Permutation Polynomials modulo p^n

Rajesh P Singh [*] Soumen Maity [†]

Abstract

A polynomial f over a finite ring R is called a *permutation polynomial* if the mapping $R \to R$ defined by f is one-to-one. In this paper we consider the problem of characterizing permutation polynomials; that is, we seek conditions on the coefficients of a polynomial which are necessary and sufficient for it to represent a permutation. We also present a new class of permutation binomials over finite field of prime order.

Keywords: Permutation polynomials, Finite rings, Combinatorial problem, Cryptography

1 Introduction

A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is said to be a permutation polynomial over a finite ring R if f permutes the elements of R. That is, f is a one-to-one map of R onto itself. A natural question to ask is: given a polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$, what are necessary and sufficient conditions on the coefficients $a_0, a_1, \ldots, a_d$ for f to be permutation? Permutation polynomials have been extensively studied; see Lidl and Niederreiter [7] Chapter 7 for a survey. Permutation polynomials have been used in Cryptography and Coding [4, 8, 10]. Most studies have assumed that R is a finite field. See, for example, the survey of Lidl and Mullen [5, 6]. It is well-known that many problems on permutation polynomials over finite fields are still open [5, 6]. Similarly there are a few work on permutation polynomials modulo integers [2]. Rivest [11] considered the case where R is the ring $(Z_m, +, \cdot)$ where m is a power of 2: $m = 2^n$. Such permutation polynomials have also been used in Cryptography recently, such as in RC6 block cipher [13], a simple permutation polynomials $f(x) = 2x^2 + x$ modulo 2^d is used, where d is the word size of the machine. In this paper, we consider the case that R is the ring $(Z_m, +, .)$ where m is a prime power: $m = p^n$ and give an exact characterization of permutation polynomials modulo p^n, for $p = 2, 3, 5$, in terms of their coefficients. Although permutation polynomials over finite fields have been a subject of study for over 140 years, only a handful of specific families of permutation polynomials of finite fields are known so far. The construction of special types of permutation polynomials becomes interesting research problem. Here we present a new class of permutation binomials over finite field of prime order.

[*]Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati 781 039, Assam, INDIA. *Email addresses*: r.pratap@iitg.ernet.in

[†]Department of Mathematics Indian Institute of Technology Kharagpur, Kharagpur, West Bengal, INDIA. *Email addresses*: sm@maths.iitkgp.ernet.in

2 Congruences to a prime-power modulus

In this section we recall some results from [2] that we need to formally present our results. Consider the congruences

$$f(x) \equiv 0 \bmod p^a \tag{1}$$

and

$$f(x) \equiv 0 \bmod p^{a-1} \tag{2}$$

where $f(x)$ is any integral polynomial, p is prime and $a > 1$. Then Theorem 123 of [2] states that

Theorem 2.1 *(Hardy & Wright [2]) The number of solutions of (1) corresponding to a solution ξ of (2) is*

(a) none, if $f'(\xi) \equiv 0$ mod p and ξ is not a solution of (1);

(b) one, if $f'(\xi) \not\equiv 0$ mod p;

(c) p, if $f'(\xi) \equiv 0$ mod p and ξ is a solution of (1).

The solutions of (1) corresponding to ξ may be derived from ξ, in case (b) by the solution of a linear congruence, in case (c) by adding any multiple of p^{a-1} to ξ.

As a consequence of this theorem we obtain the following result. If p is a prime, then Z_p denotes the finite field with p elements.

Corollary 2.1 *Let p be a prime. Then $f(x)$ permutes the elements of Z_{p^n}, $n > 1$, if and only if it permutes the elements of Z_p and $f'(a) \not\equiv 0$ mod p for every integer $a \in Z_p$.*

Proof: Suppose $f(x)$ permutes the elements of Z_{p^n}, $n > 1$. That is $f(x)$ is a one-to-one map of Z_{p^n} onto itself. Thus the congruence

$$f(x) \equiv 0 \bmod p^n \tag{3}$$

has exactly one root, say x. Then x satisfies

$$f(x) \equiv 0 \bmod p \tag{4}$$

and is of the form $\xi + sp$, $(0 \leq s < p^{n-1})$, where ξ is the root of (4) for which $0 \leq \xi < p$. Next, suppose that ξ is the root of (4) satisfying $0 \leq \xi < p$ and $f'(\xi) \not\equiv 0 \bmod p$. Then, according to Theorem 3.1, $f(x) \equiv 0 \bmod p^2$ has exactly one root corresponding to the solution ξ of (4). Repeating the argument we obtain $f(x) \equiv 0 \bmod p^n$ has exactly one root corresponding to the solution ξ of (4) for every $n > 1$.

