Toward the ergodicity of \( p \)-adic 1-Lipschitz functions represented by the van der Put series

Sangtae Jeong
Department of Mathematics, Inha University, Incheon, Korea 402-751
May 3, 2014

Abstract
Yurova [16] and Anashin et al. [3, 4] characterize the ergodicity of a 1-Lipschitz function on \( \mathbb{Z}_2 \) in terms of the van der Put expansion. Motivated by their recent work, we provide the sufficient conditions for the ergodicity of such a function defined on a more general setting \( \mathbb{Z}_p \).
In addition, we provide alternative proofs of two criteria (because of [3, 4] and [10]) for an ergodic 1-Lipschitz function on \( \mathbb{Z}_2 \), represented by both the Mahler basis and the van der Put basis.

1 Introduction
The ergodic theory of \( p \)-adic dynamical systems is an important part of non-Archimedean dynamics, and represents a rapidly developing discipline that has recently demonstrated its effectiveness in various areas such as computer science, cryptology, and numerical analysis, among others. For example, as shown in [7], it is useful to have 2-adic ergodic functions in constructing long-period pseudo-random sequences in stream ciphers. For more details on such applications, we refer the reader to [2] and the references therein.

As a substitute for the Mahler basis, the van der Put basis has recently been employed as a useful tool for building on the ergodic theory of \( p \)-adic dynamical systems. Indeed, Yurova [16] and Anashin et al. [3, 4] provide the criterion for the ergodicity of 2-adic 1-Lipschitz functions, in terms of the van der Put expansion. Their proof of this criterion relies on Anashin’s criterion for 1-Lipschitz functions on \( \mathbb{Z}_2 \) in terms of the Mahler expansion. Given the characteristic functions of \( p \)-adic balls, it is analyzed in [4] that the van der Put basis has more advantages than the Mahler basis in evaluating representations and that it is more applicable to \( T \)-functions or 1-Lipschitz functions.

On the other hand, on the function field side of non-Archimedean dynamics, Lin et al. [9] present an ergodic theory parallel to [1] and [3, 4] by using both Carlitz-Wagner basis and an analog of the van der Put basis. Along this line, Jeong [6] uses the digit derivative basis to develop a corresponding theory parallel to [9].
The purpose of the paper is to provide the sufficient conditions under which 1-Lipschitz functions on \( \mathbb{Z}_p \) represented by the van der Put series are ergodic. In addition, we provide alternative proofs of two known criteria for an ergodic 1-Lipschitz function on \( \mathbb{Z}_2 \) in terms of both the Mahler basis and the van der Put basis. We also present several equivalent conditions that may be needed to provide a complete description of the ergodicity of 1-Lipschitz functions defined on a more general setting \( \mathbb{Z}_p \). The main idea behind this paper comes from Lin et al’s work [9] on \( \mathbb{F}_2[[T]] \), and Anashin et al.’s work [4] on \( \mathbb{Z}_2 \).

Keywords: Ergodic functions, Measure-preserving, 1-Lipschitz, Van der Put basis, Mahler basis
Mathematics Subject Classification 2000: 11S80 11K41
Email: stj@inha.ac.kr
The rest of this paper is organized as follows: Section 2 recalls some prerequisites in non-Archimedean dynamics, including two known results for the ergodicity of 1-Lipschitz functions on \(\mathbb{Z}_2\) in terms of the Mahler basis and the van der Put basis. Section 3 presents the main results and alternate proofs of two criteria for an ergodic 1-Lipschitz function on \(\mathbb{Z}_2\). Section 4 employs our results or Anashin’s to re-prove then ergodicity of a polynomial over \(\mathbb{Z}_2\) in terms of its coefficients.

## 2 Ergodic theory of \(p\)-adic integers

We recall the existing results for the measure-preservation and ergodicity of 1-Lipschitz functions \(f : \mathbb{Z}_2 \to \mathbb{Z}_2\) in terms of both the Mahler expansion and the van der Put expansion.

### 2.1 Preliminaries for \(p\)-adic dynamics

We recall the elements of \(p\)-adic dynamical systems on \(\mathbb{Z}_p\). Let \(p\) be a prime and \(\mathbb{Z}_p\) be the ring of \(p\)-adic integers with the quotient field \(\mathbb{Q}_p\). Let \(|?| = |?|_p\) be the (normalized) absolute value on \(\mathbb{Q}_p\) associated with the additive valuation \(\text{ord}\) such that \(|x|_p = p^{-\text{ord}(x)}\) for \(x \neq 0\) and \(|0| = 0\) by convention.

The space \(\mathbb{Z}_p\) is equipped with the natural probability measure \(\mu_p\), which is normalized so that \(\mu_p(\mathbb{Z}_p) = 1\). Elementary \(\mu_p\)-measurable sets are \(p\)-adic balls by which we mean a set \(a + p^k\mathbb{Z}_p\) of radius \(p^{-k}\) for \(a \in \mathbb{Z}_p\). We define the volume of this ball as \(\mu_p(a + p^k\mathbb{Z}_p) = 1/p^k\).

A \(p\)-adic dynamical system on \(\mathbb{Z}_p\) is understood as a triple \((\mathbb{Z}_p, \mu_p, f)\), where \(f : \mathbb{Z}_p \to \mathbb{Z}_p\) is a measurable function. Starting with any chosen point \(x_0\) (an initial point), the trajectory of \(f\) is a sequence of elements of the form

\[x_0, x_1 = f(x_0), \ldots, x_i = f(x_{i-1}) = f^i(x_0)\ldots.\]

Here we say that \(f\) is bijective modulo \(p^n\) for a positive integer \(n\) if a sequence of \(p^n\) elements \(x_0, x_1 = f(x_0), \ldots, f^{p^n-1}(x_0)\) is distinct in the factor ring \(\mathbb{Z}_p/p^n\mathbb{Z}_p\). And \(f\) is said to be transitive modulo \(p^n\) if the above sequence forms a single cycle in \(\mathbb{Z}_p/p^n\mathbb{Z}_p\). We say that a function \(f : \mathbb{Z}_p \to \mathbb{Z}_p\) of the measurable space \(\mathbb{Z}_p\) with the Haar measure \(\mu = \mu_p\) is measure-preserving if \(\mu(f^{-1}(S)) = \mu(S)\) for each measurable subset \(S \subset \mathbb{Z}_p\). A measure-preserving function \(f : \mathbb{Z}_p \to \mathbb{Z}_p\) is said to be ergodic if it has no proper invariant subsets. That is, if \(f^{-1}(S) = S\) for a measurable subset, then \(S \subset \mathbb{Z}_p\) implies that \(\mu(S) = 1\) or \(\mu(S) = 0\). We say that \(f : \mathbb{Z}_p \to \mathbb{Z}_p\) is 1-Lipschitz (or compatible) if for all \(x, y \in \mathbb{Z}_p\),

\[|f(x) - f(y)|_p \leq |x - y|_p.\]

Note that a 1-Lipschitz function \(f\) is continuous on \(\mathbb{Z}_p\). We observe that the 1-Lipschitzness condition has several equivalent statements:

(i) \(|f(x + y) - f(x)|_p \leq |y|_p\) for all \(x, y \in \mathbb{Z}_p\);
(ii) \(|\frac{1}{p}(f(x + y) - f(x))|_p \leq 1\) for all \(x \in \mathbb{Z}_p\) and all \(y \neq 0 \in \mathbb{Z}_p\);
(iii) \(f(x + p^n\mathbb{Z}_p) \subset f(x) + p^n\mathbb{Z}_p\) for all \(x \in \mathbb{Z}_p\) and any integer \(n \geq 1\);
(iv) \(f(x) \equiv f(y) \pmod{p^n}\) whenever \(x \equiv y \pmod{p^n}\) for any integer \(n \geq 1\).

