J. Korean Math. Soc. **60** (2023), No. 1, pp. 1–32
https://doi.org/10.4134/JKMS.j210494
pISSN: 0304-9914 / eISSN: 2234-3008

MINIMAL POLYNOMIAL DYNAMICS ON THE p-ADIC INTEGERS

Sangtae Jeong

Abstract. In this paper, we present a method of characterizing minimal polynomials on the ring $\mathbf{Z}_p$ of p-adic integers in terms of their coefficients for an arbitrary prime p. We first revisit and provide alternative proofs of the known minimality criteria given by Larin [11] for $p = 2$ and Durand and Paccaut [6] for $p = 3$, and then we show that for any prime $p \geq 5$, the proposed method enables us to classify all possible minimal polynomials on $\mathbf{Z}_p$ in terms of their coefficients, provided that two prescribed prerequisites for minimality are satisfied.

1. Introduction

Dynamical systems on $\mathbf{Z}_p$ or its positive characteristic counterparts have attracted considerable attention for their theoretical value [3, 15, 16] and have been applied to computer sciences, quantum mechanics, and cryptography [3]. One practical application for them includes the construction of pseudo-random generators from polynomials with integer coefficients that lead to a large cycle modulo a given positive integer. Using the Chinese remainder theorem, this task is reduced to finding minimal polynomials on $\mathbf{Z}_p$ that induce a full-length cycle modulo any powers of a prime number, p. As we know, a complete description of minimal polynomials on $\mathbf{Z}_p$ in terms of their coefficients seems to be a much harder task, because the associated permutation polynomials modulo p are known to be difficult to characterize in terms of their coefficients [12].

The purpose of the present study is to present a method of characterizing minimal polynomials on $\mathbf{Z}_p$ in terms of their coefficients for any prime $p > 3$. To this end, we see that such a minimal polynomial satisfies two prerequisites: the reduced polynomial modulo p is transitive, that is, it induces a full-length cycle modulo p; and the product of its derivatives at $0, \ldots, p-1$ is 1 modulo p.

Received August 13, 2021; Revised February 21, 2022; Accepted May 13, 2022.
2020 *Mathematics Subject Classification.* Primary 11S85 37E99.
Key words and phrases. p-adic integers, minimal, ergodic.
This work is supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) and funded by the Ministry of Education, Science, and Technology (2020R1A2C1A01003498).

By the two prescribed conditions, there are exactly $(p-1)!(p-1)^{p-1}$ choices of $\mathbf{Z}_p$-coefficients modulo p of the polynomial. The proposed method enables us to classify all possible minimal polynomials on $\mathbf{Z}_p$ in terms of their coefficients, provided that all prescribed conditions are completely found. Thus, the general problem of finding a minimal polynomial on $\mathbf{Z}_p$ or deciding if a given polynomial map is minimal can be completely answered. Furthermore, we revisit the known cases for $p = 2, 3$ and give a complete description of minimal polynomials on $\mathbf{Z}_p$, which can be compared with the minimality criteria given by Larin [11] for $p = 2$ and by Durand and Paccaut [6] for $p = 3$, respectively.

Regarding refined dynamical properties, Fan and Liao [8] developed a linearization technique derived from the work of DesJardins and Zieve [4, 17] to obtain the complete minimal decomposition of any polynomial, $f \in \mathbf{Z}_p[x]$, of degree ≥ 2 for an arbitrary prime p. For a broader class of 1-Lipschitz functions, Anashin [1, 2] provided an ergodicity criterion on $\mathbf{Z}_p$ in terms of Mahler coefficients for $p = 2$ and necessary conditions for $p > 2$. Recently, the author of the present paper [10] presented such an ergodicity criterion of a certain class of 1-Lipschitz functions known as $\mathcal{B}$-functions on $\mathbf{Z}_p$ for all primes p. The present work applies the idea and method of [10] to polynomials.

The remainder of this paper is organized as follows. Section 2 provides a brief discussion of the prerequisites for non-Archimedean dynamics with the existing dynamical properties of 1-Lipschitz functions on $\mathbf{Z}_p$. Section 3 contains another minimality criterion of polynomials in Theorem 3.1, which states that a polynomial, $f \in \mathbf{Z}_p[x]$, is minimal if and only if the reduction of $f(x)$ modulo $\delta_p(x)$, defined in (3.1), is minimal. We characterize minimal polynomials on $\mathbf{Z}_p$ in terms of their coefficients for $p = 2$ in Section 4 and for $p = 3$ in Section 5. Finally, Section 6 is devoted to presenting a method of characterizing minimal polynomials on $\mathbf{Z}_p$ for any prime $p \geq 5$, in terms of their coefficients according to the degrees of the polynomials.

2. Basics of non-Archimedean dynamics on $\mathbf{Z}_p$

Let $\mathbf{Z}_p$ be the ring of p-adic integers for a prime number p; let $\mathbf{Q}_p$ be the ring of p-adic numbers; and let $|\cdot|$ be the (normalized) absolute value on $\mathbf{Q}_p$ associated with the additive valuation, ord_p on $\mathbf{Q}_p$, such that $|x| = p^{-\mathrm{ord}_p(x)}$.

We next define 1-Lipschitz functions on $\mathbf{Z}_p$.

Definition. A function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is said to be 1-Lipschitz if, for all $x, y \in \mathbf{Z}_p$, we have

$$|f(x) - f(y)| \leq |x - y|.$$

Typical examples of 1-Lipschitz functions on $\mathbf{Z}_p$ include polynomials having coefficients in $\mathbf{Z}_p$ and a class of $\mathcal{B}$-functions in [2].

It should be noted that a 1-Lipschitz function f has some equivalent statements.

(L1) $f(x) \equiv f(y) \pmod{p^n}$ whenever $x \equiv y \pmod{p^n}$ for any integer $n \geq 1$.

(L2) $f(x+p^n\mathbf{Z}_p) \subset f(x)+p^n\mathbf{Z}_p$ for all $x \in \mathbf{Z}_p$ and any integer $n \geq 1$.
(L3) $|f(x+y)-f(x)| \leq |y|$ for all $x, y \in \mathbf{Z}_p$.

It should be noted that (L1) implies that a 1-Lipschitz function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ induces a sequence of reduced functions, $f_{/n}$ $(n \geq 1)$, on quotient rings defined by

$$f_{/n} : \mathbf{Z}_p/p^n\mathbf{Z}_p \to \mathbf{Z}_p/p^n\mathbf{Z}_p,\ x+p^n\mathbf{Z}_p \mapsto f(x)+p^n\mathbf{Z}_p.$$

Let us briefly recall some elements of non-Archimedean dynamics on $\mathbf{Z}_p$. A p-adic dynamical system on $\mathbf{Z}_p$ is understood as a triple $(\mathbf{Z}_p, f, \mu_p)$, where $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is a measurable function, and μ_p is the Haar measure on $\mathbf{Z}_p$, which is normalized such that $\mu_p(\mathbf{Z}_p) = 1$. Elementary μ_p-measurable sets are the p-adic balls of radius p^{-k}. These are the sets of the form, $a+p^k\mathbf{Z}_p$, for $a \in \mathbf{Z}_p$ and an integer $k \geq 0$. The measure of such a ball is defined as its radius (i.e., $\mu_p(a+p^k\mathbf{Z}_p) = 1/p^k$).

Definition. Let $(\mathbf{Z}_p, f, \mu_p)$ be a p-adic dynamical system on $\mathbf{Z}_p$. A function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is said to be measure-preserving if $\mu_p(f^{-1}(M)) = \mu_p(M)$ for each measurable subset $M \subset \mathbf{Z}_p$. A measure-preserving function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is said to be ergodic if it has no proper invariant subsets (i.e., either $\mu_p(M) = 1$ or $\mu_p(M) = 0$ holds for any measurable subset, $M \subset \mathbf{Z}_p$, such that $f^{-1}(M) = M$).

Definition. A continuous function $f : \mathbf{Z}_p \to \mathbf{Z}_p$ is said to be minimal if the forward orbit of f at x is dense in $\mathbf{Z}_p$ for every $x \in \mathbf{Z}_p$.

Let S be a finite set of $N \geq 1$ elements and f be a map from S to itself. Moreover, let f^n denote the n-th iteration of f, with the convention that f^0 is the identity map on S.

Definition. A function $f : S \to S$ is transitive or minimal on S if S forms a single cycle of f; that is, $\{x_0, f(x_0), \ldots, f^{N-1}(x_0)\} = S$ for any fixed initial point, $x_0 \in S$.

A 1-Lipschitz function on $\mathbf{Z}_p$ has some equivalent statements for measure-preservation.

Proposition 2.1. *Let $f : \mathbf{Z}_p \to \mathbf{Z}_p$ be a 1-Lipschitz function. The following are thus equivalent*:

(1) *f is onto*;
(2) *f is an isometry (i.e., $|f(x)-f(y)| = |x-y|$ for all $x, y \in \mathbf{Z}_p$)*;
(3) *$f_{/n}$ is bijective for all integers $n \geq 1$*;
(4) *f is measure-preserving.*

Proof. See [6, Proposition 4]. □

A simpler measure-preservation criterion for polynomials in $\mathbf{Z}_p[x]$ is known.

Proposition 2.2. *For $f \in \mathbf{Z}_p[x]$, the following are equivalent*:

(1) *$f_{/n}$ is bijective for all integers, $n \geq 1$*;
(2) *$f_{/2}$ is bijective*;

(3) $f_{/1}$ *is bijective, and* $f'(x) \equiv 0 \pmod{p}$ *has no solutions in* $\mathbf{Z}_p$.

Proof. See [14] or [4]. □

Regarding ergodicity or minimality, we have the following equivalent statements.

Proposition 2.3. *Let* $f : \mathbf{Z}_p \to \mathbf{Z}_p$ *be a measure-preserving* 1*-Lipschitz function. Then, the following are equivalent*:

(1) f *is minimal*;
(2) f *is uniquely ergodic* (*i.e., there is only one ergodic measure*);
(3) $f_{/n}$ *is transitive on* $\mathbf{Z}_p/p^n\mathbf{Z}_p$ *for all integers,* $n \geq 1$;
(4) f *is conjugate to the translation* $t(x) = x + 1$ *on* $\mathbf{Z}_p$, *which means that there exists a homeomorphism* ϕ *on* $\mathbf{Z}_p$ *such that* $\phi \circ f = t \circ \phi$;
(5) f *is ergodic.*

Proof. See [6, Theorem 6]. □

An efficient minimality criterion for polynomials in $\mathbf{Z}_p[x]$ is known.

Proposition 2.4. *Let* $f : \mathbf{Z}_p \to \mathbf{Z}_p$ *be a polynomial in* $\mathbf{Z}_p[x]$ *such that* $\left(\mathbf{Z}_p/p^n\mathbf{Z}_p, f_{/n}\right)$ *is minimal for* $n \geq 1$. *Then, the following are equivalent*:

(1) $\left(\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p, f_{/n+1}\right)$ *is minimal*;
(2) *For all* $x \in \mathbf{Z}_p$, *we have* $f^{p^n}(x) - x \notin p^{n+1}\mathbf{Z}_p$ *and* $\left(f^{p^n}\right)'(x) \in 1 + p\mathbf{Z}_p$;
(3) *There exists* $x \in \mathbf{Z}_p$, *such that* $f^{p^n}(x) - x \notin p^{n+1}\mathbf{Z}_p$, *and* $\left(f^{p^n}\right)'(x) \in 1 + p\mathbf{Z}_p$.

Proof. See [6, Lemma 8]. □

Proposition 2.5. *A polynomial,* $f \in \mathbf{Z}_p[x]$, *is minimal if and only if* $\left(\mathbf{Z}_p/p^\mu\mathbf{Z}_p, f_{/\mu}\right)$ *is minimal, where* $\mu = 3$ *if* p *is* 2 *or* 3 *and* $\mu = 2$ *if* $p \geq 5$.

Proof. See [6, Proposition 9]. □

3. Another minimality criterion for polynomials on $\mathbf{Z}_p$

For a prime p, we set

$$\mu := \mu(p) = \begin{cases} 3 \text{ if } p \in \{2, 3\}; \\ 2 \text{ if } p \geq 5, \end{cases}$$

and let $\delta = \delta_p$ be the integer-valued binomial coefficient polynomial on $\mathbb{Z}_p$ defined by

$$\delta(x) := \delta_p(x) = \begin{cases} \binom{x}{p^2} \text{ if } p \in \{2, 3\}; \\ \binom{x}{2p} \text{ if } p \geq 5. \end{cases} \tag{3.1}$$

Here, we give another minimality criterion of a polynomial $f(x) \in \mathbf{Z}_p[x]$ in terms of its reduction by δ. Thus, the minimality of polynomials of any degree can be reduced to that of polynomials having coefficients in the residue class ring $\mathbf{Z}/p^\mu\mathbf{Z}$, of $\deg(\delta) - 1$ degree at most. In the following, we denote

by $R(p^\mu)$ the set of all non-equivalent minimal polynomials of degree $< \deg(\delta)$ with coefficients in $\mathbf{Z}/p^\mu\mathbf{Z}$. It is understood that any element in $R(p^\mu)$ can (and will) be a polynomial having integer coefficients in $\mathbf{Z}/p^\mu\mathbf{Z} := \{0, \dots, p^\mu - 1\}$.

