PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
http://dx.doi.org/10.1090/proc12777
Article electronically published on July 29, 2015

DYNAMICS OF THE SQUARE MAPPING ON THE RING OF p-ADIC INTEGERS

SHILEI FAN AND LINGMIN LIAO

(Communicated by Yingfei Yi)

Abstract. For each prime number p, the dynamical behavior of the square mapping on the ring $\mathbb{Z}_p$ of p-adic integers is studied. For $p = 2$, there are only attracting fixed points with their attracting basins. For $p \geq 3$, there are a fixed point 0 with its attracting basin, finitely many periodic points around which there are countably many minimal components and some balls of radius $1/p$ being attracting basins. All these minimal components are precisely exhibited for different primes p.

1. Introduction

The dynamics of the quadratic maps on finite fields or rings attracts much attention in the literature ([6, 14, 18, 20, 21]). In particular, Rogers [18] studied the square mapping $f : x \mapsto x^2$ on the prime field $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, with p being a prime number.

Notice that for the square mapping, the point 0 is fixed and one needs only to consider the points in the multiplicative group $\mathbb{F}_p^* := \mathbb{F}_p \setminus \{0\}$. Denote by φ the *Euler's phi function*. For an integer $d \geq 2$, the *order of* 2 *modulo* d, which will be denoted by $ord_d 2$, is the smallest positive integer i such that $2^i \equiv 1 (\text{mod } d)$. By convention, $ord_1 2$ is set to be 1. Define a directed graph $G(\mathbb{F}_p^*)$ whose vertices are the elements of $\mathbb{F}_p^*$ and whose edges are directed from x to $f(x)$ for each $x \in \mathbb{F}_p^*$. Let $\sigma(\ell, k)$ be the graph consisting of a cycle of length ℓ with a copy of the binary tree T_k of height k attached to each vertex. The dynamical structure of the square mapping on $\mathbb{F}_p^*$ is described by the following theorem of Rogers [18].

Theorem 1 ([18]). *Let p be an odd prime. Put $p = 2^k m + 1$ where m is odd. Then*

$$G(\mathbb{F}_p^*) = \bigcup_{d|m} \underbrace{(\sigma(ord_d 2, k) \cup \ldots \cup \sigma(ord_d 2, k))}_{\varphi(d)/ord_d 2}.$$

The graphs of $G(\mathbb{F}_p^*)$ for $p = 11$ and 17 are depicted in Figures 1 and 2.

In this paper, we will investigate the square mapping $f : x \mapsto x^2$ on all finite rings $\mathbb{Z}/p^n\mathbb{Z}$ and on their inverse limits $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$. The space $\mathbb{Z}_p$ is nothing

Received by the editors August 23, 2014 and, in revised form, March 7, 2015.

2010 *Mathematics Subject Classification.* Primary 37P05; Secondary 11S82, 37B05.

Key words and phrases. p-adic dynamical system, minimal decomposition, square mapping.

The first author was partially supported by self-determined research funds of CCNU (Grant No. CCNU14Z01002) and NSF of China (Grant No. 11231009). The second author was partially supported by 12R03191A - MUTADIS (France) and the project PHC Orchid of MAE and MESR of France.

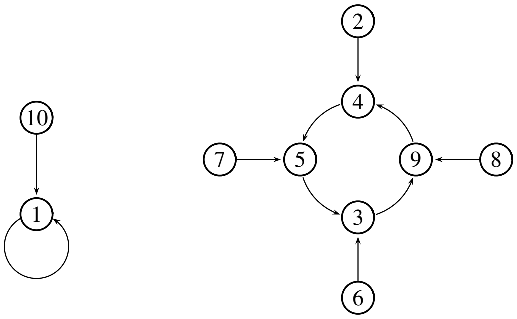

FIGURE 1. The graphs $G(\mathbb{F}_p^*)$ for primes $p = 11$ (thus $k = 1$, $m = 5$, and $d = 1$ and 5). The vertices are the elements of $\mathbb{F}_p^*$ with edges directed from x to x^2.

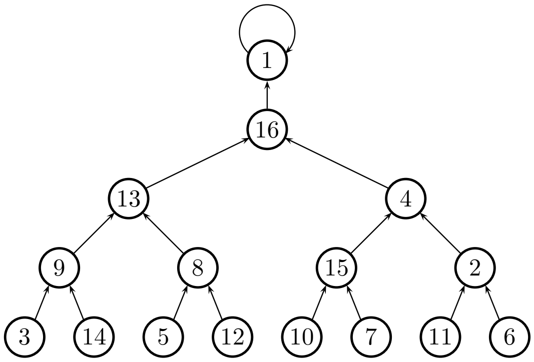

FIGURE 2. The graphs $G(\mathbb{F}_p^*)$ for primes $p = 17$ ($k = 4, m = 1$). The vertices are the elements of $\mathbb{F}_p^*$ with edges directed from x to x^2.

but the ring of p-adic integers. We are thus led to the study of the p-adic dynamical system $(\mathbb{Z}_p, f)$.

Let (X, T) be a dynamical system with X being a compact metric space and T being a continuous map from X to itself. For a point $x \in X$, the *orbit of x under T* is defined by

$$\mathcal{O}_T(x) := \{T^n(x) : n \geq 0\}.$$

If $E \subset X$ is a T-invariant (i.e., $T(E) \subset E$) compact subset, then (E, T) is a subsystem of (X, T). The subsystem (E, T) is called *minimal* if E is equal to the closure $\overline{\mathcal{O}_T(x)}$ for each $x \in E$. We refer to the book of Walters [22] for dynamical terminology.

For a prime number p, denote by $\mathbb{Q}_p$ the field of p-adic numbers. Then the ring $\mathbb{Z}_p$ of p-adic integers is the local ring of $\mathbb{Q}_p$. The absolute value on $\mathbb{Q}_p$ is denoted by $|\cdot|_p$. With this non-Archimedean absolute value, $\mathbb{Z}_p$ is the unit ball of $\mathbb{Q}_p$ which is both compact and open. For more details on p-adic numbers, one could consult Robert's book [17].

Let $f \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$. Then f defines a dynamical system on $\mathbb{Z}_p$, denoted by $(\mathbb{Z}_p, f)$. In the literature the minimality of f on the whole space $\mathbb{Z}_p$ is widely studied ([1–4, 9, 15, 23]). However, if the system is not minimal on $\mathbb{Z}_p$, what does the dynamical structure of f look like? To answer this question, one is led to do a minimal decomposition of the space $\mathbb{Z}_p$, i.e., to find all the minimal subsystems (minimal components) of f.

