On the recurrence property of $p$-adic polynomial dynamical systems

Lingmin LIAO

University Paris 12

Lorentz Center, Leiden, June 2010
Outline

1. About $p$-adic numbers

2. Minimal decomposition of $p$-adic polynomial dynamical systems

3. $p$-adic repellers in $\mathbb{Q}_p$

4. Classification for low-order polynomials
About $p$-adic numbers
I. What are $p$-adic numbers?

1. 1897, K. Hensel.
2. $p \geq 2$ a prime number
3. $\forall n \in \mathbb{N}, n = \sum_{i=0}^{N} a_ip^i \ (a_i = 0, 1, \ldots, p-1)$
4. Ring $\mathbb{Z}_p$ of $p$-adic integers:

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

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

$$\mathbb{Q}_p \ni x = \sum_{i=v(x)}^{\infty} a_ip^i, \ (\exists v(x) \in \mathbb{Z}).$$
II. Topology of $\mathbb{Q}_p$

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

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

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

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

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

Development of numbers:

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

**Theorem (Ostrowski 1918)**

Each non-trivial norm on $\mathbb{Q}$ is equivalent to $| \cdot |$ or to $| \cdot |_p$ for some $p$. 

Lingmin LIAO University Paris 12

Recurrence property of $p$-adic polynomial dynamical systems 5/27
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. $p$-adic analysis VS classical analysis

Something you like:
- $\{a_n\}$ is Cauchy $\iff \{a_n\}$ is quasi-Cauchy ($a_{n+1} - a_n \to 0$).
- $\sum_{n=0}^{\infty} a_n < \infty \iff a_n \to 0$.
- $p$-adic expansion of a $p$-adic number is unique.

Something you might do not like:
- No mean value theorem
- $f : X \subset \mathbb{Q}_p \to \mathbb{Q}_p$, $f'(x) = 0 \not\Rightarrow f = \text{const}$. 
V. $p$-adic polynomial dynamical systems

Let $X \subset \mathbb{Q}_p$ and $f \in \mathbb{Q}_p[x]$ satisfying $f : X \rightarrow X$. The couple $(X, f)$ is a $p$-adic polynomial dynamical system.

One is interested in the recurrence property (minimality, chaotic property, entropy...).

• 1-Lipschtz case (zero entropy): Let $f \in \mathbb{Z}_p[x]$, and consider the dynamical system $f : \mathbb{Z}_p \rightarrow \mathbb{Z}_p$.

**Proposition: ”Topological way = measure-theoretic way”**

Let $X \subset \mathbb{Z}_p$ be a compact subset. Let $f \in \mathbb{Z}_p[x]$ and $f : X \rightarrow X$. Then the following statements are equivalent:

1. $f$ is **minimal** on $X$. (Every orbit is dense.)
2. $f$ is **ergodic** on $X$ with respect to the Haar measure.
3. $f$ is **uniquely ergodic** on $X$.

• Chaotic case (positive entropy). Example: $f \in \mathbb{Q}[x]$ and $|f'(x)|_p > 1$.

• Mixed one and other cases.
Minimal decomposition of $p$-adic polynomial dynamical systems
I. Polynomial dynamical systems in $\mathbb{Z}_p$

- 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 (Fan-L preprint, minimal decomposition)**

Let $f \in \mathbb{Z}_p[x]$ with $\deg f \geq 2$. We can decompose $\mathbb{Z}_p$ into three parts:

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

where

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

Problem 1: Under what condition one has $A = C = \emptyset$, and $B$ admits a unique component?
(i.e., $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is minimal?)

Problem 2: If $(\mathbb{Z}_p, f)$ is not minimal, how to find the complete decomposition?
III. Known results - Minimal on the whole $\mathbb{Z}_p$

Theorem (Larin 2002 + Knuth 1969: any $p$ but $\deg(f) \leq 2$)

Let $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}_p$. $f$ is minimal iff

1. $a \equiv 0 \pmod{p}, b \equiv 1 \pmod{p}, c \not\equiv 0 \pmod{p}$, if $p \geq 5$,

2. $a \equiv 0 \pmod{9}, b \equiv 1 \pmod{3}, c \not\equiv 0 \pmod{3}$ or $ac \equiv 6 \pmod{9}, b \equiv 1 \pmod{3}, c \not\equiv 0 \pmod{3}$, if $p = 3$.