3 Permutation polynomials modulo a prime-power

In this section we give necessary and sufficient conditions on the coefficients $a_0, a_1, \ldots, a_d$ for $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ to be permutation polynomial modulo p^n, for $p = 2, 3, 5$. A characterization of permutation polynomials modulo 2^n was given in [11]. Rivest [11] proved that $f(x)$ is a permutation polynomial if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \ldots)$ is even, and $(a_3 + a_5 + a_7 + \ldots)$ is even. We first give a very short and simple proof of the above characterization. We also give new characterization of permutation polynomials modulo p^n for $p = 3, 5$, and $n > 1$.

3.1 Characterizing permutation polynomials modulo 2^n

A simple characterization of permutation polynomial modulo 2^n, $n > 1$, is presented in this section. We need the following lemma in the proof of Theorem 3.1

Lemma 3.1 *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \ldots + a_d)$ is odd.*

Proof: Since $0^i = 0$ and $1^i = 1$ modulo 2 for $i \geq 1$, we can write $f(x) = a_0 + (a_1 + a_2 + \cdots + a_d)x \bmod 2$. Clearly $f(x)$ is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \cdots + a_d) \not\equiv 0 \bmod 2$, that is, $(a_1 + a_2 + \cdots + a_d)$ is odd.

Theorem 3.1 *(Rivest [11]) A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 2^n, $n > 1$, if and only if a_1 is odd, $(a_2 + a_4 + a_6 + \ldots)$ is even, and $(a_3 + a_5 + a_7 + \ldots)$ is even.*

Proof: The proof given here is different from that of Rivest [11] and is relevant to the proof of theorems to follow. The theorem is proved by making use of Corollary 2.1 and Lemma 3.1. By Corollary 2.1, $f(x)$ is a permutation polynomial modulo 2^n if and only if it is a permutation polynomial modulo 2 and $f'(x) \not\equiv 0 \bmod 2$ for every integer $x \in Z_2$. By Lemma 3.1, $f(x)$ is a permutation polynomial modulo 2 if and only if $(a_1 + a_2 + \ldots + a_d)$ is odd. It is easy to cheek that $f'(x) = a_1 + (a_3 + a_5 + \ldots)x \bmod 2$. The condition $f'(x) \not\equiv 0 \bmod 2$ with $x = 0$ gives a_1 is odd. The condition $f'(x) \not\equiv 0 \bmod 2$ with $x = 1$ gives $(a_1 + a_3 + a_5 + \ldots)$ is odd. Hence the theorem follows.

Example 3.1 The following are all permutation polynomials modulo 2^2 of degree atmost 3 and the coefficients are from Z_4: x, $3x$, $x + 2x^2$, $3x + 2x^2$, $x + x^3$, $3x + 2x^3$, $x + 2x + 2x^3$ and $3x + 2x^2 + 2x^3$.

3.2 Characterizing permutation polynomials modulo 3^n

This section starts with a proposition regarding permutations of Z_p that is needed later on.

Proposition 3.1 *[7] If $d > 1$ is a divisor of $p-1$, then there exists no permutation polynomial of Z_p of degree d.*

The proof of Proposition 3.1 is given in [7]. As an easy consequence of this proposition we get, if p is an odd prime, no permutation over Z_p can have degree $p - 1$.

Lemma 3.2 *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 3 if and only if $(a_1 + a_3 + \ldots) \not\equiv 0$ mod 3 and $(a_2 + a_4 + \ldots) \equiv 0$ mod 3.*

Proof: Since $x^{2k+1} = x \bmod 3$ and $x^{2k} = x^2 \bmod 3$ for $k \geq 1$, we can write $f(x) = a_0 + (a_1 + a_3 + \ldots)x + (a_2 + a_4 + \ldots)x^2 \bmod 3$. Letting $A = (a_1 + a_3 + \ldots) \bmod 3$ and $B = (a_2 + a_4 + \ldots) \bmod 3$, we can write $f(x)$ more compactly as $f(x) = a_0 + Ax + Bx^2$. Since, for odd prime p, no permutation polynomial over Z_p can have degree $p-1$, we have $B \equiv 0 \bmod 3$. Thus $f(x)$ is a permutation polynomial modulo 3 if and only if $(a_1 + a_3 + \ldots) \not\equiv 0 \bmod 3$ and $(a_2 + a_4 + \ldots) \equiv 0 \bmod 3$.

