P-ADIC POLYNOMIAL DYNAMICS

AIHUA FAN

Abstract. This introductory lecture intends to present polynomial dynamics on the ring $\mathbb{Z}_p$ of p-adic integral numbers, a large class of topological symbolic dynamics. Such symbolic dynamics can be studied as algebraic dynamics using algebraic and analytic methods. To this end, we will first present p-adic numbers and analysis on the filed $\mathbb{Q}_p$ of p-adic numbers.

1. Introduction

Our objects of study are Cantor topological dynamical systems $T : X \to X$ where T is a continuous map on a Cantor set X. Typically

$$X = \{0, 1\}^{\infty}.$$

We would like to consider (T, X) as an algebraic dynamics. By identifying $0, 1$ with $2\mathbb{Z}$, $1 + 2\mathbb{Z}$, we can consider X as

$$X = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times \cdots .$$

It is a group, an infinite product group. But we will consider another group operation on X. Better is that we can make X into a ring, a local ring and even $\mathbb{Z}$-module. So, continuous maps on X include polynomials which are dense in the space of all continuous maps (Kaplansky). Calculus can also be well developed on such a local ring and on its fraction fields.

(1) Do the algebraic structure and the calculus helps us to understand the dynamics $T : X \to X$?
(2) How about the polynomial dynamics ?

Such dynamics are called dyadic dynamics and more generally we can consider p-adic dynamics for any prime p.

One of motivation for studying p-adic dynamics come from physics. Volovich [**?**] published the first paper on application of p-adic numbers to theoretical physics(p-adic string theory). The string theory attempts to reconsider foundations of physics by using space extended objets (strings) instead of pointwise objects (elementary particles). The scenarios of string spectacle is performed at Planck distances (10^{-34} cm). Physicists have the feeling that the space-time at Planck scale have some distinguishing features which cannot be described by the standard mathematical models based on the Archimedean field $\mathbb{R}$ which has the following Archimedean property:

$$\ell > 0, L > 0 \Rightarrow \exists n \in \mathbb{N}, n\ell > L.$$

There were also intuitive cosmological ideas that the space-time at Planck scale has non-Archimedean structure. On the other hand, at Planck scale, there would be no order, not like on $\mathbb{R}$. The field $\mathbb{Q}_p$ of p-adic numbers has non-Archimedean structure and is non-ordered.

The theory of p-adic dynamical systems is recently rapidly developing (see the books [4, 30, 32, 41, 49, 50]). Motivated by different parts of mathematics and physics where it is natural to treat the p-adic completion of the field $\mathbb{Q}$ of rational numbers and to use this completed field (including number theory, algebraic and arithmetic geometry, cryptography, physical models, biological models, and so on).

The p-adic dynamics appears naturally in the study of smooth dynamics. For example, an ergodic algebraic automorphism of a torus preserving Haar measure was shown by Katznelson [29] to be isomorphic to a Bernoulli shift which is of p-adic nature. This was generalized by Lind [36] to skew products with ergodic group automorphism where the understanding of the p-adic hyperbolicity was involved. See [**?**, 37, 38] for other situations where p-adic dynamics or p-adic consideration arise.

It seems that the first study of p-adic dynamical systems is the work of Oselies and Zieschang [44] where they considered the continuous automorphisms of the ring of p-adic integers $\mathbb{Z}_p$ viewed as an additive group, which are multiplication transformations $M_a(x) = ax$ with $a \in \mathbb{Z}_p^\times$, a unit in $\mathbb{Z}_p$. They constructed an ergodic decomposition of $M_a : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ which consists of the cosets of the smallest closed subgroup containing a of the unit group $\mathbb{Z}_p^\times$. These multiplication transformations were also studied by Coelho and Parry [13] in order to study the distribution of Fibonacci numbers. The simple power transformations $\psi_n(x) = x^n$ acting on the group of units $\mathbb{Z}_p^\times$ were studied by Gundlach, Khrennikov and Lindahl [25]. Herman and Yoccoz ([26]) proved that Siegel's linearization theorem in complex dynamical systems is also true for non-Archimedean fields. Their work might be the first one on complex p-adic dynamics. Lubin [40] used the formal groups from local arithmetic geometry to study iterates of p-adic analytic maps. Li [35], Benedetto [9], Hsia [27], Rivera-Letelier [46], Jones [28] and others have systematically studied iteration of rational maps over the p-adic Riemann sphere. In a different direction, Morton and Silverman [43], Arrowsmith and Vivaldi [6] and others have also studied arithmetic dynamics using p-adic techniques.

In this lecture, we first introduce p-adic numbers and present basic notions of p-adic analysis. Then we present two kinds of polynomial dynamics, one is chaotic and the other is 1-Lipschitz.

2. Random number generators

We need random numbers. p-adic dynamics are related to random number generation and to cryptography etc.

2.1. **von Neumann method.** The middle-square method is a method of generating pseudorandom numbers, a first method. The method was first described in a manuscript by a Franciscan friar (known as Brother Edvin) between 1240 and 1250. John von Neumann reinvented it and described it at a conference in 1949. The method is defined by the function N taking the middle k-digit number of the square of an integer.

Here is the method: take a seed a_0: a k-digit number.

define the recurrence$a_{n+1} = N(a_n)$: the middle k-digit number of a_n^2.

There are bad seeds ($k = 4$) like 0100, 2500, 3792, 7600. For example, 3792 is fixed by N:

$$3792^2 = 14\mathit{397}264, \quad 3972 = N(3972)$$

The following seeds ($n = 4$) 0540, 2916, 5030, 3009 are good. Actually $0540 \to 9160 \to 9056 \to 0111 \to 1232 \to 5178 \to 8116 \to 8994 \to 8920 \to 5664 \to 0808 \to 5386 \to 0089 \to 7921 \to 7422 \to 0860 \to 3960 \to 6816 \to 4578 \to 9580 \to 7764 \to \cdots$

How to find cycles as long as possible ? This method is not a good method, since its period is usually very short.

2.2. **Linear Congruently Generator (ECG).** The linear congruently generator method represents one of the oldest and best-known pseudorandom number generator algorithms. The method is easy to understand and easy implement. The generator is defined by the recurrence relation:

$$X_{n+1} = aX_n + b \qquad \mod m \quad (n \geq 0)$$

where

- $m \geq 2$: modulus
- a: multiplier
- b: increment
- X_0: seed

Remark that $X_n \in \{0, 1, \cdots, m-1\} = \mathbb{Z}/m\mathbb{Z}$ and $X_n/m \in \{0/m, 1/m, \cdots, (m-1)/m\} \subset [0, 1]$. We consider X_n/m as pseudorandom number. $\{X_n\}$ is an orbit. One problem is to find maximal period of the system, which is smaller than $\leq m$.

Is X_n/m a sample of $U(0, 1)$ (the uniform distribution on the interval $[0, 1]$) ? Non, it is not and can only consider it as pseudorandom.

Here comes the first dynamical system to study: the affine dynamics $x \mapsto ax+b$ (mod m), which is a finite dynamical system on the ring $\mathbb{Z}/m\mathbb{Z}$.

2.3. **A simple algebraic dynamics (warmup).** Notice that $\mathbb{Z}/p\mathbb{Z}$ is a field. Computations below are made in the field. For example, $a = 1$ means $a = 1$ (mod p) and a^{-1} mean the inverse in the field.

Theorem 1. *$T_{a,b}x = ax + b$ is minimal on $\mathbb{Z}/p\mathbb{Z}$ iffy $a = 1$ and $b \neq 0$.*

Proof. *Necessity.* If $b = 0$, 0 would be a fixed point. Contradiction. If $a \neq 1$, $1-a$ would be invertible. Then we solve $T_{a,b}x = x$ and get a fixed point $(1-a)^{-1}b$. Contradiction.

Sufficiency. Since $a = 1$, $T_{a,b}x = x+b$. It is clear that the orbit of 0: $0, b, \cdots, (p-1)b$ is a full cycle if $b \neq 0$. □

Let us make some remarks:

- It seems too simple. But conveniently choose b (large enough, but not too large), we see some randomness it the orbits. For example, the orbit of 0 for $12x + 5$ on $\mathbb{Z}/11\mathbb{Z}$:

  $$0, 5, 10, 4, 9, 3, 8, 2, 7, 1, 6$$

- It is not so simple on the ring $\mathbb{Z}/m\mathbb{Z}$ for general m.
- On any ring, we have

  $$T^k_{a,b}x = a^k x + (1 + a + \cdots + a^{k-1})b = a^k x + \frac{a^k - 1}{a - 1}b$$

  (assuming $a - 1$ is invertible for the last equality). So the behavior of the powers a^k play a role.

The following simple analysis gives a full picture of the dynamics of $T_{a,b}$ on $\mathbb{Z}/p\mathbb{Z}$.

Theorem 2. *Consider an arbitrary affine mapping $T_{a,b}x = ax + b$.*

(1) If $a = 0$, there is one fixed point b who attracts all other points.
(2) If $a = 1$ and $b = 0$, there are p fixed points.
(3) If $a = 1$ and $b \neq 0$, there is a (maximal) cycle.
(4) If $a \neq 0, 1$ (having d as its order), there is one fixed point $-b/(a-1)$ and $(p-1)/d$ cycles of length d.

Proof. Only the last point needs a proof. For any $k \geq 1$

$$T_{a,b}^k x - x = (a^k - 1)\left(x + \frac{b}{a-1}\right).$$

So $T_{a,b}^k x = x$ iff $x + b/(a-1) = 0$ or $a^k - 1 = 0$. The least such k is the order of a, which is independent of x ($\neq -b/(a-1)$). □

How to do with higher order polynomial generator ?