Here, we state Theorem 3.1 as the main result of this section. Part (1) of Theorem 3.1 is efficient for determining if a given polynomial $f(x) \in \mathbf{Z}_p[x]$ is minimal, and its proof is provided below. Moreover, part (2) is already known in the literature. Indeed, Larin [11] used the group theory related to permutations to show part (2) of Theorem 3.1, and Jeong [10] also deduced the same result from an ergodicity criterion of $\mathcal{B}$-functions on $\mathbf{Z}_p$. In later sections, we shall prove this again using the minimality criterion of polynomials on $\mathbf{Z}_p$.

Theorem 3.1. *Let $f \in \mathbf{Z}_p[x]$ be a polynomial of a positive degree.*

(1) *f is minimal if and only if the reduction of $f(x)$ modulo $\delta(x)$ is minimal in $R(p^\mu)$.*
(2) *The number of elements in $R(p^\mu)$ is determined as follows*:

$$\#R(p^\mu) = \begin{cases} 16 \text{ if } p = 2; \\ 2^5 3^{10} \text{ if } p = 3; \\ (p-1)!(p-1)^p p^{p-1} \text{ if } p \geq 5. \end{cases}$$

Proof. We prove part (1) only because the rest will be treated in later sections depending on p. Let $r(x)$ be the remainder of f by division with δ. Then,

$$f(x) = q(x)\delta(x) + r(x),$$

where $q, r \in \mathbf{Z}_p[x]$, and $r(x)$ is of degree $< \deg(\delta)$. By Proposition 2.5, the result follows from the claim that the congruence

$$f(x) \equiv r(x) \pmod{p^\mu}$$

holds. We will show that all coefficients of $q(x)$ are divisible by p^μ, thereby implying the claimed result.

By the Newton interpolation formula or by Mahler's result in [13], any polynomial, $f \in \mathbf{Z}_p[x]$, is uniquely represented as a finite sum of the form in terms of binomial coefficient polynomials:

$$\begin{aligned} f(x) &= \sum_{n=0}^{d} a_n \binom{x}{n} \\ &= \sum_{n=0}^{\deg(\delta)-1} a_n \binom{x}{n} + \sum_{n=\deg(\delta)}^{d} a_n \binom{x}{n}, \end{aligned} \tag{3.2}$$

where all a_n belong to $\mathbf{Z}_p$, and d is assumed to be greater than or equal to $\deg(\delta)$. Because any polynomial in $\mathbf{Z}_p[x]$ is an analytic function, from [3, Proposition 3.58], all $a_n/n!$ lie in the p-adic integers. Thus, it is checked that, for any $n \geq \deg(\delta)$, $a_n\binom{x}{n} = g(x)\delta(x)$ with $g(x) \in \mathbf{Z}_p[x]$, all coefficients are divisible by p^μ. Indeed, we do this in a unified way for all primes p. For

$n \geq \deg(\delta)$, we have

$$a_n \binom{x}{n} = \deg(\delta)! \frac{a_n}{n!}(x - \deg(\delta)) \cdots (x - n + 1)\delta(x).$$

Because $\deg(\delta)!$ is divisible by p^μ, by factoring-out a common factor δ from all terms in the second sum of the right-hand side of (3.2), the second sum in (3.2) is reduced to the product of the form, $q(x)\delta(x)$, with all coefficients of $q(x) \in \mathbf{Z}_p[x]$ divisible by p^μ, and the first sum in (3.2) is the remainder $r(x)$ of f on division by δ. Thus, the proof is complete. □

We say that a polynomial, $f \in \mathbf{Z}_p[x]$, is *vanishing* modulo m for a positive integer m if $f(\alpha) \equiv 0 \pmod{m}$ for any $\alpha \in \mathbf{Z}_p$. By observing from the proof of Theorem 3.1 that the polynomial q is vanishing modulo p^μ, we derive a known decomposition for minimal polynomials, which was first observed by Larin in [11, Proposition 19].

Corollary 3.2. *A polynomial $f \in \mathbf{Z}_p[x]$ is minimal if and only if $f(x)$ is representable in the form*

$$f(x) = r(x) + t(x),$$

where $r(x)$ belongs to $R(p^\mu)$ and $t(x)$ is vanishing modulo p^μ.

4. Characterization for $p = 2$

For $p = 2$, the minimality criterion of a polynomial in $\mathbf{Z}_p[x]$ is well known in terms of its coefficients. Larin [11] and Durand and Paccaut [6] independently gave a minimal criterion of a general polynomial in $\mathbf{Z}_2[x]$ in terms of its coefficients. Herein, we give an alternative proof of their results. For this, we recall the minimal conditions for a polynomial of degree three at most.

Lemma 4.1. *A polynomial, $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbf{Z}_2[x]$, is minimal if and only if the system of the following relations is fulfilled*:

$$\begin{aligned} a_0 &\equiv 1 \pmod 2; \\ a_2 &\equiv 0 \pmod 2; \\ a_3 &\equiv 0 \pmod 4; \\ a_1 + a_2 &\equiv 1 \pmod 4. \end{aligned}$$

Proof. See [11, Proposition 20] for an original proof. For completeness, we follow the strategy in [6] to give an alternative proof. It was shown in [6, Lemmas 12 and 13, Theorem 14] that f is minimal if and only if the following conditions are satisfied:

(M1) $f(0) \equiv 1 \pmod 2$ and $f(1) \equiv 0 \pmod 2$;
(M2) $(f^2)'(0) \equiv 1 \pmod 2$;
(M3) $(f^2)(0) \in 2\mathbf{Z}_2 \setminus 4\mathbf{Z}_2$;
(M4) $(f^4)(0) \in 4\mathbf{Z}_2 \setminus 8\mathbf{Z}_2$.

Through simple computations, it is easy to see that (M1) and (M2) are equivalent to the following relations:

$$a_0 \equiv 1 \pmod 2;\ a_1 \equiv 1 \pmod 2;\ a_2 \equiv 0 \pmod 2;\ a_3 \equiv 0 \pmod 2.$$

Secondly, because $f^2(0) \equiv 1 + a_1 + a_2 + a_3 \pmod 4$, (M3) is equivalent to $a_1 + a_2 + a_3 \equiv 1 \pmod 4$. Finally, from the proof of [6, Thereom 14], (M4) is equivalent to

$$(f^2)'(0) + (f^2)''(0) \equiv 1 \pmod 4,$$

which is also equivalent to $2a_2 + a_1(a_1 + a_3) \equiv 1 \pmod 4$. Through direct computations with the above relations, it is equivalent to $a_3 \equiv 0 \pmod 4$. Putting all the relations together gives the desired end-result. □

We now conclude the proof of part (2) of Theorem 3.1 for the case $p = 2$ by showing $\#R(p^\mu) = 16$ in the following:

Lemma 4.2. *A polynomial, $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbf{Z}_2[x]$, is minimal if and only if the map, $x \mapsto f(x) \pmod 8$, $x \in \{0, 1, \ldots, 7\}$ coincides with a map induced by any of the following 16 polynomials on the ring $\mathbf{Z}/8\mathbf{Z}$:*

$$\begin{array}{cccc} x+1 & 5x+1 & 2x^2+3x+1 & 2x^2+7x+1 \\ x+3 & 5x+3 & 2x^2+3x+3 & 2x^2+7x+3 \\ x+5 & 5x+5 & 2x^2+3x+5 & 2x^2+7x+5 \\ x+7 & 5x+7 & 2x^2+3x+7 & 2x^2+7x+7 \end{array}$$

Proof. We use Lemma 4.1 to list all distinct minimal polynomials in $R(p^\mu)$. According to Lemma 4.1, it suffices to deal with a minimal polynomial $f(x) = a_0 + a_1x + a_2x^2$, of degree < 3, with $a_i \in \mathbf{Z}/8\mathbf{Z}$, because a minimal polynomial $f(x)$ of degree three is reduced to a polynomial of lower degree due to the simple observation that $4x^3 \equiv 4x \pmod 8$. Next, we set $a_0 = 1 + 2z_0$, $a_1 = 1 + 2z_1$, $a_2 = 2z_2$ with $z_i \in \mathbf{Z}/4\mathbf{Z}$. Thus, we have a minimal polynomial, $f(x) = 1 + x + 2(z_0 + z_1x + z_2x^2)$, with a condition, $z_1 + z_2 \equiv 0 \pmod 2$. If we put the set $S = \{(z_0, z_1, z_2) \in (\mathbf{Z}/4\mathbf{Z})^3 \mid z_1 + z_2 \equiv 0 \pmod 2\}$, S has 32 elements whose each element leads to a minimal polynomial. Some of them will be equivalent modulo 8. Thus, let us find non-equivalent minimal polynomials by counting elements of S that induce such polynomials. To this end, the set S is divided into two disjoint subsets as follows:

$$S = S_0 \cup S_2,$$

where for $i \in \{0, 2\}$, $S_i := \{(z_0, z_1, z_2) \in S \mid z_1 + z_2 \equiv i \pmod 4\}$.

Suppose that two elements, (z_0, z_1, z_2) and (z_0', z_1', z_2'), in S_0 lead to an equivalent minimal polynomial modulo 8. From the representation of f, we then derive the following relation:

$$z_0 + z_1x + z_2x^2 \equiv z_0' + z_1'x + z_2'x^2 \pmod 4,$$

which is easily equivalent to the following relations:

$$z_0 = z_0';\ z_1 \equiv z_1' \pmod 2;\ z_2 \equiv z_2' \pmod 2.$$

Thus, there are exactly eight non-equivalent minimal polynomials in S_0 that violate these relations. Indeed, they constitute the first and fourth columns of the matrix array in the statement. By the same argument for S_2, we obtain eight more non-equivalent minimal polynomials that constitute the second and third columns of the matrix array. Thus, combining the two cases gives the result. □

We revisit the minimality criterion of Durand and Paccaut to remove the assumption that the polynomial has a constant term, 1. To this end, for $f(x) = a_0 + a_1x + \cdots + a_dx^d$, a polynomial of degree $d \geq 1$ in $\mathbf{Z}_2[x]$, we set

$$A_0 = \sum_{0<i\equiv 0 \pmod 2} a_i;\ A_1 = \sum_{i\equiv 1 \pmod 2} a_i.$$

Theorem 4.3. *A polynomial, $f(x) = a_0+a_1x+\cdots+a_dx^d \in \mathbf{Z}_2[x]$, is minimal if and only if the system of the following relations is fulfilled*:

$$\begin{aligned} a_0 &\equiv 1 \pmod 2;\\ a_1 &\equiv 1 \pmod 2;\\ A_1 &\equiv 1 \pmod 2;\\ A_0 + A_1 &\equiv 1 \pmod 4;\\ 2a_2 + a_1A_1 &\equiv 1 \pmod 4. \end{aligned}$$

Proof. The proof is identical with that of [6, Theorem 14], except for the assumption that $a_0 = f(0) = 1$. Because the rest of the conditions is the same, we point out that the fourth condition involving a_0 is also unchanged without the restriction on a_0 by computing $f^2(0)$ modulo 4 as follows. Using the Taylor theorem, we get

$$f^2(0) = f(a_0) = f(1 + 2z_0) \equiv f(1) + 2z_0f'(1) \equiv 2a_0 - 1 + A_0 + A_1 \pmod 4,$$

because $f'(1) \equiv A_1 \equiv 1 \pmod 2$. Thus, by (M3), it is easily seen that $f^2(0) \equiv 2 \pmod 4$ is equivalent to $A_0 + A_1 \equiv 1 \pmod 4$ as $a_0 \equiv 1 \pmod 2$. □

For completeness, we state Larin's result that follows from Lemma 4.1 through a simple reduction procedure.

Corollary 4.4. *A polynomial, $f(x) = a_0+a_1x+\cdots+a_dx^d \in \mathbf{Z}_2[x]$, is minimal if and only if the system of the following relations is fulfilled*:

$$\begin{aligned} a_0 &\equiv 1 \pmod 2;\\ a_1 &\equiv 1 \pmod 2;\\ A_1 - a_1 &\equiv 2a_2 \pmod 4;\\ A_0 &\equiv a_1 + 2a_2 - 1 \pmod 4. \end{aligned}$$

Proof. The relations in Theorem 4.3 are shown to be equivalent to those in the statement. See [11, Proposition 21] for an original proof. □

5. Characterization for $p = 3$

We now turn to the case, $p = 3$. For this case, Durand and Paccaut in [6] provided a complete minimality criterion of a polynomial, $f \in \mathbf{Z}_3[x]$, in terms of its coefficients under the assumption that $f(0) = 1$. Their characterization was mainly based on the following:

Proposition 5.1. *Let $f \in \mathbf{Z}_3[x]$ be a polynomial of a positive degree. Then, f is minimal if and only if the following conditions are satisfied*:

(M1) $f_{/1}$ *is transitive* (*i.e., f is transitive modulo* 3);
(M2) $(f^3)'(0) \equiv 1 \pmod 3$ (*i.e.,* $(f)'(f^2(0))f'(f(0))f'(0) \equiv 1 \pmod 3$);
(M3) $f^3(0) \in 3\mathbf{Z}_3 \setminus 9\mathbf{Z}_3$; *and*
(M4) $3(f^3)''(0) - 2f^3(0) \not\equiv 0 \pmod 9$.