In general, it is proved by Fan and Liao [11] that a polynomial dynamical system $(\mathbb{Z}_p, f \in \mathbb{Z}_p[x])$ admits at most countably many minimal subsystems and the polynomial system has a *minimal decomposition*.

Theorem 2 ([11])**.** *Let $f \in \mathbb{Z}_p[x]$ with degree at least 2. We have the decomposition*

$$\mathbb{Z}_p = \mathcal{P} \sqcup \mathcal{M} \sqcup \mathcal{B},$$

where $\mathcal{P}$ is the finite set consisting of all periodic points of f, $\mathcal{M} = \bigsqcup_i \mathcal{M}_i$ is the union of all (at most countably many) clopen invariant sets such that each $\mathcal{M}_i$ is a finite union of balls and each subsystem $f : \mathcal{M}_i \to \mathcal{M}_i$ is minimal, and each point of $\mathcal{B}$ lies in the attracting basin of $\mathcal{P} \sqcup \mathcal{M}$.

The minimal decomposition in Theorem 2 was first discovered by Coelho and Parry [7] for the multiplications, and by Fan, Li, Yao, and Zhou [10] for the affine polynomials. For the polynomials with higher order, the minimal decomposition seems hard to obtain. In [11], Fan and Liao succeeded in making the minimal decomposition for all quadratic polynomials but only for the prime $p = 2$. Recently, Fan, Fan, Liao, and Wang [12] also studied the minimal decomposition of the homographic maps on the projective line over the field $\mathbb{Q}_p$ of p-adic numbers.

Furthermore, in [11], the authors also described the dynamics of each minimal subsystem. Let $(p_s)_{s\geq 1}$ be a sequence of positive integers such that $p_s | p_{s+1}$ for every $s \geq 1$. We denote by $\mathbb{Z}_{(p_s)}$ the inverse limit of $\mathbb{Z}/p_s\mathbb{Z}$, which is called an *odometer*. The sequence $(p_s)_{s\geq 1}$ is called the *structure sequence* of $\mathbb{Z}_{(p_s)}$. The map $x \to x + 1$ defined on $\mathbb{Z}_{(p_s)}$ will be called the *adding machine* on $\mathbb{Z}_{(p_s)}$.

Theorem 3 ([11])**.** *Let $f \in \mathbb{Z}_p[x]$ with degree at least 2. If E is a minimal clopen invariant set of f, then $f : E \to E$ is conjugate to the adding machine on an odometer $\mathbb{Z}_{(p_s)}$, where*

$$(p_s) = (k, kd, kdp, kdp^2, \cdots),$$

with integers k and d such that $1 \leq k \leq p$ and $d|(p - 1)$.

In this paper, we fully study the square mapping $f : x \mapsto x^2$ on $\mathbb{Z}_p$. For any prime $p \geq 2$, the complete minimal decomposition for the system $(\mathbb{Z}_p, x^2)$ is obtained. The structure sequences of the minimal subsystems are given.

By Anashin [1, 2], the dynamical structure of a polynomial on $\mathbb{Z}_p$ is derived from the structures of the induced systems on $\mathbb{Z}/p^n\mathbb{Z}$. In desJardins and Zieve [8] and Fan and Liao [11], a method to study the structures on $\mathbb{Z}/p^n\mathbb{Z}$ inductively is developed. This method then allows us to do minimal decompositions for polynomials by knowing their dynamical structures at first levels. In particular, one needs to know, at least, the dynamical structure of the induced dynamics on $\mathbb{Z}/p\mathbb{Z}$ (i.e., at level 1).

For the case of the square mapping $f : x \mapsto x^2$, however, the dynamical structure at level 1 has already been described by Rogers [18] (Theorem 1 at the beginning of this section). Hence, doing the minimal decomposition of the square mapping f on $\mathbb{Z}_p$ will be possible.

For $a \in \mathbb{Z}_p$ and $r > 0$, denote $D_r(a) := \{x \in \mathbb{Z}_p : |x-a|_p < r\}$, $\overline{D}_r(a) := \{x \in \mathbb{Z}_p : |x-a|_p \le r\}$, and $S_r(a) := \{x \in \mathbb{Z}_p : |x-a|_p = r\}$. Without difficulty, we can check that by iterations of f, the points in $D_1(0)$ are attracted to the fixed point 0, which means that $D_1(0) \setminus \{0\} \subset \mathcal{B}$. It is also easy to see that for the case $p = 2$, all points in $D_1(1)$ are attracted to the fixed point 1. So we have $\mathcal{P} = \{0,1\}, \mathcal{M} = \emptyset$, and $\mathcal{B} = \mathbb{Z}_p \setminus \{0,1\}$

For $p \ge 3$, we have seen that $0 \in \mathcal{P}$ is a fixed point with $D_1(0)\setminus\{0\} = p\mathbb{Z}_p\setminus\{0\} \subset \mathcal{B}$ as its attracting basin. By Theorem 1, at level 1, $\mathbb{F}_p^*$ is a union of cycles with some binary trees of the same height attached to each vertex of the cycles. Each point in $\mathbb{F}_p^*$ is a ball of radius $1/p$. Let $\mathcal{C} \subset \mathbb{Z}_p \setminus p\mathbb{Z}_p$ be the union of balls corresponding to the points in the cycles and $\mathcal{T} = (\mathbb{Z}_p \setminus p\mathbb{Z}_p) \setminus \mathcal{C}$ be the union of balls corresponding to the points in the trees. Then $\mathcal{T}$ is attracted to $\mathcal{C}$, which means that $\mathcal{T} \subset \mathcal{B}$. Hence, we will only treat the system f restricted on $\mathcal{C}$.

For two integers m and n, we denote by (m,n) their greatest common divisor. The following minimal decomposition theorem of the square mapping f on $\mathcal{C}$ is our main result. It gives a whole picture of the dynamical structure of the square mapping on $\mathbb{Z}_p$.

Theorem 4. *Let p be an odd prime with $p = 2^k m + 1$ where m is an odd integer. Then $\mathcal{C}$ can be decomposed as the union of m periodic points and countably many minimal components around each periodic orbit.*

Let P_m be the set of periodic points, i.e.,

$$P_m = \{x \in \mathcal{C} : f^n(x) = x \ \ \text{for some integer } n \ge 1\}.$$

Then $P_m \subset \mathcal{P}$ and we can decompose P_m in the following way:

$$P_m = \bigsqcup_{d|m} \underbrace{\hat{\sigma}(ord_d 2) \sqcup \cdots \sqcup \hat{\sigma}(ord_d 2)}_{\varphi(d)/ord_d 2},$$

where $\hat{\sigma}(\ell)$ is a periodic orbit of period ℓ.

