LOCAL PERMUTATION POLYNOMIALS OVER $\mathbb{Z}_p$

GARY L. MULLEN
The Pennsylvania State University, Sharon, PA 16146

1. INTRODUCTION

If $p$ is a prime, let $\mathbb{Z}_p$ denote the integers modulo $p$ and $\mathbb{Z}_p^*$ the set of nonzero elements of $\mathbb{Z}_p$. It is well known that every function from $\mathbb{Z}_p \times \mathbb{Z}_p$ into $\mathbb{Z}_p$ can be represented as a polynomial of degree $< p$ in each variable. We say that a polynomial $f(x_1, x_2)$ with coefficients in $\mathbb{Z}_p$ is a local permutation polynomial over $\mathbb{Z}_p$ if $f(x_1, a)$ and $f(b, x_2)$ are permutations in $x_1$ and $x_2$ for all $a, b \in \mathbb{Z}_p$.

In Section 2, we obtain a set of necessary and sufficient conditions on the coefficients of a polynomial $f(x_1, x_2)$ over $\mathbb{Z}_p$, $p$ an odd prime, in order that $f(x_1, x_2)$ be a local permutation polynomial. Clearly the number of local permutation polynomials over $\mathbb{Z}_p$ equals the number of Latin squares of order $p$. Thus, the number of Latin squares of order $p$ equals the number of sets of coefficients satisfying the set of conditions given in Section 2. Finally, in Section 3, we use our theory to show that there are twelve local permutation polynomials over $\mathbb{Z}_p$ which are given by

$$f(x_1, x_2) = a_{10}x_1 + a_{01}x_2 + a_{00}$$

where $a_{10} = 1$ or 2, $a_{01} = 1$ or 2, and $a_{00} = 0, 1, or 2$.

2. A NECESSARY AND SUFFICIENT CONDITION

Clearly, the only local permutation polynomials over $\mathbb{Z}_2$ are $x_1 + x_2$ and $x_1 + x_2 + 1$ so that we may assume $p$ to be an odd prime. We will make use of the following well-known formula

$$\sum_{m=1}^{p-1} j^k = \begin{cases} 0 & \text{if } k \neq 0 \pmod{p-1}, \\ -1 & \text{if } k = 0 \pmod{p-1}. \end{cases}$$

Suppose

$$f(x_1, x_2) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{mn} x_1^m x_2^n$$

is a local permutation polynomial. Let $f(\hat{i}, \hat{j}) = k_{\hat{i}, \hat{j}}$ for $0 \leq \hat{i}, \hat{j} \leq p - 1$. Since no permutation over $\mathbb{Z}_p$ can have degree $p - 1$, we have

$$\begin{cases} a_{0, p-1} = 0, \\ \sum_{m=1}^{p-1} k_m a_{m, p-1} = 0, k = 1, \ldots, p - 1. \end{cases}$$

Suppose $\hat{i} = 0$ so that

$$f(0, j) = a_{00} + a_{01}j + \cdots + a_{0, p-1}j^{p-1} = k_{0j}.$$ Let $k_{0j}' = k_{0j} - k_{00}$ for $j = 1, \ldots, p - 1$. The set $\{k_{0j}'\} = \mathbb{Z}_p^*$ and, moreover,

$$a_{01}j^2 + a_{02}j^3 + \cdots + a_{0, p-1}j^{p-1} = k_{0j}'$$

for $j = 1, \ldots, p - 1$.

Raising each of the $p - 1$ equations to the $k$th power, summing by columns and
using (2.1), we obtain

\begin{align}
\sum \frac{k!}{i_{01}! \cdots i_{0,p-1}!} a_{01}^{i_{01}} \cdots a_{0,p-1}^{i_{0,p-1}} &= \begin{cases} 0 & \text{if } k = 2, \ldots, p - 2 \\ 1 & \text{if } k = p - 1 \end{cases}
\end{align}

(C2)

where the sum is over all \((p - 1)\)-tuples \((i_{01}, \ldots, i_{0,p-1})\) with

(a) \(0 \leq i_{01}, \ldots, i_{0,p-1} \leq k\),
(b) \(i_{01} + \cdots + i_{0,p-1} = k\),
(c) \(i_{01} + 2i_{02} + \cdots + (p - 1)i_{0,p-1} \equiv 0 \pmod{p - 1}\).

