ARITHMETIC CONVERGENCE OF DOUBLE-ITERATED POLYNOMIALS

Rin Gotou[1]
Department of Mathematics, Osaka University, Osaka, Japan
u661233h@ecs.osaka-u.ac.jp

Received: 7/19/19, Revised: 2/24/22, Accepted: 5/24/22, Published: 6/3/22

Abstract

Let f be a polynomial with integer coefficients such that $f(n)$ is positive for any positive integer n. We consider diverging sequences $\{x_n\}$ given by $x_0 = b$ and $x_{n+1} = f^{x_n}(a)$ for positive integers a and b. As a criterion of convergence in the profinite completion $\widehat{\mathbb{Z}}$ of the ring of integers, we show that such a sequence converges to the limit independent of the initial value b if and only if f does not induce a cyclic permutation of length p on $\mathbb{Z}/p\mathbb{Z}$ for any prime number p. We also show that b'-adic asymptotic approximations of the equation $f^x(a) = x$ hold in $\mathbb{N}$ for some bases b'.

1. Introduction

In [5], J. Jiménez-Urroz and Yebra proved the following result.

Theorem 1.1 ([5], Theorem 1)**.** *For any positive integers a and b, there exists a positive integer x such that*

$$a^x \equiv x \mod b. \tag{1}$$

Moreover, if b is valid *(i.e., for every pair of prime numbers p and q such that $p \mid b$ and $q \mid p-1$, we have $q \mid b$), then there exists a sequence of positive integers $\{x_n\}$ such that*

$$a^{x_n} \equiv x_n \mod b^n \text{ and } x_n = c_n b^{n-1} + x_{n-1} \quad (0 \leq c_n < b) \tag{2}$$

for every n.

As an example, they treated the case $a = 7$ and $b = 10$. It is easy to see that $b = 10$ is a valid number: indeed, if $p \mid 10$ and $q \mid (p-1)$, then $(p, q) = (5, 2)$ and

[1]The author is supported by JSPS KAKENHI Grant-in-Aid for Research Fellow JP202122197.

$q \mid 10$. An expanding sequence of solutions of (1) in this situation is as follows:

$$\begin{aligned} 7^3 &\equiv 3 && \bmod 10, \\ 7^{43} &\equiv 43 && \bmod 10^2, \\ 7^{343} &\equiv 343 && \bmod 10^3, \\ &\vdots \\ 7^{\cdots 36433312655115651723 43} &\equiv \cdots 3643312655115651723 43 && \bmod 10^n, \\ &\vdots \quad . \end{aligned}$$

The proof of Theorem 1.1 was constructive, that is, done by giving an algorithm to obtain x. In [7], D. B. Shapiro and S. D. Shapiro proved the former part of Theorem 1.1 independently, affording a more explicit form of the same algorithm. They proved the following result.

Theorem 1.2 ([7], Corollary 2.11)**.** *For any positive integers a and b, the sequence a, a^a, a^{a^a}, $a \uparrow\uparrow 4$, ..., $a \uparrow\uparrow n$,... becomes stable modulo b for $n \gg 0$, where $a \uparrow\uparrow n$ is Knuth's up-arrow notation introduced in [6]. Equivalently, the sequence converges in the ring $\mathbb{Z}_p$ of p-adic integers for every prime number p.*

This implies that $x = a \uparrow\uparrow n$ for $n \gg 0$ satisfies Equation (1). In addition, this allows us to restate the above example as

$$\lim_{n\to\infty} 7 \uparrow\uparrow n = \cdots 3643312655115651723 43 \quad \text{in} \quad \mathbb{Z}_2 \times \mathbb{Z}_5.$$

We regard the above two theorems as results on the polynomial $ax \in \mathbb{Z}[x]$ from the viewpoint of dynamical systems. For a self-map $f : X \to X$ on a set X and a positive integer n, we denote the n-th iteration of f by f^n. For an element x of X, we define a map $f \uparrow_x \colon \mathbb{N} \to X$ by $f \uparrow_x (n) := f^n(x)$, where $\mathbb{N}$ is the set of positive integers. If $X = \mathbb{N}$, then for every positive integer a, the map $f \uparrow_a \colon \mathbb{N} \to \mathbb{N}$ is again a self-map. Therefore we also can consider $f \uparrow_a \uparrow_b$ for every positive integer b. If $f(x) = ax$, then we have $f \uparrow_1 (n) = a^n = a \uparrow n$ and $f \uparrow_1 \uparrow_1 (n) = (f \uparrow_1) \uparrow_1 (n) = a \uparrow\uparrow n$.

The purpose of this paper is to generalize Theorems 1.1 and 1.2 to more general polynomials in $\mathbb{Z}[x]$. The following theorem is the first aim of this paper.

Theorem 1.3. *Let f be a polynomial of one variable with integer coefficients such that $f(\mathbb{N}) \subseteq \mathbb{N}$. Then the following conditions are equivalent to each other:*

(i) for any prime number p, the reduction map $f_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is not a cyclic permutation of length p;

(ii) for any positive integers a and b, if $\lim_{n\to\infty} f \uparrow_a \uparrow_b (n) = \infty$ in $\mathbb{R}$, then the limit $\lim_{n\to\infty} f \uparrow_a \uparrow_b (n)$ exists in $\mathbb{Z}_p$ for every prime number p and is independent of b.

We call a polynomial $f \in \mathbb{Z}[x]$ *tower-stable* if f satisfies either of the equivalent conditions in the last theorem (this definition will be generalized in Definition 3.12). Note that for every $a \in \mathbb{N}$, $f(x) = ax$ is tower-stable, because $f(0) = 0$. Therefore, Theorem 1.3 implies Theorem 1.2.

To generalize the latter part of Theorem 1.1, we introduce the following variant of the notion of valid number.

Definition 1.4. Let f be a tower-stable polynomial. A positive integer b is said to be *f-valid* if b is valid and for every pair of prime numbers p and q such that $p \mid b$ and $q \mid \lambda_f(p)$, we have that $q \mid b$, where $\lambda_f(p)$ is the period of the reduction map $f_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$.

Here we give some examples of tower-stable polynomials and f-valid numbers.

- A linear polynomial $f(x) = ax + b$ is tower-stable if and only if any prime factor of $a - 1$ divides b. In this case, a valid positive integer is also f-valid because $\lambda_f(p) \mid p - 1$.
- A quadratic polynomial $f(x) = ax^2 + bx + c$ is tower-stable if and only if $(a, b, c) \not\equiv (1, 0, 1), (0, 1, 1) \mod 2$ and for any odd prime divisor p of a, we have $p \nmid b - 1$ or $p \mid c$. The key of this fact is that the reduction f_p is not bijective if $a \not\equiv 0 \mod p$ for any odd prime p.
- Suppose that a polynomial $f \in \mathbb{Z}[x]$ satisfies $f(m) = f(n)$. Then f is tower-stable if and only if the reduction f_p is not a cyclic permutation for any prime p such that $p \mid m - n$.
- The number $\mathrm{lcm}\{1, \ldots, n\}$ or the number $n!$, or more generally any product of nonzero powers of the first k primes, is f-valid for any tower-stable polynomial $f \in \mathbb{Z}[x]$.

