Minimality of affine polynomials on a finite extension of the field of p-adic numbers

Lingmin LIAO

Université Paris-Est Créteil (University Paris 12)

The University of Warwick, April 2012

Outline

1. The field $\mathbb{Q}_p$ of p-adic numbers and p-adic dynamical systems
2. Affine polynomial dynamical systems in $\mathbb{Q}_p$
3. Finite extensions of p-adic number field
4. Affine polynomial dynamical systems in finite extensions of $\mathbb{Q}_p$

The field $\mathbb{Q}_p$ of p-adic numbers and p-adic dynamical systems

I. The p-adic numbers

- $p \geq 2$ a prime number
- $\forall n \in \mathbb{N}$, $n = \sum_{i=0}^{N} a_i p^i \quad (a_i = 0, 1, \cdots, p-1)$
- Ring $\mathbb{Z}_p$ of p-adic integers :

$$\mathbb{Z}_p \ni x = \sum_{i=0}^{\infty} a_i p^i.$$

- Field $\mathbb{Q}_p$ of p-adic numbers : fraction field of $\mathbb{Z}_p$.

$$\mathbb{Q}_p \ni x = \sum_{i=v(x)}^{\infty} a_i p^i, \quad (\exists v(x) \in \mathbb{Z}).$$

II. Topology of $\mathbb{Q}_p$

- p-adic norm of $x \in \mathbb{Q}$

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

- $|x|_p$ is a **non-Archimidean** norm :

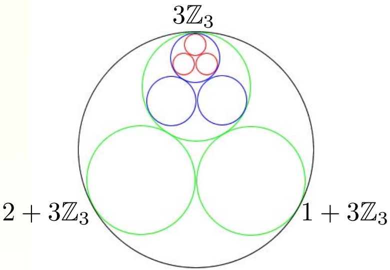
$$|-x|_p = |x|_p$$
$$|xy|_p = |x|_p |y|_p$$
$$|x+y|_p \le \max\{|x|_p, |y|_p\}$$

- $\mathbb{Q}_p$ is the $|\cdot|_p$**-completion** of $\mathbb{Q}$ ($\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\} = \overline{\mathbb{N}}$)

Development of numbers :

- $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R}([-1,1]) \to \mathbb{C}$
- $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}_p(\mathbb{Z}_p) \to \mathbb{Q}_p^{a.c.} \to \mathbb{C}_p$

Geometric representation of $\mathbb{Z}_3$



III. Arithmetic in $\mathbb{Q}_p$

Addition and multiplication : similar to the decimal way.
"**Carrying**" **from left to right**.

Example : $x = (p-1) + (p-1) \times p + (p-1) \times p^2 + \cdots$, then $x + 1 = 0$.
So,

$$-1 = (p-1) + (p-1) \times p + (p-1) \times p^2 + \cdots .$$

IV. Equicontinuous dynamics

- $T : X \to X$ 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

Let X be a compact metric space and $T : X \to X$ 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.

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

Theorem : If the continuous transformation T is uniquely ergodic (μ is the unique invariant probability measure), then for any continuous function $g : X \to \mathbb{R}$, uniformly,

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

V. Study on p-adic dynamical dystems

- Oselies, Zieschang 1975 : automorphisms of the ring of p-adic integers
- Herman, Yoccoz 1983 : complex p-adic dynamical systems
- Volovich 1987 : p-adic string theory by applying p-adic numbers
- Thiran, Verstegen, Weyers 1989 Chaotic p-adic quadratic polynomials
- Lubin 1994 : iteration of analytic p-adic maps.
- Anashin 1994 : 1-Lipschitz transformation (Mahler series)
- Coelho, Parry 2001 : ax and distribution of Fibonacci numbers
- Gundlach, Khrennikov, Lindahl 2001 : x^n
- $\cdots\cdots$

Affine polynomial dynamical systems on $\mathbb{Z}_p$

I. Polynomial dynamical systems on $\mathbb{Z}_p$

- Let $f \in \mathbb{Z}_p[x]$ be a polynomial with coefficients in $\mathbb{Z}_p$.
- Polynomial dynamical systems : $f : \mathbb{Z}_p \to \mathbb{Z}_p$, noted as $(\mathbb{Z}_p, f)$.

