Ergodic Transformations in the Space of p-adic Integers

Vladimir Anashin

Faculty of Information Security, Russian State University for the Humanities, Kirovogradskaya Str., 25/2, Moscow 113534, Russia

Abstract. Let $\mathcal{L}_1$ be the set of all mappings $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ of the space of all p-adic integers $\mathbb{Z}_p$ into itself that satisfy Lipschitz condition with a constant 1. We prove that the mapping $f \in \mathcal{L}_1$ is ergodic with respect to the normalized Haar measure on $\mathbb{Z}_p$ if and only if f induces a single cycle permutation on each residue ring $\mathbb{Z}/p^k\mathbb{Z}$ modulo p^k, for all $k = 1, 2, 3, \ldots$. The multivariate case, as well as measure-preserving mappings, are considered also.

Results of the paper in a combination with earlier results of the author give explicit description of ergodic mappings from $\mathcal{L}_1$. This characterization is complete for $p = 2$.

As an application we obtain a characterization of polynomials (and certain locally analytic functions) that induce ergodic transformations of p-adic spheres. The latter result implies a solution of a problem (posed by A. Khrennikov) about the ergodicity of a perturbed monomial mapping on a sphere.

1. INTRODUCTION

Let $\mathcal{L}_1$ be the set of all functions $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ defined on (and valuated in) the space $\mathbb{Z}_p$ of all p-adic[1] integers that satisfy Lipschitz condition with a constant 1 with respect to the p-adic metric $\|\cdot\|_p$: $\|f(x) - f(y)\|_p \le \|x - y\|_p$ for all $x, y \in \mathbb{Z}_p$. For $p = 2$ this class is of particular practical importance for computer science since it includes all mappings combined of standard microprocessor instructions, such as arithmetic ones (integer addition, multiplication, etc.) and bitwise logical ones (such as AND, bitwise logical 'and'; OR, bitwise logical 'or', etc.); see [5] and [4] for details.

Any mapping $f \in \mathcal{L}_1$ naturally induces a well-defined mapping $\bar{f}_k = f \bmod p^k\colon \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ of the residue ring $\mathbb{Z}/p^k\mathbb{Z}$ into itself by letting $\bar{f}_k(z) = f(z) \bmod p^k$, the least non-negative residue of $f(z)$ modulo p^k. That is, $\bar{f}_k(z)$ is the smallest non-negative rational integer v such that $\|v - f(z)\|_p \le p^{-k}$ or, in other words, $\bar{f}_k(z) = v_0 + v_1 \cdot p + v_2 \cdot p^2 + \cdots + v_{k-1} \cdot p^{k-1}$, whenever $f(z) = v_0 + v_1 \cdot p + v_2 \cdot p^2 + \cdots + v_{k-1} \cdot p^{k-1} + \cdots$ is a canonic p-adic representation of $f(z)$; $v_i = \delta_i(f(z)) \in \{0, 1, \ldots, p-1\}$, $i = 0, 1, 2, \ldots$. In view of what has been just said, $x \equiv y \pmod{p^k}$ for $x, y \in \mathbb{Z}_p$ means that $\|x - y\|_p \le p^{-k}$. We use the same notation in the multivariate case also, i.e. for functions $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$, $(m \le n)$ that satisfy Lipschitz condition with a constant 1.

[1] throughout the paper p is a prime

Note that under this notation, the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ satisfy Lipschitz condition with a constant 1 if and only if $f(x) \equiv f(y) \pmod{p^k}$ whenever $x \equiv y \pmod{p^k}$. Thus, functions that satisfy Lipschitz conditions with a constant 1 are exactly those ones that preserve all congruences of the ring $\mathbb{Z}_p$; i.e., they map cosets into cosets: $f(a+p^k\mathbb{Z}_p) \subset f(a)+p^k\mathbb{Z}_p$ for any $a \in \mathbb{Z}_p$ and any $k = 1,2,\ldots$.

In algebra, functions which preserve all congruences of an algebraic system are called *compatible*; so throughout the paper we use for short the term 'compatible' instead of 'satisfying Lipschitz condition with a constant 1'. Note that a coset $a+p^k\mathbb{Z}_p$ of the ring $\mathbb{Z}_p$ with respect to the ideal $p^k\mathbb{Z}_p$ is a ball of radius p^{-k} in the space $\mathbb{Z}_p$. Hence, in our case compatible mappings are exactly ones that map balls into balls. This is an exercise to prove that an analytic function which is defined by a power series $\sum_{i=0}^{\infty} a_i x^i$ (with $a_i \in Z_p$ for all $i = 0,1,2,\ldots$) that converges everywhere on $\mathbb{Z}_p$, is compatible. We denote this class of analytic functions via $\mathcal{C}$. Natural examples of these functions are polynomials over $\mathbb{Z}_p$, certain p-adic logarithms (e.g., $\ln_p(1+px) = \sum_{i=1}^{\infty}(-1)^{i+1}\frac{p^i x^i}{i}$), some rational functions (e.g., $\frac{1}{1+px} = \sum_{i=0}^{\infty}(-1)^i p^i x^i$), etc.

1.1 Definition. We say that $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is *bijective modulo* p^k whenever $f \bmod p^k$ is a permutation of elements of the ring $\mathbb{Z}/p^k\mathbb{Z}$; and we say that f is *transitive modulo* p^k whenever $f \bmod p^k$ is a permutation with a single cycle.

We say that the multivariate function $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ $(m \le n)$ is *balanced modulo* p^k whenever the induced mapping $\bar{F}_k = F \bmod p^k\colon (\mathbb{Z}/p^k\mathbb{Z})^n \to (\mathbb{Z}/p^k\mathbb{Z})^m$ of the corresponding Cartesian powers of the residue ring modulo p^k satisfy the following condition: For each $v \in (\mathbb{Z}/p^k\mathbb{Z})^m$ the cardinality $\#\bar{F}_k^{-1}(v)$ of the full preimage $\bar{F}_k^{-1}(v) = \{w \in (\mathbb{Z}/p^k\mathbb{Z})^n\colon \bar{F}_k(w) = v\}$ of v does not depend on v; that is $\#\bar{F}_k^{-1}(v) = \#\bar{F}_k^{-1}(w)$ for any two $v, w \in (\mathbb{Z}/p^k\mathbb{Z})^m$.[2]

Further in the paper we say that the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ (or $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$) is measure-preserving whenever it preserves the unique Haar measure μ_p, which is normalized so that the measure of the whole space is 1. Accordingly, we say that f is ergodic whenever f is ergodic with respect to μ_p.

The paper study measure-preserving (in particular, ergodic) transformations of the space of p-adic integers; within this context the paper is a contribution to the theory of p-adic dynamical systems. The latter are of growing interest now because of their possible applications in different areas: For instance, applications of the p-adic dynamics to physics, cognitive sciences, and neural networks are discussed in [17]. Recently ergodic transformations of the space of 2-adic integers were successfully applied to pseudorandom number generation for computer simulations and especially for cryptography (stream cipher design), see [2], [10] as well as [7, 8, 6]. The following theorem was announced in [5]:

1.2 Theorem. *For $m = n = 1$, a compatible function $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is measure-preserving (or, accordingly, ergodic) if and only if it is bijective (accordingly,*

[2] We used the term *equiprobable* instead of balanced in [5]; however, the latter is more common in cryptographic literature

transitive) modulo p^k for all $k = 1,2,3,\ldots$.

For $n \geq m$, the function F is measure-preserving if and only if it is balanced modulo p^k, for all $k = 1,2,3,\ldots$.

In the paper we prove this theorem, see Sections 2, 3 and 4. It worth notice here that from further considerations it follows that a compatible measure-preserving function $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ is an isometry, see Note 2.5. Theorem 1.2 in a combination with earlier results of the author on transitivity modulo p^k (see [3], [5] and [9]) is used further to obtain the following characterization of ergodic transformations of spheres:

1.3 Theorem. *Let f be a $\mathcal{C}$-function* (e.g., a polynomial over the ring $\mathbb{Z}_p$). *In case p odd, the mapping $z \mapsto f(z)$ is an ergodic* [3] *transformation of each sufficiently small sphere with a center at $y \in \mathbb{Z}_p$ if and only if the following two conditions hold simultaneously:*

- *$f(y) = y$, and*
- *the derivative $f'(y)$ of the function f at the point $y \in \mathbb{Z}_p$ generates modulo p^2 the whole group of units $(\mathbb{Z}/p^2\mathbb{Z})^*$ of the residue ring $\mathbb{Z}/p^2\mathbb{Z}$.*[4]

In case $p = 2$ no $\mathcal{C}$-function exists such that the mapping $z \mapsto f(z)$ is ergodic on all spheres around $y \in \mathbb{Z}_2$ of radii less than ε, whatever $\varepsilon > 0$ is taken.

As a matter of fact, Theorem 1.3 remains true for a class $\mathcal{B}$ of functions that is wider than $\mathcal{C}$, and even for a class $\mathcal{A}$ that is bigger than $\mathcal{B}$. Both these classes $\mathcal{A}$ and $\mathcal{B}$ contain functions that are not necessarily analytic $\mathbb{Z}_p$, yet only locally analytic of order 1. Moreover, Theorem 1.3 is an immediate consequence of a more general Theorem 5.7 dealing with the ergodicity on a single sphere around $y \in \mathbb{Z}_p$ rather than on all sufficiently small spheres around $y \in \mathbb{Z}_p$, see Section 5 for details.

Earlier in [15] and [14] ergodicity of monomial mappings $z \mapsto z^\ell$ on spheres $S_{p^{-r}}(1)$ of a radius p^{-r} with a center at 1 was studied: It was shown that for odd p and $r > 1$ the mapping is ergodic iff ℓ is a generator of the group $(\mathbb{Z}/p^2\mathbb{Z})^*$. Mentioned Theorem 5.7 is a generalization of that result. Moreover, with the use of this theorem we are able to solve a problem that was put at the 2nd Int'l Conference on p-adic Mathematical Physics by Professor Andrei Khrennikov (see also [15], [14], and [16]):

> We know for which ℓ and p the dynamical system $f(x) = x^\ell$ is ergodic on the sphere $S_{p^{-r}}(1)$. Let us consider the ergodicity of a perturbed system $f(x) = x^\ell + q(x)$ for some polynomial $q(x) \in \mathbb{Z}_p[x]$ such that all coefficients of $q(x)$ are p-adicaly smaller than p^{-r}. This condition is necessary in order to guarantee that $S_{p^{-r}}(1)$ is invariant. For such a system to be ergodic it is necessary that ℓ is a generator of $(\mathbb{Z}/p^2\mathbb{Z})^*$. Is this sufficient?

---

[3] with respect to the induced measure

[4] In this case they also say that $f'(y)$ is *primitive modulo p^2*, or $f'(y)$ is a *generator of the multiplicative group* $(\mathbb{Z}/p^2\mathbb{Z})^*$ of the residue ring $\mathbb{Z}/p^2\mathbb{Z}$.