The following theorem is the second main result of this paper, which generalizes the latter part of Theorem 1.1.

Theorem 1.5. *Let f be a tower-stable polynomial. If b is f-valid, then there exists a sequence of positive integers $\{x_n\}$ such that*

$$f^{x_n}(a) \equiv x_n \mod b^n \text{ and } x_n = c_n b^{n-1} + x_{n-1} \quad (0 \le c_n < b).$$

For example, we consider a polynomial $f(x) = x^2 + x + 3$ and $b = 10$. The polynomial f is tower-stable, because $f(0) = f(-1) = 3$. By direct computation, we can see $\lambda_f(5) = 2$ and $\lambda_f(2) = 1$, which implies that 10 is f-valid. In this

situation, we have the following example of the sequence x_n in Theorem 1.5:

$$\begin{aligned} f^3(0) &\equiv 3 && \bmod 10, \\ f^{43}(0) &\equiv 43 && \bmod 10^2, \\ f^{243}(0) &\equiv 243 && \bmod 10^3, \\ &\vdots \\ f^{\cdots 636048243}(0) &\equiv \cdots 636048243 && \bmod 10^n, \\ &\vdots \quad . \end{aligned}$$

The outline of the paper is as follows. In Section 2, We extend maps on $\mathbb{N}$ to some maps on $\widehat{\mathbb{Z}}$, the profinite completion of $\mathbb{Z}$. In Section 3, we use these extensions to discuss dynamical systems on $\widehat{\mathbb{Z}}$. We prove a profinite version of Theorem 1.3 (Theorem 3.14), then obtain Theorem 1.3 as a corollary at the end of the section. In Section 4, we give a more precise evaluation on the order of convergence to show Theorem 1.5. In Section 5, we discuss remaining problems.

Below is a list of frequently used notions.

$\mathbb{N}$	the set of positive integers, $\{1, 2, 3, ...\}$
$[n]$	the set $\{1, 2, 3, ..., n\}$
$a \mid b$	a divides b, a is a divisor of b
$\mathbf{Z}_n$	the ring $\mathbb{Z}/n\mathbb{Z}$
$\overline{a}$	the residue class of a
f^n	the n-th iteration of f
$f \uparrow_a (n)$	$f^n(a)$
$\mathbf{Z}_{m,n}$	the semigroup $(\mathbb{N}, +)/\langle m \sim m + n\rangle$
$\widehat{\mathbb{Z}}$	the profinite completion of the integers, $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$
$\widehat{\mathbb{N}}$	the semigroup $(\mathbb{N} \cup \widehat{\mathbb{Z}}, \widehat{+})$ (Proposition 2.1)
$\widehat{n}$	for $n \in \mathbb{N}$, the image of n by the canonical embedding $\mathbb{N} \to \mathbb{Z} \to \widehat{\mathbb{Z}}$
$\widehat{f}$	for a map $f : \mathbb{N} \to X$, the extension of f to $\widehat{\mathbb{N}}$
$\alpha(n)$	$\max\{p^a \mid a \in \mathbb{N} \cup \{0\},\ p$ is prime and p^a divides $n\}$
f_n	for a congruence preserving $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ (Definition 3.5), the reduction of f on $\mathbf{Z}_n$ (Definition 3.3)
$\lambda_f(n)$	for a congruence preserving $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$, the period of the reduction $f_n : \mathbf{Z}_n \to \mathbf{Z}_n$
$f \Uparrow_s$	for a congruence stable $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ (Definition 3.5), the restriction of the map $\widehat{f \uparrow_s} : \widehat{\mathbb{N}} \to \widehat{\mathbb{Z}}$ to $\widehat{\mathbb{Z}} \subset \widehat{\mathbb{N}}$

2. Profinite Completion of $\mathbb{N}$

Let S be a finite quotient semigroup of $(\mathbb{N}, +)$ and let $\pi : \mathbb{N} \to S$ be the quotient map. The semigroup S is generated by $\pi(1)$. Since S is finite, the set

$$P_S := \{(k, l) \in \mathbb{N}^2 \mid \pi(k) = \pi(k + l)\}$$

is nonempty. Let $(m,n) = (m_S, n_S)$ be a pair of positive integers such that

$$\begin{aligned} n &:= \min\{l \in \mathbb{N} \mid \text{ there exists } k \text{ such that } (k,l) \in P_S\} \text{ and} \\ m &:= \min\{k \in \mathbb{N} \mid (k,n) \in P_S\}. \end{aligned}$$

We write $[m-1] := \{a \in \mathbb{N} \mid a \leq m-1\}$ and $\mathbf{Z}_n := \mathbb{Z}/n\mathbb{Z}$. Then, S is uniquely determined by m and n up to isomorphism and identified with the semigroup $\mathbf{Z}_{m,n} := ([m-1] \cup \mathbf{Z}_n, \dot{+})$. Here the operator $\dot{+}$ is defined as

$$a \dot{+} b = \begin{cases} a+b \in [m-1] & (a,b \in [m-1] \text{ and } a+b < m), \\ \overline{a+b} \in \mathbf{Z}_n & (\text{otherwise}). \end{cases}$$

The quotient map $\pi_{m,n} : \mathbb{N} \to \mathbf{Z}_{m,n}$ is given by

$$\pi_{m,n}(a) = \begin{cases} a \in [m-1] & (a < m), \\ \overline{a} \in \mathbf{Z}_n & (a \geq m). \end{cases}$$

If $m \leq k$ and $n \mid l$, then there is a natural homomorphism $\phi_{(k,l),(m,n)} : \mathbf{Z}_{k,l} \to \mathbf{Z}_{m,n}$. The family $(\{\mathbf{Z}_{m,n}\}, \{\phi_{(k,l),(m,n)}\})$ of the semigroups and the homomorphisms gives a projective system. We define the profinite completion $\widehat{\mathbb{N}}$ of $\mathbb{N}$ to be the projective limit of $(\{\mathbf{Z}_{m,n}\}, \{\phi_{(k,l),(m,n)}\})$. The semigroup $\widehat{\mathbb{N}}$ has the following description using $\widehat{\mathbb{Z}} := \varprojlim_n \mathbf{Z}_n$.