Let $\hat{\sigma}(\ell) = (\hat{x}_1, \cdots, \hat{x}_\ell)$ be one of the periodic orbits of period ℓ. Around this periodic orbit, we have the decomposition

$$\bigsqcup_{1\le i\le \ell} D_1(\hat{x}_i) = \{\hat{x}_1, \cdots, \hat{x}_\ell\} \sqcup \left(\bigsqcup_{n\ge 1} \bigsqcup_{1\le i\le\ell} S_{p^{-n}}(\hat{x}_i) \right).$$

For each $n \ge 1$, the set $\bigsqcup_{1\le i\le\ell} S_{p^{-n}}(\hat{x}_i)$ belongs to the minimal part $\mathcal{M}$ and contains $\frac{(p-1)\cdot(ord_p 2,\ell)}{ord_p 2} \cdot p^{v_p(2^{p-1}-1)-1}$ minimal components, and each minimal component is a union of $j := \frac{\ell\cdot ord_p 2}{(ord_p 2,\ell)}$ closed disks of radius $p^{-n-v_p(2^{p-1}-1)}$.

For each minimal component $\mathcal{M}_i$ lying in $\bigsqcup_{1\le i\le\ell} D_1(\hat{x}_i)$, the subsystem $f : \mathcal{M}_i \to \mathcal{M}_i$ is conjugate to the adding machine on the odometer $\mathbb{Z}_{(p_s)}$, where

$$(p_s) = (\ell, \ell j, \ell j p, \ell j p^2, \cdots).$$

One of the key points in our proof of Theorem 4 is to determine the periodic orbits. In Khrennikov and Nilsson [16], some results on the number and length of periodic orbits of monomial dynamical systems $f(x) = x^n, n \ge 3$, were obtained. It seems that applying our techniques to the results of [16] might lead to precise minimal decompositions for other monomials. However, there is still a lot of work to do.

Our paper is organized as follows. In Section 2, we study the induced dynamics on $\mathbb{Z}/p^n\mathbb{Z}$. Section 3 gives some facts in number theory. The minimal decomposition is completed in Section 4. Finally in Section 5, some examples for special primes like Fermat primes and Wieferich primes are discussed.

2. Induced dynamics on $\mathbb{Z}/p^n\mathbb{Z}$

Let $p \geq 3$ be a prime and let $f \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$. The dynamics of f on $\mathbb{Z}_p$ is determined by those of its induced finite dynamics on $\mathbb{Z}/p^n\mathbb{Z}$ ([1, 2]). The idea to study these finite dynamics inductively comes from desJardins and Zieve [8]. It allows Fan and Liao [11] to give the decomposition theorem (Theorem 2) for any polynomial in $\mathbb{Z}_p[x]$. In this section, we will give some basic definitions and facts which are useful in proving our main theorem. For details, see [11] or [13].

Let $n \geq 1$ be a positive integer. Denote by f_n the induced mapping of f on $\mathbb{Z}/p^n\mathbb{Z}$, i.e.,

$$f_n(x(\text{mod } p^n)) = f(x) \ (\text{mod } p^n).$$

The dynamical behaviors of f are linked to those of f_n.

Lemma 1 ([3, 5]). *Let $f \in \mathbb{Z}_p[x]$ and let $E \subset \mathbb{Z}_p$ be a compact f-invariant set. Then $f : E \to E$ is minimal if and only if $f_n : E/p^n\mathbb{Z}_p \to E/p^n\mathbb{Z}_p$ is minimal for each $n \geq 1$.*

By Lemma 1, to study the minimality of f, we need to study the minimality of each f_n. Moreover, it is important to investigate the conditions under which the minimality of f_n implies that of f_{n+1}.

Assume that $\sigma = (x_1, \cdots, x_k) \subset \mathbb{Z}/p^n\mathbb{Z}$ is a *cycle* of f_n of length k (also called a *k-cycle*) at level n, i.e.,

$$f_n(x_1) = x_2, \cdots, f_n(x_i) = x_{i+1}, \cdots, f_n(x_k) = x_1.$$

Let

$$X_\sigma := \bigsqcup_{i=1}^{k} X_i \quad \text{where} \quad X_i := \{x_i + p^n t + p^{n+1}\mathbb{Z};\ t = 0, \cdots, p-1\} \subset \mathbb{Z}/p^{n+1}\mathbb{Z}.$$

Then

$$f_{n+1}(X_i) \subset X_{i+1} \ (1 \leq i \leq k-1) \quad \text{and} \quad f_{n+1}(X_k) \subset X_1.$$

Let $g := f^k$ be the k-th iterate of f; then we have $g_{n+1}(X_i) \subset X_i$ for all $1 \leq i \leq k$. In the following, we shall study the behavior of the finite dynamics f_{n+1} on the f_{n+1}-invariant set X_σ and determine all cycles of f_{n+1} in X_σ, which will be called *lifts* of σ (from level n to level $n+1$). Remark that the length of any lift of σ is a multiple of k.

Let

$$\mathbb{X}_i := x_i + p^n\mathbb{Z}_p = \{x \in \mathbb{Z}_p : x \equiv x_i \ (\text{mod } p^n)\}$$

be the closed disk of radius p^{-n} corresponding to $x_i \in \sigma$ and let

$$\mathbb{X}_\sigma := \bigsqcup_{i=1}^{k} \mathbb{X}_i$$

be the clopen set corresponding to the cycle σ.

For $x \in \mathbb{X}_\sigma$, denote

$$a_n(x) := g'(x) = \prod_{j=0}^{k-1} f'(f^j(x)), \tag{1}$$

$$b_n(x) := \frac{g(x) - x}{p^n} = \frac{f^k(x) - x}{p^n}. \tag{2}$$

The 1-order Taylor Expansion of g at x,

$$g(x + p^n t) \equiv g(x) + g'(x)\pi^n t \pmod{p^{2n}}, \quad \text{for } t \in \{0, \dots, p-1\},$$

implies

$$g(x + p^n t) \equiv x + p^n b_n(x) + p^n a_n(x) t \pmod{p^{2n}}, \quad \text{for } t \in \{0, \dots, p-1\}. \tag{3}$$

Define an affine map

$$\Phi(x,t) = b_n(x) + a_n(x)t \qquad (x \in \mathbb{X}_\sigma, t \in \{0, \dots, p-1\}).$$

We usually consider the function $\Phi(x, \cdot)$ as an induced function from $\mathbb{Z}/p\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$ by taking mod p and we keep the notation $\Phi(x, \cdot)$ if there is no confusion. An important consequence of the formula (3) shows that $g_{n+1} : X_i \to X_i$ is conjugate to the linear map

$$\Phi(x, \cdot) : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z},$$

for $x \in \mathbb{X}_i$. It is called the *linearization* of $g_{n+1} : X_i \to X_i$.