Theorem (Ai-Hua Fan, L 2011) minimal decomposition

Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. The space $\mathbb{Z}_p$ can be decomposed into three parts :

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

where

- A is the finite set consisting of all periodic orbits ;
- $B := \sqcup_{i \in I} B_i$ (I finite or countable)
  $\to$ B_i : finite union of balls,
  $\to$ $f : B_i \to B_i$ is minimal ;
- C is attracted into $A \sqcup B$.

II. Affine polynomials on $\mathbb{Z}_p$

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

$$\mathbb{U} = \{z \in \mathbb{Z}_p : |z| = 1\}, \quad \mathbb{V} = \{z \in \mathbb{U} : \exists m \geq 1, \text{s.t. } z^m = 1\}.$$

Easy cases :

1. $a \in \mathbb{Z}_p \setminus \mathbb{U} \quad \Rightarrow$ one attracting fixed point $b/(1-a)$.
2. $a = 1, b = 0 \;\Rightarrow$ every point is fixed.
3. $a \in \mathbb{V} \setminus \{1\} \;\Rightarrow$ every point is on a ℓ-periodic orbit, with ℓ the smallest integer $\geqslant 1$ such that $a^\ell = 1$.

Theorem (AH. Fan, MT. Li, JY. Yao, D. Zhou 2007) Case $p \geq 3$:

4. $a \in (\mathbb{U} \setminus \mathbb{V}) \cup \{1\},\; v_p(b) < v_p(1-a) \;\Rightarrow p^{v_p(b)}$ minimal parts.
5. $a \in \mathbb{U} \setminus \mathbb{V},\; v_p(b) \geq v_p(1-a) \Rightarrow (\mathbb{Z}_p, T_{a,b})$ is conjugate to $(\mathbb{Z}_p, ax)$.

   Decomposition : $\mathbb{Z}_p = \{0\} \sqcup \sqcup_{n \geq 1} p^n \mathbb{U}$.

   (1) One fixed point $\{0\}$.

   (2) All $(p^n\mathbb{U}, ax)(n \geq 0)$ are conjugate to $(\mathbb{U}, ax)$.

   For $(\mathbb{U}, T_{a,0})$: $p^{v_p(a^\ell - 1) - 1}$ minimal parts, with ℓ the smallest integer $\geqslant 1$ such that $a^\ell \equiv 1 (\text{mod } p)$.

Theorem (Fan-Li-Yao-Zhou 2007) Case $p = 2$:

4. $a \in (\mathbb{U} \setminus \mathbb{V}) \cup \{1\},\ v_p(b) < v_p(1-a)$.
   - $v_p(b) = 0 \Rightarrow p^{v_p(a+1)-1}$ minimal parts.
   - $v_p(b) > 0 \Rightarrow p^{v_p(b)}$ minimal parts.
5. $a \in \mathbb{U} \setminus \mathbb{V},\ v_p(b) \geq v_p(1-a)$

   $\Rightarrow (\mathbb{Z}_p, T_{a,b})$ is conjugate to $(\mathbb{Z}_p, ax)$.

   Decomposition : $\mathbb{Z}_p = \{0\} \sqcup \sqcup_{n \geq 1} p^n \mathbb{U}$.

   (1) One fixed point $\{0\}$.

   (2) All $(p^n\mathbb{U}, ax)(n \geq 0)$ are conjugate to $(\mathbb{U}, ax)$.

   For $(\mathbb{U}, T_{a,0})$: $p^{v_p(a-1)-1} \cdot p^{v_p(a+1)-1}$ minimal parts.

Remark : For the case $p = 2$, all minimal parts (except for the periodic orbits) are conjugate to $(\mathbb{Z}_2, x+1)$.

III. An application

Distribution of recurrence sequence.

