Lista de exercícios: Curvas elípticas

1. Apresente as propriedades das operações que fazem de curvas elípticas constituir um grupo algébrico.

2. O que é o limiar de Hasse?

3. Porque o esquema de encriptação assimétrica com curvas elípticas é considerado seguro?

4. O que é o problema de logaritmo discreto em curva elípticas?

5. Em um grupo da curva elíptica $y^2 \equiv x^3 + 2x + 2 \mod 17$, faça as operações:

- $(2, 7) + (5, 2)$
- $(3, 6) + (3, 6)$
- $28 \times (3, 6)$

6. Seja $y^2 = x^3 + 3x + 2$ uma curva elíptica definida sobre $\mathbf{Z}_7$. Faça:

- Compute todos os pontos dessa curva.
- Obtenha a ordem do grupo.
- Qual é a ordem o elemento $(0, 3)$? Ele é primitivo?

7. O que é e para que serve o algoritmo de dobrar e somar em curvas elípticas? Escreva esse algoritmo. Usando esse algoritmo na curva $y^2 = x^3 + 4x + 20 \mod 29$, com ponto base $P = (8, 10)$ obtenha

- $9 \cdot P$
- $20 \cdot P$

8. Explique como funciona o protocolo de Diffie-Hellman com curvas elípticas.

9. Usando o protocolo de Diffie-Hellman com curvas elípticas, considere que sua chave privada é $a = 6$ e a chave pública de Bob é $B = (5, 9)$. Obtenha uma chave de sessão usando a curva elíptica $y^2 \equiv x^3 + x + 6 \mod 11$.

10. Explique como funciona o ECDSA.