We prove that *the answer is affirmative* if the radius p^{-r} is sufficiently small (actually, if $r > 1$), see Proposition 5.10. Note that in view of Theorem 1.3 the mentioned perturbed mapping is ergodic on *all* spheres around 1 of radii less than p^{-r} if and only if one more condition holds: 1 is a root of the polynomial $q(x)$.

It worth notice also that with the use of Theorem 5.7 it is possible to prove the ergodicity of the 'perturbed' analogs of mappings considered in [11] and [12] on all sufficiently small spheres, namely, of mappings $z \mapsto az^\ell + q(z)$ and $z \mapsto az + b + q(z)$, where q is a 'p-adically small' perturbation. See Section 5 for details.

2. MEASURE-PRESERVING ISOMETRIES

In this section we prove that *a compatible function* $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ *preserves measure if and only if it is bijective modulo* p^k, *for all* $k = 1, 2, \ldots$. We consider a case $n = 1$ just to simplify notation; all statements of this section hold for a general case, their proofs are quite similar to ones of the case $n = 1$. It worth notice here that the main result of this section could be deduced also from a more general result of Section 3. However, we present a separate proof for the considered case since the proof gives us some extra information about the functions of considered type.

2.1 Proposition. *A compatible and measure-preserving function* $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ *is a bijection of* $\mathbb{Z}_p$ *onto itself.*

Proof. We prove that f is both injective and surjective.

Claim 1: Under conditions of Proposition 2.1 the function f is injective.

Indeed, if there exist $a, b \in \mathbb{Z}_p$ $(a \neq b)$ such that $f(a) = f(b) = z$ then for some k the balls $a + p^k\mathbb{Z}_p$ and $b + p^k\mathbb{Z}_p$ are disjoint, whereas $f(a + p^k\mathbb{Z}_p), f(a + p^k\mathbb{Z}_p) \subset z + p^k\mathbb{Z}_p$. Hence $\mu_p(f^{-1}(z + p^k\mathbb{Z}_p)) \geq 2 \cdot p^{-k}$ since $f^{-1}(z + p^k\mathbb{Z}_p)) \supset f^{-1}(a + p^k\mathbb{Z}_p)), f^{-1}(b + p^k\mathbb{Z}_p))$; so f does not preserve μ_p.

Claim 2: Under conditions of Proposition 2.1 the function f is bijective modulo p^k for all $k = 1, 2, \ldots$.

Otherwise for suitable $a, b \in \mathbb{Z}_p$ $(a \neq b)$, and k the balls $a + p^k\mathbb{Z}_p$ and $b + p^k\mathbb{Z}_p$ are disjoint, whereas $f(a + p^k\mathbb{Z}_p), f(a + p^k\mathbb{Z}_p) \subset z + p^k\mathbb{Z}_p$. Yet this leads to a contradiction, see Claim 1.

Claim 3: Under conditions of Proposition 2.1 the function f is surjective.

Take arbitrary $z \in \mathbb{Z}_p$. Then in view of Claim 2 there exists exactly one $x_1 \in \mathbb{Z}/p\mathbb{Z}$ such that $f(x_1) \equiv z \pmod p$ (here and further we identify elements of the residue ring $\mathbb{Z}/p^k\mathbb{Z}$ with non-negative rational integers $0, 1, \ldots, p^k - 1$ in an obvious way). Similarly, there exists exactly one $x_2 \in \mathbb{Z}/p^2\mathbb{Z}$ such that $f(x_2) \equiv z \pmod{p^2}$; whence necessarily $x_2 \equiv x_1 \pmod p$, etc.

So we obtain a sequence $x_2, x_2, \ldots$ such that $\|f(x_i) - z\|_p \leq p^{-i}$ and $\|x_{i+1} - x_i\|_p \leq p^{-i}$ for $i = 1, 2, \ldots$. It is an exercise to show now that the sequence $x_2, x_2, \ldots$ is a Cauchy sequence (which hence converges to some $x \in \mathbb{Z}_p$), and that $f(x) = z$. □

2.2 Note. As a bonus we have that whenever a compatible function $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is bijective modulo p^k for all $k = 1,2,\ldots$, it is a bijection of $\mathbb{Z}_p$ onto $\mathbb{Z}_p$, see proofs of Claims 2 and 3 of the proof of Proposition 2.1.

2.3 Proposition. *Let a compatible function $g\colon \mathbb{Z}_p \to \mathbb{Z}_p$ be bijective modulo p^k for all $k = 1,2,\ldots$. Then g preserves measure.*

Proof. In view of Note 2.2 the function g is a bijection of $\mathbb{Z}_p$ onto $\mathbb{Z}_p$; whence, there exist an inverse function $f = g^{-1}$, which is also a bijection of $\mathbb{Z}_p$ onto $\mathbb{Z}_p$. Moreover, f is continuous since g is continuous.

Claim 1: f is compatible.

If there are $a, b \in \mathbb{Z}_p$ such that $a \equiv b \pmod{p^k}$ and $f(a) \not\equiv f(b) \pmod{p^k}$ then assuming $a = g(u)$, $b = g(v)$ for uniquely defined $u, v \in \mathbb{Z}_p$ we have $g(u) \equiv g(v) \pmod{p^k}$ and $f(g(u)) \not\equiv f(g(v)) \pmod{p^k}$; that is, $g(u) \equiv g(v) \pmod{p^k}$ and $u \not\equiv v \pmod{p^k}$. The latter contradicts conditions of Proposition 2.3.

Claim 2: $f(a + p^k\mathbb{Z}_p) = f(a) + p^k\mathbb{Z}_p$ for every $a \in \mathbb{Z}_p$ and every $k = 1,2,\ldots$.

In view of Claim 1, $f(a + p^k\mathbb{Z}_p) \subset f(a) + p^k\mathbb{Z}_p$. To prove the inverse inclusion, denote $f(a) = b$; then $g(b) = a$. Since g is compatible, $g(b + p^k\mathbb{Z}_p) \subset g(b) + p^k\mathbb{Z}_p$. Applying a bijection f to the both sides of this inclusion, one obtains $b + p^k\mathbb{Z}_p \subset f(g(b) + p^k\mathbb{Z}_p)$, since f is compatible (see Claim 1); that is, $f(a) + p^k\mathbb{Z}_p \subset f(a + p^k\mathbb{Z}_p)$, the needed inverse inclusion.

Claim 3: f is bijective modulo p^k for all $k = 1,2,\ldots$.

Assuming there exist $u, v \in \mathbb{Z}_p$ and $k \in \{1,2,\ldots\}$ such that $u \equiv v \pmod{p^k}$ and $f(u) \not\equiv f(v) \pmod{p^k}$ one obtains that $u + p^k\mathbb{Z}_p = v + p^k\mathbb{Z}_p$, yet $f(u) + p^k\mathbb{Z}_p \neq f(v) + p^k\mathbb{Z}_p$, a contradiction in view of Claim 2.

Claim 4: f satisfies conditions of Proposition 2.3.

See Claims 1 and 3.

Claim 5: $g(a + p^k\mathbb{Z}_p) = g(a) + p^k\mathbb{Z}_p$ for every $a \in \mathbb{Z}_p$ and every $k = 1,2,\ldots$.

See Claim 4.

Claim 6: $\mu_p(g(M)) = \mu_p(M)$, for every measurable $M \subset \mathbb{Z}_p$.

Since M is measurable, then

$$\mu_p(M) = \inf\{\mu_p(V)\colon V \supset M, V \text{ is open in } \mathbb{Z}_p\}.$$

Since V is open, it is a disjoint union of a countable number of balls V_j of non-zero radius each: $V = \bigcup_{j\in J} V_j$. Then $g(V) = \bigcup_{j\in J} g(V_j)$, since g is a bijection. Note that in view of Claim 5, each $g(V_j)$ is a ball of a radius that is equal to the one

of the ball V_j; that is, $\mu_p(g(V_j)) = \mu_p(V_j)$, for all $j \in J$. Moreover, the balls are disjoint: $g(V_i)\bigcap g(V_j) = \emptyset$ whenever $i \neq j$ (since $f(g(V_i)\bigcap g(V_j)) = V_i \bigcap V_j$ in view of Claim 2). This implies that $\mu_p(g(V)) = \mu_p(V)$. Note that $g(V)$ is open since g is a continuous bijection. Hence,

$$\mu_p(g(M)) \leq \inf\{\mu_p(g(V)) \colon V \supset M, V \text{ is open in } \mathbb{Z}_p\} = \mu_p(M).$$

In view of Claim 4, one has then $\mu_p(f(R)) \leq \mu_p(R)$, for every measurable $R \subset \mathbb{Z}_p$. Now we take $R = g(M)$ (whence $f(R) = M$) and obtain $\mu_p(M) \leq \mu_p(g(M))$, thus proving the Proposition.

□

2.4 Corollary. *A compatible function $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ preserves measure if and only if it is bijective modulo p^k for all $k = 1, 2, \ldots$.*

Proof. Necessity of the conditions is proved by Claim 2 of Proposition 2.1, whereas their sufficiency is proved by Proposition 2.3. □

2.5 Note. As a bonus we have that *every compatible measure-preserving function $f \colon \mathbb{Z}_p \to \mathbb{Z}_p$ is an isometry*: A distance between two points is just a radius of the smallest ball that contains them both; however, as it was shown, a measure-preserving compatible mapping is a bijection that merely permutes balls of the same radius.

3. MEASURE-PRESERVING FUNCTIONS

In this section we prove that *a compatible function $F \colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$, $m \leq n$, preserves measure if and only if it is balanced modulo p^k, for all $k = 1, 2, \ldots$.*

3.1 Lemma. *Let a compatible function $F \colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$, $m \leq n$, be balanced modulo p^k, for all $k = 1, 2, \ldots$. Then for every $b \in \mathbb{Z}_p^m$ a full preimage $F^{-1}(b + p^s\mathbb{Z}_p^m)$ is a union of $p^{s(n-m)}$ pairwise disjoint balls $a_j + p^s\mathbb{Z}_p^n$, $j = 1, 2, \ldots, p^{s(n-m)}$.*

Proof. We start with proving the lemma 'modulo p^k'.

