MINIMAL POLYNOMIAL DYNAMICS ON THE SET OF 3-ADIC INTEGERS

FABIEN DURAND AND FRÉDÉRIC PACCAUT

Abstract. In this paper are characterized the polynomials, in terms of their coefficients, that have all their orbits dense in the set of 3-adic integers $\mathbb{Z}_3$.

1. Introduction

The study of dynamical systems on $\mathbb{Z}_p$ or $\mathbb{Q}_p$ is now developing a lot [1, 3, 4, 6, 7]. It is sometimes guided by or leading to applications in physics, cognitive science and cryptography [2, 8]. For example, in the theory of pseudo random number generators, it is usefull to have a map, defined on the integers, giving rise to large cycles modulo n for a given integer n. When n is a power of a prime, good candidates are minimal maps in the set of p-adic integers (that is maps with all their orbits dense). Namely, these minimal maps, whenever polynomial, have only one cycle with maximal length modulo p^n for every n. The point is: how to find such a minimal map or decide if a given polynomial map is minimal ?
There is a complete characterization of minimal polynomial maps (with a different vocabulary) for $p = 2$ in [11] and necessary conditions on the Mahler coefficients of 1-Lipschitz maps to be minimal are given in [1]. Complete results also exist for affine maps (see [4] and [7] where the dynamics are also studied when non minimal) and for polynomials of degree 2 for all prime p [9]. But a complete description of minimal polynomials in $\mathbb{Z}_p$ in terms of their coefficients seems to be a much harder task. Here we give this description for $p = 3$.
First, we give definitions concerning p-adic analysis and dynamical systems. In Section 3, we develop the main properties of the dynamics of a compatible map (a map that preserves congruences) on the set of p-adic integers. In particular, we prove that an onto compatible map is minimal if and only if it is conjugated to the odometer in base p. Section 4 is devoted to the characterization of minimality for polynomials. In this section, we have reorganized ideas of [5] and rewritten a proof from [11] so as to develop a strategy to deal with $\mathbb{Z}_2$ and $\mathbb{Z}_3$. We hope this strategy will also apply to $\mathbb{Z}_p$ for $p > 3$.

2. Some definitions

2.1. **p-adic integers and compatible maps.** Let p be a prime number. We endow $\mathbb{Z}/p^n\mathbb{Z}$ with the discrete topology and $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ with the product topology. Let $\varphi_n : \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$, be the canonical homomorphisms. We call $\mathbb{Z}_p$ the projective limit of $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$. This limit can be seen as

2000 Mathematics Subject Classification: Primary 37E99, Secondary 11S85

$$\mathbb{Z}_p = \left\{ (x_n)_n \in \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}; \varphi_n(x_{n+1}) = x_n \right\}$$

which is a compact subset of $\prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ (see [13]). The canonical projections are $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$. We of course have $\varphi_n \circ \pi_{n+1} = \pi_n$.
Let $x = (x_n) \in \mathbb{Z}_p$ and $y = (y_n) \in \mathbb{Z}_p$. Then $(x_n + y_n)_n$ and $(x_n.y_n)_n$ are also elements of $\mathbb{Z}_p$; this defines the addition $x + y$ and the multiplication $x.y$ in $\mathbb{Z}_p$. It can be checked that with these operations $\mathbb{Z}_p$ is a topological ring.
As a topological space $\mathbb{Z}_p$, is a Cantor set (a compact metric space with no isolated point and a countable base of its topology consisting of clopen sets). More precisely, one can prove that it is homeomorphic to $\prod_{n\in\mathbb{N}}\{0, 1, \dots, p-1\}$ endowed with the infinite product of the discrete topologies.
Through this homeomorphism, a point $x = (x_n)_n$ in $\mathbb{Z}_p$ can be represented by $x = x'_0 + x'_1 p + x'_2 p^2 + \dots$ with $x'_i \in \{0, 1, \dots, p-1\}$ and $x_i = x'_0 + x'_1 p + \dots + x'_i p^i$. In this way, $\mathbb{Z}/p^n\mathbb{Z}$ can be viewed as a subset of $\mathbb{Z}_p$:

$$\mathbb{Z}/p^n\mathbb{Z} = \{x \in \mathbb{Z}_p, \forall i \geqslant n, x'_i = 0\}.$$

Thereofore, when no confusion is possible, we will consider an element $x \in \mathbb{Z}/p^n\mathbb{Z}$ as an element $x = x'_0 + x'_1 p + x'_2 p^2 + \dots + x'_i p^i$ of $\mathbb{Z}_p$ with $i \leq n-1$. By definition, $|x|_p = p^{-\min\{i, x'_i \neq 0\}}$ is the p-adic norm of x (with $|0|_p = 0$). Each set $x + p^k\mathbb{Z}_p$ ($x \in \mathbb{Z}_p, k \in \mathbb{N}$) is a clopen ball of radius p^{-k} and for each k, $\mathbb{Z}_p$ is the union of p^k balls of radius p^{-k}.
The Haar measure, the unique translation invariant probability measure on $\mathbb{Z}_p$, gives measure p^{-k} to any ball of radius p^{-k}. This measure will be denoted by μ_p.
The following lemma will be extensively used in this paper. The proof is left to the reader.

Lemma 1. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a function. Then, the following are equivalent.*

(1) *For every n, if $\pi_n(x) = \pi_n(y)$ then $\pi_n(f(x)) = \pi_n(f(y))$;*
(2) *For every x and y in $\mathbb{Z}_p$, $|f(y) - f(x)|_p \leq |y - x|_p$;*
(3) *For every n and all $x \in \mathbb{Z}_p$, $f(x + p^n\mathbb{Z}_p) \subset f(x) + p^n\mathbb{Z}_p$;*
(4) *For every n, there exists a unique map $f_{/n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ satisfying*

$$\pi_n \circ f = f_{/n} \circ \pi_n. \tag{2.1}$$

Moreover we have the following other commuting relation:

$$f_{/n} \circ \varphi_n = \varphi_n \circ f_{/n+1}. \tag{2.2}$$

$$\begin{tikzcd}
\mathbb{Z}_p \arrow[rrr, "f"] \arrow[ddd, "\pi_n"'] \arrow[dr, "\pi_{n+1}"] & & & \mathbb{Z}_p \arrow[ddd, "\pi_n"] \arrow[dl, "\pi_{n+1}"'] \\
& \mathbb{Z}/p^{n+1}\mathbb{Z} \arrow[r, "f_{/n+1}"] \arrow[ddl, "\varphi_n"'] & \mathbb{Z}/p^{n+1}\mathbb{Z} \arrow[ddr, "\varphi_n"] & \\
& & & \\
\mathbb{Z}/p^n\mathbb{Z} \arrow[rrr, "f_{/n}"] & & & \mathbb{Z}/p^n\mathbb{Z}
\end{tikzcd}$$

Definition 2. A *compatible map* $f : \mathbb{Z}_p \to \mathbb{Z}_p$ is a map satisfying one of the assertions of Lemma 1.

