Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Acad. Sci. Paris, Ser. I 342 (2006) 129–134
COMPTES RENDUS MATHEMATIQUE
http://france.elsevier.com/direct/CRASS1/

Dynamical Systems/Number Theory

p-adic affine dynamical systems and applications

Ai-Hua Fan [a,b], Ming-Tian Li [b], Jia-Yan Yao [b], Dan Zhou [b]

[a] *LAMFA, UMR 6140 CNRS, université de Picardie, 33, rue Saint-Leu, 80039 Amiens, France*
[b] *Department of Mathematics, Wuhan University, 430072 Wuhan, PR China*

Received 7 November 2005; accepted 15 November 2005

Available online 7 December 2005

Presented by Jean-Pierre Kahane

Abstract

We consider p-adic affine dynamical systems on the ring $\mathbb{Z}_p$ of all p-adic integers, and we find a necessary and sufficient condition for such a system to be minimal. The minimality is equivalent to the transitivity, the ergodicity of the Haar measure, the unique ergodicity, and the strict ergodicity. When the condition is not satisfied, we prove that the system can be decomposed into strict ergodic subsystems. One of our applications is the study of the divisibility, by a power of prime number, of the sequence of integers $a^n - b$ with positive integers a, b and n. ***To cite this article: A.-H. Fan et al., C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Résumé

Systèmes dynamiques affines *p*-adiques et applications. Nous considérons les systèmes dynamiques affines p-adiques sur l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Nous obtenons une condition nécessaire et suffisante pour qu'un tel système soit minimal. La minimalité est équivalente à la transitivité, à l'ergodicité de la mesure de Haar, à l'unique ergodicité, et à la stricte ergodicité. Quand la condition n'est pas satisfaite, nous donnons tous les sous-systèmes strictement ergodiques du système affine p-adique en question. L'une de nos applications est l'étude de la divisibilité, par une puissance d'un nombre premier, de la suite des entiers de la forme $a^n - b$ (a, b et n étant des entiers positifs). ***Pour citer cet article : A.-H. Fan et al., C. R. Acad. Sci. Paris, Ser. I 342 (2006).***

Version française abrégée

Nous présentons dans cette Note quelques résultats sur les systèmes dynamiques affines p-adiques $(\mathbb{Z}_p, T_{\alpha,\beta})$, où $\alpha, \beta \in \mathbb{Z}_p$, et $T_{\alpha,\beta}$ est défini par $T_{\alpha,\beta}(z) := \alpha z + \beta$ $(\forall z \in \mathbb{Z}_p)$.

Rappelons que $p \geqslant 2$ désigne un nombre premier et $\mathbb{Z}_p$ l'anneau des entiers p-adiques, muni de la valeur absolue non-archimédienne $|\cdot|_p$ définie par $|z|_p = p^{-\upsilon_p(z)}$. Nous désignons respectivement par $\mathbb{U}$, $\mathbb{V}$ et $\wp$ le groupe des inversibles, le groupe des racines de l'unité, et l'idéal maximal de $\mathbb{Z}_p$. Alors

$$\mathbb{U} = \{z \in \mathbb{Z}_p : |z|_p = 1\} \quad \text{et} \quad \wp = \mathbb{Z}_p \setminus \mathbb{U} = p\mathbb{Z}_p.$$

E-mail addresses: ai-hua.fan@u-picardie.fr (A.-H. Fan), limtwd@sohu.com (M.-T. Li), jiayan69@tom.com (J.-Y. Yao), maureen28@sohu.com (D. Zhou).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2005.11.017

Il est à noter que nous avons $\mathbb{V} = \{\pm 1\}$ si $p = 2$. Finalement pour tout entier rationnel $n \geqslant 1$, notons

$$\mathbb{U}_n := 1 + \wp^n = 1 + p^n\mathbb{Z}_p \quad \text{et} \quad \mathbb{S}_n = \mathbb{U}_n \setminus \mathbb{U}_{n+1}.$$

Nous renvoyons le lecteur à [3] pour plus d'informations sur l'anneau $\mathbb{Z}_p$, et à [4] pour les notions utilisées dans cette note sur les systèmes dynamiques.