For later use, We recall the following criteria for the measure-preservation and ergodicity of a 1-Lipschitz function:

**Proposition 2.1.** [1] [5] Let \(f : \mathbb{Z}_p \to \mathbb{Z}_p\) be a 1-Lipschitz function.

(i) The following are equivalent:
   (1) \(f\) is measure-preserving;
   (2) \(f\) is bijective modulo \(p^n\) for all integers \(n > 0\);
   (3) \(f\) is an isometry, i.e., \(|f(x) - f(y)|_p = |x - y|_p\) for all \(x, y \in \mathbb{Z}_p\).

(ii) \(f\) is ergodic if and only if it is transitive modulo \(p^n\) for all integers \(n > 0\).

Throughout this paper, we denote the greatest integer that is less than or equal to a real number \(a\) by \([a]\).
2.2 Mahler basis and ergodic functions on $\mathbb{Z}_2$

It is well known [10, 11] that every continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is represented by the Mahler interpolation series

$$f(x) = \sum_{m=0}^{\infty} a_m \binom{x}{m}, \quad (1)$$

where $a_m \in \mathbb{Z}_p$ for $m = 0, \cdots$ and the binomial coefficient functions are defined by

$$\binom{x}{m} = \frac{1}{m!} x(x-1) \cdots (x-m+1) \quad (m \geq 1), \quad \binom{x}{0} = 1.$$

We now state Anashin’s characterization results for the measure-preservation and ergodicity of 1-Lipschitz functions in terms of the coefficients of the Mahler expansion.

**Theorem 2.2. Anashin [1, 2]**

(i) The function $f$ in Eq.(1) is 1-Lipschitz on $\mathbb{Z}_p$ if and only if the following conditions are satisfied: For all $m \geq 0$,

$$|a_m| \leq |p|^{|\log_p m|}.$$

(ii) The function $f$ is a measure-preserving 1-Lipschitz function on $\mathbb{Z}_p$ whenever the following conditions are satisfied:

$$|a_1| = 1; \quad |a_m| \leq |p|^{|\log_p m|+1} \quad \text{for all } m \geq 2.$$

(iii) The function $f$ is an ergodic 1-Lipschitz function on $\mathbb{Z}_p$ whenever the following conditions are satisfied:

$$a_0 \not\equiv 0 \pmod{p}; \quad a_1 \equiv 1 \pmod{p}; \quad a_m \equiv 0 \pmod{|p|^{|\log_p (m+1)|+1}} \quad \text{for all } m \geq 2.$$

(iv) The function $f$ is an ergodic 1-Lipschitz function on $\mathbb{Z}_2$ if and only if the following conditions are satisfied:

$$a_0 \equiv 1 \pmod{2}; \quad a_1 \equiv 1 \pmod{4}; \quad a_m \equiv 0 \pmod{2^{|\log_2 (m+1)|+1}} \quad \text{for all } m \geq 2.$$

Anashin’s proof of Theorem 2.2 (iv) relies on a criteria, namely Theorem 4.39 in [2], based on the algebraic normal form of Boolean functions which determines the measure-preservation and ergodicity of 1-Lipschitz functions. The tricky part of his proof is to use this criterion to derive a recursive formula for the coefficients of Boolean coordinates of a 1-Lipschitz function $f$. As an easy corollary of this theorem, Anashin [2] derives the following result, which turns out to be a useful method for constructing measure-preserving (ergodic) 1-Lipschitz functions out of an arbitrary 1-Lipschitz function. Here recall that $\Delta$ is the difference operator defined by $\Delta f(x) = f(x+1) - f(x)$.

**Corollary 2.3.** Every ergodic (resp. every measure-preserving) 1-Lipschitz function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ can be represented as $f(x) = 1 + x + 2\Delta g(x)$ (resp. as $f(x) = d + x + 2g(x)$) for a suitable constant $d \in \mathbb{Z}_2$ and a suitable 1-Lipschitz function $g : \mathbb{Z}_2 \to \mathbb{Z}_2$ and vice versa, and every function $f$ of the above form is an ergodic (thus, measure-preserving) 1-Lipschitz function.
In this paper, using the van der Put basis, we re-prove this corollary and use it to provide an alternative proof of Theorem 2.2 (iv).

For later use, we recall Lemma 4.41 in [2], from which we deduce one of the main results: Theorem 3.8.

Lemma 2.4. Given a 1-Lipschitz function \( g : \mathbb{Z}_p \to \mathbb{Z}_p \) and a \( p \)-adic integer \( d \not\equiv 0 \pmod{p} \), the function \( f(x) = d + x + p\Delta g(x) \) is ergodic.

2.3 Van der Put basis and ergodic functions on \( \mathbb{Z}_2 \)

We introduce a sequence of the van der Put basis \( \chi(m, x) \) on the ring \( \mathbb{Z}_p \) of \( p \)-adic integers. For an integer \( m \geq 0 \) and \( x \in \mathbb{Z}_p \), we define

\[
\chi(m, x) = \begin{cases} 
1 & \text{if } |x - m| \leq p^{-\lfloor \log_p(m) \rfloor - 1}; \\
0 & \text{otherwise} 
\end{cases}
\]

and

\[
\chi(0, x) = \begin{cases} 
1 & \text{if } |x| \leq p^{-1}; \\
0 & \text{otherwise}. 
\end{cases}
\]

Indeed, the van der Put basis is a characteristic function of the balls \( B_{p^{-\lfloor \log_p(m) \rfloor - 1}}(m) \) (\( m \geq 1 \)) and \( B_{1/p}(0) \). By the well-known result of van der Put [14] (see also [11, 12]), we know that every continuous function \( f : \mathbb{Z}_p \to \mathbb{Z}_p \) is represented by the van der Put series:

\[
f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x),
\]

where \( B_m \in \mathbb{Z}_p \) for \( m = 0, \cdots \). We write an integer \( m > 0 \) in the \( p \)-adic form as

\[
m = m_0 + m_1 p + \cdots + m_s p^s (m_s \neq 0)
\]

From the \( p \)-adic representation of \( m \), we see that

\[
s = \lfloor \log_p(m) \rfloor = (\text{the number of digits in the } p \text{-adic form of } m) - 1
\]

by assuming that \( \lfloor \log_p(0) \rfloor = 0 \). Throughout this paper, we set

\[
q(m) = m_s p^s, \quad m_\sim = m - q(m).
\]

Then we have \( m = m_\sim + q(m) \). What is important here is that the expansion coefficients \( \{B_m\}_{m \geq 0} \) can be recovered by the following formula:

\[
B_m = \begin{cases} 
\frac{f(m) - f(m - q(m))}{f(m)} & \text{if } m \geq p; \\
\frac{f(m) - f(m_\sim)}{f(m)} & \text{otherwise}. 
\end{cases}
\]

As a result parallel to Theorem 2.2, we state the following characterization for the ergodicity of a 1-Lipschitz function \( f \) in terms of the van der Put expansion. Indeed, Yurova [16] and Anashin et al [3, 4] deduce Theorem 2.5 from Corollary 2.3. However, in Section 3.4 we provide an alternate proof of it independently of Theorem 2.2.