Theorem 3.2 *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 3^n, $n > 1$, if and only if*

(a) $a_1 \not\equiv 0$ *mod* 3,

(b) $(a_1 + a_3 + \ldots) \not\equiv 0$ *mod* 3,

(c) $(a_2 + a_4 + \ldots) \equiv 0$ *mod* 3,

(d) $(a_1 + a_4 + a_7 + a_{10} + \ldots) + 2(a_2 + a_5 + a_8 + a_{11} + \ldots) \not\equiv 0$ *mod* 3, *and*

(e) $(a_1 + a_2 + a_7 + a_8 + \ldots) + 2(a_4 + a_5 + a_{10} + a_{11} + \ldots) \not\equiv 0$ *mod* 3.

Proof: By Corollary 2.1, $f(x)$ is a permutation polynomial modulo 3^n if and only if it is a permutation polynomial modulo 3 and $f'(x) \not\equiv 0 \bmod 3$ for every integer $x \in Z_3$. It is easy to verify that $f'(x) = a_1 + (2a_2 + a_4 + 2a_8 + a_{10} + 2a_{14} + a_{16} + \ldots)x + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots)x^2 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 0$ gives $a_1 \not\equiv 0 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 1$ gives $a_1 + (2a_2 + a_4 + 2a_8 + a_{10} + 2a_{14} + a_{16} + \ldots) + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots) \not\equiv 0 \bmod 3$. The condition $f'(x) \not\equiv 0 \bmod 3$ with $x = 2$ gives $a_1 + (a_2 + 2a_4 + a_8 + 2a_{10} + a_{14} + 2a_{16} + \ldots) + (2a_5 + a_7 + 2a_{11} + a_{13} + 2a_{17} + a_{19} + \ldots) \not\equiv 0 \bmod 3$. Now the theorem directly follows by combining above conditions and Lemma 3.2.

Example 3.2 *The following are some permutation polynomials modulo 9 of degree 5 and the coefficients are from Z_9: $7x + x^3 + 8x^5$, $x + x^2 + 8x^3 + 8x^4 + 7x^5$, $7x + 6x^2 + 8x^3 + 8x^5$ and $x + 7x^2 + 8x^3 + 8x^4 + 7x^5$. There are total 3888 permutation polynomials modulo 9 of degree atmost 5 and the coefficients are from Z_9.*

3.3 Characterizing permutation polynomials modulo 5^n

Let p be a prime and $\mathbf{F}_p = GF(p)$ be the Galois field of p elements. The following result is from [9].

Theorem 3.3 *(Mollin & Small [9]) Let $GF(p)$ have characteristic different from 3. Then $f(x) = ax^3 + bx^2 + cx + d$ $(a \neq 0)$ permutes $GF(p)$ if and only if $b^2 = 3ac$ and $p \equiv 2$ mod 3.*

We need the following lemma in the proof of Theorem 3.4.

Lemma 3.3 *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 5 if and only if $(a_4 + a_8 + a_{12} \dots) \equiv 0$ mod 5 and $(a_2 + a_6 + a_{10} + \dots)^2 \equiv 3(a_1 + a_5 + a_9 + \dots)(a_3 + a_7 + a_{11} + \dots)$ mod 5.*

Proof: Since $x^{4k+1} = x$ mod 5, $x^{4k+2} = x^2$ mod 5, $x^{4k+3} = x^3$ mod 5, and $x^{4k} = x^4$ mod 5 for $k \geq 1$, we can write $f(x) = a_0 + (a_1 + a_5 + \dots)x + (a_2 + a_6 + \dots)x^2 + (a_3 + a_7 + \dots)x^3 + (a_4 + a_8 + \dots)x^4$ mod 5. Letting $A = (a_1 + a_5 + \dots)$, $B = (a_2 + a_6 + \dots)$, $C = (a_3 + a_7 + \dots)$ and $D = (a_4 + a_8 + \dots)$ we can write $f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4$ mod 5. Since no polynomial of degree 4 can be a permutation polynomial modulo 5, we have $D \equiv 0$ mod 5. Now $f(x) = a_0 + Ax + Bx^2 + Cx^3$ mod 5 and we are in the situation of Theorem 3.3. Hence, f is a permutation if and only if $B^2 = 3AC$.