3. $a \equiv 0 \pmod{2}, a + b \equiv 1 \pmod{4}$ and $c \not\equiv 0 \pmod{2}$, if $p = 2$.

Theorem (Larin 2002: any degree but $p = 2$)

Let $p = 2$ and let $f(x) = \sum a_k x^k \in \mathbb{Z}_2[X]$ be a polynomial. Then $(\mathbb{Z}_p, f)$ is minimal iff

$$
\begin{align*}
    a_0 &\equiv 1 \pmod{2}, \\
    a_1 &\equiv 1 \pmod{2}, \\
    2a_2 &\equiv a_3 + a_5 + \cdots \pmod{4}, \\
    a_2 + a_1 - 1 &\equiv a_4 + a_6 + \cdots \pmod{4}.
\end{align*}
$$
Any degree but \( p = 3 \)

Let \( f(x) = \sum a_k x^k \in \mathbb{Z}_3[X] \). We can suppose \( a_0 = 1 \):

- \( a_0 \equiv 0 \pmod{3} \) \( \Rightarrow \) \( f \) is not minimal.
- \( a_0 \not\equiv 0 \pmod{3} \) \( \Rightarrow \) \( f \) is conjugate to a polynomial \( g \) with \( a_0 = 1 \).

Note

\[
\begin{align*}
A_0 &= \sum_{i \in \mathbb{N}, i \neq 0} a_i, \\
A_1 &= \sum_{i \in 1 + 2\mathbb{N}} a_i, \\
D_0 &= \sum_{i \in \mathbb{N}, i \neq 0} ia_i, \\
D_1 &= \sum_{i \in 1 + 2\mathbb{N}} ia_i.
\end{align*}
\]

**Theorem (Durand-Paccaut 2009)**

The system \((\mathbb{Z}_3, f)\) is minimal iff \( f \) satisfies \( A_0 \in 3\mathbb{Z}_3, A_1 \in 1 + 3\mathbb{Z}_3 \) and one of the following conditions:

1. \( D_0 \equiv 0, D_1 \equiv 2, a_1 \equiv 1 \) [3] and \( A_1 + 5 \not\equiv 0, 3a_2 + 3\sum_{j > 0} a_{5+6j} [9] \);
2. \( D_0 \equiv 0, D_1 \equiv 1, a_1 \equiv 1 \) [3] and \( A_0 + 6 \not\equiv 0, 6a_2 + 3\sum_{j > 0} a_{2+6j} [9] \);
3. \( D_0 \equiv 1, D_1 \equiv 0, a_1 \equiv 2 \) [3] and \( A_1 + 5 \not\equiv 0, 6a_2 + 3\sum_{j > 0} a_{5+6j} [9] \);
4. \( D_0 \equiv 2, D_1 \equiv 0, a_1 \equiv 2 \) [3] and \( A_0 + 6 \not\equiv 0, 3a_2 + 3\sum_{j > 0} a_{2+6j} [9] \).


III. Known results - Minimal decomposition

Theorem (Fan-Li-Yao-Zhou 2007 : any \( p \) but \( \deg(f) = 1 \))

Case \( p = 2 \) (I just show this case here):

\[
T_{a,b}x = ax + b \quad (a, b \in \mathbb{Z}_2).
\]

\[ \mathbb{U} = \{z \in \mathbb{Z}_2 : |z| = 1\} = 1 + 2\mathbb{Z}_2, \mathbb{U}_2 = 1 + 4\mathbb{Z}_2 \]

\[ \mathbb{V} = \{z \in \mathbb{U} : \exists m \geq 1, \text{s.t. } z^m = 1\} \]

1. \( a \in \mathbb{Z}_2 \setminus \mathbb{U} \Rightarrow \) one attracting fixed point \( b/(1 - a) \).

2. \( a \in \mathbb{V} \setminus \{1\} \ (a = -1) \Rightarrow \) every point is in a 2-periodic orbit. (\( \{x, -x + b\} \)).

3. \( a \in \mathbb{U}_2 \)
   - \( v(b) < v(1 - a) \Rightarrow 2^{v(b)} \) components.
   - \( v(b) \geq v(1 - a) \Rightarrow \) reduced to \( T_{a,0} \).

   • For \( T_{a,0} \), all \( (2^n \mathbb{U}, T_{a,b})(n \geq 0) \) are conjugate to \( (\mathbb{U}, T_{a,0}) \).

