A METHOD FOR GENERATING PERMUTATION POLYNOMIALS MODULO p^n

Rajesh P. Singh
Dept. of Mathematics, Central University of South Bihar, Gaya, Bihar, India
rpsingh@cub.ac.in

Received: 6/10/20, Revised: 11/6/20, Accepted: 12/16/20, Published: 1/4/21

Abstract

Using p-adic representation of integers, we obtain sufficient conditions for a polynomial over the residue class ring $\mathbb{Z}_{p^n}$ to be a permutation polynomial of $\mathbb{Z}_{p^n}$, where p is a prime number and n a positive integer.

1. Introduction

Let R be a finite commutative ring. A polynomial $f(x) \in R[x]$ is called a permutation polynomial of R if the function $x \mapsto f(x)$ is a bijection of R. A natural question is the following: given a polynomial $f(x) = a_0 + a_1x + \cdots + a_dx^d \in R[x]$, what are necessary and sufficient conditions on the coefficients $a_0, a_1, \ldots, a_d$ for $f(x)$ to be a permutation of R? This problem has not yet been solved. Permutation polynomials have several applications in combinatorics, coding theory, and cryptography, mostly when R is a finite field and the ring of residue classes of integers, (see, [1], [10], [11], [12], [13]).

We denote $\mathbb{Z}_m$ as the ring of non-negative integers less than m, under addition and multiplication modulo m. It is known that for any $m = \Pi_{i=1}^{m}\ p_i^{k_i}$, where p_i's are distinct prime numbers, $f(x)$ is a permutation polynomial over Z_m if and only if $f(x)$ is also permutation polynomial over $Z_{p_i^{k_i}}$, for each i (see [12]). In 2001, Rivest [8] considered the ring Z_m, where $m = 2^n$, $n \geq 1$, and proved that the polynomial $f(x) = a_0 + a_1x + \cdots + a_dx^d$ with integral coefficients is a permutation polynomial modulo 2^n if and only if a_1 is odd, and both $a_2 + a_4 + a_6 + \cdots$ and $a_3 + a_5 + a_7 + \cdots$ are even. This is a special case of a more general characterization given by Nöbauer(1953)[7]: the polynomial f is a permutation polynomial of Z_{p^n} if and only if f is a permutation polynomial of Z_p and $f'(x) \neq 0$ for all $x \in Z_p$. Thereby Nöbauer's characterization reduced the problem to characterizing permutation polynomials over the finite field Z_p. In 1983, Mullen and Stevens [6] used Nöbauer's characterization to count the number of permutation polynomial functions over the residue class ring Z_{p^n}, where p is a prime number and n a positive

integer. Recently Görcsös, Horváth and Mészáros [2] have generalized these results about permutation polynomials over residue class ring Z_{p^n} to finite commutative unital local rings.

Permutation polynomials with some additional properties are useful to construct public-key cryptosystems. Suppose we have a permutation polynomial $p(x)$ for which computing the inverse is hard without some additional knowledge about $p(x)$, but some structural information about $p(x)$ paves the way to make it easy, also computationally. Such a polynomial can be effectively used for cryptosystems. In [11], the authors used two permutation polynomials f and g over finite fields $\mathbb{F}_{2^m}$ and imposed a relation $f(s(x)) = g(t(y))$ between plaintext variable x and ciphertext variable y, where s and t are secret invertible linear maps of $\mathbb{F}_{2^m}$, to construct a multivariate public key cryptosystem. In [3], Khachatrian and Kyureghyan used linearized permutation polynomials over finite fields to propose a public-key cryptosystem. Permutation polynomials over residue class ring $\mathbb{Z}_m$ are used in the design of RC6 block cipher [9], and in coding theory to construct a class of deterministic interleavers for turbo codes, [12], [13].

In this paper, we obtain certain sufficient conditions for a polynomial over the residue class ring $\mathbb{Z}_{p^n}$ to be a permutation polynomial. We show that every polynomial $f(x)$ over the ring $\mathbb{Z}_{p^n}$ can be expressed as an n-tuple of multivariate triangular polynomials over $\mathbb{Z}_p$, that is, $f(x)$ can be expressed as $(f_1, f_2, \ldots, f_n)$, where $f_i = f_i(x_1, x_2, \ldots, x_i)$. Using this representation, we obtain the desired sufficient conditions.

