Pontos racionais da Curva Hermitiana

Thalita Kelen Leal do Prado **Jaime Edmundo Apaza Rodriguez**

Depto de Matemática, FEIS- UNESP,
15385-000, Ilha Solteira, SP
E-mail: tkprado1@yahoo.com.br, jaime@mat.feis.unesp.br

Seja C uma curva algébrica projetiva não-singular definida sobre um corpo finito $\mathbf{F}_q$. Em 1940, *A. Weil* mostrou a desigualdade:

$$|C(\mathbf{F}_q)| \leq 1 + q + 2g\sqrt{q}, \qquad (1)$$

onde g é o gênero de C e $|C(\mathbf{F}_q)|$ o número de pontos racionais de C. Temos que $g \leq \frac{(d-1)(d-2)}{2}$, sendo d o grau do polinômio $f(x,y) \in \mathbf{F}_q[x,y]$ que define a curva.

A curva C é dita *maximal* sobre $\mathbf{F}_q$ se atinge a cota (1) (q deve ser um quadrado).

Em 1981, *Y. Ihara* mostrou que

$$g \leq \frac{\sqrt{q}(\sqrt{q}-1)}{2}. \qquad (2)$$

Assim, a desigualdade (2) garante que se $g > \frac{q - q^{1/2}}{2}$, então $|C(\mathbf{F}_q)| < 1 + q + 2g\sqrt{q}$.

Em $\mathbf{F}_q$, a cardinalidade q é potência de um primo p. O corpo $\mathbf{F}_q$ é o *corpo de raízes* (sobre $\mathbf{F}_p$) do polinômio $x^q - x$. Assim

$$x^{q-1} = 1, \quad \forall \in \mathbf{F}_q \backslash \{0\}.$$

$\mathbf{F}_q^* = \mathbf{F}_q \backslash \{0\}$ é o grupo multiplicativo de $\mathbf{F}_q$, é cíclico de ordem $q-1$ e possui um subgrupo de ordem m, para cada m divisor de $q-1$.

Dada a extensão $\mathbf{F}_{q^r}/\mathbf{F}_q$, seu *grupo de Galois* é cíclico de ordem r. Um gerador deste grupo é o *automorfismo σ de Frobenius*

$$\sigma : \mathbf{F}_{q^r} \longrightarrow \mathbf{F}_{q^r}, \quad \sigma(x) = x^q.$$

Em particular, para uma extensão quadrática $\mathbf{F}_{p^{2n}}/\mathbf{F}_{p^n}$ temos o *traço* ($\mathcal{T}$) e a *norma* ($\mathcal{N}$) dados por

$$\mathcal{T}(y) = y + y^{p^n}, \quad \forall y \in \mathbf{F}_{p^{2n}},$$

$$\mathcal{N}(x) = x^{1+p^n}, \quad \forall x \in \mathbf{F}_{p^{2n}}.$$

O exemplo a seguir mostra uma curva maximal, com o maior gênero possível (segundo (2)).

A Curva de Hermite: Considere a curva projetiva C associada ao polinômio

$$f(x,y) = y^{p^n} + y - x^{1+p^n} \in \mathbf{F}_q[x,y],$$

onde $q = p^{2n}$, com $n \in \mathbf{N}$. O polinômio homogêneo associado é

$$F(x,y,z) = zy^{p^n} + z^{p^n}y - x^{1+p^n}.$$

Temos que C é não-singular e $g = \frac{\sqrt{q}(\sqrt{q}-1)}{2}$.

Contagem dos pontos racionais de $C(\mathbf{F}_q)$. Na parte afim $C_a(\mathbf{F}_q)$:

$$\begin{aligned} C_a(\mathbf{F}_q) &= \{(x,y) \in \mathbf{F}_q \times \mathbf{F}_q : f(x,y) = 0\} \\ &= \{(x,y) \in \mathbf{F}_q \times \mathbf{F}_q : \mathcal{T}(y) = \mathcal{N}(x)\}. \end{aligned}$$

Assim obtemos

$$\begin{aligned} |C_a(\mathbf{F}_q)| &= \sum_{x \in \mathbf{F}_q} |\{y \in \mathbf{F}_q : \mathcal{T}(y) = x^{1+p^n}\}| \\ &= \sum_{x \in \mathbf{F}_q} |\mathcal{T}^{-1}(x^{1+p^n})\}| \\ &= \sum_{x \in \mathbf{F}_q} p^n = p^{2n} \cdot p^n = p^{3n}. \end{aligned}$$

O único ponto do infinito de C é $(0:1:0)$. Assim $|C(\mathbf{F}_q)| = 1 + p^{3n}$ é o número de pontos racionais da *curva hermitiana*.

Referências

[1] A. Garcia, *Pontos racionais em curvas sobre corpos finitos*, XX Colóquio Brasileiro de Matemática, IMPA, RJ, 1995.

[2] I. Vainsencher, *Introdução às Curvas Algébricas Planas*, Coleção Matemática Universitária, SBM, RJ, 2005.