If \(i > 0\) is fixed, consider

\begin{align}
f(i, j) - k_{0} = \sum_{m=0}^{p-1} \sum_{n=1}^{p-1} a_{mn} i_{m} j_{n} = k^{i}_{j}, \quad j = 1, \ldots, p - 1,
\end{align}

(2.2)

so that \((k^{i}_{j}) = a_{0}^{i/2}\). For each \(k = 2, \ldots, p - 1\) raise each of the \(p - 1\) equations in (2.2) to the \(k\)th power, sum by columns, and use (2.1) to obtain

\begin{align}
\sum \prod_{m=0}^{p-1} \prod_{n=1}^{p-1} a_{mn}^{i_{m} j_{n}} &= \begin{cases} 0 & \text{if } k = 2, \ldots, p - 2 \\ 1 & \text{if } k = p - 1 \end{cases}
\end{align}

(C3)

for each \(i = 1, \ldots, p - 1\), where the sum is over all \((p^2 - p)\)-tuples \((i_{01}, \ldots, i_{0n}, \ldots, i_{p-1,p-1})\) which satisfy

(d) \(0 \leq i_{mn} \leq k\),
(e) \(\sum_{m=0}^{p-1} \sum_{n=1}^{p-1} i_{mn} = k\),
(f) \(\sum_{m=0}^{p-1} i_{m1} + 2 \sum_{m=0}^{p-1} i_{m2} + \cdots + (p - 1) \sum_{m=0}^{p-1} i_{m,p-1} \equiv 0 \pmod{p - 1}\).

A further word of explanation about the sum in (C3) may be helpful at this time. Conditions (d) and (e) arise because of the multinomial coefficients, while (f) determines which terms appear in the given condition. Moreover, the \(\sum m\) appearing in (C3) is understood to mean the sum, counting multiplicities, of all the first subscripts of the \(a_{mn}\)'s which appear in a given term. Finally, we note that condition (C3) actually involves a total of \((p - 1)(p - 2)\) conditions.

If we now fix \(j\) and proceed as above, we obtain another set of necessary conditions. For brevity, we simply state these as

\begin{align}
\begin{cases}
  a_{p-1,0} = 0, \\
  \sum_{n=1}^{p-1} k^{n} a_{p-1,n} = 0, \quad k = 1, \ldots, p - 1.
\end{cases}
\end{align}

(C1')
When \( j = 0 \), we have

\[
(C2') \quad \sum \frac{k!}{\hat{c}_{10}^1 \cdots \hat{c}_{p-1,0}^{1} a_{10}^{1} \cdots a_{p-1,0}^{1}} = \begin{cases} 0 & \text{if } k = 2, \ldots, p - 2 \\ 1 & \text{if } k = p - 1 \end{cases}
\]

where the sum is over all \((p - 1)\)-tuples \((\hat{c}_{10}, \ldots, \hat{c}_{p-1,0})\) with

(a') \quad 0 \leq \hat{c}_{10}, \ldots, \hat{c}_{p-1,0} \leq k,

(b') \quad \hat{c}_{10} + \cdots + \hat{c}_{p-1,0} = k,

(c') \quad \hat{c}_{10} + 2\hat{c}_{20} + \cdots + (p - 1)\hat{c}_{p-1,0} \equiv 0 \pmod{p - 1}.

When \( j = 1, \ldots, p - 1 \), we obtain

\[
(C3') \quad \sum_{m=1}^{p-1} \prod_{n=0}^{p-1} \frac{k!}{\hat{c}_{mn}^{1} \cdots \hat{c}_{mn}^{p-1}} = \begin{cases} 0 & \text{if } k = 2, \ldots, p - 2 \\ 1 & \text{if } k = p - 1 \end{cases}
\]

where the sum is over all \((p^2 - p)\)-tuples \((\hat{c}_{10}, \ldots, \hat{c}_{mn}, \ldots, \hat{c}_{p-1,p-1})\) that satisfy

(d') \quad 0 \leq \hat{c}_{mn} \leq k,

(e') \quad \sum_{n=0}^{p-1} \sum_{m=0}^{p-1} \hat{c}_{mn} = k,

(f') \quad \sum_{n=0}^{p-1} \hat{c}_{1n} + 2\sum_{n=0}^{p-1} \hat{c}_{2n} + \cdots + (p - 1)\sum_{n=0}^{p-1} \hat{c}_{p-1,n} \equiv 0 \pmod{p - 1}.

