Grupo de pontos sobre uma curva elíptica

Jaime Edmundo Apaza Rodriguez
Universidade Estadual Julio de Mesquita Filho, Depto de Matemática, FEIS, UNESP
15385-000, Ilha Solteira, SP, E-mail: jaime@mat.feis.unesp.br

Divane Aparecida de Moraes Dantas
UNESP, Campus Ilha Solteira, 15385-000, SP, E-mail: vanedantas@yahoo.com.br

RESUMO

As curvas elípticas são importantes tanto do ponto de vista teórico quanto prático. Por exemplo, são úteis para a implementação de certos algoritmos criptográficos.
Uma curva elíptica é uma curva cúbica da forma:

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$$

onde $a_1, a_2, a_4, a_5 \in K$, sendo K um corpo.

Vamos definir uma operação de adição (soma elítica) para quaisquer dois pontos da curva elítica.
Seja *s* a reta que passa pelos pontos *P* e *Q*. Como a equação de *E* possui grau 3, deve existir um terceiro ponto *T*, tal que $T \neq P$, $T \neq Q$ e $T \in (s \cap E)$. Assim definimos $P+Q=R$, onde *R* é obtido pela reflexão de *T* em relação ao eixo x.

Propriedades da soma elíptica:

1.Associativa: Para $P, Q, S \in E$, $(P+Q)+S=P+(Q+S)$.

2. Fechamento: Se $P, Q \in E$, então $(P+Q) \in E$.

3. Existência de inverso: Para todo $P \in E$, existe $Q \in E$ tal que $P+Q=\Theta$. O ponto *Q* pode ser simbolizado por $-P$.

4. Existência de elemento neutro: Para todo $P \in E$, existe Θ tal que $P+\Theta = P$.

5. Comutativa: Para $P, Q \in E$, $P+Q = Q+P$.

Assim, a curva elíptica *E*, com a operação de adição definida, é um grupo abeliano.

Casos especiais:

1)Se *s* é perpendicular ao eixo x. Neste caso, não existe uma terceira intersecção da reta *s* com a curva *E*. Convenciona-se então que $P+Q=\Theta$, onde Θ é chamado de ponto no infinito.

2) Se $P=Q$. Neste caso, *s* é a reta tangente a *E* no ponto *P* e o restante da definição segue como anteriormente.

As figuras 1 e 2 ilustram a definição dada e os casos mencionados.

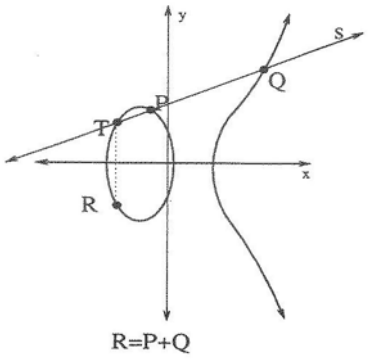

FIG 1: Soma elíptica de dois pontos distintos *P* e *Q*.

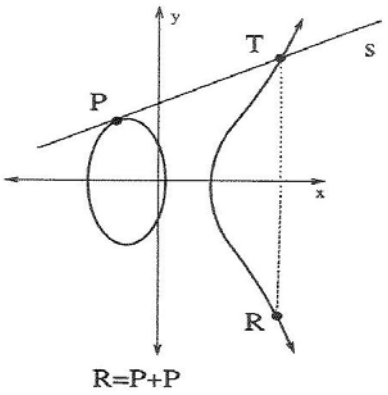

FIG 2: Soma elíptica de dois pontos iguais.

Esta estrutura de grupo abeliano de E é muito útil em Criptografia com Curvas Elípticas.

Bibliografia

[1] R. A. Miranda, Criptossistemas Baseados em Curvas Elípticas, Dissertação de Mestrado, IC, Unicamp, 2002.

[2] E. Oswald, Introduction to Elliptic Curve Cryptography, Institute for Applied Infortion Processing and Communication, Graz Austria, 2005.