Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 6, pp. 1743–1751
DOI : 10.47974/JDMSC-1671

On permutation polynomials modulo 7^n

P. L. Sharma *
Sushil Kumar
Department of Mathematics & Statistics
H. P. University
Shimla
Himachal Pradesh
India

Ashima
Department of Mathematics
Hansraj College
University of Delhi
Delhi
India

Neetu Dhiman
Department of Applied Sciences & Humanities
University Institute of Technology
H. P. University
Shimla
Himachal Pradesh
India

Abstract

A polynomial that permutes the elements of a finite ring R is known as a permutation polynomial. The conditions for the coefficients of a polynomial of degree d to be a permutation polynomial modulo p^n, are known for $p = 2, 3, 5$. In this paper, we obtain the necessary and sufficient conditions on the coefficients of a polynomial modulo 7^n to be a permutation polynomial.

Subject Classification: *12E05, 12E10, 12E20.*

Keywords: *Finite rings, Permutation polynomials, Residue classes, Congruences.*

* *E-mail:* plsharma1964@gmail.com

© Taru Publications

1. Introduction

Let R be a finite ring. A polynomial $f(x) \in R[x]$ is called a permutation polynomial if the associated polynomial function $f : c \to f(c)$ from R to R is a permutation of R. Permutation polynomials have been extensively explored, see [7] and used in different areas of mathematics, cryptography, combinatorics and coding theory, see [3, 6, 8-10, 19]. R is considered to be a finite field in most research, see the survey of Lidl and Mullen [4, 5]. Permutation polynomials over finite fields have been studied for over 140 years but only a few particular families of permutation polynomials of finite fields are known so far. In the last few decades, most of the research has been devoted to the construction of irreducible polynomials and permutation polynomials, see [12-16]. Dickson [1] has given all permutation polynomials up to degree 5 over an arbitrary finite field and all permutation polynomials of degree 6 over finite fields of an odd characteristic. Similarly, there is some work on permutation polynomials modulo integers, discussed in [2].

Now, there arises a question that what are the necessary and sufficient conditions on the coefficients of a polynomial $f(x)$ to be permutation? Several authors have worked to find the conditions on the coefficients of a polynomial. Rivest [11] have obtained the conditions for the coefficients of a polynomial to be a permutation polynomial when R is the ring $(Z_m, +, .)$ for $m = 2^w$. He proved that $f(x)$ is a permutation polynomial if and only if a_1 is odd, $(a_2 + a_4 + a_6 + ...)$ and $(a_3 + a_5 + a_7 + ...)$ are even. Singh and Maity [16] discussed a very simple and short proof of the characterization given by Rivest [11] and also introduced a new characterization of permutation polynomials modulo p^n for $p = 3, 5$. In the present paper, we obtain the necessary and sufficient conditions on the coefficients of a polynomial to be a permutation over modulo 7^n.

2. Preliminaries

In this section, we present some preliminary results which will be useful in the upcoming section.

Theorem 2.1 ([16], 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* $f'(x) \not\equiv 0 \bmod p$ *for every integer* $x \in Z_p$.

Theorem 2.2 ([18], Theorem 7) *A polynomial* $f(x) = a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5, a_5 \not\equiv 0 \bmod 7$ *is permutation polynomial iff*

(1) $4a_2(a_5)^2 = 2(a_4)^3 \ mod\ 7$ and $6a_1(a_5)^3 = (a_4)^4 \ mod\ 7$, when $5a_3a_5 = 2(a_4)^2 \ mod\ 7$, or iff

(2) $4a_2(a_5)^2 = 2(a_4)^3 + \alpha a_4(a_5)^2 \ mod\ 7$ and $6a_1(a_5)^3 = (a_4)^4 + \alpha(a_4)^2(a_5)^2 + 4\alpha^2(a_5)^4 \ mod\ 7$, where $\alpha = (a_3a_5 + (a_4)^2)((a_5)^2)^{(-1)} \ mod\ 7$ when $5a_3a_5 \neq 2(a_4)^2 \ mod\ 7$.

Theorem 2.3 ([17], Theorem 3.7) *A polynomial* $f(x) = a_1x + a_2x^2 + a_3x^3 + a_4x^4, a_4 \not\equiv 0 \ mod\ 7$ *is permutation polynomial iff* $3(a_3)^2 = a_2a_4 \ mod\ 7$ *and* $2a_1(a_4)^2 = (a_3)^3 + (a_4)^3 \ mod\ 7$.