Proposition 2.1. *We have* $\widehat{\mathbb{N}} \cong (\mathbb{N} \cup \widehat{\mathbb{Z}}, \widehat{+})$, *where*

$$a \mathbin{\widehat{+}} b = \begin{cases} a+b \in \mathbb{N} & (a,b \in \mathbb{N}), \\ a+b \in \widehat{\mathbb{Z}} & (\text{otherwise}). \end{cases}$$

Proof. We can decompose every map $\phi_{(k,l),(m,n)}$ as

$$\phi_{(k,l),(m,n)} = \phi_{(k,n),(m,n)} \circ \phi_{(k,l),(k,n)}.$$

Therefore, the definition of projective limit gives

$$\widehat{\mathbb{N}} = \varprojlim \mathbf{Z}_{m,n} = \varprojlim_n \varprojlim_m \mathbf{Z}_{m,n}.$$

We claim that

$$\varprojlim_m \mathbf{Z}_{m,n} \cong (\mathbb{N} \cup \mathbf{Z}_n, \dot{+}), \text{ where } a \dot{+} b = \begin{cases} a+b \in \mathbb{N} & (a,b \in \mathbb{N}), \\ \overline{a+b} \in \mathbf{Z}_n & (\text{otherwise}). \end{cases}$$

Indeed, we can construct maps which are the inverses of each other as follows. One is given by

$$\varprojlim_m \mathbf{Z}_{m,n} \ni a = (a_m)_{m \in \mathbb{N}} \mapsto \begin{cases} a_m \in \mathbb{N} & (\text{for the smallest } m \text{ such that} \\ & \quad a_m \in [m-1], \text{ if any}), \\ a_1 \in \mathbf{Z}_n & (\text{otherwise}). \end{cases}$$

The other is given by:

$$\mathbb{N} \cup \mathbf{Z}_n \ni a \mapsto \begin{cases} (\pi_{m,n}(a))_{m\in\mathbb{N}} & (\text{if } a \in \mathbb{N}), \\ (a)_{m\in\mathbb{N}} & (\text{if } a \in \mathbf{Z}_n). \end{cases}$$

Then, it remains to show $\varprojlim_n (\mathbb{N}\cup\mathbf{Z}_n, \dot{+}) = (\mathbb{N}\cup\widehat{\mathbb{Z}}, \widehat{+})$, which follows from $\varprojlim_n \mathbf{Z}_n = \widehat{\mathbb{Z}}$. □

There exists a unique multiplication on $\mathbf{Z}_{m,n}$ induced by the projection $\pi_{m,n} : \mathbb{N} \to \mathbf{Z}_{m,n}$ from the multiplication on $\mathbb{N}$. It gives a stracture of semiring to $\mathbf{Z}_{m,n}$. Furthermore, we regard $\mathbf{Z}_{m,n}$ as a topological semiring given with the discrete topology. Then, the projective limit $\widehat{\mathbb{N}}$ also has a natural structure of semiring, which is compact Hausdorff.

Remark 2.2. A sequence $n_1, n_2, ...$ of positive integers converges to $s \in \widehat{\mathbb{Z}}$ in $\widehat{\mathbb{N}}$ if and only if n_i tends to infinity in $\mathbb{R}$ and the sequence $\widehat{n_i}$ converges to s in $\widehat{\mathbb{Z}}$ (with respect to the standard topology of $\widehat{\mathbb{Z}}$), where $\widehat{\cdot}: \mathbb{N} \to \widehat{\mathbb{Z}}$ is the natural embedding.

Proposition 2.3. *Let X be a metric space and let $f : \mathbb{N} \to X$ be a map. Then the following conditions are equivalent.*

(i) The map f can be extended to a continuous map $\widehat{f} : \widehat{\mathbb{N}} \to X$.

(ii) For all $s \in \widehat{\mathbb{Z}}$ and for all sequence of positive integers $\{n_i\}_{i\in\mathbb{N}}$ which satisfy $n_i \to +\infty$ in $\mathbb{R}$ and $\widehat{n_i} \to s$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$, the limits $\lim_{i\to\infty} f(n_i)$ exist in X and are independent of n_i (i.e., the limit $\lim_{i\to\infty} f(n_i)$ depends only on s).

Proof. The fact that (i) implies (ii) follows by Remark 2.2 about the convergence of sequence of positive integers on $\widehat{\mathbb{N}}$. We show that (ii) implies (i). For every $s \in \widehat{\mathbb{Z}}$, we take $\{n_i\}_{i\in\mathbb{N}}$ as in (ii) and set $\widehat{f}(s) := \lim_{i\to\infty} f(n_i)$. Thus, we get a well-defined map $\widehat{f} : \widehat{\mathbb{N}} \to X$. We now show $\widehat{f}$ is continuous. Since $\widehat{\mathbb{N}}$ is the projective limit of a countable system of finite sets, $\widehat{\mathbb{N}}$ is first-countable. Therefore, it is enough to show that $\widehat{f}$ is sequentially continuous. Let $\{s_i\}_{i\in\mathbb{N}} \subset \widehat{\mathbb{Z}}$ be a sequence such that $\lim_{i\to\infty} s_i = s \in \widehat{\mathbb{Z}}$. Let us denote the metric on X by d and fix an arbitrary $\varepsilon > 0$. We take sequences of positive integers $\{n_{ij}\}_{i,j\in\mathbb{N}}$ such that for every i, $n_{ij} \to s_i$ in $\widehat{\mathbb{N}}$ as $j \to \infty$. By (ii), we have $d(f(n_{ij}), f(s_i)) < \frac{\varepsilon}{2}$ $(j \gg 0)$. Thus, we can take a sequence of positive integers $\{j_i\}_{i\in\mathbb{N}}$ such that $d(f(n_{ij_i}), f(s_i)) < \frac{\varepsilon}{2}$, $n_{ij_i} > i$ and $n_{ij_i} \equiv s_i \mod i!$. Note that $n_{ij_i} \to +\infty$ in $\mathbb{R}$ and $n_{ij_i} \to s$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$. Again by (ii), we have $d(f(n_{ij_i}), f(s)) < \frac{\varepsilon}{2}$ $(i \gg 0)$, thus $d(f(s_i), f(s)) < \varepsilon$ $(i \gg 0)$. This proves that $\widehat{f}$ is sequentially continuous, hence continuous. □

Corollary 2.4. *Let X be a complete metric space, let $f : X \to X$ be a continuous map and let x be a point in X. Then the following conditions are equivalent.*

(i) The map $f\uparrow_x : \mathbb{N} \to X$ can be extended to a continuous map $\widehat{f\uparrow_x} : \widehat{\mathbb{N}} \to X$.

(ii) For all $s \in \widehat{\mathbb{Z}}$ and all sequence of positive integers $\{n_i\}_{i\in\mathbb{N}}$ which satisfy $n_i \to +\infty$ in $\mathbb{R}$ and $\widehat{n_i} \to s$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$, the limits $\lim_{i\to\infty} f^{n_i}(x)$ exist in X and are independent of n_i (i.e., the limits $\lim_{i\to\infty} f^{n_i}(x)$ depend only on s).

Definition 2.5. Let X be a complete metric space and $f : X \to X$ be a continuous map. A point x in X is said to be a *profinitely preperiodic point* of f if x satisfies one of the equivalent conditions of Corollary 2.4. The map f is said to be *profinitely preperiodic* if every point x of X is a profinitely preperiodic point of f.