We now proceed to show that if the coefficients of a polynomial \( f(x_1, x_2) \) satisfy the above conditions, then \( f(x_1, x_2) \) is a local permutation polynomial. Suppose the coefficients of \( f(x_1, x_2) \) satisfy \((C1), (C2), (C3), (C1'), (C2'), \) and \((C3')\). For each fixed \( \hat{c} \), let \( \hat{c}_{ij} = f(\hat{c}, j) - f(\hat{c}, 0) \) for \( j = 1, \ldots, p - 1 \). The above conditions imply that for fixed \( \hat{c} = 0, 1, \ldots, p - 1 \) the \( \hat{c}_{ij} \) satisfy

\[(2.3) \quad \sum_{j=1}^{p-1} \hat{c}_{ij}^k = \begin{cases} 0 & \text{if } k = 1, \ldots, p - 2 \\ -1 & \text{if } k = p - 1 \end{cases}
\]

Let \( V \) be the matrix

\[
V = \begin{bmatrix}
1 & \cdots & 1 \\
\hat{c}_{i1} & \cdots & \hat{c}_{i,p-1} \\
\vdots & & \vdots \\
\hat{c}_{p-2}^{1} & \cdots & \hat{c}_{p-2}^{p-2} \\
\hat{c}_{i1}^{1} & \cdots & \hat{c}_{i,p-1}^{p-1}
\end{bmatrix}
\]

Using \((2.3)\), we see that
\[
\begin{pmatrix}
-1 & 0 & \ldots & 0 & 0 \\
0 & 0 & \ldots & 0 & -1 \\
0 & 0 & \ldots & -1 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & -1 & \ldots & 0 & 0 \\
\end{pmatrix} = \pm 1.
\]

Since \( \det(V) \) is the Van der Monde determinant, we have, for fixed \( i \),

\[
\det(V) = \prod_{j \neq k} (t_{ij} - t_{ik}) \neq 0
\]

so that the \( t_{ij} \) for \( j = 1, \ldots, p - 1 \) are distinct. Hence,

\[
f(i, 0) \text{ and } f(i, j) = t_{ij} + f(i, 0) \text{ for } j = 1, \ldots, p - 1
\]

constitute all of \( Z_p \).

A similar argument shows that if for each fixed \( j \),

\[
s_{i,j} = f(i, j) - f(0, j) \text{ for } i = 1, \ldots, p - 1,
\]

then

\[
f(0, j) \text{ and } f(i, j) = s_{i,j} + f(0, j) \text{ for } i = 1, \ldots, p - 1
\]

run through the elements of \( Z_p \). Hence, we have

**Theorem 1:** If \( f(x_1, x_2) \) is a polynomial over \( Z_p \), \( p \) an odd prime, then \( f \) is a local permutation polynomial over \( Z_p \) if and only if the coefficients of \( f \) satisfy \((C_1),(C_2),(C_3),(C_1'),(C_2'),(C_3')\).

**Corollary 2:** The number of Latin squares of order \( p \) an odd prime equals the number of sets of coefficients \( \{a_{mn}\} \) satisfying the above conditions.

We note from condition \((C_1)\) that \( a_{0,p-1} = a_{1,p-1} = \ldots = a_{p-1,p-1} = 0 \), since the determinant of the coefficient matrix in \((C_1)\) is the Van der Monde determinant. Similarly, \((C_1')\) implies that \( a_{p-1,0} = a_{p-1,1} = \ldots = a_{p-1,p-1} = 0 \). We further note that we have a total of \( 2(p - 1) \) conditions so that, in general, the conditions are not independent.

