7. Morgan Ward. "The Law of Apparition of Primes in a Lucasian Sequence." *Trans. AMS* 44 (1948):68-86.
8. Morgan Ward. "Memoir on Elliptic Divisibility Sequences." *Amer. J. Math.* 70 (1948):31-74.
9. Morgan Ward. "The Law of Repetition of Primes in an Elliptic Divisibility Sequence." *Duke Math. J.* 15 (1948):941-946.

*****

LOCAL PERMUTATION POLYNOMIALS IN THREE VARIABLES OVER Z_p

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

1. INTRODUCTION

If p is a prime, let Z_p denote the integers modulo p and Z_p^* the set of nonzero elements of Z_p. It is well known that every function from $Z_p \times Z_p \times Z_p$ into Z_p can be represented as a polynomial of degree $< p$ in each variable. We say that a polynomial $f(x_1, x_2, x_3)$ with coefficients in Z_p is a *local permutation polynomial* in three variables over Z_p if $f(x_1, a, b)$, $f(c, x_2, d)$, and $f(e, f, x_3)$ are permutations in x_1, x_2, and x_3, respectively, for all a, b, c, d, e, $f \in Z_p$. A general theory of local permutation polynomials in n variables will be discussed in a subsequent paper.

In an earlier paper [2], we considered polynomials in two variables over Z_p and found necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in two variables over Z_p. The number of Latin squares of order p was thus equal to the number of sets of coefficients satisfying the conditions given in [2]. In this paper, we consider polynomials in three variables over Z_p and again determine necessary and sufficient conditions on the coefficients of a polynomial in order that it represents a local permutation polynomial in three variables over Z_p.

As in [1], a *Latin cube of order* n is defined as an $n \times n \times n$ cube consisting of n rows, n columns, and n levels in which the numbers $0, 1, \ldots, n - 1$ are entered so that each number occurs exactly once in each row, column, and level. Clearly the number of Latin cubes of order p equals the number of local permutation polynomials in three variables over Z_p. We say that a Latin cube is *reduced* if row one, column one, and level one are in the form $0, 1, \ldots, n - 1$. The number of reduced Latin cubes of order p will equal the number of sets of coefficients satisfying the set of conditions given in Section 2.

In Section 3, we use our theory to show that there is only one reduced local permutation polynomial in three variables over Z_3 and, thus, there is precisely one reduced Latin cube of order three.

2. A NECESSARY AND SUFFICIENT CONDITION

Clearly, the only local permutation polynomials in three variables over Z_2 are $x_1 + x_2 + x_3$ and $x_1 + x_2 + x_3 + 1$, so that we may assume p to be an odd prime. We will make use of the following well-known formula:

$$\sum_{j=1}^{p-1} j^k = \begin{cases} 0 & \text{if } k \not\equiv 0 \pmod{p-1} \\ -1 & \text{if } k \equiv 0 \pmod{p-1}. \end{cases} \tag{2.1}$$

Suppose

$$f(x_1, x_2, x_3) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{mnr} x_1^m x_2^n x_3^r$$

is a local permutation polynomial over Z_p. We assume that $f(x_1, x_2, x_3)$ is in reduced form so that for $t = 0, 1, \ldots, p - 1$ we have

$$f(t, 0, 0) = f(0, t, 0) = f(0, 0, t) = t.$$

Thus, the corresponding Latin cube is reduced so that row one, column one, and level one are in the form $0, 1, \ldots, p - 1$. If we write out the above equations and use the fact that the coefficient matrix is the Vandermonde matrix whose determinant is nonzero, we have the condition

$$a_{t00} = a_{0t0} = a_{00t} = \begin{cases} 0 & \text{if } t = 0, 2, 3, \ldots, p-1 \\ 1 & \text{if } t = 1. \end{cases} \tag{C1}$$