Claim 1. For every $\bar{b}_k \in (\mathbb{Z}/p^k)^m$, a full preimage $\bar{F}_k^{-1}(\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m)$ of the coset $\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m \subset (\mathbb{Z}/p^k\mathbb{Z})^m$ (modulo the ideal $p^k(\mathbb{Z}/p^k\mathbb{Z})^m$ of the ring $(\mathbb{Z}/p^k\mathbb{Z})^m$) is a disjoint union of $p^{s(n-m)}$ suitable pairwise disjoint cosets (modulo the ideal $p^s(\mathbb{Z}/p^k\mathbb{Z})^n$ of the ring $(\mathbb{Z}/p^k\mathbb{Z})^n$):

$$\bar{F}_k^{-1}(\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m) = \bigcup_{j=1}^{p^{s(n-m)}} (\bar{a}_{k,j} + p^s(\mathbb{Z}/p^k\mathbb{Z})^n).$$

Here and further we assume that $s \leq k$. In this case $\#(\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m) = p^{m(k-s)}$, and since F is balanced modulo p^k, then

$$\#F_k^{-1}(\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m) = p^{k(n-m)} \cdot p^{m(k-s)} = p^{kn-ms}. \tag{3.1.1}$$

Further, since F is balanced modulo p^s, then $\#F_s^{-1}(\bar{b}_s) = p^{s(n-m)}$, for every $\bar{b}_s \in \{0,1,\dots,p^s-1\}^m = (\mathbb{Z}/p^s\mathbb{Z})^m$. Take $\bar{b}_s \equiv \bar{b}_k \pmod{p^s}$ and let

$$F_s^{-1}(\bar{b}_s) = \{\bar{a}_{s,1},\dots,\bar{a}_{s,p^{s(n-m)}}\} \subset (\mathbb{Z}/p^s\mathbb{Z})^n = \{0,1,\dots,p^s-1\}^n.$$

For $j = 1,2,\dots,p^{s(n-m)}$ choose (and fix) $\bar{a}_{k,j} \in (\mathbb{Z}/p^k\mathbb{Z})^n$ so that $\bar{a}_{k,j} \equiv \bar{a}_{s,j} \pmod{p^s}$. Note that the latter congruence, in accordance with what has been agreed in Section 1, just means that $\|\bar{a}_{k,j} - \bar{a}_{s,j}\|_p \le p^{-s}$; that is $\bar{a}_{k,j}^{(i)} \equiv \bar{a}_{s,j}^{(i)} \pmod{p^s}$ for each i^{th} component $\bar{a}_{k,j}^{(i)}$ of $\bar{a}_{k,j} \in (\mathbb{Z}/p^k\mathbb{Z})^n = \{0,1,\dots,p^k-1\}^n$, $i = 1,2,\dots,n$.

Now for $j = 1,2,\dots,p^{s(n-m)}$ take $\hat{a}_{k,j} \in (\mathbb{Z}/p^k\mathbb{Z})^n$ so that $\hat{a}_{k,j} \equiv \bar{a}_{s,j} \pmod{p^s}$; that is, $\hat{a}_{k,j} \in \bar{a}_{k,j} + p^s(\mathbb{Z}/p^k\mathbb{Z})^n$, and vice versa. Since F is compatible, $\bar{F}_k(\hat{a}_{k,j}) \equiv \bar{b}_s \pmod{p^s}$; thus, $\bar{F}_k(\hat{a}_{k,j}) \in \bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m$ (recall that $\bar{b}_s \equiv \bar{b}_k \pmod{p^s}$ by our choice). So every $\hat{a}_{k,j}$ is an $\bar{F}_k$-preimage of a certain element of the coset $b_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m$, and there are exactly $p^{s(n-m)} \cdot p^{n(k-s)} = p^{nk-ms}$ these elements $\hat{a}_{k,j}$. Comparing this number with what is given by equation (3.1.1), we conclude that all these $\hat{a}_{k,j}$ constitute the full preimage $\bar{F}_k^{-1}(\bar{b}_k + p^s(\mathbb{Z}/p^k\mathbb{Z})^m)$, which is then just the union of cosets $\bar{a}_{k,j} + p^s(\mathbb{Z}/p^k\mathbb{Z})^n$ over $j \in \{1,\dots,p^{s(n-m)}\}$. These cosets are disjoint since all $\bar{a}_{k,j}$ are different modulo p^s.

Claim 2. For $j = 1,2,\dots,p^{s(n-m)}$ fix $a_j \in \mathbb{Z}_p^n$ such that $a_j \equiv \bar{a}_{s,j} \pmod{p^s}$, where $\bar{a}_{s,j}$ are defined as above for $\bar{b}_k \equiv b \pmod{p^k}$. Then

$$F^{-1}(b + p^s\mathbb{Z}_p^m) = \bigcup_{j=1}^{p^{s(n-m)}} (a_j + p^s\mathbb{Z}_p^n).$$

First note that in this setting the definition of $\bar{a}_{s,j}$ (whence, of a_j) does not depend on k, only on b and s, since for $\bar{b}_k \equiv b \pmod{p^k}$ the set $\{\bar{a}_{s,1},\dots,\bar{a}_{s,p^{s(n-m)}}\}$ is just a full $\bar{F}_s$-preimage of $(b \bmod p^s)$; here $(b \bmod p^s)$ is a unique non-negative rational integer that lays at the distance p^{-s} from the point b; an approximation of b by a non-negative rational integer with precision p^{-s} with respect to a p-adic metric. In other words, given $b \in \mathbb{Z}_p^m$, we put $\bar{b}_s \equiv b \pmod{p^s}$, where $\bar{b}_s \in \{1,2,\dots,p^s-1\}^m$, then take all solutions $\bar{a}_{s,j} \in \{1,2,\dots,p^s-1\}^n$ of the congruence $\bar{F}_s(x) \equiv \bar{b}_s \pmod{p^s}$ in indeterminate x, and after that, for each of these $p^{s(n-m)}$ solutions $\bar{a}_{s,j}$, we choose an arbitrary $a_j \in \mathbb{Z}_p^n$ so that $a_j \equiv \bar{a}_{s,j} \pmod{p^s}$.

Form the definition of $\bar{a}_j$ it follows immediately that for every $h \in (\mathbb{Z}_p)^n$, $F(a_j + p^s \cdot h) \equiv b \pmod{p^s}$ since F is compatible; whence $F^{-1}(b + p^s\mathbb{Z}_p^m) \supset \bigcup_{j=1}^{p^{s(n-m)}} (a_j + p^s\mathbb{Z}_p^n)$. Thus, we must prove the inverse inclusion only.

Given $c \in b + p^s\mathbb{Z}_p^m$, for every $k \ge s$ from Claim 1 it follows that $F^{-1}(c) \in \bar{F}_k^{-1}(c \bmod p^k) + p^k\mathbb{Z}_p^n$, where $\bar{F}_k^{-1}(c \bmod p^k)$ is a subset of a finite set $\bigcup_{j=1}^{p^{s(n-m)}} (\bar{a}_{k,j} + p^s \cdot \{0,1,\dots,p^{k-s}-1\}^n)$.

Thus, applying Claim 1 we obtain:

$$\begin{aligned}
F^{-1}(c) &\in \bigcap_{k=s}^{\infty} (\bar{F}_k^{-1}(c \bmod p^k) + p^k \mathbb{Z}_p^n) \\
&\subset \bigcap_{k=s}^{\infty} \bigcup_{j=1}^{p^{s(n-m)}} (\bar{a}_{k,j} + p^s \cdot \{0,1,\dots,p^{k-s}-1\}^n + p^k \mathbb{Z}_p^n) \\
&= \bigcup_{j=1}^{p^{s(n-m)}} \bigcap_{k=s}^{\infty} (\bar{a}_{k,j} + p^s \cdot \{0,1,\dots,p^{k-s}-1\}^n + p^k \mathbb{Z}_p^n) \\
&= \bigcup_{j=1}^{p^{s(n-m)}} \bigcap_{k=s}^{\infty} (\bar{a}_{s,j} + p^s \cdot \{0,1,\dots,p^{k-s}-1\}^n + p^k \mathbb{Z}_p^n) \\
&= \bigcup_{j=1}^{p^{s(n-m)}} (\bar{a}_{s,j} + p^s \mathbb{Z}_p^n) = \bigcup_{j=1}^{p^{s(n-m)}} (a_j + p^s \mathbb{Z}_p^n)
\end{aligned}$$

This finishes the proof of Lemma 3.1.

□

3.2 Corollary. $\mu_p(F^{-1}(b + p^s \mathbb{Z}_p^m)) = \sum_{j=1}^{p^{s(n-m)}} \mu_p(a_j + p^s \mathbb{Z}_p^n) = p^{s(n-m)} \cdot p^{-sn} = p^{-sm} = \mu_p(b + p^s \mathbb{Z}_p^m)$.

3.3 Proposition. *Under conditions of Lemma 3.1, the function F preserves measure.*

Proof. Balls of form $b + p^s \mathbb{Z}_p^m$ constitute a base of a σ-ring of all measurable sets of the space $\mathbb{Z}_p^m$. In view of Corollary 3.2, F is then a measurable mapping; that is, any preimage of a measurable set is measurable. Now let's find $\mu_p(F^{-1}(M)$ for a measurable $M \subset \mathbb{Z}_p^m$.

Any open measurable subset $A \subset \mathbb{Z}_p^m$ is a disjoint union of such balls; hence, $F^{-1}(A)$ is open measurable subset of $\mathbb{Z}_p^n$, and $\mu_p(F^{-1}(A)) = \mu_p(A)$ in view of Corollary 3.2. Further, for a measurable M one has $\mu_p(M) = \inf\{\mu_p(V) \colon V \supset M, V \text{ is open in } \mathbb{Z}_p^m\}$; thus,

$$\mu_p(F^{-1}(M)) \le \inf\{\mu_p(F^{-1}(V)) \colon V \supset M, V \text{ is open in } \mathbb{Z}_p^m\} = \mu_p(M).$$

On the other hand, $\mu_p(M) = \sup\{\mu_p(W) \colon W \subset M, W \text{ is closed in } \mathbb{Z}_p^m\}$. Since each ball $b + p^s \mathbb{Z}_p^m$ is closed in $\mathbb{Z}_p^m$, each closed subset $W \subset \mathbb{Z}_p^m$ is a countable union of such balls (and, maybe, points); hence , the union is disjoint, whence $\mu_p(F^{-1}(W))$ is a closed subset of $\mathbb{Z}_p^n$, and $\mu_p(F^{-1}(W)) = \mu_p(W)$ in view of Corollary 3.2. Thus,

$$\mu_p(F^{-1}(M)) \ge \sup\{\mu_p(F^{-1}(W)) \colon W \subset M, W \text{ is closed in } \mathbb{Z}_p^m\} = \mu_p(M).$$

Finally we get $\mu_p(F^{-1}(M)) = \mu_p(M)$, thus proving the Proposition.

□

To finish considerations of this Section, we must now prove the inverse statement.