Voici les résultats principaux :

Théorème 0.1. *Le système dynamique $(\mathbb{Z}_p, T_{\alpha,\beta})$ est minimal si et seulement si $\alpha \in \mathbb{U}_{r_p}$ et $\beta \in \mathbb{U}$, où $r_p = 1$ (resp. $r_p = 2$) si $p > 2$ (resp. si $p = 2$). De plus, si ces conditions sont satisfaites, le système est strictement ergodique (avec la mesure de Haar normalisée sur $\mathbb{Z}_p$ comme l'unique mesure de probabilité $T_{\alpha,\beta}$-invariante), et il est topologiquement conjugué à $(\mathbb{Z}_p, T_{1,1})$, donc possède un spectre topologique discret constitué des valeurs propres 1 et $\mathrm{e}^{2\pi \mathrm{i}k/p^n}$ $(n \geqslant 1,\ 1 \leqslant k < p^n$, et $p \nmid k)$.*

Dans la suite, nous supposons $\alpha \in \mathbb{U} \setminus \mathbb{V}$. En réalité, si cette condition n'est pas vérifiée, le système dynamique est soit trivial soit conjugué au système $T_{1,1}$ qui est bien connu. En effet, si $|\alpha|_p < 1$, il existe un unique point fixe attractif $\frac{\beta}{1-\alpha}$ dont le bassin d'attraction est l'anneau $\mathbb{Z}_p$ tout entier ; si $\alpha = 1$, il est facile de voir que toutes les parties $j + \beta\mathbb{Z}_p$ $(0 \leqslant j < p^{v(\beta)})$ sont $T_{1,\beta}$-invariantes et que $T_{1,\beta}$ restreint à chaque $j + \beta\mathbb{Z}_p$ est conjugué à $T_{1,1}$; si $\alpha \in \mathbb{V} \setminus \{1\}$ et $p > 2$, tout point $z \in \mathbb{Z}_p$ se trouve dans un cycle périodique, car $T_{\alpha,\beta}$ est conjugué à $T_{\alpha,0}$ par l'application $z \mapsto z - \frac{\beta}{1-\alpha}$, et toutes les orbites de $T_{\alpha,0}$ sont cycliques ; finalement si $\alpha \in \mathbb{V} \setminus \{1\}$ et $p = 2$, alors $\alpha = -1$ et la restriction de $T_{\alpha,\beta}$ à $\{z, z - \beta\}$ est strictement ergodique, pour tout $z \in \mathbb{Z}_p$.

Théorème 0.2. *Soit $p > 2$ et $\alpha \in \mathbb{U} \setminus \mathbb{V}$. Désignons par ℓ le plus petit entier $\geqslant 1$ tel que $\alpha^\ell \equiv 1 \pmod p$.*

(A) *Si $\alpha \in \mathbb{U}$ et $v_p(\beta) < v_p(1-\alpha)$, alors le système $(\mathbb{Z}_p, T_{\alpha,\beta})$ est composé de $p^{v_p(\beta)}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_p, T_{1,1})$.*

(B) *Si $\alpha \in \mathbb{U}$ et $v_p(\beta) \geqslant v_p(1-\alpha)$, alors le système $(\mathbb{Z}_p, T_{\alpha,\beta})$ est topologiquement conjugué à $(\mathbb{Z}_p, T_{\alpha,0})$. Toutes les parties $p^n\mathbb{U}$ $(n \geqslant 0)$ sont $T_{\alpha,0}$-invariantes et forment une partition de $\mathbb{Z}_p$. Tous les sous-systèmes $(p^n\mathbb{U}, T_{\alpha,0}|_{p^n\mathbb{U}})$ sont topologiquement conjugués. Le sous-système $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ se décompose en $p^{v_p(\alpha^\ell-1)-1}(p-1)/\ell$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués au système produit $((\mathbb{Z}/\ell\mathbb{Z}) \times \mathbb{Z}_p, D \times T_{1,1})$, où $D : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z}$ est défini par $D(t) = t + 1$.*

