BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 64, No. 1, 2016

NUMBER THEORY

Ergodic Products and Powers on Compact Subsets of the p-adic Field

by

Nacima MEMIĆ

Presented by Feliks PRZYTYCKI

Summary. We study powers of ergodic functions on compact subsets of the p-adic field. The same question is considered for products of compact subsets of the p-adic field.

1. Introduction. H. Diao and C. E. Silva [6] studied rational functions on the p-adic field. They proved necessary conditions for rational functions to be locally isometric or measure preserving. They provided digraph representations for locally isometric invertible functions on compact subsets of the p-adic field. Anashin [1] gave a characterization of measure-preserving and ergodic 1-Lipschitz maps on the set $\mathbb{Z}_p$ of p-adic integers, which generalizes some of the results in [4], [5], [7].

In this work we analyse powers and products of ergodic functions on compact subsets of the p-adic field.

We begin with some basic definitions which can also be found in [6] and [8].

Let X be a compact subset of the p-adic field $\mathbb{Q}_p$ and $f : X \to X$ an invertible function. The function f is said to be *locally isometric* if there exists an integer l such that

$$(*) \qquad |f(x) - f(y)| = |x - y| \quad \text{whenever} \quad |x - y| \le p^l.$$

It was proved in [6, Theorem 3.1] that any rational function f satisfying these conditions is measure preserving and that X consists of a union of $p^{-l}\mathbb{Z}_p$-cosets which form cycles or orbits of f. Following the same steps as

2010 *Mathematics Subject Classification*: Primary 11S82; Secondary 37P20, 11K41.
Key words and phrases: p-adic field, ergodic functions, transitive functions.
Received 8 July 2015; revised 25 June 2016.
Published online 25 August 2016.

in the proof of [6, Theorem 3.1] it can be easily seen that this result can be extended to any invertible locally isometric function.

If the set X can be written as $\biguplus_{i=1}^{n} B_{p^l}(y_i)$, where l is as in $(*)$ and $B_{p^k}(z) := \{x \in \mathbb{Q}_p : |x - z| \le p^k\}$, then for all $m \le l$, X can also be put in the form $X = \biguplus_{i=1}^{np^{l-m}} B_{p^m}(x_i)$.

f is said to be *transitive modulo* p^{-m} if by permuting indices we can get $f(B_{p^m}(x_i)) = B_{p^m}(x_{i+1})$ for $i \in \{1, \dots, p^{l-m}n - 1\}$ and $f(B_{p^m}(x_{p^{l-m}n})) = B_{p^m}(x_1)$. In other words the f-orbit of $B_{p^m}(x_1)$ is the whole X.

It was proved in [2, Theorem 4.23] and [2, Proposition 4.35] that an invertible 1-Lipschitz function f is ergodic on $\mathbb{Z}_p$ if it is transitive modulo p^{-m} for all $m \le l$. Following the steps in the proof of [6, Theorem 3.2] which was formulated for rational functions, we can see that [2, Theorem 4.23] and [2, Proposition 4.35] are also valid on any compact subset of $\mathbb{Q}_p$.

2. Main results

LEMMA 2.1. *Let $X = \biguplus_{i=1}^{n} B_{p^l}(x_i)$ be a compact subset of $\mathbb{Q}_p$, where l is an arbitrary integer. Let $f : X \to X$ be invertible and locally isometric such that $|f(x) - f(y)| = |x - y|$ whenever $|x - y| \le p^l$. Let k be any positive integer.*

- (i) *If k and n are not relatively prime, then f^k is not transitive modulo p^{-l}.*
- (ii) *If k and n are relatively prime, then f^k is transitive modulo p^{-l} if and only if f is transitive modulo p^{-l}.*

Proof. It is clear that if f is not transitive modulo p^{-l} then no power of f can be transitive. Therefore, it suffices to prove this result with the assumption that f is transitive modulo p^{-l}. Without loss of generality we may assume that

$$f(B_{p^l}(x_i)) = B_{p^l}(x_{i+1}) \text{ for } i \in \{1, \dots, n-1\} \text{ and } f(B_{p^l}(x_n)) = B_{p^l}(x_1),$$

so that

$$f^{s-1}(B_{p^l}(x_1)) = B_{p^l}(x_{s \,(\mathrm{mod}\, n)}), \qquad \forall s \ge 2. \tag{2.1}$$

(i) Let $k = sd$ and $n = td$, where s and t are relatively prime and $d > 1$. Then

$$(f^k)^t(B_{p^l}(x_1)) = (f^n)^s(B_{p^l}(x_1)) = B_{p^l}(x_1).$$

The result follows since $t < n$.