We see that x is a preperiodic point of f if and only if $f\uparrow_x$ factors through some finite semigroup $\mathbf{Z}_{m,n}$; this is why we chose the term "profinitely preperiodic".

For a profinitely preperiodic point x, we define $f^s(x)$ for $s \in \widehat{\mathbb{Z}}$ by $f^s(x) := \lim_{i\to\infty} f^{n_i}(x)$, where the integer sequence n_i is taken as in (ii) of Corollary 2.4. If f is profinitely preperiodic, then for every $a, b \in \widehat{\mathbb{N}}$, we have $f^a \circ f^b = f^{a+b}$ and $(f^a)^b = f^{ab}$.

3. Dynamical System on $\widehat{\mathbb{Z}}$

Before discussing dynamical systems on $\widehat{\mathbb{Z}}$, we begin with reviewing basic facts on finite dynamical systems. Let $\alpha : \mathbb{N} \to \mathbb{N}$ be a function of "the largest factor prime power," that is,

$$\alpha(n) = \max\{p^a \mid a \in \mathbb{N}\cup\{0\},\ p \text{ is prime and } p^a \text{ divides } n\}.$$

By prime factorization, we can see $\alpha(\mathrm{lcm}\{n_i\}) = \max\{\alpha(n_i)\}$ and $\alpha(mn) \le \alpha(m)\alpha(n)$.

Lemma 3.1. *Let n be a positive integer, let F be a finite set of cardinality n and let $\sigma : F \to F$ be a map.*

(i) For every $a \in F$, there exist nonnegative integers k and l such that $l \ge 1$, $\sigma^k(a) = \sigma^{k+l}(a)$ and $k + l \le n$.

(ii) For every $a \in F$, if $\sigma^{k_i}(a) = \sigma^{k_i+l_i}(a)$ for $i = 1, 2$, then $\sigma^k(a) = \sigma^{k+l}(a)$ holds for $(k, l) = (\min\{k_1, k_2\}, \gcd\{l_1, l_2\})$.

(iii) For every $a \in F$, there exists an unique pair of nonnegative integers (k, l) such that $\sigma^{k'}(a) = \sigma^{k'+l'}(a)$ if and only if $k \le k'$ and $l \mid l'$. (We denote this pair by (k_a, l_a).)

(iv) Let $K = \max_{a\in F}\{k_a\}$ and $L = \mathrm{lcm}_{a\in F}\{l_a\}$. Then $\sigma^{K'} = \sigma^{K'+L'}$ if and only if $K \le K'$ and $L \mid L'$.

(v) We have $K + \alpha(L) \le n$.

Proof. (i) The assertion is obvious from the pigeonhole principle.

(ii) Without loss of generality, we assume $k = k_1$. We take a pair of integers (x, y) as $xl_1 + yl_2 = l$. Then, we have

$$\sigma^{k'+l}(a) = \sigma^{k'+xl_1+yl_2}(a) = \sigma^{k'}(a) \ (k' \gg 0).$$

In particular, for $k' = k + Nl_1$, we have

$$\sigma^{k+Nl_1}(a) = \sigma^{k+Nl_1+l}(a) = \sigma^{l}(\sigma^{k+Nl_1}(a)) \ (N \gg 0).$$

The assumption $k = k_1$ implies $\sigma^{k+Nl_1}(a) = \sigma^k(a)$ for every N. Thus, we have $\sigma^k(a) = \sigma^l(f^k(a)) = \sigma^{k+l}(a)$.

(iii) Let

$$k := \min\{k' \mid \sigma^{k'}(a) = \sigma^{k'+l'}(a) \text{ for some } l'\}$$

and

$$l := \gcd\{l' \mid \sigma^{k'}(a) = \sigma^{k'+l'}(a) \text{ for some } k'\}.$$

By (i) and (ii), the pair (k, l) satisfies the condition.

(iv) This is obvious from (iii).

(v) We have

$$K + \alpha(L) = \max\ k_a + \alpha(\operatorname{lcm}\ l_a) = \max k_a + \max \alpha(l_a) \leq \max k_a + \max l_a.$$

Let $b, c \in F$ be elements such that $\max k_a = k_b$ and $\max l_a = l_c$. Let

$$\begin{aligned} T_b &:= \{b, \sigma(b), ..., \sigma^{k_b-1}(b)\} \\ &= \{\sigma^k(b) \mid k \in \mathbb{N} \text{ such that } \sigma^k(b) \neq \sigma^{k+l}(b) \text{ for every } l \in \mathbb{N}\}, \\ C_c &:= \{\sigma^{k_c}(c), \sigma^{k_c+1}(c), ..., \sigma^{k_c+l_c-1}(c)\} \\ &= \{\sigma^k(c) \mid k \in \mathbb{N} \text{ such that } \sigma^k(c) = \sigma^{k+l_c}(c)\}. \end{aligned}$$

Then, T_b and C_c are disjoint subsets of F, which shows $k_b + l_c \leq n$. □

Definition 3.2. Integers $k = k_a$ and $l = l_a$ in (iii) of Lemma 3.1 are called the *tail length* and the *cycle length* of σ on a respectively. Integers K and L in (iv) of Lemma 3.1 are called the *preperiod length* and the *period* of σ respectively.

Definition 3.3. Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be a continuous map. A map $P : \mathbb{N} \to \mathbb{N}$ is said to be a *period map* of f if it satisfies one of the following equivalent conditions.

(i) For every $s, t \in \widehat{\mathbb{Z}}$ and $n \in \mathbb{N}$, if $s \equiv t \mod P(n)$ then $f(s) \equiv f(t) \mod n$.

(ii) For every $n \in \mathbb{N}$, there exists a map $f_n : \mathbf{Z}_{P(n)} \to \mathbf{Z}_n$ that makes the following diagram commutative:

$$\begin{array}{ccc} \widehat{\mathbb{Z}} & \xrightarrow{f} & \widehat{\mathbb{Z}} \\ \downarrow & & \downarrow \\ \mathbf{Z}_{P(n)} & \xrightarrow{f_n} & \mathbf{Z}_n \end{array}$$

Here the vertical arrows are projections.

Maps f_n are called *reductions* of f.

We note that $\widehat{\mathbb{Z}}$ is metrizable with some metric which is invariant by translations of the form $s \mapsto s + c$. Since $\widehat{\mathbb{Z}}$ is compact, any continuous map $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ is also uniformly continuous for such a metric, so every continuous map has a period map. We also note that a period map of f is not uniquely determined by f in our definition.

Proposition 3.4. *Let P be a period map of f and let Q be a period map of g. Then, $Q \circ P$ is a period map of $f \circ g$. In particular, P^n is a period map of f^n.*

Proof. We check Condition (i) of Definition 3.3. If we take $s, t \in \widehat{\mathbb{Z}}$ such that $s \equiv t \mod Q(P(n))$, then $g(s) \equiv g(t) \mod P(n)$ and hence $f(g(s)) \equiv f(g(t)) \mod n$. □

Definition 3.5. Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be a continuous map.

