International J.Math. Combin. Vol.2 (2009), 58-65

Permutation Polynomials modulo n, $n \neq 2^w$ and Latin Squares

Vadiraja Bhatta G. R. and Shankar B. R.

Department of Mathematical and Computational Sciences

National Institute of Technology Karnataka

Surathkal Mangalore - 575 025, India

E-mail: grvbhatta@yahoo.co.in, shankarbr@gmail.com

Abstract: Our work is motivated by a recent paper of Rivest [6], concerning permutation polynomials over the rings Z_n with $n = 2^w$. Permutation polynomials over finite fields and the rings Z_n have lots of applications, including cryptography. For the special case $n = 2^w$, a characterization has been obtained in [6] where it is shown that such polynomials can form a Latin square ($0 \leq x, y \leq n-1$) if and only if the four univariate polynomials $P(x,0), P(x,1), P(0,y)$ and $P(1,y)$ are permutation polynomials. Further, it is shown that pairs of such polynomials will never form Latin squares. In this paper, we consider bivariate polynomials $P(x,y)$ over the rings Z_n when $n \neq 2^w$. Based on preliminary numerical computations, we give complete results for linear and quadratic polynomials. Rivest's result holds in the linear case while there are plenty of counterexamples in the quadratic case.

Key Words: Permutation polynomials, Latin squares, Orthogonal Latin squares, Orthomorphisms.

AMS(2000): 05B15

§1. Permutation Polynomials

A polynomial $P(x) = a_0 + a_1x + ... + a_dx^d$ is said to be a permutation polynomial over a finite ring R if P permutes the elements of R. R. Lidl and H. Niderreiter [2] have described various types of permutation polynomials over finite fields F_q. Lidl and Mullen [3], [4] gave a survey of various possibilities of polynomials over finite fields as permutation polynomials and also gave the applications of these permutation polynomials. Rivest [6] has considered the class of rings Z_n, where $n = 2^w$ to study the permutaion polynomials. He derived necessary and sufficient conditions for a polynomial to be a permutation polynomial over Z_n, where $n = 2^w$, in terms of the coefficients of the polynomials. The following is from [6]:

Theorem 1(Rivest) *Let $P(x) = a_0 + a_1x + ... + a_dx^d$ be a polynomial with integral coefficients. Then $P(x)$is a permutation polynomial modulo $n = 2^w$, $w \geq 2$, if and only if a_1 is odd and both $(a_2 + a_4 + ...)$ and $(a_3 + a_5 + ...)$ are even.*

Also, Rivest gave a result about bivariate polynomials $P(x,y)$ giving latin squares modulo

[1]Received April 3, 2009. Accepted June 2, 2009.

$n = 2^w$,$w \geq 2$. The following result is also from [6]:

Theorem 2(Rivest) *A bivariate polynomial $P(x, y) = \sum_{i,j} a_{ij} x^i y^j$ represents a Latin square modulo $n = 2^w$, where $w \geq 2$, if and only if the four univariate polynomials $P(x, 0), P(x, 1), P(0, y)$ and $P(1, y)$ are all permutation polynomials modulo n.*

§2. Latin squares

A Latin square of order n is an $n \times n$ array based on some set S of n symbols, with the property that every row and every column contains every symbol exactly once. In other words, every row and every column is a permutation of S. Since the arithmetical properties of symbols are not used, the nature of the elements of S is immaterial. An example of a Latin square of order 4 is shown below.

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

Two Latin squares A and B of the same order are said to be equivalent if it is possible to reorder the rows of A, reorder the columns of A, and/or relabel the symbols of A in such a way as to produce the square B. A partial Latin square of order n is an $n \times n$ array in which some cells are filled with the elements of some n-set while others are empty, such that no row or column contains a repeated element. A Latin rectangle of size $k \times n$ is a $k \times n$ array with entries from $S = \{0, 1, 2...., n-1\}$ such that every row is a permutation of S and the columns contain no repetitions.
The following theorem is proved in [7]:

Theorem 3 *If A is a $k \times n$ Latin rectangle, then one can append $(n-k)$ further rows to A so that the resulting array is a Latin square.*

If L is Latin square of order s and $n \geq 2s$, then there is a Latin square of order n with L as a subsquare [7]. Starting from a partial Latin square of order n, it is possible to complete it to a Latin square of order n, see [5].