(ii) Suppose that k and n are relatively prime. If f^k is not transitive then there exists $i \in \{2, \dots, n\}$ such that $f^{ks}(B_{p^l}(x_1)) \ne B_{p^l}(x_{i \,(\mathrm{mod}\, n)})$ for every positive integer s. From (2.1) we see that $i - 1 \ne ks \pmod{n}$ or equivalently $i - 1 \ne ks - rn$ for all nonnegative integers r, s, which obviously contradicts the Euclidean algorithm. ∎

THEOREM 2.2. *Let $X = \biguplus_{i=1}^{n} B_{p^l}(x_i)$ be a compact subset of $\mathbb{Q}_p$, where l is an arbitrary integer, and let k be any positive integer. Let $f : X \to X$ be invertible and locally isometric such that $|f(x) - f(y)| = |x - y|$ whenever $|x - y| \le p^l$. Then f^k is ergodic if and only if:*

(1) *f is ergodic,*
(2) *$p \cdot n$ and k are relatively prime.*

Proof. Suppose that (1) and (2) are true. By Lemma 2.1 we infer that f^k is transitive modulo p^{-s} for every integer $s \le l$.

On the other hand, if (1) is not valid then obviously f^k is not ergodic. Moreover, if f is ergodic and (2) is not valid, Lemma 2.1 implies that f^k is not transitive modulo p^{l-1}, so f^k is not ergodic. ∎

PROPOSITION 2.3. *Let $X = \biguplus_{i=1}^{n} B_{p^l}(x_i)$ be a compact subset of $\mathbb{Q}_p$, where l is an arbitrary integer, and let k be any positive integer. Let $f : X \to X$ be invertible and locally isometric such that $|f(x) - f(y)| = |x - y|$ whenever $|x - y| \le p^l$. Assume in addition that f is transitive modulo p^{-l}. Then f is ergodic if and only if for every subset $Y = \biguplus_{s=1}^{m} B_{p^l}(x_{i_s})$ of X, the function $g : Y \to Y$ defined by*

$$g(x) = \begin{cases} f^{i_{s+1}-i_s}(x), & x \in B_{p^l}(x_{i_s}),\ s \in \{1, \dots, m-1\}, \\ f^{i_1-i_m+n}(x), & x \in B_{p^l}(x_{i_m}), \end{cases}$$

is ergodic.

Proof. It suffices to prove the claim for Y of the form $\biguplus_{i=1}^{n-1} B_{p^l}(x_i)$ and show that the choice of x_n is arbitrary and can be replaced by any other element from $\{x_1, \dots, x_{n-1}\}$. Indeed, if the previous assertion is proved then recursively we can generalise the result. In this way we would also have proved that f is ergodic if and only if there exists one subset Y composed of a disjoint union of $p^{-l}\mathbb{Z}_2$-cosets on which g is ergodic.

First suppose that f is ergodic. Let $m < l$. For every $y \in B_{p^l}(x_{n-1})$ we have $g(B_{p^m}(y)) = f^2(B_{p^m}(y)) \subset B_{p^l}(x_1)$. Thus the g-orbit of $B_{p^m}(x_1)$ is its f-orbit from which we have removed the set $B_{p^l}(x_n)$. Hence this is in fact the whole set Y where each $p^{-m}\mathbb{Z}_2$-coset appears only once. By [6, Theorem 3.2] we conclude that g is ergodic.