3. Main Results

We obtain necessary and sufficient conditions for the coefficients $a_0, a_1, ..., a_d$ of $f(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$; $d \in \mathbb{N}$, to be a permutation polynomial modulo 7.

Lemma 3.1 : *A polynomial* $f(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d; d \geq 1$ *and* $\sum_{k\in\mathbb{N}} a_{6k-1} \not\equiv 0 \ mod\ 7$ *with integer coefficients is a permutation polynomial modulo 7 iff*

(a) $4(\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^3 \ mod\ 7$ and $6(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-1})^3 = (\sum_{k\in\mathbb{N}} a_{6k-2})^4 \ mod\ 7$, for $5(\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^2 \ mod\ 7$ or iff

(b) $4(\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^3 + \alpha(\sum_{k\in\mathbb{N}} a_{6k-2})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 \ mod\ 7$ and $6(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-1})^3 = (\sum_{k\in\mathbb{N}} a_{6k-2})^4 + \alpha(\sum_{k\in\mathbb{N}} a_{6k-2})^2(\sum_{k\in\mathbb{N}} a_{6k-1})^2 + 4\alpha^2(\sum_{k\in\mathbb{N}} a_{6k-1})^4 \ mod\ 7$, where $\alpha = ((\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) + (\sum_{k\in\mathbb{N}} a_{6k-2})^2)((\sum_{k\in\mathbb{N}} a_{6k-1})^2)^{(-1)} \ mod\ 7$, for $5(\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) \neq 2(\sum_{k\in\mathbb{N}} a_{6k-2})^2 \ mod\ 7$.

Proof: Since, $x^{(6k+1)} = x \ mod\ 7$, $x^{(6k+2)} = x^2 \ mod\ 7$, $x^{(6k+3)} = x^3 \ mod\ 7$, $x^{(6k+4)} = x^4 \ mod\ 7$, $x^{(6k+5)} = x^5 \ mod\ 7$, and $x^{(6k+6)} = x^6 \ mod\ 7$ for $k \geq 1$.

So, we have

$$f(x) = a_0 + (\sum_{k\in\mathbb{N}} a_{6k-5})x + (\sum_{k\in\mathbb{N}} a_{6k-4})x^2 + (\sum_{k\in\mathbb{N}} a_{6k-3})x^3 + (\sum_{k\in\mathbb{N}} a_{6k-2})x^4 + (\sum_{k\in\mathbb{N}} a_{6k-1})x^5 + (\sum_{k\in\mathbb{N}} a_{6k})x^6 \ mod\ 7.$$

Consider

$$A = \sum_{k\in\mathbb{N}} a_{6k-5}, B = \sum_{k\in\mathbb{N}} a_{6k-4}, C = \sum_{k\in\mathbb{N}} a_{6k-3}, D = \sum_{k\in\mathbb{N}} a_{6k-2},$$
$$E = \sum_{k\in\mathbb{N}} a_{6k-1} \text{ and } F = \sum_{k\in\mathbb{N}} a_{6k}.$$

$$f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 \ mod\ 7.$$

Since, no polynomial of degree 6 can be a permutation polynomial modulo 7, so

$$F \equiv 0 \ mod\ 7.$$

Hence,

$$f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 \ mod\ 7. \tag{3.1}$$

Now, using Theorem 2.2 in (3.1), we obtain the required result.

In the following example, we give some permutation polynomials modulo 7 upto degree 16 by using Lemma 3.1.

Example 3.2 : $x^5 + x^4 + 6x^3 + 4x^2 + 6x, 5x^5 + 2x^4 + 2x^3 + x^2 + 2x, x^5 + 4x^4 + 5x^3 + 4x^2 + 3x, 3x^5 + 5x^4 + 6x^3 + 3x^2 + 3x, x^{11} + 2x^{10} + 3x^8 + x^7 + 2x^5 + 3x^4 + x^3 + 2x^2 + x, 2x^{11} + 4x^{10} + 4x^8 + 5x^7 + 2x^4 + 3x^3 + 2x^2 + x, 2x^{16} + x^{14} + x^{13} + 2x^{11} + 2x^{10} + x^9 + 2x^8 + x^5 + x^4 + 2x^2 + x.$

Further, we give the conditions on coefficients of polynomial to be permutation polynomial modulo 7^n for $\sum_{k\in\mathbb{N}} a_{6k-1} \not\equiv 0 \ mod\ 7$.