Theorem 4 *A partial Latin square of order n with at most $n-1$ filled cells can be completed to a Latin square of order n.*

Two Latin squares of order n are called orthogonal if each of the n^2 ordered pairs $(0, 0), ., (n-1, n-1)$ appears exactly once in the two squares. A pair of orthogonal Latin squares of order 4 is shown below.

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

A Latin square is called self-orthogonal if it is orthogonal to its own transpose.Latin squares and orthogonal Latin squares have been extensively studied since Euler considered it first in 1779. Euler knew that a pair of orthogonal Latin squares of order n existed for all odd values of n and all $n \equiv 0(mod4)$. Euler went on to assert that no such pairs exist for $n \equiv 2(mod4)$, this was known as *Euler's conjecture* for 177 years until it was suddenly and completely disproved by Bose, Parker and Shrikhande. Indeed, the only exceptions are $n = 2, 6$ and for all other values, pairs of orthogonal Latin squares exist [5]. Recently, G. Appa, D. Magos, I. Mourtos gave an LP-based proof that there is no pair of orthogonal Latin squares of order 6 (see [1]).

Rivest [6] considered such polynomials *modulo* $n = 2^w$, where $w \geq 2$ and showed that orthogonal pairs of Latin squares do not exist [6]. Here we have considered them modulo n, $n \neq 2^w$ and to our surprise, found that there are many examples of orthogonal pairs of Latin squares. Based on preliminary computations, if $n \neq 2^w$, we have found that a bivariate polynomial can fail to form a Latin square even when these 4 univariate polynomials are permutation polynomials. In a Latin square determined by $P(x, y)$, values of $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$ are given by the entries of first two columns and first two rows.

Theorem 5 *A bivariate linear polynomial $a + bx + cy$ represents a latin square over Z_n if and only if one of the following equivalent conditions is satisfied:*

(i) *both b and c are coprime with n;*

(ii) *$a + bx$, $a + cy$, $(a + c) + bx$ and $(a + b) + cy$ are all permutation polynomials modulo n.*

Proof For linear polynomials over any Z_n,we can observe that $a + bx + cy$ forms a Latin square if and only if $a + bx$, $a + cy$, $(a + c) + bx$, $(a + b) + cy$ are permutation polynomials. This is because, whenever b and c are both co-prime with n, all those 4 polynomials will be permutation polynomials and in those cases we can fill all the entries of the Latin squares by just looking at first row and first column. As these are all distinct elements in the first row and column, and polynomial $bx + cy$ having only two terms, the entries are got by just adding $a(mod\ n)$ to all entries of $bx + cy$. So Rivest's result holds in the linear case. □

Quadratic case: We also tried to characterize quadratic bivariate polynomials in this way. If a polynomial $P(x, y)$ represents a Latin square, then our 4 polynomials $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$ will be obviously permutation polynomials, as they form the first two rows and first two columns of the Latin squares. However, to our surprise, many quadratic polynomials failed to form Latin squares, even though the 4 polynomials $P(x, 0)$, $P(x, 1)$, $P(0, y)$ and $P(1, y)$ are permutation polynomials. The number of such polynomials over different rings Z_n are shown below.

Ring	**No. of polynomials**	**Examples**
Z_6	48	$1 + 5x + 2y + 2xy + 3y^2$
Z_7	1,050	$x + y + xy$
Z_9	4,374	$x + y + xy + 3y^2$
Z_{10}	1,440	$9x + 9y + 8xy$
Z_{11}	8,910	$10x + 10y + 10xy$
Z_{12}	768	$7x + 7y + 10xy + 6x^2 + 6y^2$
Z_{13}	1,8876	$12x + 12y + 12xy$
Z_{14}	8,400	$13x + 11y + 6xy$
Z_{15}	3,720	$8x + 14y + 14xy$

However, there are plenty of quadratic bivariate polynomials which do form Latin squares. But we are not able to characterize them using the permutation behavior of the corresponding univariate polynomials. From the data collected, we observed that in all cases where $P(x, y)$ formed a Latin square, the cross term xy was always absent. Hence we could formulate and prove two interesting results.