Théorème 0.3. *Soit $p = 2$ et $\alpha \in \mathbb{U} \setminus \mathbb{V}$.*

(A) *Si $\alpha \in \mathbb{U} = \mathbb{U}_1$ et $v_2(\beta) < v_2(1-\alpha)$, alors il y a deux possibilités :*
  (a) *Si $\alpha \in \mathbb{U}_2$, le système $(\mathbb{Z}_2, T_{\alpha,\beta})$ est composé de $2^{v_2(\beta)}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_2, T_{1,1})$.*
  (b) *Si $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, le système $(\mathbb{Z}_2, T_{\alpha,\beta})$ est composé de $2^{v_2(1+\alpha)-1}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_2, T_{1,1})$.*

(B) *Si $\alpha \in \mathbb{U}$ et $v_2(\beta) \geqslant v_2(1-\alpha)$, le système $(\mathbb{Z}_2, T_{\alpha,\beta})$ est topologiquement conjugué à $(\mathbb{Z}_2, T_{\alpha,0})$. Toutes les parties $2^n\mathbb{U}$ $(n \geqslant 0)$ sont $T_{\alpha,0}$-invariantes et forment une partition de $\mathbb{Z}_2$. De plus, tous les sous-systèmes $(2^n\mathbb{U}, T_{\alpha,0}|_{2^n\mathbb{U}})$ sont topologiquement conjugués. Pour $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$, on a deux cas à distinguer :*
  (a) *Si $\alpha \in \mathbb{U}_2$, alors $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ est composé de $2^{v_2(\alpha-1)-1}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_2, T_{1,1})$.*
  (b) *Si $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, alors $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ est composé de $2^{v_2(\alpha+1)-1}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_2, T_{1,1})$.*

Le cas spécial $T_{\alpha,0}$ a été étudié par Coelho et Parry dans [1]. Leur résultat sur l'ergodicité de $T_{\alpha,0}|_{\mathbb{U}}$ est inclus dans le Théorème 0.2 (B) ci-dessus.

L'étude sur les systèmes dynamiques affines s'applique à celle des systèmes dynamiques monomiaux $S_{n,\rho} : \mathbb{U}_1 \to \mathbb{U}_1$ definis par $z \mapsto \rho z^n$, où $n \geqslant 2$ est un entier rationnel et $\rho \in \mathbb{U}_1$.

Par exemple, dans le cas $p > 2$, nous avons le résultat suivant.

Théorème 0.4. *Soit $p > 2$ un nombre premier, $\rho \in \mathbb{U}_1$, et $n \geqslant 2$ un entier rationnel tel que $p \nmid n$.*

(A) *Si $\upsilon_p(\rho - 1) < \upsilon_p(1-n) + 1$, alors $(\mathbb{U}_1, S_{n,\rho})$ est composé de $p^{\upsilon_p(\rho-1)-1}$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués à $(\mathbb{Z}_p, T_{1,1})$.*

(B) *Si $\upsilon_p(\rho - 1) \geqslant \upsilon_p(1-n) + 1$, alors $(\mathbb{U}_1, S_{n,\rho})$ est topologiquement conjugué à $(\mathbb{U}_1, S_{n,1})$. Toutes les sphères $\mathbb{S}_m$ $(m \geqslant 1)$ sont $S_{n,1}$-invariantes et forment une partition de $\mathbb{U}_1$. De plus, tous les sous-systèmes $(\mathbb{S}_m, S_{n,1}|_{\mathbb{S}_m})$ sont topologiquement conjugués. Le sous-système $(\mathbb{S}_1, S_{n,1}|_{\mathbb{S}_1})$ est composé de $p^{\upsilon_p(n^\ell-1)-1}(p-1)/\ell$ sous-systèmes strictement ergodiques qui sont tous topologiquement conjugués au système produit $((\mathbb{Z}/\ell\mathbb{Z}) \times \mathbb{Z}_p, D \times T_{1,1})$, où ℓ est le plus petit entier $\geqslant 1$ tel que $n^\ell \equiv 1 \pmod p$, et $D : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z}$ est défini par $D(t) = t + 1$.*

Le cas spécial $S_{n,1}$ a été étudié par Khrennikov, Lindahl, et Gundlach dans [2]. Leur résultat est inclus dans le Théorème 0.4(B).