   • For \( (\mathbb{U}, T_{a,0}) : 2^{v(a-1) - 1} \) components.

4. \( a \in \mathbb{U} \setminus (\mathbb{U}_2 \cup \mathbb{V}) \) : similar to the case \( a \in \mathbb{U}_2 \).
IV. An application
We can calculate some frequencies.

Corollary (Fan-Li-Yao-Zhou 2007)

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

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

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

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

One motivation:
V. Minimal decomposition for quadratic polynomials

Theorem (Fan-L, preprint)
Let \( p = 2 \). We obtain the minimal decomposition of quadratic polynomials.

→ Look at a special case.

Theorem (Fan-L, preprint)
For \((\mathbb{Z}_2, x^2 + x)\),

1. The ball \( 1 + 2\mathbb{Z}_2 \) is mapped into \( 2\mathbb{Z}_2 \).
2. The ball \( 2\mathbb{Z}_2 \) can be decomposed as:

\[
2\mathbb{Z}_2 = \{0\} \bigsqcup \left( \bigsqcup_{n \geq 2} 2^{n-1} + 2^n\mathbb{Z}_2 \right),
\]

and for each \( n \geq 2 \), \( 2^{n-1} + 2^n\mathbb{Z}_2 \) is decomposed as \( 2^{n-2} \) minimal component:

\[
2^{n-1} + t2^n + 2^{2n-2}\mathbb{Z}_2, \quad t = 0, \ldots, 2^{n-2} - 1.
\]
→ decomposition of $x^2 + x$

```
1 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0 → 0

0  8  4  12 (mod 2)

0  8  4  12 (mod 2^2)

0  8  4  12 (mod 2^3)

0  8  4  12 (mod 2^4)

0  8  4  12 (mod 2^5)

0  8  4  12 (mod 2^6)
```
VI. Ideas and methods

Theorem (Anashin 1994, Chabert, Fan and Fares 2007)

Let $X \subset \mathbb{Z}_p$ be a compact set.

$f : X \to X$ is minimal $\iff f_n : X/p^n\mathbb{Z}_p \to X/p^n\mathbb{Z}_p$ is minimal for all $n \geq 1$.

Predicting the behavior of $f_{n+1}$ by the structure of $f_n$.

→ Idea of Desjardins and Zieve 1994 (ArXiv)
$p$-adic repellers in $\mathbb{Q}_p$
I. Settings

- \( f : X \to \mathbb{Q}_p, \ X \subset \mathbb{Q}_p \) compact open.
- Assume that
  1. \( f^{-1}(X) \subset X \);
  2. \( X = \bigcup_{i \in I} B_{p^{-\tau}}(c_i) \) (with some \( \tau \in \mathbb{Z} \)), \( \forall i \in I, \ \exists \tau_i \in \mathbb{Z} \) s.t.

\[
|f(x) - f(y)|_p = p^{\tau_i}|x - y|_p \quad (\forall x, y \in B_{p^{-\tau}}(c_i)). \tag{1}
\]

- Define **Julia set**:

\[
J_f = \bigcap_{n=0}^{\infty} f^{-n}(X).
\]

We have \( f(J_f) \subset J_f \). \((X, J_f, f)\) is called

- a **\( p \)-adic weak repeller** if all \( \tau_i \geq 0 \) in (1), but at least one \( > 0 \).
- a **\( p \)-adic repeller** if all \( \tau_i > 0 \) in (1).
II. A result of analysis on \( \mathbb{Q}_p \)

- \( f : X (\subset \mathbb{Q}_p) \to \mathbb{Q}_p \) is **continuously differentiable** at \( a \in X \) if the following exists:

\[
\lim_{(x,y) \to (a,a), x \neq y } \frac{f(x) - f(y)}{x - y}.
\]

**Lemma (Local rigidity lemma)**

Let \( U \) be a clopen set and \( a \in U \). Suppose

\( f : U \to \mathbb{Q}_p \) is continuously differentiable, \( f'(a) \neq 0 \).

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

\[
|f(x) - f(y)|_p = |f'(a)|_p |x - y|_p
\]

(\( \forall x, y \in B_r(a) \)).
III. Theorem and examples

**Theorem (Fan-L-Wang-Zhou, 2007)**

Let \((X, J_f, f)\) be a transitive \(p\)-adic weak repeller. Then the dynamics \((J_f, f, | \cdot |_p)\) is isometrically conjugate to a subshift of finite type.