Note that compatible maps are exactly 1-Lipschitz maps. This terminology can be found in [1]. In the sequel, whenever f is a compatible map, $f_{/n}$ will always denote the map defined in Lemma 1.

Proposition 3. *Any polynomial whose coefficients belong to $\mathbb{Z}_p$ is compatible.*

2.2. **Dynamical systems.** Let X be a compact metric space and $T : X \to X$ be a homeomorphism. The couple (X, T) is called a topological dynamical system. Let $\mathcal{B}$ be the Borel σ-algebra of X and μ a probability measure defined on $\mathcal{B}$.
A set $A \in \mathcal{B}$ is called invariant by T if $T^{-1}A = A$. We say that μ is invariant by T if, for every set $A \in \mathcal{B}$, $\mu(T^{-1}A) = \mu(A)$. The dynamical stystem (X, T) is called ergodic for μ if for every invariant set $A \in \mathcal{B}$, $\mu(A) = 0$ or $\mu(X \setminus A) = 0$. It is called minimal if $A = \emptyset$ or $A = X$ whenever A is a closed invariant set. It is equivalent to every orbit being dense in X. It is called uniquely ergodic if it has only one invariant ergodic probability measure. Two topological dynamical systems (X, T) and (Y, S) are called conjugate if there exists a homeomorphism $\Psi : X \to Y$ such that $\Psi \circ T = S \circ \Psi$.

3. Dynamics of compatible maps in $\mathbb{Z}_p$

In this section we give dynamical properties of compatible maps. These are known results but we give the proofs for the sake of completeness and a better understanding of the next section.

Proposition 4. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a compatible map. The following are equivalent :*

1. *f is onto;*
2. *f is an isometry;*
3. *for all $n \in \mathbb{N}$, $f_{/n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ (defined in Lemma 1) is bijective;*
4. *f preserves the Haar measure.*

Proof. (1) $\implies$ (2) : Let f be onto. Let us show that for all $x \in \mathbb{Z}_p$ and all $n \in \mathbb{N}$, $f(x + p^n\mathbb{Z}_p) = f(x) + p^n\mathbb{Z}_p$ (we already have one inclusion because of the compatibility of f). By contradiction, suppose it is not true : there exist $x \in \mathbb{Z}_p$, $n \in \mathbb{N}$, and $z \in \mathbb{Z}_p$ with $z \in f(x) + p^n\mathbb{Z}_p \setminus f(x + p^n\mathbb{Z}_p)$. Then $f(x) + p^n\mathbb{Z}_p = z + p^n\mathbb{Z}_p$.

As f is onto, there exists $y \in \mathbb{Z}_p$ with $z = f(y)$ and $y \notin x + p^n\mathbb{Z}_p$. This implies $(x + p^n\mathbb{Z}_p) \cap (y + p^n\mathbb{Z}_p) = \emptyset$. We can write

$$\mathbb{Z}_p = (x + p^n\mathbb{Z}_p) \cup (y + p^n\mathbb{Z}_p) \cup \bigcup_{i\in\{0,\ldots,p^n-1\}, i\neq x, i\neq y} (i + p^n\mathbb{Z}_p)$$

and, using the compatibility of f,

$$f(\mathbb{Z}_p) = \mathbb{Z}_p \subset (z + p^n\mathbb{Z}_p) \cup \bigcup_{i\in\{0,\ldots,p^n-1\}, i\neq x, i\neq y} (f(i) + p^n\mathbb{Z}_p)$$

which means that at least one ball of radius p^{-n} is lacking in $\mathbb{Z}_p$.
$(2) \Longrightarrow (3)$: As $\mathbb{Z}/p^n\mathbb{Z}$ is finite, it suffices to show that $f_{/n}$ is one-to-one. Let a, b be two different elements of $\mathbb{Z}/p^n\mathbb{Z}$ such that $f_{/n}(a) = f_{/n}(b)$. We can consider a and b as elements of $\mathbb{Z}_p$. This implies that $f(a) - f(b) \in p^n\mathbb{Z}_p$. Consequently, $\frac{1}{p^{n-1}} \leq |a - b|_p = |f(a) - f(b)|_p \leq \frac{1}{p^n}$, a contradiction. Hence $f_{/n}$ is bijective.
$(3) \Longrightarrow (4)$: Let us prove that for all $n \in \mathbb{N}$, any $i \in \mathbb{Z}/p^n\mathbb{Z}$, we have

$$f^{-1}(i + p^n\mathbb{Z}_p) = {f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p$$

where ${f_{/n}}^{-1}(i)$ is reduced to one point as $f_{/n}$ is bijective. This will do the job as this will imply

$$\mu_p(f^{-1}(i + p^n\mathbb{Z}_p)) = \mu_p({f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p) = \frac{1}{p^n} = \mu_p(i + p^n\mathbb{Z}_p)$$

First inclusion : using compatibility, $f({f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p) \subset f({f_{/n}}^{-1}(i)) + p^n\mathbb{Z}_p = i + p^n\mathbb{Z}_p$ and so ${f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p \subset f^{-1}(f({f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p)) \subset f^{-1}(i + p^n\mathbb{Z}_p)$.
For the other inclusion, let $x \in f^{-1}(i + p^n\mathbb{Z}_p)$. We have $f(x) \in i + p^n\mathbb{Z}_p$. Let $x_n = \pi_n(x)$. Using compatibility, we have $f(x) \in f(x_n + p^n\mathbb{Z}_p) \subset f_{/n}(x_n) + p^n\mathbb{Z}_p$. Hence $f(x)$ is a point common to the two balls with the same radius $f_{/n}(x_n) + p^n\mathbb{Z}_p$ and $i + p^n\mathbb{Z}_p$. This implies that both balls have the same center, so $i = f_{/n}(x_n)$ and $x \in {f_{/n}}^{-1}(i) + p^n\mathbb{Z}_p$.
$(4) \Longrightarrow (1)$: By contradiction, suppose that there exists $x \in \mathbb{Z}_p \setminus f(\mathbb{Z}_p)$. Let us show there exists n such that $x + p^n\mathbb{Z}_p \subset \mathbb{Z}_p \setminus f(\mathbb{Z}_p)$. If it is not the case, for all $n \in \mathbb{N}$ there exists $x_n \in (x + p^n\mathbb{Z}_p) \cap f(\mathbb{Z}_p)$ and y_n with $x_n = f(y_n)$ and $|f(y_n) - x|_p \leq p^{-n}$. By compacity one can suppose that (y_n) converges to some $y \in \mathbb{Z}_p$ and, thus, that $x = f(y)$. This contradicts our assumption.
To end remark that $\mu_p(f(\mathbb{Z}_p)) = \mu_p(f^{-1}(f(\mathbb{Z}_p))) = \mu_p(\mathbb{Z}_p) = 1$ which is absurd because a ball $x + p^n\mathbb{Z}_p$ (which has a measure p^{-n}) is lacking in $f(\mathbb{Z}_p)$. □

Now we deal with minimality of maps in $\mathbb{Z}_p$. Let T be the translation in $\mathbb{Z}_p$:

$$\begin{array}{rccc} T: & \mathbb{Z}_p & \to & \mathbb{Z}_p \\ & x & \mapsto & x+1 \end{array}$$

It is sometimes called odometers in base $(p^n)_n$ ([10]).