Le cas $p = 2$ est un peu plus compliqué car le groupe additif $\mathbb{Z}_2$ n'est pas isomorphe au groupe multiplicatif $\mathbb{U}_1$, le dernier étant non-monothétique. Mais un théorème similaire au Théorème 0.4 subsiste.

Signalons une application. Soit $a > 1$ et $b \geqslant 1$ deux entiers premiers avec p. Désignons par ℓ le plus petit entier $\geqslant 1$ tel que $a^\ell \equiv 1 \pmod p$ et posons $\upsilon = \upsilon_p(a^\ell - 1)$. Pour tout entier $k \geqslant 1$, posons $s_k = \ell p^{\max(k-\upsilon,0)}$. Si $b \not\equiv a^j \pmod{p^k}$ pour tout $0 \leqslant j < s_k$, alors $p \nmid a^n - b$ $(\forall\, n \geqslant 1)$; sinon, nous avons

$$\lim_{N\to\infty} \frac{\operatorname{Card}\{1 \leqslant n \leqslant N\colon\ p^k \mid (a^n - b)\}}{N} = \frac{1}{s_k}.$$

Le résultat précédent, qui concerne effectivement les temps de retour de $T_{a,0}$, peut être aussi démontré par un argument purement algébrique.

1. Statements of main results

In this Note we will present some results on p-adic affine topological dynamical systems $(\mathbb{Z}_p, T_{\alpha,\beta})$, where $\alpha, \beta \in \mathbb{Z}_p$, and $T_{\alpha,\beta}$ is defined by

$$T_{\alpha,\beta}(z) := \alpha z + \beta \quad (\forall z \in \mathbb{Z}_p). \tag{1}$$

Recall that $p \geqslant 2$ is a prime number and $\mathbb{Z}_p$ is the ring of all p-adic integers, endowed with the usual non-Archimedean absolute value $|\cdot|_p$ defined by $|z|_p = p^{-\upsilon_p(z)}$. This is a local ring (i.e., a commutative ring which has only one maximal ideal). The group of units, the group of roots of unity and the maximal ideal of $\mathbb{Z}_p$ will be respectively denoted by $\mathbb{U}$, $\mathbb{V}$, and $\wp$. Then we have

$$\mathbb{U} = \big\{z \in \mathbb{Z}_p\colon\ |z|_p = 1\big\}, \quad \mathbb{V} = \big\{z \in \mathbb{U}\colon\ z^m = 1 \text{ for some } m \geqslant 1\big\}, \quad \text{and} \quad \wp = \big\{z \in \mathbb{Z}_p\colon\ |z|_p < 1\big\}. \tag{2}$$

By the way, we remark that we have $\mathbb{V} = \{\pm 1\}$ if $p = 2$. Finally for all integers $n \geqslant 1$, we denote

$$\mathbb{U}_n := 1 + \wp^n = 1 + p^n\mathbb{Z}_p, \quad \text{and} \quad \mathbb{S}_n = \mathbb{U}_n \setminus \mathbb{U}_{n+1}. \tag{3}$$

By convention, $\mathbb{U}_0 = \mathbb{U}$. All $\mathbb{U}_n$'s and $\mathbb{S}_1$ are multiplicative groups, but not $\mathbb{S}_n$ $(n \geqslant 2)$. We will write $r_p = 1$ for $p > 2$ and $r_2 = 2$. As we shall see later, there are some differences between the case $p > 2$ and the case $p = 2$.

The reader can consult [3] and [4] for more information about the ring $\mathbb{Z}_p$, and for notions about dynamical systems respectively.

Our main results are stated in the following three theorems:

Theorem 1.1. *The dynamical system $(\mathbb{Z}_p, T_{\alpha,\beta})$ is minimal if and only if $\alpha \in \mathbb{U}_{r_p}$ and $\beta \in \mathbb{U}$. Moreover if all these conditions are fulfilled, then the system is strictly ergodic* (*with the normalized Haar measure on $\mathbb{Z}_p$ as the unique $T_{\alpha,\beta}$-invariant probability measure*)*, and is topologically conjugate to $(\mathbb{Z}_p, T_{1,1})$, thus has discrete topological spectrum consisting of eigenvalues* 1 *and* $\mathrm{e}^{2\pi \mathrm{i}k/p^n}$ $(n \geqslant 1,\ 1 \leqslant k < p^n$, *and* $p \nmid k)$.