→ **Example 1**

Let \(c = \frac{c_0}{p^\tau} \in \mathbb{Q}_p\) with \(|c_0|_p = 1\) and \(\tau \geq 1\).

Define **\(p\)-adic logistic map** \(f_c : \mathbb{Q}_p \rightarrow \mathbb{Q}_p\)

\[
 f_c(x) = cx(x - 1).
\]

- \(X = p^\tau \mathbb{Z}_p \sqcup (1 + p^\tau \mathbb{Z}_p)\),
- \(J_c = \bigcap_{n=0}^{\infty} f_c^{-n}(X)\).

**Corollary (Fan-L-Wang-Zhou, 2007)**

\((J_c, f_c)\) is conjugate to \((\{0, 1\}^\mathbb{N}, \sigma)\).
Example 2

Let $m \in \mathbb{N}^*$ be a positive integers and $x_1, \ldots, x_m \in \mathbb{Z}_p$.
Suppose $x_i \equiv x_0 \not\equiv 0 \pmod{p} (1 \leq i < p)$ and $x_i \not\equiv x_j \pmod{p^2} (i \neq j)$.
Consider 
$$f(x) = \frac{x(x-x_1)(x-x_2)\cdots(x-x_m)}{p^{m-1}}.$$ 
Take 
$$X = p^m\mathbb{Z}_p \cup (kp^{m-1} + p^m\mathbb{Z}_p) \cup \bigcup_{j=1}^{m} x_i + p^m\mathbb{Z}_p, \quad J_f := \bigcap_{n=0}^{\infty} f^{-n}(X)$$

Corollary (L, manuscript)

System $(J_f, f)$ is conjugate to a subshift of finite type of $m + 2$ symbols.

$$A = \begin{pmatrix}
1 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 1 \\
1 & 0 & 0 & \cdots & 0 \\
1 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & 0 & 0 & \cdots & 0 \\
\end{pmatrix}$$
Classification for

low-order polynomials
I. Quadratic polynomials
Let \( f(x) := Ax^2 + Bx + C \) \((A, B, C \in \mathbb{Q}_p, A \neq 0)\).

- Chaotic property :
  - Shabat unpublished,
  - Thiran-Verstegen-Weyers 1989,
  - Woodcock-Smart 1998,
  - Dremov-Shabat-Vytnova 2006,
  - Benedetto- Briend-Perdry 2007,
  - Our methods also work

- Minimality : \( p = 2 \), we have complete minimal decomposition.

Classification :

- OK for \( p = 2 \).
- \( p \geq 3 \) : difficulty in minimal part.
II. Cubic polynomials

- $f(x) = x^3 + ax$ or $f(x) = x^3 + a$ with $|a|_p > 1$
  (Possible subsystem : full shift with two symbols)

- $f(x) = x^3 + ax^2$ where $|a|_p > 1$
  (Possible subsystems : minimal components, full shift with two symbols)
  (Also studied by Mukhamedov and Mendes 2007).

A special example :

- $f(x) = \frac{x^3}{6} + x^2 - \frac{x}{2}$, attracting and expanding mixed :

$$1 + 4 + 8\mathbb{Z}_2 \Leftrightarrow 2 + 4 + 16\mathbb{Z}_2$$

$$1 + 8\mathbb{Z}_2 \Leftrightarrow 2 + 4 + 8 + 16\mathbb{Z}_2.$$
II. Cubic polynomials

- \( f(x) = x^3 + ax \) or \( f(x) = x^3 + a \) with \( |a|_p > 1 \)
  (Possible subsystem : full shift with two symbols)

- \( f(x) = x^3 + ax^2 \) where \( |a|_p > 1 \)
  (Possible subsystems : minimal components, full shift with two symbols)
  (Also studied by Mukhamedov and Mendes 2007).

A special example :

- \( f(x) = \frac{x^3}{6} + x^2 - \frac{x}{2} \), attracting and expanding mixed :

  \[ 1 + 4 + 8\mathbb{Z}_2 \leftrightarrow 2 + 4 + 16\mathbb{Z}_2 \]
  \[ 1 + 8\mathbb{Z}_2 \leftrightarrow 2 + 4 + 8 + 16\mathbb{Z}_2. \]
Some notes and books

- **Andrew Baker** : An Introduction to $p$-adic Numbers and $p$-adic Analysis. (Version 2010, available on his homepage.)