However, we need an interesting fact regarding orthomorphisms in proving the theorem. The definition as well as proof of the theorem quoted are given in the well-known text of J.H.Van Lint and R.M.Wilson, *A Course in Combinatorics*, chapter 22, page 297.

Definition 2.1 *An* orthomorphism *of an abelian group G is a permutation σ of the elements of G such that $x \mapsto \sigma(x) - x$ is also a permutation of G.*

Theorem 6 *If an abelian group G admits an orthomorphism, then its order is odd or its Sylow 2-subgroup is not cyclic.*

We are now ready to state and prove the main results of this paper:

Theorem 7 *If $P(x, y)$ is a bivariate polynomial having* no cross term*, then $P(x, y)$ gives a Latin square if and only if $P(x, 0)$ and $P(0, y)$ are permutation polynomials.*

Proof $P(x, 0)$ is the first column of the square and $P(0, y)$ is the first row. If $P(x, y) = f(x)+g(y)$, looking at first row and column, we can complete the square just as addition modulo n (which is a group). So, $P(x, y)$ will be a Latin square. □

Theorem 8 *Let n be even and $P(x, y) = f(x) + g(y) + xy$ be a bivariate quadratic polynomial, where $f(x)$ and $g(x)$ are permutation polynomials modulo n. Then $P(x, y)$ does not give a Latin square modulo n.*

Proof We assume that n is even and greater than 2. If $f(x)$ is a permutation polynomial then $f(x) + k$ is also a permutation polynomial. So, we can assume that $k = 0$.Now $f(x) + g(y)$ always represents a Latin square whenever $f(x)$ and $g(y)$ are permutation polynomials, by the last theorem. When $x = c$, the cth row entries will be $P(c, 0), P(c, 1), ...P(c, n-1)$. i.e., $f(c)+$

$g(0)+0, f(c)+g(1)+c, f(c)+g(2)+2c, ..., f(c)+g(n-1)+(n-1)c$ Let $f(c)=\theta$, a constant. Then, $\theta+0, \theta+c, ..., \theta+(n-1)c$ will be a permutation of $\{0,1,.....,n-1\}$ if $g.c.d.(n,c)=1$. So, let c be such that $g.c.d.(n,c)=1$ Without loss of generality, we may ignore the constant θ in the sequence.Also $g(0), g(1), ..., g(n-1)$ is some permutation of $\{0,1,\ldots,n-1\}$. The sum of these two permutations fails to be a permutation of Z_n, since there are no orthomorphisms of Z_n as n is even. Hence the cth row contains repetitions and $P(x,y)$ does not represent a Latin square. □

In case of some bivariate polynomials, the resulting squares will not be Latin squares. But we can get a Latin square of lower order by deleting some rows and columns in which entries have repetitions.Obviously, number of rows and columns deleted must be equal. For example, the polynomial $5x+2y+2xy+3y^2$ over Z_6 will not form a latin square as shown below.

0	5	4	3	2	1
5	0	1	2	3	4
4	1	4	1	4	1
3	2	1	0	5	4
2	3	4	5	0	1
1	4	1	4	1	4

The third and sixth rows as well as columns contain repetitions . In these rows and columns we see only the entries 1 and 4. Deleting these two rows and columns, we get a square of order 4×4, which is a Latin square over the set $\{0,2,3,5\}$.