2. The Main Result

Let p be a prime and $n > 1$. A mapping $F : \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ is *triangular* if $F(x_1, \ldots, x_n) = (f_1(x_1), f_2(x_1, x_2), \ldots, f_i(x_1, \ldots, x_i), \ldots, f_n(x_1, \ldots, x_n))$, where $f_i : \mathbb{Z}_p^i \to \mathbb{Z}_p$ are arbitrary functions, mapping $(x_1, x_2, \cdots, x_i) \mapsto f_i(x_1, x_2, \cdots, x_i)$, for $i = 1, 2. \cdots, n$. In 2002 [4], Klimov *et. al.* construct some classes of invertible transformations over n-bit words which can mix arithmatic and boolean operations (not, xor, and or). Motivated by this work, we show that every polynomial over finite ring $\mathbb{Z}_{p^n}$ can be expressed as a n-tuple of multivariate triangular polynomials over $\mathbb{Z}_p$. Note that by using p-adic representation of integers, any element $x \in \mathbb{Z}_{p^n}$ can be uniquely expressed as $x = \sum_{i=1}^{n} x_i p^{i-1}$, where $x_i \in \mathbb{Z}_p$. Let $\theta : \mathbb{Z}_{p^n} \mapsto \mathbb{Z}_p^n$ be a map defined as $\theta(x) = (x_1, x_2, \ldots, x_n)$. It is easy to see that the map θ is a bijection. Since there is a one-one correspondence between $\mathbb{Z}_{p^n}$ and $\mathbb{Z}_p^n$, we can identify x by n-tuple $(x_1, x_2, \ldots, x_n)$ over $\mathbb{Z}_p^n$. Let $\mathbb{Z}_{p^n}[x]$ be the ring of polynomials over $\mathbb{Z}_{p^n}$; let $R = \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ be the ring of multivariate polynomials in the variables $x_1, x_2, \ldots, x_n$. Now using the expansion $f(x) = f(\sum_{i=1}^{n} x_i p^{i-1}) = \sum_{i=1}^{n} f_i p^{i-1}$, where $f(x) \in \mathbb{Z}_{p^n}[x]$, and $f_i \in R$, $1 \leq i \leq n$, we have an induced mapping

$\mathbb{Z}_{p^n}[x] \to R^n$, which we also denote by θ given by $\theta(f(x)) = (f_1, f_2, \ldots, f_n)$, each f_i is a multivariate polynomial over $\mathbb{Z}_p$ in variables $x_1, x_2, \ldots, x_n$. To present our results systematically we need some lemmas.

Lemma 1. *Let $x, y \in \mathbb{Z}_{p^n}$ and $x_i, y_i, (x+y)_i$ and $(xy)_i$ respectively denote the i-th coordinates in the n-tuple representation of $x, y, x+y$ and xy over $\mathbb{Z}_p^n$. Then*

(i) $(x+y)_1 = (x_1 + y_1) \bmod p$.

(ii) for $i \geq 2$, $(x+y)_i = (x_i + y_i + \alpha_i) \bmod p$, *where α_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}, y_1, y_2, \ldots, y_{i-1}$.*

(iii) for $i \geq 2$, $(xy)_i = (x_i y_1 + x_1 y_i + \beta_i) \bmod p$, *where β_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}, y_1, y_2, \ldots, y_{i-1}$.*

(iv) for any integer $m \geq 2$, $(x^m)_1 = (x_1)^m \bmod p$ *and* $(x^m)_i = (m x_i (x_1)^{m-1} + \gamma_i) \bmod p$, *if $i \geq 2$, where γ_i is a function of the coordinates $x_1, x_2, \ldots, x_{i-1}$.*

Proof. We have $x = \sum_{i=1}^{n} x_i p^{i-1}$ and $y = (y_1, y_2, \ldots, y_n) = \sum_{i=1}^{n} y_i p^{i-1}$. The first assertion in trivial. In (ii) α_i is the carry over from the previous coordinates in the sum, so depends only on the coordinates $x_1, x_2, \ldots, x_{i-1}$, $y_1, y_2, \ldots, y_{i-1}$. For (iii) we note that $xy = x_1y_1 + (x_1y_2 + y_1x_2)p + \cdots + (x_iy_1 + y_ix_1 + x_{i-1}y_2 + \cdots + x_2y_{i-1})p^{i-1} + \cdots + (x_ny_1 + x_{n-1}y_2 + \cdots + x_1y_n)p^{n-1}$ from which it follows that $(xy)_i$ is the sum modulo p of the coefficient of p^{i-1} and the carry over from the previous coordinates. Finally, the second part of (iv) follows easily from (iii) by induction on m. □

Lemma 2. *Let $x = \sum_{i=1}^{n} x_i p^{i-1}$, $k \geq 1$, $1 \leq r \leq p-1$. Then for $i \geq 2$*

(i) $\left(x^{pk}\right)_i = \alpha_i \bmod p$,

(ii) $\left(x^{pk+r}\right)_i = r x_i (x_1)^{pk+r-1} + \beta_i \bmod p$,

where α_i, β_i are functions of $x_1, x_2, \ldots, x_{i-1}$.

