Number Theory Session

ON FUNCTIONAL GRAPHS OVER FINITE FIELDS.

Abílio Lemos*
(Universidade Federal de Viçosa, Minas Gerais, Brazil)

Thursday, February 08, 2024.
14h50 - 15h30

Online

Abstract.

The dynamic of iterations of polynomials over finite fields have attracted much attention in recent years in part due to their applications in cryptography and integer factorization methods like Pollard rho algorithm. We define the functional graph $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ as the directed graph $\mathcal{G}(f) = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V} = \mathbb{F}_{q^2}$ and $\mathcal{E} = \{\langle x, f(x)\rangle \,|\, x \in \mathbb{F}_{q^2}\}$. We define the iterations of f as $f^{(0)}(x) = x$ and $f^{(n+1)}(n+1)(x) = f(f^{(n)}(x))$. Since f is defined over finite field, fixing $\alpha \in \mathbb{F}_q$, there are integers $0 \le i < j$, minimal, such that $f^{(i)}(\alpha) = f^{(j)}(\alpha)$. In the case when $i > 0$, we call the list $\alpha, f(\alpha), f^{(2)}(\alpha), \cdots, f^{(i-1)}(\alpha)$ the pre-cycle and $f^{(i)}(\alpha), f^{(i+1)}(\alpha), \cdots, f^{(j-1)}(\alpha)$ the cycle of length $(j-i)$ or the $(j-i)$-cycle. If α is an element of a cycle, we call it a periodic element and, if $f(\alpha) = \alpha$ we say it is a fixed point. In this talk, we present some results in this topic and some results of the functional graph $\mathcal{G}(f)$ of the map $a \mapsto f(a)$, where $f(X) = X(X^{q-1} - c)^{q+1}$, for $c \in \mathbb{F}_q^*$.

JOINT WORK WITH JOSIMAR J.R. AGUIRRE AND VICTOR G.L. NEUMANN.

Keywords: Dynamics of polynomials, finite fields.

*Email: ABILIOLEMOS@UIFV.BR