In the sequel we can always suppose without loss of generality $\alpha \in \mathbb{U} \setminus \mathbb{V}$. Actually if this assumption is not verified, the dynamical system is trivial or can be reduced directly to $T_{1,1}$, which is known as adding machine and has already been well understood. In fact, if $|\alpha|_p < 1$, there is a unique attracting fixed point $\frac{\beta}{1-\alpha}$ with the whole $\mathbb{Z}_p$ as

its attracting basin; if $\alpha = 1$, it is easy to see that $j + \beta\mathbb{Z}_p$ ($0 \leqslant j < p^{v(\beta)}$) are $T_{1,\beta}$-invariant and $T_{1,\beta}$ restricted on each $j + \beta\mathbb{Z}_p$ is conjugate to $T_{1,1}$; if $\alpha \in \mathbb{V} \setminus \{1\}$ and $p > 2$, every point $z \in \mathbb{Z}_p$ is in a periodic cycle, because $T_{\alpha,\beta}$ is conjugate to $T_{\alpha,0}$ with conjugacy $z \mapsto z - \frac{\beta}{1-\alpha}$, and all orbits of $T_{\alpha,0}$ are cycles; finally if $\alpha \in \mathbb{V} \setminus \{1\}$ and $p = 2$, then $\alpha = -1$, and the restriction of $T_{\alpha,\beta}$ on each two-point subset $\{z, -z + \beta\}$ is strictly ergodic.

Theorem 1.2. *Let $p > 2$, and let $\alpha \in \mathbb{U} \setminus \mathbb{V}$. Denote by ℓ the least integer $\geqslant 1$ such that $\alpha^\ell \equiv 1 \pmod{p}$.*

(A) *If $\alpha \in \mathbb{U}$ and $v_p(\beta) < v_p(1-\alpha)$, then $(\mathbb{Z}_p, T_{\alpha,\beta})$ consists of $p^{v_p(\beta)}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_p, T_{1,1})$.*

(B) *If $\alpha \in \mathbb{U}$ and $v_p(\beta) \geqslant v_p(1-\alpha)$, then the system $(\mathbb{Z}_p, T_{\alpha,\beta})$ is topologically conjugate to $(\mathbb{Z}_p, T_{\alpha,0})$. All $p^n\mathbb{U}$ ($n \geqslant 0$) are $T_{\alpha,0}$-invariant and form a partition of $\mathbb{Z}_p$. Moreover all the subsystems $(p^n\mathbb{U}, T_{\alpha,0}|_{p^n\mathbb{U}})$ are topologically conjugate. The subsystem $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ consists of $p^{v_p(\alpha^\ell-1)-1}(p-1)/\ell$ strictly ergodic subsystems which are all topologically conjugate to the product system $((\mathbb{Z}/\ell\mathbb{Z}) \times \mathbb{Z}_p, D \times T_{1,1})$, where $D : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z}$ is defined by $D(t) = t + 1$.*

Theorem 1.3. *Let $p = 2$, and let $\alpha \in \mathbb{U} \setminus \mathbb{V}$.*

(A) *If $\alpha \in \mathbb{U} = \mathbb{U}_1$ and $v_2(\beta) < v_2(1-\alpha)$, then we have two possibilities*:
  (a) *If $\alpha \in \mathbb{U}_2$, then the system $(\mathbb{Z}_2, T_{\alpha,\beta})$ consists of $2^{v_2(\beta)}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_2, T_{1,1})$.*
  (b) *If $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, then the system $(\mathbb{Z}_2, T_{\alpha,\beta})$ consists of $2^{v_2(1+\alpha)-1}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_2, T_{1,1})$.*

