Proceedings of the Conference on March 14 - International Day of Mathematics

Vuković, Mirjana, urednik; Nurkanović, Mehmed, urednik

2024-12-26

Academy of Sciences and Arts of Bosnia and Herzegovina

https://bastina.anubih.ba/handle/123456789/798

PROCEEDINGS OF THE CONFERENCE ON MARCH 14 – INTERNATIONAL DAY OF MATHEMATICS
Special Editions ANUBiH, Book CCXVI, OPMN Book 30
Sarajevo 2024, **p. 68–80** DOI: 10.5644/PI2024.216.09

ERGODICITY OF UNIFORMLY DIFFERENTIABLE FUNCTIONS MODULO p ON $\mathbb{Z}_p$ AND SOME CLASSES OF 1-LIPSCHITZ MEASURE PRESERVING FUNCTIONS ON $\mathbb{Z}_p$

JASMINA MUMINOVIĆ HUREMOVIĆ

ABSTRACT. Various applications in physics, cognitive science and cryptography often lead to the study of the behavior of dynamical systems on $\mathbb{Z}_p$. For example, in the theory of pseudorandom number generation, it is useful to have a mapping, defined on the set of integers, that gives large cycles modulo n for a given integer n . Given that minimal mappings have only one cycle of maximal length modulo p^n, for each n, good candidates are precisely minimal mappings in the set of p-adic integers (maps whose orbits are all dense).
In this paper we give theoretical research in the field of p-adic analysis, p-adic ergodic functions and dynamical systems defined on the set of p-adic integers $\mathbb{Z}_p$. In [5] it was shown that for 1-Lipschitz functions, which are measure preserving, the notions of minimality and ergodicity are equivalent. Guided by the results from the mentioned paper, here we give some results about the necessary and sufficient conditions for the ergodicity of uniformly differentiable functions modulo p on p-adic integers $\mathbb{Z}_p$. The class of uniformly differentiable functions modulo p includes the space of rational functions, so we also give the application of the obtained results to rational functions in $\mathbb{Z}_3$ and $\mathbb{Z}_5$. Finally, some classes of 1-Lipschitz functions that preserve measure on the group of p-adic integers $\mathbb{Z}_p$ are considered, and necessary and sufficient conditions for their ergodicity in terms of their Van der Put coefficients are established.

1. INTRODUCTION

We recall some facts about the ring of p-adic integers $\mathbb{Z}_p$. Let p be a fixed prime number. The p-adic ordinal or valuation of $0 \neq x \in \mathbb{Z}$ we define as

$$ord_p x = max\{r : p^r | x\} \geq 0.$$

If $a/b \in \mathbb{Q}$, then we define p-adic valuation as

$$ord_p \frac{a}{b} = ord_p a - ord_p b.$$

2020 *Mathematics Subject Classification.* 11S82,37A05.
Key words and phrases. p-adic dynamical system, ergodic function, uniformly differentiable functions modulo p, Van der Put basis, 1-Lipschitz function.

Definition 1.1. *Let $x \in \mathbb{Q}$. p-adic absolute value of x is given by*

$$|x|_p = \begin{cases} p^{-ord_p x}, & x \neq 0, \\ 0, & x = 0. \end{cases}$$

The p-adic absolute value is non-Archimedean and it induces a metric

$$\rho(x, y) = |x - y|_p.$$

Definition 1.2. *The completion of $\mathbb{Q}$, with respect to the p-adic norm is the field of p-adic numbers, $\mathbb{Q}_p$.*

Definition 1.3. *The unit disk about $0 \in \mathbb{Q}_p$ is called the set of p-adic integers and it is denoted by $\mathbb{Z}_p$, i.e.*

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leq 1\}.$$

Theorem 1.1. *Every p-adic number $\alpha \in \mathbb{Q}_p$ has unique p-adic representation*

$$\alpha = \alpha_{-r} p^{-r} + \alpha_{1-r} p^{1-r} + \alpha_{2-r} p^{2-r} + \ldots + \alpha_{-1} p^{-1} + \alpha_0 + \alpha_1 p^1 + \alpha_2 p^2 + \ldots$$

with $\alpha_n \in \mathbb{Z}$ i $0 \leq \alpha_n \leq (p-1)$. Moreover, $\alpha \in \mathbb{Z}_p$ if and only if $\alpha_{-r} = 0$, for all $r > 0$.

Definition 1.4. *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be 1-Lipschitz if for all $x, y \in \mathbb{Z}_p$ we have*

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

Definition 1.5. *Let $\mathbb{Z}_p$ be the ring of p-adic integers endowed with its ultra-metric norm $|.|$ and natural probability measure μ.*

(1) *A bijective function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be measure preserving if and only if $\mu(f^{-1}(S)) = \mu(S)$ for every measurable subset S of $\mathbb{Z}_p$.*
(2) *A measure preserving function is said to be ergodic if it has no proper invariant subset, i.e. $\mu(S) = 1$ or $\mu(S) = 0$ for every measurable subset $S \subset \mathbb{Z}_p$ such that $f^{-1}(S) = S$.*

Definition 1.6. *The dynamical system $(\mathbb{Z}_p, \mu, f)$ is called minimal if $S = \emptyset$ or $S = \mathbb{Z}_p$ whenever is S a closed invariant set, or equivalently, every orbit $Orb_f(x) = \{f^n(x) | n \in \mathbb{Z}\}$ is dense in $\mathbb{Z}_p$.*