Proof. The results follows from (iv) of Lemma 1. □

Next we give some examples.

Example 1. Consider the monomials x, x^2, x^3 over $\mathbb{Z}_{2^3}$. For $x = x_1 + x_2.2 + x_3.2^2$, we have

$$\begin{aligned} \theta(x) &= (x_1, x_2, x_3), \\ \theta(x^2) &= (x_1, 0, x_2 + x_1x_2), \quad \text{and} \\ \theta(x^3) &= (x_1, x_1x_2, x_1x_3). \end{aligned}$$

Example 2. Consider the monomials x, x^2, x^3 over $\mathbb{Z}_{3^3}$. For $x = x_1 + x_2.3 + x_3.3^2$, we have

$$\begin{aligned} \theta(x) &= (x_1, x_2, x_3), \\ \theta(x^2) &= (x_1^2, 2x_1x_2, x_2^2 + 2x_1x_3), \quad \text{and} \\ \theta(x^3) &= (x_1^3, 0, x_1^2x_2). \end{aligned}$$

It is clear from part (iv) of Lemma 1 that $\theta(x^m)$, for positive integer m, is a triangular map from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$. In the next proposition, we prove that $\theta(f(x))$, for any polynomial $f(x) \in \mathbb{Z}_{p^n}[x]$, is a triangular map from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$.

Proposition 1. *Let $f(x) = \sum_{i=0}^{d} a_i x^i$ is a any polynomial of degree d over $\mathbb{Z}_{p^n}$. Suppose $\theta(f(x)) = (f_1, f_2, \ldots, f_n)$. Then $\theta(f(x))$ is a triangular mapping from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$.*

Proof. By part (i) of Lemma 1, we have $f_1 = (f(x))_1 = \sum_{i=0}^{d} (a_i)_1 (x_1)^i \mod p$. Similarly, using Lemmas 1 and 2, it is easy to see that for $i \geq 1$, $(f(x))_i = f_i(x_1, x_2, \ldots, x_i)$, that is, the i-th coordinate of $f(x)$ is function of the first i coordinates of x. □

Proposition 1 tells us that-non triangular mappings from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$ cannot be represented by a polynomial over $\mathbb{Z}_{p^n}$. In view of Proposition 1, we have the following lemma.

Lemma 3. *Let $f(x) = \sum_{i=0}^{d} a_i x^i$ be a polynomial over $\mathbb{Z}_{p^n}$. Then $f(x)$ is a permutation polynomial of $\mathbb{Z}_{p^n}$ if and only if the corresponding triangular mapping $\theta(f(x))$ is permutation of $\mathbb{Z}_p^n$.*

Example 3. Suppose $f(x) = x + 2x^2 + x^3 + 4x^4 + x^5$ is a polynomial over $\mathbb{Z}_{2^3}$, then $\theta(f(x)) = (x_1, x_2, x_3 + x_1x_2)$. Since the mapping from $\mathbb{Z}_2^3$ to $\mathbb{Z}_2^3$ given by $\theta(f(x))$ is a surjection, therefore, it is a permutation of $\mathbb{Z}_2^3$. Hence $f(x) = x + 2x^2 + x^3 + 4x^4 + x^5$ is a permutation polynomial of $\mathbb{Z}_{2^3}$.

The following is a well known result which is used in the sequel.

Proposition 2. *([5]) If $d > 1$ is a divisor of $p-1$, then there exists no permutation polynomial of Z_p of degree d.*

Now, using triangular representation of polynomials, we give some sufficient conditions for a polynomial over $\mathbb{Z}_{p^n}$ to be a permutation polynomial..