(B) *If $\alpha \in \mathbb{U}$ and $v_2(\beta) \geqslant v_2(1-\alpha)$, then the system $(\mathbb{Z}_2, T_{\alpha,\beta})$ is topologically conjugate to $(\mathbb{Z}_2, T_{\alpha,0})$. All the $2^n\mathbb{U}$ ($n \geqslant 0$) are $T_{\alpha,0}$-invariant and form a partition of $\mathbb{Z}_2$. Moreover all the subsystems $(2^n\mathbb{U}, T_{\alpha,0}|_{2^n\mathbb{U}})$ are topologically conjugate. About the subsystem $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$, we distinguish two cases*:
  (a) *If $\alpha \in \mathbb{U}_2$, then the subsystem $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ consists of $2^{v_2(\alpha-1)-1}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_2, T_{1,1})$.*
  (b) *If $\alpha \in \mathbb{U}_1 \setminus \mathbb{U}_2$, then the subsystem $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ consists of $2^{v_2(\alpha+1)-1}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_2, T_{1,1})$.*

The special case $T_{\alpha,0}$ was studied by Coelho and Parry in [1], and their result on the ergodicity of $T_{\alpha,0}|_{\mathbb{U}}$ is contained in Theorem 1.2(B) above.

We shall apply the above results to study the monomial dynamical systems $(\mathbb{U}_1, S_{n,\rho})$, where $n \geqslant 2$ is an integer, $\rho \in \mathbb{U}_1$, and $S_{n,\rho}$ is defined as follows:

$$S_{n,\rho}(z) := \rho z^n \quad (\forall z \in \mathbb{U}_1). \tag{4}$$

Notice that the case $p \mid n$ is trivial: in this case $S_{n,\rho}$ has a unique attracting fixed point $\rho^{1/(1-n)}$ with $\mathbb{U}_1$ as its attracting basin.

We remark that when $p > 2$, the p-adic monomial dynamical system $(\mathbb{U}_1, S_{n,\rho})$ is topologically conjugate to the p-adic affine dynamical system $(\mathbb{Z}_p, T_{n,\beta})$, with $\beta := \mathrm{Log}(\rho)/\mathrm{Log}(1+p)$. Thus Theorem 1.2 can be translated into the following theorem:

Theorem 1.4. *Let $p > 2$ be a prime number, $\rho \in \mathbb{U}_1$, and $n \geqslant 2$ an integer such that $p \nmid n$.*

(A) *If $v_p(\rho-1) < v_p(1-n) + 1$, then $(\mathbb{U}_1, S_{n,\rho})$ consists of $p^{v_p(\rho-1)-1}$ strictly ergodic subsystems which are all topologically conjugate to $(\mathbb{Z}_p, T_{1,1})$.*

(B) *If $v_p(\rho-1) \geqslant v_p(1-n) + 1$, then $(\mathbb{U}_1, S_{n,\rho})$ is topologically conjugate to $(\mathbb{U}_1, S_{n,1})$. All the spheres $\mathbb{S}_m$ ($m \geqslant 1$) are $S_{n,1}$-invariant and form a partition of $\mathbb{U}_1$. Moreover, all the subsystems $(\mathbb{S}_m, S_{n,1}|_{\mathbb{S}_m})$ are topologically conjugate. The subsystem $(\mathbb{S}_1, S_{n,1}|_{\mathbb{S}_1})$ consists of $p^{v_p(n^\ell-1)-1}(p-1)/\ell$ strictly ergodic subsystems which are all topologically conjugate to the product system $((\mathbb{Z}/\ell\mathbb{Z}) \times \mathbb{Z}_p, D \times T_{1,1})$, where ℓ is the least integer $\geqslant 1$ such that $n^\ell \equiv 1 \pmod{p}$, and $D : \mathbb{Z}/\ell\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z}$ is defined by $D(t) = t + 1$.*

The special case $S_{n,1}$ was studied by Khrennikov, Lindahl, and Gundlach in [2]. Their result is contained in Theorem 1.4(B).

The case $p = 2$ is slightly more complicated. The reason is that in this case, there does not exist any homeomorphic group isomorphism from the additive group $\mathbb{Z}_2$ onto the multiplicative group $\mathbb{U}_1$, for the latter is not monothetic. We are thus obliged to consider the direct decomposition $\mathbb{U}_1 = \{\pm 1\}\cdot\mathbb{U}_2$, and reduce our study to that of the direct product of two systems respectively on $\{\pm 1\}$ and on $\mathbb{U}_2$. We do not give here the statement of our theorem for the case $p = 2$, because it is too long.

