A class of Permutation Polynomials

Christian Rodriguez
Alex D. Santos

Department of Computer Science
University of Puerto Rico, Rio Piedras

May 19, 2013

The polynomial

$$F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$$

Our Problem

Let $p \equiv 1 \bmod 3$. *Find* a *and* b *such that* $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ *is a permutation polynomial over* $\mathbb{F}_p$.

The polynomial

Let N_p be the number of permutation polynomials of the type $F_{a,b}(x) = x^{\frac{p-1}{2}+1} + ax^{\frac{p-1}{6}+1} + bx$ of $\mathbb{F}_p$.

p	N_p	p	N_p
13	18	127	234
19	0	139	270
31	18	151	276
37	12	157	438
43	36	163	378
61	30	181	552
67	108	193	612
73	54	199	624
79	48	211	756
97	102	223	540
103	72	229	858
109	120	241	828

The polynomial

Conjecture

Let $p \equiv 1 \bmod 3$. The number of Permutation Polynomials over $\mathbb{F}_p$ of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ is divisible by 6.

Results

In the case $p = 31$ we have: $F_{a,b}(x) = x^{16} + ax^6 + bx$. For the following $[a, b]$ $F(x)$ is a permutation polynomial:

$$[2, 7], [2, 24], [10, 7][10, 24], [16, 13], [16, 18],$$

$$[17, 5], [17, 26], [18, 13], [18, 18], [19, 7], [19, 24],$$

$$[22, 5], [22, 26], [23, 5], [23, 26], [28, 13], [28, 18]$$

In the case $p = 37$ we have: $F_{a,b}(x) = x^{16} + ax^6 + bx$. For the following $[a, b]$ $F(x)$ is a permutation polynomial:

$$[11, 5], [11, 32], [18, 17][18, 20], [24, 17], [24, 20],$$

$$[27, 5], [27, 32], [32, 17], [32, 20], [36, 5], [36, 32],$$

Conjectures

Conjecture

Consider the polynomial $F(x)$. If (a, b) produces a permutation, then $(a, -b)$ also produces a permutation.

Conjecture

The number of Permutation Polynomials over $\mathbb{F}_p$ of the form $F_{a,b}(x) = x^{\frac{p+1}{2}} + ax^{\frac{p+5}{6}} + bx$ is divisible by 3.

Approach

Our approach in studying $F(x)$ is to use the division algorithm to consider $x = \alpha^n$ where $n = 6k + r, r = 0, ..., 5$.

We expect that if $F_{a,b}(x)$ is a permutation, this partitions $\mathbb{F}_q^\times$ into 6 classes: $F_{a,b}(\alpha^{6k+r})$ for $r = 0, ..., 5$

Results

Definition

$A_i = \{F_{a,b}(\alpha^{6k+i}) \mid k = 0, ..., \frac{p-1}{6}\}$

Lemma

For $i = 1, ..., 5$ $|A_i| = \frac{p-1}{6}$