(i) The map f is said to be *congruence stable* if there exists a period map P of f such that $P^k(n) = P^{k+1}(n)$ $(k \gg 0)$ for each positive integer n.

(ii) The map f is said to be *congruence preserving* if $\mathrm{id}_{\mathbb{N}}$, the identity function on $\mathbb{N}$, is a period map of f.

Remark 3.6. Every polynomial in $\widehat{\mathbb{Z}}[x]$ regarded as a map $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ is congruence preserving, but not every congruence preserving map is a polynomial with $\widehat{\mathbb{Z}}$ coefficients, see [3] and [2].

Lemma 3.7. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be a continuous map and let P be a period map of f. Let k, m and n be positive integers such that*

$$m = P^k(n) = P^{k+1}(n).$$

Let $f_m : \mathbf{Z}_m \to \mathbf{Z}_m$ be the reduction of f and let K and L be the preperiod length and the period of f_m respectively.

Then, for every $s, t \in \widehat{\mathbb{Z}}$ and $u, v \in \mathbb{N}$ such that $s \equiv t \mod m$, $u, v \geq k + K$ and $u \equiv v \mod L$, we have $f \uparrow_s (u) \equiv f \uparrow_t (v) \mod n$.

Proof. If we have $u - k, v - k \geq K$ and $u - k \equiv v - k \mod L$, then

$$f^{u-k}(s) \equiv f^{v-k}(s) \equiv f^{v-k}(t) \mod m.$$

By Proposition 3.4, P^k is a period map of f^k. We obtain

$$f^k(f^{u-k}(s)) \equiv f^k(f^{v-k}(t)) \mod n,$$

that is, $f \uparrow_s (u) \equiv f \uparrow_t (v) \mod n$. □

Theorem 3.8. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be a congruence stable map. Then, f is profinitely preperiodic.*

Proof. We check Condition (ii) of Corollary 2.4. Let $\{n_i\}$ be a sequence of positive integers such that $n_i \to \infty$ in $\mathbb{R}$ and $\widehat{n_i} \to s$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$ for some $s \in \widehat{\mathbb{Z}}$.

Firstly, we will show that the sequence $\{f^{n_i}(s) = f \uparrow_s (n_i)\}_i$ converges, that is, becomes eventually stable modulo n for an arbitrary positive integer n. We fix a positive integer n. Since f is congruence stable, there is a period map P of f such that $P^k(n) = P^{k+1}(n)$ for some k. Then, we take K and L as in Lemma 3.7. By the choice of the sequence $\{n_i\}$, we have

$$n_i, n_j \geq k + K \text{ and } n_i \equiv n_j \mod L \ (i, j \gg 0).$$

By Lemma 3.7, this implies

$$f \uparrow_x (n_i) \equiv f \uparrow_x (n_j) \mod n \ (i, j \gg 0).$$

Thus, the sequence $\{f \uparrow_x (n_i) \mod n\}_i$ become eventually stable.

Next, let $\{n_i'\}$ be another sequence such that $n_i' \to \infty$ in $\mathbb{R}$ and $\widehat{n_i'} \to s$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$. Then, by a similar argument, we have

$$\lim_{i\to\infty} f \uparrow_s (n_i) \equiv \lim_{i\to\infty} f \uparrow_s (n_i') \mod n$$

for every positive integer n. This means that

$$\lim_{i\to\infty} f \uparrow_x (n_i) = \lim_{i\to\infty} f \uparrow_x (n_i')$$

in $\widehat{\mathbb{Z}}$. □

By Corollary 2.4, we obtain a continuous map $\widehat{f \uparrow_s} : \widehat{\mathbb{N}} \to \widehat{\mathbb{Z}}$. By Proposition 2.1, we may regard the domain $\widehat{\mathbb{N}}$ as $\mathbb{N} \cup \widehat{\mathbb{Z}}$ and denote the restriction $\widehat{f \uparrow_s}|_{\widehat{\mathbb{Z}}} : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ by $f \Uparrow_s$. The map $f \Uparrow_s$ is again continuous.

Proposition 3.9. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be a congruence stable map, let P be a period map of f and let $\mu : \mathbb{N} \to \mathbb{N}$ be a map. Suppose that for every $n \in \mathbb{N}$, there exists $k \in \mathbb{N}$ satisfying $\mu(n) = P^k(n) = P^{k+1}(n)$. Let $\lambda : \mathbb{N} \to \mathbb{N}$ be the map such that*

$$\lambda(n) = \text{ the period of the reduction } f_{\mu(n)} : \mathbf{Z}_{\mu(n)} \to \mathbf{Z}_{\mu(n)}.$$

Then, λ is a period map of $f \Uparrow_x$ for every x in $\widehat{\mathbb{Z}}$.

Moreover, for $x, y, s \in \widehat{\mathbb{Z}}$, if $x \equiv y \mod \mu(n)$, then $f \Uparrow_x (s) \equiv f \Uparrow_y (s) \mod n$.

Proof. We take $s, t \in \widehat{\mathbb{Z}}$ such that $t \equiv s \mod \lambda(n)$. Let $\{n_i\}$ and $\{n_i'\}$ be sequences of positive integers such that the limits in $\widehat{\mathbb{N}}$ are s and t respectively. Then, by an argument similar to one in the proof of Theorem 3.8, we have

$$f \uparrow_x (n_i) \equiv f \uparrow_x (n_j') \mod n \ (i, j \gg 0).$$

Therefore, we have

$$f \uparrow_x (t) \equiv f \uparrow_x (s) \mod n.$$

This shows the first assertion of the proposition.

We show the latter part. Let n be a positive integer and let n_i be a sequence of positive integers such that $n_i \to s$ in $\widehat{\mathbb{N}}$. By the assumption $P(\mu(n)) = \mu(n)$, if $n_i \geq k$ then we have

$$f^{n_i-k}(x) \equiv f^{n_i-k}(y) \mod \mu(n)$$

for any $x, y \in \widehat{\mathbb{Z}}$ such that $x \equiv y \mod \mu(n)$. Then, by the assumption $P^k(n) = \mu(n)$ and Proposition 3.4, we have

$$\begin{aligned} f \uparrow_x (n_i) &= f^{n_i}(x) \\ &\equiv f^{n_i}(y) \mod n \\ &= f \uparrow_y (n_i) \ (i \gg 0). \end{aligned}$$

By passing to the limits, we obtain $f \uparrow_x (s) \equiv f \uparrow_y (s) \mod n$. □

We now discuss the case that $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ is congruence preserving. We denote the period of the reduction $f_n : \mathbf{Z}_n \to \mathbf{Z}_n$ by $\lambda_f(n)$, which defines a map $\lambda_f : \mathbb{N} \to \mathbb{N}$. We can restate Proposition 3.9 for congruence preserving functions as follows.

Proposition 3.10. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be congruence preserving and let $s \in \widehat{\mathbb{Z}}$. Then, λ_f is a period map of $f \uparrow_s$.*

Now we shall evaluate λ_f.