Proof. See [6, Lemma 17 and Theorem 18] for an original proof. □

General polynomials use a conjugacy homeomorphism to provide a minimality criterion of a polynomial that involves higher powers of its constant term. Herein, we revisit the criterion of Durand and Paccaut from different perspectives and provide a complete minimality criterion of a polynomial, $f \in \mathbf{Z}_3[x]$, in terms of its coefficients, without any restriction on the constant term. To state it properly, we set the following constants associated with the coefficients of a polynomial, $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbf{Z}_3[x]$, of degree $d \geq 1$:

$$\begin{aligned} &a_0 = a_0;\ \sum_{i\in 1+2\mathbf{Z}} a_i = A_1;\ \sum_{0<i\in 2\mathbf{Z}} a_i = A_0;\\ &a_1 = D_0;\ \sum_{i=1}^{d} ia_i = D_1;\ \sum_{i=1}^{d} ia_i2^{i-1} = D_2. \end{aligned} \tag{5.1}$$

We are now in a position to prove Theorem 5.2 using Proposition 5.1.

Theorem 5.2. *A polynomial, $f(x) = a_0 + a_1x + \cdots + a_dx^d \in \mathbf{Z}_3[x]$ of degree $d \geq 1$, is minimal if and only if f satisfies one of the conditions,* (i)–(viii):
Setting $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \ldots, \cdot]$,

(i) $[1,1,0,1,1,1]$, $A_0 + 6 \not\equiv 0$ [9], $A_0 + 6 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2}$ [9];
(ii) $[1,1,0,1,2,2]$, $A_1+a_0+4 \not\equiv 0$ [9], $A_1+a_0+4 \not\equiv 3a_2+3\sum_{j\geq 0} a_{6j+5}$ [9];
(iii) $[1,1,0,2,1,2]$, $A_1+2a_0+3 \not\equiv 0$ [9], $A_1+2a_0+3 \not\equiv 6a_2+3\sum_{j\geq 0} a_{6j+5}$ [9];
(iv) $[1,1,0,2,2,1]$, $A_0+2a_0+4 \not\equiv 0$ [9], $A_0+2a_0+4 \not\equiv 3a_2+3\sum_{j\geq 0} a_{6j+2}$ [9];
(v) $[2,1,0,1,1,1]$, $A_0 + 3 \not\equiv 0$ [9], $A_0 + 3 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2}$ [9];
(vi) $[2,1,0,1,2,2]$, $A_1+2a_0+7 \not\equiv 0$ [9], $A_1+2a_0+7 \not\equiv 6a_2+3\sum_{j\geq 0} a_{6j+5}$ [9];
(vii) $[2,1,0,2,1,2]$, $A_0+2a_0+5 \not\equiv 0$ [9], $A_0+2a_0+5 \not\equiv 3a_2+3\sum_{j\geq 0} a_{6j+2}$ [9];
(viii) $[2,1,0,2,2,1]$, $A_1+a_0+6 \not\equiv 0$ [9], $A_1+a_0+6 \not\equiv 3a_2+3\sum_{j\geq 0} a_{6j+5}$ [9].

Proof. The key idea for this proof requires viewing the equations in (5.1) as the linear system modulo 3 in variables $a_0 \cdots a_d$ for a given constant column vector, $[a_0, A_1, A_0, D_0, D_1, D_2]^t \bmod 3$, where t indicates the transpose of a

matrix. We then find the necessary and sufficient conditions for minimality of a polynomial, f, having the prescribed vectors, $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$.

To ensure that both (M1) and (M2) are satisfied, we list the set of all possible eight row vectors, $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$, that constitute

$$\text{Type I}: [1,1,0,1,1,1],\ [1,1,0,1,2,2],\ [1,1,0,2,1,2],\ [1,1,0,2,2,1];$$
$$\text{Type II}: [2,1,0,1,1,1],\ [2,1,0,1,2,2],\ [2,1,0,2,1,2],\ [2,1,0,2,2,1].$$

It is observed that the transitivity of f modulo 3 induces Types I and II, with the former being $f(0) \equiv 1 \pmod 3$ and the latter being $f(0) \equiv 2 \pmod 3$. For each type, there are exactly four cases for $[D_0, D_1, D_2] \bmod 3$ satisfying $D_0D_1D_2 \equiv 1 \pmod 3$ in (M2). Altogether, there are eight choices for constant vectors, $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$. For simplicity, we may assume that the degree of f is less than or equal to $6k$, if necessary, by setting the coefficients of higher degrees to be 0. Hence, the augmented coefficient matrix of the above linear systems modulo 3 is given by a matrix of the form $[A|B] = [R|S|B]$:

$$\left(\begin{array}{cccccccccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&\cdot&\cdots&\cdot&1&1&1&1&2&2&2&2\\
0&1&0&1&0&1&0&1&0&1&0&1&\cdot&\cdots&\cdot&1&1&1&1&1&1&1&1\\
0&0&1&0&1&0&1&0&1&0&1&0&\cdot&\cdots&\cdot&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&\cdot&\cdots&\cdot&1&1&2&2&1&1&2&2\\
0&1&2&0&1&2&0&1&2&0&1&2&\cdot&\cdots&\cdot&1&2&1&2&1&2&1&2\\
0&1&1&0&2&2&0&1&1&0&2&2&\cdot&\cdots&\cdot&1&2&2&1&1&2&2&1
\end{array}\right)$$

The coefficient matrix A of size $6 \times (6k+1)$ comes from the linear system in (5.1) and is divided into two submatrices R and S, where R is a 6×6 matrix, which is row reduced to the identity matrix I_6 in (5.2). The matrix S of size $6 \times 6(k-1)+1$ is of the form $S = [M|\cdots|M|C_1]$, where M is the submatrix that consists of the first six column vectors of S and repeats $k-1$ times in S, and C_1 is the first column of M. The reason that the matrix S has this type of pattern is that the entries of the second and third rows of S have a period of length 2 and those of the fifth and sixth rows have a period of length 3. This pattern of the matrix S is also the reason why the degree d of f is taken as $d = 6k$. Furthermore, the constant 6×8 matrix B is formed by transposing the eight row vectors, $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$, that appear in the orders of Type I/II. Thus, by applying row operations to the augmented coefficient matrix, we can determine all solutions, $[a_0, \ldots, a_d] \bmod 3$, to the linear systems simultaneously for all eight constant vectors, $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$.

The reduced row echelon form of the augmented coefficient matrix of the above linear systems is simultaneously given by a matrix of the form $[A'|B'] = [R'|S'|B']$:

$$\left(\begin{array}{cccccccccccccc|cccccccc}
1&0&0&0&0&0&0&0&0&0&0&0&\cdot&\cdots&\cdot&1&1&1&1&2&2&2&2\\
0&1&0&0&0&0&0&0&0&0&0&0&\cdot&\cdots&\cdot&1&1&2&2&1&1&2&2\\
0&0&1&0&0&0&2&0&1&0&0&0&\cdot&\cdots&\cdot&0&0&1&2&0&0&1&2\\
0&0&0&1&0&0&0&2&0&1&0&0&\cdot&\cdots&\cdot&0&1&0&0&0&1&0&0\\
0&0&0&0&1&0&2&0&0&0&1&0&\cdot&\cdots&\cdot&0&0&2&1&0&0&2&1\\
0&0&0&0&0&1&0&2&0&0&0&1&\cdot&\cdots&\cdot&0&2&2&2&0&2&2&2
\end{array}\right). \tag{5.2}$$

It is observed here that the matrix R' in the reduced form (5.2) is the identity matrix of size 6, and owing to the pattern of S, the matrix S' is of the form $S' = [M'|\cdots|M'|C_1']$, where M' is a submatrix formed by the first 6 column vectors of S' and M' appears $k-1$ times in S', and C_1' is the first column of M', that is, the 7th column of the matrix A'. Further, the 6×8 matrix B' is formed from the matrix B via row operations.

Using the reduced row echelon in (5.2), the parametric representations for solutions to the chosen linear system are given by the following relations:

$$
\begin{aligned}
a_0 &= r_0 + 3z_0;\\
a_1 &= r_1 + 3z_1;\\
a_2 &= r_2 + 3z_2 + (a_6 + a_{12} + \cdots + a_{6k}) + 2(a_8 + a_{14} + \cdots + a_{6k-4});\\
a_3 &= r_3 + 3z_3 + (a_7 + a_{13} + \cdots + a_{6k-5}) + 2(a_9 + a_{15} + \cdots + a_{6k-3});\\
a_4 &= r_4 + 3z_4 + (a_6 + a_{12} + \cdots + a_{6k}) + 2(a_{10} + a_{16} + \cdots + a_{6k-2});\\
a_5 &= r_5 + 3z_5 + (a_7 + a_{13} + \cdots + a_{6k-5}) + 2(a_{11} + a_{17} + \cdots + a_{6k-1}),
\end{aligned}
\tag{5.3}
$$

where $[r_0, \ldots, r_5]^t$ is one of the eight constant column vectors of the matrix B' in (5.2), and $\{z_i\}_{0\le i\le 5}$ belong to $\mathbf{Z}_3$. From the entries of each column $[r_0, \ldots, r_5]^t$ of B', we form a polynomial, $r(x) = \sum_{i=0}^{5} r_i x^i$, and all such polynomials are listed in the column order of the matrix B':

$$
\begin{aligned}
P_8 := \{&1 + x, 1 + x + x^3 + 2x^5, 1 + 2x + x^2 + 2x^4 + 2x^5,\\
&1 + 2x + 2x^2 + x^4 + 2x^5, 2 + x, 2 + x + x^3 + 2x^5,\\
&2 + 2x + x^2 + 2x^4 + 2x^5, 2 + 2x + 2x^2 + x^4 + 2x^5\}.
\end{aligned}
$$

Substituting these relations (5.3) into $f(x)$ yields

$$
f(x) = r(x) + H(x), \tag{5.4}
$$

where r belongs to P_8 and

$$
H(x) = 3\sum_{i=0}^{5} z_i x^i + \sum_{j=6}^{6k} a_j h_j(x), \tag{5.5}
$$

where, for $6 \le j = 6i + l \le 6k$ with $1 \le i \le k$ and $0 \le l \le 5$,

$$
\begin{aligned}
&h_{6i}(x) = x^2 + x^4 + x^{6i}, h_{6i+1}(x) = x^3 + x^5 + x^{6i+1}, h_{6i+2}(x) = 2x^2 + x^{6i+2},\\
&h_{6i+3}(x) = 2x^3 + x^{6i+3}, h_{6i+4}(x) = 2x^4 + x^{6i+4}, h_{6i+5}(x) = 2x^5 + x^{6i+5}.
\end{aligned}
$$

Note that the polynomials, h_j, are vanishing modulo 3, and it is easy to compute $h_j(2)$ modulo 9 as $2^6 \equiv 1 \pmod 9$. Thus, the following crucial properties of H in (5.5) are easily checked and will be heavily and implicitly used in later computations:

- $H(x)$ and $H'(x)$ are vanishing modulo 3;
- $H(x + t(x)) \equiv H(x) \pmod 9$ if $t(x)$ is vanishing modulo 3.

The values of $H(i)$ modulo 9 are obtained for each $i = 0, 1, 2$ as follows:

$$\begin{aligned} H(0) &= 3z_0; \\ H(1) &\equiv 3(z_0 + z_1 + z_2 + z_3 + z_4 + z_5) \\ &\quad + 3E_0 + 3E_1 + 3E_2 + 3E_3 + 3E_4 + 3E_5 \pmod 9; \\ H(2) &\equiv 3(z_0 + 2z_1 + z_2 + 2z_3 + z_4 + 2z_5) \\ &\quad + 3E_0 + 6E_1 + 3E_2 + 6E_3 + 3E_4 + 6E_5 \pmod 9, \end{aligned} \tag{5.6}$$

where for $0 \le l \le 5$, $E_l = \sum_{i \ge 6, i \equiv l \pmod 6} a_i$.