As proved in Lemma 1 of [11], the coefficient $a_n(x) \pmod p$ is always constant on $\mathbb{X}_i$ and the coefficient $b_n(x) \pmod p$ is also constant on $\mathbb{X}_i$ but under the condition $a_n(x) \equiv 1 \pmod p$. For simplicity, sometimes we write a_n and b_n without mentioning x.

From the values of a_n and b_n, one can predict the behaviors of f_{n+1} on X_σ. The linearity of the map $\Phi = \Phi(x, \cdot)$ is the key to what follows:

(a) If $a_n \equiv 1 \pmod p$ and $b_n \not\equiv 0 \pmod p$, then Φ preserves a single cycle of length p, so that f_{n+1} restricted to X_σ preserves a single cycle of length pk. In this case we say σ *grows.*

(b) If $a_n \equiv 1 \pmod p$ and $b_n \equiv 0 \pmod p$, then Φ is the identity, so f_{n+1} restricted to X_σ preserves p cycles of length k. In this case we say σ *splits.*

(c) If $a_n \equiv 0 \pmod p$, then Φ is constant, so f_{n+1} restricted to X_σ preserves one cycle of length k and the remaining points of X_σ are mapped into this cycle. In this case we say σ *grows tails.*

(d) If $a_n \not\equiv 0, 1 \pmod p$, then Φ is a permutation and the ℓ-th iterate of Φ reads

$$\Phi^\ell(t) = b_n(a_n^\ell - 1)/(a_n - 1) + a_n^\ell t,$$

so that

$$\Phi^\ell(t) - t = (a_n^\ell - 1)\left(t + \frac{b_n}{a_n - 1}\right).$$

Thus, Φ admits a single fixed point $t = -b_n/(a_n - 1)$, and the remaining points lie on cycles of length d, where d is the order of a_n in $(\mathbb{Z}/p\mathbb{Z})^*$. So, f_{n+1} restricted to X_σ preserves one cycle of length k and $\frac{p-1}{d}$ cycles of length kd. In this case we say σ *partially splits.*

We want to see the change of nature from a cycle to its lifts, so it is important to study the relation between (a_n, b_n) and (a_{n+1}, b_{n+1}). The following lemmas are useful for our study of the dynamics of the square mapping on $\mathbb{Z}_p$. For details see [8, 11].

Lemma 2 ([8], see also [11], Proposition 2)**.** *Let $p \geq 3$ be a prime and let $n \geq 2$ be an integer. If σ is a growing cycle of f_n and $\tilde{\sigma}$ is the unique lift of σ, then $\tilde{\sigma}$ grows.*

Lemma 3 ([11])**.** *Let $p \geq 3$ be a prime and let $n \geq 2$ be an integer. If σ is a growing cycle of f_n, then σ produces a minimal component, i.e., the set $\mathbb{X}_\sigma$ is a minimal subsystem of f.*

Proof. By Lemma 2, if $\tilde{\sigma}$ is the lift of σ, then $\tilde{\sigma}$ also grows. Applying Lemma 2 again, the lift of $\tilde{\sigma}$ grows. Consecutively, we find that the descendants of σ will keep on growing. (In this case, we usually say σ *always grows* or *grows forever.*) Hence, f_m is minimal on $\mathbb{X}_\sigma/p^m\mathbb{Z}_p$ for each $m \geq n$. Therefore, by Lemma 1, $(\mathbb{X}_\sigma, f)$ is minimal. □

3. Preliminary facts in number theory

In this section we give some preliminary facts in number theory.

The field $\mathbb{Q}_p$ of p-adic numbers always contains a cyclic subgroup of order $p-1$, defined as

$$\mu_{p-1} := \{x \in \mathbb{Q}_p : x^{p-1} = 1\} \subset \mathbb{Z}_p^\times.$$

Here, $\mathbb{Z}_p^\times$ stands for the set of all invertible elements in $\mathbb{Z}_p$.

As a cyclic group, μ_{p-1} is isomorphic to the multiplicative group $\mathbb{F}_p^*$.

Lemma 4. *When p is an odd prime, the group of roots of unity in the field $\mathbb{Q}_p$ is μ_{p-1}.*

Proof. See Proposition 1 of Section 6.7 of [17]. □

Lemma 5. *Let p be an odd prime and let μ_{p-1} be the group of roots of unity in the field $\mathbb{Q}_p$. Let*

$$\varepsilon : \mu_{p-1} \to \mathbb{F}_p^*$$

be the reduction homomorphism. Then the following graph commutes:

$$\begin{tikzcd}
\mu_{p-1} \arrow[r, "x^2"] \arrow[d, "\varepsilon"'] & \mu_{p-1} \arrow[d, "\varepsilon"] \\
\mathbb{F}_p^* \arrow[r, "x^2"'] & \mathbb{F}_p^*
\end{tikzcd}$$

Proof. Notice that μ_{p-1} and $\mathbb{F}_p^*$ are cyclic multiplicative groups, and

$$\varepsilon : \mu_{p-1} \to \mathbb{F}_p^*$$

is a group automorphism. Furthermore, the square mapping on μ_{p-1} and the square mapping on $\mathbb{F}_p^*$ are group homomorphisms. Hence the graph commutates. □

For a periodic orbit $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{Z}_p^\times$ and a cycle $\sigma_n = (x_1, x_2, \cdots, x_\ell) \subset (\mathbb{Z}/p^n\mathbb{Z})^*$ at level n, of the same length ℓ, we write $\sigma_n \equiv \hat{\sigma} \pmod{p^n}$ if

$$x_i \equiv \hat{x}_i \pmod{p^n} \quad \forall 1 \leq i \leq \ell.$$

The following proposition is directly derived from Lemma 5.