3.4 Proposition. *Any compatible measure-preserving function $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is balanced modulo p^k, for all $k = 1, 2, \ldots$.*

Proof. Let for some k there exists $\bar{x}, \bar{y} \in (\mathbb{Z}/p^k)^m = \{0, 1, \ldots, p^k - 1\}^m$ such that $\#\bar{F}_k^{-1}(\bar{x}) \neq \#\bar{F}_k^{-1}(\bar{y})$; note that both $F_k^{-1}(\bar{x})$ and $F_k^{-1}(\bar{y})$ lie in a finite set $(\mathbb{Z}/p^k)^n = \{0, 1, \ldots, p^k - 1\}^n$. Consider two balls $\bar{x} + p^k\mathbb{Z}_p^m$ and $\bar{y} + p^k\mathbb{Z}_p^m$ in $\mathbb{Z}_p^m$. Then

$$F^{-1}(\bar{x} + p^k\mathbb{Z}_p^m) = \bigcup_{z \in \bar{F}_k^{-1}(\bar{x})} (z + p^k\mathbb{Z}_p^n),$$
$$F^{-1}(\bar{y} + p^k\mathbb{Z}_p^m) = \bigcup_{z \in \bar{F}_k^{-1}(\bar{y})} (z + p^k\mathbb{Z}_p^n).$$

Thus, $\mu_p(F^{-1}(\bar{x} + p^k\mathbb{Z}_p^m)) \neq \mu_p(F^{-1}(\bar{y} + p^k\mathbb{Z}_p^m))$; a contradiction. □

4. ERGODIC FUNCTIONS

In dynamical systems theory an ergodic mapping is, by the definition, a metric endomorphism T (i.e., a measure-preserving mapping of a measurable space X into itself) that has no non-trivial (that is, of positive measure < 1) invariant sets (we assume as usual that the measure is normalized so that the measure of X is 1). In this section we characterize ergodic functions among all compatible functions $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^n$.

4.1 Proposition. *A compatible function $F\colon \mathbb{Z}_p^n \to \mathbb{Z}_p^n$ is ergodic if and only if F is transitive modulo p^k, for all $k = 1, 2, \ldots$.*

Proof. We start with the 'if' part of the statement. By the definition, the function F is ergodic whenever $F^{-1}(A) = A$ implies either $\mu_p(A) = 1$ or $\mu_p(A) = 0$, for any measurable $A \subset \mathbb{Z}_p^n$. Let F be transitive modulo p^k for every $k = 1, 2, \ldots$, yet let F be not ergodic. That is, let there exist a measurable non-empty $A \subset \mathbb{Z}_p^n$ such that $0 < \mu_p(A) < 1$ and $F^{-1}(A) = A$ (whence $F(A) = A$, since F is a bijection, see Section 2).

We claim that then there exists a closed F-invariant subset $\overline{C} \subset A$ (that is, $F^{-1}(\overline{C}) = \overline{C}$) such that $1 > \mu_p(\overline{C}) > 0$. Moreover, this closed subset $\overline{C}$ is a union of some finite number of balls of pairwise equal radii.

Indeed, as any open subset of $\mathbb{Z}_p^n$ is a countable union of balls, and since a complement of a ball of a positive radius r is a union of a finite number of balls of this radius r each, every closed subset of $\mathbb{Z}_p^n$ is a countable union of balls, some of which are, maybe, of zero radius (i.e., points). However,

$$\mu_p(A) = \sup\{\mu_p(S)\colon S \subset A, S \text{ is closed in } \mathbb{Z}_p^n\},$$

since μ_p is a regular measure. Thus, there exists a closed subset $B \subset A$ such that $\mu_p(B) > 0$ since $\mu_p(A) > 0$. Hence, there exists a subset $C \subset B$, which is a ball of

a positive radius r; thus, $\mu_p(C) > 0$. Since in force of Section 2 the mapping F is a compatible and measure-preserving bijection, both $F^{-1}(C)$ and $F(C)$ are balls of the same radius r. Thus, the set $\overline{C} = \bigcup_{s=-\infty}^{\infty} F^s(C)$ is an F-invariant subset of A: $F^{-1}(\overline{C}) = \overline{C}$, and $\overline{C} \subset A$. As the union $\bigcup_{s=-\infty}^{\infty} F^s(C)$ is a union of balls of the same radius r, then $\overline{C}$ is a union of a finite number of balls of radius r, since there are only finitely many balls of the radius r. Obviously, $\mu_p(\overline{C}) < 1$ since $\mu_p(A) < 1$ by our assumption. Also, $\mu_p(\overline{C}) \geq \mu_p(C) > 0$.

Now, to prove the 'if' part of the proposition we may additionally suggest that A is either a ball (of radius, say, $1 > p^k > 0$), or A is not a ball, yet a union of a finite number of balls of radius $r = p^k > 0$ each. In all cases the mapping $\bar{F}_k$ is not transitive since it has a proper invariant subset, which consists of all images modulo p^k of these balls. Yet this contradicts our assumption that F is transitive modulo p^k for all $k = 1, 2, \ldots$.

Now we prove the 'only if' part of the proposition. Let F be ergodic. Then F preserves measure, so in view of Section 2 for each $k = 1, 2, \ldots$ the mapping $\bar{F}_k$ is a permutation of the elements of the ring $(\mathbb{Z}/p^k\mathbb{Z})^n$. In case for some k the permutation $\bar{F}_k$ has more than one cycle, we have that there exists a proper subset $\bar{A} \subset (\mathbb{Z}/p^k\mathbb{Z})^n = \{0, 1, \ldots, p^k - 1\}^n$ such that $\bar{F}_k(\bar{A}) = \bar{A}$. This implies that $F(\bar{A} + p^k\mathbb{Z}_p^n) = \bar{A} + \mathbb{Z}_p^n$, i.e. $F^{-1}(\bar{A} + p^k\mathbb{Z}_p^n) = \bar{A} + p^k\mathbb{Z}_p^n$, since F is a bijection, see Section 2. Yet $\mu_p(\bar{A} + p^k\mathbb{Z}_p^n) = (\#\bar{A}) \cdot p^{-kn}$, and $0 < (\#\bar{A}) \cdot p^{-kn} < 1$, since $\bar{A}$ is a proper subset in $\{0, 1, \ldots, p^k - 1\}^n$. This contradicts our assumption that F is ergodic.

□

5. THE ERGODICITY ON SPHERES

In this section we study compatible ergodic transformations of spheres centered at $y \in \mathbb{Z}_p$. Let $S_{p^{-r}}(y)$ be a sphere of radius $\frac{1}{p^r} < 1$ with a center at $y \in \mathbb{Z}_p$; that is

$$S_{p^{-r}}(y) = \left\{ z \in \mathbb{Z}_p \colon \|z - y\|_p = \frac{1}{p^r} \right\}.$$

Note that this sphere is a disjoint union of balls of radius $\frac{1}{p^{r+1}}$ each,

$$S_{p^{-r}}(y) = \bigcup_{s=1}^{p-1} (y + p^r s + p^{r+1}\mathbb{Z}_p), \tag{5.0.1}$$

since $S_{p^{-r}}(y)$ is a set-theoretic complement of the ball $y + p^{r+1}\mathbb{Z}_p$ to the ball $y + p^r\mathbb{Z}_p$. So $S_{p^{-r}}(y)$ is a closed and simultaneously an open (whence, a measurable) subset of $\mathbb{Z}_p$. We consider a measure $\hat{\mu}_p$ induced on $S_{p^{-r}}(y)$ by the Haar measure μ_p on the whole space $\mathbb{Z}_p$; we assume that $\hat{\mu}_p$ is normalized so that $\hat{\mu}_p(S_{p^{-r}}(y)) = 1$. Now, if $f \in \mathcal{L}_1$ is a compatible mapping of $\mathbb{Z}_p$ into $\mathbb{Z}_p$ such that the sphere $S_{p^{-r}}(y)$ is invariant under the action of f (that is, $f(S_{p^{-r}}(y)) \subset S_{p^{-r}}(y)$), we can consider

a restriction of f (which we denote by the same symbol f) on the sphere $S_{p^{-r}}(y)$ and study ergodicity of the restriction f with respect to the measure $\hat{\mu}_p$. We say then that f *is ergodic on the sphere* $S_{p^{-r}}(y)$ whenever $S_{p^{-r}}(y)$ is invariant under action of f, and the action is ergodic with respect to $\hat{\mu}_p$, in the above mentioned meaning.

The following easy proposition holds:

5.1 Proposition. *Whenever $S_{p^{-r}}(y)$ is invariant under action of $f \in \mathcal{L}_1$, $f(y) \equiv y \pmod{p^r}$.*

Proof. Since $S_{p^{-r}}(y)$ is invariant, and since f maps balls into balls, $f(y+p^r s+p^{r+1}\mathbb{Z}_p) \subset y+p^r\hat{s}+p^{r+1}\mathbb{Z}_p$ for a suitable $\hat{s} \in \{1,2,\dots,p-1\}$ (see (5.0.1)). However, $f(y+p^r s) \equiv f(y) \pmod{p^r}$ since $f \in \mathcal{L}_1$, and the result follows. □

From this Proposition we immediately get the following

5.2 Corollary. *Let all spheres around $y \in \mathbb{Z}_p$ of radii less than $\varepsilon > 0$ are invariant under action of $f \in \mathcal{L}_1$. Then $f(y) = y$.*

Further, as it follows from their proofs, all results of preceding sections hold not only for the whole space $\mathbb{Z}_p$, but (up to a proper re-statement) for any finite disjoint union of balls of pairwise equal radii as well[5]. This implies the following important note:

5.3 Note. A compatible mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is ergodic on the sphere $S_{p^{-r}}(y)$ if and only if it induces on the residue ring $\mathbb{Z}/p^{k+1}\mathbb{Z}$ a mapping which acts on the subset

$$S_{p^{-r}}(y) \bmod p^{k+1} = \{y+p^r s+p^{r+1}\mathbb{Z}\colon\ s = 1,2,\dots,p-1\} \subset \mathbb{Z}/p^{k+1}\mathbb{Z}$$

as a permutation with a single cycle, for all $k = r, r+1, \dots$.

It worth notice also that whenever a compatible mapping f is ergodic on the sphere $S_{p^{-r}}(y)$, f is a bijection of this sphere onto itself; moreover, it is an isometry of this sphere, see Notes 2.2 and 2.5. The same holds for balls.

From these notices we deduce the following lemma:

5.4 Lemma. *A compatible mapping $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is ergodic on the sphere $S_{p^{-r}}(y)$ if and only if the following two conditions hold simultaneously:*

1) the mapping $z \mapsto f(z) \bmod p^{r+1}$ permutes cyclically elements of the set

$$S_{p^{-r}}(y) \bmod p^{r+1} = \{y+p^r s\colon\ s = 1,2,\dots,p-1\} \subset \mathbb{Z}/p^{r+1}\mathbb{Z};$$

2) the mapping $z \mapsto f^{p-1}(z) \bmod p^{r+t+1}$ permutes cyclically elements of the set

$$B_{p^{-(r+1)}}(y+p^r s) \bmod p^{r+t+1} = \{y+p^r s+p^{r+1}S\colon\ S = 0,1,2,\dots,p^t-1\},$$

---

[5] Moreover, following the ideas of these proofs the corresponding results could be proved for arbitrary measurable subset of $\mathbb{Z}_p$ of a positive measure, instead of the whole space $\mathbb{Z}_p$.

for all $t = 1,2,\ldots$ and some (equivalently, all) $s \in \{1,2,\ldots,p-1\}$. Here f^k stands for the k^{th} iterate of f

$$f^k(a) = \underbrace{f(f\ldots(f}_{k\ times}(a))\ldots).$$

Condition 2) holds if and only if f^{p-1} is an ergodic transformation of the ball $B_{p^{-(r+1)}}(y+p^r s) = y+p^r s+p^{r+1}\mathbb{Z}_p$ of radius $\frac{1}{p^{r+1}}$ with center at the point $y+p^r s$, for some (equivalently, all) $s \in \{1,2,\ldots,p-1\}$.

