como

$$-2^s + 2^{s+t}.$$

Repetindo este processo, encontrar-se-á uma expansão de  $n$  da forma (4.4) em que não existem dois  $u_i$  consecutivos não-nulos.  $\square$

**Exemplo 4.2.** Decomponha 39 e escreva-o na base 2, e utilizando a Proposição 4.2, rescreva a decomposição do Algoritmo de Euclides para que

$$u_0, u_1, \dots, u_k \in \{-1, 0, 1\},$$

em que  $k = \lfloor \log n \rfloor + 1$  e que no máximo  $\frac{1}{2}k$  de  $u_i$  são não nulos. Seguir-se-á o seguinte roteiro:

(i) Escrever 39 na base 2.

$$39 = 100111, \text{ logo } 39 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 \cdot 2^0.$$

(ii) Separar as parcelas não nulas de potências de 2 consecutivas.

$$(1 \cdot 2^2 + 1 \cdot 2^1) + 1 = 2 \cdot (2 + 1) + 1 = 2 \cdot (4 - 1) + 1 = 2^3 - 2 + 1 = 2^3 - 1.$$

(iii) Substituir (ii) em (i). Logo,

$$39 = 1 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 2^3 - 1,$$

ou seja,

$$39 = 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 - 1.$$

(iv) Verificar o chão de  $\log_2 39$ . Têm-se que  $\log_2 39 \approx 5,2854$ , logo  $\lfloor 5,2854 \rfloor = 5$ . Daí

$$k = \lfloor \log_2 39 \rfloor + 1 = 5 + 1 = 6 \Rightarrow k = 6.$$

Assim,  $\frac{1}{2}k = \frac{1}{2} \cdot 6 = 3$ . Logo 3 dos  $u_i$  são não nulos.

#### 4.4 Protocolo Diffie-Hellman (ECDH)

O primeiro algoritmo de chave pública que apareceu no artigo inicial de Diffie e Hellman que definia a criptografia de chave pública [DIFF76b], é geralmente chamado de troca de chaves Diffie-Hellman. Diversos produtos comerciais empregam essa técnica de troca de chaves. A finalidade do algoritmo é permitir que dois usuários troquem uma chave com segurança, que pode, então, ser usada para a criptografia subsequente das mensagens. O próprio algoritmo é limitado à troca de valores secretos. O algoritmo Diffie-Hellman depende, para a sua eficácia, da dificuldade de se calcular logaritmos discretos.

##### 4.4.1 Descrição do Protocolo (ECDH)

Esta subseção apresenta a descrição do Protocolo Diffie-Hellman (ECDH); este protocolo é uma aplicação das curvas elípticas à criptografia e o mesmo se resume a uma troca de chaves.

Os parâmetros do protocolo e a descrição do mesmo são dados, respectivamente, nas Tabelas 4.2 e 4.3.

*Observação 4.4.* Têm-se de fato que  $aB = a(bP) = b(aP) = bA$ .

**Exemplo 4.3.** Considere ECDH com os seguintes parâmetros:

**Tabela 4.2** – Parâmetros em ECDH.

<p><b>Parâmetros conhecidos em ECDH</b></p> <p>1. Escolha um primo <math>p</math> e a curva elíptica</p> $E : y^2 \equiv x^3 + a \cdot x + b \pmod{p}$ <p>2. Escolha um elemento primitivo <math>P = (x_P, y_P)</math></p>
--

Fonte: (Paar, 1998, p.250).

