Curvas Elípticas, Criptossistemas e o Teorema de Hasse

Jaime Edmundo Apaza Rodriguez **Divane Aparecida de Moraes Danta**
Douglas Silva Maiole

Departamento de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP
E-mail: jaime@mat.feis.unesp.br vanedantas@yahoo.com.br douglasmaioli@bol.com.br

RESUMO

Seja $\mathbb{K}$ um corpo arbitrário. Uma Curva Elíptica $\mathcal{E}$ sobre $\mathbb{K}$ é definida pela equação de Weierstrass da forma

$$\mathcal{E} : y^2 + a_1x^2y + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad \text{onde} \quad a_i \in \mathbb{K}.$$

Se a característica de $\mathbb{K}$ é diferente de 2 ou 3, por meio de uma mudança linear de variáveis, a curva $\mathcal{E}$ toma a forma

$$\mathcal{E} : y^2 = x^3 + ax + b,$$

com $a, b \in \mathbb{K}$, onde a cúbica da direita não possui raízes múltiplas e o discriminante $\triangle = -16(4a^3 + 27b^2) \neq 0$.

O conjunto de pontos de $\mathcal{E}$ consiste das soluções da equação $y^2 = x^3 + ax + b$, e o ponto no infinito $(0 : 1 : 0)$. Se $\mathbb{K} = \mathbb{R}$, este ponto corresponde à direção vertical à qual a reta tangente a $\mathcal{E}$ se aproxima quando $x \longrightarrow \infty$.

Os pontos da curva elíptica $\mathcal{E}$ formam um grupo cujo elemento identidade é o ponto no infinito. Se $\mathbb{K} = \mathbb{F}_q$, com $q = p^n$ e p primo, então os pontos de $\mathcal{E}$ formam um grupo abeliano finito, similar ao grupo multiplicativo $\mathbb{F}_q^*$ do corpo $\mathbb{K}$.

É possível implementar sistemas criptográficos de chave-pública (assimétricos) usando curvas elípticas sobre corpos finitos do tipo $\mathbb{F}_q$. Todos os sistemas criptográficos assimétricos são baseados em algum problema matemático de difícil solução. Por exemplo, o método RSA (1978) está baseado na fatoração de inteiros em seus fatores primos. O método de ElGamal (1985) está baseado no Problema do Logaritmo Discreto (PLD). Constantes buscas de algoritmos eficientes para resolver o PLD nos grupos multiplicativos $\mathbb{Z}_p^*$ e $\mathbb{F}_{2^m}^*$ foram feitas entre os anos 1978 e 1984, o que obrigou a aumentar o tamanho das chaves utilizadas no protocolo *Diffie-Hellman (1976)*. Isto levou à observar que os algoritmos de troca de chaves de Diffie-Hellman como do sistema ElGamal podem ser estendidos a grupos abelianos arbitrários (*Klobitz (1987)*. Assim, os esforços de pesquisa foram orientados à busca de grupos abelianos onde o PLD possa ser tratável e as operações no grupo possam ser implementadas eficientemente em software ou em hardware. De forma independente, *N. klobitz (1897)* e *V. Miller (1986)* propuseram utilizar o grupo de pontos de uma curva elíptica sobre um corpo finito para implementar criptossistemas de chave pública. Estes criptossistemas (CCE) têm sua segurança baseada na suposta intratabilidade do PLD no grupo de pontos de uma curva elíptica. Outro fator que recentemente trouxe muita atenção ao uso de curvas elípticas na criptografia é a chamada *criptografia baseada em identidaes*, proposta originalmente por *Shamir (1985)*.

A priori, uma curva elíptica definida sobre o corpo $\mathbb{F}_q$ possui, no máximo, $2q - 1$ pontos, ou seja, um ponto no infinito e, para cada x, temos duas possibilidades para y, pois $(x, y) \in \mathcal{E} \iff (x, -y) \in \mathcal{E}$. Neste sentido, um resultado interesante sobre a cardinalidade do conjunto

de pontos de uma curva elíptica $\mathcal{E}$ é o *Teorema de Hasse*, conjecturado inicialmente por *A. Weil* e demonstrado logo por *H. Hasse*. Este resultado garante que para primos muito grandes o grupo de pontos da curva também fica muito grande e este fato é fundamental para o estudo dos criptossistemas com curvas elípticas.

Teorema de Hasse: Seja $\mathcal{E}/\mathbb{F}_q$ uma Curva Elíptica definida sobre $\mathbb{F}_q$ e N o número de pontos de $\mathcal{E}$ ou ordem de $\mathcal{E}$ sobre $\mathbb{F}_q$. Então vale a desigualdade

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

O intervalo $(q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q})$é chamado de teorema de Hasse.

Assim, o número de pontos de uma curva elíptica é, aproximadamente, o tamanho do corpo.

Exemplo: (Curva Elíptica sobre o corpo primo $\mathbb{F}_{29}$) Sejam $q = 29, a = 4$ e $b = 20$, e considere a Curva Elíptica $\mathcal{E} : y^2 = x^3 + 4x + 20$, definida sobre $\mathbb{F}_{29}$. Observe que $\triangle = -16(4a^3 + 27b^2) = -176896 \neq 0 \ mod\ 29$. Assim $\mathcal{E}$ é de fato uma Curva Elíptica e tem 37 pontos, que são os seguintes:

$$\infty\ (2,6)\ (4,19)\ (8,10)\ (13,23)\ (16,2)\ (19,16)\ (27,2)(0,7)\ (2,23)$$

$$(5,7)\ (8,19)\ (14,6)\ (16,27)\ (20,3)\ (27,27)(0,22)\ (3,1)\ (5,22)\ (10,4)$$

$$(14,23)\ (17,10)\ (20,26)\ (1,5)\ (3,28)\ (6,12)\ (10,25)\ (15,2)\ (17,19)$$

$$(24,7)\ (1,24)\ (4,10)\ (6,17)\ (13,6)\ (15,27)\ (19,13)\ (24,22)$$

Um exemplo de adição de dois pontos da Curva Elíptica é:

$$(5,22) + (16,27) = (13,6) \quad e \quad 2(5,22) = (14,6).$$

Palavras-chave: *Corpos Finitos, Criptografia, Curvas Elipticas, Criptossistemas.*

Referências

[1] C. S. L. Pedro e B. O. Fábio, Criptografia com Curvas Elípticas sobre Corpos Finitos, *LNCC (Laboratório Nacional de Computação Científica).*

[2] N. Klobitz, A course in Number Theory and Cryptography, Springer-Verlag, New York, 1999.

[3] N. Klobitz, Elliptic Curve Cryptosystems, Mathematics of Computation, Vol. 48, Number 177, p. 203-209, 1987.

[4] I. N. Herstein, Topics in Algebra, Lexington, Mass. College Publishing, 1975.

[5] F. G. Lima, Introdução à Criptografia e ao Código RSA, PUC-Rio, 2004.

[6] A. V. Mendes, Estudo de Criptografia com Chave Pública baseada em Curvas Elípticas, Monografia Depto de Ciências, Montes Claros, 2007.

[7] A. C. de A. Neto, Um algoritmo de Criptografia de Chave Pública Semanticamente Seguro baseado em Curvas Elípticas, Dissertação de Mestrado, UFRS-Porto alegre, 2006.