3. Ring of integer-valued polynomials Int($\mathbb{Z}$)

Integer-valued polynomials were studied by Polya (see [10]). We say that $P \in \mathbb{Q}[x]$ is an integer-valued polynomials (we write $P \in \mathrm{Int}(\mathbb{Z})$): if $P(\mathbb{Z}) \subset \mathbb{Z}$. Examples: $\frac{x(x-1)}{2}, \frac{x(x+1)(x+2)}{6}$. Typical examples:

$$B_0(x) \equiv 1, \quad B_n(x) = \frac{x(x-1)(x-2)\cdots(x-n+1)}{n!} = \binom{x}{n}.$$

Theorem 3 (Polya)**.** *$\{B_k\}_{0 \leq k \leq n}$ is a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}_n[x]$. It is also a basis of the $\mathbb{Z}$-module $\mathrm{Int}_n(\mathbb{Z}) = \mathrm{Int}(\mathbb{Z}) \cap \mathbb{Q}_n[x]$.*

Proof The first assertion follows from the basic properties of B_n:

- $\deg B_k = k$.
- If $0 \leq k < n$, $B_n(k) = 0$ (all zeros of B_n).
- If $k > n$, $B_n(k) \in \mathbb{N}^*$ (choose n from k)
- If $x < 0$, $B_n(k) = (-1)^n B_n(n + |k| - 1) \in \mathbb{Z}$.

For the second assertion, we need to observe that $B_k \in \mathrm{Int}(\mathbb{Z})$. □

Conclusion: $f \in \mathrm{Int}(\mathbb{Z})$ with $\deg f = n$ iff there exists (unique) $(a_0, a_1, \cdots, a_n) \in \mathbb{Z}^{n+1}$ such that

$$f(x) = \sum_{k=0}^{n} a_k \binom{x}{n}.$$

How to find $a_0, a_1, \cdots, a_n$? The Gregory-Newton interpolation gives a solution.

Define the (forward) difference operator

$$\Delta f(x) = f(x+1) - f(x)$$

and the translation operator

$$Tf(x) = f(x+1).$$

They have the relations:

$$\Delta = T - I, \qquad \Delta^n = (T - I)^n = \sum_{k=0}^{n} (-1)^{n-k} \left(\begin{array}{c} n \\ k \end{array} \right) T^k.$$

So,

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \left(\begin{array}{c} n \\ k \end{array} \right) f(x+k).$$

Theorem 4 (Gregory-Newton)**.** *For $f \in \mathbb{R}_n[x]$, we have*

$$f(x) = \sum_{k=0}^{n} \Delta^k f(0) B_k(x).$$

Proof It is a consequence of the facts: $B_n(k) = \delta_{n,k}$ for $0 \leq k \leq n$); $\Delta B_n = B_{n-1}$ ($B_{-1} \equiv 0$) which is a consequence of Pascal relation; and

$$\Delta^k f(x) = a_k B_0(x) + a_{k+1} B_1(x) + \cdots + a_n B_{n-k}(x).$$

□

This result will be generalized to the Mahler expansion of p-adic continuous functions.

4. p-adic Numbers

In this section, we construct from different ways the field $\mathbb{Q}_p$ of p-adic numbers and we prove a first theorem in the p-adic analysis, namely the theorem on Mahler expansions in $C(\mathbb{Z}_p, \mathbb{Q}_p)$ which is the space of all continuous functions defined on $\mathbb{Z}_p$ taking values in $\mathbb{Q}_p$. The result is a generalization of the above mentioned Polya theorem. See [42, 47, 48] for the theory of p-adic numbers.

4.1. **Systems of numbers constructed from** $\mathbb{N}$**.** Suppose that we are given a sequence of positive integers $(m_0, m_1, \cdots, m_k, \cdots)$ with $m_k \geq 2$. The most important case is $m_k = p$ for all k, where p is a prime. We claim that

$$\mathbb{N} \simeq \coprod \{0, 1, \cdots, m_k - 1\}.$$

In other word, for any integer $n \in \mathbb{N}$, there exists unique $a_k \in \{0, 1, \cdots, m_k - 1\}$ such that

$$n = a_0 + a_1 m_0 + a_2 m_0 m_1 + \cdots + a_N m_0 m_1 \cdots m_{N-1}. \tag{1}$$

We can actually find the a_k's (called digits) recursively by the Euclidean algorithm:

$$\text{(Euclid)} \qquad n = m_0 n' + a_0, \quad n' = m_1 n'' + a_1, \cdots .$$

We define the product space

$$\mathbb{Z}_{(m_k)} := \prod_{k=0}^{\infty} \mathbb{Z}/m_k\mathbb{Z}.$$

For $x = (a_0, a_1, \cdots) \in \mathbb{Z}_{(m_k)}$, we can formally write

$$x = \sum_{k=0}^{\infty} a_k m_0 \cdots m_{k-1}. \tag{2}$$

Actually, as we will see, the series converges with respect to a metric which is compatible with the product topology. The space $\mathbb{Z}_{(m_k)}$ is compact, by Tychonov's theorem.

We have the embedding $\mathbb{N} \subset \mathbb{Z}_{(m_k)}$?according to (1) and $\mathbb{N}$ is evidently dense in $\mathbb{Z}_{(m_k)}$ (i.e. $\overline{\mathbb{N}} = \mathbb{Z}_{(m_k)}$).

For the special case $m_k = p$, we denote special $\mathbb{Z}_{(m_k)}$ with $m_k = p$ by $\mathbb{Z}_p$. In this case, we have the (formal) expansion

$$x = \sum_{k=0}^{\infty} a_k p^k.$$

4.2. $\mathbb{Z}_{(m_k)}$ **is a ring.** Addition and multiplication are defined in $\mathbb{N}$, which is dense in $\mathbb{Z}_{(m_k)}$. These operations defined from $\mathbb{N} \times \mathbb{N}$ into $\mathbb{N}$ are uniformly continuous. So, they can be uniquely extended on $\mathbb{Z}_{(m_k)}$.

How to add and multiply two positive integers using their digits? Just as usual, we manipulate (add or multiply) the digits with carry to the right. In the same we can add and multiply two "numbers" in $\mathbb{Z}_{(m_k)}$ by manipulating their digits with carry to the right. For example,

$$(1, 0, 0, \cdots) + (m_0 - 1, m_1 - 1, m_2 - 1, \cdots) = (0, 0, 0, \cdots).$$

Recall that

$$1 = (1, 0, 0, \cdots)$$

So, we could say that

$$-1 = (m_0 - 1, m_1 - 1, m_2 - 1, \cdots).$$

Theorem 5. *$\mathbb{Z}_{(m_k)}$ is a ring. In particular, $\mathbb{Z}_p$ is a ring.*

Proof. Clearly, $0 = (0, 0, \cdots)$ is the neutral element of the addition and $1 = (1, 0, \cdots)$ is the unit of the multiplication. The commutativity, associativity and distributivity are consequences of those in $\mathbb{N}$. It is easy to check that

$$-(a_0, a_1, a_k, \cdots) = (m_0 - a_0 - 1, m_1 - a_1 - 1, m_2 - a_2 - 1? \cdots).$$

□

The proof shows that $\mathbb{Z} \subset \mathbb{Z}_{(m_k)}$. But any strictly negative integer has infinitely many non zero digits.

The mapping on $\mathbb{Z}_{(m_k)}$ defined by $x \mapsto x + 1$ s called the Odometer on $\mathbb{Z}_{(m_k)}$.

4.3. **Field of p-adic numbers.** If $m_k = p$ for some prime p, we get a better structure.

Theorem 6. *Let $p \geq 2$ be a prime. Then $\mathbb{Z}_p$ is an integral ring. An element $\sum_{k=0}^{\infty} a_k p^k \in \mathbb{Z}_p$ is invertible iff $a_0 \neq 0$.*

Proof. The commutative ring $\mathbb{Z}_p$ contains $\mathbb{Z}$ as subring. We are going to show that it has no zero divisor. Let

$$a = \sum_{k=0}^{\infty} a_k p^k \neq 0, \quad b = \sum_{k=0}^{\infty} b_k p^k \neq 0.$$

Define u (respectively v) to be the first k such that $a_k \neq 0$ (respectively $b_k \neq 0$). Then a_u and b_v are not divisible by p, and then so is $a_n b_v$. By definition of multiplication, the first nonzero digit c_{u+v} of the product ab is the digit associated to p^{u+v} and it is defined by

$$0 \leq c_{u+v} < p, \quad c_{u+v} = a_u b_v (\bmod p).$$

Since $a_u b_v$ is not divisible by p, we have $c_{u+v} \neq 0$, so that $ab \neq 0$.

If a is invertible and b is its inverse, the above proof shows that we must have $u = v = 0$, in particular $u = 0$. Now suppose $u = 0$. Choose $0 < b_0 < p$ such that

$a_0b_0 = 1(\text{mod } p)$. So we can write $a_0b_0 = 1 + kp$ for some integer $0 \leq k < p$. Now if we write $a = a_0 + p\alpha$, then

$$ab_0 = 1 + kp + p\alpha b_0 = 1 + p\beta$$

for $\beta \in \mathbb{Z}_p$. We claim that it suffices to show that $1 + p\beta$ is invertible, because $a \cdot b_0(1 + p\beta)^{-1} = 1$. So we get

$$a^{-1} = b_0(1 + p\beta)^{-1}.$$

For the inverse of $1 + p\beta$, we can formally take

$$(l + p\beta)^{-1} = 1 - p\beta + p^2\beta^2 - \cdots = 1 + c_1p + c_2p^2 + \cdots .$$

with $0 \leq c_j < p$. We can surely find c_j's by applying the rules for carries, although the procedure is cumbersome. □

For example, $1 - p$ is invertible in $\mathbb{Z}_p$. Actually we have

$$(1 - p)^{-1} = \frac{1}{1 - p} = 1 + p + p^2 + \cdots \in \mathbb{Z}_p.$$

Elements in $\mathbb{Z}_p$ are called p-adic integers. The sets $\mathbb{N}$ and $\mathbb{Z}$ are both dense subset of $\mathbb{Z}_p$. By definition, the field of p-adic numbers, denoted by $\mathbb{Q}_p$, is the fraction field of $\mathbb{Z}_p$. The following theorem provides a canonical representation for p-adic numbers.