Lemma 3.11. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be congruence preserving and let p be a prime number. The following conditions are equivalent to each other.*

(i) We have $\lambda_f(p) \neq p$.

(ii) The reduction $f_p : \mathbf{Z}_p \to \mathbf{Z}_p$ of f is not a cyclic permutation of length p.

(iii) For every $x \in \mathbf{Z}_p$, for the cycle length l_x of f_p on x is less than p.

(iv) We have $\alpha(\lambda_f(p)) < p$.

Proof. ((i) implies (ii)) The contraposition is obvious.

((ii) implies (iii)) We show the contraposition. Assume that there is some $x \in \mathbf{Z}_p$ such that $f_p^k(x) = {f_p}^{k+l}(x)$ implies $l \geq p$. Then $x, f_p(x), ..., (f_p)^{p-1}(x)$ are distinct elements of $\mathbf{Z}_p$ and $(f_p)^p(x) = x$, that is, f_p is a cyclic permutation of length p.

((iii) implies (iv)) Assume (iii). By Lemma 3.1 (iv), the period $\lambda_f(p)$ of $f_p : \mathbf{Z}_p \to \mathbf{Z}_p$ satisfies

$$\begin{aligned}\alpha(\lambda_f(p)) &= \alpha(\mathrm{lcm}\{l_x \mid x \in \mathbf{Z}_p\}) \\ &= \max\{\alpha(l_x) \mid x \in \mathbf{Z}_p\} \\ &\leq \max\{l_x \mid x \in \mathbf{Z}_p\} \\ &< p.\end{aligned}$$

((iv) implies (i)) The contraposition is obvious, because p is a prime number. □

Definition 3.12. A congruence preserving function $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ is said to be *tower-stable* if f satisfies $\alpha(\lambda_f(p)) < p$, i.e., Condition (iv) of Lemma 3.11, for every prime number p.

Lemma 3.13. *Let f be a congruence preserving map and let n, n' be positive integers.*

(i) We have $\mathrm{lcm}(\lambda_f(n), \lambda_f(n')) = \lambda_f(\mathrm{lcm}(n, n'))$. *In particular, if we have $n \mid n'$, then we have $\lambda_f(n) \mid \lambda_f(n')$.*

(ii) For every prime number p and every positive integer a, we have $\lambda_f(p^{a+1}) \mid \mathrm{lcm}\{1, 2, \ldots, p\} \cdot \lambda_f(p^a)$.

(iii) We have $\lambda_f^k(n) = \lambda_f^{k+1}(n)$ $(k \gg 0)$.

(iii') If f is tower-stable, then we have $\lambda_f^k(n) = 1$ $(k \gg 0)$.

Proof. (i) We show that for each positive integer N, $\lambda_f(\mathrm{lcm}(n, n')) \mid N$ if and only if $\lambda_f(n) \mid N$ and $\lambda_f(n) \mid N$. By Lemma 3.1 (iv), for positive integers N and ν, we have $\lambda_f(\nu) \mid N$ if and only if

$$f^M(x) \equiv f^{M+N}(x) \mod \nu \ (M \gg 0) \text{ for all } x \in \widehat{\mathbb{Z}}.$$

Thus, the problem is reduced to show that

$$\begin{aligned}&f^M(x) \equiv f^{M+N}(x) \mod \mathrm{lcm}(n, n') \ (M \gg 0) \text{ for all } x \in \widehat{\mathbb{Z}} \text{ if and only if} \\ &f^M(x) \equiv f^{M+N}(x) \mod n \text{ and } f^M(x) \equiv f^{M+N}(x) \mod n' \ (M \gg 0) \text{ for all } x \in \widehat{\mathbb{Z}}.\end{aligned}$$

This follows from the Chinese remainder theorem.

(ii) Let $\pi : \widehat{\mathbb{Z}} \twoheadrightarrow \mathbf{Z}_{p^a}$ and $\pi_a : \mathbf{Z}_{p^{a+1}} \twoheadrightarrow \mathbf{Z}_{p^a}$ be the cannonical surjections. Let $s \in \widehat{\mathbb{Z}}$ and $t = f^k(s)$. We put

$$T := \pi_a^{-1}(\pi(t)) = \{\overline{t + cp^a} \mid 0 \leq c < p\} \subset \mathbf{Z}_{p^{a+1}}.$$

Let $l := \lambda_f(p^a)$ and let k be the preperiod length of the reduction $f_{p^a} : \mathbf{Z}_{p^a} \to \mathbf{Z}_{p^a}$. For every $\overline{t'} \in T$, from $t = f^k(s)$, it follows that

$$\begin{aligned} f^l(t') &\equiv f^l(t) \mod p^a \\ &= f^{k+l}(s) \\ &\equiv f^k(s) \mod p^a \\ &= t, \end{aligned}$$

which shows $f^l(T) \subset T$. Therefore by Lemma 3.1 (i), there exists k_t and l_t such that

$$f^{lk_t}(t) \equiv f^{l(k_t+l_t)}(t) \mod p^{a+1} \text{ and } k_t + l_t \leq \mathrm{card}(T) = p.$$

Since $k_t \leq p$ and $l_t \mid \mathrm{lcm}\{1, 2, ..., p\} = \mathrm{lcm}[p]$, we have

$$\begin{aligned} f^{k+lp}(s) &= f^{lp}(t) \\ &\equiv f^{l(p+\mathrm{lcm}[p])}(t) \mod p^{a+1} \\ &= f^{k+lp+l\cdot\mathrm{lcm}[p]}(s). \end{aligned}$$

Thus, Lemma 3.1 (iv) leads to

$$\lambda_f(p^{a+1}) \mid l \ \mathrm{lcm}[p] = \lambda_f(p^a)\mathrm{lcm}[p].$$

(iii) We use the induction on $\alpha(n)$. The case $\alpha(n) = 1$ is obvious. Let us assume that the assertion holds for every m with $\alpha(m) < p^a$ and consider n with $\alpha(n) = p^a$. By (ii), we have

$$\alpha(\lambda_f(p^a)) \leq p \cdot \alpha(\lambda_f(p^{a-1})).$$

Thus, we have

$$\alpha(\lambda_f(p^a)) \leq p \cdot \alpha(\lambda_f(p^{a-1})) \leq \cdots \leq p^{a-1}\alpha(\lambda_f(p)) \leq p^a. \tag{3}$$

Hence by (i), we have

$$\alpha(\lambda_f(n)) \leq \alpha(n).$$

The case $\alpha(\lambda_f(n)) < \alpha(n)$ is evident from the assumption of the induction. Let us assume $\alpha(\lambda_f(n)) = \alpha(n) = p^a$, that is, $\alpha(\lambda_f(p^a)) = p^a$. We put $\lambda_f(p^a) = cp^a$. By (i) of this lemma, we have

$$\lambda_f(n) = \mathrm{lcm}\left\{\lambda_f(p^a), \lambda_f\left(\frac{n}{p^a}\right)\right\} = \mathrm{lcm}\left\{p^a, c, \lambda_f\left(\frac{n}{p^a}\right)\right\}.$$

By applying (i) inductively, we obtain

$$\lambda_f^k(n) = \mathrm{lcm}\left\{p^a, c, \lambda_f(c), ..., \lambda_f^{k-1}(c), \lambda_f^k\left(\frac{n}{p^a}\right)\right\}.$$

Since $\alpha(c)$ and $\alpha\left(n/p^a\right)$ are both less than p^a, by the assumption of the induction, $\lambda_f^k(n)$ is eventually constant.