Definition 1.7. *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be bijective modulo p^n, where n is a positive integer if for arbitrary $x \in \mathbb{Z}_p$ the elements $x, f(x), \ldots, f^{p^n-1}(x)$ are representatives of distinct classes of $\mathbb{Z}_p / p^n \mathbb{Z}_p$.*

Definition 1.8. *A function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is said to be transitive modulo p^n if it is bijective modulo p^n and the set $x, f(x), \ldots, f^{p^n-1}(x)$ is composed of only one cycle. In other words, $f^{p^n}(x) = x \pmod{p^n}$, but $f^r(x) \neq x \pmod{p^n}$, for all $r < p^n$.*

We recall that in [2, Theorem 1.1.] and [3, Proposition 4.35.] it is proved that a 1-Lipschitz measure preserving function is ergodic if and only if it is transitive modulo p^n for every positive integer n. Some equivalent definitions of 1-Lipschitz measure preserving and ergodic functions are presented in [2], [1], [3], and [5].

Proposition 1.1. Let $f:\mathbb{Z}_p\to\mathbb{Z}_p$ be a polynomial. Then $(\mathbb{Z}_p,f)$ is minimal if and only if $(\mathbb{Z}/p^{\delta}\mathbb{Z},f_{/\delta})$ is minimal, where $\delta=2$, if $p>3$ and $\delta=3$, if $p\in\{2,3\}$.

Proof. See [5]. □

In [5] it is proved that the 1-Lipschitz function $f:\mathbb{Z}_p\to\mathbb{Z}_p$ is minimal if and only if it is ergodic for Haar measure.

We recall the Van der Put representation for functions on $\mathbb{Z}_p$ (see [7]). If the p-adic expansion of the positive integer k is given by

$$k=\sum_{i=0}^{s}k_ip^i,\ \ 0\le k_i<p,\ \ k_s\neq 0,$$

then we define $q(k)=k_sp^s$.

For every function $f:\mathbb{Z}_p\to\mathbb{Z}_p$ we define the coefficients

$$B_k=\begin{cases} f(k), & k\in\{0,\dots,p-1\};\\ f(k)-f(k-q(k)), & k\ge p.\end{cases}$$

In this way the function f can be represented in the so called Van der Put basis as follows

$$f(x)=\sum_{k=0}^{\infty}B_k\chi(k,x),$$

where if $k>0$,

$$\chi(k,x)=\begin{cases}1, & |x-k|\le p^{-\lfloor\log_p k\rfloor-1};\\ 0, & \text{otherwise.}\end{cases}$$

For $k=0$ we have

$$\chi(0,x)=\begin{cases}1, & |x|\le p^{-1};\\ 0, & \text{otherwise.}\end{cases}$$

A function $f:\mathbb{Z}_p\to\mathbb{Z}_p$ is said to be uniformly differentiable modulo p^k if there exists a positive integer N and a function $\partial_k f:\mathbb{Z}_p\to\mathbb{Q}_p$ such that for all $r\ge N$ and $h\in\mathbb{Z}_p$, we have

$$f(u+p^rh)=f(u)+p^rh\partial_kf(u)\ \ (mod\ p^{k+r}),\forall u\in\mathbb{Z}_p.$$

The smallest integer N satisfying this property is denoted by $N_k(f)$. In [3, Proposition 3.41.] it was proved that if f is 1-Lipschitz , then $\partial_k f$ takes its values in $\mathbb{Z}_p$.

2. Ergodic uniformly differentiable functions modulo p on $\mathbb{Z}_p$

Theorem 2.1. *Let f be an isometric and uniformly differentiable function modulo p on $\mathbb{Z}_p$, where $N_1(f)=1$. Then, f is ergodic on $\mathbb{Z}_p$ if and only if the following conditions are satisfied:*

(1) *f is transitive modulo p.*

(2) *For every positive integer k, $f^{p^k}(0)\neq 0\ \ (mod\ p^{k+1})$.*

(3) *For every positive integer k,*

$$\frac{\prod_{j=0}^{p^k-1} B_{j+p^k}}{(p^k)^{p^k}} = 1 \pmod p.$$

Proof. Conditions (1) and (2) are obviously necessary. According to [3, Proposition 4.35.] it suffices to prove that for every fixed positive integer k, if f is transitive modulo p^k, then it is transitive modulo p^{k+1} if and only if

$$\frac{\prod_{j=0}^{p^k-1} B_{j+p^k}}{(p^k)^{p^k}} = 1 \pmod p. \tag{2.1}$$

Namely, it suffices to prove that if $f^{p^k}(0) \neq 0 \pmod{p^{k+1}}$, then (2.1) holds if and only if for every $l \in \{2,\dots,p-1\}$, $f^{lp^k}(0) \neq 0 \pmod{p^{k+1}}$.