2. Applications

As more or less direct applications of our above theorems, we can obtain as corollaries all the following results. The first ones are dynamical, and the others are arithmetical.

Corollary 2.1. *Let $T'_{\alpha',\beta'}$ be another affine transformation defined similarly as $T_{\alpha,\beta}$ by the formula* (1)*, but on a different ring $\mathbb{Z}_q$ ($q \neq p$). If $|\alpha|_p = |\alpha'|_q = 1$, then $T'_{\alpha',\beta'}$ and $T_{\alpha,\beta}$ are not topologically conjugate.*

Corollary 2.2. *Let $p > 2$ and $\alpha \in \mathbb{U}$. Then the following statements are equivalent*:

(i) *the system $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ is strictly ergodic,*
(ii) *α is a primitive root* mod p *and $\alpha^{p-1} \not\equiv 1 \pmod{p^2}$,*
(iii) *the set $\{\alpha^m\colon\ m \in \mathbb{N}\}$ is dense in $\mathbb{U}$,*
(iv) *$\alpha \pmod{p^n}$ generates $(\mathbb{Z}/p^n\mathbb{Z})^\times$, for all integers $n \geqslant 1$,*
(v) *$\alpha \pmod{p^2}$ generates $(\mathbb{Z}/p^2\mathbb{Z})^\times$.*

Corollary 2.3. *If $p = 2$ and $\alpha \in \mathbb{U}$, then $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$ can never be strictly ergodic. But if $\alpha \in \mathbb{U}_2$, then the following statements are equivalent*:

(i) *the system $(\mathbb{U}_2, T_{\alpha,0}|_{\mathbb{U}_2})$ is strictly ergodic,*
(ii) *$\alpha \in \mathbb{U}_2 \backslash \mathbb{U}_3$,*
(iii) *the set $\{\alpha^m\colon\ m \in \mathbb{N}\}$ is dense in $\mathbb{U}_2$,*
(iv) *$\pm\alpha \pmod{2^n}$ generates $(\mathbb{Z}/2^n\mathbb{Z})^\times$, for all integers $n \geqslant 3$,*
(v) *$\pm\alpha \pmod 8$ generates $(\mathbb{Z}/8\mathbb{Z})^\times$,*
(vi) *$\alpha \equiv 5 \pmod 8$.*

Corollary 2.4. *Let $n \geqslant 1$ be an integer.*

(i) *If $p > 2$, the multiplicative group $(\mathbb{Z}/p^n\mathbb{Z})^\times$ is cyclic, and can be generated by $\theta(1 + p) \pmod{p^n}$, where $\theta \in \mathbb{V}$ is a generator of $\mathbb{V}$.*
(ii) *If $p = 2$ and $n \geqslant 3$, then the multiplicative group $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is isomorphic to the direct product group $\{\pm 1\} \times \langle\bar{5}\rangle$, where $\langle\bar{5}\rangle$ is the subgroup of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ generated by $\bar{5} := 5 + 2^n\mathbb{Z}$.*

Given two rational integers $a \neq 1$ and b, we consider the sequence of integers $a^n - b$. How many integers in this sequence are divided by a given power of prime number p^k? For this, we have the following corollary (similar result holds for $p = 2$).

Corollary 2.5. *Let $p > 2$ be a prime number. Let $a > 1$ and $b \geqslant 1$ be two integers coprime with p. Let ℓ be the least integer $\geqslant 1$ such that $a^\ell \equiv 1 \pmod{p}$, and $\upsilon = \upsilon_p(a^\ell - 1)$. For all integers $k \geqslant 1$, put $s_k = \ell p^{\max(k-\upsilon,0)}$. If $b \not\equiv a^j \pmod{p^k}$ for all $0 \leqslant j < s_k$, then $p^k \nmid a^n - b$ for all $n \geqslant 1$; otherwise we have*

$$\lim_{N\to\infty} \frac{\operatorname{Card}\{1 \leqslant n \leqslant N\colon\ p^k \mid (a^n - b)\}}{N} = \frac{1}{s_k}.$$

The above result can also be proved by a purely algebraic argument. The case that p divides a or b is either trivial or can be reduced to the above case. Moreover, the same result equally holds for p-adic integers a and b, but there is a new case that a ($\neq 1$) is a root of unity.