It is well known that no permutation over Z_p can have degree $p - 1$. By considering the polynomials $f(0, n, x_3)$ for $n = 0, 1, \ldots, p - 1$, one can show that $a_{0,n,p-1} = 0$ for $n = 0, 1, \ldots, p - 1$. Proceeding in a similar manner, we find that

$$\left.\begin{aligned} a_{0,t,p-1} &= a_{t,0,p-1} = 0 \\ a_{0,p-1,t} &= a_{t,p-1,0} = 0 \\ a_{p-1,t,0} &= a_{p-1,0,t} = 0 \end{aligned}\right\} \text{ for } t = 0, 1, \ldots, p-1. \tag{C2}$$

Let

$$f(i, j, x_3) = \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{mnr} i^m j^n x_3^r, \text{ for } 1 \le i, j \le p-1$$

and consider the coefficient of x_3^{p-1}. Using the fact that no permutation over Z_p can have degree $p - 1$, we see that

$$\sum_{m=0}^{p-1} \sum_{n=0}^{p-1} a_{m,n,p-1} i^m j^n = 0, \text{ for } 1 \le i, j \le p-1. \tag{C3}$$

Similarly, one can show that

$$\sum_{m=0}^{p-1} \sum_{r=0}^{p-1} a_{m,p-1,r} i^m k^n = 0, \text{ for } 1 \le i, k \le p-1. \tag{C4}$$

and

$$\sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{p-1,n,r} j^n k^n = 0, \text{ for } 1 \le j, k \le p-1. \tag{C5}$$

We note that the above conditions correspond to conditions (C1) and (C1′) of [2].

Let $f(i, j, k) = \ell(i, j, k)$ for $0 \le i, j, k \le p - 1$. Suppose $i = 0$ so that

$$f(0, j, k) = \sum_{n=0}^{p-1} \sum_{r=0}^{p-1} a_{0nr} j^n k^r.$$

Let $\ell'(0, j, k) = f(0, j, k) - \ell(0, 0, 0)$. Fix j and write out the $p - 1$

equations for $k = 1, \ldots, p-1$. For fixed j, $\{\ell'(0, j, k)\}$ runs through the elements of Z_p^*. If we raise each of the equations to the ℓth power, sum by columns using (2.1), we obtain for each $j = 1, \ldots, p-1$,

$$\text{(C6)} \qquad \sum \prod_{r=1}^{p-1} \prod_{n=0}^{p-1} \frac{\ell! a_{0nr}^{i_{0nr}} j^{\Sigma n}}{i_{0nr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{0nr} such that

$$\text{(2.2)} \qquad 0 \le i_{0nr} \le \ell$$

$$\text{(2.3)} \qquad \sum_{r=1}^{p-1} \sum_{n=0}^{p-1} i_{0nr} = \ell$$

$$\text{(2.4)} \qquad \sum_{r=1}^{p-1} \sum_{n=0}^{p-1} r i_{0nr} \equiv 0 \pmod{p-1}.$$

In the condition (C6), Σn is understood to mean the sum, counting multiplicities, of all second subscripts of the a_{0nr}'s which appear in a given term.

Similarly, if we fix k and write out the $p-1$ equations for $j = 1, \ldots, p-1$, raise each equation to the ℓth power, sum by columns using (2.1), we obtain for each $k = 1, \ldots, p-1$,

$$\text{(C7)} \qquad \sum \prod_{n=1}^{p-1} \prod_{r=0}^{p-1} \frac{\ell! a_{0nr}^{i_{0nr}} k^{\Sigma r}}{i_{0nr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{0nr} such that

$$\text{(2.5)} \qquad 0 \le i_{0nr} \le \ell$$

$$\text{(2.6)} \qquad \sum_{n=1}^{p-1} \sum_{r=0}^{p-1} i_{0nr} = \ell$$

$$\text{(2.7)} \qquad \sum_{n=1}^{p-1} \sum_{r=0}^{p-1} n i_{0nr} \equiv 0 \pmod{p-1}.$$

We observe that we can obtain the condition (C7) from the condition (C6) as follows. In (C6), (2.2), (2.3), and (2.4), let $n = r$, $r = n$, and $j = k$. After making these substitutions, replace the subscripts $0rn$ by $0nr$ to obtain (C7).