Assume that f is transitive modulo p^k for some arbitrary and fixed $k \geq 1$. Let $\{t_0,\dots,t_{p^k-1}\}$ be representatives of $p^k\mathbb{Z}_p$-cosets such that $f(t_i) = t_{i+1} \pmod{p^k}$, for $0 \leq i \leq p^k-2$ and $f(t_{p^k-1}) = t_0 \pmod{p^k}$. We may choose

$$\{t_0,\dots,t_{p^k-1}\} = \{0,\dots,p^k-1\}. \tag{2.2}$$

Our first task is to prove that for all $l \in \{1,\dots,p-1\}$ and $s \in \{0,\dots,p^k-1\}$

$$\begin{aligned} f^{lp^k}(0) \;=\; & f(t_{p^k-1}) + \sum_{i=1}^{s} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k} \\ & + \frac{f^{lp^k-s-1}(0) - t_{p^k-s-1}}{p^{k(s+1)}} \prod_{j=1}^{s+1} B_{t_{p^k-j}+p^k} \pmod{p^{k+1}}. \end{aligned} \tag{2.3}$$

We know from [6, Formula (4.3)] that for all $j < p^k$, $r \in \{1,\dots,p-1\}$, $B_{j+rp^k} = rB_{j+p^k} \pmod{p^{k+1}}$. It follows that

$$\begin{aligned} f^{lp^k}(0) \;&=\; f(f^{lp^k-1}(0)) = f(t_{p^k-1} + p^k \frac{f^{lp^k-1}(0) - t_{p^k-1}}{p^k}) \\ &=\; f(t_{p^k-1}) + \frac{f^{lp^k-1}(0) - t_{p^k-1}}{p^k} B_{t_{p^k-1}+p^k} \pmod{p^{k+1}}. \end{aligned}$$

Hence, (2.3) holds for $s = 0$. Assume it is true for some $s \in \{0,\dots,p^k-2\}$. Applying [6, Formula (4.3)] we get

$$\begin{aligned} f^{lp^k-s-1}(0) \;&=\; f(f^{lp^k-s-2}(0)) = f(t_{p^k-s-2} + p^k \frac{f^{lp^k-s-2}(0) - t_{p^k-s-2}}{p^k}) \\ &=\; f(t_{p^k-s-2}) + \frac{f^{lp^k-s-2}(0) - t_{p^k-s-2}}{p^k} B_{t_{p^k-s-2}+p^k} \pmod{p^{k+1}}. \end{aligned}$$

Hence, (2.3) becomes

$$f^{lp^k}(0) = f(t_{p^k-1}) + \sum_{i=1}^{s+1} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k} + \frac{f^{lp^k-s-2}(0) - t_{p^k-s-2}}{p^{k(s+2)}} \prod_{j=1}^{s+2} B_{t_{p^k-j}+p^k} \pmod{p^{k+1}}.$$

Then, (2.3) holds for every $s \in \{0, \dots, p^k - 1\}$.

Now, for $l = 1$ and $s = p^k - 2$, (2.3) takes the form

$$\begin{aligned} f^{p^k}(0) &= f(t_{p^k-1}) + \sum_{i=1}^{p^k-2} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k} \\ &\quad + \frac{f(0) - t_1}{p^{k(p^k-1)}} \prod_{j=1}^{p^k-1} B_{t_{p^k-j}+p^k} \pmod{p^{k+1}} \\ &= f(t_{p^k-1}) + \sum_{i=1}^{p^k-1} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k}. \end{aligned} \tag{2.4}$$

On the other hand for $l \geq 2$ and $s = p^k - 2$, (2.3) takes the form

$$f^{lp^k}(0) = f(t_{p^k-1}) + \sum_{i=1}^{p^k-2} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k} + \frac{f^{(l-1)p^k+1}(0) - t_1}{p^{k(p^k-1)}} \prod_{j=1}^{p^k-1} B_{t_{p^k-j}+p^k} \pmod{p^{k+1}}.$$

Applying the same techniques as above we get

$$\frac{f^{(l-1)p^k+1}(0) - t_1}{p^{k(p^k-1)}} = \frac{f(0 + p^k \frac{f^{(l-1)p^k}(0)}{p^k}) - t_1}{p^{k(p^k-1)}} = \frac{f(0) - t_1 + \frac{f^{(l-1)p^k}(0)}{p^k} B_{p^k}}{p^{k(p^k-1)}} \pmod{p^{k+1}}.$$

Therefore, applying (2.2), (2.3) becomes

$$f^{lp^k}(0) = f(t_{p^k-1}) + \sum_{i=1}^{p^k-1} \frac{f(t_{p^k-i-1}) - t_{p^k-i}}{p^{ki}} \prod_{j=1}^{i} B_{t_{p^k-j}+p^k} + \frac{f^{(l-1)p^k}(0)}{p^{kp^k}} \prod_{j=0}^{p^k-1} B_{j+p^k} \pmod{p^{k+1}}.$$

Then, (2.4) yields

$$f^{lp^k}(0) = f^{p^k}(0) + \frac{f^{(l-1)p^k}(0)}{p^{kp^k}} \prod_{j=0}^{p^k-1} B_{j+p^k} \pmod{p^{k+1}}.$$

Replacing l by $l-1$, then $l-1$ by $l-2$,...gives

$$f^{lp^k}(0) = f^{p^k}(0)\left(1 + \frac{\prod_{j=0}^{p^k-1} B_{j+p^k}}{p^{kp^k}} + \ldots + \left(\frac{\prod_{j=0}^{p^k-1} B_{j+p^k}}{p^{kp^k}}\right)^{l-1}\right).$$

We conclude that if $f^{p^k}(0) \neq 0 \pmod{p^{k+1}}$, then (2.1) holds if and only if for every $l \in \{2,\ldots,p-1\}$, $f^{lp^k}(0) \neq 0 \pmod{p^{k+1}}$. □

Remark 2.1. Notice that for any analytic function f we have $\frac{B_{i+p^k}}{p^k} = f'(i) \pmod{p^k}$, for every positive integer k and every $i \in \{0,\ldots,p^k-1\}$, because $f(i+p^k) = f(i) + p^k f'(i) \pmod{p^{2k}}$.