Theorem 3.3 : *A polynomial* $f(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d; d \in \mathbb{N}$ *and* $\sum_{k\in\mathbb{N}} a_{6k-1} \not\equiv 0 \ mod\ 7$ *with integer coefficients is a permutation polynomial modulo* 7^n *if and only if*

(a) $4(\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^3 \ mod\ 7$
and $6(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-1})^3 = (\sum_{k\in\mathbb{N}} a_{6k-2})^4 \ mod\ 7,$
for $5(\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^2 \ mod\ 7$
or iff

(b) $4(\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 = 2(\sum_{k\in\mathbb{N}} a_{6k-2})^3 + \alpha(\sum_{k\in\mathbb{N}} a_{6k-2})(\sum_{k\in\mathbb{N}} a_{6k-1})^2 \ mod\ 7$
and $6(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-1})^3 = (\sum_{k\in\mathbb{N}} a_{6k-2})^4 + \alpha(\sum_{k\in\mathbb{N}} a_{6k-2})^2(\sum_{k\in\mathbb{N}} a_{6k-1})^2$
$+ 4\alpha^2(\sum_{k\in\mathbb{N}} a_{6k-1})^4 \ mod\ 7,$
where $\alpha = ((\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) + (\sum_{k\in\mathbb{N}} a_{6k-2})^2)((\sum_{k\in\mathbb{N}} a_{6k-1})^2)^{(-1)} \ mod\ 7,$
for $5(\sum_{k\in\mathbb{N}} a_{6k-3})(\sum_{k\in\mathbb{N}} a_{6k-1}) \neq 2(\sum_{k\in\mathbb{N}} a_{6k-2})^2 \ mod\ 7.$

(c) $a_1 \not\equiv 0 \ mod\ 7$,

(d) $(\sum_{k\in\mathbb{N}}\alpha^{k-1}a_{7k-6})+2(\sum_{k\in\mathbb{N}}\alpha^{k}a_{7k-5})+3(\sum_{k\in\mathbb{N}}\alpha^{k+1}a_{7k-4})+4(\sum_{k\in\mathbb{N}}\alpha^{k+2}a_{7k-3})$
$+5(\sum_{k\in\mathbb{N}}\alpha^{k+3}a_{7k-2})+6(\sum_{k\in\mathbb{N}}\alpha^{k+4}a_{7k-1})\not\equiv 0 \ mod\ 7$, where $\alpha = 1,2,3,4,5,6$.

Proof: It follow from the Theorem 2.1 that $f(x)$ is a permutation polynomial modulo 7^n if and only if it is a permutation modulo 7 and $f'(x)\not\equiv 0 \ mod\ 7$ for every integer $x \in Z_7$. Using Lemma 3.1, the conditions (a) and (b) are obviously true.

Further,

$$f'(x) = a_1 + \sum_{k\in\mathbb{N}}(6k-4)a_{(6k-4)}x + \sum_{k\in\mathbb{N}}(6k-3)a_{(6k-3)}x^2 + \sum_{k\in\mathbb{N}}(6k-2)a_{(6k-2)}x^3$$
$$+\sum_{k\in\mathbb{N}}(6k-1)a_{(6k-1)}x^4 + \sum_{k\in\mathbb{N}}(6k)a_{6k}x^5 + \sum_{k\in\mathbb{N}}(6k+1)a_{(6k+1)}x^6$$

$$\equiv a_1 + (2a_2 + a_8 + 6a_{20} + 5a_{26} + 4a_{32} + 3a_{38} + 2a_{44} + ...)x + (3a_3 + 2a_9 + a_{15} + 6a_{27}$$
$$+5a_{33} + 4a_{39} + 3a_{45} + ...)x^2 + (4a_4 + 3a_{10} + 2a_{16} + a_{22} + 6a_{34} + 5a_{40} + 4a_{46} + ...)x^3$$
$$+(5a_5 + 4a_{11} + 3a_{17} + 2a_{23} + a_{29} + 6a_{41} + 5a_{47} + ...)x^4 + (6a_6 + 5a_{12} + 4a_{18} + 3a_{24}$$
$$+2a_{30} + a_{36} + 6a_{48} + ...)x^5 + (6a_{13} + 5a_{19} + 4a_{25} + 3a_{31} + 2a_{37} + a_{43} + ...)x^6 \ mod\ 7.$$

Therefore, $f'(0)\not\equiv 0 \ mod\ 7$, that is, $a_1 \not\equiv 0 \ mod\ 7$.