It is useful to compute

$$H(0) + H(1) + H(2) \equiv 6(z_2 + z_4) + 6E_0 + 6E_2 + 6E_4 \pmod 9.$$

For (M3), we now compute $f^3(0)$ modulo 9 in terms of the coefficients, a_i. The Taylor theorem for a polynomial in (5.4) yields

$$\begin{aligned} f^2(x) &\equiv f(r(x) + H(x)) \equiv f(r(x)) + H(x)r'(r(x)) \pmod 9 \\ &\equiv r^2(x) + H(r(x)) + H(x)r'(r(x)) \pmod 9. \end{aligned} \tag{5.7}$$

Similarly, computing $f^3(x)$ once more yields

$$f^3(x) \equiv r^3(x) + H(r^2(x)) + H(r(x))r'(r^2(x)) + H(x)r'(r(x))r'(r^2(x)) \pmod 9.$$

Therefore,

$$\begin{aligned} f^3(0) &\equiv r^3(0) + r'(r^2(0))r'(r(0))H(0) \\ &\quad + r'(r^2(0))H(r(0)) + H(r^2(0)) \pmod 9. \end{aligned} \tag{5.8}$$

Computing $r(0)$ modulo 9 for each $r \in P_8$ gives

$$f^3(0) \equiv \begin{cases} 3 + H(0) + H(1) + H(2) \pmod 9 & \text{if Case 1;} \\ H(0) + 2H(1) + H(2) \pmod 9 & \text{if Case 2;} \\ 2H(0) + 2H(1) + H(2) \pmod 9 & \text{if Case 3;} \\ 2H(0) + H(1) + H(2) \pmod 9 & \text{if Case 4;} \\ 6 + H(0) + H(1) + H(2) \pmod 9 & \text{if Case 5;} \\ 3 + H(0) + H(1) + 2H(2) \pmod 9 & \text{if Case 6;} \\ 6 + 2H(0) + H(1) + H(2) \pmod 9 & \text{if Case 7;} \\ 6 + 2H(0) + H(1) + 2H(2) \pmod 9 & \text{if Case 8.} \end{cases} \tag{5.9}$$

Using the values in (5.6), the expressions in (5.9) can be rewritten in terms of a_i's:

$$f^3(0) \equiv \begin{cases} 2(A_0 + 6) \pmod 9 & \text{if Case 1;} \\ A_1 + a_0 + 4 \pmod 9 & \text{if Case 2;} \\ A_1 + 2a_0 + 3 \pmod 9 & \text{if Case 3;} \\ 2(A_0 + 5a_0 + 1) \pmod 9 & \text{if Case 4;} \\ 2(A_0 + 3) \pmod 9 & \text{if Case 5;} \\ 2(A_1 + 5a_0 + 1) \pmod 9 & \text{if Case 6;} \\ 2(A_0 + 5a_0 + 8) \pmod 9 & \text{if Case 7;} \\ 2(A_1 + a_0 + 6) \pmod 9 & \text{if Case 8.} \end{cases} \tag{5.10}$$

We now turn to (M4) by computing the value $(f^3)''(0) \pmod 3$ as follows:

$$\begin{aligned}(f^3)''(0) &= f'(f^2(0))f'(f(0))f''(0) + f'(f^2(0))f'(0)^2 f''(f(0)) \\ &\quad + f'(f(0))^2 f'(0)^2 f''(f^2(0)) \\ &\equiv f'(f^2(0))f'(f(0))f''(0) + f'(f^2(0))f''(f(0)) \\ &\quad + f''(f^2(0)) \pmod 3,\end{aligned} \tag{5.11}$$

because $\lambda^2 \equiv 1 \pmod 3$ for any $\lambda \not\equiv 0 \pmod 3$.

Because $f(x) \equiv r(x) \pmod 3$ and $f'(x) \equiv r'(x) \pmod 3$, from (5.11), we have

$$\begin{aligned}(f^3)''(0) &\equiv r'(r^2(0))r'(r(0))f''(0) + r'(r^2(0))f''(r(0)) \\ &\quad + f''(r^2(0)) \pmod 3.\end{aligned} \tag{5.12}$$

Note that there is a perfect coincidence between r'-related coefficients in (5.8) and (5.12). Using the formula in (5.12), we obtain

$$(f^3)''(0) \equiv \begin{cases} f''(0) + f''(1) + f''(2) \pmod 3 & \text{if Case 1;} \\ f''(0) + 2f''(1) + f''(2) \pmod 3 & \text{if Case 2;} \\ 2f''(0) + 2f''(1) + f''(2) \pmod 3 & \text{if Case 3;} \\ 2f''(0) + f''(1) + f''(2) \pmod 3 & \text{if Case 4;} \\ f''(0) + f''(1) + f''(2) \pmod 3 & \text{if Case 5;} \\ f''(0) + f''(1) + 2f''(2) \pmod 3 & \text{if Case 6;} \\ 2f''(0) + f''(1) + f''(2) \pmod 3 & \text{if Case 7;} \\ 2f''(0) + f''(1) + 2f''(2) \pmod 3 & \text{if Case 8.} \end{cases} \tag{5.13}$$

A direct computation yields

$$f''(0) = 2a_2;\ f''(1) \equiv -\sum_{j\geq 0} a_{3j+2} \pmod 3;\ f''(2) \equiv -\sum_{j\geq 0} (-1)^j a_{3j+2} \pmod 3.$$

Applying these identities to (5.13) yields

$$(f^3)''(0) \equiv \begin{cases} 2a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if Case 1;} \\ 2a_2 + 2\sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if Case 2;} \\ a_2 + 2\sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if Case 3;} \\ a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if Case 4;} \\ 2a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if Case 5;} \\ 2a_2 + \sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if Case 6;} \\ a_2 + \sum_{j\geq 0} a_{6j+2} \pmod 3 & \text{if Case 7;} \\ a_2 + \sum_{j\geq 0} a_{6j+5} \pmod 3 & \text{if Case 8.} \end{cases} \tag{5.14}$$

Hence, the equivalent condition of (M3) is given by (5.10) for each case, as shown in the statement of Theorem 5.2. Regarding (M4), computing $2f^3(0) \not\equiv 3(f^3)''(0) \pmod 9$ from (5.10) and (5.14) yields the equivalent condition for each case, as shown in the statement of Theorem 5.2. □

Focusing on $a_0 = 1$ from Theorem 5.2 yields the result of Durand and Paccaut [6].

Corollary 5.3. *A polynomial,* $f(x) = 1 + a_1x + \cdots + a_dx^d \in \mathbf{Z}_3[x]$ *of degree* $d \geq 1$*, is minimal if and only if* f *fulfills one of the conditions* (i)–(iv):

Setting $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \ldots, \cdot]$,

(i) $[1,1,0,1,1,1]$, $A_0 + 6 \not\equiv 0$ [9], $A_0 + 6 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+2}$ [9];
(ii) $[1,1,0,1,2,2]$, $A_1 + 5 \not\equiv 0$ [9], $A_1 + 5 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+5}$ [9];
(iii) $[1,1,0,2,1,2]$, $A_1 + 5 \not\equiv 0$ [9], $A_1 + 5 \not\equiv 6a_2 + 3\sum_{j\geq 0} a_{6j+5}$ [9];
(iv) $[1,1,0,2,2,1]$, $A_0 + 6 \not\equiv 0$ [9], $A_0 + 6 \not\equiv 3a_2 + 3\sum_{j\geq 0} a_{6j+2}$ [9].

In light of Theorem 3.1, it is of interest to deduce a complete minimal criterion of a polynomial of degree 8 at most from Theorem 5.2.

Corollary 5.4. *A polynomial,* $f(x) = a_0 + a_1x + \cdots + a_8x^8 \in \mathbf{Z}_3[x]$*, is minimal if and only if* f *fulfills one of the conditions,* (i)–(viii):

Setting $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \ldots, \cdot])$,

(i) $[1,1,0,1,1,1]$, $a_2+a_4+a_6+a_8+6 \not\equiv 0$ [9], $a_2+a_4+a_6+7a_8+6 \not\equiv 0$ [9];
(ii) $[1,1,0,1,2,2]$, $a_0 + a_1 + a_3 + a_5 + a_7 + 4 \not\equiv 0$ [9], $a_0 + a_1 + 6a_2 + a_3 + 7a_5 + a_7 + 4 \not\equiv 0$ [9];
(iii) $[1,1,0,2,1,2]$, $2a_0 + a_1 + a_3 + a_5 + a_7 + 3 \not\equiv 0$ [9], $2a_0 + a_1 + 3a_2 + a_3 + 7a_5 + a_7 + 3 \not\equiv 0$ [9];
(iv) $[1,1,0,2,2,1]$, $2a_0 + a_2 + a_4 + a_6 + a_8 + 4 \not\equiv 0$ [9], $2a_0 + 4a_2 + a_4 + a_6 + 7a_8 + 4 \not\equiv 0$ [9];
(v) $[2,1,0,1,1,1]$, $a_2+a_4+a_6+a_8+3 \not\equiv 0$ [9], $a_2+a_4+a_6+7a_8+3 \not\equiv 0$ [9];
(vi) $[2,1,0,1,2,2]$, $2a_0 + a_1 + a_3 + a_5 + a_7 + 7 \not\equiv 0$ [9], $2a_0 + a_1 + 3a_2 + a_3 + 7a_5 + a_7 + 7 \not\equiv 0$ [9];
(vii) $[2,1,0,2,1,2]$, $2a_0 + a_2 + a_4 + a_6 + a_8 + 5 \not\equiv 0$ [9], $2a_0 + 4a_2 + a_4 + a_6 + 7a_8 + 5 \not\equiv 0$ [9];
(viii) $[2,1,0,2,2,1]$, $a_0 + a_1 + a_3 + a_5 + a_7 + 6 \not\equiv 0$ [9], $a_0 + a_1 + 6a_2 + a_3 + 7a_5 + a_7 + 6 \not\equiv 0$ [9].

Proof. It is immediate from Theorem 5.2. □

The following lemma remains to be proven to complete the proof of part (2) of Theorem 3.1 for the case, $p = 3$.

Lemma 5.5. $\#R(3^3) = 2^5 \cdot 3^{10}$.

Proof. We use Corollary 5.4 to assert that the number of all possible non-equivalent minimal polynomials modulo 3^3 is $4 \cdot 3^{10}$ for each of the eight cases. We do this for case 1, only because the rest can be done in a similar way. Let $f(x) = a_0 + a_1x + \cdots + a_8x^8 \in \mathbf{Z}/27\mathbf{Z}[x]$ be a minimal polynomial of degree 8 at most in Case (i) of Corollary 5.4. From (5.3), the parametric representation of f is given by the following relations:

$$\begin{aligned} &a_0 = 1 + 3z_0, a_1 = 1 + 3z_1, a_2 = a_6 + 2a_8 + 3z_2, a_3 = a_7 + 3z_3; \\ &a_4 = a_6 + 3z_4, a_5 = a_7 + 3z_5, a_6 = e_6 + 3z_6, a_7 = e_7 + 3z_7, a_8 = e_8 + 3z_8, \end{aligned} \tag{5.15}$$

where $z_i \in \mathbf{Z}/9\mathbf{Z}$ $(0 \le i \le 8)$ and $e_i \in \mathbf{Z}/3\mathbf{Z}$ $(6 \le i \le 8)$. These relations yield the decomposition of f of the form,

$$f(x) = 1 + x + H(x), \tag{5.16}$$

where

$$\begin{aligned} H(x) = 3\big(&z_0 + z_1x + (z_2 + z_6 + 2z_8)x^2 + (z_3 + z_7)x^3 + (z_4 + z_6)x^4 \\ &+(z_5 + z_7)x^7\big) + 3\big(z_6x^6 + z_7x^7 + z_8x^8\big) \\ &+ e_6(x^2 + x^4 + x^6) + e_7(x^3 + x^5 + x^7) + e_8(2x^2 + x^8). \end{aligned} \tag{5.17}$$

From Corollary 5.4 for Case 1, the minimal conditions of f are given by

$$a_2 + a_4 + a_6 + a_8 + 6 \not\equiv 0 \ [9],\ a_2 + a_4 + a_6 + 7a_8 + 6 \not\equiv 0 \ [9].$$

Through (5.15), they are respectively equivalent to

$$z_2 + z_4 + e_6 + e_8 + 2 \not\equiv 0 \ [3],\ z_2 + z_4 + e_6 + 2 \not\equiv 0 \ [3]. \tag{5.18}$$

Let S be the set of all coefficient vectors, $\mathbf{z} := [z_0, \ldots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \in (\mathbf{Z}/9\mathbf{Z})^6 \times (\mathbf{Z}/3\mathbf{Z})^3 \times (\mathbf{Z}/9\mathbf{Z})^3$, satisfying the two conditions of (5.18). It is straightforward to show that S has a cardinality of $4 \cdot 3^{19}$. Indeed, owing to a complement set, the number of all vectors in S is equal to

$$\begin{aligned} 3^{21} &-\#\{[z_0, \ldots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + e_8 + 2 \equiv 0 \pmod 3\} \\ &-\#\{[z_0, \ldots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + 2 \equiv 0 \pmod 3\} \\ &+\#\{[z_0, \ldots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + e_8 + 2 \equiv 0 \pmod 3; \\ &\qquad z_2 + z_4 + e_6 + 2 \equiv 0 \pmod 3\}, \end{aligned}$$

which is equal to

$$3^{21} - 3^{20} - 3^{20} + 3^{19} = 4 \cdot 3^{19}.$$

Because there are possibly minimal polynomials in S that induce the same polynomial modulo 27, we now count the subset of non-equivalent minimal polynomials in S by considering an equivalence relation on S. For two vectors, $\mathbf{z}$ and $\mathbf{z}'$ in S, we say that $\mathbf{z} \sim \mathbf{z}'$ if two polynomials, $f_{\mathbf{z}}$ and $f_{\mathbf{z}'}$, associated with them induce the same minimal polynomial, where $f_{\mathbf{z}}(x) = 1 + x + H_{\mathbf{z}}(x)$ and $f_{\mathbf{z}'}(x) = 1 + x + H_{\mathbf{z}'}(x)$ as in (5.17). Then, it is obvious to check that $\sim$ is an equivalence relation on S. To count the equivalence class of any vector, $\mathbf{z}$, we start with the congruence,

$$1 + x + H_{\mathbf{z}}(x) \equiv 1 + x + H_{\mathbf{z}'}(x) \pmod{27},$$

which immediately gives:

$$\frac{1}{3}H_{\mathbf{z}}(x) \equiv \frac{1}{3}H_{\mathbf{z}'}(x) \pmod 9. \tag{5.19}$$

Setting $Z = (Z_0, \ldots, Z_5, E_6, E_7, E_8, Z_6, Z_7, Z_8) := \mathbf{z} - \mathbf{z}'$, we substitute $x = 0, \ldots, 8$ into the congruence equation in (5.19) to obtain the system of linear equations modulo 9 in terms of the Z_i's and E_i's. Because we work over the

ring, $\mathbf{Z}/9\mathbf{Z}$, the row echelon form of the resulting coefficient matrix is given by the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 6 & 0 & 3 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 7 & 3 & 0 & 3 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \end{pmatrix} \tag{5.20}$$

From the echelon form in (5.20), we yield the following trivial relations:

$$Z_0 = 0; E_6 = 0; E_7 = 0; E_8 = 0$$

since $Z_i \in \mathbf{Z}/9\mathbf{Z}$ and $E_i \in \mathbf{Z}/3\mathbf{Z}$. With these relations, some non-trivial relations are also given:

$$\begin{gathered} Z_1 + Z_3 + Z_5 + 3Z_7 \equiv 0 \pmod 9; \\ Z_2 + Z_4 + 3Z_6 + 3Z_8 \equiv 0 \pmod 9; \\ 3Z_3 \equiv 0 \pmod 9; \\ 3Z_4 \equiv 0 \pmod 9; \\ 3Z_5 \equiv 0 \pmod 9. \end{gathered}$$

From these relations, we observe that the minimal conditions for f in S are invariant.