2.1. **Ergodic rational functions on $\mathbb{Z}_3$**

In the following corollaries we study ergodic rational functions $R = \frac{P}{Q}$ on $\mathbb{Z}_3$ where the numerator P is not an ergodic polynomial. We study cases where the denominator is always a unit. Without loss of generality we may assume that $P(0) = Q(0) = 1$.

Corollary 2.1. *Let P be an isometric polynomial on $\mathbb{Z}_3$. Assume that P is transitive modulo 3, $P(0) = 1$,*

$$P^3(0) = 0 \pmod{9}$$

and

$$P'(0)P'(1)P'(2) = 1 \pmod{3}.$$

Then, $R = \dfrac{P}{Q}$ is ergodic if the following conditions are satisfied

(1) $Q(\mathbb{Z}_3) \subseteq 1 + 3\mathbb{Z}_3$,
(2) $Q'(x) = 0 \pmod{3}$, *for every* $x \in \mathbb{Z}_3$,
(3) $Q(1) \neq 1 \pmod{9}$,
(4) $P^3(0) + P^3(3) + P^3(6) + 2P'(2)\left(\frac{1}{Q(1)} + \frac{1}{Q(4)} + \frac{1}{Q(7)} - 3\right)$
$+P'(1)P'(2)\left(\frac{1}{Q(0)} + \frac{1}{Q(3)} + \frac{1}{Q(6)} - 3\right) \neq 0 \pmod{3^3}$.

Proof. See [9]. □

Example 2.1. *Let $P(x) = 3x^2 + x + 1$. This is an isometric polynomial, transitive modulo 3, and it satisfies the conditions*

(i) $P(0) = 1$,
(ii) $P^3(0) = 0 \pmod{9}$,
(iii) $P'(0)P'(1)P'(2) = 1 \pmod{3}$.

According to Corollary 2.1, the function $\dfrac{3x^2+x+1}{Q(x)}$ would be an ergodic function if the polynomial $Q(x)$ satisfies the following conditions:

(1) $Q(\mathbb{Z}_3) \subseteq 1+3\mathbb{Z}_3$,
(2) $Q'(x) = 0 \pmod 3$ *for* $\forall x \in \mathbb{Z}_3$,
(3) $Q(1) \neq 1 \pmod 9$, *and*
(4) $9 - \left(\frac{1}{Q(1)} + \frac{1}{Q(4)} + \frac{1}{Q(7)}\right) + 10\left(\frac{1}{Q(0)} + \frac{1}{Q(3)} + \frac{1}{Q(6)}\right) \neq 0 \pmod{27}$.

One of the polynomials that satisfy these conditions is $Q(x) = 3x^3 + 1$. *So, the function* $R(x) = \dfrac{3x^2+x+1}{3x^3+1}$ *is an ergodic function.*

Corollary 2.2. *Let* P *be an isometric polynomial on* $\mathbb{Z}_3$. *Assume that* $P(0) = 1$, P *is transitive modulo 9, but not modulo* 3^3.

Then, $R = \dfrac{P}{Q}$ *is ergodic if the following conditions are satisfied*

(1) $Q(\mathbb{Z}_3) \subseteq 1+3\mathbb{Z}_3$,
(2) $Q'(x) = 0 \pmod 3$, *for every* $x \in \mathbb{Z}_3$,
(3) $Q(1) = 1 + P(2)P'(2) + P(1) - 2 \pmod 9$,
(4) $2P'(2)\left(\frac{1}{Q(1)} + \frac{1}{Q(4)} + \frac{1}{Q(7)} - 3\right) + P'(1)P'(2)\left(\frac{1}{Q(0)} + \frac{1}{Q(3)} + \frac{1}{Q(6)} - 3\right) \neq 0 \pmod{3^3}$.

Proof. See [9]. □

2.2. **Ergodic rational functions on** $\mathbb{Z}_5$

Corollary 2.3. *Let* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1$ *be an isometric polynomial on* $\mathbb{Z}_5$. *Let* t_i *be representatives of* $5\mathbb{Z}_5$*-cosets such that* $P(t_i) = t_{i+1} \pmod 5$ *and* $P(t_4) = t_0 = 0 \pmod 5$. *Assume that*

$$P^5(t_0) = t_0 \pmod{25}$$

and

$$P'(t_0)P'(t_1)P'(t_2)P'(t_3)P'(t_4) = 1 \pmod 5.$$

Then $R = \dfrac{P}{Q}$ *is ergodic if the polynomial* $Q(x)$ *satisfies the following conditions*

(1) $Q(\mathbb{Z}_5) \subseteq 1+5\mathbb{Z}_5$,
(2) $Q'(x) = 0 \pmod 5$, *for all* $x \in \mathbb{Z}_5$,
(3) $t_4\left(1 - \frac{1}{Q(t_3)}\right) + t_3P'(t_3)\left(1 - \frac{1}{Q(t_2)}\right) + t_2P'(t_3)P'(t_2)\left(1 - \frac{1}{Q(t_1)}\right) \neq 0 \pmod{25}$.