Along the same line, let $j = 0$ and $\ell'(i, 0, k) = f(i, 0, k) - \ell(0, 0, 0)$. If i is fixed, then for each $i = 1, \ldots, p-1$, we obtain

$$\text{(C8)} \qquad \sum \prod_{r=1}^{p-1} \prod_{m=0}^{p-1} \frac{\ell! a_{m0r}^{i_{m0r}} i^{\Sigma m}}{i_{m0r}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases}$$

where the sum is over all i_{m0r} such that

$$\text{(2.8)} \qquad 0 \le i_{m0r} \le \ell$$

$$\sum_{r=1}^{p-1}\sum_{m=0}^{p-1} i_{m0r} = \ell \tag{2.9}$$

$$\sum_{r=1}^{p-1}\sum_{m=0}^{p-1} r i_{m0r} \equiv 0 \pmod{p-1}. \tag{2.10}$$

If $j = 0$ and k is fixed, then for each $k = 1, \ldots, p-1$ we obtain a set of conditions (C9) which can be obtained from the condition (C8) as follows. In (C8), (2.8), (2.9), and (2.10), let $m = r$, $r = m$, and $i = k$. After making these substitutions, replace the subscripts $r0m$ by $m0r$ to obtain (C9).

Finally, if $k = 0$, then for $i = 1, \ldots, p-1$, we obtain

$$\sum \prod_{n=1}^{p-1} \prod_{m=0}^{p-1} \frac{\ell! a_{mn0}^{i_{mn0}} i^{\Sigma m}}{i_{mn0}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases} \tag{C10}$$

where the sum is over all i_{mn0} such that

$$0 \le i_{mn0} \le \ell \tag{2.11}$$

$$\sum_{n=1}^{p-1}\sum_{m=0}^{p-1} i_{mn0} = \ell \tag{2.12}$$

$$\sum_{n=1}^{p-1}\sum_{m=0}^{p-1} n i_{mn0} \equiv 0 \pmod{p-1}. \tag{2.13}$$

If $k = 0$, then for $j = 1, \ldots, p-1$ we obtain a set of conditions (C11) which can be obtained from (C10) as follows. In (C10), (2.11), (2.12), and (2.13), let $m = n$, $n = m$, and $i = j$. After making these substitutions, replace the subscripts $nm0$ by $mn0$ to obtain (C11).

Thus, we have six sets of conditions involving coefficients where at least one subscript on the coefficient is zero. These conditions correspond to the conditions (C2) and (C2′) of [2].

We will now consider the general case where $ijk > 0$. Let $f(i, j, k) = \ell(i, j, k)$ and suppose $\ell'(i, j, k) = f(i, j, k) - \ell(i, j, 0)$ for fixed i and j. The set $\{\ell'(i, j, k)\}$ for $k = 1, \ldots, p-1$ constitutes all of Z_p^*. Raising each of the equations to the ℓth power, summing by columns using (2.1), we obtain for each $1 \le i, j \le p-1$,

$$\sum \prod_{r=1}^{p-1} \prod_{m=0}^{p-1} \prod_{n=0}^{p-1} \frac{\ell! a_{mnr}^{i_{mnr}} i^{\Sigma m} j^{\Sigma n}}{i_{mnr}!} = \begin{cases} 0 & \text{if } \ell = 2, \ldots, p-2 \\ 1 & \text{if } \ell = p-1, \end{cases} \tag{C12}$$

where the sum is over all i_{mnr} such that

$$0 \le i_{mnr} \le \ell \tag{2.14}$$

$$\sum_{r=1}^{p-1}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} i_{mnr} = \ell \tag{2.15}$$

$$\sum_{r=1}^{p-1}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1} r i_{mnr} \equiv 0 \pmod{p-1}. \tag{2.16}$$

Fixing i and k and proceeding as above for each $1 \leq i, k \leq p - 1$, we obtain a set of conditions (C13) which can be obtained from (C12) as follows. In (C12), (2.14), (2.15), and (2.16), let $n = r$, $r = n$, and $j = k$. After making these substitutions, replace the subscripts mrn by mnr to obtain (C13).