Proposition 1. *Let p be an odd prime and let $f : x \mapsto x^2$ be the square mapping. If $\sigma_1 = (x_1, x_2, \cdots, x_\ell) \subset (\mathbb{Z}/p\mathbb{Z})^*$ is a cycle of the induced mapping f_1 of length ℓ, then there exists a unique periodic orbit $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{Z}_p^\times$ such that $\sigma_1 \equiv \hat{\sigma} \pmod p$*

Conversely, for a periodic orbit of f in $\mathbb{Z}_p$, there exists a corresponding periodic orbit of f_1 in $\mathbb{Z}/p\mathbb{Z}$. Furthermore, for each integer $n \geq 1$, there exists a corresponding periodic orbit of f_n in $\mathbb{Z}/p^n\mathbb{Z}$. By Lemma 5, the proof of the following proposition is evident.

Proposition 2. *Let p be an odd prime and let $f : x \mapsto x^2$ be the square mapping. Let $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{Z}_p^\times$ be a periodic orbit of f of length ℓ. Then $\ell \leq p-1$ and for each $n \geq 1$, there exists a unique cycle $\sigma_n \subset \mathbb{Z}/p^n\mathbb{Z}$ of f_n of length ℓ such that $\sigma_n \equiv \hat{\sigma} \pmod{p^n}$.*

The following lemma is a basic fact in number theory.

Lemma 6. *Let p be an odd prime and let $\ell \geq 1$ be an integer. Then the order of 2^ℓ in $(\mathbb{Z}/p\mathbb{Z})^*$ is $\frac{ord_p 2}{(\ell, ord_p 2)}$. In particular, if $2^\ell \equiv 1 \pmod p$, we have $ord_p 2 \mid \ell$.*

Proof. Notice that

$$2^{\ell \cdot \frac{ord_p 2}{(\ell, ord_p 2)}} = 2^{ord_p 2 \cdot \frac{\ell}{(\ell, ord_p 2)}} \equiv 1 \pmod p.$$

Thus the order of 2^ℓ is no more than $\frac{ord_p 2}{(\ell, ord_p 2)}$.

Write $\ell = k \cdot ord_p 2 + s$ with $k \geq 0$ and $0 \leq s < ord_p 2$.

If $2^\ell \equiv 1 \pmod p$, then

$$1 \equiv 2^\ell = 2^{k \cdot ord_p 2 + s} \equiv 2^s \pmod p.$$

So by the definition of $ord_p 2$, we have $s = 0$. Hence

$$ord_p 2 \mid \ell \quad \text{and} \quad \frac{ord_p 2}{(\ell, ord_p 2)} = 1.$$

Since $ord_p(2^\ell) \leq \frac{ord_p 2}{(\ell, ord_p 2)}$, we conclude that

$$ord_p(2^\ell) = 1 = \frac{ord_p 2}{(\ell, ord_p 2)}.$$

If $2^\ell \not\equiv 1 \pmod p$, then $s \neq 0$ and $(\ell, ord_p 2) = (s, ord_p 2)$. Hence for any positive integer $i < \frac{ord_p 2}{(\ell, ord_p 2)} = \frac{ord_p 2}{(s, ord_p 2)}$, we have $ord_p 2 \nmid i \cdot s$. So we have

$$2^{i\ell} = 2^{ik \cdot ord_p 2 + is} \equiv 2^{is} \not\equiv 1 \pmod p.$$

Thus we also have

$$ord_p(2^\ell) = \frac{ord_p 2}{(\ell, ord_p 2)}.$$

□

Now we calculate the p-valuations, denoted by $v_p(\cdot)$, of some numbers. It will be useful for finding the minimal decomposition of the square mapping on $\mathbb{Z}_p$.

Lemma 7. *Let p be an odd prime. Then for all $1 \leq i < p$,*

$$v_p(2^{ord_p 2} - 1) = v_p(2^{i \cdot ord_p 2} - 1) < p - 1.$$

In particular,

$$v_p(2^{ord_p 2} - 1) = v_p(2^{p-1} - 1).$$

Proof. Assume that $v_p(2^{ord_p2}-1)=s\geq 1$. Then we can write

$$2^{ord_p2}=1+p^st,$$

for some integer $t\geq 1$ such that $(t,p)=1$. For all $1\leq i<p$, we have

$$(1+p^st)^i\equiv 1+ip^st \pmod{p^{s+1}}.$$

So,

$$v_p(2^{i\cdot ord_p2}-1)=s.$$

Since

$$p^s<2^{ord_p2}\leq 2^{p-1}<p^{p-1},$$

we conclude $s<p-1$.

In particular, by taking $i=(p-1)/ord_p2$, we have

$$v_p(2^{ord_p2}-1)=v_p(2^{p-1}-1).$$

□

Proposition 3. *Let p be an odd prime, and let $\hat{\sigma}=(\hat{x}_1,\hat{x}_2,\cdots,\hat{x}_\ell)\subset\mathbb{Z}_p^\times$ be a periodic orbit of $f:x\mapsto x^2$. If $x_1=\hat{x}_1+p^n\alpha$ for some $\alpha\in\mathbb{Z}_p\setminus p\mathbb{Z}_p$ and $n\geq 1$, then*

$$v_p(x_1^{2^{\ell r}-1}-1)=n+v_p(2^{p-1}-1),$$

where $r=\frac{ord_p2}{(\ell,ord_p2)}$.

Proof. By Theorem 1 and Proposition 1, we have $\ell<p-1$. Then

$$\ell r=\frac{\ell\cdot ord_p2}{(\ell,ord_p2)}<p\cdot ord_p2.$$

Observe that $ord_p2\mid\ell r$. By Lemma 7, we have

$$v_p(2^{\ell r}-1)=v_p(2^{p-1}-1).$$

Let $s=v_p(2^{p-1}-1)$; then $2^{\ell r}=1+p^sh$ for some $h\in\mathbb{Z}\setminus p\mathbb{Z}$. Observe that $\hat{x}_1\in\mathbb{Z}_p^\times$ is a periodic point of f of period ℓ. Thus $\hat{x}_1^{2^\ell}=\hat{x}_1$ and then $\hat{x}_1^{2^{\ell r}}=\hat{x}_1$. Multiplying $\hat{x}_1^{-1}$, we obtain

$$\hat{x}_1^{p^sh}=\hat{x}_1^{2^{\ell r}-1}=1.$$

So,

$$\begin{aligned}x_1^{2^{\ell r}-1}-1&=(\hat{x}_1+p^n\alpha)^{p^sh}-1\\&=\sum_{i=1}^{p^sh}\binom{p^sh}{i}\hat{x}_1^{p^sh-i}\alpha^ip^{ni}.\end{aligned}$$

Let

$$C_i=\binom{p^sh}{i}\hat{x}_1^{p^sh-i}\alpha^ip^{ni},\ 1\leq i\leq p^sh.$$

Then $v_p(C_1)=n+s$. Moreover, if $i>s+1$, then

$$v_p(C_i)\geq ni>n(s+1)=ns+n\geq s+n.$$

If $1<i\leq s+1$, then by Lemma 7, we know that $i<p$. Thus $v_p(\binom{p^sh}{i})=s$. Therefore,

$$v_p(C_i)=ni+s>n+s.$$

So,

$$v_p(x_1^{2^{\ell r}-1}-1)=v_p(C_1)=n+s.$$

□

4. Minimal decomposition of the square mapping on $\mathbb{Z}_p$

In this section, we focus on the minimal decomposition of the square mapping on $\mathbb{Z}_p$.