3. **ILLUSTRATIONS**

As a simple illustration of the above theory, we determine all local permutation polynomials over \( Z_3 \). If

\[
f(x_1, x_2) = \sum_{m=0}^{2} \sum_{n=0}^{2} a_{mn} x_1^m x_2^n
\]

then the set of necessary and sufficient conditions becomes

\[(2.4)\]
\[
a_{02} = a_{12} = a_{22} = a_{21} = a_{20} = 0,
\]

\[(2.5)\]
\[
a_{01}^2 + a_{02}^2 = a_{10}^2 + a_{20}^2 = 1,
\]

\[(2.6)\]
\[
a_{01}^2 + a_{11}^2 + 2a_{01}a_{11} = a_{10}^2 + a_{11}^2 + 2a_{10}a_{11} = 1,
\]

\[(2.7)\]
\[
a_{01}^2 + a_{11}^2 + a_{01}a_{11} = a_{10}^2 + a_{11}^2 + a_{10}a_{11} = 1.
\]
Using (2.4) and (2.5), we see that \( a_{11} = 1 \) or \( 2 \) and \( a_{10} = 1 \) or \( 2 \). From (2.6) and (2.7), we have \( a_{11} = 0 \). Since \( a_{10} \) is arbitrary, we see that there are a total of twelve local permutation polynomials over \( \mathbb{Z}_3 \), given by

\[
f(x_1, x_2) = a_{10} x_1 + a_{01} x_2 + a_{00},
\]

where \( a_{10} = 1 \) or \( 2 \), \( a_{01} = 1 \) or \( 2 \), and \( a_{00} = 0, 1, \) or \( 2 \).

*****

GENERALIZED CYCLOTOMIC POLYNOMIALS, FIBONACCI CYCLOTOMIC POLYNOMIALS, AND LUCAS CYCLOTOMIC POLYNOMIALS*

CLARK KIMBERLING
University of Evansville, Evansville, IN 47702

1. INTRODUCTION AND MAIN THEOREM

In [6], Hoggatt and Long ask what polynomials in \( I[x] \) are divisors of the Fibonacci polynomials, which are defined by the recursion

\[
F_0(x) = 0, \quad F_1(x) = 1, \quad F_n(x) = x F_{n-1}(x) + F_{n-2}(x) \quad \text{for} \quad n \geq 2.
\]

In this paper, we answer this question in terms of cyclotomic polynomials. We prove that each Fibonacci polynomial \( F_n(x) \), for \( n \geq 2 \), has one and only one irreducible factor which is not a factor of any \( F_k(x) \) for any positive \( k \) less than \( n \). We call this irreducible factor the \( n \)th Fibonacci cyclotomic polynomial and denote it \( \Phi_n(x) \).

The method applied to \( F_n \)'s to produce \( \Phi_n \)'s applies naturally to the more general polynomials \( \delta_n(x, y, z) \) which were introduced in [7] and are defined just below. Accordingly, in Section 2, we shall apply the method at this more general level rather than directly to the \( F_n \)'s. The polynomials \( \delta_n(x, y, z) \) so obtained from the \( \delta_n(x, y, z) \)'s we call generalized cyclotomic polynomials. Special cases of the \( \delta_n \)'s are the ordinary cyclotomic polynomials \( \Phi_n(x, 1, 0) \), the Fibonacci cyclotomic polynomials \( \Phi_n(x) \) already mentioned, and a sequence

\[
\delta_n(x) = \delta_n(x, 0, 1)
\]

which we call the Lucas cyclotomic polynomials. Section 3 is devoted to the \( \delta_n \)'s and Section 4 to the \( \Phi_n \)'s. In Sections 3, 4, and 5, we determine all the irreducible factors of the Fibonacci polynomials, the modified Lucas polynomials defined in [7] as \( \delta_n(x, 0, 1) \), and the Lucas polynomials.

In Section 6, we transform the generalized Fibonacci and Lucas polynomials into sequences \( U_n(x, y) \) and \( V_n(x, y) \) having the same divisibility properties as the \( F_n \)'s and \( L_n \)'s, respectively. The coefficients of these polynomials are all binomial coefficients, in accord with the identity

\[
2U_n(x, y) + V_n(x, y) = (x + y)^n.
\]

The polynomials \( \delta_n(x, y, z) \) may be defined as follows:

\[
L_n(x, y) = L_n(x, y) - \frac{L_n(x, y)}{x - y} \quad \text{for} \quad n \geq 0,
\]

*Supported by a University of Evansville Alumni Research Fellowship.