Proof. See [11]. □

Remark 2.2. Let $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1$. If we introduce the notation

$$\sum_{i \in 1+4\mathbb{N}} a_i = A_1, \quad \sum_{i \in 2+4\mathbb{N}} a_i = A_2, \quad \sum_{i \in 3+4\mathbb{N}} a_i = A_3, \quad \sum_{i \in 4\mathbb{N}} a_i = A_4,$$

then, according [4, Proposition 4.2], we have six classes of transitive polynomials modulo 5. Hence, the third condition from the previous Corollary for all six classes , can be written in the following way:

$$\begin{cases} 4\Big(1-\frac{1}{Q(3)}\Big)+3P'(3)\Big(1-\frac{1}{Q(2)}\Big)+2P'(2)P'(3)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 1, \quad A_2\equiv 0, \quad A_3\equiv 0 \quad \text{i} \quad A_4\equiv 0 \pmod 5; \\ 3\Big(1-\frac{1}{Q(4)}\Big)+4P'(4)\Big(1-\frac{1}{Q(2)}\Big)+2P'(2)P'(4)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 4, \quad A_2\equiv 4, \quad A_3\equiv 3 \quad \text{i} \quad A_4\equiv 0 \pmod 5, \\ 4\Big(1-\frac{1}{Q(2)}\Big)+2P'(2)\Big(1-\frac{1}{Q(3)}\Big)+3P'(2)P'(3)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 1, \quad A_2\equiv 3, \quad A_3\equiv 3 \quad \text{i} \quad A_4\equiv 0 \pmod 5, \\ 2\Big(1-\frac{1}{Q(4)}\Big)+4P'(4)\Big(1-\frac{1}{Q(3)}\Big)+3P'(3)P'(4)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 1, \quad A_2\equiv 4, \quad A_3\equiv 2 \quad \text{i} \quad A_4\equiv 0 \pmod 5, \\ 3\Big(1-\frac{1}{Q(2)}\Big)+2P'(2)\Big(1-\frac{1}{Q(4)}\Big)+4P'(2)P'(4)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 4, \quad A_2\equiv 2, \quad A_3\equiv 2 \quad \text{i} \quad A_4\equiv 0 \pmod 5, \\ 2\Big(1-\frac{1}{Q(3)}\Big)+3P'(2)\Big(1-\frac{1}{Q(4)}\Big)+4P'(2)P'(3)\Big(1-\frac{1}{Q(1)}\Big)\neq 0 \pmod{25}, \\ \text{if} \quad A_1\equiv 0, \quad A_2\equiv 0, \quad A_3\equiv 3 \quad \text{i} \quad A_4\equiv 0 \pmod 5. \end{cases}$$

Example 2.2. *Let $P(x)=2x^7+3x^6+5x^5+5x^4+3x^3+2x^2+x+1$. This is an isometric polynomial, transitive modulo 5 and it satisfies conditions*

(i) $P(i)=i+1$ *for all* $i\in\{0,1,2,3,4\}$,
(ii) $P^5(0)=0 \pmod{25}$,
(iii) $P'(0)P'(1)P'(2)P'(3)P'(4)=1 \pmod 5$.

The function $R=\dfrac{P}{Q}$ would be ergodic if the polynomial $Q(x)$ satisfies the conditions of Corollary 2.3. One of the polynomials which satisfies these conditions is $Q(x)=10x^4+5x^2+1$. Hence, such a function $R(x)$ is ergodic.

The next result is in the case when the numerator is not transitive modulo 5.

Corollary 2.4. *Let P be an isometric polynomial on $\mathbb{Z}_5$. Assume that P is not transitive modulo 5 and let $2\leq i\leq 4$ be a fixed number such that*

(i) $P(k)=(k+1)i \pmod 5$, $0\leq k\leq 4$ *and*
(ii) $P'(0)P'(1)P'(2)P'(3)P'(4)=i \pmod 5$.

Then $R=\dfrac{P}{Q}$ is ergodic if the polynomial $Q(x)$ satisfies conditions

(1) $Q(\mathbb{Z}_5)\subseteq i+5\mathbb{Z}_5$,
(2) $Q'(x)=0 \pmod 5$, *for all* $x\in\mathbb{Z}_5$,
(3) $1+\sum_{s=0}^{4}\frac{l_{4-s}}{i^s}\prod_{j=1}^{s}P'(t_{5-j})\neq 0 \pmod 5$, *where* $l_k\in\{0,\ldots,4\}$ *satisfy*
$P(k)=(k+1+5l_k)Q(k) \pmod{25}$.