By the proof of Lemma 3, if a cycle at a certain level always grows (grows forever) then it will produce a minimal component of f. The following proposition shows when a cycle always grows (grows forever) for the square mapping. A cycle σ at level n is said to *split ℓ times* if σ splits, and the lifts of σ at level $n+1$ split and inductively all lifts at level $n+j(2\leq j<\ell)$ split.

Proposition 4. *Let p be an odd prime and let $f:x\mapsto x^2$ be the square mapping. Suppose that $\hat{\sigma}=(\hat{x}_1,\hat{x}_2,\cdots,\hat{x}_\ell)\subset\mathbb{Z}_p^\times$ is an ℓ-periodic orbit of f. For each $n\geq 1$, let $\sigma_n=(x_1,\cdots,x_\ell)\subset\mathbb{Z}/p^n\mathbb{Z}$ be the ℓ-cycle of the induced map f_n such that*

$$\sigma_n\equiv\hat{\sigma}\pmod{p^n},\quad \textit{i.e., for all } 1\leq i\leq\ell,\ x_i\equiv\hat{x}_i\pmod{p^n}.$$

1) If $2^\ell\equiv 1\pmod p$, then σ_n splits. There is one lift σ_{n+1} such that $\sigma_{n+1}\equiv\hat{\sigma}\pmod{p^{n+1}}$ and all other lifts split $v_p(2^{p-1}-1)-1$ times and all descendants at level $n+v_p(2^{p-1}-1)$ grow forever.

2) If $2^\ell\not\equiv 1\pmod p$, then σ_n partially splits. Let σ_{n+1} be a lift of σ_n.

(a) If σ_{n+1} is the lift of length ℓ, then $\sigma_{n+1}\equiv\hat{\sigma}\pmod{p^n}$, and σ_{n+1} partially splits.

(b) If σ_{n+1} is a lift of length ℓr for some integer $r>1$, then $r=\frac{ord_p2}{(ord_p2,\ell)}$ and σ_{n+1} split $v_p(2^{p-1}-1)-1$ times and all descendants of σ_{n+1} at level $n+v_p(2^{p-1}-1)$ grow forever.

Proof. Let $g=f^\ell:x\mapsto x^{2^\ell}$ be the ℓ-th iterate of f. Then,

$$a_n(x_1)=g'(x_1)=2^\ell x_1^{2^\ell-1},$$
$$b_n(x_1)=\frac{x_1^{2^\ell}-x_1}{p^n}.$$

Since $\hat{x}_1^{2^\ell}=\hat{x}_1$, then $\hat{x}_1^{2^\ell-1}=1$ and hence $x_1^{2^\ell-1}\equiv 1\pmod{p^n}$. Thus,

$$a_n(x_1)\equiv 2^\ell\pmod p.$$

1) Assume $2^\ell\equiv 1\pmod p$. Then $a_n(x_1)\equiv 1\pmod p$. Let $s=v_p(2^{p-1}-1)$. Observe that $ord_p2\leq\ell\leq p-1$ and $ord_p2\mid\ell$. By Lemma 7, we have $v_p(2^\ell-1)=s\geq 1$. Write

$$2^\ell=1+p^sh,$$

for some integer h with $(h,p)=1$. Since $x_1\equiv\hat{x}_1\pmod{p^n}$, we have $x_1=\hat{x}_1+p^nt$ for some $t\in\mathbb{Z}_p$. Thus by Proposition 3 and

$$g(x_1)-x_1=x_1(x_1^{2^\ell-1}-1),$$

we deduce that $b_n(x_1)\equiv 0\pmod p$. Thus σ_n splits.

Let $\sigma_{n+1} = (y_1, \cdots, y_\ell) \subset \mathbb{Z}/p^{n+1}\mathbb{Z}$ be a lift of σ_n. We distinguish the following two cases.

i) Assume $y_1 \equiv \hat{x}_1 \pmod{p^{n+1}}$. Then $\sigma_{n+1} \equiv \hat{\sigma} \pmod{p^{n+1}}$ and σ_{n+1} behaves the same as σ_n.

ii) Assume $y_1 \not\equiv \hat{x}_1 \pmod{p^{n+1}}$. Then $y_1 = \hat{x}_1 + p^n\alpha$ for some $\alpha \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$. Since $2^\ell \equiv 1 \pmod p$, we have $ord_p 2 \mid \ell$. By Proposition 3 and

$$g(y_1) - y_1 = y_1(y_1^{2^\ell - 1} - 1),$$

we get

$$v_p(b_{n+1}(y_1)) = s - 1.$$

If $s = 1$, then σ_{n+1} grows. By Lemma 2, the lift of σ_{n+1} grows forever.

If $s > 1$, then σ_{n+1} splits. By induction, let σ_{n+1+i} be a lift of σ_{n+1} at level $n+1+i$ for $0 \leq i < s-1$, then σ_{n+1+i} splits. Let $\sigma_{n+s} = (z_1, \cdots, z_\ell)$ be a lift of σ_{n+1} at level $n+s$. By Proposition 3, $v_p(b_{n+s}(z_1)) = 0$, so σ_{n+s} grows. By Lemma 2, the lift of σ_{n+s} grows forever.

2) Assume $2^\ell \not\equiv 1 \pmod p$. Then $a_n(x_1) \not\equiv 0, 1 \pmod p$. Thus σ_n partially splits. Let $\sigma_{n+1} = (y_1, \cdots, y_{\ell r}) \subset \mathbb{Z}/p^{n+1}\mathbb{Z}$ be a lift of σ_n of length ℓr.

If $r = 1$, then by Proposition 2, we get that $\sigma_{n+1} \equiv \hat{\sigma} \pmod{p^{n+1}}$, and σ_{n+1} behaves the same as σ_n.