Proof. As every compatible and ergodic transformation f of the sphere is bijective on this sphere, and f is an isometry on this sphere as well (see above notions), $f(a+p^k\mathbb{Z}_p) = f(a)+p^k\mathbb{Z}_p$, for all $a \in \mathbb{Z}_p$ and all $k = 1,2,\ldots$. Thus, the mapping $z \mapsto f(z) \bmod p^{k+1}$ $(k > r)$ permutes cyclically elements of the set

$$S_{p^{-r}}(y) \bmod p^{k+1} = \{y+p^r s+p^{r+1}S\colon\ s = 1,2,\ldots,p-1; S = 0,1,2,\ldots,p^{k-r}-1\}$$

if and only if conditions 1) and 2) hold simultaneously for $t = k-r$. This proves the first part of the statement of the lemma, in view of Note 5.3. The second part of the statement is just an analogue of Note 5.3 for balls instead of spheres. □

To state the central result of this section, which describes ergodic mappings of a sphere into itself in a rather wide class $\mathcal{B}$ of compatible mappings, we introduce this class first: Consider the following class $\mathcal{B}$ of mappings from $\mathbb{Z}_p$ into $\mathbb{Z}_p$

$$\mathcal{B} = \left\{ f(x) = \sum_{i=0}^{\infty} a_i \binom{x}{i} : \frac{a_i}{i!} \in \mathbb{Z}_p, \quad i = 0,1,2,\ldots \right\}, \tag{5.4.1}$$

which was studied in detail in [5]. In view of the well-known criterion for the convergence of Mahler's series (see e.g. [20]), the series of the definition of $\mathcal{B}$ is convergent everywhere on $\mathbb{Z}_p$ and defines a uniformly continuous function on $\mathbb{Z}_p$. Note that, obviously, $\mathcal{B}$ is the class of all functions that could be represented by 'descending factorial' power series with p-adic integer coefficients, that is, $f \in \mathcal{B}$ if and only if $f(x) = \sum_{i=0}^{\infty} b_i x^{\underline{i}}$, $(b_i \in \mathbb{Z}_p)$, where $x^{\underline{0}} = 1$, $x^{\underline{i}} = x(x-1)\cdots(x-i+1)$.

The class $\mathcal{B}$ is endowed with a non-Archimedean norm $\max_{z\in\mathbb{Z}_p} \|f(z)\|_p$, which defines a metric D_p on $\mathcal{B}$. The following is proved in [5]:

- $\mathcal{B} \subset \mathcal{L}_1$, i.e., all functions of $\mathcal{B}$ are compatible;
- $\mathcal{B}$ is a completion (with respect to the metric D_p) of the class $\mathcal{P}$ of all polynomials over $\mathbb{Z}_p$;
- the class $\mathcal{C}$ of all analytic on $\mathbb{Z}_p$ functions that could be represented by convergent power series with coefficients of $\mathbb{Z}_p$, is a proper subclass of $\mathcal{B}$;
- $\mathcal{B}$ is closed with respect to addition, multiplication, compositions, and derivations of functions.

We stress that, in a contrast to the class $\mathcal{C}$, which consists of analytic functions, the class $\mathcal{B}$ is closed under compositions of functions. Further we intensively use this property without special remarks.

Despite among $\mathcal{B}$-functions there exist functions that are not analytic on $\mathbb{Z}_p$ (e.g., the function $\sum_{i=0}^{\infty} i!\binom{x}{i} = \sum_{i=0}^{\infty} x^{\underline{i}}$), all $\mathcal{B}$-functions are analytic on all balls of radii less than 1; namely, the following theorem holds:

5.5 Theorem (Taylor theorem for $\mathcal{B}$-functions). *For every $f \in \mathcal{B}$, $a, h \in \mathbb{Z}_p$ and $k = 1, 2, 3, \ldots$ the following equality holds:*

$$f(a+p^k h) = f(a) + f'(a)\cdot p^k h + \frac{f''(a)}{2!}\cdot p^{2k}h^2 + \frac{f'''(a)}{3!}\cdot p^{3k}h^3 + \cdots, \qquad (5.5.1)$$

where, as usual, $f^{(j)}(a)$ stands for the j^{th} derivative of the function f at the point $a \in \mathbb{Z}_p$. Moreover, all $\frac{f^{(j)}(a)}{j!}$ are p-adic integers, $j = 0, 1, 2, \ldots$.

Proof. We prove the second claim of the theorem first:

5.6 Lemma. *Under conditions of Theorem 5.5, all $\frac{f^{(j)}(a)}{j!}$ are p-adic integers.*

Proof of Lemma 5.6. As we have demonstrated in [5], for every $f \in \mathcal{B}$ and every $x \in \mathbb{Z}_p$

$$f'(x) = \sum_{i=1}^{\infty} (-1)^{i+1} \frac{\Delta^i f(x)}{i},^{6} \qquad (5.6.1)$$

where Δ is a difference operator; $\Delta f(x) = f(x+1) - f(x)$. Thus, as $\Delta\binom{x}{i} = \binom{x}{i-1}$, from (5.4.1) we have $f'(x) = \sum_{k=0}^{\infty}\binom{x}{k}\sum_{i=1}^{\infty}(-1)^{i+1}\frac{a_{k+i}}{i}$ and further by induction,

$$f^{(n)}(x) = \sum_{k=0}^{\infty}\binom{x}{k}\sum_{i_1,i_2,\ldots,i_n\geq 1}\frac{a_{k+i_1+i_2+\cdots+i_n}}{i_1\cdot i_2\cdots i_n}(-1)^{n+i_1+i_2+\cdots+i_n}.$$

However,

$$\sum_{i_1,i_2,\ldots,i_n\geq 1}\frac{a_{k+i_1+i_2+\cdots+i_n}}{i_1\cdot i_2\cdots i_n}(-1)^{n+i_1+i_2+\cdots+i_n} = \sum_{s=n}^{\infty}\sum_{\substack{i_1,i_2,\ldots,i_n\geq 1\\ i_1+i_2+\ldots+i_n=s}}\frac{a_{k+s}}{i_1\cdot i_2\cdots i_n}(-1)^{n+s}, \qquad (5.6.2)$$

and $\frac{a_{k+s}}{i_1\cdot i_2\cdots i_n} = \frac{a_{k+s}}{s!}\frac{s!}{i_1\cdot i_2\cdots i_n} \in \mathbb{Z}_p$ since both $\frac{(i_1+i_2+\cdots+i_n)!}{i_1\cdot i_2\cdots i_n} \in \mathbb{Z}$ and $\frac{a_{k+s}}{(k+s)!} \in \mathbb{Z}_p$, see the definition of a $\mathcal{B}$-function (5.4.1) for the latter. Thus, the sum

$$\sigma_s = \sum_{\substack{i_1,i_2,\ldots,i_n\geq 1\\ i_1+i_2+\ldots+i_n=s}}\frac{a_{k+s}}{i_1\cdot i_2\cdots i_n}(-1)^{n+s}$$

---

[6] However, it is well known that whenever the left-hand side is convergent, it converges to $f'(x)$

in the right-hand side of (5.6.2) is a p-adic integer. Moreover, as $\frac{a_{k+s}}{i_1\cdot i_2\cdots i_n} = \frac{a_{k+s}}{j_1\cdot j_2\cdots j_n}$ whenever $j_1, j_2, \ldots, j_n$ is a permutation of $i_1, i_2, \ldots, i_n$, the sum σ_s is a multiple of $n!$, i.e., $\frac{\sigma_s}{n!} \in \mathbb{Z}_p$. This proves the lemma. □

The rest of the proof of the theorem follows from a general result of Y. Amice, [1]: The result implies that any $\mathcal{B}$-function is analytic of order 1; this constitutes the first claim of Theorem 5.5.

Indeed, according to [1, Ch. III, Sec. 10, Th. 3, Cor. 1(c)] the function $f(x) = \sum_{i=0}^{\infty} a_i \cdot i!\binom{x}{i}$ $(a_i \in \mathbb{Q}_p)$ is locally analytic of order n on $\mathbb{Z}_p$ (that is, $f(a+p^n h) = \sum_{i=0}^{\infty} p^{in} h^i \frac{f^{(n)}(a)}{i!}$ for $h \in \mathbb{Z}_p$) if and only if

$$\lim_{i\to\infty}\left(\frac{i}{p-1}\cdot\left(1-\frac{1}{p^n}\right)-\log_p\|a_i\|_p\right)=+\infty,$$

which obviously holds with $n=1$ for any $\mathcal{B}$-function f in force of the definition of the class $\mathcal{B}$, see (5.4.1). □

Now we state the main result of the section.

5.7 Theorem. *Let the function f lie in $\mathcal{B}$. The function f is ergodic on the sphere $S_{p^{-r}}(y)$ of sufficiently small* [7] *radius p^{-r} if and only if one of the following alternatives holds:*

1. *Whenever p is odd, then simultaneously*
   - $f(y) \equiv y \pmod{p^{r+1}}$,
   - $f'(y)$ *generates the whole group of units modulo* p^2.
2. *Whenever $p=2$, then simultaneously*
   - $f(y) \equiv y \pmod{2^{r+1}}$,
   - $f(y) \not\equiv y \pmod{2^{r+2}}$,
   - $f'(y) \equiv 1 \pmod{4}$.

Proof. As it immediately follows from Theorem 5.5, for every $g \in \mathcal{B}$ and all $k \in \mathbb{Z}_p$, $k = 1, 2, 3, \ldots$ the following equality holds

$$g(a+p^k h) = g(a) + g'(a)\cdot p^k h + p^{2k} h^2 \cdot \hat{g}(h), \tag{5.7.1}$$

for a suitable $\mathcal{C}$-function $\hat{g}$ of variable h. [8]

Since $f(y) = y + p^r z$ for a suitable $z \in \mathbb{Z}_p$ in view of Proposition 5.1, we deduce from (5.7.1) that the following equalities hold:

$$\begin{aligned} f(y+p^r s+p^{r+1}S) = f(y) + (p^r s + p^{r+1}S)\cdot f'(y) + p^{2r}\cdot(s+pS)^2\cdot\hat{w}(s+pS) = \\ y + p^r z + p^r s\cdot f'(y) + p^{r+1}S\cdot f'(y) + p^{2r}\cdot v(s) + p^{2r+1}\cdot w(S), \end{aligned} \tag{5.7.2}$$

---

[7] $p^{-r} < 1$ in case $p > 3$, and $p^{-r} < \frac{1}{p}$ in case $p \le 3$

[8] Of course, coefficients of series (5.4.1) that represents the function $p^{2k}\cdot g \in \mathcal{B}$ depend also on a and k, but this is of no importance at the moment

where v, $\hat{w}$ and w are $\mathcal{C}$-functions in the respective variables (note that we have used (5.7.1) twice; with $g=f$, $a=y$, $p^k h = p^r s + p^{r+1} S$, for the first time, and with $g=w$, $a=s$, $p^k h = p^S$), for the second time. Note that w depends also on s, yet this is of no importance in future argument.