Theorem 7. *Let $x \in \mathbb{Q}_p$ be a p-adic number. Then there exists an integer $v(x) \in \mathbb{Z}$ such that*

$$x = \sum_{i=v(x)}^{\infty} a_i p^i$$

where $a_i \in \{0, 1, \cdots, p-1\}$ for all i with $a_{v(x)} \neq 0$. This expansion is unique. The rules of addition and multiplication in $\mathbb{Q}_p$ is the same as in $\mathbb{Q}_p$.

Proof. Assume $x \neq 0$. Otherwise $v(x) = -\infty$ and $a_k = 0$ for all k. By definition, there are $z_1, z_2 \in \mathbb{Z}_p$ such that $x = \frac{z_1}{z_2}$. We can assume that $z_1 = p^{-v}a$ for some $v \in \mathbb{Z}$ and $z_2 = b$ where

$$a = \sum_{k=0}^{\infty} a_k p^k, \quad b = \sum_{k=0}^{\infty} b_k p^k$$

with $a_0 \neq 0$ and $b_k \neq 0$. Then $a, b \in \mathbb{Z}_p$ and b is invertible in $\mathbb{Z}_p$. So $\frac{a}{b} \in \mathbb{Z}_p$. Write

$$\frac{a}{b} = \sum_{k=0}^{\infty} c_k p^k.$$

Thus

$$x = p^{-v} \sum_{k=0}^{\infty} c_k p^k = \sum_{n=v}^{\infty} c_{n+v} p^n.$$

The uniqueness of the expansion is left as exercise. For the above number x, after multiply x by p^v we get a p-adic integer xp^v. This fact allows us immediately to understand how operate the addition and the multiplication. □

If x has the above expansion, the following fraction

$$\{x\} := \sum_{v(x) \leq i < 0} a_i p^i$$

is called the fractional part of x. While $x - \{x\}$ is the integral part of x.

It is easy to see that the shift on $\mathbb{Z}_p$ has the following algebraic expression:

$$(x_0, x_1, \cdots) \mapsto \sigma_p(x) = (x_1, x_2, \cdots) = \frac{x}{p} - \left\{\frac{x}{p}\right\}.$$

Thus, we could consider the shift as an "algebraic" dynamics. But it is not polynomial in the strict sense.

As we shall see, odometers and shifts are prototypes of our algebraic dynamical systems.

4.4. **Norm and valuation on $\mathbb{Q}_p$ (second way of introducing $\mathbb{Q}_p$).** Now let us explain the second way to construct the field of p-adic numbers. The usual field $\mathbb{R}$ of real numbers is the completion of the field $\mathbb{Q}$ of rational numbers relative to the usual absolute value $|\cdot|$.

We can construct the field $\mathbb{Q}_p$ in the same way but with another absolute value (also called norm).

The p-adic norm of a rational number $x \in \mathbb{Q}$, denoted by $|x|_p$, is defined as follows:

$$|x|_p = p^{-v_p(x)} \quad \text{if} \quad x = p^{v_p(x)}\frac{r}{s} \quad \text{with} \quad (r,p) = (s,p) = 1$$

where the integer $v_p(x)$ is called the p-adic valuation of x.

It is not difficult to check that $|x|_p$ is a non-Archimedean norm in the sense that

- $|-x|_p = |x|_p$
- $|xy|_p = |x|_p|y|_p$
- $|x+y|_p \leq \max\{|x|_p, |y|_p\}$

The last inequality is called ultra triangle inequality, which implies that there are only isocele triangles in $(\mathbb{Q}, |\cdot|_p)$.

Theorem 8 (Ostrowski)**.** *Each non-trivial norm on $\mathbb{Q}$ is equivalent to $|\cdot|$ or to $|\cdot|_p$ for some prime p.*

By definition, the field of p-adic numbers $\mathbb{Q}_p$ is the $|\cdot|_p$-completion of $\mathbb{Q}$.

The fields $\mathbb{C}$ of complex numbers is the quadratic extension $\mathbb{R}(i)$ of $\mathbb{R}$. The field $\mathbb{C}$ is topologically complete and algebraically closed. But no finite extension $\mathbb{Q}_p(\alpha_1, \cdots, \alpha_r)$ is algebraically closed. Take an algebraically closed extension $\mathbb{Q}_p^{ac}$. The completion of $\mathbb{Q}_p^{ac}$ is denoted $\mathbb{C}_p$ which is topologically complete and algebraically closed. We call $\mathbb{C}_p$ the field of "complex" p-adic numbers.

As a vector space over $\mathbb{Q}_p$, $\mathbb{C}_p$ has an infinite dimension. Also notice that, unlike $\mathbb{C}$, $\mathbb{C}_p$ is not locally compact.

4.5. **Properties of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ (Third point of view).** The ring $\mathbb{Z}_p$ is equal to the inverse limit

$$\mathbb{Z}_p \leftarrow \cdots \leftarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \leftarrow \mathbb{Z}/p^n\mathbb{Z} \leftarrow \cdots \leftarrow \mathbb{Z}/p\mathbb{Z}.$$

In other word, $z \in \mathbb{Z}_p$ is identified with $(z_n) \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ such that

$$z_{n+1} = z_n \pmod{p^n}.$$

We can actually take $z_n = \sum_{k=0}^{n-1} p^k a_k$ when $z = \sum_{k=0}^{\infty} p^k a_k$.

Let us give the following list of properties:

(1) We have
$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$
and the closed (open) ball $B_{p^{-k}}(a)$ centered at a of radius P^{-k} equals $a + p^k\mathbb{Z}_p$.
(2) $\mathbb{U} := \{x \in \mathbb{Z}_p : |x|_p = 1\}$ is the group of units of $\mathbb{Z}_p$ and
$$\mathbb{U} = \bigsqcup_{i=1}^{p-1} B_{1/p}(i).$$
(3) $\mathcal{P} = \{x \in \mathbb{Z}_p : |x|_p < 1\} = B_{1/p}(0)$ is the unique maximal ideal of $\mathbb{Z}_p$.
(4) $|Q_p^*|_p = \{p^k : k \in \mathbb{Z}\}$ a discrete subgroup of $(\mathbb{R}_+^*, \times)$.
(5) $\mathbb{Q}_p$ is separable, locally compact and totally disconnected.

4.6. **Legendre formula.** Let us present the Legendre formula. Its proof shows how to compute the valuation of a number.

Theorem 9. *Write $n = \sum_{k=0}^{t} a_k p^k$. Then*
$$v_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - s_p(n)}{p-1}$$
where $s_p(n) = \sum_{k=0}^{t} a_k$.

Proof. Consider the sequence $\{1, 2, \cdots, n\}$. The subsequence of $\lfloor n/p \rfloor$ elements
$$p, 2p, \cdots, \lfloor n/p \rfloor p$$
is compose of those divisible by p, and that of $\lfloor n/p^2 \rfloor$ elements
$$p^2, 2p^2, \cdots, \lfloor n/p^2 \rfloor p^2$$
is composed of those divisible by p^2 (an element in both sequences will be accounted twice), and so on. Thus the first equality is proved. Notice that
$$\left\lfloor \frac{n}{p^j} \right\rfloor = a_j + a_{j+1}p + \cdots + a_t p^{t-j} = p^{-j}(a_j p^j + \cdots + a_t p^t).$$
Then $v_p(n!)$ is equal to
$$\sum_{j=1}^{t} p^{-j} \sum_{i=j}^{t} a_i p^i = \sum_{i=1}^{t} a_i p^i \sum_{j=1}^{i} p^{-j} = \frac{p^{-1}}{1-p^{-1}} \sum_{i=0}^{t} (1 - p^{-i}) a_i p^i = \frac{n - s_p(n)}{p-1}.$$
□

4.7. **Mahler expansion.** Continuous functions on $\mathbb{Z}_p$ taking values in $\mathbb{Q}_p$ are described by the following theorem.

Theorem 10. *Any $f \in C(\mathbb{Z}_p \to \mathbb{Q}_p)$ is uniquely expanded as*
$$f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}$$
where
$$a_n = \triangle^n f(0) = \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} f(j).$$

Proof. Recall that $Tf(x) = f(x+1)$, $\triangle f(x) = f(x+1) - f(x)$. Thus $\triangle = T - I$. Then

$$\triangle^n = (T-I)^n = \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} T^j.$$

Since $f \in C(\mathbb{Z}_p \to \mathbb{Q}_p)$ is uniformly continuous, we have $\lim \omega_n(f) = 0$ where

$$\omega_n(f) := \sup_{|x-y|_p \le p^{-n}} |f(x) - f(y)|_p.$$

For $x \in \mathbb{Z}_p$, we have

$$\Delta^n f(x) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} [f(x+k) - f(x)]$$

(Notice that the sum of coefficients equals to zero because of $(1-1)^n = 0$). For $0 \le k \le p^n$ we have $|\binom{p^n}{k}|_p = p^{-n+v_p(k)}$ (Exercise, try by Legendre formula) so that

$$\left\| \Delta^{p^n} f \right\|_\infty \le \max_{0 \le s \le n} p^{-n+s} \omega_s(f) \to 0.$$

Then $\Delta^n f$ converges uniformly to zero (using $\|\Delta g\|_\infty \le \|g\|_\infty$) so that

$$a_n := \Delta^n f(0) \to 0.$$

On the other hand,

$$\forall x \in \mathbb{N}, \quad f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n}.$$

(it is a finite sum). We finish the proof by using the fact that $\mathbb{N}$ is dense in $\mathbb{Z}_p$. □

5. p-ADIC ANALYSIS

5.1. **Sequence, Series, Continuity, Derivative.** $(\mathbb{Q}_p, |\cdot|_p)$ is a complete normed field. Notions like limit of a sequence, convergence of a series and continuity of a function are "classical". The ultra-metric inequality makes things simpler in p-adic world, and sometimes different.