If $r > 1$, then r is the order of a_n in $(\mathbb{Z}/p\mathbb{Z})^*$. By Lemma 6, $r = \frac{ord_p 2}{(ord_p 2, \ell)}$. By Lemma 7, we have

$$v_p(2^{\ell r - 1}) = v_p(2^{p-1}) = s.$$

Notice that $y_1 \equiv \hat{x}_1 \pmod{p^n}$ and $y_1 \not\equiv \hat{x}_1 \pmod{p^{n+1}}$. By Proposition 3,

$$v_p(g^r(y_1) - y_1) = v_p(y_1(y_1^{2^{\ell r - 1}} - 1)) = v_p(y_1^{2^{\ell r - 1}} - 1) = n + s.$$

The same argument as the case ii) of 1) implies that if σ_{n+1} splits $s-1$ times, then all the descendants of σ_{n+1} at level $n+s$ grow forever. □

Now we are ready to prove our main result.

Proof of Theorem 4. By Theorem 1, we know the dynamical structure of f at the first level. Let $\sigma = (x_1, x_2, \cdots, x_\ell) \subset (\mathbb{Z}/p\mathbb{Z})^*$ be a cycle of length ℓ at the first level. By Proposition 1, there exists a unique periodic orbit $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{X}_\sigma$ of f with the same length of σ.

By Proposition 4 and Lemmas 1 and 2, we get the minimal decomposition of system $(\mathbb{X}_\sigma, f)$,

$$\mathbb{X}_\sigma = \{\hat{x}_1, \cdots, \hat{x}_\ell\} \sqcup \left(\bigsqcup_{n \geq 1} \bigsqcup_{1 \leq i \leq \ell} S_{p^{-n}}(\hat{x}_i) \right),$$

where for each $n \geq 1$, the set $\bigsqcup_{1 \leq i \leq \ell} S_{p^{-n}}(\hat{x}_i)$ consists of

$$\frac{(p-1) \cdot (ord_p 2, \ell)}{ord_p 2} \cdot p^{v_p(2^{p-1}-1)-1}$$

minimal components and each minimal component consists of $j := \frac{\ell \cdot ord_p 2}{(ord_p 2, \ell)}$ closed disks of radius $p^{-n - v_p(2^{p-1}-1)}$.

By Theorem 3 and Proposition 4, each nontrivial minimal subsystem (which is not a periodic orbit) of $(\mathbb{X}_\sigma, f)$ is conjugate to the adding machine on the odometer $\mathbb{Z}_{(p_s)}$, where

$$(p_s) = (\ell, \ell j, \ell j p, \ell j p^2, \cdots).$$

$\square$

5. Examples

Recall that $S_1(0)$ is the unit sphere and f is the square mapping. For different primes, the dynamical behaviors of $(S_1(0), f)$ are quite different.

A Fermat prime is a prime number p of the form $p = 2^{2^n} + 1$ where n is a nonnegative integer. It is known that the iteration graph of square mapping on $\mathbb{F}_p^*$ of the nonzero elements in the finite field $\mathbb{F}_p$ is a tree attached to the unique loop of 1 when p is a Fermat prime, and conversely, if there is only one loop, then p must be a Fermat prime ([18]). In this case, 0 and 1 are the only fixed points of f, the disk $D_1(0)$ is the attracting basin of the fixed point 0. The disk $D_1(1)$ is the unique Siegel disk. Furthermore, we have a minimal decomposition of $D_1(1)$ by Theorem 4. The other open disks with radius 1 are attracted by the Siegel disk $D_1(1)$. Decompose $D_1(1)$ as

$$D_1(1) = \{1\} \sqcup \left(\bigsqcup_{i \geq 1} S_{p^{-i}}(1) \right).$$

Then each sphere $S_{p^{-i}}(1)$ consists of $p^{v_p(2^{p-1}-1)-1}$ minimal components, and each minimal component is a union of p closed disks of radius $p^{-i-v_2(2^{p-1}-1)}$.

An odd prime p is called a Wieferich prime if

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

If an odd prime p is not a Wieferich prime, we know that $v_p(2^{p-1} - 1) = 1$. For a cycle $\sigma = (x_1, x_2, \cdots, x_\ell) \subset \mathbb{Z}/p\mathbb{Z}$ of length ℓ at the first level, Proposition 1 implies that there exists a unique periodic orbit $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{X}_\sigma$ of f with the same length of σ. By Proposition 4, the lifts which do not correspond to the periodic orbit grow forever and the lift corresponding to the periodic orbit behaves the same as σ. Thus for each integer $n \geq 1$, the union $\bigsqcup_{1 \leq i \leq \ell} S_{p^{-n}}(\hat{x}_i)$ of the spheres consists of $\frac{(p-1)\cdot(ord_p 2, \ell)}{ord_p 2}$ minimal components and each minimal component consists of $\frac{\ell \cdot ord_p 2}{(ord_p 2, \ell)}$ closed disks of radius p^{-n-1}.

The only known Wieferich primes, 1093 and 3511, were found by Meissner in 1913 and Beeger in 1922, respectively. It has been conjectured that only finitely many Wieferich primes exist. Silverman [19] showed in 1988 that if the abc conjecture holds, then there exist infinitely many non-Wieferich primes. Numerical evidence suggests that very few of the prime numbers in a given interval are Wieferich primes. A proof of the abc conjecture would not automatically prove that there are only finitely many Wieferich primes, since the set of Wieferich primes and the set of non-Wieferich primes could possibly both be infinite and the finiteness or infiniteness of the set of Wieferich primes would have to be proven separately.

For the known Wieferich primes $p = 1093$ or 3511, we have $v_p(2^{p-1} - 1) = 2$. Fix a cycle $\sigma = (x_1, x_2, \cdots, x_\ell) \subset \mathbb{Z}/p\mathbb{Z}$ of length ℓ at the first level. Similar to the general case, there exists a unique periodic orbit $\hat{\sigma} = (\hat{x}_1, \hat{x}_2, \cdots, \hat{x}_\ell) \subset \mathbb{X}_\sigma$ of

f with the same length of σ. Different from the non-Wieferich primes, the lifts which do not correspond to the periodic orbit split one time at first and then all the descendants grow forever. For each integer $n \geq 1$, the union $\bigsqcup_{1 \leq i \leq \ell} S_{p^{-n}}(\hat{x}_i)$ of the spheres consists of $\frac{p(p-1)\cdot(ord_p 2,\ell)}{ord_p 2}$ minimal components and each minimal component consists of $\frac{\ell \cdot ord_p 2}{(ord_p 2,\ell)}$ closed disks of radius p^{-n-2}.