Proof. See [11]. □

3. On some classes of 1-Lipschitz measure preserving ergodic functions on $\mathbb{Z}_p$

Lemma 3.1. *Let f be a 1-Lipschitz measure preserving function on $\mathbb{Z}_p$. Assume that f is transitive modulo p and satisfies*

$$B_{i+lp^k} = lB_{i_0+p^k} \pmod{p^{k+1}},\ \forall k \geq 1,\ \forall l \in \{1,\dots,p-1\},\ \forall i < p^k, \tag{3.1}$$

where $i_0 \in \{0,\dots,p-1\}$ is a unique integer depending on i and satisfying $i = i_0 \pmod p$. Then,

(1) *for every $x \in \mathbb{Z}_p$, $l \in \{1,\dots,p-1\}$ and $k \geq 1$,*

$$f(x+lp^k) = f(x) + lB_{x_0+p^k} \pmod{p^{k+1}}, \tag{3.2}$$

where $x_0 \in \{0,\dots,p-1\}$ is a unique integer depending on x and satisfying $x = x_0 \pmod p$,

(2) *for every $x \in \mathbb{Z}_p$, $l \in \{1,\dots,p-1\}$ and $n,k \geq 1$,*

$$f^n(x+lp^k) = f^n(x) + l\left(\prod_{i=0}^{p-1}\frac{B_{i+p^k}}{p^k}\right)^{n-m}\left(\prod_{i=s}^{m+s-1}\frac{B_{y_i+p^k}}{p^k}\right)p^k \pmod{p^{k+1}}, \tag{3.3}$$

where the sequence $(y_i)_i$ is such that $\{y_i, i \geq 0\} = \{0,\dots,p-1\}$, $y_0 = 0$ and $y_{i+1} = f(i) \pmod p$, for every nonnegative integer i. The numbers $s,m \in \{0,\dots,p-1\}$ are such that $m = n \pmod p$ and $x = y_s \pmod p$. The second product is taken to be equal to 1 if $m = 0$.

Proof. See [10]. □

Theorem 3.1. *Let f be a function satisfying the conditions of Lemma 3.1. Then, under the notation of Lemma 3.1, f is ergodic if and only if the following conditions are satisfied*

(1)
$$\prod_{i=0}^{p-1}\frac{B_{i+p^k}}{p^k} = 1 \pmod p, \forall k \geq 1,$$

(2)
$$\sum_{s=0}^{p-1}\prod_{t=s+1}^{p-1}\frac{B_{y_t+p}}{p}B_{y_s} \neq \sum_{s=0}^{p-1}\prod_{t=s}^{p-1}\frac{B_{y_t+p}}{p}y_s \pmod{p^2},$$

and

$$\sum_{s=0}^{p-1}\prod_{t=s+1}^{p-1}\frac{B_{y_t+p^k}}{p^k}\left(p^{k-1}B_{y_s} + \sum_{l=1}^{k-1}p^{k-l-1}\sum_{\substack{m\in\{p^l,\dots,p^{l+1}-1\}\\ m=y_s \pmod p}}B_m\right)$$
$$\neq \sum_{s=0}^{p-1}\prod_{t=s}^{p-1}\frac{B_{y_t+p^k}}{p^k}\left(\frac{p}{2}(p-1)+y_s\right)p^{k-1} \pmod{p^{k+1}},\ \forall k \geq 2.$$

Proof. Since f is transitive modulo p, it can be easily seen ([9]) that f is ergodic if and only if

$$f^{lp^k}(0) \neq 0 \pmod{p^{k+1}},\ \forall k \geq 1,\ \forall l \in \{1,\dots,p-1\}.$$

Following the steps made in the proof of [9, Theorem 2.1], we can see that for every $l \in \{1,\dots,p-1\}$ and $k \geq 1$,

$$f^{lp^k}(0) = f^{p^k}(0)\left(1 + \prod_{j=0}^{p^k-1} \frac{B_{j+p^k}}{p^k} + \dots + \left(\prod_{j=0}^{p^k-1} \frac{B_{j+p^k}}{p^k}\right)^{l-1}\right).$$

Hence, f is ergodic if and only if for every $l \in \{1,\dots,p-1\}$ and $k \geq 1$

$$f^{p^k}(0) \neq 0 \pmod{p^{k+1}}, \tag{3.4}$$

and

$$\prod_{j=0}^{p^k-1} \frac{B_{j+p^k}}{p^k} = 1 \pmod{p}. \tag{3.5}$$

We first prove that (3.5) is equivalent to condition (1). According to (3.1), identity (3.5) is equivalent to

$$\left(\prod_{j=0}^{p-1} \frac{B_{j+p^k}}{p^k}\right)^{p^{k-1}} = 1 \pmod{p}.$$

Since

$$\left(\prod_{j=0}^{p-1} \frac{B_{j+p^k}}{p^k}\right)^{p-1} = 1 \pmod{p},$$

then, (3.5) is equivalent to

$$\left(\prod_{j=0}^{p-1} \frac{B_{j+p^k}}{p^k}\right)^{(p-1)(1+\dots+p^{k-2})+1} = \prod_{j=0}^{p-1} \frac{B_{j+p^k}}{p^k} \pmod{p} = 1 \pmod{p},\ \forall k \geq 1.$$

It remains to verify that (3.4) is equivalent to condition (2).

By induction on $k \geq 1$ it can be seen that

$$\sum_{\substack{m\in\{0,\dots,p^k-1\}\\ m=y_s \pmod{p}}} f(m) = p^{k-1}B_{y_s} + \sum_{l=1}^{k-1} p^{k-l-1} \sum_{\substack{m\in\{p^l,\dots,p^{l+1}-1\}\\ m=y_s \pmod{p}}} B_m. \tag{3.6}$$

On the other hand it can be easily seen that

$$\sum_{\substack{m\in\{0,\dots,p^k-1\}\\ m=y_s \pmod{p}}} m = \left(\frac{p}{2}(p-1)+y_s\right)p^{k-1} \pmod{p^{k+1}}. \tag{3.7}$$

If we prove that for every $k \geq 1$,

$$f^{p^k}(0)=\sum_{s=0}^{p-1}\prod_{t=s+1}^{p-1}\frac{B_{y_t+p^k}}{p^k}\sum_{\substack{m\in\{0,\ldots,p^k-1\}\\ m=y_s \pmod p}} f(m)-\sum_{s=0}^{p-1}\prod_{t=s}^{p-1}\frac{B_{y_t+p^k}}{p^k}\sum_{\substack{m\in\{0,\ldots,p^k-1\}\\ m=y_s \pmod p}} m \pmod{p^{k+1}}, \tag{3.8}$$

then condition (2) can be obtained by a combination of (3.4), (3.8), (3.6) and (3.7).