A sequence $(a_n) \subset \mathbb{Q}_p$ is a Cauchy sequence iff $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. A series $\sum_{n=1}^{\infty} a_n$ converges iff $\lim_{n\to\infty} a_n = 0$. Cauchy-Hadamard formula holds for Taylor series $\sum_{n=0}^{\infty} a_n x^n$.

The *derivative* is defined formally as usual:

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}.$$

But the space C^1 of continuously differentiable function is not a "good" space.

(1) Locally constant functions admits zero derivatives. There are even injective maps having zero derivative: $f(x) = \sum_{n=0}^{\infty} x_n p^{2n}$ for $x = \sum_{n=0}^{\infty} x_n p^n \in \mathbb{Z}_p$. We have $|f(x) - f(y)|_p = |x-y|_p^2$.

(2) The mean value theorem doesn't holds in $C^1(\mathbb{Z}_p \to \mathbb{Q}_p)$:

$$f(x) - f(y) = f'(\xi)(x-y) \quad (\text{for some } \xi \text{ between } x \text{ and } y)$$

[Between means $\xi = tx + (1-t)y$ with $|t|_p \le 1$].

5.2. **Strict differentiability.** We define a stronger differentiability. Let $f : U \to \mathbb{Q}_p$ be defined on an open set and $a \in U$. We say f is *strictly differentiable* at a if the limit exists:

$$f'(a) = \lim_{(x,y)\to(a,a),x\neq y} \frac{f(x) - f(y)}{x - y}.$$

We denote by $C^1_s(U \to \mathbb{Q}_p) \subset C^1(U \to \mathbb{Q}_p$ the space of all functions defined and strictly differentiable in U taking values in $\mathbb{Q}_p$.

We remark that

(1) $C^1_s(U \to \mathbb{Q}_p) \subset C^1(U \to \mathbb{Q}_p$ (strict inclusion).
(2) $f \in C^1_s(U \to \mathbb{Q}_p)$ iff there exists $R \in C(U \times U \to \mathbb{Q}_p)$ such that
$$f(x) - f(y) = (x - y)R(x, y).$$
Then we must have $R(a, a) = f'(a)$.
(3) $Lip_{1+\delta}(U \to \mathbb{Q}_p) \subset C^1_s(U \to \mathbb{Q}_p)$.
(4) analytic functions are strictly differentiable.

Theorem 11 (local injectivity)**.** *Let $f \in C^1_s(U \to \mathbb{Q}_p)$ and $a \in U$. Suppose $f'(a) \neq 0$, then there is an neighborhood V of a such that*

$$\forall x, y \in V, \quad |f(x) - f(y)|_p = |f'(a)|_p|x - y|_p.$$

Proof. Directly from the definition and the fact $f'(a) \neq 0$. For x and y close to a, we have

$$\left|\frac{f(x) - f(y)}{x - y} - f'(a)\right|_p < |f'(a)|_p.$$

□

As an example, let us examine the differentiability of the shift σ_p. The shift map σ_p is derivable and even strictly derivable and

$$\sigma'_p(x) = \frac{1}{p}$$

In fact, the shift σ_p is locally affine:

$$\sigma_p(x) = \sum_{j=0}^{p-1} \left(\frac{x}{p} - \frac{j}{p}\right) 1_{[j]}(x).$$

The differentiability follows immediately. So does the strict differentiability, because when $|x - y| \leq p^{-1}$ we have

$$\sigma_p(x) - \sigma_p(y) = \frac{x - y}{p}.$$

But σ_p is not analytic at 0.

5.3. **Newton Approximation and Local invertibility.**

Theorem 12 (Newton Approximation)**.** *Let $f : B_r(a) \to \mathbb{Q}_p$. Suppose there exists $s \in \mathbb{Q}_p$ such that*

$$\sup_{x,y\in B_r(a);x\neq y} \left|\frac{f(x) - f(y)}{x - y} - s\right|_p < |s|_p.$$

Then $s^{-s}f$ is an isometry, which maps any ball $B_{r'}(b)$ onto $B_{|s|_p r'}(f(b))$, where $r' \leq r$.

Proof. The condition implies

$$|f(x) - f(y)|_p = |s||x - y|_p.$$

Then the isometry follows. Consequently

$$f(B_{r'}(b)) \subset B_{|s|_p r'}(f(b)).$$

For $c \in f(B_{r'}(b))$, we shall find a zero of $f(x) - c$ in $B_{r'}(b)$ by the Newton method: let

$$g(x) = x - s^{-1}(f(x) - c).$$

Actually $g : B_{r'}(b) \to B_{r'}(b)$ is an contraction and admits a fixed point. □

In particular, if f is strictly differentiable and $f'(a) \neq 0$, then we can locally inverse the mapping f.

Theorem 13 (Local invertibility)**.** *Let $f : B_r(a) \to \mathbb{Q}_p$ be strictly differentiable. Suppose $f'(a) \neq 0$. Then for sufficiently small r', $f : B_{r'}(a) \to B_{|f'(a)|_p r'}(f(a))$ is a diffeomorphism and*

$$(f^{-1})'(f(a)) = (f'(a))^{-1}.$$

Proof. Apply the above lemma with $s = f'(a)$. $g := f^{-1}$ is a scalar multiple of an isometry and it is then continuous. For $z, w \in B_{|f'(a)|_p r}(f(a))$, we have

$$\frac{g(z) - g(w)}{z - w} = \left(\frac{f(g(z)) - f(g(w))}{g(z) - g(w)} \right)^{-1}.$$

It follows the strict differentiability of g at $f(a)$. □

5.4. **Analytic functions, exponential and logarithmic functions.** As usual, a function f defined in a disk D is *analytic* if there exists $u \in D$ such that

$$f(x) = \sum_{n=0}^{\infty} a_n (x - u)^n, \forall x \in D.$$

A function f defined in an open set U is *locally analytic function* if for any $a \in U$, f is analytic in a disk containing a.

Theorem 14 (non analytic continuation by power series)**.** *If f is analytic in a disk D, then for any $v \in D$, $f(x)$ is equal to some power series $\sum_{n=0}^{\infty} b_n (x - v)^n$ around v for all $x \in D$.*

Let us make the following remarks:

(1) If $f(x) = \sum_{n=0}^{\infty} a_n (x - u)^n, \forall x \in D$, then $a_n n! = f^{(n)}(u)$.
(2) The zeros of an analytic function don't have accumulation points.
(3) Composition of analytic functions are not necessarily analytic. Counter example: $f(x) = x^p - x$ is analytic in $\mathbb{Z}_p$ taking values in $p\mathbb{Z}_p$ and $g(x) = (1 - x)^{-1}$ is analytic in $p\mathbb{Z}_p$. But $g \circ f$ is not analytic in $\mathbb{Z}_p$.
(4) Composition is stable for locally analytic functions.

The *exponential function* on $\mathbb{Q}_p$ is defined formally as usual:

$$\exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

A big difference from usual analysis is that the p-adic exponential function is not defined on the whole space $\mathbb{Q}_p$. Let us recall the Legendre formula, which is useful to

determine the domain of convergence of the series defining the exponential function. Let $s_p(n)$ be the sum of p-adic digits of n. Then

$$v_p(n!) = \sum_{j=0}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - s_p(n)}{p-1}.$$

Here are some properties of the exponential function:

- Domain of convergence: $E = \{x : |x|_p < p^{-1/(p-1)} < 1\}$.
- $E = p\mathbb{Z}_p$ for $p \neq 2$ $(1/p < 1/(p-1) < 1)$;
  $E = 4\mathbb{Z}_2$ for $p = 2$ $(1/(p-1) = 1$, divergence at $x = 2)$.
- $\exp(x+y) = \exp x \exp y \quad (\forall x, y \in E)$.
- $(\exp x)' = \exp x$.
- $|\exp x - 1|_p < 1$. The image of E under exp is $1 + E$.

The *Logarithm function* on $\mathbb{Q}_p$ is defined formally as usual:

$$\log x = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}.$$

The estimate $v_p(n) = O(\log n)$ (or for $p^{v_p(n)} \leq n$) is useful to determine the domain of convergence of the series defining the logarithmic function.

Here are some properties of the logarithmic function:

- Domain of convergence: $L = \{x : |x-1|_p < 1\} = 1 + p\mathbb{Z}_p$.
- $\log(xy) = \log x + \log y \quad (\forall x, y \in L)$.
- $(\log x)' = 1/x$.
- $\forall x \in 1 + E$, $|\log x|_p < p^{-1/(p-1)}$.
  The image of $1 + E$ under $\log x$ is E.
- $\log \exp x = x$ $(\forall x \in E)$; $\exp \log y = y$ $(\forall y \in 1 + E)$.
- exp and log are isometries, respectively on E and $1 + E$.

5.5. **Hensel lemma.** Hensel lemma is a very useful tool for finding zeros of an analytic or polynomial function.

Theorem 15 (Hensel Lemma)**.** *Let f be analytic in $\mathbb{Z}_p$, given by*

$$f(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Suppose that

$$|a_n|_p \leq 1, \quad |f(a)|_p < 1, \quad |f'(a)|_p = 1$$

for some $a \in \mathbb{Z}_p$. Then f admits a (unique) zero $b \in \mathbb{Z}_p$ such that $|b-a|_p \leq |f(a)|_p$.