Corollary (Fan-Li-Yao-Zhou 2007)

Let $k \geqslant 1$ be an integer, and let a, b, c be three integers in $\mathbb{Z}$ coprime with $p \geqslant 2$. Let s_k be the least integer $\geqslant 1$ such that $a^{s_k} \equiv 1 \pmod{p^k}$.

(a) If $b \not\equiv a^j c \pmod{p^k}$ for all integers j $(0 \leqslant j < s_k)$, then $p^k \nmid (a^n c - b)$, for any integer $n \geqslant 0$.

(b) If $b \equiv a^j c \pmod{p^k}$ for some integer j $(0 \leqslant j < s_k)$, then we have

$$\lim_{N \to +\infty} \frac{1}{N} \mathrm{Card}\{1 \leqslant n < N : p^k \mid (a^n c - b)\} = \frac{1}{s_k}.$$

One motivation :

Coelho and Parry 2001 : Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers.

Finite extensions of p-adic number field

I. Notations

- K is a finite extension of $\mathbb{Q}_p$.
- Still denote by $|\cdot|_p$ the extended absolute value of K.
- Degree : $n = [K : \mathbb{Q}_p]$. Ramification index : e
- Valuation function : $v_p(x) := -\log_p(|x|_p)$. $\mathrm{Im}(v_p) = \frac{1}{e}\mathbb{Z}$.
- $\mathcal{O}_K := \{x \in K : |x|_p \leq 1\}$: the local ring of K,
  $\mathcal{P}_K := \{x \in K : |x|_p < 1\}$: its maximal ideal.
- Residual field : $\mathbb{K} = \mathcal{O}_K/\mathcal{P}_K$. Then $\mathbb{K} = \mathbb{F}_{p^f}$, with $f = n/e$.

Example : For $\mathbb{Q}_p(\sqrt{p})$ $(p \geq 3)$:

$$n = 2, e = 2, f = 1.$$

II. Uniformizer and representation

An element $\pi \in K$ is a uniformizer if $v_p(\pi) = 1/e$.

Define $v_\pi(x) := e \cdot v_p(x)$ for $x \in K$. Then $\mathrm{Im}(v_\pi) = \mathbb{Z}$, and $v_\pi(\pi) = 1$.

Let $C = \{c_0, c_1, \ldots, c_{p^f-1}\}$ be a fixed complete set of representatives of the cosets of $\mathcal{P}_K$ in $\mathcal{O}_K$. Then every $x \in K$ has a unique π-adic expansion of the form

$$x = \sum_{i=i_0}^{\infty} a_i \pi^i,$$

where $i_0 \in \mathbb{Z}$ and $a_i \in C$ for all $i \geq i_0$.

Example : For $\mathbb{Q}_p(\sqrt{p})$ $(p \geq 3)$, take $\pi = \sqrt{p}$, and

$$x = a_0 + a_1\sqrt{p} + a_2 p + a_3 p^{3/2} + a_4 p^2 + \cdots .$$

Affine polynomial dynamical systems on $\mathcal{O}_K$

I. Minimal subsystems and odometer

Given a positive integer sequence $(p_s)_{s\geq 0}$ such that $p_s|p_{s+1}$.

Profinite groupe : $\mathbb{Z}_{(p_s)} := \lim\limits_{\leftarrow} \mathbb{Z}/p_s\mathbb{Z}$.

Odometer : The transformation $\tau : x \mapsto x+1$ on $\mathbb{Z}_{(p_s)}$.

Theorem (Chabert-Fan-Fares 2007)

Let E be a compact set in $\mathcal{O}_K$ and $T : E \to E$ a 1-lipschitzian transformation. If the dynamical system (E,T) is minimal, then

- (E,T) is conjugate to the odometer $(\mathbb{Z}_{(p_s)}, \tau)$ where (p_s) is determined by the structure of E.

Consider polynomial $T \in \mathcal{O}_K[x]$ as a dynamical system : $T : \mathcal{O}_K \to \mathcal{O}_K$.