Writing $Z_i = 3w_i$, where $w_i \in \mathbf{Z}/3\mathbf{Z}$ for $1 \leq i \leq 5$, and $Z_i = w_i + 3d_i$, where $w_i, d_i \in \mathbf{Z}/3\mathbf{Z}$ for $i = 6, 7, 8$, from the above relations, we obtain

$$\begin{aligned} w_1 + w_3 + w_5 + w_7 &\equiv 0 \pmod 3; \\ w_2 + w_4 + w_6 + w_8 &\equiv 0 \pmod 3. \end{aligned} \tag{5.21}$$

Because all w_i run over $\mathbf{Z}/3\mathbf{Z}$, there are exactly 3^6 choices for the vectors, $[w_1, w_2, \ldots, w_8]$, satisfying the relations in (5.21). Thus, we conclude that the number of vectors Z is 3^9; thus, the equivalence class of the coefficient vector, $\mathbf{z}$ in S, has cardinality $4 \cdot 3^{19}/3^9 = 4 \cdot 3^{10}$. Therefore, the number of non-equivalent minimal polynomials in S is $4 \cdot 3^{10}$, as required. Thus, the proof is complete. □

6. Minimal polynomials for arbitrary primes, $p \geq 5$

It is of great interest to give a complete description of minimal polynomials having integer coefficients modulo any positive composite. Using the Chinese remainder theorem, this task is reduced to classifying transitive (minimal) polynomials modulo any power of a fixed prime number p. From the previous sections, we completed this work for cases where $p = 2$ or $p = 3$. Herein, we work over $\mathbf{Z}_p[x]$ for arbitrary primes $p \geq 5$.

6.1. Description of minimal polynomials of degree $\leq 2p-1$

The minimal criterion of polynomials in $\mathbf{Z}_p[x]$ can be developed by the following well-known result, which follows from Propositions 2.4 and 2.5.

Proposition 6.1. *A polynomial, $f \in \mathbf{Z}_p[x]$, is minimal if and only if the following conditions are satisfied*:

(i) *f is transitive modulo p;*
(ii) *$(f^p)'(0) \equiv 1 \pmod{p}$; and*
(iii) *$f^p(0) \in p\mathbf{Z}_p \setminus p^2\mathbf{Z}_p$.*

By reduction with δ from Theorem 3.1, we first restrict ourselves to polynomials in $\mathbf{Z}_p[x]$ of degree $\leq 2p-1$ and give a complete description of all minimal polynomials of degree $2p-1$ at most, with integer coefficients in the ring, $\mathbf{Z}/p^2\mathbf{Z}$.

We are now in a position to prove Theorem 6.2 that shows the structure of minimal polynomials in the set, $R(p^2)$.

Theorem 6.2. (1) *A polynomial $f \in \mathbf{Z}/p^2\mathbf{Z}[x]$ is minimal in $R(p^2)$ if and only if*

$$f(x) = f_0(x) + pf_1(x),$$

where

(i) *$f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in \mathbf{Z}/p\mathbf{Z}[x]$ is a transitive polynomial modulo p of degree $2p-1$ at most, whose coefficient column vector, $[e_0, \ldots, e_{2p-1}]^t$, is a unique solution to the linear system of the form,*

$$M\mathbf{x} \equiv \mathbf{b} \pmod{p},$$

where the coefficient matrix M is given by (6.6)*, and $\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t$ in* (6.3) *is a given constant vector that is chosen among $(p-1)!(p-1)^{p-1}$ choices satisfying conditions* (i) *and* (ii) *of Proposition 6.1.*

(ii) *the coefficient row vector, $[z_0, \ldots, z_{2p-1}]$ of $f_1(x) = \sum_{i=0}^{2p-1} z_i x^i \in \mathbf{Z}/p\mathbf{Z}[x]$, satisfies the non-vanishing modulo p of the linear polynomial l*:

$$l(z_0, \ldots, z_{2p-1}) \not\equiv 0 \pmod{p},$$

where $l(z_0, \ldots, z_{2p-1})$ is given explicitly by the formula:

$$l(z_0, \ldots, z_{2p-1}) = \frac{1}{p} f_0^p(0) + \frac{1}{f_0'(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)), \tag{6.1}$$

where, for $1 \leq i \leq p-2$,

$$w_i = \prod_{j=i+1}^{p-1} f_0'(f_0^j(0)) \text{ and } w_{p-1} = 1. \tag{6.2}$$

(2) $\#R(p^2) = (p-1)!(p-1)^p p^{p-1}$.

Proof. For $f(x) = a_0 + a_1x + \cdots + a_{2p-1}x^{2p-1} \in \mathbf{Z}/p^2\mathbf{Z}[x]$, a polynomial of degree $2p-1$ at most, we set the constants, $B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}$, as follows:

$$\begin{aligned} a_0 &= B_0; \\ a_1 + a_p + a_{2p-1} &= B_1; \\ a_2 + a_{p+1} &= B_2; \\ &\vdots \\ a_{p-1} + a_{2p-2} &= B_{p-1}; \\ a_1 &= D_0; \\ \sum_{i=1}^{2p-1} ia_i &= D_1; \\ &\vdots \\ \sum_{i=1}^{2p-1} i(p-1)^{i-1}a_i &= D_{p-1}. \end{aligned} \tag{6.3}$$

Note that, because $x^p \equiv x \pmod{p}$, the polynomial, f, is reduced modulo p to

$$f(x) \equiv B_0 + B_1x + \cdots + B_{p-1}x^{p-1}. \tag{6.4}$$

Furthermore, $f'(i) = D_i$ for each $0 \le i \le p-1$. We next consider (6.3) as a linear system in variables, $\mathbf{x} = [a_0, \ldots, a_{2p-1}]^t$, for a given constant column vector, $\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t$ modulo p, satisfying conditions (i) and (ii) of Proposition 6.1:

$$M\mathbf{x} \equiv \mathbf{b} \pmod{p}, \tag{6.5}$$

where M is a $2p \times 2p$ coefficient matrix explicitly given by the following form:

$$M = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & p-1 & p & \cdots & 2p-1 \\ 0 & 1 & 2\cdot 2 & \cdots & (p-1)\cdot 2^{p-2} & p\cdot 2^{p-1} & \cdots & (2p-1)\cdot 2^{2p-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & 2\cdot(p-1) & \cdots & (p-1)\cdot(p-1)^{p-2} & p\cdot(p-1)^{p-1} & \cdots & (2p-1)\cdot(p-1)^{2p-2} \end{pmatrix} \tag{6.6}$$

It is an interesting exercise to verify that the matrix M modulo p is invertible. Indeed, one can use the row operations and Fermat's little theorem to show that the reduced row-echelon form of M is the identity matrix by deriving the Vandermonde submatrix. The invertibility of M modulo p implies that the

solution to the linear system in (6.5) is unique whenever a constant column vector, $\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t$ modulo p, is selected appropriately.

Let us now count the number of constant column vectors $\mathbf{b}$ of the linear system in (6.5), satisfying conditions (i) and (ii) of Proposition 6.1. Because the reduced function of f in (6.4) turns out to be a transitive polynomial modulo p from condition (i) of Proposition 6.1, it is easily seen that the first p entries, $[B_0, B_1, \ldots, B_{p-1}] \bmod p$, of $\mathbf{b}$ should be coefficients of a transitive polynomial modulo p, which induces a full-cycle permutation on the finite field $\mathbf{Z}_p/p\mathbf{Z}_p$; hence, such a permutation is called a *transitive* one. Since there are exactly $(p-1)!$ transitive permutations on $\mathbf{Z}_p/p\mathbf{Z}_p$, by the Lagrange interpolation formula in (6.19), there are the same number of transitive polynomials of degree $\leq p$ modulo p. Therefore, there are exactly $(p-1)!$ choices for the coefficient vectors, $[B_0, B_1, \ldots, B_{p-1}] \bmod p$, that correspond to transitive polynomials modulo p. Simultaneously, the second p entries, $[D_0, D_1, \ldots, D_{p-1}] \bmod p$, of the constant vector to be chosen, $\mathbf{b}$, should satisfy condition (ii) of Proposition 6.1:

$$(f^p)'(0) \equiv f'(0) \cdot f'(1) \cdots f'(p-1) \equiv D_0 \cdot D_1 \cdots D_{p-1} \equiv 1 \pmod{p}.$$

From this congruence, there are exactly $(p-1)^{p-1}$ choices for such vectors, $[D_0, D_1, \ldots, D_{p-1}] \bmod p$. Taken together, there are exactly $(p-1)!(p-1)^{p-1}$ choices for the constant vectors,

$$\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t \bmod p$$

such that conditions (i) and (ii) of Proposition 6.1 are satisfied simultaneously. See Remark 6.6 for more details on this.

Let $E = [e_0, \ldots, e_{2p-1}] \bmod p$ be a unique solution to the linear system in (6.5) for a constant vector, $\mathbf{b}$, which is chosen from $(p-1)!(p-1)^{p-1}$ choices. To a solution vector, E, we associate a polynomial,

$$f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in \mathbf{Z}/p\mathbf{Z}[x].$$

Then, $f(x) \equiv f_0(x) \pmod{p}$ and $f'(x) \equiv f_0'(x) \pmod{p}$. Next, using f_0, it remains to find a simpler condition equivalent to condition (iii) of Proposition 6.1. To do so, we first derive the following congruence with $a_0 = e_0 + pz_0$:

$$\frac{1}{p} f^p(0) \equiv \frac{1}{p} f^{p-1}(e_0) + \frac{1}{f_0'(0)} z_0 \pmod{p}. \tag{6.7}$$

Indeed, the Taylor theorem yields

$$f^2(0) = f(e_0 + pz_0) \equiv f(e_0) + pz_0 f'(e_0) \equiv f(e_0) + pz_0 f_0'(e_0) \pmod{p^2}.$$

Similarly,

$$f^3(0) \equiv f(f(e_0) + pz_0 f_0'(e_0)) \equiv f^2(e_0) + pz_0 f_0'(e_0) f_0'(f_0(e_0)) \pmod{p^2}.$$

Continuing in this fashion, we get

$$f^p(0) \equiv f^{p-1}(e_0) + pz_0 f_0'(e_0) f_0'(f_0(e_0)) \cdots f_0'(f_0^{p-2}(e_0)) \pmod{p^2}.$$

Since $\prod_{i=0}^{p-1} f'(i) \equiv \prod_{i=0}^{p-1} f_0'(i) \equiv 1 \pmod p$, because $f \equiv f_0 \pmod p$ is transitive modulo p, and f satisfies condition (ii), it gives the following congruence:

$$f^p(0) \equiv f^{p-1}(e_0) + \frac{1}{f_0'(0)} p z_0 \pmod{p^2}.$$

Thus, division by p yields a desired congruence in (6.7).