Theorem 2.5. Yurova [16] and Anashin et al [3, 4]

(i) The function \( f \) in Eq. (2) is 1-Lipschitz on \( \mathbb{Z}_p \) if and only if the following conditions are satisfied: For all \( m \geq 0 \),

\[
|B_m| \leq |p|^{\lfloor \log_p(m) \rfloor}.
\]
(ii) The 1-Lipschitz function \( f \) on \( \mathbb{Z}_2 \) represented by the van der Put series

\[
f(x) = b_0 \chi(0, x) + \sum_{m=1}^{\infty} 2^{\lfloor \log_2 m \rfloor} b_m \chi(m, x) \quad (b_m \in \mathbb{Z}_2)
\]

is measure-preserving on \( \mathbb{Z}_2 \) if and only if

(1) \( b_0 + b_1 \equiv 1 \pmod{2} \);
(2) \( |b_m| = 1 \) for all \( m \geq 2 \).

(iii) The 1-Lipschitz function \( f \) represented by the van der Put series in Eq. (4) is ergodic on \( \mathbb{Z}_2 \) if and only if the following conditions are satisfied:

(1) \( b_0 \equiv 1 \pmod{2} \);
(2) \( b_0 + b_1 \equiv 3 \pmod{4} \);
(3) \( b_2 + b_3 \equiv 2 \pmod{4} \);
(4) \( |b_m| = 1 \) for all \( m \geq 2 \);
(5) \( \sum_{m=2^{n-1}}^{2^n-1} b_m \equiv 0 \pmod{4} \) for all \( n \geq 3 \).

3 Ergodic \( p \)-adic maps on \( \mathbb{Z}_p \)

In this section, which is divided into four subsections, we present the main results of this paper. We first re-prove the 1-Lipschitz property of \( p \)-adic functions represented by the van der Put series and then provide the sufficient conditions for the measure-preservation of such functions. Using the latter conditions and Corollary 2.4, we provide several conditions for coefficients under which 1-Lipschitz functions on \( \mathbb{Z}_p \) are ergodic. In addition, we present several equivalent conditions for the van Put coefficients for \( p \)-adic functions. We use these equivalent conditions for \( p = 2 \) to provide an alternate proof of Anashin et al.’s criterion in \([3, 4]\), that is, Theorem 2.5 (iii). Finally, using this fact, we provide a simple proof of Anashin’s criterion in \([1]\), that is, Theorem 2.2 (iv).

3.1 Measure-preserving 1-Lipschitz functions on \( \mathbb{Z}_p \)

We provide the necessary and sufficient conditions for \( f \) to be 1-Lipschitz in terms of the coefficients of the van der Put expansion. This result is known \([4]\), but we provide a simple proof.

**Proposition 3.1.** Let \( f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) be a continuous function represented by the van der Put series. Then \( f \) is 1-Lipschitz if and only if \( |B_m| \leq p^{-\lfloor \log_p m \rfloor} \) for all nonnegative integers \( m \).

**Proof.** Assuming that \( f \) is 1-Lipschitz, by the formula for \( B_m \) in Eq. (3) we compute the following for \( m \geq p \):

\[
|B_m| = |f(m) - f(m - q(m))| \leq |q(m)| = p^{-\lfloor \log_p m \rfloor}.
\]

Then the result follows by noting that the inequality holds trivially for \( 0 \leq m < p \).

Conversely, assuming that the inequality holds, we first observe that if \( x \equiv y \pmod{p^n} \), then \( \chi(m, x) = \chi(m, y) \) for all \( 0 \leq m < p^n \). Then, under the assumption that \( x \equiv y \pmod{p^n} \), we compute

\[
f(x) - f(y) = \sum_{m=0}^{\infty} B_m (\chi(m, x) - \chi(m, y)) \equiv \sum_{m=0}^{p^n-1} B_m (\chi(m, x) - \chi(m, y)) \equiv 0 \pmod{p^n},
\]

where the last congruence follows from the observation. Therefore, the result follows.

We now provide the sufficient conditions for a 1-Lipschitz function \( f \) on \( \mathbb{Z}_p \) to be measure-preserving.
Theorem 3.2. The 1-Lipschitz function \( f(x) = \sum_{n=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) is measure-preserving whenever the following conditions are satisfied:

1. \( \{B_0, B_1, \cdots, B_{p-1}\} \) is distinct modulo \( p \).
2. \( B_m \equiv q(m) \pmod{p^{|\log_p m|+1}} \) for all \( m \geq p \).

Proof. By Proposition 2.1 it suffices to show that \( f \) is bijective modulo \( p^n \) for every positive integer \( n \). Because \( \mathbb{Z}_p/p^n\mathbb{Z}_p \) is a finite set, it is also equivalent to showing that \( f \) is injective modulo \( p^n \). Suppose that \( f \) is not injective modulo \( p^n \) for some integer \( n > 0 \). Then we observe \( n \geq 2 \) because \( f \) is injective modulo \( p \), by assumption (1). Here we see that there exist \( a \) and \( b \) in \( \mathbb{Z}_p/p^n\mathbb{Z}_p \) with \( a \neq b \pmod{p^n} \) such that \( f(a) \equiv f(b) \pmod{p^n} \). Write

\[
\begin{align*}
  a &= a_0 + a_1 p + \cdots + a_{n-1} p^{n-1} \quad \text{with} \quad 0 \leq a_i < p, \\
  b &= b_0 + b_1 p + \cdots + b_{n-1} p^{n-1} \quad \text{with} \quad 0 \leq b_i < p.
\end{align*}
\]

Since \( a \neq b \pmod{p^n} \), there exists a nonnegative integer \( r \) such that \( a_r \neq b_r \), for which we may assume that \( r \) is the minimal index (thus \( r \leq n-1 \)). Set

\[
\begin{align*}
  m_1 &= a_0 + a_1 p + \cdots + a_r p^r, \\
  m_2 &= b_0 + b_1 p + \cdots + b_r p^r.
\end{align*}
\]

We can assume that \( a_r \neq 0 \) and \( b_r \neq 0 \). Otherwise, the following argument can be applied in a similar fashion. Because \( f \) is 1-Lipschitz, we first deduce the following inequality:

\[
|f(m_1) - f(m_2)| = |f(m_1) - f(a) + f(a) - f(b) + f(b) - f(m_2)| \\
\leq \max\{|f(m_1) - f(a)|, |f(a) - f(b)|, |f(b) - f(m_2)|\} \\
\leq |p|^{r+1}.
\]

Then we have \( B_{m_1} = f(m_1) - f(m_1) \) and \( B_{m_2} = f(m_2) - f(m_2) \). Since \( m_1 = m_2 \), the preceding inequality yields

\[ B_{m_1} - B_{m_2} = f(m_1) - f(m_2) \equiv 0 \pmod{p^{r+1}}. \]

On the other hand, by assumption (2), we have

\[ B_{m_1} - B_{m_2} \equiv q(m_1) - q(m_2) = (a_r - b_r) p^r \pmod{p^{r+1}}. \]

Because \( a_r \neq b_r \), the preceding congruence gives \( B_{m_1} - B_{m_2} \equiv 0 \pmod{p^{r+1}} \). Therefore, we have a contradiction.

\[ \square \]