Example 3.3 *The permutation binomials modulo 5 of degree atmost 3 are: x, x^3, $2x+x^2+x^3$, $3x + 2x^2 + x^3$, $3x + 3x^2 + x^3$, and $2x + 4x^2 + x^3$.*

Theorem 3.4 *A polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 5^n if and only if*

(a) $a_1 \not\equiv 0$ *mod* 5,

(b) $(a_4 + a_8 + a_{12} \dots) \equiv 0$ *mod* 5,

(c) $(a_2 + a_6 + a_{10} + \dots)^2 \equiv 3(a_1 + a_5 + a_9 + \dots)(a_3 + a_7 + a_{11} + \dots)$ *mod* 5,

(d) $(a_1+a_6+a_{11}+\dots)+2(a_2+a_7+a_{12}+\dots)+3(a_3+a_8+a_{13}+\dots)+4(a_4+a_9+a_{14}+\dots) \not\equiv 0$ *mod* 5,

(e) $(a_1 + 2a_6 + 4a_{11} + 3a_{16} + a_{21} + \dots) + 2(2a_2 + 4a_7 + 3a_{12} + a_{17} + 2a_{22} + \dots) + 3(4a_3 + 3a_8 + a_{13} + 2a_{18} + 4a_{23} + \dots) + 4(3a_4 + a_9 + 2a_{14} + 4a_{19} + 3a_{24} + \dots) \not\equiv 0$ *mod* 5,

(f) $(a_1 + 3a_6 + 4a_{11} + 2a_{16} + a_{21} + \dots) + 2(3a_2 + 4a_7 + 2a_{12} + a_{17} + 3a_{22} + \dots) + 3(4a_3 + 2a_8 + a_{13} + 3a_{18} + 4a_{23} + \dots) + 4(2a_4 + a_9 + 3a_{14} + 4a_{19} + 2a_{24} + \dots) \not\equiv 0$ *mod* 5, *and*

(g) $(a_1 + 4a_6 + a_{11} + 4a_{16} + a_{21} + \dots) + 2(4a_2 + a_7 + 4a_{12} + a_{17} + 4a_{22} + \dots) + 3(a_3 + 4a_8 + a_{13} + 4a_{18} + a_{23} + \dots) + 4(4a_4 + a_9 + 4a_{14} + a_{19} + 4a_{24} + \dots) \not\equiv 0$ *mod* 5.

Proof: By Corollary 2.1, $f(x)$ is a permutation polynomial modulo 5^n if and only if it is a permutation polynomial modulo 5 and $f'(x) \not\equiv 0 \bmod 5$ for every integer $x \in Z_5$. We obtain

$$\begin{aligned}
f'(x) &= a_1 + \sum_k (4k+2)a_{4k+2}x + \sum_k (4k+3)a_{4k+3}x^2 + \sum_k (4k)a_{4k}x^3 \\
&\quad + \sum_k (4k+1)a_{4k+1}x^4 \\
&\equiv a_1 + (2a_2 + a_6 + 4a_{14} + 3a_{18} + 2a_{22} + \ldots)x \\
&\quad + (3a_3 + 2a_7 + a_{11} + 4a_{19} + 3a_{23} + \ldots)x^2 \\
&\quad + (4a_4 + 3a_8 + 2a_{12} + a_{16} + 4a_{24} + \ldots)x^3 \\
&\quad + (4a_9 + 3a_{13} + 2a_{17} + a_{21} + 4a_{29} + \ldots)x^4 \bmod 5
\end{aligned}$$

