A Study of Self-reciprocal Polynomials

Sean Baker and Neranga Fernando
Department of Mathematics and Computer Science, College of the Holy Cross

Introduction

Let p be a prime number. The finite prime field with characteristic p is given by

$$\mathbb{F}_p = \{0, 1, 2, \ldots, p-1\}.$$

We present self-reciprocal polynomials arising from Dickson polynomials over $\mathbb{F}_p$.

Dickson Polynomials of the First Kind

The nth Dickson polynomial of the first kind is given by the explicit expression

$$D_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i\, x^{n-2i},$$

where $a \in \mathbb{F}_p$ is a parameter. The recurrence relation of Dickson polynomials of the first kind $D_n(x,a)$ is given by

$$D_0(x,a) = 2,\ D_1(x,a) = x,$$

$$D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a) \ \text{ for } n \geq 2.$$

Dickson Polynomials of the Second Kind

The nth Dickson polynomial of the second kind is given by the explicit expression

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}(-a)^i\, x^{n-2i},$$

where $a \in \mathbb{F}_p$ is a parameter. The recurrence relation of Dickson polynomials of the second kind $E_n(x,a)$ is given by

$$E_0(x,a) = 1,\ E_1(x,a) = x,$$

$$E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a) \ \text{ for } n \geq 2.$$

Dickson Polynomials of the $(k+1)$th Kind

The nth Dickson polynomial of the $(k+1)$th kind is given by the explicit expression

$$D_{n,k}(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n-ki}{n-i}\binom{n-i}{i}(-a)^i\, x^{n-2i},$$

where $a \in \mathbb{F}_p$ is a parameter. The recurrence relation of Dickson polynomials of the $(k+1)$th kind $D_{n,k}(x,a)$ is given by

$$D_{0,k}(x,a) = 2-k,\ D_{1,k}(x,a) = x,$$

$$D_{n,k}(x,a) = x\, D_{n-1,k}(x,a) - a\, D_{n-2,k}(x,a) \ \text{ for } n \geq 2.$$

Self-reciprocal Polynomials

Self-reciprocal polynomials are polynomials whose coefficients form a **palindrome**.

Example $f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$

Definition The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f(\frac{1}{x})$, i.e. if

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n,$$

then

$$f^*(x) = a_n + a_{n-1}x + a_{n-2}x^2 + \ldots + a_0x^n.$$

A polynomial $f(x)$ is called self-reciprocal if $f^*(x) = f(x)$, i.e. if $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, a_n \neq 0$, is self-reciprocal, then $a_i = a_{n-i}$ for $0 \leq i \leq n$.

Conjectures

1. $D_n(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_3$ if and only if

$$n = 0 \cdot 3^0 + \ldots + 0 \cdot 3^{k-1} + 2 \cdot 3^k, \ \text{ or}$$

$$n = 0 \cdot 3^0 + \ldots + 0 \cdot 3^{l-1} + 2 \cdot 3^l + 1 \cdot 3^{l+1} + \ldots + 1 \cdot 3^e,$$

   where $k \geq 0$ and $0 \leq l < l+1 < e$.

2. Let $n > 4$. If $E_n(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_p$, then $p = 3$ or $p = 5$.

3. $E_n(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_3$ if and only if

$$n = 1 \cdot 3^0 + \ldots + 1 \cdot 3^w, \quad n = 2 \cdot 3^0 + \ldots + 2 \cdot 3^l, \ \text{ or}$$

$$n = 2 \cdot 3^0 + 2 \cdot 3^1 + \ldots + 2 \cdot 3^k + 1 \cdot 3^{k+1} + \ldots + 1 \cdot 3^e,$$

   where $e, k, l,$ and w are odd and $e > k \geq 1$.

4. $E_n(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_5$ if and only if

$$n = 4 \cdot 5^0 + \ldots + 4 \cdot 5^w, \quad n = 2 \cdot 5^0 + \ldots + 2 \cdot 5^l, \ \text{ or}$$

$$n = 2 \cdot 5^0 + \ldots + 2 \cdot 5^k + 4 \cdot 5^{k+1} + \ldots + 4 \cdot 5^e,$$

   where k and l are odd, $w \geq 0$, $l \geq 1$, and $1 \leq k < k+1 \leq e$.

A Note on Confirming the Conjectures: We apply Lucas' Theorem and Kummer's Theorem to show that

$$\underbrace{\frac{n-ki}{n-i}\binom{n-i}{i}(-1)^i}_{i\text{th term}} \equiv \underbrace{\frac{n-k(\frac{n}{2}-i)}{n-(\frac{n}{2}-i)}\binom{n-(\frac{n}{2}-i)}{\frac{n}{2}-i}(-1)^{\frac{n}{2}-i}}_{(\frac{n}{2}-i)\text{th term}} \pmod{p},$$

for $0 \leq i \leq \frac{n}{2}$.

Results

1. If $D_n(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_p$, then p = 3.
2. Let $p > 5$. $E_n(x,1)$ is a self-reciprocal polynomial if and only if n = 4.
3. There exist no self-reciprocal polynomials resulting from Dickson polynomials of the third kind $D_{n,2}(x,1)$.
4. $D_{n,3}(x,1)$ is a self-reciprocal polynomial over $\mathbb{F}_p$ if and only if $n = 2$.
5. Let $k > 3$. There exist no self-reciprocal polynomials resulting from $D_{n,k}(x,1)$.

Future Plans

1. Let $f \in \mathbb{F}_q[x]$ be a nonzero polynomial. If $f(0) \neq 0$, the **order** of f is the least positive integer e such that $f | x^e - 1$. If $f(0) = 0$, let $f(x) = x^r \cdot g(x)$ for some integer $r \geq 1$ and $g \in \mathbb{F}_q[x]$ with $g(0) \neq 0$. In this case, the order of f is the order of g. We plan on studying any patterns in the order of self-reciprocal polynomials that arise from Dickson polynomials.
2. **Cullen numbers** are defined by $C_n = n \cdot 2^n + 1$, where n is a natural number. They were first studied by Rev. Father James Cullen who was a Jesuit. He studied pure and applied mathematics at Trinity College Dublin. We seek to determine whether there exist any Dickson polynomials that generate Cullen numbers. We also plan to study the patterns in the kind of polynomials generated when the index of a Dickson polynomial is a Cullen number.
3. **Polynomial** g_n The nth polynomial g_n is given by the explicit expression

$$g_n(x) = \sum_{\frac{n}{p} \leq l \leq \frac{n}{p-1}} \frac{n}{l}\binom{l}{n-l(p-1)} x^{n-l(p-1)} \quad \in \mathbb{Z}[x],$$

   where n is the index of the polynomial. The recurrence relation of polynomial g_n is given by

$$g_n = 0, \ \text{ for } 0 \leq n \leq p-1, \ \ g_{p-1} = -1,$$

$$g_n = xg_{n-p} + g_{n-p+1}, \ \text{ for } n \geq p.$$

   We plan on studying the self-reciprocal behaviour of polynomial g_n.

Acknowledgements

We would like to thank the Weiss Summer Research Program at the College of the Holy Cross as well as Dr. Dan Kennedy '68 for financial support.