Lemma 5. *Let $n \in \mathbb{N}$ and $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. Then g is minimal if and only if:*

$$\begin{cases} \forall x \in \mathbb{Z}/n\mathbb{Z}, g^n(x) = x, \text{ and }, \\ \forall x \in \mathbb{Z}/n\mathbb{Z}, g^k(x) = x \Longrightarrow k \equiv 0 \ [n]. \end{cases}$$

Proof. The proof is easy and left to the reader. □

A *cycle* for a map $h : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is a finite sequence $(x_k)_{0\leq k\leq K-1}$ such that for every $i \in \{0, \dots, K-2\}$, $x_{i+1} = h(x_i)$, $h(x_{K-1}) = x_0$ and $\#\{x_k; 0 \leq k \leq K-1\} = K$. It is a *full-cycle* for h if $K = p^n$.

Theorem 6. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be an onto compatible map. The five following propositions are equivalent:*

(1) *f is minimal;*
(2) *for all n, $f_{/n}$ has a full-cycle in $\mathbb{Z}/p^n\mathbb{Z}$;*
(3) *f is conjugate to the translation $T(x) = x + 1$ on $\mathbb{Z}_p$;*
(4) *f is uniquely ergodic;*
(5) *f is ergodic for the Haar measure.*

Proof. (1) $\Longrightarrow$ (2): First note that as f is onto, for every n, $f_{/n}$ is bijective. By contradiction, suppose that $f_{/n}$ does not have a full-cycle in $\mathbb{Z}/p^n\mathbb{Z}$ for some n. Then, as $f_{/n}$ is bijective, it has several cycles and there exists a proper subset A of $\mathbb{Z}/p^n\mathbb{Z}$ such that $f_{/n}(A) = A$. Then $A + p^n\mathbb{Z}_p$ is a non empty closed invariant proper subset of $\mathbb{Z}_p$ and f is not minimal.
(2) $\Longrightarrow$ (3): We need to find a conjugacy $\Psi : \mathbb{Z}_p \to \mathbb{Z}_p$ such that

$$\Psi \circ f = T \circ \Psi = \Psi + 1.$$

Actually, we will look for a compatible conjugacy Ψ. Hence we only need to define maps $\psi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ such that $\psi_n \circ \varphi_n = \varphi_n \circ \psi_{n+1}$ and $\psi_n \circ f_{/n} = T_{/n} \circ \psi_n$. Indeed, defining $\Psi_n = \pi_n^{-1} \circ \psi_n \circ \pi_n$ for any n, one can check that $(\Psi_n)_n$ uniformly converges to a conjugacy Ψ we are looking for.
Let us fix $n \in \mathbb{N}$. As $f_{/n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ is onto and has only one cycle, it has a full-cycle, and thus $(\mathbb{Z}/p^n\mathbb{Z}, f_{/n})$ is minimal. Consequently, it is sufficient to define ψ_n on the orbit of 0, which is a dense orbit. Notice that in this case, dense orbit only means that the orbit goes through each point of $\mathbb{Z}/p^n\mathbb{Z}$.
For all $n \in \mathbb{N}$ and $k \in \{1, \dots, p^n - 1\}$ we set

$$\psi_n(0) = 0 \text{ and } \psi_n(f_{/n}^k(0)) = k.$$

Hence, $\psi_n \circ f_{/n} = T_{/n} \circ \psi_n$ for all $n \in \mathbb{N}$.
Let us now check the compatibility condition $\psi_n \circ \varphi_n = \varphi_n \circ \psi_{n+1}$, that is to say, if $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$:

$$\forall n \in \mathbb{N}, \psi_{n+1}(x_{n+1}) \equiv \psi_n(x_n)\ [p^n].$$

As x_n and x_{n+1} belong to, respectively, $\mathbb{Z}/p^n\mathbb{Z}$ and $\mathbb{Z}/p^{n+1}\mathbb{Z}$, there exist $0 \leq k_n < p^n$ and $0 \leq k_{n+1} < p^{n+1}$ such that $x_n = f_{/n}^{k_n}(0)$ and $x_{n+1} = f_{/n+1}^{k_{n+1}}(0)$. Consequently, $f_{/n+1}^{k_{n+1}}(0) \equiv f_{/n}^{k_n}(0)\ [p^n]$ because $\varphi_n(x_{n+1}) = x_n$. Moreover, f being compatible, $f_{/n+1}^{k_{n+1}}(0) \equiv f_{/n}^{k_{n+1}}(0)\ [p^n]$. This implies $f_{/n}^{k_{n+1}}(0) \equiv f_{/n}^{k_n}(0)\ [p^n]$ and, using Lemma 5, $k_{n+1} - k_n = 0$ in $\mathbb{Z}/p^n\mathbb{Z}$ which is equivalent to $\psi_{n+1}(f_{/n+1}^{k_{n+1}}(0)) \equiv \psi_n(f_{/n}^{k_n}(0))\ [p^n]$, that is to say $\psi_{n+1}(x_{n+1}) \equiv \psi_n(x_n)\ [p^n]$.
(3) $\Longrightarrow$ (4): By definition of the Haar measure.
(4) $\Longrightarrow$ (5): Suppose that f is uniquely ergodic. Using Proposition 4, f being an isometry, the Haar measure μ_p is invariant. Thus it is the only invariant ergodic probability measure.
(5) $\Longrightarrow$ (1): Let x, y in $\mathbb{Z}_p$ and $\epsilon > 0$. It suffices to show that for some k, $|f^k(x) - y|_p < \epsilon$. Let n such that $p^{-n} < \varepsilon/2$. As f is ergodic for the Haar measure, there

exists some $k > 0$ such that $\mu_p(f^k(x+p^n\mathbb{Z}_p) \cap (y+p^n\mathbb{Z}_p)) > 0$. As f is compatible $f^k(x+p^n\mathbb{Z}_p) \subset f^k(x)+p^n\mathbb{Z}_p$ and thus $(f^k(x)+p^n\mathbb{Z}_p) \cap (y+p^n\mathbb{Z}_p) \neq \emptyset$. Therefore these two balls coincide and $f^k(x)$ and y lie in the same ball of radius p^{-n}. Then $|f^k(x) - y|_p \leq 2p^{-n} \leq \varepsilon$. This concludes the proof. □

It is well known that minimal isometries on topological groups are conjugate to group rotations [10]. Here, we obtain a little more, namely we prove that the conjugacy goes from $\mathbb{Z}_p$ to $\mathbb{Z}_p$.