To find a simpler formula for $f^p(0)$, we proceed a step further to derive a formula equivalent to $f^{p-1}(e_0)$ modulo p^2. To this end, we write $a_i = e_i + pz_i$ $(0 \le i \le 2p-1)$ to decompose f into a sum of two polynomials:

$$f(x) = f_0(x) + p f_1(x),$$

where

$$f_1(x) = \sum_{i=0}^{2p-1} z_i x^i \in \mathbf{Z}/p\mathbf{Z}[x].$$

A task here is to find conditions on z_i's modulo p, equivalently on a_i modulo p^2, so that f is a transitive polynomial modulo p^2. Thus, f is minimal. This can be done because we know the polynomial, f_0, from scratch. Therefore, the decomposition of f can be used to compute $f^{p-1}(e_0)$ modulo p^2. First, the Taylor theorem gives

$$\begin{aligned} f^2(e_0) &\equiv f(f_0(e_0) + p f_1(e_0)) \equiv f(f_0(e_0)) + p f_1(e_0) f'(f_0(e_0)) \pmod{p^2} \\ &\equiv f_0^2(e_0) + p f_1(f_0(e_0)) + p f_1(e_0) f_0'(f_0(e_0)) \pmod{p^2}. \end{aligned}$$

Once again

$$\begin{aligned} f^3(e_0) &\equiv f(f_0^2(e_0) + p f_1(f_0(e_0)) + p f_1(e_0) f_0'(f_0(e_0))) \\ &\equiv f_0^3(e_0) + p f_1(f_0^2(e_0)) + (p f_1(f_0(e_0)) + p f_1(e_0) f_0'(f_0(e_0)))\, f_0'(f_0^2(e_0)) \\ &\equiv f_0^3(e_0) + p f_1(f_0^2(e_0)) + p f_1(f_0(e_0)) f_0'(f_0^2(e_0)) \\ &\quad + p f_1(e_0) f_0'(f_0(e_0)) f_0'(f_0^2(e_0)) \pmod{p^2}. \end{aligned}$$

Iterating this process, we have modulo p^2,

$$\begin{aligned} f^{p-1}(e_0) \equiv\ & f_0^{p-1}(e_0) + p f_1(f_0^{p-2}(e_0)) + p f_1(f_0^{p-3}(e_0)) f_0'(f_0^{p-2}(e_0)) \\ & + p f_1(f_0^{p-4}(e_0)) f_0'(f_0^{p-2}(e_0)) f_0'(f_0^{p-3}(e_0)) + \cdots \\ & + p f_1(f_0(e_0) f_0'(f_0^2(e_0)) f_0'(f_0^3(e_0)) \cdots f_0'(f_0^{p-2}(e_0) \\ & + p f_1(e_0) f_0'(f_0(e_0)) f_0'(f_0^2(e_0)) \cdots f_0'(f_0^{p-2}(e_0)). \end{aligned}$$

Setting $w_i = \prod_{j=i}^{p-2} f_0'(f_0^j(e_0)) = \prod_{j=i+1}^{p-1} f_0'(f_0^j(0))$ for $1 \le i \le p-2$, and $w_{p-1} = 1$, it is equal to

$$f^{p-1}(e_0) \equiv f_0^{p-2}(e_0) + p \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p^2}. \tag{6.8}$$

From (6.7) and (6.8), the formula for $\frac{1}{p}f^p(0)$ in condition (iii) of Proposition 6.1 is expressed explicitly in terms of f_0 and f_1:

$$\frac{1}{p}f^p(0) \equiv \frac{1}{p}f_0^p(0) + \frac{1}{f_0'(0)}z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p}. \tag{6.9}$$

Henceforth, the right-hand side of (6.9) is denoted by $l(z_0, \ldots, z_{2p-1})$. From the polynomial, f_1, it turns out that $l(z_0, \ldots, z_{2p-1})$ is a polynomial in variables, $z_0, \ldots, z_{2p-1}$, with coefficients in $\mathbf{Z}/p\mathbf{Z}$, of degree 1 at most. Finally, by means of Lemma 6.3 below, the condition equivalent to condition (iii) is determined by the non-vanishing modulo p of a linear polynomial l in (6.1) or (6.9):

$$l(z_0, \ldots, z_{2p-1}) \not\equiv 0 \pmod{p}.$$

Thus, we complete the proof of the first part of Theorem 6.2.

Lemma 6.3. *$l(z_0, \ldots, z_{2p-1})$ is a linear polynomial.*

Proof. Note that $l(z_0, \ldots, z_{2p-1})$ is a polynomial of degree 1 at most in each variable, because it is observed from both (6.1) and the polynomial representation of f_1 that l is of the form

$$l(z_0, \ldots, z_{2p-1}) = \frac{1}{p}f_0^p(0) + (\frac{1}{f_0'(0)} + \sum_{i=1}^{p-1} w_i)z_0 + \sum_{j=1}^{2p-1}\left(\sum_{i=1}^{p-1}(f_0^i(0))^j w_i\right) z_j.$$

The result now follows by showing that $l(z_0, \ldots, z_{2p-1})$ has a non-vanishing coefficient of variable z_j for some $1 \le j \le p-1$. Suppose that all (linear) coefficients of variables $z_1, \ldots, z_{p-1}$ in the above expansion of $l(z_0, \ldots, z_{2p-1})$ are 0 modulo p. Then, we will obtain a homogeneous linear system in variables $w_1, \ldots, w_{p-1}$, whose coefficient matrix is of the Vandermonde related to the $p-1$ distinct values, $f_0(0), \ldots, f_0^{p-1}(0)$ modulo p. The invertibility of the Vandermonde matrix implies that the solution vector, $[w_1, \ldots, w_{p-1}]$, is trivial, which contradicts that the w_i's are all non-zero modulo p from condition (ii) of Proposition 6.1 or Proposition 2.2. □

Let us now prove part (2) of Theorem 6.2 using Lemma 6.3. For a fixed constant column vector, $\mathbf{b}$, out of $(p-1)!(p-1)^{p-1}$ choices, we need to count the set of non-equivalent minimal polynomials in $R(p^2)$ that correspond to all coefficient vectors, $[z_0, \ldots, z_{2p-1}]$ mod p, satisfying the condition, $l(z_0, \ldots, z_{2p-1}) \not\equiv 0 \pmod{p}$. For this, we consider the set,

$$S := \{[z_0, \ldots, z_{2p-1}] \in (\mathbf{Z}/p\mathbf{Z})^{2p} \mid l(z_0, \ldots, z_{2p-1}) \not\equiv 0 \pmod{p}\}.$$

Then, owing to Lemma 6.3, S is of cardinality $(p-1)p^{2p-1}$ by counting a complementary set. For $\mathbf{z} = [z_0, \ldots, z_{2p-1}]$ and $\mathbf{z}' = [z_0', \ldots, z_{2p-1}']$ in S, we define a relation $\mathbf{z} \sim \mathbf{z}'$ on the set S, if they induce the same minimal polynomial, $f \in R(p^2)$, which has the decomposition,

$$f = f_0 + pf_{1,\mathbf{z}} \equiv f_0 + pf_{1,\mathbf{z}'} \pmod{p^2}, \tag{6.10}$$

where $f_{1,\mathbf{z}}(x) = \sum_{i=0}^{2p-1} z_i x^i$ and $f_{1,\mathbf{z}'}(x) = \sum_{i=0}^{2p-1} z'_i x^i$. It is easy to check that $\sim$ is an equivalence relation on S. Because $x^p \equiv x \pmod p$, $f_{1,\mathbf{z}}(x)$ and $f_{1,\mathbf{z}'}(x)$ are reduced to the polynomial, $\sum_{i=0}^{p-1} B_i x^i$ of the form in (6.4), the congruence in (6.10) is equivalent to

$$\sum_{i=0}^{p-1} B_i(\mathbf{z}) x^i \equiv \sum_{i=0}^{p-1} B_i(\mathbf{z}') x^i \pmod p, \tag{6.11}$$

where $B_i(\mathbf{v})$ denotes the coefficient obtained by replacing elements defining B_i with entries of the vector, $\mathbf{v}$. It is easily seen that the congruence (6.11) is equivalent to stating that $\mathbf{z} - \mathbf{z}'$ lies in the null space of the matrix, T, where T is the upper $p \times 2p$ submatrix of M in (6.6). Because T has rank p, the nullity of T is p, so that the set of equivalence classes on S has cardinality $(p-1)p^{2p-1}/p^p = (p-1)p^{p-1}$. Thus, we conclude that, for each $\mathbf{b}$, there are exactly $(p-1)p^{p-1}$ non-equivalent minimal polynomials. Thus, $\#R(p^2) = (p-1)!(p-1)^p p^{p-1}$. The proof of part (2) of Theorem 6.2 is complete, thereby finishing the proof of part (2) of Theorem 3.1. □

Remark 6.4. The method described in Theorem 6.2 can be compared with those proposed by Anashin [3, Page 296] and the present author [10]. In Anashin's work, one needed to calculate the interpolation polynomials, f_φ and $f_{\varphi,\psi}$ in [3], and to test whether they were transitive modulo p^2. In the method of [10], one used the minimal conditions of a polynomial represented as the binomial coefficient polynomials. In these respects, the proposed method is more natural and efficient than the existing methods, and it applies to polynomials of any degree, as in Subsection 6.2.

We now illustrate the procedure of Theorem 6.2 with some examples constructed from MATLAB computations.

Example 1. Let φ =(1 3 2 4 5 6 0) be a single-cycle permutation on $\mathbf{F}_7$. By the Lagrange interpolation formula in (6.19) or [12, Equation 7.1], the interpolation polynomial, $f_\varphi(x) = 3x^5 + 6x^4 + 3x^3 + 5x^2 + 6x + 1$ is determined. Thus, the vector $[B_0, \ldots, B_6] \bmod 7 = [1, 6, 5, 3, 6, 3, 0]$ is found. For a well-chosen vector, $[B_0, \ldots, B_6, D_0, \ldots, D_6] \bmod 7 = [1, 6, 5, 3, 6, 3, 0, 1, 1, 1, 1, 1, 6, 6]$, we find a unique solution modulo 7, $[1, 1, 6, 0, 6, 5, 1, 2, 6, 3, 0, 5, 6, 3]$, to the linear system in (6.5), which gives

$$f_0(x) = 3x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 6x^4 + 6x^2 + x + 1.$$

From f_0, we obtain $f_0^7(0) \equiv 14 \pmod{7^2}$, $[f'_0(0), f'_0(1), \ldots, f'_0(6)] \bmod 7 = [1, 1, 1, 1, 1, 6, 6]$ and $[w_1, w_2, \ldots, w_6] \bmod 7 = [1, 1, 1, 1, 6, 1]$. Hence, we obtain $f_1 = \sum_{i=0}^{13} z_i x^i$, whose coefficients satisfy the minimal condition in (6.1):

$$\begin{aligned} l(z_0, \ldots, z_{13}) = {} & 5z_0 + 4z_1 + 6z_2 + 2z_3 + 3z_4 + z_5 + 4z_6 + 4z_7 \\ & + 6z_8 + 2z_9 + 3z_{10} + z_{11} + 4z_{12} + 4z_{13} + 2 \not\equiv 0 \pmod 7. \end{aligned}$$

Thus, by taking a vector, $[z_0, \ldots, z_{13}] \bmod 7 = [5,0,0,2,2,0,0,0,0,0,0,0,0,0]$, satisfying this condition, we obtain the minimal polynomial:

$$\begin{aligned} f(x) &= f_0 + 7f_1 \\ &= 3x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 20x^4 \\ &\quad + 14x^3 + 6x^2 + x + 36, \end{aligned}$$

whose single-cycle orbit modulo 7^2 is given by

$$\begin{aligned} &(0, 36, 45, 9, 39, 33, 27, 14, 1, 10, 23, 4, 47, 13, 28, 15, 24, 37, 18, 12, 48, 42, 29, 38, \\ &2, 32, 26, 34, 7, 43, 3, 16, 46, 40, 20, 21, 8, 17, 30, 11, 5, 6, 35, 22, 31, 44, 25, 19, 41). \end{aligned}$$

For another minimal polynomial, take a vector, $[z_0, \ldots, z_{13}] \bmod 7 = [1,1,1,0, 1,0,0,0,0,0,0,0,0,1]$, that satisfies the same minimal condition and obtain

$$f(x) = 10x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 13x^4 + 13x^2 + 8x + 8,$$

whose single-cycle orbit modulo 7^2 is given by

$$\begin{aligned} &(0, 8, 38, 16, 46, 40, 41, 21, 29, 10, 37, 18, 12, 20, 42, 1, 31, 9, 39, 33, 48, 14, 22, 3, \\ &30, 11, 5, 27, 35, 43, 24, 2, 32, 26, 6, 7, 15, 45, 23, 4, 47, 34, 28, 36, 17, 44, 25, 19, 13). \end{aligned}$$

6.2. Description of minimal polynomials of any degree

Herein, we provide a method of finding the minimal conditions of a polynomial, $f \in \mathbf{Z}_p[x]$, of any degree in terms of its coefficients, as in the case with $p = 3$.