Finally, fixing j and k and proceeding as above, for each $1 \leq j, k \leq p - 1$, we obtain a set of conditions (C14) which can be obtained from (C12) as follows. In (C12), (2.14), (2.15), and (2.16), let $m = r$, $r = m$, and $i = k$. After making these substitutions, replace subscripts rnm by mnr to obtain (C14).

We observe that the conditions (C12), (C13), and (C14) correspond to the conditions (C3) and (C3′) of [2]. We note that the set of conditions (C1), ..., (C14) actually involves a total of

$$9p + 3(p - 1)^2 + 6(p - 1)(p - 2) + 3(p - 1)^2(p - 2) = 3p^3 - 3p^2 + 9$$

conditions. Further, it should be noted that some of the above conditions may be simplified by making substitutions from (C1) and (C2). However, we will not make these substitutions at the present time.

We now proceed to show that, if the coefficients of a polynomial $f(x_1, x_2, x_3)$ satisfy the above conditions, then $f(x_1, x_2, x_3)$ is a local permutation polynomial over Z_p. Suppose the coefficients of $f(x_1, x_2, x_3)$ satisfy the conditions (C1), ..., (C14). For each fixed $0 \leq i, j \leq p - 1$, let $t_{ijk} = f(i, j, k) - f(i, j, 0)$ for $k = 1, \ldots, p - 1$. The above conditions imply that for fixed i and j the t_{ijk} satisfy

$$\sum_{k=1}^{p-1} t_{ijk}^{\ell} = \begin{cases} 0 & \text{if } \ell = 1, \ldots, p - 2 \\ -1 & \text{if } \ell = p - 1. \end{cases} \tag{2.17}$$

Let V be the matrix

$$V = \begin{bmatrix} 1 & \cdots & 1 \\ t_{ij1} & \cdots & t_{i,j,p-1} \\ \vdots & & \vdots \\ t_{ij1}^{p-2} & \cdots & t_{i,j,p-1}^{p-2} \end{bmatrix}.$$

Using (2.17), we see that

$$\det(V^2) = \det(V)\det(V^t) = \det \begin{bmatrix} -1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 \end{bmatrix} = \pm 1.$$

Since $\det(V)$ is the Vandermonde determinant, we have for fixed i and j,

$$\det(V) = \prod_{k_1 > k_2} (t_{ijk_1} - t_{ijk_2}) \neq 0,$$

so that the t_{ijk} are distinct for $k = 1, \ldots, p - 1$. Hence, for fixed i and j, $f(i, j, 0)$ and $f(i, j, k) = t_{ijk} + f(i, j, 0)$ for $k = 1, \ldots, p - 1$ constitute all of Z_p.

If $0 \leq i, k \leq p - 1$ are fixed, let $s_{ijk} = f(i, j, k) - f(i, 0, k)$ for $j = 1, \ldots, p - 1$. Proceeding as above, $f(i, 0, k)$ and $f(i, j, k) = s_{ijk} + f(i, 0, k)$ are distinct for $j = 1, \ldots, p - 1$ and thus constitute all of Z_p.

Similarly, if $0 \leq j,\ k \leq p-1$ are fixed, let $u_{ijk} = f(i,\ j,\ k) - f(0,\ j,\ k)$ for $i = 1, \ldots, p-1$. Hence, $f(0,\ j,\ k)$ and $f(i,\ j,\ k) = u_{ijk} + f(0,\ j,\ k)$ are distinct for $i = 1, \ldots, p-1$ and thus constitute all of Z_p.

We have now proven the following.

Theorem 1: If $f(x_1,\ x_2,\ x_3)$ is a polynomial over Z_p, p an odd prime, then f is a reduced local permutation polynomial over Z_p if and only if the coefficients of f satisfy (C1), ..., (C14).

Corollary 2: The number of reduced Latin cubes of order p an odd prime equals the number of sets of coefficients $\{a_{mnr}\}$ satisfying the above conditions.