4. Minimality for polynomials

4.1. **Some preliminary results.** In this section, we are interested in polynomials $f : \mathbb{Z}_p \to \mathbb{Z}_p$ with coefficients in $\mathbb{Z}_p$. For the sequel, we need some definitions inspired by [5]. Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a polynomial. Let $g_n = f^{p^n}$.
Suppose there exists a finite sequence $x_0, \dots, x_{p^n-1}$ in $\mathbb{Z}_p$ so that $f_{/n}$ has a full cycle $\pi_n(x_0), \dots, \pi_n(x_{p^n-1})$ in $\mathbb{Z}/p^n\mathbb{Z}$. Then, $g_n(x_0)$ belongs to $x_0+p^n\mathbb{Z}_p$. Consequently $\frac{g_n(x_0)-x_0}{p^n}$ belongs to $\mathbb{Z}_p$. Using Taylor's expansion, for $n \geqslant 1$, we get for all $z \in \mathbb{Z}_p$:

$$g_n(x_0 + p^n z) \in x_0 + p^n \left(\frac{g_n(x_0) - x_0}{p^n}\right) + p^n \left(g_n\right)'(x_0)z \; + p^{2n}\mathbb{Z}_p. \tag{4.1}$$

We set

$$\alpha_n(x_0) = (g_n)'(x_0),\ \beta_n(x_0) = \frac{g_n(x_0) - x_0}{p^n} \text{ and}$$
$$\begin{array}{rccc} \Phi_n(x_0) : & \mathbb{Z}_p & \to & \mathbb{Z}_p \\ & z & \mapsto & \alpha_n(x_0)z + \beta_n(x_0). \end{array}$$

We have

$$g_n(x_0 + p^n z) \in x_0 + p^n\Phi_n(x_0)(z) + p^{2n}\mathbb{Z}_p. \tag{4.2}$$

Then,

$$\begin{aligned} p^n\beta_n(f(x_0)) &= g_n(f(x_0)) - f(x_0) = f(g_n(x_0)) - f(x_0) \\ &\equiv f(x_0 + p^n\Phi_n(x_0)(0)) - f(x_0) \equiv p^n\Phi_n(x_0)(0)f'(x_0)\ [p^{2n}] \end{aligned}$$

Hence

$$\beta_n(f(x_0)) \equiv \beta_n(x_0)f'(x_0)\ [p^n]. \tag{4.3}$$

Lemma 7. *Let $a, b \in \mathbb{Z}/p\mathbb{Z}$, and*

$$\begin{array}{rccc} h : & \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/p\mathbb{Z} \\ & t & \mapsto & b + at \end{array}$$

then $(\mathbb{Z}/p\mathbb{Z}, h)$ is minimal if and only if $a = 1$ and $b \neq 0$.

Proof. The proof is easy and left to the reader. □

Lemma 8. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a polynomial and $n \geqslant 1$ be such that $(\mathbb{Z}/p^n\mathbb{Z}, f_{/n})$ is minimal. Then, the following are equivalent :*

(1) *$(\mathbb{Z}/p^{n+1}\mathbb{Z}, f_{/n+1})$ is minimal;*
(2) *For all $x \in \mathbb{Z}_p$, $f^{p^n}(x) - x \notin p^{n+1}\mathbb{Z}_p$ and $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$;*
(3) *There exists $x \in \mathbb{Z}_p$ such that $f^{p^n}(x) - x \notin p^{n+1}\mathbb{Z}_p$ and $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$.*

Proof. Suppose $(\mathbb{Z}/p^{n+1}\mathbb{Z}, f_{/n+1})$ is minimal. Let $x \in \mathbb{Z}_p$. If $f^{p^n}(x) - x$ belongs to $p^{n+1}\mathbb{Z}_p$, then $f_{/n+1}$ has a cycle of length p^n, which is not possible. From (4.2) we see that, $(\mathbb{Z}/p^{n+1}\mathbb{Z}, f_{/n+1})$ being minimal, $\Phi_n(x)_{/1} : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ should be minimal. Lemma 7 implies $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$. Hence (1) implies (2). Suppose (2). Then, $\Phi_n(x)_{/1}$ is minimal for all $x \in \mathbb{Z}_p$. We deduce with (4.2) that $(\mathbb{Z}/p^{n+1}\mathbb{Z}, f_{/n+1})$ is minimal : (2) implies (1). It is trivial that (2) gives (3). Let us show that (3) implies (2). Suppose there exists $x \in \mathbb{Z}_p$ such that $f^{p^n}(x) - x \notin p^{n+1}\mathbb{Z}_p$ and $\left(f^{p^n}\right)'(x) \in 1 + p\mathbb{Z}_p$. Let $y \in \mathbb{Z}_p$. Then, $(f^i_{/n}(y))_{0 \le i \le p^n - 1}$ is a full cycle in $\mathbb{Z}/p^n\mathbb{Z}$. Hence,

$$1 \equiv \left(f^{p^n}\right)'(x) \equiv \prod_{i=0}^{p^n-1} f'\left(f^i(x)\right) \equiv \prod_{i=0}^{p^n-1} f'(i) \equiv \prod_{i=0}^{p^n-1} f'\left(f^i(y)\right) \equiv \left(f^{p^n}\right)'(y)\ [p^n].$$

We conclude using (4.3). □

Proposition 9. *Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$ be a polynomial, then $(\mathbb{Z}_p, f)$ is minimal if and only if $(\mathbb{Z}/p^\delta\mathbb{Z}, f_{/\delta})$ is minimal, where $\delta = 2$ if $p > 3$ and $\delta = 3$ if $p \in \{2, 3\}$.*

Proof. The necessary condition is due to Theorem 6. Suppose $(\mathbb{Z}/p^\delta\mathbb{Z}, f_{/\delta})$ is minimal, i.e $f_{/\delta} : \mathbb{Z}/p^\delta\mathbb{Z} \to \mathbb{Z}/p^\delta\mathbb{Z}$ has one full-cycle. From Theorem 6, it is sufficient to prove that, for any n, $f_{/n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ has a full-cycle. Remark that, as the number of cycles in $\mathbb{Z}/p^n\mathbb{Z}$ is non decreasing with n, this implies that $f_{/n}$ has only one cycle for all $n \le \delta$.
Let us proceed by induction on n for the other cases. Suppose $(\mathbb{Z}/p^n\mathbb{Z}, f_{/n})$ is minimal. From Lemma 8 it suffices to prove that $\beta_n(0) \notin p\mathbb{Z}_p$ and $\alpha_n(0) \in 1 + p\mathbb{Z}_p$. As δ is greater than 2, Lemma 8 implies that $\alpha_{n-1}(0)$ belongs to $1+p\mathbb{Z}_p$ and $\beta_{n-1}(0)$ does not belong to $p\mathbb{Z}_p$. We set $\alpha_k = \alpha_k(0)$, $\beta_k = \beta_k(0)$ and $\Phi_k = \Phi_k(0)$ for all k. In order to conclude, we establish relations between (α_n, β_n) and $(\alpha_{n-1}, \beta_{n-1})$. Remark that $g_{n+1} = g_n^p$ so, using (4.2),

$$\alpha_n = (g_{n-1}^p)'(0) = \prod_{i=0}^{p-1} g'_{n-1}(g^i_{n-1}(0)) \in g'_{n-1}(0)^p + p^{n-1}\mathbb{Z}_p \subset 1 + p\mathbb{Z}_p. \tag{4.4}$$