Proof. Assume $r := |f(a)|_p > 0$ (otherwise, $b = 0$). We shall apply the lemma of Newton approximation to $f|_{B_r(a)}$ and $s = f'(a)$. First develop f at a: $f(x) = \sum_{n=0}^{\infty} b_n (x-a)^n$ $(|x|_p \leq 1)$. Observe that $b_0 = f(a)$, $b_1 = f'(a)$, $|b_n|_p \leq 1$. Then for $x, y \in B_r(a)$ with $x \neq y$,

$$\left| \frac{f(x) - f(y)}{x - y} - f'(a) \right|_p = \left| \sum_{n=2}^{\infty} b_n \frac{(x-a)^n - (y-a)^n}{x-y} \right|_p.$$

Let $u = x - a$ and $v = x - b$. We have $u \neq v$, $|u|_p \leq r$, $|v|_p \leq r$.

The last sum is then bounded by

$$\sup_{n\geq 2}\frac{|u^n-v^n|_p}{|u_v|_p}\leq \sup_{n\geq 2} r^{n-1}=r=|f(a)|_p<1=|f'(a)|_p.$$

The Newton Approximation lemma shows that $f: B_r(a)\to B_r(f(a))$ is surjective. But $0\in B_r(f(a))$. So there is a $b\in B_r(a)$ such that $f(b)=0$. □

Theorem 16 (Hensel lemma for polynomials)**.** *Let $P\in\mathbb{Z}_p[x]$. Suppose there exists $\beta\in\mathbb{Z}_p$ such that*

$$P(\beta)=0\ (\mod p),\quad P'(\beta)\neq 0\ (\mod p).$$

Then there exists a unique $\alpha\in\mathbb{Z}_p$ such that

$$\alpha=\beta\ (\mod p),\quad P(\alpha)=0.$$

5.6. **Integration and Antiderivative.** There is no Newton-Leibniz formula for the p-adic analysis. There is no $\mathbb{Q}_p$-valued Lebesgue measure. $\int f(x)dx$ is not well defined as usual.

We say that f is an antiderivative of f' if f' exists. If f admits an antiderivative F, so is $F+g$ for every locally constant g.

Theorem 17 (Dieudonné)**.** *Each $f\in C(\mathbb{Z}_p\to\mathbb{Q}_p)$ admits an antiderivative.*

Theorem 18 (No Lebesgue measure)**.** *Additive, translation invariant and bounded $\mathbb{Q}_p$-valued measure μ on clopens of $\mathbb{Z}_p$ is the zero measure.*

Proof. For each n, $\mathbb{Z}_p$ is the disjoint union of $a+p^n\mathbb{Z}_p$ $(0\leq a<p^n)$. Then we get $\mu(\mathbb{Z}_p)=p^n\mu(p^n\mathbb{Z}_p)$. The boundedness implies

$$\mu(\mathbb{Z}_p)=\lim_n p^n\mu(p^n\mathbb{Z}_p)=0.$$

Thus $\mu(a+p^n\mathbb{Z}_p)=\mu(p^n\mathbb{Z}_p)=p^{-n}\mu(\mathbb{Z}_p)=0$. □

Here is a version of p-adic Riesz representation. This can be generalized to compact ultrametric spaces.

Let $X\subset\mathbb{Q}_p$ be compact. Let $\mathcal{A}=\mathcal{A}(X)$ be the set of all *clopens* of X.

An *integral* on $C(X\to\mathbb{Q}_p)$ is by definition a continuous linear functional on $C(X\to\mathbb{Q}_p)$, i.e. an element of $C(X\to\mathbb{Q}_p)'$. A *measure* is by definition a function $\mu:\mathcal{A}\to\mathbb{Q}_p$ which is finitely additive, and bounded in the sense

$$\|\mu\|=\sup_{K\in\mathcal{A}}|\mu(K)|_p<\infty.$$

Let $M(X\to\mathbb{Q}_p)$ denote the set of measures.

Theorem 19 (p-adic Riesz representation)**.** *The $C(X\to\mathbb{Q}_p)'$ of integrals is isometrically isomorphic to the space $M(X\to\mathbb{Q}_p)$ of measures. The isomorphism $\phi\mapsto\mu_\phi$ is defined by*

$$\mu_\phi(K)=\mu(1_K).$$

The so-called Volkenborn integral is a different integral. It is a functional on $C^1_s(\mathbb{Z}_p\to\mathbb{Q}_p)$ but not on $C(\mathbb{Z}_p\to\mathbb{Q}_p)$.

Let us first recall the following general principle of interpolation. Any uniformly continuous map from $\mathbb{N}$ to $\mathbb{Q}_p$ uniquely extends to a continuous function in $C(\mathbb{Z}_p\to\mathbb{Q}_p)$.

Theorem 20. *Let $f \in C(\mathbb{Z}_p \to \mathbb{Q}_p)$ be a continuous function. The function defined on $\mathbb{N}$ by*

$$F(0) = 0, \quad F(n) = f(0) + f(1) + \cdots + f(n-1)$$

is uniformly continuous. The extended function is denoted by $Sf(x)$ (called indefinite sum of f). If f is strictly differentiable, so is Sf.

The *Volkenborn integral* of $f \in C^1_s(\mathbb{Z}_p \to \mathbb{Q}_p)$ is defined by the "Riemann sum"

$$\int_{\mathbb{Z}_p} f(x)dx = \lim_{n\to\infty} p^{-n} \sum_{j=0}^{p^n-1} f(j) = \lim_{n\to\infty} \frac{Sf(p^n) - Sf(0)}{p^n} = (Sf)'(0).$$

5.7. **Fourier Analysis.** Here we would like to present a Fourier analysis of functions defined in the field of p-adic numbers but taking values in the field of usual numbers. So it is a special case of commutative harmonic analysis. We need to know what are the group characters.

A *character* of the group $(\mathbb{Z}_P, +)$ is a continuous function $\gamma : \mathbb{Z}_p \to \mathbb{C}$ such that $|\gamma(z)| = 1$ for all $z \in$ and

$$\gamma(z_1 + z_2) = \gamma(z_1)\gamma(z_2) \qquad (z_1, z_2 \in \mathbb{Z}_p).$$

The set of all continuous characters, denoted by $\widehat{\mathbb{Z}}_p$, is a group for the usual pointwise multiplication.

Define

$$\gamma_{n,k}(z) := \exp(2i\pi\{\frac{k}{p^n}z\}), \quad (n \geqslant 1, p^n > k \geqslant 1, p \nmid k).$$

Theorem 21. $\widehat{\mathbb{Z}}_p = \{1\} \cup \{\gamma_{n,k}\}$.

Proof. Each $\gamma_{n,k}$ is a character because

- $\{x + y\} = \{x\} + \{y\} \pmod{\mathbb{Z}}$.
- $\mathbb{Z}_p \ni x \mapsto \mathbb{R}$ is locally constant then continuous.

Let $\gamma \in \widehat{\mathbb{Z}}_p$. We have $\gamma(1) = e^{2i\pi\theta}$ for some $\theta \in [0, 1)$ and $\gamma(p^n) = \gamma(1)^{p^n}$.

$$\gamma \text{ continuous}, p^m \to 0 \Rightarrow \lim_{m\to+\infty} \exp(2i\pi p^m\theta) = \lim_{m\to+\infty} \gamma(p^m) = \gamma(0) = 1.$$

Write $\theta = \sum_{j=1}^{+\infty} \frac{\theta_j}{p^j}$ $(0 \leqslant \theta_j < p)$.

$$\exp(2i\pi p^m\theta) \to 1 \Rightarrow \lim_{m\to\infty} \theta^m\theta = \lim_{m\to\infty} \sum_{j>m}^{+\infty} \frac{\theta_j}{p^{j-m}} = 0.$$

It follows that the digit θ_m ends with 0's. Write

$$\theta = 0 \text{ or } \theta = k/p^n \quad (p^n > k \geqslant 1, p \nmid k).$$

Now for any $z = \sum_{j=0}^{+\infty} z_j p^j \in \mathbb{Z}_p$, we have

$$\gamma(z) = \lim_{N\to+\infty} \gamma(\sum_{j=0}^{N} z_j p^j) = \lim_{N\to+\infty} \exp(2i\pi\theta \sum_{j=0}^{N} z_j p^j) = \exp(2i\pi\{\theta z\}).$$

Hence we have $\gamma = 1$ or $\gamma_{n,k}$. □

Then for any $f \in L^1(\lambda_p)$ where λ_p is the Haar measure of $\mathbb{Z}_p$, we have a *Fourier series*

$$f(x) \sim a_0 + \sum_{n,k} a_{n,k}\gamma_{n,k}(x).$$

6. p-ADIC REPELLERS

6.1. **Basic notions of dynamical systems.** Recall that a *dynamical system* is a couple (X,T) where $T: X \to X$. We assume that X is compact, T is continuous.

Here are some notions and notation:

- $O(x) := \{T^n x\}_{n\in\mathbb{N}}$ is an *orbit*;
- T is *transitive* if $\overline{O(x)} = X$ $(\exists x \in X)$;
- T is *minimal* if $\overline{O(x)} = X$ $(\forall x \in X)$;
- A probability measure μ is *invariant* if $\mu = \mu \circ T^{-1}$;
- T is *ergodic* w.r.t. μ if $\mu(A) = \mu(T^{-1}A)$ implies $\mu(A) = 0$ or 1;
- T is *uniquely ergodic* if $\exists$! invariant probability measure;
- T is *strictly ergodic* if "uniquely ergodic" + "minimal".