Now, the congruence $f'(1)\not\equiv 0 \ mod\ 7$ gives

$$(\sum_{k\in\mathbb{N}}a_{7k-6})+2(\sum_{k\in\mathbb{N}}a_{7k-5})+3(\sum_{k\in\mathbb{N}}a_{7k-4})+4(\sum_{k\in\mathbb{N}}a_{7k-3})+5(\sum_{k\in\mathbb{N}}a_{7k-2})$$
$$+\ 6(\sum_{k\in\mathbb{N}}a_{7k-1})\not\equiv 0 \ mod\ 7,$$

For, $f'(2)\not\equiv 0 \ mod\ 7$ we have,

$$(\sum_{k\in\mathbb{N}}2^{k-1}a_{7k-6})+2(\sum_{k\in\mathbb{N}}2^{k}a_{7k-5})+3(\sum_{k\in\mathbb{N}}2^{k+1}a_{7k-4})+4(\sum_{k\in\mathbb{N}}2^{k+2}a_{7k-3})$$
$$+5(\sum_{k\in\mathbb{N}}2^{k+3}a_{7k-2})+6(\sum_{k\in\mathbb{N}}2^{k+4}a_{7k-1})\not\equiv 0 \ mod\ 7,$$

Now, $f'(3)\not\equiv 0 \ mod\ 7$ implies that,

$$(\sum_{k\in\mathbb{N}}3^{k-1}a_{7k-6})+2(\sum_{k\in\mathbb{N}}3^{k}a_{7k-5})+3(\sum_{k\in\mathbb{N}}3^{k+1}a_{7k-4})+4(\sum_{k\in\mathbb{N}}3^{k+2}a_{7k-3})$$
$$+5(\sum_{k\in\mathbb{N}}3^{k+3}a_{7k-2})+6(\sum_{k\in\mathbb{N}}3^{k+4}a_{7k-1})\not\equiv 0 \ mod\ 7,$$

For, $f'(4)\not\equiv 0 \ mod\ 7$ we have,

$$(\sum_{k\in\mathbb{N}}4^{k-1}a_{7k-6})+2(\sum_{k\in\mathbb{N}}4^{k}a_{7k-5})+3(\sum_{k\in\mathbb{N}}4^{k+1}a_{7k-4})+4(\sum_{k\in\mathbb{N}}4^{k+2}a_{7k-3})$$
$$+5(\sum_{k\in\mathbb{N}}4^{k+3}a_{7k-2})+6(\sum_{k\in\mathbb{N}}4^{k+4}a_{7k-1})\not\equiv 0 \ mod\ 7,$$

Now, $f'(5) \not\equiv 0 \ mod\ 7$ implies that

$$(\sum_{k\in\mathbb{N}} 5^{k-1} a_{7k-6}) + 2(\sum_{k\in\mathbb{N}} 5^{k} a_{7k-5}) + 3(\sum_{k\in\mathbb{N}} 5^{k+1} a_{7k-4}) + 4(\sum_{k\in\mathbb{N}} 5^{k+2} a_{7k-3}) + 5(\sum_{k\in\mathbb{N}} 5^{k+3} a_{7k-2}) + 6(\sum_{k\in\mathbb{N}} 5^{k+4} a_{7k-1}) \not\equiv 0 \ mod\ 7,$$

For, $f'(6) \not\equiv 0 \ mod\ 7$ we have,

$$(\sum_{k\in\mathbb{N}} 6^{k-1} a_{7k-6}) + 2(\sum_{k\in\mathbb{N}} 6^{k} a_{7k-5}) + 3(\sum_{k\in\mathbb{N}} 6^{k+1} a_{7k-4}) + 4(\sum_{k\in\mathbb{N}} 6^{k+2} a_{7k-3}) + 5(\sum_{k\in\mathbb{N}} 6^{k+3} a_{7k-2}) + 6(\sum_{k\in\mathbb{N}} 6^{k+4} a_{7k-1}) \not\equiv 0 \ mod\ 7.$$

This completes the proof.

Lemma 3.4 : *A polynomial* $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d ; d \in \mathbb{N}$, $\sum_{k\in\mathbb{N}} a_{6k-1} \equiv 0 \ mod\ 7$ *and* $\sum_{k\in\mathbb{N}} a_{6k-2} \not\equiv 0 \ mod\ 7$ *with integer coefficients is a permutation polynomial modulo 7 iff*

$$3(\sum_{k\in\mathbb{N}} a_{6k-3})^2 = (\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-2}) \ mod\ 7$$

and $2(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-2})^2 = (\sum_{k\in\mathbb{N}} a_{6k-3})^3 + (\sum_{k\in\mathbb{N}} a_{6k-2})^3 \ mod\ 7.$

Proof: As we know that $x^{(6k+1)} = x \ mod\ 7$, $x^{(6k+2)} = x^2 \ mod\ 7$, $x^{(6k+3)} = x^3 \ mod\ 7$, $x^{(6k+4)} = x^4 \ mod\ 7$, $x^{(6k+5)} = x^5 \ mod\ 7$, and $x^{(6k+6)} = x^6 \ mod\ 7$ for $k \geq 1$.