Suppose that for some $m < l$, f is not transitive modulo p^{-m}. Then the f-orbit of $B_{p^m}(y)$ is strictly contained in X for every $y \in B_{p^l}(x_{n-1})$. Since f is transitive modulo p^{-l}, the intersection of the f-orbit of $B_{p^m}(y)$ with any of the balls $B_{p^l}(x_i)$, $i \in \{1, \dots, n\}$, is not empty and it is strictly contained in that ball. Since $g(y) = f^2(y)$ is also in the f-orbit of y, we conclude that the g-orbit of $B_{p^m}(y)$ remains strictly contained in Y, hence g cannot be transitive modulo p^{-m}. ∎

By means of the characterization of ergodic 1-Lipschitz functions on $\mathbb{Z}_2$ given in [9], [3] and Proposition 2.3 we suggest an ergodicity test for some subsets of $\mathbb{Z}_2$, for example a union of two $4\mathbb{Z}_2$-cosets as shown in the example below.

First we recall Yurova and Anashin's theorem on ergodicity of 1-Lipschitz functions on $\mathbb{Z}_2$.

Theorem 2.4 (Yurova and Anashin [9], [3], [1]). *A 1-Lipschitz function f is ergodic on $\mathbb{Z}_2$ if and only if the following conditions are satisfied:*

(1) $f(0) = 1 \pmod 2$,
(2) $f(0) + f(1) = 3 \pmod 4$,
(3) $\dfrac{f(2) - f(0) + f(3) - f(1)}{2} = 2 \pmod 4$,
(4) $|f(m) - f(m - 2^n)| = 2^{-n}$ *for all* $m \in \{2^n, \dots, 2^{n+1} - 1\}$,
(5) $2^{-n+1} \displaystyle\sum_{m=2^{n-1}}^{2^n - 1} (f(m) - f(m - 2^{n-1})) = 0 \pmod 4$ *for all* $n \geq 3$.

Example 2.5. *Let $g : 4\mathbb{Z}_2 \cup 1 + 4\mathbb{Z}_2 \to 4\mathbb{Z}_2 \cup 1 + 4\mathbb{Z}_2$ be isometric invertible and transitive modulo 4. Then g is ergodic if and only if:*

- $\dfrac{g(1) - g(0) - 1}{2} = 2 \pmod 4$,
- $\displaystyle\sum_{m=4,5} (g(m) - g(m-4)) = 2^3 \pmod{2^4}$,
- $\displaystyle\sum_{m=0,1 \pmod 4} (g(m) - g(m - 2^{n-1})) = 0 \pmod{2^{n+1}}$ *for* $n \geq 4$,

where the last sum over m is taken over $m \in \{2^{n-1}, \dots, 2^n - 1\}$.

Proof. Let $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ be defined as follows:

$$f(x) = \begin{cases} g(x), & x \in 4\mathbb{Z}_2, \\ x + 2, & x \in 1 + 4\mathbb{Z}_2, \\ x - 1, & x \in 3 + 4\mathbb{Z}_2, \\ g(x-1), & x \in 2 + 4\mathbb{Z}_2. \end{cases}$$

Notice that f and g are equal on $4\mathbb{Z}_2$ and $g = f^3$ on $1 + 4\mathbb{Z}_2$. Then f and g are related as in Proposition 2.3, which implies that they are either simultaneously ergodic or non-ergodic. Conditions (1), (2) and (4) of Theorem 2.4 are obviously satisfied for f.

Now we analyse under what conditions f satisfies condition (3) of Theorem 2.4. Since