For $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbf{Z}_p[x]$, a polynomial of degree $d \geq 2p$, we set the constants, $B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}$, as follows:

$$\begin{aligned} a_0 &= B_0; \\ \sum_{i \equiv 1 \pmod{p-1}} a_i &= B_1; \\ \sum_{i \equiv 2 \pmod{p-1}} a_i &= B_2; \\ &\vdots \\ \sum_{0 < i \equiv 0 \pmod{p-1}} a_i &= B_{p-1}; \\ a_1 &= D_0; \\ \sum_{i=1}^{d} i a_i &= D_1; \\ &\vdots \end{aligned} \tag{6.12}$$

$$\sum_{i=1}^{d} i(p-1)^{i-1}a_i = D_{p-1}.$$

As in the case for polynomials of degree at most $2p-1$, the equations in (6.12) will be considered a linear system in variables $\mathbf{x} = [a_0, \ldots, a_d]^t$ for $\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t$ modulo p, a given constant column vector:

$$\tilde{M}\mathbf{x} \equiv \mathbf{b} \pmod{p}, \tag{6.13}$$

where $\tilde{M}$ is the $2p\times(d+1)$ coefficient matrix of the form, $\tilde{M} = [MM']$, where M is the $2p\times 2p$ matrix in (6.6), and M' is the remaining $2p\times(d-2p-1)$ submatrix. We observe that $\tilde{M}$ modulo p has a certain pattern. Indeed, all columns except for the first column of the submatrix corresponding to B_i appear periodically with periodic length $p-1$, as does the submatrix corresponding to D_i's with periodic length $p(p-1)$, because if $i \equiv j \pmod{p(p-1)}$, then $i\alpha^{i-1} \equiv j\alpha^{j-1} \pmod{p}$ for $\alpha \in \{1, \ldots, p-1\}$. For this reason, we may assume that the degree of f is $d = p(p-1)k + 2p - 1$, if necessary, by adding the terms whose coefficients are zero. Note that there are exactly $(p-1)!(p-1)^{p-1}$ choices for a constant column vector, $\mathbf{b}$, that satisfy conditions (i) and (ii) of Proposition 6.1, as shown in the previous section. For such a well-chosen $\mathbf{b}$, the reduced row echelon form of the augmented coefficient matrix, $[\tilde{M}|\mathbf{b}]$, is given by the matrix of the form,

$$[I_{2p}R|E],$$

where I_{2p} is the $2p \times 2p$ identity matrix, and R and E is the reduced part of M' and $\mathbf{b}$, respectively. Owing to the pattern of $\tilde{M}$, $R = (R_{ij})$ has a certain pattern that the first $p(p-1)$ column vectors appear exactly k times in the column order. Thus, the parametric representations to the concerned linear system are given by the equations of the following form:

$$\begin{aligned}
a_0 &= e_0 + pz_0;\\
a_1 &= e_1 + pz_1;\\
a_2 &= e_2 + pz_2 - \sum_{j\in J_2} a_j R_{2j};\\
&\vdots\\
a_{2p-1} &= e_{2p-1} + pz_{2p-1} - \sum_{j\in J_{2p-1}} a_j R_{(2p-1)j},
\end{aligned} \tag{6.14}$$

where $[e_0, \ldots, e_{2p-1}]^t = E$ and for each $0 \le i \le 2p-1$, the index set, J_i, is defined as $J_i = \{j \mid 2p+1 \le j \le d+1 \text{ and } R_{ij} \not\equiv 0 \pmod{p}\}$. Note that J_i is the empty set for $i = 0, 1$.

Substituting these relations in (6.14) into $f(x)$ yields

$$f(x) = f_0(x) + pf_1(x), \tag{6.15}$$

where $f_0(x) = \sum_{j=0}^{2p-1} e_j x^j$, and

$$f_1(x) = \sum_{j=0}^{2p-1} z_j x^j + \frac{1}{p} \sum_{j=2p}^{d} a_j h_j(x), \tag{6.16}$$

where h_j is a polynomial obtained by collecting the non-zero terms whose coefficient is a_j. Because the polynomial f_0 is transitive modulo p, f_0 and satisfies the following properties:

$$f(x) \equiv f_0(x) \pmod{p}; \; f'(x) \equiv f_0'(x) \pmod{p}.$$

Hence, as in (6.9), in order for f to be minimal, its minimal condition should be satisfied with the non-vanishing modulo p^2 of

$$f^p(0) \equiv f_0^p(0) + \frac{1}{f_0'(0)} p z_0 + p \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p^2}, \tag{6.17}$$

where $w_i = \prod_{j=i+1}^{p-1} f_0'(f_0^j(0))$ for $1 \le i \le p-2$, and $w_{p-1} = 1$, as in (6.2). Substituting pz_i in (6.14) into (6.17) gives the minimal condition for f, which are expressed in terms of its coefficients. As in (6.1), from (6.17), the minimal condition of f is also given by the non-vanishing modulo p of the linear polynomial,

$$l(z_0, \ldots, z_d) = \frac{1}{p} f_0^p(0) + \frac{1}{f_0'(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p}, \tag{6.18}$$

where w_i is given as above. The discussion above then summarizes the following result:

Theorem 6.5. *A polynomial $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbf{Z}/p^2\mathbf{Z}[x]$ is minimal if and only if*

$$f(x) = f_0(x) + p f_1(x),$$

where

(i) *$f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in \mathbf{Z}/p\mathbf{Z}[x]$ is determined as in* (i) *of Theorem 6.2, and*

(ii) *the polynomial $f_1(x)$ in* (6.16) *satisfies the non-vanishing modulo p of the linear polynomial $l(z_0, \ldots, z_d)$ in* (6.18).

Remark 6.6. Every minimal polynomial, $f \in \mathbf{Z}_p[x]$, induces a permutation, φ on $\mathbf{F}_p$, of full length; hence, the task of finding a minimal polynomial of any degree is to first find the coefficient vector, $[B_0, \ldots, B_{p-1}] \pmod{p}$ of the reduced function modulo p, f_φ, which is obtained by the Lagrange interpolation formula [12]:

$$f_\varphi(x) = \sum_{\alpha \in \mathbf{F}_p} \varphi(\alpha)(1 - (x - \alpha)^{p-1}). \tag{6.19}$$

Indeed, with this formula, for each j, B_j is given by

$$B_j = -\sum_{\alpha \in \mathbf{F}_p} \varphi(\alpha)\alpha^{p-1-j}.$$

Next, we select a vector, $[D_0, \ldots, D_{p-1}] \pmod p$, satisfying condition (ii) of Proposition 6.1, which can be easily done by finding the inverse modulo p, of the product, $D_0 \cdots D_{p-2}$, after these $p-1$ non-zero elements are randomly chosen.

Remark 6.7. One can find a complete list of all possible minimal conditions for polynomials $f \in \mathbf{Z}_p[x]$ in terms of their coefficients, provided that a list of all $(p-1)!(p-1)^{p-1}$ constant vectors, $\mathbf{b} = [B_0, \ldots, B_{p-1}, D_0, \ldots, D_{p-1}]^t$ modulo p, satisfying conditions (i) and (ii) of Proposition 6.1, is completely found.

Remark 6.8. It is crucial to decide if a given polynomial, $g \in \mathbf{Z}_p[x]$, is minimal. To this end, we use Theorem 3.1 to find the remainder, $f(x)$ of g, via reduction with δ. Then, using Hermite's criterion [12, Theorem 7.4.] or Theorem 6.9, we determine whether or not $f(x)$ is bijective modulo p, and then we decide if it is of a full cycle. If so, we must check whether or not f satisfies condition (ii) of Proposition 6.1 by finding its derivatives at $x = 0, \ldots, p-1$. If f passes through this process, one can find the f_0 by solving for the linear system in (6.5) for an obtained vector, $\mathbf{b}$. With f_0, after finding f_1, we can check if f satisfies the minimal condition in (6.1). If so, f (hence g) is declared to be minimal.

We state Hermite's criterion for permutation polynomials over a finite prime field, $\mathbf{F}_p$.

Theorem 6.9 (Hermite's Criterion)**.** *Let $\mathbf{F}_p$ be a prime field. Then, $f \in \mathbf{F}_p[x]$ is a permutation polynomial over $\mathbf{F}_p$ if and only if the following two conditions hold*:

(i) *f has exactly one root in $\mathbf{F}_p$; and*
(ii) *for each integer t with $1 \le t \le p-1$, the reduction of $f(x)^t \bmod (x^p - x)$ has degree $\le p-2$.*

Corollary 6.10. *If $d > 1$ is a divisor of $p-1$, then there is no minimal polynomial on $\mathbf{Z}_p$ of degree d.*

Proof. Suppose such a minimal polynomial exists, then it is a permutation polynomial modulo p of full cycle. However, such a permutation polynomial does not exist from [12, Corollary 7.5] of Hermite's criterion. Thus, the proof is complete. □

Example 2. We use the method described above to find the minimal conditions of a polynomial of degree 29, $f(x) = \sum_{i=0}^{29} a_i x^i \in \mathbf{Z}_5[x]$, with a prescribed condition on $\mathbf{b} = [B_0, \ldots, B_4, D_0, \ldots, D_4]^t \bmod 5 = [2100014411]$. From the

reduced row echelon form of the augmented coefficient matrix in (6.13), the parametric representations are given by the following equations:

$$
\begin{aligned}
a_0 &= 2 + 5z_0;\\
a_1 &= 1 + 5z_1;\\
a_2 &= 3 + 5z_2 + a_{10} + 2a_{14} + 3a_{18} + 4a_{22};\\
a_3 &= 0 + 5z_3 + a_{11} + 2a_{15} + 3a_{19} + 4a_{23};\\
a_4 &= 1 + 5z_4 + a_{12} + 2a_{16} + 3a_{20} + 4a_{24};\\
a_5 &= 4 + 5z_5 + a_{13} + 2a_{17} + 3a_{21} + 4a_{25};\\
a_6 &= 2 + 5z_6 + 3a_{10} + 2a_{14} + a_{18} + 4a_{26};\\
a_7 &= 0 + 5z_7 + 3a_{11} + 2a_{15} + a_{19} + 4a_{27};\\
a_8 &= 4 + 5z_8 + 3a_{12} + 2a_{16} + a_{20} + 4a_{28};\\
a_9 &= 1 + 5z_9 + 3a_{13} + 2a_{17} + a_{21} + 4a_{29}.
\end{aligned}
\tag{6.20}
$$

Thus,

$$f(x) = f_0(x) + 5f_1(x),$$

where $f_0(x) = 2 + x + 3x^2 + x^4 + 4x^5 + 2x^6 + 4x^8 + x^9$, and

$$f_1(x) = \sum_{i=0}^{9} z_i x^i + \frac{1}{5}\sum_{i=10}^{29} a_i h_i(x),$$

where, for $2 \le i \le 5$,

$$
\begin{aligned}
h_{8+i}(x) &= x^i + 3x^{4+i} + x^{8+i},\\
h_{12+i}(x) &= 2x^i + 2x^{4+i} + x^{12+i},\\
h_{16+i}(x) &= 3x^i + x^{4+i} + x^{16+i}
\end{aligned}
$$

and $2 \le i \le 9$, $h_{20+i}(x) = 4x^i + x^{20+i}$. Because $f_0 \equiv 2 + x \pmod 5$, its orbit mod 5 is given by (0 2 4 1 3), and, because $[f_0'(0), f_0'(1), f_0'(2,)f_0'(3), f_0'(4)] \bmod 5 = [1, 4, 4, 1, 1]$, we have $[w_1, w_2, w_3, w_4] \bmod 5 = [4, 4, 1, 1]$. Hence, from (6.17), we get

$$f^5(0) \equiv 5 + 5f_1(0) + 5f_1(1) + 20f_1(2) + 5f_1(3) + 20f_1(4) \pmod{5^2}.$$

Because it is easy to compute $h_i(\alpha)$ modulo 5^2 for $0 \le \alpha \le 4$ and $i \ge 10$,

$$
\begin{aligned}
f^5(0) \equiv\ & 5a_{11} + 15a_{13} + 5a_{15} + 15a_{17} + 5a_{19} + 15a_{21} + 5a_{23} + 15a_{25} + 5a_{27}\\
& + 15a_{29} + 5z_0 + 15z_1 + 5z_3 + 15z_5 + 5z_7 + 15z_9 + 5 \pmod{5^2}.
\end{aligned}
$$

Substituting $5z_i$ in (6.20) into the above equation yields the minimal condition of f:

$$
\begin{aligned}
& a_0 + 3a_1 + a_3 + 3a_5 + a_7 + 3a_9 + a_{11} + 3a_{13} + a_{15} + 3a_{17} + a_{19}\\
& + 3a_{21} + a_{23} + 3a_{25} + a_{27} + 3a_{29} + 10 \not\equiv 0 \pmod{5^2}.
\end{aligned}
\tag{6.21}
$$

If we take $[a_0, \dots, a_{29}] = [2, 1, 26, 3, 28, 14, 19, 13, 29, 23, 0, 1, 2, 0, 3, 1, 2, 0, 3, 0, 3, 2, 2, 0, 3, 1, 2, 2, 3, 5]$ satisfying the conditions in (6.20) and (6.21), then, the minimal polynomial, f, of degree 29 is given by

$$\begin{aligned} f(x) = {} & 5x^{29} + 3x^{28} + 2x^{27} + 2x^{26} + x^{25} + 3x^{24} + 2x^{22} + 2x^{21} + 3x^{20} \\ & + 3x^{18} + 2x^{16} + x^{15} + 3x^{14} + 2x^{12} + x^{11} + 23x^9 + 4x^8 + 13x^7 \\ & + 19x^6 + 14x^5 + 3x^4 + 3x^3 + x^2 + x + 2, \end{aligned} \tag{6.22}$$

whose single-cycle orbit modulo 5^2 is determined by

$$(0, 2, 4, 16, 3, 20, 22, 9, 21, 23, 15, 17, 14, 1, 18, 10, 12, 19, 6, 13, 5, 7, 24, 11, 8).$$

As an illustration of Remark 6.8, let us show again that the polynomial in (6.22) is minimal. By dividing the polynomial by $\binom{x}{10}$, its remainder is reduced modulo 25 to

$$f(x) = 6x^9 + 24x^8 + +5x^7 + 2x^6 + 24x^5 + 21x^4 + 15x^3 + 3x^2 + 16x + 2.$$

From Theorem 6.2, f is decomposed as the sum, $f = f_0 + 5f_1$, where $f_0 = x^9 + 4x^8 + 2x^6 + 4x^5 + x^4 + 3x^2 + x + 2$, $f_1 = x^9 + 4x^8 + x^7 + 4x^5 + 4x^4 + 3x^3 + 3x$. Using this decomposition, by (6.1), the minimal condition of f is determined by the non-vanishing modulo 5 of $l(z_0, \dots, z_9) = z_0 + 1$. Because the coefficients of f_1 satisfy this condition, f is minimal, thus, so is the polynomial in (6.22).