Observe that $f'(0) \not\equiv 0 \bmod 5$ means $a_1 \not\equiv 0 \bmod 5$;
$f'(1) \not\equiv 0 \bmod 5$ means $(a_1 + a_6 + a_{11} + \ldots) + 2(a_2 + a_7 + a_{12} + \ldots) + 3(a_3 + a_8 + a_{13} + \ldots) + 4(a_4 + a_9 + a_{14} + \ldots) \not\equiv 0 \bmod 5$;
$f'(2) \not\equiv 0 \bmod 5$ means $(a_1 + 2a_6 + 4a_{11} + 3a_{16} + a_{21} + \ldots) + 2(2a_2 + 4a_7 + 3a_{12} + a_{17} + 2a_{22} + \ldots) + 3(4a_3 + 3a_8 + a_{13} + 2a_{18} + 4a_{23} + \ldots) + 4(3a_4 + a_9 + 2a_{14} + 4a_{19} + 3a_{24} + \ldots) \not\equiv 0 \bmod 5$;
$f'(3) \not\equiv 0 \bmod 5$ means $(a_1 + 3a_6 + 4a_{11} + 2a_{16} + a_{21} + \ldots) + 2(3a_2 + 4a_7 + 2a_{12} + a_{17} + 3a_{22} + \ldots) + 3(4a_3 + 2a_8 + a_{13} + 3a_{18} + 4a_{23} + \ldots) + 4(2a_4 + a_9 + 3a_{14} + 4a_{19} + 2a_{24} + \ldots) \not\equiv 0 \bmod 5$; and
$f'(4) \not\equiv 0 \bmod 5$ means $(a_1 + 4a_6 + a_{11} + 4a_{16} + a_{21} + \ldots) + 2(4a_2 + a_7 + 4a_{12} + a_{17} + 4a_{22} + \ldots) + 3(a_3 + 4a_8 + a_{13} + 4a_{18} + a_{23} + \ldots) + 4(4a_4 + a_9 + 4a_{14} + a_{19} + 4a_{24} + \ldots) \not\equiv 0 \bmod 5$. Now the theorem directly follows by combining above conditions and Lemma 3.3. However the situation becomes complicated for $p = 7, 11, 13, \ldots$ Thus, in the following section we consider the problem of characterizing only permutation binomials modulo prime p.

4 A new class of permutation binomials over finite field F_p

Let p be a prime and $\mathbf{F}_p = GF(p)$ be the Galois field of p elements. In [5], the open problem P2 states: Find new classes of permutation polynomials of $\mathbf{F}_q$, $q = p^n$, n is a positive integer. Recently some classes of permutation binomials are presented in [1, 3]. Here we present a new class of permutation binomials of $\mathbf{F}_p$. We now recall the definition and some properties of quadratic residue.

Definition 4.1 Suppose p is an odd prime and a is an integer. a is defined to be a *quadratic residue* modulo p if $a \not\equiv 0 \pmod p$ and the congruence $y^2 \equiv a \pmod p$ has a solution $y \in \mathbf{F}_p$. a is defined to be a *quadratic non-residue* modulo p if $a \not\equiv 0 \pmod p$ and a is not a quadratic residue modulo p.

Euler's Criteria states that a is a quadratic residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ and a is a quadratic non-residue modulo p if and only if $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Theorem 4.1 *Let p be a prime and $f(x) = x^u(x^{\frac{p-1}{2}} + a)$ where u is an integer such that $(u, p-1) = 1$ and a is a non-zero element in $\boldsymbol{F}_p$. Then $f(x)$ is a permutation binomial over $\boldsymbol{F}_p$ if and only if $(a^2 - 1)^{\frac{p-1}{2}} = 1 \bmod p$.*

Proof: It is known that the monomial x^u is a permutation polynomial of $\mathbf{F}_p$ if and only if $\gcd(u, p-1) = 1$. Using Euler's criteria we can rewrite

$$f(x) = \begin{cases} 0, & \text{if } x = 0; \\ x^u(a+1), & \text{if } x \text{ is quadratic residue;} \\ x^u(a-1), & \text{if } x \text{ is quadratic non-residue.} \end{cases}$$