For β_n the situation is not so easy. We need to consider three different cases.
Let us first consider the case $p = 3$ and $n \geqslant 3$. We have

$$\beta_n = \frac{g_n(0)}{p^n} = \frac{g^p_{n-1}(0)}{p^n},\ g^p_{n-1}(0) \in \Phi^p_{n-1}(0)p^{n-1} + p^{2(n-1)}\mathbb{Z}_p \text{ and}$$

$$\Phi^p_{n-1}(0) = \beta_{n-1}\left(1 + \alpha_{n-1} + \ldots + \alpha^{p-1}_{n-1}\right) \in \beta_{n-1}p + p^2\mathbb{Z}_p.$$

Hence $\beta_n \in \beta_{n-1} + p\mathbb{Z}_p$, which conclude the proof for $p = 3$.

Let us now consider the case $p=2$ and $n\geqslant 3$. Then $n-2\geqslant 1$ and $(\mathbb{Z}/p^{n-2}\mathbb{Z}, f_{/n-2})$ is minimal. From Lemma 8 we obtain $\alpha_{n-2}=1+pz$ for some $z\in\mathbb{Z}_p$. Consequently, proceeding as in (4.4),

$$\begin{aligned}\alpha_{n-1} &= \alpha_{n-2}\alpha_{n-2}(g_{n-2}(0)) = \alpha_{n-2}\left(\alpha_{n-2}+p^{n-2}z'g''_{n-2}(0)\right)\\ &= 1+2pz+p^2z^2+\alpha_{n-2}p^{n-2}z'g''_{n-2}(0)\in 1+p^2\mathbb{Z}_p,\end{aligned}$$

for some $z'\in\mathbb{Z}_p$, because $g''_{n-2}(x)$ belongs to $p\mathbb{Z}_p$ for all $x\in\mathbb{Z}_p$. Then, doing as in the previous case, we deduce that $\beta_n\in\beta_{n-1}+p\mathbb{Z}_p$.
Let us end with the case $p\geqslant 5$ and $n\geqslant 2$. Note that what we did in the case $p=3$ also holds here. Hence we just have to consider the case $n=2$ and thus to prove that $\beta_2\in\beta_1+p\mathbb{Z}_p$. We set $\gamma=g''_1(0)/2$ (as $p\geqslant 5$, it belongs to $\mathbb{Z}_p$). By induction, as observed in [5], we can prove that

$$g_1^i(0)\equiv p\beta_1\sum_{j=0}^{i-1}\alpha_1^j+p^2\gamma\beta_1^2\sum_{j=0}^{i-2}\alpha_1^{i-2-j}\left(1+\alpha_1+\cdots+\alpha_1^j\right)^2 \quad [p^3],$$

hence

$$g_1^p(0)\equiv p^2\beta_1+p^2\gamma\beta_1^2\frac{(p-1)p(2p-1)}{6}=p^2\beta_1 \quad [p^3]. \tag{4.5}$$

This achieves the proof. □

Remark 10. The value of δ obtained in Proposition 9 cannot be smaller.
For $p=2$, let $f(x)=1+3x+2x^3$. The map $f_{/2}$ has a full cycle 0,1,2,3 but $(\mathbb{Z}_2,f)$ is not minimal : $f_{/3}$ has a cycle 0,1,6,3.
For $p=3$, let $f(x)=1+4x+4x^3+2x^5$. The map $f_{/2}$ has a full cycle 0,1,2,6,7,5,3,4,8 but $(\mathbb{Z}_3,f)$ is not minimal, $f_{/3}$ has a cycle 0,1,11,15,7,23,3,13,17.

Remark 11. Let f be a polynomial with $f(0)=a_0$. If f is minimal, then $a_0\not\equiv 0$ $[p]$, otherwise 0 is a fixed point modulo p for f. Let $g(x)=\frac{1}{a_0}f(a_0x)$. Then $g(0)=1$ and $(\mathbb{Z}_p,f)$ and $(\mathbb{Z}_p,g)$ are conjugate. Therefore, f is minimal if and only if g is minimal. Hence we will restrict in the following to polynomials f with $f(0)=1$.

4.2. **Characterization for $p=2$.** Using the previous ideas, we can characterize the polynomials that are minimal in $\mathbb{Z}_2$. The result is not new (see for example [11]) but the method described here is interesting as it will also apply to $\mathbb{Z}_3$.
Let $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+1$ be a polynomial of degree d. We set

$$A_0=\textstyle\sum_{i\in 2\mathbb{Z}, i\neq 0}a_i,\quad A_1=\sum_{i\in 1+2\mathbb{Z}}a_i.$$

Lemma 12. *The dynamical system $(\mathbb{Z}/2\mathbb{Z}, f_{/1})$ is minimal if and only if*

$$A_0+A_1\in 1+2\mathbb{Z}_2.$$

Proof. If comes from the fact that $f_{/1}(0)=1$ and $f_{/1}(1)=1+A_0+A_1$. Hence $f_{/1}$ is minimal if and only if $1+A_0+A_1\equiv 0$ $[2]$. □

Lemma 13. *The dynamical system $(\mathbb{Z}/4\mathbb{Z}, f_{/2})$ is minimal if and only if*

$$\begin{cases} a_1\equiv 1 \ [2]\\ A_1\equiv 1 \ [2]\\ A_0+A_1\equiv 1 \ [4]\end{cases}$$

Proof. Suppose $(\mathbb{Z}/4\mathbb{Z}, f_{/2})$ minimal, then $(\mathbb{Z}/2\mathbb{Z}, f_{/1})$ is also minimal, therefore $A_0 + A_1 \equiv 1$ [2] (see Lemma 12). In view of Lemma 8, $(\mathbb{Z}/4\mathbb{Z}, f_{/2})$ is minimal if and only if

$$A_0 + A_1 \equiv 1\ [2]\ ,\ (f^2)'(0) \in 1 + 2\mathbb{Z}_2 \text{ and } f^2(0) \in 2\mathbb{Z}_2 \setminus 4\mathbb{Z}_2$$

First, $(f^2)'(0) \equiv f'(0)f'(1) \equiv a_1 \sum_{i\geqslant 1} ia_i \equiv a_1 A_1$ [2], which is equivalent to $a_1 \in 1+2\mathbb{Z}_2$ and $A_1 \in 1+2\mathbb{Z}_2$. Secondly, $f^2(0) = 1 + A_0 + A_1$. We thus get immediately $1 + A_0 + A_1 \not\equiv 0$ [4] and consequently $A_0 + A_1 \equiv 1$ [4]. □