(iii') Assertion (ii) and the inequality $\alpha(\lambda_f(p)) < p$ lead to the strict inequality in Equation (3), $\alpha(\lambda_f(p^a)) < p^a$. Thus, we have $\alpha(\lambda_f(N)) < \alpha(N)$ for every $N > 1$. Therefore, we have

$$\alpha(\lambda_f^k(n)) = 1 \ (k \gg 0),$$

that is, $\lambda_f^k(n) = 1 \ (k \gg 0)$. □

Theorem 3.14. *Let $f : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$ be congruence preserving and let $s \in \widehat{\mathbb{Z}}$. Then, the map $f \uparrow_s$ is profinitely preperiodic. Moreover, if f is tower-stable, then $f \uparrow_s \uparrow_t$ is a constant function and independent of t.*

Proof. By Proposition 3.10, λ_f is a period map of the map $f \uparrow_s$. Therefore, by Lemma 3.13 (iii), $f \uparrow_s$ is congruence stable. Theorem 3.8 shows that $f \uparrow_s$ is profinitely preperiodic.

We now assume that f is tower-stable. By Lemma 3.13 (iii'), we can apply Proposition 3.9 to $f \uparrow_s$ and λ_f with the constant functions $\mu(n) = 1$ and $\lambda(n) = 1$. We therefore obtain that if $t \equiv t' \mod 1$ and $u \equiv u' \mod 1$, then for every n,

$$\begin{aligned} f \uparrow_s \uparrow_t (u) &\equiv f \uparrow_s \uparrow_t (u') \mod n \\ &\equiv f \uparrow_s \uparrow_{t'} (u') \mod n. \end{aligned}$$

Thus, we have $f \uparrow_s \uparrow_t (u) = f \uparrow_s \uparrow_{t'} (u')$ for any $t, t', u, u' \in \widehat{\mathbb{Z}}$. □

Proof of Theorem 1.3. ((i) implies (ii)) Let $\widehat{\cdot} : \mathbb{Z} \to \widehat{\mathbb{Z}}, a \mapsto \widehat{a}$ be the natural embedding. For a given polynomial $f(x) = \sum a_i x^i \in \mathbb{Z}[x]$, set $\widehat{f}(x) := \sum \widehat{a_i} x^i \in \widehat{\mathbb{Z}}[x]$. Let $F : \widehat{\mathbb{N}} \to \widehat{\mathbb{N}}$ be a map such that

$$F(n) = \begin{cases} f \uparrow_a (n) = f^n(a) \in \mathbb{N} & (n \in \mathbb{N}), \\ \widehat{f} \uparrow_{\widehat{a}} (n) = \widehat{\widehat{f} \uparrow_{\widehat{a}}}(n) \in \widehat{\mathbb{Z}} & (n \in \widehat{\mathbb{Z}}). \end{cases}$$

Let $\{n_i\}$ be a sequence of positive integers such that $n_i \to \infty$ in $\mathbb{R}$ and $n_i \to s \in \widehat{\mathbb{Z}}$ in $\widehat{\mathbb{Z}}$ as $i \to \infty$. Then, we have

$$\widehat{F(n_i)} = \widehat{f^{n_i}(a)} = \widehat{f}^{n_i}(\widehat{a}) = \widehat{f} \uparrow_{\widehat{a}} (n_i) \to \widehat{f} \uparrow_{\widehat{a}} (s) = F(s) \ \text{ in } \widehat{\mathbb{Z}} \ \ (i \to \infty).$$

If there exists a sequence $F(n_i) \nrightarrow \infty$ in $\mathbb{R}$, then $F(n_i) = F(n_{i'})$ holds for some distinct positive integers i and i'. Namely, a is a preperiodic point of f. Therefore the function $f \uparrow_a$ is bounded on $\mathbb{N}$ and Assertion (ii) holds automatically.

Therefore we can assume that $F(n_i) \to \infty$ in $\mathbb{R}$, which implies that the map F is continuous on $\widehat{\mathbb{N}}$. By Lemma 3.11 and Theorem 3.14, there exists $t \in \widehat{\mathbb{Z}}$ such that the following equation holds for any $s \in \widehat{\mathbb{Z}}$:

$$F^n(s) = (\widehat{f} \uparrow_{\widehat{a}})^n(s) \to t \ (n \to \infty).$$

We note that this is equivalent to

$$\bigcap_{n=1}^{\infty} F^n(\widehat{\mathbb{Z}}) = \{t\},$$

because $\widehat{\mathbb{Z}}$ is compact and Hausdorff.

Let b be a positive integer. We assume $F^n(b) \nrightarrow t$, or equivalently that there exists a neighborhood N of t in $\widehat{\mathbb{Z}}$ and a subsequence $F^{n_1}(b), F^{n_2}(b), ...$ of $\{F^n(b)\}$ such that the sequence $\{n_i\}$ is increasing and $\{F^{n_i}(b)\} \cap N = \emptyset$.

Since $\widehat{\mathbb{Z}}$ is compact and metrizable, there exists a converging subsequence $\{F^{n_{k(i)}}(b)\}_i$ of $\{F^{n_i}(b)\}_i$ which converges to $s \in \widehat{\mathbb{Z}}$. We write $m(i) = n_{k(i)}$.

We fix a positive integer i. We have

$$F^{m(i)}(F^{m(i+j)-m(i)}(b)) = F^{m(i+j)}(b) \to s \ (j \to \infty). \tag{4}$$

Again from the fact that $\widehat{\mathbb{Z}}$ is compact and metrizable, we can take a converging subsequence of the sequence $\{F^{m(i+j)-m(i)}(b)\}_j$. Let the limit of the subsequence be $s_i' \in \widehat{\mathbb{Z}}$. By Equation (4), we have $F^{m(i)}(s_i') = s$.

Therefore, we obtain

$$s \in \bigcap_{i=1}^{\infty} F^{m(i)}(\widehat{\mathbb{Z}}) = \bigcap_{n=1}^{\infty} F^n(\widehat{\mathbb{Z}}) = \{t\},$$

which is a contradiction. Thus, for any b, $F^n(b) = f\uparrow_a\uparrow_b(n)$ converges to the same $t \in \widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ and Assertion (ii) follows.

