IMBM istanbul matematiksel bilimler merkezi
istanbul center for mathematical sciences

Maximal curves over finite fields

Saeed Tafazolian

Unicamp/Brazil

Abstract

By a curve we mean a smooth geometrically irreducible projective curve. Explicit curves (i.e., curves given by explicit equations) over finite fields with many rational points with respect to their genera have attracted a lot of attention, after Goppa discovered that they can be used to construct good linear error-correcting codes. For the number of $\mathbb{F}_q$-rational points on the curve $\mathcal{C}$ of genus $g(\mathcal{C})$ over $\mathbb{F}_q$ we have the following bound

$$\#\mathcal{C}(\mathbb{F}_q) \leq 1 + q + 2\sqrt{q}g(\mathcal{C}),$$

which is well-known as the *Hasse-Weil bound*. This is a deep result due to Hasse for elliptic curves, and for general curves is due to A. Weil. When the cardinality of the finite field is square, a curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is called maximal if it attains the Hasse-Weil bound, i.e., if we have the equality

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = 1 + q^2 + 2qg(\mathcal{C}).$$

We introduce some geometric properties of curves with many rational points to classify certain maximal curves.

Date : Friday, June 28, 2019

Time: 15:30

Place: IMBM Seminar Room, Boğaziçi University South Campus