$$\frac{f(2) - f(0) + f(3) - f(1)}{2} = \frac{g(1) - g(0) - 1}{2},$$

f satisfies condition (3) of Theorem 2.4 if and only if

$$\frac{g(1)-g(0)-1}{2} = 2 \pmod 4.$$

Similarly,

$$\begin{aligned}
&\sum_{m=2^{n-1}}^{2^n-1} (f(m)-f(m-2^{n-1}))\\
&= \Big(\sum_{m=0 \,(\mathrm{mod}\, 4)} + \sum_{m=1 \,(\mathrm{mod}\, 4)} + \sum_{m=2 \,(\mathrm{mod}\, 4)} + \sum_{m=3 \,(\mathrm{mod}\, 4)}\Big)(f(m)-f(m-2^{n-1}))\\
&= \sum_{m=0 \,(\mathrm{mod}\, 4)} (g(m)-g(m-2^{n-1}))\\
&\quad + \sum_{m=2 \,(\mathrm{mod}\, 4)} (g(m-1)-g(m-2^{n-1}-1)) + \sum_{m=1,3 \,(\mathrm{mod}\, 4)} 2^{n-1}\\
&= \sum_{m=0,1 \,(\mathrm{mod}\, 4)} (g(m)-g(m-2^{n-1})) + 2^{n-1}2^{n-2}.
\end{aligned}$$

Therefore, f satisfies condition (5) of Theorem 2.4 if and only if

$$\begin{cases} \displaystyle\sum_{m=0,1 \,(\mathrm{mod}\, 4)} (g(m)-g(m-2^{n-1})) = 2^3 \pmod{2^4}, & n=3,\\ \displaystyle\sum_{m=0,1 \,(\mathrm{mod}\, 4)} (g(m)-g(m-2^{n-1})) = 0 \pmod{2^{n+1}}, & n \geq 4, \end{cases}$$

where the sums are taken over $m \in \{2^{n-1}, \dots, 2^n-1\}$. ∎

THEOREM 2.6. *Let $X^j = \biguplus_{i=1}^{n^j} B_{p^l}(x_i^j)$, $j \in \{1,\dots,m\}$, be compact subsets of $\mathbb{Q}_p$, where l is an arbitrary integer. For every $j \in \{1,\dots,m\}$ let $f_j : X^j \to X^j$ be invertible and locally isometric such that $|f_j(x)-f_j(y)| = |x-y|$ whenever $x,y \in X^j$ with $|x-y| \leq p^l$. Let k_j, $j \in \{1,\dots,m\}$, be any positive integers. Then $f_1^{k_1} \times \cdots \times f_m^{k_m} : X^1 \times \cdots \times X^m \to X^1 \times \cdots \times X^m$ is ergodic if and only if*

(1) *f_j, $j \in \{1,\dots,m\}$, are ergodic,*
(2) *pn^j and k_j are relatively prime for every $j \in \{1,\dots,m\}$,*
(3) *n^i and n^j are relatively prime for all $i \neq j$ from $\{1,\dots,m\}$.*

Proof. We first handle the special case when $k_j = 1$ for all $j \in \{1,\dots,m\}$. We will prove that $f_1 \times \cdots \times f_m$ is ergodic if and only if conditions (1) and (3) are satisfied.

It is easily seen that if some f_j is not ergodic then $f_1 \times \cdots \times f_m$ cannot be ergodic. Now assume that all f_j are ergodic.

Without loss of generality we may assume that n^1 and n^2 are not relatively prime. Let M be the smallest common multiple of $n^1, \dots, n^m$.

There exist integers s and t such that $M = sn^1 = tn^2$. We will show that for each $n \in \mathbb{N}$,

$$(f_1 \times \cdots \times f_m)^n(B_{p^l}(x_1^1) \times \cdots \times B_{p^l} x_1^m))$$

differs from

$$B_{p^l}(x_1^1) \times B_{p^l}(f_2^{tn^2+1}(x_1^2)) \times B_{p^l}(t_3) \times \cdots \times B_{p^l}(t_m),$$

for every $t_j \in X^j$, $j \geq 3$.

Indeed, suppose that for some positive integer n we have

$$B_{p^l}(x_1^1) = f_1^n(B_{p^l}(x_1^1))$$

and

$$f_2^{tn^2+1}(B_{p^l}(x_1^2)) = f_2^n(B_{p^l}(x_1^2)).$$

If f_1 and f_2 are ergodic then n must be a multiple of n^1 and $f_2^{tn^2}(B_{p^l}(x_1^2)) = B_{p^l}(x_1^2)$. Hence, $f_2^{n-1}(B_{p^l}(x_1^2)) = B_{p^l}(x_1^2)$ and $n-1$ is a multiple of n^2. It follows that $n = rn^1 = t'n^2 + 1$, but this is impossible if n^1 and n^2 are not relatively prime.