Theorem 22 (Birkhoff Theorem)**.** *Suppose (T,X,μ) is ergodic. Then for any $f \in L^1(\mu)$ we have*

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=0}^{n-1} f(T^k x) = \int f d\mu \quad \mu\text{-a.e. } x$$

Theorem 23 (Unique ergodicity)**.** *(X,T) is uniquely ergodic iff for any continuous function $g: X \to \mathbb{R}$,*

$$\frac{1}{n}\sum_{k=0}^{n-1} g(T^k x) \rightrightarrows \int g d\mu.$$

Recall that $T: X \to X$ is *equicontinuous* if

$$\forall \epsilon > 0, \exists \delta > 0 \ \text{ s. t. } \ d(T^n x, T^n y) < \epsilon \ (\forall n \geq 1, \forall d(x,y) < \delta).$$

Theorem 24 (Strict ergodicity)**.** *Suppose $T: X \to X$ be an equicontinuous transformation. Then the following statements are equivalent:*

(1) T is **minimal**.
(2) T is **uniquely ergodic**.
(3) T is **ergodic** *for any/some invariant measure with X as its support.*

There are many equicontinuous p-adic dynamics:

- 1-Lipschitz transformation is equicontinuous.
- Polynomial $f \in \mathbb{Z}_p[x] : \mathbb{Z}_p \to \mathbb{Z}_p$ is equicontinuous.

6.2. **Shift dynamics (an example and a model).** The full shift dynamics (Σ_m^+, T) is defined as follows. Let $m \geq 2$ be an integer. Let $\Sigma_m^+ = \{0,1,\cdots,m-1\}^{\mathbb{N}}$ be the space of sequences with distance defined by

$$d(x,y) = \sum_{n=0}^{\infty} \frac{|x_n - y_n|}{m^n}.$$

The shift $T: \Sigma_m^+ \to \Sigma_m^+$ is defined by

$$(x_n)_{n\geq 0} \mapsto (x_{n+1})_{n\geq 0}.$$

Properties of (Σ_m^+, T):

(1) T is not minimal, not unique ergodic.
(2) T is chaotic (sensitively depending on the initial points).
(3) There are many invariant measures, including Markov measures.

(4) Compare it with $f:[0,1)\to[0,1)$, $f(x)=2x \pmod 1$. $\frac{k}{2^n-1}$ is n-periodic:

$$\frac{3}{7}\to\frac{6}{7}\to\frac{5}{7}\to\frac{3}{7}.$$

(5) (Cantor) Σ_m^+ is compact, perfect, totally disconnected.
(6) (Density of periodic points) $\Sigma_m^+=\overline{\mathrm{Per}(T)}$.

$$\overline{x_1x_2\cdots x_n}=x_1x_2\cdots x_nx_1x_2\cdots x_n\cdots.$$

(7) (Transitivity) The orbit $\{T^nz\}_{n\geq 0}$ is dense for some z.

$$z=\text{concatenation of all words.}$$

(8) (Topological entropy) $h(T)=\log m$.
(9) A subset Λ of $\mathbb{N}$ corresponds to a point $x\in\Sigma_2^+$: $x=1_\Lambda(n)$.

A *subshit* X is a closed T-invariant subset (i.e. $TX\subset X$). Then (X,T) becomes a **subshift dynamics**. If $A=(a_{i,j})$ is a $m\times m$ matrix of entries $0,1$, then

$$\Sigma_A^+=\{x\in\Sigma_m^+:\forall n\geq 0, a_{x_n,x_{n+1}}=1\}$$

is a subshift, called a *subshift of finite type*.

(1) If $A^N>0$ for some $N\geq 1$, then $T:\Sigma_A^+\to\Sigma_A^+$ is transitive.
(2) There are $\mathrm{tr}(A^n)$ n-periodic points. In fact,

$$A^n_{i,j}=\mathrm{Card}\{i_0i_1\cdots i_n: i_0=i, i_n=j, a_{i_k,i_{k+1}}=1\}.$$

(3) If $A^N>0$ for some $N\geq 1$, then $h(T,X)=\log\rho(A)$. $\rho(A)$ is the spectral radius of A.
(4) (Gibbs measure) For any Hölder function $\phi:\Sigma_A\to\mathbb{R}$, there exists a unique invariant probability measure μ such that

$$\mu([x_0,x_1,\cdots,x_{n-1}])\approx\exp[\sum_{k=0}^{n-1}\phi(T^kx)-nP].$$

Look at an example: Fibonacci subshift Σ_A^+, where

$$A=\begin{pmatrix}1&1\\1&0\end{pmatrix}.$$

We have $uA=\rho u$, $Av=\rho v$ where

$$\rho=\frac{1+\sqrt{5}}{2},\quad u=v^t=(\rho^{-1},\rho^{-2}).$$

(1) (Parry measure) Maximal entropy measure is the Markov measure

$$\mu_{\max}([x_0x_1\cdots x_n])=\pi_{x_0}p_{x_0,x_1}\cdots p_{x_{n-1},x_n}$$

$$p_{i,j}=\frac{a_{i,j}u_j}{\rho u_i},\quad \pi_i=\frac{u_iv_i}{\sum_k u_kv_k}.$$

(2) (Frequency) For $\mu_{\max}$-a.e. x,

$$\lim_{n\to\infty}\frac{1}{n}\sum_{k=1}^n x_k=\pi_1=\frac{5-\sqrt{5}}{10}=0,27639...<\frac{1}{2}.$$

(3) (Entropy) $h(T,\Sigma_A^+)=\log\frac{1+\sqrt{5}}{2}$.

6.3. **p-adic Repellers.** Let us first recall the local rigidity: Let U be a clopen set and $a \in U$. Suppose

$$f : U \to \mathbb{Q}_p \text{ is analytic}, \quad f'(a) \neq 0.$$

Then there exists $r > 0$ such that $B_r(a) \subset U$ and

$$|f(x) - f(y)|_p = |f'(a)|_p |x - y|_p$$

$(\forall x, y \in B_r(a))$. Moreover, if $f(x) = \sum_{n=0}^{\infty} a_n (x-a)^n$, then we may take r to be the one satisfying

$$\max_{n \geq 2} |a_n| r^{n-1} < |f'(a)|_p.$$

Therefore for a fixed point a of f (i.e. $f(a) = a$). There are three configurations:
$|f'(a)|_p < 1$ (Attractive),
$|f'(a)|_p > 1$ (Repulsive),
$|f'(a)|_p = 1$ (Siegel disk).

Now we define our p-adic repellers $f : X \to \mathbb{Q}_p$ by the assumptions

- (Expansiveness): $X \subset \mathbb{Q}_p$ clopen, $f^{-1}(X) \subset X$;
- (Local rigidity): $X = \bigsqcup_{i \in I} B_{p^{-\tau}}(c_i)$, $\forall i \in I$, $\exists \tau_i \in \mathbb{Z}$

$$|f(x) - f(y)|_p = p^{\tau_i} |x - y|_p \qquad (\forall x, y \in B_{p^{-\tau}}(c_i)). \tag{3}$$

Then we define the *Julia set* of F by

$$J_f := \bigcap_{n=0}^{\infty} f^{-n}(X). \tag{4}$$

Theorem 25. *We have*

$$f^{-1}(J_f) = J_f, \quad f(J_f) \subset J_f.$$

(J_f, f) is conjugate to a subshift of finite type if f is transitive, $\tau_i \geq 0$ and at least one $\tau_i > 0$.

Sketch of Proof. For any $i \in I$, let

$$I_i := \{j \in I : B_j \cap f(B_i) \neq \emptyset\} = \{j \in I : B_j \subset f(B_i)\}.$$

Then define the incidence matrix $A = (A_{i,j})$ by

$$A_{i,j} = 1 \text{ iff } j \in I_i.$$

- $\forall i \in I$, $f : B_{p^{-\tau}}(c_i) \to B_{p^{-\tau+\tau_i}}(f(c_i))$ is a bijection.
- $\tau_i = 0 \Rightarrow \exists n \geq 1$ such that f is expanding on $f^n(B_{p^{-\tau}}(c_i))$.
- $(j_n)_{n \geq 0}$ is the coding of $x \in J_f$:

$$x \in B_{p^{-\tau}}(c_{j_0}), f(x) \in B_{p^{-\tau}}(c_{j_1}), \cdots, f^n(x) \in B_{p^{-\tau}}(c_{j_n}), \cdots$$

- $h(x) = (j_n)$ is the conjugacy map between J_f and Σ_A.

□

The following theorem provides many examples.

Theorem 26. *Let $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Q}_p[x]$, $a_n \neq 0$, $n \geq 2$. Then exists a compact open set X on which f is expansive and that $\lim_n |f^n(x)|_p = \infty$ for $x \notin X$.*

Sketch of Proof. $\exists \ell$ (so sufficiently large $|x|_p^{n-1}|a_n| \geq p$) such that if $|x|_p \geq p^\ell$ we have

$$|f(x)| = |x^n|_p \left|a_n + \frac{a_{n-1}}{x} + \cdots + \frac{a_0}{x^n}\right| = |x^n|_p |a_n| = |x|_p^{n-1}|a_n| \cdot |x|_p \geq p|x|_p$$

by the ultra-metric property

$$|x+y|_p \leq \max\{|x|_p, |y|_p\}.$$

Let $X = B_{p^\ell}(0)$. □

Remark that We should make the assumption: $f'(x) \neq 0$ on X. Then f will have the rigidity property on X.

Example 1. Let $f_{m,a}(x) = \frac{x^p - ax}{p^m}, \quad a \in \mathbb{Z}_p, |a|_p = 1, m \geq 1$. If $a = 1 \mod p$, (J_f, f) is conjugate to a full shift of p symbols, so its entropy is $\log p$. If $a \neq 1 \mod p$, $J_f = \{0\}$.