We note that condition (1) in Theorem 3.2 is well known to be equivalent to the following congruence (see Lemma 7.3. in [18]): For any prime \( p > 2 \),

\[ \sum_{m=0}^{p-1} B_m k \equiv \begin{cases} 0 \pmod{p} & \text{if } 0 \leq k \leq p - 2; \\
-1 \pmod{p} & \text{if } k = p - 1. \end{cases} \]

For the converse of Theorem 3.2, we have the following

Proposition 3.3. Let \( f(x) = \sum_{n=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) be a measure-preserving 1-Lipschitz function. Then we have the following:

1. \( \{B_0, B_1, \cdots, B_{p-1}\} \) is distinct modulo \( p \).
2. \( |B_m| = |q(m)| = |p|^{\log_p m} \) for all \( m \geq p \).
Proof. It is easy to see that part (1) follows from Proposition 2.1. To deduce part (2), write \( m \geq p \) as \( m = m_1 + q(m) \). Because \( f \) is a measure-preserving \( 1 \)-Lipschitz function, by Proposition 2.1(3) and Eq. (3), we have

\[
|B_m| = |f(m) - f(m_1)| = |m - m_1| = |q(m)|,
\]

which completes the proof. \( \square \)

From Proposition 3.3, we see that the conditions in Theorem 3.2 are necessary for the case in which \( p = 2 \), and therefore we provide an alternate proof of Theorem 2.5 (ii).

**Proposition 3.4.** Let \( f(x) = \sum_{n=0}^{\infty} B_n \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) be a measure-preserving \( 1 \)-Lipschitz function. For \( p^{n-1} \leq m \leq p^n - 1 \) \((n \geq 2)\), set

\[
B_m = p^{n-1}b_m = p^{n-1}(b_{m0} + b_{m1}p + \cdots) \quad (b_{m0} \neq 0, 0 \leq b_{mi} \leq p - 1, i = 0, 1, \ldots).
\]

Then, for all \( n \geq 2 \), we have

\[
\sum_{m=p^{n-1}}^{p^n-1} B_m = \frac{1}{2}(p - 1)p^{2n-1} + T_n p^n \pmod{p^{n+1}},
\]

where \( T_n \) is defined by \( T_n = \sum_{m=p^{n-1}}^{p^n-1} b_{m1} \).

Proof. For given \( m \), write \( m = ip^{n-1} + j \) with \( 1 \leq i \leq p - 1 \), \( 0 \leq j \leq p^{n-1} - 1 \) and \( n \geq 2 \). We show that for any fixed \( j \), \( \{b_{ip^{n-1}+j,0} \mid 1 \leq i \leq p - 1\} \) is distinct, that is, a permutation of \( 1, \ldots, p - 1 \). For such \( j \), we consider \( B_{ip^{n-1}+j} \) for all \( i = 1, \ldots, p - 1 \). Because \( f \) is a measure-preserving \( 1 \)-Lipschitz function, by Eq. (3) and Proposition 2.1(3), we have the following for \( 1 \leq i, i' \leq p - 1 \):

\[
B_{ip^{n-1}+j} - B_{i'p^{n-1}+j} = f(ip^{n-1} + j) - f(i'p^{n-1} + j) \equiv (i - i')p^{n-1} \pmod{p^n}.
\]

From the definition of \( B_m \) in the statement, we also have

\[
B_{ip^{n-1}+j} - B_{i'p^{n-1}+j} \equiv (b_{ip^{n-1}+j,0} - b_{i'p^{n-1}+j,0})p^{n-1} \pmod{p^n},
\]

By equating these two congruence relations, we see that \( i \neq i' \) if and only if \( b_{ip^{n-1}+j,0} \neq b_{i'p^{n-1}+j,0} \), which implies the assertion. Here, by using the assertion to compute the congruence

\[
\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv \sum_{j=0}^{p^n-1} \sum_{i=1}^{p-1} b_{ip^{n-1}+j,0} + T_n p^n \pmod{p^{n+1}},
\]

we obtain the desired result. \( \square \)

### 3.2 Some conditions for ergodic functions on \( \mathbb{Z}_p \)

In this subsection, we provide several conditions for \( B_m \) under which a measure-preserving \( 1 \)-Lipschitz function \( f \) on \( \mathbb{Z}_p \) is ergodic. Therefore, Anashin et al.’s result [3, 4] can be extended to a general case for a prime \( p \).

To begin with, we have the connection between the van der Put expansions of a continuous function \( f \) and \( \Delta f \).

**Proposition 3.5.** If a \( 1 \)-Lipschitz (continuous) function \( f = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) is of the form \( f(x) = \Delta g(x) \) for some \( 1 \)-Lipschitz function \( g = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x) \), then we have

\[
B_m = \begin{cases} 
\tilde{B}_{m+1} - \tilde{B}_m & \text{if } 0 \leq m \leq p - 2; \\
B_0 + \tilde{B}_0 - \tilde{B}_{p-1} & \text{if } m = p - 1;
\end{cases}
\]

\[
= \begin{cases} 
\tilde{B}_{m+1} - \tilde{B}_m & \text{if } m \neq p^{n-1} - 1 + m_{n-1}p^{n-1}, p^{n-1} \leq m \leq p^n - 1, n \geq 2; \\
\tilde{B}_{m+1} - \tilde{B}_m - \tilde{B}_{p-1} & \text{if } m = p^{n-1} - 1 + m_{n-1}p^{n-1}, 1 \leq m_{n-1} \leq p - 1, n \geq 2.
\end{cases}
\]
Proof. For given $g(x) = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x)$, write $g(x + 1) = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x)$ in terms of the van der Put expansion. We first need to determine the relationship between $\tilde{B}_m$ and $\tilde{B}_m'$. By Eq. (3), it is easy to see that for $0 \leq m < p - 1$, $\tilde{B}_m = g(m + 1) = \tilde{B}_{m+1}$ and that $\tilde{B}_p^{-1} = g(p) = \tilde{B}_0 + B_0$. Write $m$ in the $p$-adic form as $m = m_0 + m_1 p + \cdots + m_{n-1} p^{n-1}$ with $0 \leq m_i < p$, $m_{n-1} \neq 0$, and $n \geq 2$. If $m \neq p^{n-1} - 1 + m_{n-1} p^{n-1}$, then we have $g(m + 1) = q(m)$, and therefore, by Eq. (3), we again have

$$\tilde{B}_m = g(m + 1) - g(m + 1 - q(m)) = g(m + 1) - g(m + 1 - q(m + 1)) = \tilde{B}_{m+1}.$$ 

If $m = p^{n-1} - 1 + m_{n-1} p^{n-1} \leq p^n - 1$ with $1 \leq m_{n-1} \leq p - 1$, then $g(m + 1) = q(m) + p^{n-1}$, and therefore we have

$$\tilde{B}_m \equiv g(m + 1) - g(m + 1 - q(m)) = g((m_{n-1} + 1)p^{n-1}) - g(p^{n-1})$$

$$= g((m_{n-1} + 1)p^{n-1}) - g(0) - (g(p^{n-1}) - g(0))$$

$$= \tilde{B}_{m+1} - \tilde{B}_{p^{n-1}}.$$ 

The result follows by equating the coefficients of $f(x)$ and $\Delta g(x)$.

A natural question arising from Proposition 3.5 is under what conditions for coefficients of a 1-Lipschitz function $f$ we have $f$ of the form $f(x) = \Delta g(x)$ for a suitable 1-Lipschitz function $g$. The following result answers this question:

**Proposition 3.6.** Let $f = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function satisfying

1. $\sum_{m=0}^{p-1} B_m \equiv 0 \pmod{p}$;
2. $\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^n}$ for all $n \geq 2$.