Now, suppose that (1) and (3) are satisfied. For every $j \in \{1, \dots, m\}$, let $i_j \in \{1, \dots, n^j\}$ be arbitrary. We will show that

$$B_{p^l}(x_{i_1}^1) \times \cdots \times B_{p^l}(x_{i_m}^m) = (f_1 \times \cdots \times f_m)^n(B_{p^l}(x_1^1) \times \cdots \times B_{p^l}(x_1^m))$$

for some integer n.

Indeed, for each $j \in \{1, \dots, m\}$ there exists an integer r_j such that

$$r_1 n^1 + i_1 = r_2 n^2 + i_2 = \cdots = r_m n^m + i_m.$$

The result follows immediately by setting $n = r_1 n^1 + i_1$.

Now, let k_j, $j \in \{1, \dots, m\}$, be any positive integers and assume that conditions (1)–(3) are satisfied. By Theorem 2.2, condition (2) implies that each $f_j^{k_j}$, $j \in \{1, \dots, m\}$, is ergodic. Then the first part of the proof shows that $f_1^{k_1} \times \cdots \times f_m^{k_m}$ is ergodic.

Conversely, if $f_1^{k_1} \times \cdots \times f_m^{k_m}$ is ergodic then by the first part of the proof we see that condition (3) is satisfied and each $f_j^{k_j}$, $j \in \{1, \dots, m\}$, is ergodic. Similarly, Theorem 2.2 implies that conditions (1) and (2) are satisfied. ∎

Remark 2.7. In [2, Theorem 4.51] it was proved that there is no ergodic uniformly differentiable function with integer-valued partial derivatives modulo p on $\mathbb{Z}_p^m$ for $m \geq 2$. From condition (3) we can see that Theorem 2.6 is stated in a different context. Namely, the product is taken between mutually different sets X_j, $j \in \{1, \dots, m\}$. Hence, Theorem 2.6 cannot be applied on $\mathbb{Z}_p^m$.

Acknowledgements. I would like to thank the referees for their remarks and suggestions.

References

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

[2] V. Anashin and A. Khrennikov, *Applied Algebraic Dynamics*, de Gruyter Exp. Math. 49, de Gruyter, Berlin, 2009.

[3] V. Anashin, A. Khrennikov and E. Yurova, *Characterization of ergodicity of p-adic dynamical systems by using the van der Put basis*, Dokl. Mat. 83 (2011), 306–308 (in Russian).

[4] J. Bryk and C. E. Silva, *Measurable dynamics of simple p-adic polynomials*, Amer. Math. Monthly 112 (2005), 212–232.

[5] Z. Coelho and W. Parry, *Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers*, in: Topology, Ergodic Theory, Real Algebraic Geometry, Amer. Math. Soc. Transl. (2) 202, Amer. Math. Soc., 2001, 51–70.

[6] H. Diao and C. E. Silva, *Digraph representations of rational functions over the p-adic numbers*, p-Adic Numbers Ultrametric Anal. Appl. 3 (2011), 23–38.

[7] M. Gundlach, A. Khrennikov and K.-O. Lindahl, *On ergodic behavior of p-adic dynamical systems*, Infin. Dimens. Anal. Quantum Probab. Related Topics 4 (2001), 569–577.

[8] S. Jeong, *Toward the ergodicity of p-adic 1-Lipschitz functions represented by the van der Put series*, J. Number Theory 133 (2013), 2874–2891.

[9] E. Yurova, *Van der Put basis and p-adic dynamics*, p-Adic Numbers Ultrametric Anal. Appl. 2 (2010), 175–178.

Nacima Memić
Department of Mathematics
Faculty of Natural Sciences and Mathematics
University of Sarajevo
Zmaja od Bosne 33-35
Sarajevo, Bosnia and Herzegovina
E-mail: nacima.o@gmail.com