However, the existence of prime number p such that $v_p(2^{p-1}-1) > 2$ is still unknown.

Acknowledgement

The authors thank the referee for drawing their attention to reference [16].

References

[1] V. S. Anashin, *Uniformly distributed sequences of p-adic integers* (Russian, with Russian summary), Mat. Zametki **55** (1994), no. 2, 3–46, 188, DOI 10.1007/BF02113290; English transl., Math. Notes **55** (1994), no. 1-2, 109–133. MR1275316 (95f:11096)

[2] V. S. Anashin, *Uniformly distributed sequences of p-adic integers* (Russian, with Russian summary), Diskret. Mat. **14** (2002), no. 4, 3–64; English transl., Discrete Math. Appl. **12** (2002), no. 6, 527–590. MR1964120 (2004a:11077)

[3] Vladimir Anashin, *Ergodic transformations in the space of p-adic integers*, p-adic mathematical physics, AIP Conf. Proc., vol. 826, Amer. Inst. Phys., Melville, NY, 2006, pp. 3–24, DOI 10.1063/1.2193107. MR2258670 (2007m:37015)

[4] V. S. Anashin, A. Yu. Khrennikov, and E. I. Yurova, *Characterization of ergodic p-adic dynamical systems in terms of the van der Put basis* (Russian), Dokl. Akad. Nauk **438** (2011), no. 2, 151–153, DOI 10.1134/S1064562411030100; English transl., Dokl. Math. **83** (2011), no. 3, 306–308. MR2857398 (2012g:37177)

[5] Jean-Luc Chabert, Ai-Hua Fan, and Youssef Fares, *Minimal dynamical systems on a discrete valuation domain*, Discrete Contin. Dyn. Syst. **25** (2009), no. 3, 777–795, DOI 10.3934/dcds.2009.25.777. MR2533975 (2010h:37021)

[6] Guy Chassé, *Applications d'un corps fini dans lui-même* (French), Série: A [Series: A], vol. 149, Université de Rennes I, U.E.R. de Mathématiques et Informatique, Rennes, 1984. Dissertation, Université de Rennes I, Rennes, 1984. MR782298 (86e:11118)

[7] Zaqueu Coelho and William Parry, *Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers*, Topology, ergodic theory, real algebraic geometry, Amer. Math. Soc. Transl. Ser. 2, vol. 202, Amer. Math. Soc., Providence, RI, 2001, pp. 51–70. MR1819181 (2002e:11103)

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

[9] Fabien Durand and Frédéric Paccaut, *Minimal polynomial dynamics on the set of 3-adic integers*, Bull. Lond. Math. Soc. **41** (2009), no. 2, 302–314, DOI 10.1112/blms/bdp003. MR2496506 (2010h:37219)

[10] Ai-Hua Fan, Ming-Tian Li, Jia-Yan Yao, and Dan Zhou, *Strict ergodicity of affine p-adic dynamical systems on $\mathbb{Z}_p$*, Adv. Math. **214** (2007), no. 2, 666–700, DOI 10.1016/j.aim.2007.03.003. MR2349716 (2008g:37038)

[11] Aihua Fan and Lingmin Liao, *On minimal decomposition of p-adic polynomial dynamical systems*, Adv. Math. **228** (2011), no. 4, 2116–2144, DOI 10.1016/j.aim.2011.06.032. MR2836116 (2012i:37143)

[12] Aihua Fan, Shilei Fan, Lingmin Liao, and Yuefei Wang, *On minimal decomposition of p-adic homographic dynamical systems*, Adv. Math. **257** (2014), 92–135, DOI 10.1016/j.aim.2014.02.007. MR3187646

[13] Shilei Fan and Lingmin Liao, *Dynamics of convergent power series on the integral ring of a finite extension of $\mathbb{Q}_p$*, J. Differential Equations **259** (2015), no. 4, 1628–1648, DOI 10.1016/j.jde.2015.03.042. MR3345863

[14] Christie L. Gilbert, Joseph D. Kolesar, Clifford A. Reiter, and John D. Storey, *Function digraphs of quadratic maps modulo p*, Fibonacci Quart. **39** (2001), no. 1, 32–49. MR1812618 (2002e:05068)

[15] Sangtae Jeong, *Toward the ergodicity of p-adic 1-Lipschitz functions represented by the van der Put series*, J. Number Theory **133** (2013), no. 9, 2874–2891, DOI 10.1016/j.jnt.2013.02.006. MR3057052

[16] Andrei Khrennikov and Marcus Nilsson, *On the number of cycles of p-adic dynamical systems*, J. Number Theory **90** (2001), no. 2, 255–264, DOI 10.1006/jnth.2001.2665. MR1858076 (2002g:11172)

[17] Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer-Verlag, New York, 2000. MR1760253 (2001g:11182)

[18] Thomas D. Rogers, *The graph of the square mapping on the prime fields*, Discrete Math. **148** (1996), no. 1-3, 317–324, DOI 10.1016/0012-365X(94)00250-M. MR1368298 (96m:11115)

[19] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237, DOI 10.1016/0022-314X(88)90019-4. MR961918 (89m:11027)

[20] Lawrence Somer and Michal Křížek, *Structure of digraphs associated with quadratic congruences with composite moduli*, Discrete Math. **306** (2006), no. 18, 2174–2185, DOI 10.1016/j.disc.2005.12.026. MR2255611 (2008g:05087)

[21] Troy Vasiga and Jeffrey Shallit, *On the iteration of certain quadratic maps over* GF(p), Discrete Math. **277** (2004), no. 1-3, 219–240, DOI 10.1016/S0012-365X(03)00158-4. MR2033734 (2004k:05104)

[22] Peter Walters, *An introduction to ergodic theory*, Graduate Texts in Mathematics, vol. 79, Springer-Verlag, New York-Berlin, 1982. MR648108 (84e:28017)

[23] E. Yurova, *On ergodicity of p-adic dynamical systems for arbitrary prime p*, p-Adic Numbers Ultrametric Anal. Appl. **5** (2013), no. 3, 239–241, DOI 10.1134/S2070046613030072. MR3090218

School of Mathematics and Statistics, Central China Normal University, 430079, Wuhan, People's Republic of China

E-mail address: slfan@mail.ccnu.edu.cn

LAMA, UMR 8050, CNRS, Université Paris-Est Créteil Val de Marne, 61 Avenue du Général de Gaulle, 94010 Créteil Cedex, France

E-mail address: lingmin.liao@u-pec.fr