We use the above minimality criterion to reprove the minimal conditions of polynomials over $\mathbf{Z}_p$ of a special form in [9, Theorem 1.1].

Corollary 6.11. *Let $f(x) = a_0 + a_1 x + \cdots + a_d x^d \in \mathbf{Z}_p[x]$ be a polynomial of degree $d \geq 1$ that satisfies the following system of relations*:

$$\begin{aligned} a_0 &\not\equiv 0 \pmod{p}; \\ a_1 &\equiv 1 \pmod{p}; \\ a_i &\equiv 0 \pmod{p} \text{ for } i \geq 2; \\ \sum_{i>0; i \equiv 0 \pmod{p-1}} & a_i/p \not\equiv a_0 \pmod{p}. \end{aligned}$$

Then, f is minimal.

Proof. From the assumption, writing $a_i = e_i + pz_i$ for all $0 \leq i \leq d$ with $0 < e_0 < p$, $e_1 = 1$, and $e_i = 0$ for $i \geq 2$, f is decomposed into a sum,

$$f = f_0 + pf_1,$$

where $f_0 = x + e_0$ and $f_1 = \sum_{i=0}^{d} z_i x^i \in \mathbf{Z}_p[x]$ is a polynomial of degree d. From Theorem 6.2, we may assume that $d \geq 2p$. Note that f_0 is a transitive linear polynomial modulo p, whose coefficient vector, $[e_0, 1, 0, \dots, 0]$ is a solution to the linear system, $\tilde{M}\mathbf{x} \equiv \mathbf{b} \pmod{p}$, in (6.13) for a chosen constant vector, $\mathbf{b} = [e_0, 1, 0, \dots, 0, 1, \dots, 1]^t$, the last p entries of which are all 1, because

$f' \equiv f'_0 = 1 \pmod{p}$. Furthermore, because $w_i = 1$ for all i, we compute the minimal condition, l of f, in (6.18) as follows:

$$\begin{aligned} l(z_0, \ldots, z_d) &= \sum_{j=1}^{p-1} f_1(je_0) + z_0 + e_0 \\ &= \sum_{j=1}^{p-1} \sum_{i=0}^{d} z_i (je_0)^i + z_0 + e_0 \\ &= \sum_{i=0}^{d} z_i \left(\sum_{j=1}^{p-1} (je_0)^i \right) + z_0 + e_0. \end{aligned}$$

Because je_0 are distinct modulo p for $1 \leq j \leq p-1$, by the well konwn fact that $\sum_{\alpha \in \mathbf{F}_p^*} \alpha^i = -1$ if $(p-1) \mid i$, and 0 otherwise [12, Lemma 7.3], we have

$$l(z_0, \ldots, z_d) \equiv - \sum_{i=1, (p-1)|i}^{d} z_i + e_0 \pmod{p}.$$

We conclude from Theorem 6.5 that f is minimal as long as $l(z_0, \ldots, z_d)$ is non-zero modulo p, which is equivalent to the last condition in the assumption. □

Corollary 6.12. *A linear polynomial, $f(x) = a_0 + a_1 x \in \mathbf{Z}_p[x]$, is minimal if and only if $a_0 \not\equiv 0 \pmod{p}$, and $a_1 \equiv 1 \pmod{p^{r_p}}$, where $r_p = 2$ if $p = 2$ and 1 otherwise.*

Proof. This result is well-known. See, for example, [7, Theorem 1] or [3, Theorem 4.36]. We give a simple and alternative proof using Theorem 6.2 for $p \geq 5$. The proof for $p = 2$ and 3 follows respectively from Lemma 4.1 and Corollary 5.4 cases (i) and (v). Thus, we treat only the cases, $p \geq 5$. It is simple to check from [3, Lemma 4.37] that f is transitive modulo p if and only if $a_0 \not\equiv 0 \pmod{p}$ and $a_1 \equiv 1 \pmod{p}$. We show here that these conditions are necessary and sufficient for the transitivity of f modulo p^2, being equivalent to the minimality of f. As in the proof of Corollary 6.11, f is decomposed into a sum, $f = f_0 + pf_1$, where $f_0 = x + e_0$, $f_1 = z_0 + z_1 x \in \mathbf{Z}_p[x]$. Then, f is minimal precisely when e_0 or a_0 is non-zero modulo p, because $l(z_0, z_1) = e_0$ for any values of z_0 and z_1. □

Corollary 6.13. *A polynomial, $f(x) = a_0 + a_1 x + a_2 x^2 \in \mathbf{Z}_p[x]$, is minimal if and only if one of the following occurs*:

(i) *For $p = 2$, $a_0 \equiv 1 \pmod{p}$, $a_2 \equiv 0 \pmod{p}$, $a_1 + a_2 \equiv 1 \pmod{p^2}$;*
(ii) *For $p \geq 3$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 \equiv 1 \pmod{p}$, $a_2 \equiv 0 \pmod{p}$.*

Proof. The proof is similar to that of Corollary 6.12, together with Proposition 2.2(iii) for the case, $p \geq 5$. □

Corollary 6.14. *A polynomial, $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 \in \mathbf{Z}_p[x]$, is minimal if and only if one of the following occurs*:

(i) *For* $p = 2$, $a_0 \equiv 1 \pmod{p}$, $a_1 \equiv 1 \pmod{p}$, $a_3 \equiv 2a_2 \pmod{p^2}$, $a_1 + a_2 \equiv 1 \pmod{p^2}$;
(ii) *For* $p = 3$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 - 1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{p}$, $a_2/p \not\equiv a_0 \pmod{p}$;
(iii) *For* $p \geq 5$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 - 1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{p}$.

Proof. We present case (iii) only, because cases (i) and (ii) follow from Corollary 4.4 and Corollary 5.4 cases (i) and (v), respectively . The sufficiency for case (iii) is immediate from Corollary 6.11. Conversely, the proof follows easily from the observation that $a_3 \equiv 0 \pmod{p}$. Suppose this is not the case. Then, we derive a contradiction by following the argument of [9, Proposition 3.2]. Indeed, by a change of variable, we see that the minimal polynomial, f, of degree 3 is conjugate modulo p^2 to a polynomial, $Q(x) = a_3x^3 + e_1x + e_0$, with $e_i \in \mathbf{Z}_p$. Then, Dickson's result [5] or [12, Table 7.1 on p. 352] forces us to obtain $e_1 = 0$, and $p \equiv 2 \pmod{3}$. Because Q is not minimal, neither is f. □

Corollary 6.15. *A polynomial,* $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 \in \mathbf{Z}_p[x]$, *is minimal if and only if one of the following occurs*:

(i) *For* $p = 2$, $a_0 \equiv 1 \pmod{p}$, $a_1 \equiv 1 \pmod{p}$, $a_3 \equiv 2a_2 \pmod{p^2}$, $a_1 + a_2 \equiv a_4 + 1 \pmod{p^2}$;
(ii) *For* $p = 3$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 - 1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{p}$, $(a_2 + a_4)/p \not\equiv a_0 \pmod{p}$;
(iii) *For* $p = 5$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 - 1 \equiv a_2 \equiv a_3 \equiv 0 \pmod{p}$, $a_4/p \not\equiv a_0 \pmod{p}$;
(iv) *For* $p \equiv 1 \pmod{3}$, $a_0 \not\equiv 0 \pmod{p}$, $a_1 - 1 \equiv a_2 \equiv a_3 \equiv a_4 \equiv 0 \pmod{p}$.

For all $p > 7$, *such that* $p \equiv 2 \pmod{3}$, *the conditions are only sufficient.*

Proof. The proof for cases (i) and (ii) is similar to that of Corollary 6.14. We first prove the necessity of $p = 5$, because its converse follows from Corollary 6.11. Now, it suffices to show that there is no minimal polynomial, f, satisfying $a_3 \not\equiv 0 \pmod{p}$. Suppose that it is not the case. Then, f modulo p is a permutation polynomial of degree 3 (with full cycle), and it is easily observed that $a_4 \equiv 0 \pmod{p}$. By Lagrange's interpolation formula, this polynomial f is reduced modulo p to one of all possible 20 permutation polynomials modulo p of degree 3, whose derivatives all have a root modulo p. Thus, we conclude that f is not minimal. For case (iv) with $p = 7$, we see through an exhaustive search that there is no minimal polynomial with either $a_4 \not\equiv 0 \pmod{7}$ or $a_4 \equiv 0 \pmod{7}$, and $a_3 \not\equiv 0 \pmod{7}$. Hence, the conditions provided are necessary and sufficient. For all primes, $p > 7$, we note that $a_4 \equiv 0 \pmod{7}$, otherwise Dickson's result [5] or [12, Table 7.1 on p. 352] forces $p = 7$. Additionally, if $a_3 \not\equiv 0 \pmod{7}$, then, Dickson's result again forces us to have $p \equiv 2 \pmod{3}$. Thus, the above conditions are only sufficient from Corollary 6.11. Otherwise, it is straightforward to see that they are necessary and sufficient. □

Remark 6.16. It is of interest to give a complete list of minimal polynomials in $\mathbf{Z}_p[x]$ of small primes, p, by using the method of Theorem 6.5.

Acknowledgements. This work was conceived from a question of F. Durand while I was participating in the workshop on 2019 Numeration and Substitution, which was held in the Erwin Schrödinger International Institute for Mathematics and Physics. I would like to thank him for his question and interest in my early work. I would also like to express gratitude to the referee for some suggestions, which improve the paper for clearer understanding.

References

[1] V. S. Anashin, *Uniformly distributed sequences of p-adic integers*, Math. Notes **55** (1994), no. 1-2, 109–133; translated from Mat. Zametki **55** (1994), no. 2, 3–46, 188. https://doi.org/10.1007/BF02113290

[2] V. S. Anashin, *Uniformly distributed sequences of p-adic integers*, Discrete Math. Appl. **12** (2002), no. 6, 527–590; translated from Diskret. Mat. **14** (2002), no. 4, 3–64.

[3] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, De Gruyter Expositions in Mathematics, 49, Walter de Gruyter & Co., Berlin, 2009. https://doi.org/10.1515/9783110203011

[4] D. L. DesJardins and M. E. Zieve, *Polynomial mappings mod* p^n, arXiv:math/0103046v1.

[5] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1896/97), no. 1-6, 65–120. https://doi.org/10.2307/1967217

[6] F. Durand and F. Paccaut, *Minimal polynomial dynamics on the set of* 3*-adic integers*, Bull. Lond. Math. Soc. **41** (2009), no. 2, 302–314. https://doi.org/10.1112/blms/bdp003

[7] A. Fan, M. Li, J. Yao, and D. Zhou, *Strict ergodicity of affine p-adic dynamical systems on* $\mathbb{Z}_p$, Adv. Math. **214** (2007), no. 2, 666–700. https://doi.org/10.1016/j.aim.2007.03.003

[8] A. Fan and L. Liao, *On minimal decomposition of p-adic polynomial dynamical systems*, Adv. Math. **228** (2011), no. 4, 2116–2144. https://doi.org/10.1016/j.aim.2011.06.032

[9] M. Javaheri and G. Rusak, *On transitive polynomials modulo integers*, Notes on Number Theory and Discrete Mathematics, Vol. **22** No. 2, (2016) 23–35.

[10] S. Jeong, *Ergodic functions over* $\mathbb{Z}_p$, J. Number Theory **232** (2022), 423–479. https://doi.org/10.1016/j.jnt.2021.01.026

[11] M. V. Larin, *Transitive polynomial transformations of residue class rings*, Discrete Math. Appl. **12** (2002), 141–154.

[12] R. Lidl and H. Niederreiter, *Finite fields*, second edition, Encyclopedia of Mathematics and its Applications, 20, Cambridge University Press, Cambridge, 1997.

[13] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*, J. Reine Angew. Math. **199** (1958), 23–34. https://doi.org/10.1515/crll.1958.199.23

[14] W. Nöbauer, *Zur Theorie der Polynomtransformationen und Permutationspolynome*, Math. Ann. **157** (1964), 332–342. https://doi.org/10.1007/BF01360874

[15] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Graduate Texts in Mathematics, 241, Springer, New York, 2007. https://doi.org/10.1007/978-0-387-69904-2

[16] Z. Yang, *Ergodic functions over* $\mathbb{F}_q[[T]]$, Finite Fields Appl. **53** (2018), 189–204. https://doi.org/10.1016/j.ffa.2018.06.004

[17] M. E. Zieve, *Cycles of polynomial mappings*, PhD thesis, UC Berkeley, 1996.

Sangtae Jeong
Department of Mathematics
Inha University
Incheon, 22212, Korea
Email address: stj@inha.ac.kr