Theorem 14. *The dynamical system $(\mathbb{Z}_2, f)$ is minimal if and only if*

$$\begin{cases} a_1 \equiv 1\ [2] \\ A_1 \equiv 1\ [2] \\ A_0 + A_1 \equiv 1\ [4] \\ 2a_2 + a_1 A_1 \equiv 1\ [4] \end{cases}$$

Proof. Lemma 8 implies that $(\mathbb{Z}_2, f)$ is minimal if and only if

$$(\mathbb{Z}/4\mathbb{Z}, f_{/2}) \text{ is minimal, } (f^4)'(0) \in 1 + 2\mathbb{Z}_2 \text{ and } f^4(0) \in 4\mathbb{Z}_2 \setminus 8\mathbb{Z}_2.$$

First, $(f^4)'(0) \equiv ((f^2)'(0))^2$ [2] so this condition has already been checked. Secondly, using Taylor's expansion, we get

$$f^2(pz) \equiv p(\beta_1 + \alpha_1 z) + p^2 z^2 \frac{(f^2)''(0)}{2}\ [8]$$

and then

$$f^4(0) \equiv 2\beta_1(1 + (f^2)'(0)) + 4\beta_1^2 \frac{(f^2)''(0)}{2}\ [8]$$

with $\beta_1 \equiv 1[2]$ and $1+(f^2)'(0) \equiv 0$ [2]. The condition $f^4(0) \in 4\mathbb{Z}_2 \setminus 8\mathbb{Z}_2$ is therefore equivalent to

$$(f^2)'(0) + (f^2)''(0) \equiv 1\ [4].$$

Using $a_1 \equiv 1$ [2],

$$\begin{aligned} (f^2)'(0) &\equiv a_1 \sum_{i\geqslant 1} ia_i \equiv a_1 \left(\sum_{i\geqslant 0} a_{4i+1} + 2\sum_{i\geqslant 0} a_{4i+2} - \sum_{i\geqslant 0} a_{4i+3} \right)\ [4] \\ &\equiv a_1 \sum_{i\geqslant 0} a_{4i+1} + 2\sum_{i\geqslant 0} a_{4i+2} - a_1 \sum_{i\geqslant 0} a_{4i+3}\ [4]. \end{aligned}$$

Moreover, as $\sum_{i\geqslant 2} i(i-1)a_i \equiv 0$ [2], $a_1^2 \equiv 1$ [2] and $\sum_{i\geqslant 1} ia_i \equiv A_1 \equiv 1$ [2]:

$$\begin{aligned} (f^2)''(0) &= f''(0)f'(1) + (f'(0))^2 f''(1) = 2a_2 \sum_{i\geqslant 1} ia_i + a_1^2 \sum_{i\geqslant 2} i(i-1)a_i \\ &\equiv 2a_2 + \sum_{i\geqslant 2} i(i-1)a_i \equiv \sum_{i\geqslant 3} i(i-1)a_i\ [4] \\ &\equiv 2\sum_{i\geqslant 1} a_{4i+2} + 2\sum_{i\geqslant 0} a_{4i+3}\ [4]. \end{aligned}$$

This gives, using $2 - a_1 \equiv a_1$ [4]

$$\begin{aligned} (f^2)'(0) + (f^2)''(0) &\equiv 2a_2 + a_1 \sum_{i\geqslant 0} a_{4i+1} + (2 - a_1) \sum_{i\geqslant 0} a_{4i+3}\ [4] \\ &\equiv 2a_2 + a_1 A_1\ [4]. \end{aligned}$$

This achieves the proof. □

These conditions are easily proved to be equivalent to those given in [11]:

$$\begin{cases} a_1 \equiv 1 \ [2] \\ A_1 - a_1 \equiv 2a_2 \ [4] \\ A_0 - a_2 \equiv a_1 + a_2 - 1 \ [4]. \end{cases}$$

Corollary 15. *Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ be a polynomial of degree d. The dynamical system $(\mathbb{Z}_2, f)$ is minimal if and only if*

$$\begin{cases} a_1 \equiv 1 \ [2] \\ A'_1 \equiv 1 \ [2] \\ A'_0 + A'_1 \equiv 1 \ [4] \\ 2a_2 a_0 + a_1 A'_1 \equiv 1 \ [4] \end{cases}$$

where

$$A'_0 = \sum_{i \in 2\mathbb{Z}, i \neq 0} a_i a_0^{i-1} \quad \text{and} \quad A'_1 = \sum_{i \in 1+2\mathbb{Z}} a_i a_0^{i-1}.$$

4.3. **Characterization for $p = 3$.** Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + 1$ be a polynomial of degree d. We set

$$\begin{array}{ll} A_0 = \sum_{i \in 2\mathbb{Z}, i \neq 0} a_i, & A_1 = \sum_{i \in 1+2\mathbb{Z}} a_i, \\ D_0 = \sum_{i \in 2\mathbb{Z}, i \neq 0} i a_i, & D_1 = \sum_{i \in 1+2\mathbb{Z}} i a_i. \end{array}$$

Lemma 16. *The dynamical system $(\mathbb{Z}/3\mathbb{Z}, f_{/1})$ is minimal if and only if*

$$A_0 \in 3\mathbb{Z}_3 \text{ and } A_1 \in 1 + 3\mathbb{Z}_3.$$

Proof. Suppose f is minimal. We remark that if $x \neq 0$ then $f_{/1}(x) = 1 + A_0 + A_1 x$ and $f_{/1}(0) = 1$. Hence $A_0 + A_1 x \not\equiv 0$ [3] for all $x \not\equiv 0$ [3]. Then, $A_0 \equiv 0$ [3] and $A_1 \equiv 1$ [3]. Consequently $(\mathbb{Z}/3\mathbb{Z}, f_{/1})$ is minimal. The reciprocal is as easy to establish. □

Lemma 17. *The dynamical system $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal if and only if $A_0 \in 3\mathbb{Z}_3$, $A_1 \in 1 + 3\mathbb{Z}_3$ and f fulfils one of the following conditions:*

1. *$D_0 \in 3\mathbb{Z}_3$, $D_1 \in 2 + 3\mathbb{Z}_3$, $a_1 \in 1 + 3\mathbb{Z}_3$ and $A_1 + 5 \notin 9\mathbb{Z}_3$;*
2. *$D_0 \in 3\mathbb{Z}_3$, $D_1 \in 1 + 3\mathbb{Z}_3$, $a_1 \in 1 + 3\mathbb{Z}_3$ and $A_0 + 6 \notin 9\mathbb{Z}_3$;*
3. *$D_1 \in 3\mathbb{Z}_3$, $D_0 \in 1 + 3\mathbb{Z}_3$, $a_1 \in 2 + 3\mathbb{Z}_3$ and $A_1 + 5 \notin 9\mathbb{Z}_3$;*
4. *$D_1 \in 3\mathbb{Z}_3$, $D_0 \in 2 + 3\mathbb{Z}_3$, $a_1 \in 2 + 3\mathbb{Z}_3$ and $A_0 + 6 \notin 9\mathbb{Z}_3$;*