There are $\frac{1}{2}(p-1)$ residues and $\frac{1}{2}(p-1)$ non-residues of an odd prime p. The product of two residues, or of two non-residues, is a residue, while the product of a residue and a non-residue is a non-residue. Since u is odd, x^u is residue (resp. non-residue) if x is residue (resp. non-residue). If both $a+1$ and $a-1$ are residues, then $f(x)$ maps residues to residues and non-residues to non-residues and if both $a+1$ and $a-1$ are non-residues, then $f(x)$ maps residues to non-residues and non-residues to residues. On the other hand, if $a+1$ is residue and $a-1$ is non-residue then $f(x)$ maps all the non-zero elements to residues and if $a+1$ is non-residue and $a-1$ is residue then $f(x)$ maps all the non-zero elements to non-residues. Since x^u is a permutation polynomial, therefore $f(x)$ is a permutation polynomial if and only if both $a+1$ and $a-1$ are either quadratic residues or quadratic non residues. In other words, $f(x)$ is a permutation polynomial over $\mathbf{F}_p$ if and only if $(a^2-1)^{\frac{p-1}{2}} = 1 \bmod p$. In Theorem 4.1, if the degree $u + \frac{p-1}{2}$ of binomial $f(x)$ is greater than $p-1$ for some values of u then the polynomial is reduced modulo $x^p - x$. In the following, as an application of Theorem 4.1, we give some examples of permutation binomials of $\mathbf{F}_p$.

Example 4.1 *Let $p = 7$. Then $u = 1, 5$. Thus $x(x^3+a)$ and $x^5(x^3+a)$ mod $x^7 - x$ are permutation binomials over $\boldsymbol{F}_7$ if and only if $(a^2-1)^3 \equiv 1$ mod 7. That is, $x(x^3+a)$ and $x^5(x^3+a)$ are permutation binomials over $\boldsymbol{F}_7$ for $a = 3, 4$. We can write $x^5(x^3+a) \equiv x^2 + ax^5 \equiv ax^2(x^3 + a^{-1})$ mod $x^7 - x$. Hence the permutation binomials over $\boldsymbol{F}_7$ are $x(x^3+3)$, $x(x^3+4)$, $x^2(x^3+2)$, and $x^2(x^3+5)$.*

Example 4.2 *Let $p = 11$. Then $x^u(x^5+a)$ is a permutation binomial of $\boldsymbol{F}_{11}$ for $u = 1, 3, 7, 9$ and $a = 2, 4, 7, 9$. Therefore $x(x^5+2)$, $x(x^5+4)$, $x(x^5+7)$, $x(x^5+9)$, $x^3(x^5+2)$, $x^3(x^5+4)$, $x^3(x^5+7)$, $x^3(x^5+9)$, $x^2(x^5+3)$, $x^2(x^5+5)$, $x^2(x^5+6)$, $x^2(x^5+8)$, $x^4(x^5+3)$, $x^4(x^5+5)$, $x^4(x^5+6)$, $x^4(x^5+8)$ are permutation binomials of $\boldsymbol{F}_{11}$.*

References

[1] A. Akbary and Q. Wang. A generalized Lucas sequence and permutation binomials. *Proceeding of the American Mathematical Socity*, 134(1), 15-22, 2005.

[2] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*, Oxford Science Publications, 5th ed., 1979.

[3] L. Wang. On permutation polynomials. *Finite Fields and Their Applications*, 8, 311-322, 2002.

[4] R. Lidl, On cryptosystems based on permutation polynomials and finite fields, In *Advance in Cryptology-EuroCrypt 1984*, Lecture Notes in Computer Science, Vol. 209, 10-15, 1985.

[5] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? *The American Math. Monthly*, 95(3), 243-246, 1988.

[6] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? II *The American Math. Monthly*, 100(1), 71-74, 1993.

[7] R. Lidl and H. Niederreiter. *Finite Fields.* Addision-Wesley, 1983.

[8] R. Lidl and W. B. Muller. Permutation polynomials in RSA-ctyptosystems. In *Proc. CRYPTO 83,* 293-301, 1948, New York, Plenum Press.

[9] R. A. Mollin and C. Small. On permutation polynomials over finite fields. *Internat. J. Math. & Math. Sci.*, 10 (3), 1987, 535-544.

[10] Gary L. Mullen, Permutation polynomials and nonsingular feedback shift registers over finite fields. *IEEE Trans. Information Theory*, 35 (4), 1989, 900-902.

[11] R. L. Rivest, Permutation polynomials modulo 2^w. *Finite Fields and Their Applications*, 7, 287-292, 2001.

[12] R. L. Rivest, Adi Shamir, and L. M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM,* 21(2), 120-126, 1978.

[13] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y.L. Yin, The RC6 block cipher. See http://theory.lcs.mit.edu/ rivest/rc6.pdf or http://csrc.nist.gov/encryption/aes/.