Exposé court

30 *Existence of primitive pairs with two prescribed traces over finite fields*

Choudhary, Aakash (Department of Mathematics, IIT Delhi)

Let $\mathbb{F}_p$ represent a field of finite order p, where p is a prime power. The multiplicative group of $\mathbb{F}_p$ is cyclic, and its generator is referred to as a primitive element in $\mathbb{F}_p$. For any rational function $f(x) \in \mathbb{F}_p(x)$ and $\epsilon \in \mathbb{F}_p$, we call the pair $(\epsilon, f(\epsilon))$, a primitive pair if both ϵ and $f(\epsilon)$ are primitive elements in $\mathbb{F}_p$. Let $\mathbb{F}_{p^t}$ be an extension of $\mathbb{F}_p$ of degree t, for $\epsilon \in \mathbb{F}_{p^t}$, the trace of ϵ over $\mathbb{F}_p$ denoted by $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon)$, is defined as $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = \epsilon + \epsilon^p + \epsilon^{p^2} + \cdots + \epsilon^{p^{t-1}}$.

In this talk, for the extension $F = \mathbb{F}_{p^t}$ with $t \geq 7$, and for $f = f_1/f_2$, a rational function in F such that f_1, f_2 are distinct irreducible polynomials with $deg(f_1) + deg(f_2) = n$ in $F[x]$, we will present a sufficient condition on (p, t) which guarantees primitive pairing $(\epsilon, f(\epsilon))$ exists in F such that $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(\epsilon) = a$ and $Tr_{\mathbb{F}_{p^t}/\mathbb{F}_p}(f(\epsilon)) = b$ for any prescribed $a, b \in \mathbb{F}_p$. Further, we demonstrate for any positive integer n, such a pair definitely exists for large t. For $n = 2$, we verified that such a pair exists for all (p, t) except for finitely many values of p. This is a joint work with Prof. R.K. Sharma.