Let X be a finite union of balls in $\mathcal{O}_K$. We say that X is of type $(k, \vec{E})$ if (X,T) is decomposed into uncountable (cardinality of $\mathbb{R}$) many minimal subsystems, all of them are conjugate to the odometer $(\mathbb{Z}_{(p_s)}, \tau)$ with

$$(p_s) = (k,\ \underbrace{kp, \cdots, kp}_{E_1},\ \underbrace{kp^2, \cdots, kp^2}_{E_2},\ \underbrace{kp^3, \cdots, kp^3}_{E_3},\ \cdots).$$

If $\vec{E} = (e, e, e, \dots)$, we call simply that X is of type (k, e).

II. Minimal decomposition for $\alpha x + \beta$ on $\mathcal{O}_K$

Let $T(x) = \alpha x + \beta$. Denote

$$\mathbb{U} := \{x \in \mathcal{O}_K : |x|_p = 1\}, \ \mathbb{V} := \{x \in \mathbb{U} : \exists m \in \mathbb{N}, m \geq 1, x^m = 1\}.$$

Easy cases :

1. $\alpha \notin \mathbb{U}(|\alpha|_p < 1) \Rightarrow$ one attracting fixed point $\beta/(1-\alpha)$.
2. $\alpha = 1, \beta = 0 \Rightarrow$ every point is fixed.
3. $\alpha \in \mathbb{V} \setminus \{1\} \Rightarrow$ every point is on a ℓ-periodic orbit, with ℓ the smallest integer $\geqslant 1$ such that $\alpha^\ell = 1$.

III. Minimal decomposition for $\alpha x + \beta$ on $\mathcal{O}_K$, $p \geq 3$

Theorem (L, preprint)

4. $\alpha \in (\mathbb{U} \setminus \mathbb{V}) \cup \{1\}, v_\pi(\beta) < v_\pi(1-\alpha)$.
   - $v_\pi(\beta) = 0 \Rightarrow \mathcal{O}_K$ is decomposed into p^{d-1} compact sets. Each compact set is of type (p, e).
   - $v_\pi(\beta) > 0 \Rightarrow \mathcal{O}_K$ is decomposed into $p^{v_\pi(\beta)\cdot f}$ compact sets. Each compact set is of type $(1, e)$.
5. $\alpha \in \mathbb{U} \setminus \mathbb{V}, v_\pi(\beta) \geq v_\pi(1-\alpha) \Rightarrow (\mathcal{O}_K, T)$ is conjugate to $(\mathcal{O}_K, \alpha x)$.

   Decomposition : $\mathcal{O}_K = \{0\} \cup \cup_{k=0}^{\infty} \pi^k \mathbb{U}$,

   (1) The point 0 is fixed.

   (2) Each $(\pi^k \mathbb{U}, \alpha x)$ is conjugate to $(\mathbb{U}, \alpha x)$.

   ⋆ Denote by ℓ the smallest integer $\geqslant 1$ such that $\alpha^\ell \equiv 1 \pmod{\pi}$. Pour $(\mathbb{U}, \alpha x)$, $\mathbb{U}$ is decomposed into

$$(p^f - 1) \cdot p^{v_\pi(\alpha^\ell - 1)f - f} / \ell$$

   compact sets and each compact set is of type (ℓ, e).

IV. Minimal decomposition for $\alpha x + \beta$ on $\mathcal{O}_K$, $p = 2$

Theorem (L, preprint)

4. $\alpha \in (\mathbb{U} \setminus \mathbb{V}) \cup \{1\}, v_\pi(\beta) < v_\pi(1-\alpha)$.

   Denote by N the biggest integer such that $v_\pi(\alpha^{2^N} + 1) < e$.