Theorem 1. *Let p be a prime and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ be a polynomial with integral coefficients. Let t_r $(0 \leq r \leq p-2)$ be the largest integers*

such that $t_r(p-1)+r \le d$, *that is,* $t_r = \lfloor \frac{d-r}{p-1} \rfloor$, *where* $= \lfloor . \rfloor$ *denotes the greatest integer function. Then* $f(x)$ *is a permutation polynomial over* $\mathbb{Z}_{p^n}$, $n \ge 1$, *if*

$$\sum_{k=1}^{t_1} a_{k(p-1)+1} \neq 0 \bmod p, \tag{1}$$

$$\sum_{k=1}^{t_r} a_{k(p-1)+r} = 0 \bmod p, \quad \textit{for } r = 0, 2, 3, \ldots, p-2, \textit{ and} \tag{2}$$

$$\sum_{r=1}^{p-1} \sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r a_{pk+r} \ell^{pk+r-1} \neq 0 \bmod p \quad \textit{for } \ell = 0, 1, 2, \ldots, p-1. \tag{3}$$

Proof. We show that the mapping from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^n$ given by $\theta(f(x))$ is a surjection if the conditions (1), (2) and (3) are satisfied. We show that for $1 \le i \le n$, $(f(x))_i$, as a function of x_i and for fixed x_j, $j < i$, is invertible. For $i = 1$ we note that $\left(x^k\right)_1 = (x_1)^k \bmod p$, and $(x_1)^{k(p-1)+r} = (x_1)^r \bmod p$ for $1 \le r \le p-2$. Therefore, we get

$$\begin{aligned}
(f(x))_1 &= \left(a_0 + a_1 x + a_2 x^2 + \cdots + a_d x^d\right)_1 \\
&= (a_0)_1 + (a_1)_1 x_1 + (a_2)_1 (x_1)^2 + (a_3)_1 (x_1)^3 + \cdots + (a_d)_1 (x_1)^d \bmod p \\
&= (a_0)_1 + \sum_{k=1}^{t_0} \left(a_{k(p-1)}\right)_1 (x_1)^{k(p-1)} + \sum_{k=1}^{t_1} \left(a_{k(p-1)+1}\right)_1 (x_1)^{k(p-1)+1} + \cdots \\
&\quad + \sum_{k=1}^{t_{p-2}} \left(a_{k(p-1)+p-2}\right)_1 (x_1)^{k(p-1)+p-2} \bmod p \\
&= (a_0)_1 + \left(\sum_{k=1}^{t_0} \left(a_{k(p-1)}\right)_1\right) (x_1)^{k(p-1)} + \left(\sum_{k=1}^{t_1} \left(a_{k(p-1)+1}\right)_1\right) x_1 + \cdots \\
&\quad + \left(\sum_{k=1}^{t_{p-2}} \left(a_{k(p-1)+p-2}\right)_1\right) (x_1)^{p-2} \bmod p.
\end{aligned} \tag{4}$$

If $\sum_{k=1}^{t_1} \left(a_{k(p-1)+1}\right)_1 \neq 0 \bmod p$, and $\sum_{k=1}^{t_r} \left(a_{k(p-1)+r}\right)_1 = 0 \bmod p$, for $r = 0, 2, 3 \ldots\ldots p-2$, then the mapping in Equation (4) is invertible.

Next, for $i > 1$, using the part (ii) of Lemma 1 recursively, we get

$$\begin{aligned}(f(x))_i &= (a_0 + a_1x + a_2x^2 + \ldots + a_dx^d)_i \\ &= \left(a_0 + \sum_{k=1}^{\lfloor \frac{d}{p} \rfloor} a_{pk}x^{pk} + \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} a_{pk+r}x^{pk+r}\right)_i \\ &= \sum_{k=1}^{\lfloor \frac{d}{p} \rfloor} \left(a_{pk}x^{pk}\right)_i + \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} \left(a_{pk+r}x^{pk+r}\right)_i + \beta_1 \mod p,\end{aligned}$$

where β_1 is a function of the first $i-1$ coordinates of x. Using Lemmas 1 and 2 we get

$$\begin{aligned}\left(a_{pk}x^{pk}\right)_i &= (a_{pk})_i \left(x^{pk}\right)_1 + (a_{pk})_1 \left(x^{pk}\right)_i + \beta_2 \mod p \\ &= \beta',\end{aligned}$$

where β' is a function of the first $i-1$ coordinates of x. Again

$$\begin{aligned}(a_{pk+r}x^{pk+r})_i &= (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1(x^{pk+r})_i + \beta_3 \mod p \\ &= (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1\left(r(x_1)^{pk+r-1}x_i + \beta_4\right) + \beta_3 \mod p \\ &= r(a_{pk+r})_1(x_1)^{pk+r-1}x_i + \gamma' \mod p,\end{aligned}$$

where β_3, β_4 and γ' are functions of the first $i-1$ coordinates of x. Note that $\gamma' = (a_{pk+r})_i(x^{pk+r})_1 + (a_{pk+r})_1\beta_4 + \beta_3$. Bringing them all together, we have

$$\begin{aligned}(f(x))_i &= \sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1(x_1)^{pk+r-1}x_i + \beta^\star \mod p \\ &= x_i\sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1(x_1)^{pk+r-1} + \beta^\star \mod p,\end{aligned}$$

where $\beta^\star$ is a function of the first $i-1$ coordinates of x. For $f(x)$ to be permutation polynomial this mapping should be invertible for all values of x_1. Thus we get the conditions

$$\sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} r(a_{pk+r})_1(x_1)^{pk+r-1} \neq 0 \mod p.$$