So, we have

$$f(x) = a_0 + (\sum_{k\in\mathbb{N}} a_{6k-5})x + (\sum_{k\in\mathbb{N}} a_{6k-4})x^2 + (\sum_{k\in\mathbb{N}} a_{6k-3})x^3 + (\sum_{k\in\mathbb{N}} a_{6k-2})x^4 + (\sum_{k\in\mathbb{N}} a_{6k-1})x^5 + (\sum_{k\in\mathbb{N}} a_{6k})x^6 \ mod\ 7.$$

Consider

$$A = \sum_{k\in\mathbb{N}} a_{6k-5}, B = \sum_{k\in\mathbb{N}} a_{6k-4}, C = \sum_{k\in\mathbb{N}} a_{6k-3}, D = \sum_{k\in\mathbb{N}} a_{6k-2}, E = \sum_{k\in\mathbb{N}} a_{6k-1} \text{ and } F = \sum_{k\in\mathbb{N}} a_{6k}.$$

It follows that

$$f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4 + Ex^5 + Fx^6 \ mod\ 7.$$

As we know, there is no permutation polynomial of degree 6 modulo 7, so we have

$$F \equiv 0 \ mod\ 7$$

and

$$E \equiv 0 \ mod\ 7.$$

Hence,

$$f(x) = a_0 + Ax + Bx^2 + Cx^3 + Dx^4 \ mod\ 7.$$

Therefore, using Theorem 2.3 in above equation, we obtain the required result.

In the following example, we give some permutation polynomials modulo 7 upto degree 10 by using Lemma 3.4.

Example 3.5 : $x^4 + x^3 + 3x^2 + x, 2x^4 + 2x^3 + 6x^2 + 2x, 6x^4 + 4x^3 + x^2, x^8 + x^4 + x^3 + 2x^2 + x, 3x^8 + 5x^4 + 3x^3 + x^2 + 5x, x^{10} + x^8 + x^4 + 2x^3 + 2x^2 + 2x, 3x^{10} + 3x^4 + 4x^3 + x^2.$

Further, we give the conditions on coefficients of polynomial to be permutation polynomial modulo 7^n for $\sum_{k\in\mathbb{N}} a_{6k-1} \equiv 0\ mod\ 7$ and $\sum_{k\in\mathbb{N}} a_{6k-2} \not\equiv 0\ mod\ 7$.

Theorem 3.6 : *A polynomial* $f(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d; d \in \mathbb{N}$, $\sum_{k\in\mathbb{N}} a_{6k-1} \equiv 0\ mod\ 7$ *and* $\sum_{k\in\mathbb{N}} a_{6k-2} \not\equiv 0\ mod\ 7$ *with integer coefficients is a permutation polynomial modulo* 7^n *if and only if*

(a) $3(\sum_{k\in\mathbb{N}} a_{6k-3})^2 = (\sum_{k\in\mathbb{N}} a_{6k-4})(\sum_{k\in\mathbb{N}} a_{6k-2})\ mod\ 7$

(b) $2(\sum_{k\in\mathbb{N}} a_{6k-5})(\sum_{k\in\mathbb{N}} a_{6k-2})^2 = (\sum_{k\in\mathbb{N}} a_{6k-3})^3 + (\sum_{k\in\mathbb{N}} a_{6k-2})^3\ mod\ 7.$

(c) $a_1 \not\equiv 0\ mod\ 7,$

(d) $(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^{k-1} a_{7k-6}) + 2(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^k a_{7k-5}) + 3(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^{k+1} a_{7k-4}) + 4(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^{k+2} a_{7k-3}) + 5(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^{k+3} a_{7k-2}) + 6(\sum_{k\in\mathbb{N},k\neq 6n-1} \alpha^{k+4} a_{7k-1}) \not\equiv 0\ mod\ 7,$ where $\alpha = 1, 2, 3, 4, 5, 6.$