Iterating (5.7.2) we obtain

$$f^{p-1}(y+p^r s+p^{r+1}S) = y + p^r z \sum_{i=0}^{p-2} (f'(y))^i + p^r s \cdot (f'(y))^{p-1} + p^{r+1} S \cdot (f'(y))^{p-1} + p^{2r} \cdot \breve{v}(s) + p^{2r+1} \cdot \breve{w}(S), \quad (5.7.3)$$

for suitable $\breve{v}$ and $\breve{w}$, which are $\mathcal{B}$-functions now (since they are obtained with the use of compositions of $\mathcal{C}$-functions).

Now, to satisfy condition (2) of Lemma 5.4, the ball $y + p^r s + p^{r+1}\mathbb{Z}_p$ must be invariant under action of f^{p-1}, and f^{p-1} must act ergodically on this ball. However, 5.7.3 implies that the ball is invariant if and only if

$$\sigma(z,s) = z \sum_{i=0}^{p-2} (f'(y))^i + s \cdot (f'(y))^{p-1} \equiv s \pmod{p}. \quad (5.7.4)$$

Assuming the ball is invariant, we have $\sigma(z,s) = s + p \cdot \gamma(z,s)$ for a suitable p-adic integer $\gamma(z,s)$. So, having s fixed, from 5.7.3 we see under this assumption that

$$f^{p-1}(y+p^r s+p^{r+1}S) = y + p^r s + p^{r+1} \cdot (\gamma(z,s) + S \cdot (f'(y))^{p-1} + p^{r-1} \cdot \breve{v}(s) + p^r \cdot \breve{w}(S));$$

Thus, to satisfy condition (2) of Lemma 5.4, the following $\mathcal{B}$-function

$$G_{z,s}(S) = \gamma(z,s) + S \cdot (f'(y))^{p-1} + p^{r-1} \cdot \breve{v}(s) + p^r \cdot \breve{w}(S) \quad (5.7.5)$$

in variable S must be ergodic on $\mathbb{Z}_p$.

However, $\mathcal{B}$-functions (in particular, polynomials with p-adic integer coefficients) that are ergodic on $\mathbb{Z}_p$ are completely characterized in [5].[9] We state the result as the following lemma.

5.8 Lemma. *A $\mathcal{B}$-function is ergodic on $\mathbb{Z}_p$ if and only if it is transitive modulo p^3 for $p \in \{2,3\}$, or modulo p^2, otherwise.*

Hence, if $r > 1$ in case $p > 3$, or if $r > 2$ in case $p \le 3$, we conclude that the $\mathcal{B}$-function $G_{z,s}(S)$ of (5.7.5) is ergodic on $\mathbb{Z}_p$ if and only if the polynomial

$$L_{z,s}(S) = \gamma(z,s) + p^{r-1} \cdot \breve{v}(s) + S \cdot (f'(y))^{p-1} \quad (5.8.1)$$

of degree 1 in variable S is transitive modulo p^2 for $p > 3$, or modulo p^3 for $p \le 3$.

---

[9] As for polynomials with integer coefficients, M. V. Larin was the first who gave the characterization in the beginning of 1980$^{\text{th}}$. He used different terminology and techniques and published his result in [19] only in 2002. Also the characterization for polynomials over $\mathbb{Z}_p$ with odd p could be derived from a general study of cycle structure of polynomial mappings in [13]

Necessary and sufficient conditions providing the polynomial $\alpha+\beta\cdot x\in\mathbb{Z}_p[x]$ is transitive modulo p^k for $k\geq 2$ are well known, see e.g. [18, Section 3.2.1]. We again state the result as the lemma.

5.9 Lemma. *The polynomial $\alpha+\beta\cdot x\in\mathbb{Z}_p[x]$ is transitive modulo p^k for some $k\geq 2$ (equivalently, for all $k=1,2,\ldots$)[10] if and only if the following conditions hold simultaneously:*

- $\alpha\not\equiv 0 \pmod p$;
- $\beta\equiv 1 \pmod p$ *for odd p, and* $\beta\equiv 1 \pmod 4$ *for $p=2$.*

From this lemma in view of (5.8.1) we immediately conclude that $f'(y)\not\equiv 0 \pmod p$. Now 5.7.2 immediately implies that to satisfy condition (1) of Lemma 5.4, the mapping $s\mapsto z+sf'(y) \pmod p$ must cyclically permute elements of the multiplicative group (i.e., the whole group of units) $(\mathbb{Z}/p\mathbb{Z})^*$ of the field $\mathbb{Z}/p\mathbb{Z}$. Hence, $z\equiv 0 \pmod p$ (that is, $f(y)\equiv y \pmod{p^{r+1}}$) since otherwise $s\mapsto 0 \pmod p$ for $s\equiv -\frac{z}{f'(y)} \pmod p$. From this moment we start considering the two cases $p=2$ and $p>2$ separately.

Case 1: $p>2$. In this case the mapping $s\mapsto sf'(y) \pmod p$ cyclically permutes elements of $(\mathbb{Z}/p\mathbb{Z})^*$ if and only if $f'(y)$ is a primitive element of the field $\mathbb{Z}_p$ (that is, $f'(y)$ generates the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$).

Whenever this holds, each ball $y+p^rs+p^{r+1}\mathbb{Z}_p$, $s\in\{1,2,\ldots,p-1\}$ is invariant under action of f^{p-1} in view of (5.7.4). Moreover, since $z\equiv 0 \pmod p$, in case $f'(y)$ is primitive modulo p we have that $\sigma(z,s)\equiv s\cdot(f'(y))^{p-1} \pmod{p^2}$ and whence $\gamma(z,s)\equiv bs \pmod p$, where $(f'(y))^{p-1}=1+pb$, $b\in\mathbb{Z}_p$ (see (5.7.4) and the text thereafter for the definition of $\sigma(z,s)$ and $\gamma(z,s)$).

Now, the polynomial (5.8.1) in variable S is ergodic on $\mathbb{Z}_p$ (and so condition (2) of Lemma 5.4 is satisfied) if and only if $b\not\equiv 0 \pmod p$, see Lemma 5.9. Yet this means that $f'(y)$ must be a generator of the multiplicative group $(\mathbb{Z}/p^2\mathbb{Z})^*$.

Case 2: $p=2$. In this case the sphere $S_{2^{-r}}(y)=y+2^r+2^{r+1}\mathbb{Z}_2$ is a ball, see (5.0.1). Moreover, the above condition $f'(y)\not\equiv 0 \pmod p$ means that $f'(y)\equiv 1 \pmod 2$, and so the condition that the mapping $s\mapsto sf'(y) \pmod p$ is a single cycle permutation on the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$, which just means that $z+f'(y)\equiv 1 \pmod 2$ in this case, is automatically satisfied since we have already proved that $z\equiv 0 \pmod p$, (i.e., $z=pc$ for suitable $c\in\mathbb{Z}_p$) for any p.

Further, the condition that the polynomial $L_{z,s}(S)$ in variable S is transitive modulo p^3 implies that $f'(y)\equiv 1 \pmod 4$, see (5.8.1) and Lemma 5.9. That is, $f'(y)=1+4b$ for some $b\in\mathbb{Z}_2$. Hence $\gamma(z,s)=c+2b$ (see (5.7.4) and the text thereafter), so in view of (5.8.1) and Lemma 5.9, to provide the polynomial $L_{z,s}(S)$ is transitive modulo 8, must be $c\equiv 1 \pmod 2$; that is, $f(y)=y+2^rz=y+2^{r+1}c\not\equiv y \pmod{2^{r+2}}$. This proves Theorem 5.7. □

[10] So in view of Theorem 1.2, the lemma states necessary and sufficient conditions providing a polynomial of degree 1 over $\mathbb{Z}_p$ is ergodic on $\mathbb{Z}_p$: It must be transitive modulo p for odd p, or modulo 4 for $p=2$.

The first important consequence of Theorem 5.7 is a solution of the problem of A. Khrennikov mentioned in Section 1:

5.10 Proposition. *The perturbed monomial mapping* $f\colon x \mapsto x^\ell + q(x)$, *where* $q(x) = p^{r+1}u(x)$ *for some function* $u \in \mathcal{B}$ (e.g., for a polynomial $u(x) \in \mathbb{Z}_p[x]$) *is ergodic on the sphere* $S_{p^{-r}}(1)$ (where $r > 1$) *if and only if* ℓ *is a generator of the multiplicative group* $(\mathbb{Z}/p^2\mathbb{Z})^*$.

Proof. Immediately follows from Theorem 5.7 with the only exception of the case $p = 3$ and $r = 2$. To handle this case, some extra efforts should be undertaken. Namely, for $p = 3$ in view of Theorem 5.5 one obtains

$$f^2(1+3^r s+3^{r+1}S) = f^2(1)+(3^r s+3^{r+1}S)\cdot f'(f(1))\cdot f'(1)+ \\ \frac{1}{2}(3^r s+3^{r+1}S)^2\cdot(f''(f(1))\cdot(f'(1))^2+f'(f(1))\cdot f''(1))+3^{3r+1}\cdot\hat{w}(S), \quad (5.10.1)$$

where $\hat{w}(S)$ is a $\mathcal{B}$-function in variable S. Now taking $f(x) = x^\ell + 3^{r+1}q(x)$, from (5.10.1) we obtain

$$f^2(1+3^r s+3^{r+1}S) = 1+(\ell+1)3^{r+1}u(1)+(3^r s+3^{r+1}S)\cdot\ell^2+ \\ \frac{1}{2}(3^r s+3^{r+1}S)^2\cdot\ell^2(\ell-1)(\ell+1)+3^{2r+1}v(s)+3^{2r+2}w(S), \quad (5.10.2)$$

where v and w are $\mathcal{B}$-functions in variables s and S, respectively. However, ℓ must be primitive modulo 3 (see Case 2 of the proof of Theorem 5.7); so $\ell \equiv 2 \pmod 3$. Hence, $\ell^2 = 1+3b$ for a suitable $b \in \mathbb{Z}$. Also, $\ell(\ell-1)(\ell+1)$ is a multiple of 3; combining this altogether with (5.10.2) we obtain:

$$f^2(1+3^r s+3^{r+1}S) = 1+3^r s+3^{r+1}\cdot(b+(\ell+1)\cdot u(1)+S\ell^2+ \\ 3^r\cdot\breve{v}(s)+3^{r+1}\cdot\breve{w}(S)), \quad (5.10.3)$$

for suitable $\mathcal{B}$-functions $\breve{v}$ and $\breve{w}$. Now we must check whether the $\mathcal{B}$-function

$$L(S) = b+(\ell+1)\cdot u(1)+S\ell^2+3^r\cdot\breve{v}(s)+3^{r+1}\cdot\breve{w}(S)$$

is ergodic on $\mathbb{Z}_3$; cf. (5.7.5) where the residue term is $p^r\cdot\breve{w}(S)$ rather than $3^{r+1}\cdot\breve{w}(S)$ as in the case under consideration. The reason for this is that now extra factor 3 in the fourth term of 5.10.2 arises because of the multiplier $\ell(\ell-1)(\ell+1)$.