Then there exists a 1-Lipschitz function $g(x)$ such that $f(x) = \Delta g(x)$.

**Proof.** By Proposition 3.5 we need to find a 1-Lipschitz function $g(x) = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x)$ whose coefficients $\tilde{B}_m$ satisfy a system of linear equations in Eqs. (6)–(8). We view $B_m$ as the variables required for solving a system of linear equations for countably many variables $\tilde{B}_m$. As in [4] for the case $p = 2$, we inductively construct a sequence of $p$-adic integers $\{\tilde{B}_m\}_{m \geq 0}$ with $\tilde{B}_m \equiv 0 \pmod{p^{|\log_p m|}}$ satisfying the above linear system. From a system of linear equations in Eqs. (6) and (8), we find $p$-adic integers $\tilde{B}_0, \ldots, \tilde{B}_p \in \mathbb{Z}_p$ such that

$$\tilde{B}_m = \tilde{B}_0 + \sum_{i=0}^{m-1} B_i \quad (m = 1, \ldots, p - 1);$$

$$\tilde{B}_p = \sum_{i=0}^{p-1} B_i.$$ 

We take $\tilde{B}_0 \in \mathbb{Z}_p$ arbitrarily and see that assumption (1) guarantees $\tilde{B}_p \equiv 0 \pmod{p}$ for the 1-Lipschitz property. Given that $\tilde{B}_{p^{n-1}} \in \mathbb{Z}_p$ with $\tilde{B}_{p^{n-1}} \equiv 0 \pmod{p^{n-1}}$ ($n \geq 2$), from a system of linear equations in Eqs. (6) and (8), we take $\{\tilde{B}_m\}_{m=p^{n-1}}^{p^n}$ with $\tilde{B}_{p^n} \equiv 0 \pmod{p^n}$ such that for all $\alpha = 1, \ldots, p^{n-1} - 1$,

$$\tilde{B}_{ip^{n-1} + \alpha} = i\tilde{B}_{p^{n-1}} + \sum_{m=p^{n-1}+1}^{ip^{n-1}+\alpha} B_m \quad (i = 1, \ldots, p - 1);$$

$$\tilde{B}_{ip^{n-1}} = i\tilde{B}_{p^{n-1}} + \sum_{m=p^{n-1}+1}^{ip^{n-1}-1} B_m \quad (i = 2, \ldots, p).$$
We see that \( \tilde{B}_{p^m} \equiv 0 \pmod{p^n} \) follows from assumption (2) and check that \( \tilde{B}_m \) \( (p^{n-1} < m < p^n) \) satisfies the 1-Lipschitz property. This completes the proof.

The first part of the following result is observed through Lemma 4.41 in [2]. However, the second part provides a clue about coefficient conditions for the ergodicity of 1-Lipschitz functions in terms of the van der Put expansion.

**Theorem 3.7.** Let \( f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) be a measure-preserving 1-Lipschitz function of the form \( f(x) = d + \varepsilon x + p \Delta g(x) \) for a suitable 1-Lipschitz function \( g(x) \), where \( \varepsilon \equiv 1 \pmod{p} \) and \( d \not\equiv 0 \pmod{p} \). Then (i) the function \( f \) is ergodic.

(ii) We have the following congruence relations:

(1) \( B_0 \equiv s \pmod{p} \) for some \( 0 < s < p \);
(2) \( \sum_{m=0}^{p-1} B_m \equiv ps + \frac{1}{2}(p-1)p \pmod{p^2} \);
(3) \( \sum_{m=p}^{p^2-1} B_m \equiv \frac{1}{2}(p-1)p^3 \equiv \begin{cases} 4 \pmod{p^3} & \text{if } fp = 2; \\ 0 \pmod{p^3} & \text{if } fp > 2; \end{cases} \)

(4) \( B_m \equiv q(m) \pmod{p^{|\log_p m|+1}} \) for all \( m \geq p \);
(5) \( \sum_{m=p}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}} \) for all \( n \geq 3 \).

**Proof.** It is known that the first assertion follows from Lemma 4.41 [2]. For the second assertion, we first note that two simple functions, a constant \( d \in \mathbb{Z}_p \), and \( x \) have an explicit expansion in terms of the van der Put series:

\[
d = \sum_{m=0}^{p-1} d \chi(m, x); \\
x = \sum_{m=1}^{p-1} m \chi(m, x) + \sum_{m=p}^{p^2-1} q(m) \chi(m, x).
\]

If we write a 1-Lipschitz function \( g(x) = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x) \), then we have from Proposition [5,5]

\[
B_m = \begin{cases} 
    d + \varepsilon m + p(\tilde{B}_{m+1} - \tilde{B}_m) & \text{if } 0 \leq m \leq p - 2; \\
    d + \varepsilon(p-1) + p(\tilde{B}_p + B_0 - \tilde{B}_{p-1}) & \text{if } m = p - 1; \\
    \varepsilon q(m) + p(\tilde{B}_{m+1} - \tilde{B}_m) & \text{if } m \neq p^{n-1} - 1 + m_{n-1}p^{n-1}, 1 \leq m_{n-1} \leq p - 1, n \geq 2; \\
    \varepsilon q(m) + p(\tilde{B}_{m+1} - \tilde{B}_m - \tilde{B}_{p^{n-1}}) & \text{if } m = p^{n-1} - 1 + m_{n-1}p^{n-1}, 1 \leq m_{n-1} \leq p - 1, n \geq 2.
\end{cases}
\]

From these formulas for \( B_m \), it is now straightforward to deduce conditions (1)-(4) together with the assumptions about \( d \) and \( \varepsilon \). For condition (5), we have, for all \( n \geq 3 \),

\[
\sum_{m=p}^{p^n-1} B_m \equiv \sum_{m=p}^{p^n-1} B_m - \varepsilon q(m) \pmod{p^{n+1}} \\
\equiv \sum_{m=p}^{p^n-1} p(\tilde{B}_{m+1} - \tilde{B}_m) - p(p-1)\tilde{B}_{p^{n-1}} \\
= p\tilde{B}_{p^n} - p^2\tilde{B}_{p^{n-1}} \equiv 0 \pmod{p^{n+1}},
\]

because \( \tilde{B}_m \) satisfy the 1-Lipschitz property. This completes the proof. \[\square\]
We provide a partial answer for the converse of Theorem 3.7 under some additional condition that is trivially satisfied for the case in which $p = 2$ or $3$. For the first main result, we provide the sufficient conditions under which a measure-preserving 1-Lipschitz function on $\mathbb{Z}_p$ represented by the van der Put series is ergodic. The conditions in Theorem 3.7 reduce to all conditions in Theorem 2.5 (iii) for the case $p = 2$.

**Theorem 3.8.** Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function satisfying all conditions in Theorem 3.7 (ii). If $f$ satisfies the additional condition $B_m \equiv B_0 + m \pmod{p}$ for $0 < m < p$, then $f$ is ergodic.