Proof. We have $|f'_m(x)|_p = p^m$. We have even

$$|f(x) - f(y)|_p = p^m |x-y|_p \forall x, y \in \mathbb{Z}_p, |x-y|_p < 1.$$

On the other hand, we have $|x^p - ax|_p \geq |x|_p$ for al $x \notin \mathbb{Z}_p$. So, we can restricted to $X = \mathbb{Z}_p$. Let

$$X_{m,a} = \bigsqcup_{k \in I_{m,a}} (k + p^m \mathbb{Z}_p)$$

where

$$I_{m,a} := \{0 \leq k \leq p^m - 1 : k^p - ak \equiv 0 \pmod{p^m}\}.$$

Other small balls will be mapped outside $\mathbb{Z}_p$.

If $a = 1 \pmod p$, $x^p - ax = 0$ has p solutions on $\mathbb{Z}_p$ (by Little Fermat theorem and Hensel lemma). Then $J_{m,a} \simeq \Sigma_p^+$.

If $a \neq 1 \pmod p$, then $I_{m,a} = \{0\}$ (Fermat) and $J_{m,a} = \{0\}$. For all $\forall x \notin J_{m,a}$, we have $\lim_{n\to\infty} |f^n(x)|_p = \infty$. □

We have used the following local isometry of $h(x) = x^p - ax$ with $|a|_p = 1$.

Lemma 27. *If $a \neq 1$, then for all $x, y \in \mathbb{Z}_p$ with $|x-y|_p < 1$ we have*

$$|h(x) - h(y)|_p = |x-y|_p.$$

Proof. The condition $|x-y|_p < 1$ means x, y are in a ball of radius p^{-1}. Let c $(0 \leq c < p)$ be a center of the ball. Let $x = c+u$ and $y = c+v$ ($|u|_p < 1$, $|v|_p < 1$). Write

$$h(x) - h(y) = (c+u)^p - (c+v)^p - a(u-v).$$

Then

$$h(x) - h(y) = \sum_{k=1}^{p} \binom{p}{k} c^{n-k}(u^k - v^k) - a(u-v).$$

Remark that for $1 \leq k \leq p$, $|\binom{p}{k}|_p = 1$ and $u^k - v^k$ contains a factor $u - v$ and the other factor is in $\mathbb{Z}_p$. Since $|a|_p = 1$, by the ultrametric triangle inequality we get

$$|h(x) - h(y)|_p = |u-v|_p| - a|_p = |x-y|_p.$$

Remark that for $p \geq 3$ and $n \geq 1$ an integer. If $|x|_p = |y|_p = 1$ and $|x-y|_p < 1$, we have

$$|x^n - y^n|_p = |n|_p |x-p|_p.$$

□

Example 2. Consider $f(x) = \frac{x(x-1)(x+1)}{2}, \quad x \in \mathbb{Q}_2$. *The Julia set* (J_f, f) is conjugate to the subshift of finite type defined by

$$A = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

The topological entropy of (J_f, f) is equal to $\log 1.6956...$

7. Lip_1-DYNAMICS

We can study the following class of dynamics :

- The class $\mathbb{Z}_p[x]$ of polynomials
$$f(x) = \sum_{j=0}^{n} a_j x^j.$$
- The class $\mathcal{A}(\mathbb{Z}_p)$ of analytic functions
$$f(x) = \sum_{j=0}^{\infty} a_j x(x-1)\cdots(x-j+1) \quad (a_j \in \mathbb{Z}_p.$$
- The class $\mathcal{L}_1(\mathbb{Z}_p)$ of 1-Lipschtz functions f i.e.
$$|f(x) - f(y)|_p \leq |x-y|_p$$
Or equivalently
$$f \text{ sends } \mathbb{Z}/p^n\mathbb{Z} \text{ into } \mathbb{Z}/p^n\mathbb{Z}.$$
We will denote this mapping by f_n, called n-reduction.

Notice that $\mathcal{A}(\mathbb{Z}_p)$ is closed under composition and we have

$$\mathbb{Z}_p[x] \subset \mathcal{A}(\mathbb{Z}_p) \subset \mathcal{L}_1(\mathbb{Z}_p).$$

The main question in which we are is as the following one. Let $f \in \mathcal{L}_1(\mathbb{Z}_p)$ and let E be a clopen set of $\mathbb{Z}_p$ or $\mathbb{Q}_p$. Suppose

$$f : E \to E.$$

When is $f : E \to E$ is minimal?

7.1. Ergodicity criterion.

Theorem 28 (Anashin, [2, 3])**.** *Let $f \in \mathcal{L}_1(\mathbb{Z}_p)$. Then f is ergodic iff all reductions $f_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ are transitive.*

Proof. The necessity is immediate because f_n is a factor. For the sufficiency, construct the following conjugacy between f and the odometer $x \mapsto x+1$: Fix $w \in \mathbb{Z}_p$. For any $z \in \mathbb{Z}_p$, the following limit

$$\varphi_w(z) = \lim_{\substack{\mathbb{Z} \ni n \to z \\ in\ \mathbb{Z}_p}} f^n(z)$$

exists. It is a required congugacy. □

The following are also true. That f is measure preserving iff all f_n are bijections; The theorem holds in the high dimension case, on open compact set in any local fields; The same holds for compatible dynamics on profinite groups.

7.2. **Behavior on $\mathbb{Z}_p$ of a general polynomial.** The behavior on $\mathbb{Z}_p$ of an arbitrary polynomial from $\mathbb{Z}_p[x]$ is clear, due to the following result. The notion of minimal decomposition reflects the common feature of integer-valued polynomial dynamics.

Theorem 29 (Fan-Liao, [17]). *Let $f \in \mathbb{Z}_p[x]$ be a polynomial. We have the following minimal decomposition*

$$\mathbb{Z}_p = A \sqcup B \sqcup C$$

- *A: the finite set of all periodic points*
- *B: at most countable union of minimal sets*
- *C: every point of C is attracted by A or B.*

This result is generalized to other analytic dynamics and rational dynamics [21, 18].

7.3. **Minimality on $\mathbb{Z}_p$.**

Theorem 30 (Anashin [3]). *Let $f(x) = \sum_{k=0}^{\infty} a_k \binom{x}{k}$ be a 1-Lip mapping on $\mathbb{Z}_2$. The dynamics $(\mathbb{Z}_p, f)$ is minimal iff the following conditions hold simultaneously:*

- $a_0 \not\equiv 0 \ (mod\ 2)$;
- $a_1 \equiv 1 \ (mod\ 4)$,
- $a_k \equiv 0 \ (mod\ 2^{\lfloor \log_2(i+1) \rfloor + 1})$, *($k \geq 2$)*

Similar conditions are sufficient for $p \geq 3$, but not necessary (Anashin). The Result for polynomials ($p = 2$) using Taylor coefficients is due to Larin (1995). Durand and Paccaut ([15]) obtained a necessary and sufficient condition for polynomials in $\mathbb{Z}_3$ to be minimal, using Taylor coefficients.

Theorem 31 (Larin [34]). *Let $f(x) = \sum a_k x^k \in \mathbb{Z}_2[x]$. Then $(\mathbb{Z}_2, f)$ is minimal iff*

(1) $a_0 \equiv 1 \ (mod\ 2)$;
(2) $a_1 \equiv 1 \ (mod\ 2)$;
(3) $2a_2 \equiv a_3 + a_5 + \cdots \ (mod\ 4)$;
(4) $a_2 + a_1 - 1 \equiv a_4 + a_6 + \cdots \ (mod\ 4)$.

Durand-Paccaut's result on $\mathbb{Z}_3$ is similarly stated.

For general quadratic polynomial on any $\mathbb{Z}_p$, there is a complete characterization (Larin, Knuth).

Theorem 32 (Larin [34], Knuth [33]). *Let $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}_p$. Then f is minimal iff*

(1) When $p \geq 5$,

$$a = 0(\bmod p), b = 1(\bmod p), c \neq 0(\bmod p).$$

(2) When $p = 3$,

$$a = 0(\bmod 3^2), b = 1(\bmod 3), c \neq 0(\bmod 3)$$

or

$$ac = 6(\bmod 3^2), b = 1(\bmod 3), c \neq 0(\bmod 3).$$

(3) When $p = 2$,

$$a = 0(\bmod 2), a + b = 1(\bmod 4), c \neq 0(\bmod 2).$$

7.4. **Affine dynamics.** Affine maps are of the form

$$T_{a,b}x = ax + b \quad (a, b \in \mathbb{Q}_p).$$

Assume $a, b \in \mathbb{Z}_p$. We get a dynamics $(\mathbb{Z}_p, T_{a,b})$.

Theorem 33 (Fan-Li-Yao-Zhou, [16])**.** *Suppose $a, b \in \mathbb{Z}_p$ and $p \geq 3$.*

(1) $T_{a,b}$ is ergodic on $\mathbb{Z}_p$ iff

$$a = 1 \ (\mod p), \quad b \neq 0 \ (\mod p).$$

(2) The space $\mathbb{Z}_p$ is decomposed into at most countable components, restricted on each of which $T_{a,b}$ is uniquely ergodic.

Proof. We give a short proof of (1), which is very specific to affine dynamics.

Necessity. Since $b\mathbb{Z}_p$ is T is $T_{a,b}$-invariant (for $a(bx) + b = b(ax + 1)$), we must have $|b|_p = 1$. If $a \not\equiv 1 \pmod p$, $a - 1$ would be invertible and then $T_{a,b}$ admits a fixed point $(a-1)^{-1}b$, contradiction.

