Permutations of the Form $x^k - \gamma \mathrm{Tr}(x)$ and Curves over Finite Fields

Nurdagül Anbar

Sabancı University

Let q be a power of a prime p, and let $\mathbb{F}_q$ be the finite field with q elements. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called a *permutation* of $\mathbb{F}_q$ if the associated map from $\mathbb{F}_q$ to $\mathbb{F}_q$ defined by $x \mapsto P(x)$ is a bijection, i.e., it permutes the elements of $\mathbb{F}_q$. In this talk, we consider the polynomials of the form $P(x) = x^k - \gamma \mathrm{Tr}(x)$ over $\mathbb{F}_{q^n}$ for $n \geq 2$, where $\mathbb{F}_{q^n}$ is the extension of $\mathbb{F}_q$ of degree n and Tr is the absolute trace from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$. We show that $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$ in the case $\gcd(k, q^n - 1) > 1$. Our proof uses an absolutely irreducible curve over $\mathbb{F}_{q^n}$ and the number of rational points on it.