# Fibonacci permutation polynomials

Neranga Fernando

Department of Mathematics
Northeastern University
Boston, MA 02115

*Fibonacci polynomials* were first studied in 1833 by Eugene Charles Catalan. Since then, Fibonacci polynomials have been extensively studied by many for their general and arithmetic properties.

Fibonacci polynomials are defined by the recurrence relation $f_0(x) = 0,\ f_1(x) = 1$, and

$$f_n(x) = xf_{n-1}(x) + f_{n-2}(x),\ \text{for } n \geq 2.$$

Let $p$ be a prime. Then the finite prime field with characteristic $p$ is $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. We denote $\mathbb{Z}_p$ by $\mathbb{F}_p$.

Let me first give you an example of a permutation polynomial of $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$. Consider the polynomial $g(x) = x^3 + 1$ and evaluate it at each element in $\mathbb{F}_5$. Then in characteristic 5 we have

$$g(0) = 1,\ g(1) = 2,\ g(2) = 4,\ g(3) = 3,\ g(4) = 0.$$

Note that the associated mapping $x \mapsto g(x)$ from $\mathbb{F}_5$ to $\mathbb{F}_5$ is a permutation of $\mathbb{F}_5$, i.e. $g(x)$ is a permutation polynomial of $\mathbb{F}_5$.

Now let $\mathbb{F}_{p^e}$ be the finite field with $p^e$ elements. I will explain how to construct $\mathbb{F}_{p^e}$ from the finite prime field $\mathbb{F}_p$ (I promise). A polynomial $f \in \mathbb{F}_{p^e}[\mathrm{x}]$ is called a *permutation polynomial* of $\mathbb{F}_{p^e}$ if the associated mapping $x \mapsto f(x)$ from $\mathbb{F}_{p^e}$ to $\mathbb{F}_{p^e}$ is a permutation of $\mathbb{F}_{p^e}$. Permutation polynomials over finite fields have important applications in coding theory, cryptography, finite geometry, combinatorics and computer science, among other fields.

In this talk, I will present the permutation polynomials over finite fields arising from Fibonacci polynomials.

This is a joint work with Mohammad H. Rashid.