Sufficiency. Assume $|b|_p = 1$. Then $T_{a,b}$ is conjugate to $T_{a,1}$:

$$T_{b,0} \circ T_{a,1}(x) = b(ax + 1) = a(bx) + b = T_{a,b} \circ T_{b,0}.$$

We can assume that $b = 1$. Write $T_a = T_{a,1}$. Define

$$\Phi_a(z) := \frac{a^z - 1}{a - 1} = \frac{\mathrm{Exp}(z\mathrm{Log}(a)) - 1}{a - 1}, \quad \Psi_a(z) := \frac{\mathrm{Log}(1 + (a - 1)z)}{\mathrm{Log}(a)}.$$

which are homeomorphisms from $\mathbb{Z}_p$ onto $\mathbb{Z}_p$ and one is the inverse of the other (to check). They realize a congugacy between T_a and T_1 (odometer):

$$T_a(\Phi_a(z)) = a\frac{a^z - 1}{a - 1} + 1 = \frac{a^{z+1} - 1}{a - 1} = \Phi_a(z + 1) = \Phi_a(T_1(z)).$$

□

We finish by making some remarks:

- The theorem holds for $p = 2$, but the condition $a = 1 \pmod p$ must be replaced by $a = 1 \pmod{2^2}$.
- The multiplication ax was studied by Coelho and Parry.
- Another proof uses Fourier series ([16]): Solutions of $f(T_{a,b}(x)) = f(x)$ are constants.
- A third method is to project on $\mathbb{Z}/p^n\mathbb{Z}$ and to study finite dynamics ([14]).
- The presented method is difficult to be adapted to other systems, polynomials of higher order, for example. But it shows that any minimal affine system is *analytically* conjugate to the odometer. We have the following commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\Psi_{a,b}} & \mathbb{Z}_p \\ {\scriptstyle T_{a,b}}\uparrow & & \uparrow{\scriptstyle T_{1,1}} \\ \mathbb{Z}_p & \xleftarrow[\Phi_{a,b}]{} & \mathbb{Z}_p \end{array}$$

We wonder if a polynomial is analytically conjugate to an odometer when the two systems are conjugate.

References

[1] V. S. Anashin, Uniformly distributed sequences of p-adic integers, *Diskret. Mat.*, 14 (2002) 3–64; translation in *Discrete Math. Appl.*, 12 (6) (2002), 527–590.

[2] V. S. Anashin, Uniformly distributed sequences of p-adic integers, II, *Available at http://arXiv.org/math.NT/0209407*.

[3] V. S. Anashin, Ergodic transformations in the space of p-adic integers, in *p-adic mathematical physics* ed. A. Y. Khrennikov, Z. Rakić and I. V. Volovich, AIP Conference Proceedings vol. 826, 2006, 3–24.

[4] V. S. Anashin and A. Khrennikov, Applied Algebraic Dynamics, de Gruyter Expositions in Mathematics. 49. Walter de Gruyter & Co., Berlin, 2009.

[5] D. K. Arrowsmith and F. Vivaldi, Some p-adic representations of the Smale horseshoe, *Phys. Lett. A*, 176 (1993), 292294.

[6] D. K. Arrowsmith and F. Vivaldi, Geometry of p-adic Siegel discs, *Physica D*, 71 (1994), 222236.

[7] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math.*, 490 (1997), 101–127.

[8] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly*, 107 (2000), 783–799.

[9] R. Benedetto, Fatou components in p-adic dynamics, *PhD thesis*, Brown University, 1998.

[10] P. J. Cahen and J. L. Chabert, *Integer-valued polynomials*, Mathematical Survey and Monographs, vol. 48, *American Mathematical Society*, Providence, 1997.

[11] J. L. Chabert, A. H. Fan and Y. Fares, Minimal dynamical systems on a discrete valuation domain, DCDS, 2009.

[12] A. Chambert-Loir, Mesures et équidistribution sur les espaces de Berkovich, *J. Reine Angew. Math.*, 595 (2006), 215–235.

[13] Z. Coelho and W. Parry, Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers, in *Topology, Ergodic Theory, Real Algebraic Geometry*, Amer. Math. Soc. Transl. Ser. 2, no. 202, American Mathematical Society, Providence, (2001), 51–70.

[14] 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.

[15] F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic integers, *Bull. Lond. Math. Soc.*, 41(2):302–314, 2009.

[16] A. H. Fan, M. T. Li, J. Y. Yao and D. Zhou, Strict ergodicity of affine p-adic dynamical systems on $\mathbb{Z}_p$, *Adv. Math.*, 214 (2007), 666-700. See also A. H. Fan, M. T. Li, J. Y. Yao et D. Zhou, p-adic affine dynamical systems and applications, *C. R. Acad. Sci. Paris*, Ser. I 342 (2006), 129–134.

[17] A. H. Fan and L. M. Liao, On minimal decomposition of p-adic polynomial dynamical systems, *Adv. Math.*, 228:2116–2144, 2011.

[18] On minimal decomposition of p-adic rational functions with good reduction, preprint 2015.

[19] A.H. Fan, S. L. Fan, L. M. Liao, and Y. F. Wang, On minimal decomposition of p-adic homographic dynamical systems, *Adv. Math.*, 257:92–135, 2014.

[20] A. H. Fan, L. M. Liao, Y. F. Wang and D. Zhou, p-adic repellers in $\mathbb{Q}_p$ are subshifts of finite type , *C. R. Acad. Sci. Paris*, 344 (4) (2007), 219–224.

[21] S. L. Fan and L. M. Liao, Dynamics of convergent power series on the integral ring of a finite extension of $\mathbb{Q}_p$, *J. Differential Equations*, 259(4):1628–1648, 2015.

[22] S. L. Fan and L. M. Liao, Dynamics of the square mapping on the ring of p-adic integers, To appear in Pro. American Math. Society, 2015.

[23] C. Favre and J. Rivera-Letelier, Théorème d'équidistribution de Brolin en dynamique p-adique, *C. R. Math. Acad. Sci. Paris*, 339 (4) (2004), 271–276.

[24] C. Favre and J. Rivera-Letelier, Équidistribution quantitative des points de petite hauteur sur la droite projective, *Math. Ann.*, 335 (2) (2006), 311–361.

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

[26] M. R. Herman and J. C. Yoccoz, Generalization of some theorem of small divisors to non-archimedean fields. In: *Geometric Dynamics*, LNM 1007, Springer-Verlag (1983), 408-447.

[27] L. Hsia, Closure of periodic points over a non-Archimedean field, *J. London Math. Soc.*, 62 (3)(2000), 685–700.

[28] R. Jones, Galois Martingales and the hyperbolic subset of the p-adic Mandelbrot set, *PhD thesis*, Brown University, 2005.
[29] Y. Katznelson, Ergodic automorphisms of T^n are Bernoulli shifts, *Israel J. Math.*, 10 (1971), 186–195.
[30] A. Khrennikov, *Non-Archimedean Analysis: Quantum Paradoxes, Dynamical Systems and Biological Models*, Kluwer, Dordrecht, 1997.
[31] A. Khrennikov and M. Nilsson, On the number of cycles of p-adic dynamical systems, *J. Number Th.*, 90 (2) (2001), 255–264.
[32] A. Yu. Khrennikov and M. Nilsson, *p-adic deterministic and random dynamics*, Kluver Academic Publ., Dordrecht, 2004.
[33] D. Knuth, *The art of computer programming*, vol. 2, Seminumerical algorithms, Addison-Wesley, Third edition, 1998.
[34] M. V. Larin, Transitive polynomial transformations of residue class rings, *Discrete Mathematics and Applications*, 12(2) (2002), 141–154.
[35] H. C. Li, p-adic dynamical systems and formal groups, *Compositio Math.*, 104, no. 1 (1996), 41–54.
[36] D. A. Lind, The structure of skew products with ergodic group automorphisms, *Israel J. Math.*, 28 (3) (1977), 205–248.
[37] D. Lind and K. Schmidt, Bernoullicity of solenoidal automorphisms and global fields, *Israel J. Math.*, 87 no. 1-3 (1994), 33–35.
[38] D. A. Lind and T. Ward, Automorphisms of solenoids and p-adic entropy, *Erg. Th. Dynam. Syst.*, 8(3) (1988), 411-419.
[39] K-O. Lindahl, On Siegel's linearization theorem for fields of prime characteristic, *Nonlinearity*, 17 (2004), 745-763.
[40] J. Lubin, Non-Archimedean dynamical systems, *Compositio Mathematica*, 94 (1994), 321–346.
[41] J. M. Luck, P. Moussa and M. Waldschmidt (editors), *Number theory and physics*, No 47 in Springer Proceeding in Physics, Berlin, Springer-Verlag, 1990.
[42] K. Mahler, *p-adic Numbers and their Functions*, Cambridge Tracts in Mathematics, vol. 76., Cambridge University Press, 1980.
[43] P. Morton and J. Silverman, Periodic points, multiplicities and dynamical units, *J. Reine Angew. Math.*, 461 (1995), 81–122.
[44] R. Oselies and H. Zieschang, Ergodische Eigenschaften der Automorphismen p-adischer Zahlen, *Arch. Math.*, 26 (1975), 144–153.
[45] T. Pezda, Polynomial cycles in certain local domains, *Acta Arithmetica*, vol. LXVI (1994), 11–22.
[46] J. Rivera-Letelier, Dynamique des fonctions rationnelles sur des corps locaux, Geometric methods in dynamics. II. *Astérisque* No. 287 (2003), xv, 147–230.
[47] A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics 198, Springer-Verlag, New York, 2000.
[48] W. H. Schikhof, *Ultrametric calculus*, Cambridge University Press, 1984.
[49] J. Silverman, *The Arithmetic of Dynamical Systems*, Springer-Verlag, 2007.
[50] V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov, *p-adic Analysis and Mathematical Physics*, Series on Soviet and East European Mathematics, Vol. 1, World Scientific Co., Inc. 1994.
[51] C. F. Woodcock and N. P. Smart, p-adic chaos and random number generation, *Experiment Math.*, (1998), 333–342.

Laboratoire Amiénois de Mathématiques Fondamentales et Appliquées, CNRS-UMR 7352, Université de Picardie Jules Verne, 33 rue Saint Leu, 80039 Amiens cedex 1, France.

E-mail address: ai-hua.fan@u-picardie.fr