Applying Lemmas 5.8 and 5.9 to the $\mathcal{B}$-function L in variable S we see that L is ergodic on $\mathbb{Z}_p$ if and only if $b \not\equiv 0 \pmod 3$ (since $(\ell+1)q(1) \equiv 0 \pmod 3$; we remind that $\ell \equiv 2 \pmod 3$). Thus, we finally conclude that ℓ must be primitive modulo p^2. □

There are some more consequences of Theorem 5.7. To start with, *Theorem 1.3, which is stated in Section 1, becomes now obvious in view of Theorem 5.7 and Corollary 5.2.*

Yet another immediate consequence follows:

5.11 Corollary. *Let $y \in \mathbb{Z}_p$ be a fixed point of the function $f \in \mathcal{B}$, and let p be odd. Then, f is ergodic on <u>all</u> spheres around y of sufficiently small radii if and only if f is ergodic on <u>some</u> sphere around y of a sufficiently small radius.*

Some known results on ergodicity of polynomial mappings also follow from Theorem 5.7. For instance, [11] concerns ergodicity of simple polynomial mappings $M_{a,\ell}\colon z \mapsto az^\ell$ on spheres, where $\ell > 0$ is rational integer, $a \in \mathbb{Z}_p$. From Hensel's Lemma it follows that whenever $\ell \not\equiv 1 \pmod p$ and $a \in B_{p^{-1}}(1)$, the mapping $M_{a,\ell}$ has a unique fixed point $x_0 \in B_{p^{-1}}(1)$ (see [11, Lemma 8.2]). Under these assumptions, from Theorem 5.7 it immediately follows that $M_{a,\ell}$ is ergodic on $S_{p^{-r}}(x_0)$ (for p odd) if and only if $a \cdot \ell$ is primitive modulo p^2, that is, *if and only if ℓ is primitive modulo p^2* since $a \equiv 1 \pmod p$ by the assumption; cf. [11, Theorem 8.4]. Similarly, the translation $T_{a,b}\colon z \mapsto az + b$, with $a, b \in \mathbb{Z}_p$, has a fixed point $y_0 = \frac{b}{1-a} \in \mathbb{Q}_p$ whenever $a \neq 1$. In case $y \in \mathbb{Z}_p$, Theorem 5.7 yields $T_{a,b}$ is ergodic on $S_{p^{-r}}(y)$ *if and only if a is primitive modulo p^2*, cf. [11, Theorem 7.3].[11]

In view of Theorem 5.7 it is obvious that these results remain true in a 'perturbed form', that is, for mappings $z \mapsto M_{a,\ell}(z) + p^{r+1}v(z)$ and $z \mapsto T_{a,b} + p^{r+1}v(z)$, where v is an arbitrary polynomial over $\mathbb{Z}_p$ (or even a $\mathcal{B}$-function), despite in this case x_0 (respectively, y_0) are not necessarily fixed points of the corresponding mappings.

Some important functions (for instance, some compatible integer-valued polynomials over $\mathbb{Q}_p$; i.e., those polynomials, which have not necessarily integer p-adic coefficients, that map $\mathbb{Z}_p$ into itself, and that satisfy Lipschitz condition with a constant 1 everywhere on $\mathbb{Z}_p$) do not lie in $\mathcal{B}$. However, they lie in a wider class $\mathcal{A}$, which is also introduced and studied in [5]: By the definition, the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ lies in $\mathcal{A}$ if and only if f is compatible (i.e., satisfies Lipschitz condition with a constant 1), and $p^n f \in \mathcal{B}$ for some non-negative rational integer n. It is important to note that *Theorem 5.7 remains true for $\mathcal{A}$-functions.*

Namely, since $f = \frac{1}{p^n}\bar{f}$ for a suitable $\mathcal{B}$-function $\bar{f}$ and suitable non-negative rational integer n, from Theorem 5.5 we immediately conclude that Taylor theorem for every $\mathcal{A}$-function f holds in the following form:

5.12 Theorem (Taylor theorem for $\mathcal{A}$-functions). *For every $f \in \mathcal{A}$, $a, h \in \mathbb{Z}_p$ and $k = 1, 2, 3, \ldots$ the function $f(a + p^k h)$ in variable h could be represented via convergent Taylor series*

$$f(a+p^k h) = f(a) + f'(a)\cdot p^k h + \frac{f''(a)}{2!}\cdot p^{2k}h^2 + \frac{f'''(a)}{3!}\cdot p^{3k}h^3 + \cdots . \qquad (5.12.1)$$

Note that $\frac{f^{(j)}(a)}{j!}$ are *not* necessarily p-adic integers now; however, in view of the second claim of Theorem 5.5, $\|\frac{f^{(j)}(a)}{j!}\|_p \leq p^n$ for all $j = 0, 1, 2, \ldots$. Moreover, $f'(a)$ *is a p-adic integer*: It is not difficult to prove that a derivative of a compatible function is a p-adic integer at any point the derivative exists, see e.g. [5].

---

[11] We note however that we prove not exactly the same results as in [11] since we impose conditions that are slightly different from the ones in [11].

Thus, we can re-write key equation 5.7.1 of Theorem 5.7 in the following form:

$$g(a+p^k h) = g(a) + g'(a)\cdot p^k h + p^{2k-n}\cdot h^2 \cdot \hat{g}(h), \tag{5.12.2}$$

where $\hat{g} \in \mathcal{C}$ and k is sufficiently large (to make $2k-n$ positive). Then from (5.7.2) we obtain (for a sufficiently large r) that

$$f(y+p^r s+p^{r+1}S) = f(y) + (p^r s+p^{r+1}S)\cdot f'(y) + p^{2r-n}\cdot (s+pS)^2 \cdot \hat{w}(s+pS) = \\ y + p^r z + p^r s\cdot f'(y) + p^{r+1}S\cdot f'(y) + p^{2r-n}\cdot v(s) + p^{2r+1-n}\cdot w(S), \tag{5.12.3}$$

where v, $\hat{w}$ and w are $\mathcal{C}$-functions in the respective variables. Now we assume that r is so large that $2r-n \geq r+3$ and finish the proof in the same way as in the one of Theorem 5.7. Note that now how small the sphere $S_{p^{-r}}(y)$ must be to satisfy the theorem depends not only on p (as it is in case of Theorem 5.7) but also on n, i.e., on the function f.

Now in the same manner we could re-state the rest of results of the section for $\mathcal{A}$-functions rather than for $\mathcal{B}$-functions. We omit details.

We note in conclusion that Theorems 5.5 and 5.12 imply that despite a $\mathcal{B}$-function (or, an $\mathcal{A}$-function) f may be non-analytic on $\mathbb{Z}_p$, it is analytic on every ball $a+p\mathbb{Z}_p$; that is, f is locally analytic of order 1, in terminology of [22].

6. DISCUSSION

Main results of the paper are Theorem 1.2, which characterizes measure-preserving (or ergodic) transformations of the space of p-adic integers $\mathbb{Z}_p$, and Theorem 5.7, which characterizes ergodic transformations of a p-adic sphere, and which gives a solution to the problem of A. Khrennikov mentioned in the introduction. All the transformations are assumed to be compatible, that is, satisfying Lipschitz condition with a constant 1 (the latter class is denoted via $\mathcal{L}_1$).

To demonstrate the importance of Theorem 1.2 for the p-adic ergodic theory, we use for some time the already mentioned mappings, translations $T_{a,b}\colon z \mapsto az+b$ and simple polynomial mappings $M_{a,\ell}\colon z \mapsto az^\ell$ as running examples, since these mappings have seemingly attracted certain attention in the p-adic ergodic theory: We already have refer to [11] in this connection. Also, paper [12] considers the ergodicity of the mapping $M_a\colon z \mapsto az$ on the sphere $S_{p^{-1}}(0)$ in connection with a distribution modulo p^n of Fibonacci numbers. In [21] ergodic decompositions of continuous automorphisms of the additive group $\mathbb{Z}_p$ were studied; the latter are of the form M_a for $a \in S_1(0)$.

We see the role Theorem 1.2 (together with Note 5.3, with notes that precede Note 5.3, and with Lemma 5.4) plays in study of ergodicity of mappings on spheres and balls, as follows: *These results act like a bridge connecting together results from the p-adic ergodic theory with the number-theoretic results* concerning residue rings $\mathbb{Z}/p^n\mathbb{Z}$.

For instance, Theorem 1.2 implies that the translation $T_{a,b}$ is ergodic on $\mathbb{Z}_p$ if and only if the mapping $\bar{T}_{a,b}\colon z \mapsto az+b \pmod{p^n}$ is transitive for all $n =$

$1, 2, \ldots$. However, the latter mapping is the recurrence law of the so-called 'linear congruential generator', which is very well known to computer scientists, and which is often used in software to produce pseudorandom sequences, see [18, Section 3.2.1]. In the latter case it is important that the period of the sequence is a maximum possible, i.e., p^n. We already have quoted the corresponding criterion during the proof of Theorem 5.7, see Lemma 5.9 there; here we mention only that this Lemma is a 40-year old result of Hull and Dobell, see [18, Section 3.2.1, Theorem A].

Moreover, using the same approach (and Lemma 5.4) we immediately conclude that the translation M_a is ergodic on the sphere $S_{p^{-r}}(0)$ if and only if a is a generator of the multiplicative group $\mathbb{Z}/p^n\mathbb{Z}$ for all $n = 1, 2, \ldots$. Again, it is well-known (the result goes back to Gauss, see [18, Section 3.2.1, Theorem B, Exercise 12]) that this holds if and only if a is primitive modulo p, and $a^p \not\equiv 1 \pmod{p^2}$; that is, if and only if a is a generator of the cyclic group $(\mathbb{Z}/p^2\mathbb{Z})^*$. Now cf. [12, Theorem 1] and [11, Theorem 7.2].