**Tabela 4.3** – Descrição do Protocolo ECDH.

<b>Protocolo Diffie-Hellman (ECDH)</b>	
<p><b>Livia</b></p> <p>Escolhe <math>K_{prA} = a \in \{2, 3, \dots, \#E - 1\}</math>          Calcula <math>K_{pubA} = aP = A = (x_A, y_A)</math></p>	<p><b>Larissa</b></p> <p>Escolhe <math>K_{prB} = b \in \{2, 3, \dots, \#E - 1\}</math>          Calcula <math>K_{pubB} = bP = B = (x_B, y_B)</math></p>
	$\xrightarrow{A}$ $\xleftarrow{B}$
<p>Calcula <math>aB = T_{AB}</math>          Segredo conjunto entre Livia e Larissa: <math>T_{AB} = (x_{AB}, y_{AB})</math>.</p>	<p>Calcula <math>bA = T_{AB}</math></p>

Fonte: (Paar, 1998, p.250).

$$E : y^2 \equiv x^3 + x + 1 \pmod{7} \text{ e } P = (0, 6).$$

O protocolo se processa como segue:

<p><b>Livia</b></p> <p>Escolhe <math>K_{prA} = a = 3</math>          Calcula <math>A = K_{pubA} = 3P</math></p>	<p><b>Larissa</b></p> <p>Escolhe <math>K_{prB} = b = 4</math>          Calcula <math>B = K_{pubB} = 4P</math></p>
	$\xrightarrow{A}$ $\xleftarrow{B}$
<p>Calcula <math>T_{AB} = aB = 3B</math>.</p>	<p>Calcula <math>T_{AB} = bA = 4A</math>.</p>

Mas, da Tabela 3.1, têm-se que:

$$\left\{ \begin{array}{l} A = 3P = (0, 6) + (0, 6) + (0, 6) = (2, 2) + (0, 6) = (2, 5) \\ \text{e} \\ B = 4P = (0, 6) + (0, 6) + (0, 6) + (0, 6) = (2, 2) + (2, 2) = (0, 1) \end{array} \right.$$

Portanto, ainda pela Tabela 3.1, têm-se:

$$\left\{ \begin{array}{l} T_{AB} = 3B = (0, 1) + (0, 1) + (0, 1) = (2, 5) + (0, 1) = (2, 2) \\ T_{AB} = 4A = (2, 5) + (2, 5) + (2, 5) + (2, 5) = (0, 6) + (0, 6) = (2, 2) \end{array} \right. .$$

## 5 CONSIDERAÇÕES FINAIS

A segurança de qualquer sistema criptográfico, seja ele de chave simétrica ou de chave pública, está diretamente ligada ao grau de dificuldade da descoberta da chave secreta (quebra do sistema). Neste sentido, concluímos neste trabalho que a aplicação das curvas elípticas à criptografia através do Protocolo Diffie-Hellman (ECDH), que tem a finalidade de permitir que dois usuários troquem uma chave secreta que pode ser usada na criptografia subsequente, aumenta a segurança dos sistemas criptográficos, trazendo um elemento a mais de dificuldade para os criptoanalistas inimigos que desejam quebrar o sistema; esta dificuldade está vinculada à solução do problema do logaritmo discreto para pontos de curvas elípticas definidas sobre corpos finitos e esta solução é tão mais difícil quanto maior for o número primo considerado.

## REFERÊNCIAS

- ENDLER, Otto. **Teoria dos números algébricos**. (Projeto Euclides) IMPA, 1986.
- HOFFSTEIN, J. et al. **An Introduction to Mathematical Cryptography**. Springer-Verlag, 2008.
- PAAR, C.; PELZL, J. **Understanding Cryptography: A Textbook for Students and Practitioners**. Springer-Verlag, 1998.
- SALEHYAN, Parham. **Curvas Elípticas e Aplicações Familiares: Fatoração em Primos**. III<sup>o</sup> Colóquio de Matemática da Região Sul, SC, 2014.
- SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3 ed. Rio de Janeiro: IMPA, 2009.
- SILVERMAN, J. H.; TATE, J. **Rational Points on Elliptic Curves**. Springer-Verlag, 1992.
- STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. 6<sup>a</sup> ed./SP: Pearson Education, 2015.
- VAINSENER, Israel. **Introdução às Curvas Algébricas Planas**. IMPA, 2005.
- VIEIRA, Vandenberg Lopes. **Um curso Básico em Teoria dos Números**. Campina Grande: EDUEPB, 2015.
- VIEIRA, Vandenberg Lopes. **Álgebra abstrata para licenciatura**. Campina Grande: EDUEPB, 2013.