3. ILLUSTRATIONS

As a simple illustration of the above theory, we determine all reduced local permutation polynomials in three variables over Z_3. Let

$$f(x_1,\ x_2,\ x_3) = \sum_{m=0}^{2} \sum_{n=0}^{2} \sum_{r=0}^{2} a_{mnr} x_1^m x_2^n x_3^r. \tag{3.1}$$

The corresponding Latin cube will be in reduced form, so that row one, column one, and level one are in the form 0, 1, and 2. From (C1), we see that

$$\begin{aligned} a_{000} &= 0 \\ a_{100} = a_{010} = a_{001} &= 1 \\ a_{200} = a_{020} = a_{002} &= 0. \end{aligned} \tag{3.2}$$

From (C2), we see that

$$\begin{aligned} a_{012} = a_{102} = a_{021} = a_{120} = a_{210} = a_{201} &= 0 \\ a_{022} = a_{202} = a_{022} = a_{220} = a_{202} = a_{220} &= 0. \end{aligned} \tag{3.3}$$

We have thus uniquely determined 16 coefficients from the conditions (C1) and (C2).

From (C3), we obtain, after some simplification,

$$\begin{aligned} a_{112} + a_{122} + a_{212} + a_{222} &= 0 \\ 2a_{112} + a_{122} + 2a_{212} + a_{222} &= 0 \\ 2a_{112} + 2a_{122} + a_{212} + a_{222} &= 0 \\ a_{112} + 2a_{122} + 2a_{212} + a_{222} &= 0, \end{aligned} \tag{3.4}$$

so that $a_{112} = a_{122} = a_{212} = a_{222} = 0$.

From (C4), we obtain, after some simplification,

$$\begin{aligned} a_{121} + a_{221} &= 0 \\ 2a_{121} + 2a_{221} &= 0 \\ 2a_{121} + a_{221} &= 0 \\ a_{121} + 2a_{221} &= 0, \end{aligned} \tag{3.5}$$

so that $a_{121} = a_{221} = 0$. Using (C5), after some simplification, we see that $a_{211} = 0$.

From (C6), with $j = 1$, we have, after some simplification,

$$a_{001}^2 + a_{011}^2 + 2a_{001}a_{011} = 1. \tag{3.6}$$

If $j = 2$ in (C6), we obtain

(3.7) $$a_{001}^2 + a_{011}^2 + a_{001}a_{011} = 1.$$

Using (3.6) and (3.7) along with the fact that $a_{001} = 1$, we see that $a_{011} = 0$.

Since all the variables in (C7) have already been uniquely determined, we proceed to (C8), where we obtain

(3.8) $$a_{001}^2 + a_{101}^2 + 2a_{001}a_{101} = 1$$

and

(3.9) $$a_{001}^2 + a_{101}^2 + a_{001}a_{101} = 1,$$

so that $a_{101} = 0$.

From (C10), we obtain

(3.10) $$a_{010}^2 + a_{110}^2 + 2a_{010}a_{110} = 1$$

and

(3.11) $$a_{010}^2 + a_{110}^2 + a_{010}a_{110} = 1,$$

so that $a_{110} = 0$.

From (C12), we obtain, after simplification,

(3.12) $$a_{111}^2 + 2a_{111} = 0$$

and

(3.13) $$a_{111}^2 + a_{111} = 0,$$

so that $a_{111} = 0$.

We have now uniquely determined all 27 coefficients in (3.1). Thus,

$$f(x_1, x_2, x_3) = x_1 + x_2 + x_3$$

is the only reduced local permutation polynomial in three variables over Z_3 and, hence, there is precisely one reduced Latin cube of order three. If we list the cube in terms of the three Latin squares of order three which form its different levels, we can list the only reduced Latin cube of order three as

012	120	201
120	201	012
201	012	120.

REFERENCES

1. J. Arkin and E. G. Straus. "Latin k-cubes." *The Fibonacci Quarterly* 12 (1974):288-292.
2. G. L. Mullen. "Local Permutation Polynomials over Z_p." *The Fibonacci Quarterly* 18 (1980):104-108.

*****

SOME COMBINATORIAL IDENTITIES

MORDECHAI LEWIN

Israel Institute of Technology, Haifa

In this paper, we wish to derive some combinatorial identities (partly known, partly apparently new) by combining well-known recurrence relations with known forms for characteristic polynomials of paths and cycles (i.e., of their adjacency matrices). We also obtain some extensions of known results.