We first consider the case when $k=1$. Formula (3.3) yields

$$\begin{aligned} f^p(0) &= f^{p-1}(f(0)) = f^{p-1}(y_1+f(0)-y_1)\\ &= f^{p-1}(y_1)+(f(0)-y_1)\prod_{t=1}^{p-1}\frac{B_{y_t+p}}{p} \pmod{p^2}. \end{aligned} \tag{3.9}$$

In a similar way, for every $r\in\{1,\ldots,p-2\}$,

$$f^{p-r}(y_r)=f^{p-r-1}(y_{r+1})+(f(y_r)-y_{r+1})\prod_{t=r+1}^{p-1}\frac{B_{y_t+p}}{p} \pmod{p^2}. \tag{3.10}$$

Combining (3.9) and (3.10) gives

$$\begin{aligned} f^p(0) &= f(y_{p-1})+\sum_{r=0}^{p-2}(f(y_r)-y_{r+1})\prod_{t=r+1}^{p-1}\frac{B_{y_t+p}}{p} \pmod{p^2}\\ &= \sum_{r=0}^{p-1}\prod_{t=r+1}^{p-1}\frac{B_{y_t+p}}{p}f(y_r)-\sum_{r=1}^{p-1}\prod_{t=r}^{p-1}\frac{B_{y_t+p}}{p}y_r \pmod{p^2}. \end{aligned}$$

Let $k\geq 2$ be such that f is transitive modulo p^k. Proceeding as in the proof of [8, Theorem 2.2], we put $i_j^s=f^s(j\cdot p^k) \pmod{p^{k+1}}$, for $j\in\{0,\ldots,p-1\}$ and $s\in\{0,\ldots,p^{k-1}-1\}$, where $\{i_j^s, j\in\{0,\ldots,p-1\}, s\in\{0,\ldots,p^{k-1}-1\}\}=\{0,\ldots,p^k-1\}$. Let $\{s_1,\ldots,s_{p-1}\}=\{1,\ldots,p-1\}$ be such that

$$f^{p^{k-1}}(0)=s_1p^{k-1} \pmod{p^k}, \tag{3.11}$$

and for $i\in\{1,\ldots,p-2\}$,

$$f^{p^{k-1}}(s_ip^{k-1})=s_{i+1}p^{k-1} \pmod{p^k}. \tag{3.12}$$

It is clear that

$$f^{p^{k-1}}(s_{p-1}p^{k-1})=0 \pmod{p^k}. \tag{3.13}$$

Combining (3.3), (3.11) and condition (1) gives

$$\begin{aligned} f^{p^k}(0) &= f^{p^{k-1}(p-1)}(f^{p^{k-1}}(0)) = f^{p^{k-1}(p-1)}(s_1p^{k-1}+f^{p^{k-1}}(0)-s_1p^{k-1})\\ &= f^{p^{k-1}(p-1)}(s_1p^{k-1})+f^{p^{k-1}}(0)-s_1p^{k-1} \pmod{p^{k+1}}. \end{aligned}$$

Similarly, combining (3.12) in a recursive way with (3.3) and condition (1), we obtain

$$\begin{aligned} f^{p^k}(0) &= f^{p^{k-1}}(s_{p-1}p^{k-1})+f^{p^{k-1}}(s_{p-2}p^{k-1})\\ &\quad -s_{p-1}p^{k-1}+\ldots+f^{p^{k-1}}(0)-s_1p^{k-1} \pmod{p^{k+1}}\\ &= \sum_{j=0}^{p-1}f^{p^{k-1}}(i_j^0)-\sum_{j=0}^{p-1}i_j^0 \pmod{p^{k+1}}. \end{aligned} \tag{3.14}$$

For every $j \in \{0,\dots,p-1\}$, since $i_j^1 = 1 \pmod p$, an application of (3.3) and condition (1) gives

$$\begin{aligned} f^{p^{k-1}}(i_j^0) &= f^{p^{k-1}-1}(i_j^1 + f(i_j^0) - i_j^1) \\ &= f^{p^{k-1}-1}(i_j^1) + (f(i_j^0) - i_j^1) \prod_{t=1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \pmod{p^{k+1}}. \end{aligned} \tag{3.15}$$

In a similar way, for all $r \in \{1,\dots,p^{k-1}-2\}$,

$$\begin{aligned} f^{p^{k-1}-r}(i_j^r) &= f^{p^{k-1}-r-1}(i_j^{r+1} + f(i_j^r) - i_j^{r+1}) \\ &= f^{p^{k-1}-r-1}(i_j^{r+1}) + (f(i_j^r) - i_j^{r+1}) \prod_{t=r+1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \pmod{p^{k+1}}. \end{aligned} \tag{3.16}$$