**Proof.** By Lemma 4.41 in [2] or Lemma 2.4 in Section 2, it suffices to show that the function $f$ is of the form $f = B_0 + x + p\Delta g(x)$ with some 1-Lipschitz function $g(x)$. By Theorem 3.7, we observe that $f$ is measure-preserving. Indeed, this follows from condition (4) in Theorem 3.7 and the additional condition. We now use the said conditions and Eq.(9) to break $f(x)$ up as follows:

$$f(x) = \sum_{m=0}^{p-1} B_m \chi(m, x) + \sum_{m \geq p} (q(m) + pB'_m) \chi(m, x) \text{ with } B'_m \equiv 0 \pmod{p^{\lfloor \log_p m \rfloor}}$$

$$= B_0 \chi(0, x) + \sum_{m=1}^{p-1} (B_0 + m) \chi(m, x) + \sum_{m \geq p} q(m) \chi(m, x) + p \sum_{m \geq 0} B''_m \chi(m, x)$$

$$= B_0 + x + p \sum_{m \geq 0} B''_m \chi(m, x)$$

By equating the coefficients of $f$ on both sides of the preceding equation, we have

$$B_m = \begin{cases} B_0 + m + pB''_m & \text{if } 0 \leq m \leq p - 1; \\ q(m) + pB'_m & \text{if } m \geq p. \end{cases}$$

We use this equation to see that condition (2) in Theorem 3.7 is equivalent to $\sum_{m=0}^{p-1} B''_m \equiv 0 \pmod{p}$ and that conditions (5) and (3) are equivalent to $\sum_{m=p-1}^{p^n-1} B''_m \equiv 0 \pmod{p^n}$ for all $n \geq 2$. Because $B'_m$ for $m \geq p$ satisfy the 1-Lipschitz property, so do $B''_m$ for $m \geq p$. Therefore, we see from Proposition 3.5 that $\sum_{m \geq 0} B''_m \chi(m, x) = \Delta g(x)$ for some 1-Lipschitz function $g(x)$, and we are done.

### 3.3 Equivalent Statements

We provide several equivalent conditions that may be needed for a complete description of the ergodicity of 1-Lipschitz functions on $\mathbb{Z}_p$. For this, we need to observe the following property for 1-Lipschitz functions.

**Lemma 3.9.** Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a 1-Lipschitz function represented by the van der Put series. Then, for all $n \geq 2$, we have

$$\sum_{m=p^{n-1}}^{p^n-1} B_m = \sum_{m=0}^{p^n-1} f(m) - p \sum_{m=0}^{p^{n-1}-1} f(m).$$
Proof. For \( p^{n-1} \leq m < p^n \) with \( n \geq 2 \), write \( m = ip^{n-1} + j \), where \( 1 \leq i < p \) and \( 0 \leq j < p^{n-1} \). We use the formula for \( B_m \) in Eq. (3) to compute \( \sum_{m=p^{n-1}}^{p^n-1} f(m) \) as follows:

\[
\sum_{m=0}^{p^n-1} f(m) - \sum_{m=0}^{p^{n-1}-1} f(m) = \sum_{m=p^{n-1}}^{p^n-1} f(m) = \sum_{m=p^{n-1}}^{p^n-1} B_m + f(m -)
\]

\[
= \sum_{i=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} B_{ip^{n-1}+j} + \sum_{i=1}^{p-1} \sum_{j=0}^{p^{n-1}-1} f(j)
\]

\[
= \sum_{m=p^{n-1}}^{p^n-1} B_m + (p - 1) \sum_{m=0}^{p^{n-1}-1} f(m).
\]

Then we have the desired result. \( \square \)

Remarks 1. If the 1-Lipschitz function \( f = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p \) satisfies the relationship \( f = \Delta g \) for a suitable 1-Lipschitz function \( g = \sum_{m=0}^{\infty} \tilde{B}_m \chi(m, x) \), then it is known from Proposition 3.5 that for \( n \geq 1 \),

\[
\sum_{m=p^{n-1}}^{p^n-1} B_m = \tilde{B}_p^n - p\tilde{B}_{p^{n-1}}.
\]

2. If the additional condition \( g(0) = 0 \) is satisfied, then by Theorem 34.1 in [12], we have

\[
\sum_{m=0}^{p^n-1} f(m) = g(p^n) = \tilde{B}_p^n
\]

for all \( n \geq 1 \).

From this point onward, we assume that \( f : \mathbb{Z}_p \to \mathbb{Z}_p \) is a measure-preserving 1-Lipschitz function. For a nonnegative integer \( m \), we write

\[
f(m) = \sum_{i=0}^{\infty} f_{mi} p^i \text{ with } 0 \leq f_{mi} \leq p - 1 \quad (i = 0, 1, \cdots)
\]

(10)

For an integer \( n \geq 1 \), we define \( S_n \) to be

\[
S_n = \sum_{m=0}^{p^{n-1}} f_{mn}.
\]

(11)

From Lemma 3.9, we immediately see that for all \( n \geq 2 \),

\[
\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}} \Leftrightarrow \sum_{m=0}^{p^n-1} f(m) \equiv p \sum_{m=0}^{p^{n-1}-1} f(m) \pmod{p^{n+1}}.
\]

(12)

Because \( f \) is measure-preserving, the congruence on the right-hand side of Eq. (12) is equivalent to rewriting it as

\[
\frac{1}{2}(p^n - 1)p^n + S_n p^n \equiv p \sum_{m=0}^{p^{n-1}-1} f(m) \pmod{p^{n+1}}.
\]
Canceling $p$ out, we have
\[
\frac{1}{2}(p^n - 1)p^{n-1} + S_n p^{n-1} \equiv \sum_{m=0}^{p^n-1} f(m) \pmod{p^n}.
\]
Because $f$ is again measure-preserving, we have
\[
\frac{1}{2}(p^n - 1)p^{n-1} + S_n p^{n-1} \equiv \frac{1}{2}(p^{n-1} - 1)p^{n-1} + S_{n-1} p^{n-1} \pmod{p^n}.
\]
Canceling $p^{n-1}$ out gives
\[
\frac{1}{2}(p - 1)p^{n-1} + S_n \equiv S_{n-1} \pmod{p} \quad (n \geq 2).
\]
This gives the following congruence:
\[
S_n \equiv \begin{cases} 
S_{n-1} \pmod{p} & (n \geq 2) \text{ if } p \neq 2; \\
S_{n-1} \pmod{2} & (n \geq 3) \text{ if } p = 2.
\end{cases}
\]
On the other hand, because $f$ is measure-preserving, by proposition [5.4] we obtain
\[
\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv \frac{1}{2}(p-1)p^{2n-1} + T_n p^n \pmod{p^{n+1}}.
\]  \quad (13)
This gives the following equivalence: For the case $(p, n)$ in which $n \geq 2$ if the prime $p$ is odd, and $n \geq 3$ otherwise, we have either
\[
\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv 0 \pmod{p^{n+1}} \iff T_n \equiv 0 \pmod{p},
\]
or
\[
\sum_{m=p^{n-1}}^{p^n-1} B_m \equiv T_n p^n \not\equiv 0 \pmod{p^{n+1}} \iff T_n \not\equiv 0 \pmod{p}.
\]
For the case $(p, n) = (2, 2)$, we have from Eq. (13) that either
\[
\sum_{m=2}^{3} B_m \equiv 0 \pmod{2^3} \iff T_2 \equiv 1 \pmod{2},
\]
or
\[
\sum_{m=2}^{3} B_m \equiv 4 \pmod{2^3} \iff T_2 \equiv 0 \pmod{2}.
\]
From Lemma [3.9] and Eq. (13) we deduce the following congruence: For all $n \geq 2$, we have
\[
T_n \equiv S_n - S_{n-1} \pmod{p}.
\]
In sum, we have the following equivalence:

**Theorem 3.10.** Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : \mathbb{Z}_p \to \mathbb{Z}_p$ be a measure-preserving 1-Lipschitz function represented by the van der Put series. In addition, let $b_n, T_n$ and $S_n$ be defined as in Proposition [3.4] and in Eq. (11). Then we have the following equivalence:
(1) \( n = 2 \):
(a) \( p = 2 \):
\[
\sum_{m=2}^{2^2-1} B_m \equiv 4 \pmod{2^3} \iff \sum_{m=2}^{2^2-1} b_m \equiv 2 \pmod{2^3}
\]
\[
\iff S_2 \equiv S_1 \pmod{2} \iff T_2 \equiv 0 \pmod{2};
\]
or
\[
\sum_{m=2}^{2^2-1} B_m \equiv 0 \pmod{2^3} \iff \sum_{m=2}^{2^2-1} b_m \equiv 0 \pmod{2^3}
\]
\[
\iff S_2 \equiv S_1 + 1 \pmod{2} \iff T_2 \equiv 1 \pmod{2}.
\]
(b) \( p > 2 \):
\[
\sum_{m=p}^{p^2-1} B_m \equiv rp^2 \pmod{p^3} \iff \sum_{m=p}^{p^2-1} b_m \equiv rp \pmod{p^2}
\]
\[
\iff S_2 \equiv S_1 + r \pmod{p} \iff T_2 \equiv r \pmod{p}.
\]
(2) \( n \geq 3 \) and any prime \( p \):
\[
\sum_{m=p^n-1}^{p^n-1} B_m \equiv rp^n \pmod{p^{n+1}} \iff \sum_{m=p^n-1}^{p^n-1} b_m \equiv rp \pmod{p^2}
\]
\[
\iff S_n \equiv S_{n-1} + r \pmod{p} \iff T_n \equiv r \pmod{p}.
\]

### 3.4 Alternative proofs of Anashin’s and Anashin et al.’s results

In this section, we use Theorem \[8\] to provide an alternative proof of Theorem \[2,3,10\] (iv). For this, we need the following lemma, which is an analog in \( \mathbb{Z}_2 \) of the result for the formal power series ring \( \mathbb{F}_2[[T]] \) over the field \( \mathbb{F}_2 \) of two elements (see Lemma 1 in \[9\]).

**Lemma 3.11.** Let \( f : \mathbb{Z}_2 \to \mathbb{Z}_2 \) be a measure-preserving 1-Lipschitz function such that \( f \) is transitive modulo \( 2^n, n \geq 1 \). Then \( f \) is transitive modulo \( 2^{n+1} \) if and only if \( S_n \) is odd, where \( S_n \) is defined as in Eq. (14).

**Proof.** (\( \Rightarrow \)): We put \( R_{<n} = \{0, 1, \ldots, 2^n - 1\} \) for a complete set of the least nonnegative representatives of \( \mathbb{Z}_2/2^n\mathbb{Z}_2 \). When we consider the trajectory of \( f(x) \) modulo \( 2^k \), we view \( x \) and \( f(x) \) as elements whose representatives are in \( R_{<k} \). If \( f \) is transitive modulo \( 2^{n+1} \), then there exist \( x_0, x_1 \in R_{<n} \) such that \( f(x_0) = x_1 + 2^n \). Starting with \( x_0 \) as the initial point, we list the trajectory of \( f \) modulo \( 2^{n+1} \) as follows:

\[
x_0 \to f(x_0) \to f^2(x_0) \to f^3(x_0) \to \cdots \to f^{2^n-1}(x_0) \to f^{2^n}(x_0) \to f^{2^n+1}(x_0) \to \cdots \to f^{2^{n+1}-1}(x_0) \to f^{2^{n+1}}(x_0) = x_0 + 2^{n+1}u \pmod{2^{n+1}}
\]

where \( u \in 1 + 2\mathbb{Z}_2 \). Because \( f \) is both measure-preserving and transitive modulo \( 2^{n+1} \), we have \( f^{2^n}(x_0) = x_0 + 2^n \). We use this relationship to iteratively derive the relationship

\[
f^{2^{n+i}}(x_0) \equiv f^i(x_0) + 2^n \pmod{2^{n+1}} \quad (0 \leq i \leq 2^n - 1).
\]
We claim that $S_n$ is odd and thus that $S_n = \#\{0 \leq m \leq 2^n - 1 : f_{mn} = 1\}$ is odd, where $f_{mn}$ is defined in Eq. (10). If there exists a number in $R_{<n}$ other than $x_0$ mapped by $f$ to an element in $R_{<n} + 2^n$ in the first row of the diagram in Eq. (11), then there exists another element in $R_{<n} + 2^n$ that maps to an element in $R_{<n}$. By the relationship in Eq. (15), we see that there must be an element in $R_{<n}$ that is mapped by $f$ to an element in $R_{<n} + 2^n$ in the second row. This implies that the total number of elements in $R_{<n}$ that are mapped by $f$ to an element in $R_{<n} + 2^n$ is odd and thus that $S_n$ is odd.

Conversely, assuming that $S_n$ is odd, we see that there exist $x_0, x_1 \in R_{<n}$ such that $f(x_0) = x_1 + 2^n$. From the above diagram, because $f$ is transitive modulo $2^n$, we observe that the elements of the first row as well as those in the second row are distinct modulo $2^n$. We now show that $f^{2^n}(x_0) = x_0 + 2^n$. Otherwise, we have $f^{2^n}(x_0) = x_0$, and therefore we see that $\#\{0 \leq m \leq 2^n - 1 : f_{mn} = 1\}$ is even, which is a contradiction. As in the "only if" part, we use $f^{2^n}(x_0) = x_0 + 2^n$ to derive the relationship in Eq. (15). Therefore, these relationships imply that the trajectory of $f$ modulo $2^{n+1}$ are all distinct modulo $2^{n+1}$. Hence, $f$ is transitive modulo $2^{n+1}$.

\[ \square \]

**Theorem 3.12.** Let $f(x) = \sum_{m=0}^{\infty} B_m \chi(m, x) : Z_2 \to Z_2$ be a 1-Lipschitz function. Then $f$ is ergodic if and only if all conditions in Theorem 2.5 (iii) are satisfied.

**Proof.** We see that the "if" part follows immediately from Theorem 3.8 because the additional condition there is trivially satisfied for $p = 2$. For the "only if" part, we note that $S_1 = 1$, so this direction follows from Lemma 2.14 and Theorem 3.10. \[ \square \]

As a corollary, we reproduce Corollary 2.3.

**Corollary 3.13.** Let $f : Z_2 \to Z_2$ be a 1-Lipschitz function. Then, (1) $f$ is measure-preserving if and only if $f$ is of the form $f(x) = d + x + 2g(x)$ for some 2-adic integer $d \in Z_2$ and some 1-Lipschitz function $g(x)$.

(2) $f$ is ergodic if and only if $f$ is of the form $f(x) = 1 + x + 2\Delta g(x)$ for some 1-Lipschitz function $g(x)$.

**Proof.** For the first assertion, the "if" part follows from Proposition 2.1 (3). And the "only if" part comes from Theorem 3.2 because the conditions there is necessary in the case $p = 2$.