Proof. In Lemma 8 we prove $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal if and only if

$$(\mathbb{Z}/3\mathbb{Z}, f_{/1}) \text{ is minimal, } (f^3)'(0) \in 1 + 3\mathbb{Z}_3 \text{ and } f^3(0) \in 3\mathbb{Z}_3 \setminus 9\mathbb{Z}_3.$$

Suppose $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal. From Lemma 16, $A_0 \in 3\mathbb{Z}_3$ and $A_1 \in 1 + 3\mathbb{Z}_3$. We easily check that $(f^3)'(0) \equiv f'(0)f'(1)f'(2) \equiv a_1(D_1^2 - D_0^2)$ [3]. Hence either $D_0 \in 3\mathbb{Z}_3$ and $D_1 \notin 3\mathbb{Z}_3$ or $D_1 \in 3\mathbb{Z}_3$ and $D_0 \notin 3\mathbb{Z}_3$. Moreover we have $f(0) = 1$, $f^2(0) = 1 + A_0 + A_1$ and

$$
\begin{aligned}
f^3(0) \equiv & 1+\sum_{i=1}^{d} a_i(1+A_0+A_1)^i \equiv 1+\sum_{i=1}^{d} a_i\left((1+A_1)^i+iA_0(1+A_1)^{i-1}\right) && [9]\\
\equiv & 1+\sum_{i=1}^{d} a_i\left(2^i+i2^{i-1}(A_1-1)+iA_0 2^{i-1}\right) && [9]\\
\equiv & 1+\sum_{i=1}^{d} a_i\left((-1)^i+3i(-1)^{i-1}+i(-1)^{i-1}(A_0+A_1-1)\right) && [9]\\
\equiv & 1+A_0-A_1+(A_0+A_1+2)(D_1-D_0) && [9].
\end{aligned}
$$

Consequently, $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal if and only if $A_0 \in 3\mathbb{Z}_3$, $A_1 \in 1+3\mathbb{Z}_3$, $a_1(D_1^2-D_0^2) \in 1+3\mathbb{Z}_3$ and $1+A_0-A_1+(A_0+A_1+2)(D_1-D_0) \in 3\mathbb{Z}_3 \setminus 9\mathbb{Z}_3$. Suppose $D_0 \in 3\mathbb{Z}_3$. Then $a_1 \in 1+3\mathbb{Z}_3$ and

$$
f^3(0) \equiv \begin{cases} 3+2A_0 & [9] \quad \text{if } D_1 \in 1+3\mathbb{Z}_3,\\ 5+A_1 & [9] \quad \text{if } D_1 \in 2+3\mathbb{Z}_3.\end{cases}
$$

Suppose $D_1 \in 3\mathbb{Z}_3$. Then $a_1 \in 2+3\mathbb{Z}_3$ and

$$
f^3(0) \equiv \begin{cases} -1-2A_1 & [9] \quad \text{if } D_0 \in 1+3\mathbb{Z}_3,\\ -6-A_0 & [9] \quad \text{if } D_0 \in 2+3\mathbb{Z}_3.\end{cases}
$$

This achieves the proof. □

Theorem 18. *The dynamical system $(\mathbb{Z}_3, f)$ is minimal if and only if $A_0 \in 3\mathbb{Z}_3$, $A_1 \in 1+3\mathbb{Z}_3$ and f fulfils one of the conditions (1), (2), (3) or (4):*

	D_0 [3]	D_1 [3]	a_1 [3]	
(1)	0	2	1	$A_1+5 \not\equiv 0$ [9] $A_1+5 \not\equiv 3a_2+3\sum_{j\geqslant 0} a_{5+6j}$ [9]
(2)	0	1	1	$A_0+6 \not\equiv 0$ [9] $A_0+6 \not\equiv 6a_2+3\sum_{j\geqslant 0} a_{2+6j}$ [9]
(3)	1	0	2	$A_1+5 \not\equiv 0$ [9] $A_1+5 \not\equiv 6a_2+3\sum_{j\geqslant 0} a_{5+6j}$ [9]
(4)	2	0	2	$A_0+6 \not\equiv 0$ [9] $A_0+6 \not\equiv 3a_2+3\sum_{j\geqslant 0} a_{2+6j}$ [9]

Proof. From Lemma 8 and Proposition 9, we know that $(\mathbb{Z}_3, f)$ is minimal if and only if $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal, $\left(f^9\right)'(0) \in 1+3\mathbb{Z}_3$ and $f^9(0) \notin 3^3\mathbb{Z}_3$. From Lemma 8, as $(\mathbb{Z}/9\mathbb{Z}, f_{/2})$ is minimal, $\left(f^3\right)'(0) \in 1+3\mathbb{Z}_3$. The calculus (4.4) shows that $\left(f^9\right)'(0) \in 1+3\mathbb{Z}_3$. Hence, using Lemma 17, $(\mathbb{Z}_3, f)$ is minimal if and only if f fulfils Conditions (1), (2), (3), (4), of Lemma 17, and $f^9(0) \notin 3^3\mathbb{Z}_3$. But from (4.5) we see that

$$
f^9(0) \equiv 3^2\beta_1 + 3^2\gamma\beta_1^2 5 = 3^2(\beta_1-\gamma) \; [3^3],
$$

where $\beta_1 = \frac{f^3(0)}{3}$ and $\gamma = \frac{\left(f^3\right)''(0)}{2}$. Thus, $f^9(0) \notin 3^3\mathbb{Z}_3$ if and only if $\beta_1 \not\equiv \gamma$ [3]. That is to say

$$2f^3(0) \not\equiv 3\left(f^3\right)''(0)\ [9].$$

We already computed $f^3(0)$ in the proof of Lemma 17. Let us compute $\left(f^3\right)''(0)$:

$$\begin{aligned}
\left(f^3\right)''(0) \equiv & f'(f^2(0))f'(1)f''(0) + f'(f^2(0))f''(1)f'(0)^2 + f''(f^2(0))f'(1)^2f'(0)^2 \\
\equiv & f'(1+A_0+A_1)f'(1)2a_2 + f'(1+A_0+A_1)f''(1) + f''(1+A_0+A_1)\ [3] \\
\equiv & -f'(-1)f'(1)a_2 + f'(-1)f''(1) + f''(-1)\ [3] \\
\equiv & -(D_1^2 - D_0^2)a_2 + (D_1 - D_0)f''(1) + f''(-1)\ [3]
\end{aligned}$$

Moreover, we easily obtain that

$$f''(1) = -\sum_j a_{2+3j} \text{ and } f''(-1) = -\sum_j a_{2+3j}(-1)^j.$$

This gives:

	$2f^3(0)$ [9]	$3\left(f^3\right)''(0)$ [9]
(1) Lemma 17	$2A_1+1$	$6a_2 + 6\sum_{j\geqslant 0} a_{5+6j}$
(2) Lemma 17	$4A_0+6$	$6a_2 + 3\sum_{j\geqslant 0} a_{2+6j}$
(3) Lemma 17	$2A_1+1$	$3a_2 + 6\sum_{j\geqslant 0} a_{5+6j}$
(4) Lemma 17	$4A_0+6$	$3a_2 + 3\sum_{j\geqslant 0} a_{2+6j}$

which gives the conditions :

	Condition
(1) Lemma 17	$A_1 + 5 \not\equiv 3a_2 + 3\sum_{j\geqslant 0} a_{5+6j}$ [9]
(2) Lemma 17	$A_0 + 6 \not\equiv 6a_2 + 3\sum_{j\geqslant 0} a_{2+6j}$ [9]
(3) Lemma 17	$A_1 + 5 \not\equiv 6a_2 + 3\sum_{j\geqslant 0} a_{5+6j}$ [9]
(4) Lemma 17	$A_0 + 6 \not\equiv 3a_2 + 3\sum_{j\geqslant 0} a_{2+6j}$ [9]

This achieves the proof. □

Corollary 19. *Let $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ be a polynomial defined by $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. The dynamical system $(\mathbb{Z}_3, f)$ is minimal if and only if $A_0' \in 3\mathbb{Z}_3$, $A_1' \in 1 + 3\mathbb{Z}_3$ and f fulfils one of the Conditions (1), (2), (3) or (4):*

	D_0' [3]	D_1' [3]	a_1 [3]	
(1)	0	2	1	$A_1' + 5 \not\equiv 0$ [9] $A_1' + 5 \not\equiv 3a_2a_0 + 3\sum_{j\geqslant 0} a_{5+6j}a_0^{4+6j}$ [9]
(2)	0	1	1	$A_0' + 6 \not\equiv 0$ [9] $A_0' + 6 \not\equiv 6a_2a_0 + 3\sum_{j\geqslant 0} a_{2+6j}a_0^{1+6j}$ [9]
(3)	1	0	2	$A_1' + 5 \not\equiv 0$ [9] $A_1' + 5 \not\equiv 6a_2a_0 + 3\sum_{j\geqslant 0} a_{5+6j}a_0^{4+6j}$ [9]
(4)	2	0	2	$A_0' + 6 \not\equiv 0$ [9] $A_0' + 6 \not\equiv 3a_2a_0 + 3\sum_{j\geqslant 0} a_{2+6j}a_0^{1+6j}$ [9]

where

$$A'_0 = \sum_{i\in 2\mathbb{Z}, i\neq 0} a_i a_0^{i-1}, \quad A'_1 = \sum_{i\in 1+2\mathbb{Z}} a_i a_0^{i-1},$$
$$D'_0 = \sum_{i\in 2\mathbb{Z}, i\neq 0} i a_i a_0^{i-1}, \quad D'_1 = \sum_{i\in 1+2\mathbb{Z}} i a_i a_0^{i-1}.$$

Corollary 20. *Let $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ be a polynomial defined by $f(x) = a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + 1$. Then, $(\mathbb{Z}_3, f)$ is minimal if and only f satisfies one of the following conditions*

	a_1 [3]	a_2 [3]	a_3 [3]	a_4 [3]	a_5 [3]	
(1)	1	0	1	0	2	$a_1 + a_3 + a_5 \equiv 7$ [9]
(2)	1	0	0	0	0	$a_2 + a_4 \equiv 0$ *or* 6 [9]
(3)	2	1	0	2	2	$a_1 + a_3 + a_5 \equiv 7$ [9]
(4)	2	2	0	1	2	$a_2 + a_4 \equiv 0$ [9]

4.4. **Discussion.** We had planned to address the question of minimality of polynomial dynamics in $\mathbb{Z}_p$ for any prime p. We have no idea if this is tractable or not to get a general condition for all prime numbers $p > 3$. We have obtained sufficient conditions for any p, but they are far from necessary, as we have seen performing simulations. In some sense, it is not surprising since giving conditions on the coefficients to ensure bijectivity of polynomials is already known to be a difficult problem [12].

Acknowledgement

We would like to thank the mathematical department of Vaxjö University, Sweden, where part of this work has been initiated, for its hospitality. We are grateful to Prof. Anashin, Prof. Fan and Prof. Khrennikov for fruitful discussions

References

[1] V. Anashin, *Uniformly distributed sequences of p-adic integers II*, Discrete Math. Appl. **12** (2002), no. 6, 527-590.

[2] V. Anashin, *Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers. Computing mathematics and cybernetics, 2*, J. Math. Sci.**89** (1998) no. 4, 1355-1390.

[3] J. Bryk and C.E. Silva, *Measurable dynamics of simple p-adic polynomials*, Amer. Math. Monthly **112** (2005) no. 3, 212-232.

[4] Z. Coelho and W. Parry, *Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers*, Amer. Math. Soc. Transl. Ser. 2, **202** (2001) American Mathematical Society, 51-70.

[5] D.L. Desjardins and M.E. Zieve, *On the structure of polynomial mappings modulo an odd prime power*, Preprint, http://fr.arXiv.org/abs/math.NT/0103046.

[6] A-H. Fan, L. Liao, Y-F. Wang, D. Zhou, *p-adic repellers in $\mathbb{Q}_p$ are subshifts of finite type*, C. R. Math. Acad. Sci. Paris **344** (2007), no. 4, 219-224.

[7] A-H. Fan, M-T. Li, J-Y. Yao, D. Zhou, *Strict ergodicity of affine p-adic dynamical systems on $\mathbb{Z}_p$*, Adv. Math. **214** (2007), no. 2, 666-700.

[8] A. Y. Khrennikov and M. Nilsson, *P-adic deterministic and random dynamics*, Mathematics and Its Applications **574**, Kluwer Academic Publishers, 2004.

[9] D. E. Knuth, *The art of computer programming, Vol. 2 : Seminumerical algorithms (3rd edition)*, Addison-Wesley Publ. Co, 1998.

[10] P. Kurka, *Topological and symbolic dynamics*, Cours spécialisés, Collection SMF, 2003.

[11] M. V. Larin, *Transitive polynomial transformations of residue class rings*, Discrete Math. Appl. Vol **12** (2002) no. 2, 127-140.

[12] R. Lidl, H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[13] A.M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics 198, Springer, 2000.

Université de Picardie Jules Verne
Laboratoire Amiénois de Mathématiques Fondamentales et Appliquées
CNRS-UMR 6140
33 rue Saint Leu
80039 Amiens Cedex 01
France.
E-mail address: fabien.durand@u-picardie.fr
E-mail address: frederic.paccaut@u-picardie.fr