0	5	3	2
5	0	2	3
3	2	0	5
2	1	5	0

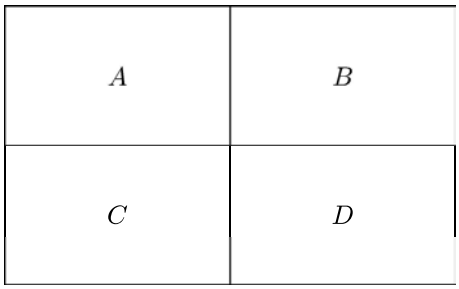
Similarly, the bivariate $P(x,y)=9x+9y+8xy$ over Z_{10} will give a 10×10 square which can be reduced to a Latin square of order 8×8 after deleting 2 rows and 2 columns, having only the entries 3 and 8.

$$P(2,y)=\begin{cases} 3 & \text{for all odd y} \\ 8 & \text{for all even y} \end{cases}$$

$$P(7,y)=\begin{cases} 8 & \text{for all odd y} \\ 3 & \text{for all even y} \end{cases}$$

Similar expressions hold for $P(x,2)$ and $P(x,7)$, because $P(x,y)$ is a symmetric polynomial. So we delete the rows and columns corresponding to both x and y equal to 2 and 7.

Rivest [6] proved that no two bivariate polynomials modulo 2^w, for $w \geq 1$ can form a pair of orthogonal Latin squares. This is because all the bivariate polynomials over Z_n, where $n = 2^w$, will form Latin squares which can be equally divided into 4 parts as shown below, where the $n/2 \times n/2$ squares A and D are identical and $n/2 \times n/2$ squares B and C are identical.



So, no two such Latin squares can be orthogonal.

But we do have examples of bivariate polynomials modulo $n \neq 2^w$, such that resulting Latin squares are orthogonal. The two bivariate quadratic polynomials $6x^2+3y^2+3xy+x+5y$ and $3x^2+6y^2+6xy+4x+7y$ give two orthogonal Latin squares over Z_9. Also, $x+4y+3xy$ is a quadratic bivariate which gives a Latin square orthogonal to Latin square formed by $6x^2 + 3y^2 + 3xy + x + 5y$ over Z_9.

0	8	4	6	5	1	3	2	7
7	0	8	4	6	5	1	3	2
8	4	6	5	1	3	2	7	0
3	2	7	0	8	4	6	5	1
1	3	2	7	0	8	4	6	5
2	7	0	8	4	6	5	1	3
6	5	1	3	2	7	0	8	4
4	6	5	1	3	2	7	0	8
5	1	3	2	7	0	8	4	6

Latin square formed by
$6x^2 + 3y^2 + 3xy + x + 5y$

0	4	2	3	7	5	6	1	8
7	8	3	1	2	6	4	5	0
2	0	1	5	3	4	8	6	7
3	7	5	6	1	8	0	4	2
1	2	6	4	5	0	7	8	3
5	3	4	8	6	7	2	0	1
6	1	8	0	4	2	3	7	5
4	5	0	7	8	3	1	2	6
8	6	7	2	0	1	5	3	4

Latin square formed by
$3x^2 + 6y^2 + 6xy + 4x + 7y$

We have found many examples in which the rows or columns of the Latin square formed by quadratic bivariates over Z_n are cyclic shifts of a single permutation of $\{0, 1, 2, ..., n-1\}$. If two bivariates give such Latin squares, then corresponding to any one entry in one Latin square, if there are n different entries in n rows of the other Latin square, then those two Latin squares will be orthogonal. For instance, in the above example, the entries in the second square corresponding to the entry 0 in the first square are 0,8,7,6,5,4,3,2,1. The rows of the first square are all cyclic shifts of the permutation (0,8,4,6,5,1,3,2,7), not in order. Also the columns of the second square are the cyclic shifts of the permutation (0,7,2,3,1,5,6,4,8), not in order. We have listed below the number of quadratic bivariates that form Latin squares over Z_n, for $5 \leq n \leq 24$.

n	number of quadratic bivariates (with constant term = 0) forming Latin squares	n	number of quadratic bivariates (with constant term = 0) forming Latin squares
5	16	15	64
6	16	16	32,768
7	36	17	256
8	1,024	18	32,888
9	972	19	324
10	64	20	512
11	100	21	144
12	128	22	400
13	144	23	484
14	144	24	4,096

The following have been noted from the extensive computations carried out on a Personal Computer:

If we write a quadratic bivariate $P(x, y) = a_{10}x + a_{01}y + a_{11}xy + a_{20}x^2 + a_{02}y^2$, then the numbers in the above table can be explicitly given as the possible choices for the coefficients in $P(x, y)$. We can clearly observe that if $P(x, y)$ forms a Latin square then $P(y, x)$ will form the Latin square which is just a transpose of the former.