Combining (3.15) and (3.16) we obtain

$$f^{p^{k-1}}(i_j^0) = f(i_j^{p^{k-1}-1}) + \sum_{r=0}^{p^{k-1}-2} (f(i_j^r) - i_j^{r+1}) \prod_{t=r+1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \pmod{p^{k+1}}.$$

Therefore,

$$\begin{aligned} \sum_{j=0}^{p-1} f^{p^{k-1}}(i_j^0) &= \sum_{j=0}^{p-1} f(i_j^{p^{k-1}-1}) + \sum_{r=0}^{p^{k-1}-2} \prod_{t=r+1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \sum_{j=0}^{p-1} f(i_j^r) \\ &\quad - \sum_{r=0}^{p^{k-1}-2} \prod_{t=r+1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \sum_{j=0}^{p-1} i_j^{r+1} \pmod{p^{k+1}}. \end{aligned}$$

Since for all $r \in \{1,\dots,p^{k-1}-2\}$, $j \in \{0,\dots,p-1\}$, $i_j^r = y_r \pmod p$, we get

$$\begin{aligned} \sum_{j=0}^{p-1} f^{p^{k-1}}(i_j^0) &= \sum_{r=0}^{p^{k-1}-1} \prod_{t=r+1}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \sum_{j=0}^{p-1} f(i_j^r) \\ &\quad - \sum_{r=1}^{p^{k-1}-1} \prod_{t=r}^{p^{k-1}-1} \frac{B_{y_t+p^k}}{p^k} \sum_{j=0}^{p-1} i_j^r \pmod{p^{k+1}} \\ &= \sum_{s=0}^{p-1} \prod_{t=s+1}^{p-1} \frac{B_{y_t+p^k}}{p^k} \sum_{\substack{m\in\{0,\dots,p^k-1\} \\ m=y_s \pmod p}} f(m) \\ &\quad - \sum_{s=0}^{p-1} \prod_{t=s}^{p-1} \frac{B_{y_t+p^k}}{p^k} \sum_{\substack{m\in\{0,\dots,p^k-1\} \\ m=y_s \pmod p \\ m\neq 0 \pmod{p^k}}} m \pmod{p^{k+1}}, \end{aligned}$$

where the latter equality follows from the properties of the sequence $(y_i)_i$ and condition (1).

Hence, (3.14) yields (3.8). □

Corollary 3.1. *Let f be a* 1*-Lipschitz measure preserving function on $\mathbb{Z}_p$. Assume that f is transitive modulo p and satisfies*

$$B_{i+lp^k} = lp^k \pmod{p^{k+1}},\ \forall k \geq 1,\ \forall l \in \{1,\dots,p-1\},\ \forall i < p^k. \tag{3.17}$$

Then, f is ergodic if and only if

$$\sum_{m=0}^{p-1} p^{k-1}B_m + \sum_{l=1}^{k-1} p^{k-l-1} \sum_{m=p^l}^{p^{l+1}-1} B_m \neq \frac{p^k}{2}(p-1) \pmod{p^{k+1}},\ \forall k \geq 1. \tag{3.18}$$

Proof. See [10]. □

References

[1] V. Anashin, *Ergodic transformations in the space of p-adic integers*, p-Adic Mathematical Physics, AIP Conf. Proc. **826**, 3–24, 2006.

[2] V. S. Anashin, *Uniformly distributed sequences of p-adic integers*, Math. Notes, **55**, No. 1-2, 109-133, 1994.

[3] V. Anashin, A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Expositions in Mathematics 49. Berlin, 2009.

[4] K. Donggyun, K. Youngwoo and S. Kyunghwan, *Minimality of 5-adic polynomial dynamics, Dyn. Syst.* **35**, No. 4, 584-596, 2020.

[5] F. Durand and F. Paccaut, *Minimal polynomial dynamics on the set of 3-adic integers*, Bull. Lond. Math. Soc., **41**, No. 2, 302-314, 2009.

[6] S. Jeong, *Measure-preservation and the existence of a root of p-adic* 1*-Lipschitz functions in Mahler's expansion*, p-Adic Numbers Ultrametric Anal. Appl. **10**, No. 3, 192–208, 2018.

[7] K. Mahler, *p-Adic Numbers and Their Functions*, Cambridge Univ. Press, Cambridge, 1981.

[8] N. Memić, *On some compatible functions on the set of* 3*-Adic integers*, Colloq. Math. **155**, No. 2, 197-214, 2019.

[9] N. Memić, J. Muminović Huremović, *Ergodic uniformly differentiable functions modulo p on $\mathbb{Z}_p$*, p-Adic Numbers Ultrametric Anal. Appl. **12**, No. 1, 49-59, 2020.

[10] N. Memić, J. Muminović Huremović, *On some classes of* 1*-Lipschitz measure-preserving ergodic functions on $\mathbb{Z}_p$*, Asian-European Journal of Mathematics, **16**, No. 9, 2250167, 2022.

[11] J. Muminović Huremović, *On some ergodic rational functions on $\mathbb{Z}_5$*, Advances in Mathematics: Scientific Journal, **12**, No. 10, 2023.

(Received: 17 May, 2024)
(Revised: 16 September, 2024)

Jasmina Muminović Huremović
University of Tuzla
Department of Mathematics
Urfeta Vejzagića 4
75000 Tuzla
Bosnia and Herzegovina
e-mail: *jasmina.muminovic@untz.ba*