Proof: It follows from the Theorem 2.1 that $f(x)$ is a permutation polynomial modulo 7^n if and only if it is a permutation polynomial modulo 7 and $f'(x) \not\equiv 0\ mod\ 7$ for every integer $x \in Z_7$. Using Lemma 3.4, the conditions (a) and (b) are obviously true. Further,

$$f'(x) = a_1 + \sum_{k\in\mathbb{N}}(6k-4)a_{6k-4}x + \sum_{k\in\mathbb{N}}(6k-3)a_{6k-3}x^2 + \sum_{k\in\mathbb{N}}(6k-2)a_{6k-2}x^3 + \sum_{k\in\mathbb{N}}(6k)a_{6k}x^5 + \sum_{k\in\mathbb{N}}(6k+1)a_{6k+1}x^6$$

$$\equiv a_1 + (2a_2 + a_8 + 6a_{20} + 5a_{26} + 4a_{32} + 3a_{38} + 2a_{44} + ...)x + (3a_3 + 2a_9 + a_{15} + 6a_{27} + 5a_{33} + 4a_{39} + 3a_{45} + ...)x^2 + (4a_4 + 3a_{10} + 2a_{16} + a_{22} + 6a_{34} + 5a_{40} + 4a_{46} + ...)x^3 + (6a_6 + 5a_{12} + 4a_{18} + 3a_{24} + 2a_{30} + a_{36} + 6a_{48} + ...)x^5 + (6a_{13} + 5a_{19} + 4a_{25} + 3a_{31} + 2a_{37} + a_{43} + ...)x^6 \ mod\ 7.$$

Now proceeding same as in Theorem 3.3, we get the required results.

Acknowledgement

The authors gratefully acknowledge the support of UGC-SAP. Also, the second and third authors thankfully acknowledge the financial support of UGC and CSIR, respectively. We are also thankful to the anonymous reviewers for the valuable comments that helped to improve the manuscript.

References

[1] Dickson L. E., The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, part I, *Ann. of Math.* 11, 65-120, 1896-1897.

[2] Hardy G. H. and Wright E. M., An introduction to the theory of numbers, Oxford Science Publications, 5th edition, 1979.

[3] Lidl R., On cryptosystems based on permutation polynomials and finite fields, In Advanced in Cryptology-Euro Crypt 1984, Lecture Notes in Computer Science, 209, 10-15, 1985.

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

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

[6] Lidl R. and Muller W. B., Permutation polynomials in RSA-cryptosystem, In Proc. CRYPTO, New York, Plennum Press, 83, 293-301, 1948.

[7] Lidl R. and Niederreiter H., Finite Fields, Encyclopedia of Mathematics and its Application, Addision-Wesley, Reading, MA. 20 1983.

[8] Mollin R. A. and Small C., On permutation polynomial over finite fields, *Internat. J. Math. & Math. Sci.*, 10 (3), 535-544, 1948.

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

[10] Mullen G. L. and Panario D., Hanbook of Finite Fields, Discrete Mathematics and its Application, CRC Press, Taylor & Francis Group, 2013.

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

[12] Sharma P. L. and Ashima, Construction of irreducible polynomials over finite fields, *Asian-European Journal of Mathematics*, 15(7), 2250130, 2022.

[13] Sharma P. L., Ashima and Sharma A. K., Recursive construction of normal polynomials over finite fields, *Journal of Discrete Mathematical Sciences and Cryptography,* Published online, https://doi.org/10.1080/0970529.2021.1897215.

[14] Sharma P. L., Rehan M. and Sharma S., Counting irreducible polynomial polynomials over GF(3) with first and third coefficients given, *Asian-European Journal of Mathematics,* 8 (1), 1550015 (27 Pages), 2015.

[15] Sharma P. L., Sharma S. and Rehan M., On construction of irreducible polynomials over F_3, *Journal of Discrete Mathematical Sciences and Cryptography,* 18 (4), 335-347, 2015.

[16] Singh R. P. and Maity S., Permutation polynomials modulo p^n, Accessed: Sep. 20, 2016. [Online]. Available: https://eprint.iacr.org/2009/ 393.pdf

[17] Trifina L. and Tarniceriu D., A coefficient test for fourth degree permutation polynomials over integer rings, AEU-Int. *J. Electron. Commun.*, 70 (11), 1565-1568, 2016.

[18] Trifina L. and Tarniceriu D., A coefficient test for quintic permutation polynomials over integer rings, *IEEE Access,* 6, 37893-37909, 2018.

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

Received February, 2022

Revised August, 2022