Trabalho Prático: Repetido Quadrado em Curvas de Edwards

Data de Entrega: [30 de maio de 2025]

1 Introdução

Este trabalho prático tem como objetivo implementar o algoritmo de repetido quadrado para realizar multiplicações escalares eficientes em curvas de Edwards. As curvas de Edwards são uma forma de curva elíptica com propriedades aritméticas interessantes, particularmente no que diz respeito à completeza da lei de grupo.

2 Curvas de Edwards (página 619 do livro no SIGAA)

Uma curva de Edwards sobre um corpo $\mathbb{F}_p$ é definida pela equação:

$$ax^2 + by^2 = 1 + dx^2y^2$$

onde $a, b, d \in \mathbb{F}_p$ são constantes que satisfazem certas condições para garantir que a curva seja não-singular e completa.

3 Lei do Grupo

A lei de grupo para a adição de dois pontos $P_1 = (x_1, y_1)$ e $P_2 = (x_2, y_2)$ em uma curva de Edwards é dada por:

$$P_1 + P_2 = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right)$$

O ponto neutro da curva de Edwards é $\mathcal{O} = (0, 1)$.

4 Algoritmo de Repetido Quadrado

O algoritmo de repetido quadrado é um método eficiente para calcular o múltiplo escalar de um ponto em uma curva elíptica. Dado um ponto P e um inteiro n, o algoritmo calcula nP da seguinte forma:

1. Escreva n em sua representação binária: $n = (b_k b_{k-1} \dots b_1 b_0)_2$.
2. Inicialize $R = \mathcal{O}$.
3. Para i de k até 0:
   (a) $R = R + R$ (Duplicação).
   (b) Se $b_i = 1$, então $R = R + P$ (Adição).
4. Retorne R.

5 Tarefa

Implementar um programa que execute os seguintes passos:

1. Receber como entrada os parâmetros da curva de Edwards (a, b, d), um ponto $P = (x, y)$ na curva e um inteiro n.
2. Implementar a lei de grupo para a adição de pontos em curvas de Edwards, conforme definido na Seção 3.
3. Implementar o algoritmo de repetido quadrado, conforme descrito na Seção 4, para calcular nP.
4. Retornar as coordenadas do ponto nP.

6 Formato de Entrega

O trabalho deve ser entregue em formato de código fonte, e os resultados obtidos para alguns exemplos de entrada.

7 Critérios de Avaliação

O trabalho será avaliado com base nos seguintes critérios:

- Correção da implementação da lei de grupo.
- Correção da implementação do algoritmo de repetido quadrado.
- Eficiência do código.
- Clareza e organização do código.