For the second assertion, the "if" part follows from Lemma 4.41 in [2] and the "only if" part follows from Theorems 3.12 and 3.8. \[ \square \]

We now use Corollary 3.13 to provide an alternate proof of Theorem 2.4 (iv). For this, we first need to provide the 1-Lipschitz conditions in Theorem 2.2 (i). However, we just mention that this property can be proved in the similar way by using the well-known binomial formula in [9, 15] for Carlitz polynomials over functions fields.

**Corollary 3.14.** Let $f(x) = \sum_{m=0}^{\infty} a_m \left(\frac{x}{d}\right) : Z_2 \to Z_2$ be a 1-Lipschitz function. Then $f$ is ergodic if and only if all conditions in Theorem 2.2 (iv) are satisfied.

**Proof.** It follows from Corollary 3.13. \[ \square \]

4 **An Application**

In this final section, we use Theorem 2.5 to derive a characterization for the ergodicity of a polynomial over $Z_2$ in terms of its coefficients. For simplicity, we take a polynomial $f \in Z_2[x]$ with $f(0) = 1$. That is, let $f = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_1x + 1$ be a polynomial of degree $d$ over $Z_2$. Then we set

$$ A_0 = \sum_{i \equiv 0 \pmod{2}, i > 0} a_i, \quad A_1 = \sum_{i \equiv 1 \pmod{2}} a_i. $$
**Theorem 4.1.** The polynomial $f$ is ergodic over $\mathbb{Z}_2$ if and only if the following conditions are simultaneously satisfied:

\[
\begin{align*}
    a_1 & \equiv 1 \pmod{2}; \\
    A_1 & \equiv 1 \pmod{2}; \\
    A_0 + A_1 & \equiv 1 \pmod{4}; \\
    a_1 + 2a_2 + A_1 & \equiv 2 \pmod{4}.
\end{align*}
\]

**Proof.** From Theorem 2.5 (iii) or Theorem 3.12, we derive the equivalent conditions as required. Because $B_0 + B_1 = f(0) + f(1) = 2 + A_0 + A_1$, we can easily see that $B_0 \equiv 1 \pmod{2}$ and $B_1 \equiv 1 \pmod{2}$. We have:

\[
B_0 + B_1 = f(0) + f(1) = 2 + A_0 + A_1.
\]

Because $B_2 = 2b_2 = f(2) - f(0), B_3 = 2b_3 = f(3) - f(1)$, we see that $b_2 + b_3 \equiv 2 \pmod{4}$ is equivalent to $f(2) - f(0) + f(3) - f(1) \equiv 4 \pmod{8}$. Because $f(3) = \sum_{i=0}^{d} a_i 3^i \equiv 1 + A_0 + 3A_1 \pmod{8}$, we have the following equivalence:

\[
b_2 + b_3 \equiv 2 \pmod{4} \iff a_1 + 2a_2 + A_1 \equiv 2 \pmod{4}.
\]

For all $m \geq 2$, we have:

\[
B_m = f(m) - f(m) = \sum_{i=1}^{d} a_i (m^i - m_\text{rad}) = \sum_{i=1}^{d} a_i \sum_{j=1}^{i} \binom{i}{j} m_{\text{rad}}^{i-j} q(m)^j = \sum_{j=1}^{d} \left( \sum_{i=j}^{d} \binom{i}{j} a_i m_{\text{rad}}^{i-j} \right) q(m)^j.
\]

The preceding equation implies that condition (4) is equivalent to $f'(m_{\text{rad}}) \in 1 + 2\mathbb{Z}_2$ for all $m \geq 2$, where $f'(x)$ is the derivative of $f$. Equivalently, $f'(0) = a_1 \in 1 + 2\mathbb{Z}_2$ and $f'(1) = A_1 \in 1 + 2\mathbb{Z}_2$. From Eq. (16), we can deduce that for all $m \geq 2$, $b_m \equiv f'(m_{\text{rad}}) \pmod{q(m)}$. From this, we obtain the following congruence: For $n \geq 3$,

\[
\sum_{m=2^n-1}^{2^n-2} b_m \equiv \sum_{m=2^n-1}^{2^n-2} f'(m_{\text{rad}}) = \sum_{j=0}^{2^n-1} f'(j) \equiv 2^{n-3}(f'(0) + f'(1) + f'(2) + f'(3)) \equiv 2^{n-2}(A_1 - a_1) \pmod{4}.
\]

This congruence implies that condition (5) is redundant. This completes the proof.

**Remarks**

1. We first mention that all conditions in Theorem 4.1 are easily proved to be equivalent to those in 5 or 8.

2. We point out that the result for this theorem extends to a class of analytic functions on $\mathbb{Z}_p$ by which we mean those functions represented by the Taylor series on all $\mathbb{Z}_p$.

3. The characterization for the ergodicity of 1-Lipschitz functions provides a clue for a complete description of the necessary and sufficient conditions for a polynomial function on $\mathbb{Z}_p$ in terms of its coefficients, as in Theorem 4.1.

4. Future research should use the results in this paper, particularly those for Theorems 3.8 and 3.10 to provide a complete description of an ergodic 1-Lipschitz function $\mathbb{Z}_p$ represented by the van der Put series for all odd primes $p$. 


References

[1] V. S. Anashin, Uniformly distributed sequences of $p$-adic integers, *Math. Notes* 55 (1994), no. 1-2, 109-133
[2] V. Anashin, A. Khrennikov, *Applied algebraic dynamics*, de Gruyter Expositions in Mathematics, 49. Walter de Gruyter & Co., Berlin, 2009. xxiv+533 pp.
[3] V. Anashin, A. Khrennikov and E. Yurova, Characterization of ergodicity of $p$-adic dynamical systems by using the van der Put basis, *Doklady Mathematics* 83 (3) (2011) 1-3
[4] V. Anashin, A. Khrennikov and E. Yurova, *T*-Functions Revisited: New Criteria for Bijectivity/Transitivity, arXiv:1111.3093v1
[5] 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.
[6] S. Jeong, Characterization of ergodicity of $T$-adic maps on $\mathbb{F}_2[[T]]$ using digit derivatives basis, preprint.
[7] A. Klimov and A. Shamir, Cryptographic applications of $T$-functions, Selected areas in cryptography, 248-261, Lecture Notes in Comput. Sci., 3006, Springer, Berlin, 2004,
[8] M. V. Larin, Transitive polynomial transformations of residue class rings, *Discrete Math. Appl.* 12 (2002) 127-140.
[9] D. Lin, T. Shi and Z. Yang, Ergodic Theory over $\mathbb{F}_2[[T]]$, *Finite Fields and Their Applications*, 18 (2012), 473-491.
[10] K. Mahler, An interpolation series for a continuous function of a $p$-adic variable, *J. Reine Angew. Math.*, 199 (1958),23-34.
[11] K. Mahler, *p-adic numbers and their applications*, second edition, Cambridge University Press. (1981).
[12] W. Schikhof, *Ultrametric Calculus*, Cambridge University Press, 1984.
[13] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications 20 (Cambridge University Press, Cambridge, 1997)
[14] M. van der Put, Alg’ebres de fonctions continues p-adiques, Universiteit Utrecht, 1967. 2
[15] Z. Yang, $C^n$-functions over completions of $\mathbb{F}_r[T]$ at finite places of $\mathbb{F}_r(T)$, *J. Number Theory* 108 (2004), no. 2, 346-374
[16] E. Yurova, Van der Put basis and $p$-adic dynamics, *P-adic Numbers, Ultrametric Analysis and Applications* 2 (2) (2010), 175-178.