   - $v_\pi(\beta) = 0 \Rightarrow \mathcal{O}_K$ is decomposed into $p^{f \cdot v_\pi(\alpha+1)-1}$ compact sets. Each compact set is of type $(p, \vec{E})$ avec

   $$\vec{E} = \Big(v_\pi(\alpha^2+1),\ v_\pi(\alpha^4+1),\ \cdots,\ v_\pi(\alpha^{2^N}+1),\ e,\ e,\ \cdots\Big).$$

   - $v_\pi(\beta) > 0 \Rightarrow \mathcal{O}_K$ is decomposed into $p^{v_\pi(\beta)\cdot f}$ compact sets. Each compact set is of type $(p, \vec{E})$ with

   $$\vec{E} = \Big(v_\pi(\alpha+1),\ v_\pi(\alpha^2+1),\ \cdots,\ v_\pi(\alpha^{2^N}+1),\ e,\ e,\ \cdots\Big).$$

V. Decomposition for $\alpha x + \beta$, $p = 2$, continued

Theorem (L, preprint)

5. $\alpha \in \mathbb{U} \setminus \mathbb{V}, v_\pi(\beta) \geq v_\pi(1-\alpha) \Rightarrow (\mathcal{O}_K, T)$ is conjugate to $(\mathcal{O}_K, \alpha x)$.
   Decomposition : $\mathcal{O}_K = \{0\} \cup \cup_{k=0}^{\infty} \pi^k \mathbb{U}$,
   (1) The point 0 is fixed.
   (2) Each $(\pi^k \mathbb{U}, \alpha x)$ is conjugate to $(\mathbb{U}, \alpha x)$.
   ⋆ Denote by ℓ the smallest integer $\geqslant 1$ such that $\alpha^\ell \equiv 1 \pmod{\pi}$. For $(\mathbb{U}, \alpha x)$, $\mathbb{U}$ is decomposed into

$$(p^f - 1) \cdot p^{v_\pi(\alpha^\ell - 1)f - f} / \ell$$

compact sets and each compact set is of type $(\ell, \vec{E})$ with

$$\vec{E} = \Big(v_\pi(\alpha^\ell + 1),\ v_\pi(\alpha^{\ell p} + 1),\ \cdots,\ v_\pi(\alpha^{\ell p^N} + 1),\ e,\ e,\ \cdots\Big),$$

where N the biggest integer such that $v_\pi(\alpha^{\ell p^N} + 1) < e$.

VI. An example

Let $p \geq 3$.

Consider the finite extension $K = \mathbb{Q}_p(\sqrt{p})$, and $T(x) = \alpha x$ with $\alpha \in \mathbb{Z}_p$.

Let ℓ be the least integer $\geqslant 1$ such that $\alpha^\ell \equiv 1 \pmod{p}$.
Consider T as a system on $X = \{x \in \mathbb{Z}_p : |x|_p = 1\}$. Then X consists of $p^{v_p(\alpha^\ell - 1)-1}(p-1)/\ell$ minimal parts.

As a system on $\mathcal{O}_K$,

- we have the decomposition ($\mathbb{U} = \{x \in \mathcal{O}_K : |x|_p = 1\}$)

$$\mathcal{O}_K = \{0\} \cup \bigcup_{k=0}^{\infty} \pi^k \mathbb{U}.$$

- All $(\pi^k \mathbb{U}, T)$ are conjugate to $(\mathbb{U}, T)$.
- For $(\mathbb{U}, T)$, we have uncountable (cardinality of real numbers) many minimal parts which can be written as

$$E \cdot (1 + \sqrt{p} y),$$

with E a minimal part of T on X ($\subset \mathbb{Z}_p$) and $y \in \mathbb{Z}_p$.

VII. Ideas and methods

Fan, Li, Yao, Zhou : Fourier analysis.

Our methodes :

Theorem (Anashin 1994, Chabert, Fan and Fares 2009)

Let $X \subset \mathcal{O}_K$ be a compact set.
$f : X \to X$ is minimal $\Leftrightarrow$
$f_k : X/\pi^k\mathcal{O}_K \to X/\pi^k\mathcal{O}_K$ is minimal for all $k \geq 1$.

Predicting the behavior of f_{k+1} by the structure of f_k.
$\to$ Idea of Desjardins and Zieve 1994 (arXiv) and Zieve's Ph.D. Thesis 1996.