In Z_9, there are 972 quadratics with constant term zero, forming Latin squares. These polynomials have the coefficients a_{10} and a_{01} from the set $\{1, 2, 4, 5, 7, 8\}$, coefficients a_{20} and a_{02} from the set $\{0, 3, 6\}$ and the coefficient a_{11} from the set $\{0, 3, 6\}$. So,there are 6 choices for both a_{10} and a_{01}, and 3 choices for each of the coefficients a_{20}, a_{02} and a_{11}. So, the number of such polynomials is equal to $6 \times 6 \times 3 \times 3 \times 3 = 972$. Also we observe that in the case of Z_n where n is a prime or a product of distinct odd primes, the coefficients of x^2, y^2 and xy are all zero. So, in these type of rings we find the number of polynomials that yield Latin squares is k^2, where k is the number of possible coefficients of x and y. When n is a prime number, all $n - 1$ nonzero elements of Z_n occur as coefficients of both x and y. When n is a product of distinct odd primes, then all the $\varphi(n)$ nonzero elements of Z_n which are coprime with n occur as as coefficients of both x and y.

We tabulate a few cases below:

n	number of P(x,y)	set of possible values of a_{10} and a_{01}
3	$4 = 2^2$	$\{1, 2\}$
5	$16 = 4^2$	$\{1, 2, 3, 4\}$
7	$36 = 6^6$	$\{1, 2, 3, 4, 5, 6\}$
11	$100 = 10^2$	$\{1, 2, ...10\}$

n	**number of P(x,y)**	**set of possible values of a_{10} and a_{01}**
13	$144 = 12^2$	$\{1, 2, ...12\}$
15	$64 = 8^2$	$\{1, 2, 4, 7, 8, 11, 13, 14\}$
17	$256 = 16^2$	$\{1, 2, ...16\}$
19	$324 = 18^2$	$\{1, 2, ...18\}$
21	$144 = 12^2$	$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
23	$484 = 22^2$	$\{1, 2, ...22\}$

From the above table we can see that the number N of bivariate quadratic polynomials $P(x, y)$ with constant term zero which yield Latin squares is given by $N = (\varphi(n))^2$, if n is a prime or product of distinct odd primes.

§3. Conclusion

We have examined Rivest's results when $n \neq 2^w$. A computational study, though on a small scale, has revealed lot of surprises. The bivariate permutation polynomials producing Latin squares do not seem to depend on the behavior of the corresponding univariate polynomials. Several pairs of orthogonal Latin squares are obtained through Latin squares got via permutation polynomials. It would be interesting to know the relation between the coefficients of the polynomials and the relation to the Latin squares and if possible get an expression for their number in terms of the prime decomposition of n. Also, the cubic and higher degrees seem to be much more challenging and will be taken up for later study.

References

[1] G. Appa , D. Magos, I. Mourtos, An LP - based proof for the non existance of a pair of orthogonal Latin squares of order 6, *Operations Research Letters*, 32, 336-344, 2004.

[2] Lidl Rudolf , Niederreiter Harald *Finite Fields*, Cambridge University Press, Cambridge, New York, 1987.

[3] Lidl Rudolf , L. Mullen Gary, When does a polynomial over a finite field permute the elements of the field?, *American Mathematical Monthly*, 95(3):243-246, 1988.

[4] Lidl Rudolf , L. Mullen Gary When does a polynomial over a finite field permute the elements of the field? (II), *American Mathematical Monthly*, 100(1): 71-74, 1990.

[5] J.H. Lint Van , R. M. Wilson *A Course in Combinatorics*, Second Edition, Cambridge University Press, Cambridge, New York, 2001.

[6] L.Rivest Ronald. *Permutation Polynomials Modulo* 2^w, Finite Fields and Applications 7(2); 287-292, 2001.

[7] W. D. Wallis *Introduction to Combinatorial Designs*, second edition, Chapman and Hall/CRC, 1998.