Suppose $\ell = x_1$. Then we can rewrite it in the form

$$\sum_{r=1}^{p-1}\sum_{k=0}^{\lfloor \frac{d-r}{p} \rfloor} ra_{pk+r}\ell^{pk+r-1} \neq 0 \mod p$$

for $\ell = 0, 1, \ldots, p-1$. □

Example 4. We give an example of a permutation polynomial satisfying the conditions given in Theorem 1. Consider the polynomial $f(x) = x + 11x^2 + 7x^3 + 11x^{10} + 2x^{11} + 4x^{13} + 6x^{21}$. It can be seen easily that the coefficients of $f(x)$ satisfy (1) and (2). Moreover, the condition (3) amounts to

$$1 + 2.11\,l + 3.7\,l^2 + 10.11\,l^9 + 2.4\,l^{13} + 10.6\,l^{20} \not\equiv 0 \mod 11,$$

for $l = 0, 1, \ldots, 10$. This can be easily verified to be true, noting that $l^{10} \equiv 1 \mod 11$ for $1 \leq l \leq 10$. Hence, $f(x)$ is a permutation polynomial of $\mathbb{Z}_{11^n}$ for all $n \geq 1$.

3. Conclusion

In this paper, we have obtained sufficient conditions in terms of coefficients of a polynomial to be a permutation polynomial of $\mathbb{Z}_{p^n}$. Information about such type of sufficient conditions over arbitrary finite commutative rings seems elusive at the moment and needs further intensive investigations. It can be interesting to generalize our result to Galois rings.

Acknowledgements. I am grateful to the anonymous referees and Prof. B. K. Sarma (Department of Mathematics, IIT Guwahati) for their constructive suggestions that helped to improve the content of the paper.

References

[1] C. Ding, J. Yuan, A family of skew hadmard diffrence sets, *J. Combin. Theory Ser. A* **113** (2006), 345–352.

[2] D. Görcsös, G.Horváth, A.Mészáros, Permutation polynomials over finite rings, *Finite Fields Appl.* **49** (2018), 198–211.

[3] G. Khachatrian, M. Kyureghyan, Permutation polynomials and a new public-key encryption, *Discrete Appl. Math.* **216 (3)** (2017), 622–626.

[4] A. Klimov, A. Shamir, A new class of invertible mappings, *CHES-2002*, LNCS, Vol **2523** (2003), 470–483.

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

[6] G. Mullen, H. Stevens, Polynomial functions (mod (m)), *Acta Math. Hungar.* **44** (1984), 237–241.

[7] W. Nöbauer, Über Gruppen von restklassen nach respolynomidealen, *Österreich. Akad. Wiss. Math-Nat. KI. S.-B. IIa* **162** (1953), 207–233.

[8] R. L. Rivest, Permutation polynomials modulo 2^w, *Finite Fields Appl.* **7** (2001), 287–292.

[9] R. L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Y. Yin, The RC6 Block Cipher, *M. I. T. Laboratory for computer Science, 545 Technology Square, Cambridge, M A 02139, version 1.1-August, 20, 1998*. Available on the site: http://people.csail.mit.edu/rivest/RC6.pdf.

[10] Rajesh P. Singh, M. K. Singh, Two Congurence identies on ordered partitions, *Integers* **18**, #A73.

[11] Rajesh P. Singh, Anupam Saikia and B. K. Sarma, Poly-Dragon: An efficient multivariate cryptosystem, *J. Math. Cryptol.* **4 (4)** (2011), 349–364.

[12] J. Sun, O. Y. Takeshita, Interleavers for turbo codes using permutation polynomials over integer rings, *IEEE Trans. Inform. Theory* **51 (1)** (2005), 101–119.

[13] O. Y. Takeshita, On maximum contention free interleavers and permutation polynomials over integer rings, *IEEE Trans. Inform. Theory* **52 (3)** (2006), 1249–1253.