Another use of Theorem 1.2 is that it brings a number of examples of ergodic transformations of balls and spheres, and moreover, invokes earlier results in order to obtain complete characterizations (in various forms) of ergodic transformations of the space $\mathbb{Z}_p$. Actually, in [3, 5, 7, 9, 8] we have proved a number of results on transitivity of compatible mappings modulo p^n for all n. That is, in view of Theorem 1.2 these are statements about ergodicity of the mappings. Among them, the following results are of interest:

- **'Closed' form of ergodic functions:** For arbitrary $v \in \mathcal{L}_1$, the function $f(x) = 1 + x + p \cdot (v(x+1) - v(x))$ is ergodic on $\mathbb{Z}_p$; in case $p = 2$ the converse is true: Any ergodic function $f \in \mathcal{L}_1$ is of the form $f(x) = 1 + x + 2 \cdot (v(x+1) - v(x))$, for a suitable $v \in \mathcal{L}_1$.
- **Representation via Mahler's series:** For $p = 2$ the function $f\colon \mathbb{Z}_p \to \mathbb{Z}_p$ is compatible[12] and ergodic on $\mathbb{Z}_p$ if and only if

$$f(x) = 1 + x + \sum_{i=1}^{\infty} c_i \cdot p^{\lfloor \log_p (i+1) \rfloor + 1} \binom{x}{i},$$

  for suitable $c_i \in \mathbb{Z}_p$. For $p \neq 2$ the conditions remain sufficient, and not necessary.
- **Ergodicity of polynomials over $\mathbb{Q}_p$:** A polynomial $f(x) \in \mathbb{Q}_p[x]$ of degree d with rational (and not necessarily integer) coefficients is integer-valued (i.e., $f(\mathbb{Z}_p) \subset \mathbb{Z}_p$)) compatible, and ergodic on $\mathbb{Z}_p$ if and only if f takes values in $\mathbb{Z}_p$ at the points $0, 1, \ldots, p^{\lfloor \log_p d \rfloor + 3} - 1$, and the mapping $z \mapsto f(z) \bmod p^{\lfloor \log_p d \rfloor + 3}$ is compatible and transitive on the residue ring $\mathbb{Z}/p^{\lfloor \log_p d \rfloor + 3}\mathbb{Z}$. Thus, to check whether the polynomial $f(x) \in \mathbb{Q}_p[x]$ is, simultaneously, integer-valued, satisfies Lipschitz condition with a constant 1, and is ergodic, it is enough to evaluate it at approximately dp^3 points.

[12] this means, we recall, that f lies in $\mathcal{L}_1$

Theorem 5.7 gives a complete description of $\mathcal{B}$-functions that are ergodic on a p-adic sphere. The class $\mathcal{B}$ (which is, loosely speaking, a closure in the sense of Stone-Weierstrass theorem of the class $\mathcal{P}$ of all polynomials over $\mathbb{Z}_p$) contains the class $\mathcal{C}$ of all functions that could be represented by everywhere convergent power series over $\mathbb{Z}_p$ (thus, all $\mathcal{C}$-functions are analytic on $\mathbb{Z}_p$). However, $\mathcal{B}$ is wider than $\mathcal{C}$, a $\mathcal{B}$-function is not necessarily analytic on $\mathbb{Z}_p$.

With the use of Theorem 5.7 we immediately obtain a number of examples of various functions that are ergodic on a p-adic sphere: For instance, whenever a positive rational integer ℓ generates modulo p^2 the whole group of units of the residue ring $\mathbb{Z}/p^2\mathbb{Z}$, the functions $1+\ell\cdot(-1+x+p^2\cdot v(x))$ and $\ell\cdot(ax+a^x-2a)+1$ are ergodic on all (sufficiently small) spheres around 1, for every $a\in 1+p^2\mathbb{Z}_p$ and every $\mathcal{B}$-function v (say, for v being a polynomial over $\mathbb{Z}_p$); accordingly, the functions $\ell\cdot x+\ln_p(1+p^2x)$ and $\frac{\ell\cdot x}{1+p^2x}$ are ergodic on all (sufficiently small) spheres around 0 (here $\ln_p$ stands for the p-adic logarithm).

With respect to the problem of A. Khrennikov on ergodicity of perturbed monomial mappings on spheres, it worth notice that in virtue of Theorem 5.7 the answer for the problem is affirmative if the perturbations are 'p-adically small' $\mathcal{B}$-functions (and even $\mathcal{A}$-functions), and not only 'p-adically small' polynomials over $\mathbb{Z}_p$, as in the original statement of the problem: e.g., $x^\ell+\frac{1}{p}(x^p-x)^2$.

Also, with the use of the above mentioned criterion of ergodicity for $\mathcal{B}$-functions on $\mathbb{Z}_p$ (see Lemma 5.8) we immediately conclude that the following functions are ergodic on $\mathbb{Z}_p$: $ax+a^x$ with $a\in 1+p\mathbb{Z}_p$, $1+x+\frac{p^3}{1+px}$, $1+x+p^3\cdot(1+px)^{\frac{1}{1+px}}$, etc.

Some important functions (e.g., the above mentioned compatible and integer-valued polynomials over $\mathbb{Q}_p$) do not lie in $\mathcal{B}$. However, they lie in a wider class $\mathcal{A}$: By the definition, $f\in\mathcal{A}$ if and only if f is compatible and $p^nf\in\mathcal{B}$ for some non-negative rational integer n. Theorem 5.7, as well as the consequences it implies, remain true for $\mathcal{A}$-functions. Here are examples of $\mathcal{A}$-functions (which are *not* $\mathcal{B}$-functions) that are ergodic on all sufficiently small spheres around 0 (ℓ is the same as above): $\ell\cdot x+\ln_p(1+p^2x)+\frac{1}{p}(x^p-x)^2$ and $\frac{\ell\cdot x}{1+p^2x}+\frac{1}{p}(x^p-x)^2$.

We have demonstrated also that all $\mathcal{A}$-functions (whence, all $\mathcal{B}$-functions) are locally analytic of order 1, in terminology of [22]. Within this context it would be interesting to study whether it is possible to expand Theorem 5.7 to the class of all compatible functions that are locally analytic of order n, $n=1,2,\ldots$.

ACKNOWLEDGMENTS

I am grateful to Professor Andrei Khrennikov for (a number of!) fruitful discussions, and also for his hospitality during my stay at the University of Växjö. I am indebted to Professor Franco Vivaldy for his stimulating questions, and to Professor Igor Volovich for his interest to my area of research. Last, but not the lest, I wold like to express my admire with Professor Branko Dragovich for his really great work of organizing this excellent conference, the 2nd International Conference on p-adic Mathematical Physics.

REFERENCES

1. Y. Amice. Interpolation p-adique. *Bull. Soc. Math. France*, 92:117–180, 1964.
2. V. Anashin, A. Bogdanov, and I. Kizhvatov. ABC: A New Fast Flexible Stream Cipher, Version 2. Available from http://crypto.rsuh.ru/papers/abc-spec-v2.pdf, 2005.
3. V. S. Anashin. Uniformly distributed sequences of p-adic integers. *Mathematical Notes*, 55(2):109–133, 1994.
4. V. S. Anashin. Uniformly distributed sequences in computer algebra, or how to constuct program generators of random numbers. *J. Math. Sci.*, 89(4):1355–1390, 1998.
5. V. S. Anashin. Uniformly distributed sequences of p-adic integers, II. *Discrete Math. Appl.*, 12(6):527–590, 2002. A preprint available from http://arXiv.org/math.NT/0209407.
6. V. S. Anashin. On finite pseudorandom sequences. In *Kolmogorov and contemporary mathematics.*, pages 382–383, Moscow, June 2003. Russian Academy of Sciences, Moscow State University. Abstracts of the Int'l Conference.
7. V. S. Anashin. Pseudorandom number generation by p-adic ergodic transformations. Available from http://arxiv.org/abs/cs.CR/0401030, January 2004.
8. V. S. Anashin. Pseudorandom number generation by p-adic ergodic transformations: An addendum. Available from http://arxiv.org/abs/cs.CR/0402060, February 2004.
9. Vladimir Anashin. Uniformly distributed sequences over p-adic integers. In I. Shparlinsky A. J. van der Poorten and H. G. Zimmer, editors, *Number theoretic and algebraic methods in computer science. Proceedings of the Int'l Conference (Moscow, June–July, 1993)*, pages 1–18. World Scientific, 1995.
10. Vladimir Anashin, Andrey Bogdanov, and Ilya Kizhvatov. Increasing the ABC Stream Cipher Period. Technical report, ECRYPT, July 2005. http://www.ecrypt.eu.org/stream/papersdir/050.pdf.
11. J. Bryk and C. E. Silva. Measurable dynamics of simple p-adic polynomials. *Amer. Math. Monthly*, 112(3):212–232, 2005.
12. Z. Coelho and W. Parry. Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers. In *Topology, Ergodic Theory, Real Algebraic Geometry*, number 2 in Amer. Math. Soc. Transl. Ser. 2, pages 51–70. American Mathematical Society, Providence, 2001.
13. D. L. Desjardins and M. E. Zieve. On the structure of polynomial mappings modulo an odd prime power. Available at http://arXiv.org/math.NT/0103046, 2001.
14. M. Gundlach, A. Khrennikov, and K.-O. Lindahl. Ergodicity on p-adic sphere. In *German Open Conference on Probability and Statistics*, page 61, University of Hamburg, March 21–24 2000.
15. A. Khrennikov and K.-O. Lindahl. On ergodic behavior of p-adic dynamical systems. *Infinite Dimensional Analysis, Quantum Probability and Related Topics*, 4(4):569–577, 2001.
16. A. Yu. Khrennikov, K.-O. Lindahl, and M. Gundlach. Ergodicity in the p-adic framework. In S. Albeverio, N. Elander, W. N. Everitt, and P. Kurasov, editors, *Operator Methods in Ordinary and Partial Differential Equations (S.Kovalevski Symproium, Univ. of Stockholm, June 2000)*, volume 132 of *Operator Methods: Advances and Applications*. Birkhäuser, Basel-Boston-Berlin, 2002.
17. A. Yu. Khrennikov and M. Nilsson. *p-adic deterministic and random dynamics*. Kluver Academic Publ., Dordrecht etc., 2004.
18. D. Knuth. *The Art of Computer Programming*, volume 2/Seminumerical Algorithms. Addison-Wesley, Third edition, 1998.
19. M. V. Larin. Transitive polynomial transformations of residue class rings. *Discrete Mathematics and Applications*, 12(2):141–154, 2002.
20. K. Mahler. *p-adic numbers and their functions*. Cambridge Univ. Press, 1981. (2nd edition).
21. R. Oselies and H. Zieschang. Ergodische Eigenschaften der Automorphismen p-adischer Zahlen. *Arch. Math.*, 26:144–153, 1975.
22. W. H. Schikhof. *Ultrametric calculus*. Cambridge University Press, 1984.