3. Proofs (sketches)

We have two methods for proving Theorem 1.1. The most important is to find a dense orbit under suitable condition. Our first method is to use Fourier expansion to find exact condition for the Haar measure to be ergodic, and then show that such a condition implies the existence of dense orbits. This method, which also allows us to find all topological eigenvalues, suggests that a strictly ergodic system $(\mathbb{Z}_p, T_{\alpha,\beta})$ is conjugate to $(\mathbb{Z}_p, T_{1,1})$. Actually a direct proof is provided by the conjugacy $h \circ T_{\alpha,\beta} = T_{1,1} \circ h$, where $h(z) = \beta\frac{\alpha^z-1}{\alpha-1}$. Remark here that we have $h^{-1}(z) = \frac{\mathrm{Log}(1+((\alpha-1)/\beta)z)}{\mathrm{Log}\,\alpha}$. Remark also that in this p-adic context, the exponential function $\mathrm{Exp}(z)$ is isometric and its inverse is the logarithmic function $\mathrm{Log}(z)$.

The proof of Theorem 1.2(A) is based on the observation that $\mathbb{Z}_p$ is a disjoint union of the $T_{\alpha,\beta}$-invariant subsets $\mathbb{A}_j := j + p^\beta\mathbb{Z}_p$ ($0 \leqslant j < p_p^\upsilon(\beta)$). Actually, the subsystem $(\mathbb{A}_j, T_{\alpha,\beta}|_{\mathbb{A}_j})$ is strictly ergodic, and conjugate to $(\mathbb{Z}_p, T_{1,1})$. When the condition of Theorem 1.2(B) is satisfied, $T_{\alpha,\beta}$ is conjugate to $T_{\alpha,0}$ via a linear conjugacy. For the latter, $\mathbb{Z}_p$ admits a partitions consisting of $T_{\alpha,0}$-invariant sets $p^n\mathbb{U}$ ($n \geqslant 0$). It is easy to see that all the subsystems $(p^n\mathbb{U}, T_{\alpha,0}|_{p^n\mathbb{U}})$ are conjugate. To analyze the subsystem $(\mathbb{U}, T_{\alpha,0}|_{\mathbb{U}})$, we follow Coelho and Parry by using the direct product decomposition $\mathbb{U} = \mathbb{V} \cdot \mathbb{U}_1$. Indeed this is precisely the case studied by Coelho and Parry in [1].

The proof of Theorem 1.3 is similar to that of Theorem 1.2. However, in this case, we have $\mathbb{U} = \mathbb{U}_1$, and we need decompose $\mathbb{U}$ into $\{\pm 1\} \cdot \mathbb{U}_2$. The case $p = 2$ is usually not studied. It is actually more complicated, due to the above mentioned reason.

Theorem 1.4 is a consequence of Theorem 1.2.

Acknowledgements

A.H. Fan was partially supported by the program of Changjiang Scholarship. J.Y. Yao would like to thank the National Natural Science Foundation of China and the Morningside Center of Mathematics (CAS) for partial financial support.

References

[1] Z. Coelho, W. Parry, Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers, in: Amer. Math. Soc. Transl. Ser. 2, vol. 202, Amer. Math. Soc., Providence, RI, 2001, pp. 51–70.

[2] A. Khrennikov, K.-O. Lindahl, M. Gundlach, Ergodicity in the p-adic framework, in: Operator Methods in Ordinary and Partial Differential Equations, Stockholm, 2000, in: Oper. Theory Adv. Appl., vol. 132, Birkhäuser, 2002, pp. 245–251.

[3] J.-P. Serre, A Course in Arithmetic, Grad. Texts in Math., vol. 7, Springer-Verlag, 1973. See also Cours d'arithmétique, Paris PUF, 1970.

[4] P. Walters, An Introduction to Ergodic Theory, Grad. Texts in Math., vol. 79, Springer-Verlag, 1982.