((ii) implies (i)) We prove the contraposition. We assume that for a prime number p and an integer x, $f^b(x) \equiv f^c(x) \mod p$ if and only if $b \equiv c \mod p$ for any positive integers b and c. Then, for every $a \in \mathbb{N}$, the map $f\uparrow_a : \mathbb{N} \to \mathbb{N}$ induces the bijection $(f\uparrow_a)_p : \mathbf{Z}_p \to \mathbf{Z}_p$. The assumption also shows that f is a non-constant polynomial. Therefore, there exists $a \in \mathbb{N}$ such that for every $b \in \mathbb{N}$, $\lim_{n\to\infty} f\uparrow_a\uparrow_b(n) = \infty$ in $\mathbb{R}$.

If $(f\uparrow_a)_p$ has two or more cycles, then we take $b, b' \in \mathbb{N}$ which map into distinct cycles of $(f\uparrow_a)_p$. In particular, for every n, we have

$$f\uparrow_a\uparrow_b(n) = (f\uparrow_a)^n(b) \not\equiv f\uparrow_a\uparrow_{b'}(n) \mod p.$$

This contradicts to the independence of the limit $\lim_{i\to\infty} f\uparrow_a\uparrow_b(n)$ from b in (ii).

If $(f\uparrow_a)_p$ is a permutation with only one cycle, then its cycle length is p and $f\uparrow_a\uparrow_b$ is also a permutation on $\mathbf{Z}_p$. Therefore, the sequence $\{f\uparrow_a\uparrow_b(n) \mod p\}_n$ cannot be eventually stable. □

4. Period Maps of Iterated Polynomial

Throughout this section, we assume that $f(x) = \sum_i c_i x^i \in \mathbb{Z}[x]$ is a tower-stable polynomial. For every integer a, let $\kappa_{f,a}(n)$ (resp. $\lambda_{f,a}(n)$) be the tail (resp. cycle) length on $\overline{a} \in \mathbf{Z}_n$ of the reduction $f_n : \mathbf{Z}_n \to \mathbf{Z}_n$ of f. To show Theorem 1.5, we evaluate $\lambda_{f,a}$ and $\kappa_{f,a}$. Evaluation of $\lambda_{f,a}$ was established by Fan and Liao in [4], in a context of p-adic dynamics. On the other hand, they evaluated $\kappa_{f,a}$ only implicitly in the process of evaluating $\lambda_{f,a}$. We re-evaluate the tail length along their method. We use the following Lemmas 4.1 and 4.2.

Lemma 4.1. *Let a, c, n be positive integers and let p be a prime number. Then we have that*

(i) $f(a + cp^n) \equiv f(a) + cf'(a)p^n \mod p^{n+1}$ *and*

(ii) (chain rule) $(f^n)' = \prod_{i=0}^{n-1} f' \circ f^i$

where g' denotes the derivative of g for each polynomial g.

Proof. (i) By the Taylor expansion of f around a, we can see that there exists a polynomial h such that

$$f(a + x) - (f(a) + xf'(a)) = x^2 h(x, a).$$

This formula also shows that the coefficients of h are integers. By substituting $x = cp^n$, we obtain the assertion.

(ii) The assertion is evident. □

Lemma 4.2. *Let p be a prime number, let $g(x) = bx + c \in \mathbb{Z}[x]$ be a linear polynomial and let s be an integer. Then we have*

$$\lambda_{g,s}(p) \mid \begin{cases} 1 & (b \equiv 0 \mod p), \\ p & (b \equiv 1 \mod p) \end{cases} \text{ and } \kappa_{g,s}(p) \leq \begin{cases} 1 & (b \equiv 0 \mod p), \\ 0 & (b \equiv 1 \mod p). \end{cases}$$

Proof. The assertion is evident. More general case is shown in [4, Lemma 1]. □

In what follows, we fix a positive integer a. We denote $\kappa_{f,a}$ by κ, and $\lambda_{f,a}$ by λ. We define the *mod p multiplier* of f on a to be

$$\mu_p := (f^{\lambda(p)})'(f^{\kappa(p)}(a)) = \prod_{i=0}^{\lambda(p)-1} f'(f^{\kappa(p)+i}(a)).$$

Theorem 4.3 ([4])**.** *Let k be a positive integer and let p be a prime number.*

(i) If $\mu_p \equiv 0 \mod p$, then we have $\lambda(p^k) = \lambda(p)$ and $\kappa(p^k) \leq \kappa(p) + (k-1) \cdot \lambda(p)$.

(ii) If $\mu_p \not\equiv 0 \mod p$, then we have $\kappa(p^k) = \kappa(p)$ and $\lambda(p^k) \mid \lambda(p) \cdot (p-1) \cdot p^{k-1}$.

Proof. From Lemma 3.1 and the evident inequality $\kappa(p^k) \geq \kappa(p)$, it is enough to show the claim that $f^{K+L}(a) \equiv f^K(a) \mod p^k$ for

$$(K, L) = \begin{cases} (\kappa(p) + (k-1) \cdot \lambda(p), & \lambda(p) &) & \text{if } \mu_p \equiv 0 \mod p, \\ (\kappa(p), & \lambda(p) \cdot (p-1) \cdot p^{k-1} &) & \text{if } \mu_p \not\equiv 0 \mod p. \end{cases} \tag{5}$$

We show this by induction on k. The case $k = 1$ is evident. We take a pair (K, L) as above and assume that they satisfy

$$f^{K+L}(a) \equiv f^K(a) \mod p^k.$$

Putting $t := f^K(a)$, we obtain

$$t \equiv f^L(t) \mod p^k.$$

We put $f^L(t) = cp^k + t$. Applying Lemma 4.1 (i) to f^L, we obtain

$$\begin{aligned} f^L(t + sp^k) &\equiv s(f^L)'(t)p^k + cp^k + t \mod p^{k+1} \\ &= ((f^L)'(t)s + c)p^k + t. \end{aligned}$$

Namely, if we write $g(s) := (f^L)'(t)s + c$, then

$$f^L(t + sp^k) \equiv t + g(s)p^k \mod p^{k+1}.$$

This implies

$$(f^L)^n(t + sp^k) \equiv t + g^n(s)p^k \mod p^{k+1}.$$

Therefore, if $g^m(s) \equiv g^{m+n}(s) \mod p$ for some m and n, then we have

$$(f^L)^m(t) \equiv (f^L)^{m+n}(t) \mod p^{k+1}. \tag{6}$$

Applying Lemma 4.1(ii) to f^L, we have:

$$\begin{aligned} (f^L)'(t) &= \prod_{i=0}^{L-1} f'(f^i(t)) \\ &= \prod_{i=0}^{\frac{L}{\lambda(p)}-1} \prod_{j=0}^{\lambda(p)-1} f'(f^{i\lambda(p)+j}(t)) \\ &\equiv \prod_{i=0}^{\frac{L}{\lambda(p)}-1} \prod_{j=0}^{\lambda(p)-1} f'(f^{\kappa(p)+j}(a)) \mod p \\ &= \mu_p^{\frac{L}{\lambda(p)}} \\ &= \begin{cases} \mu_p & \equiv 0 \mod p \ (\mu_p \equiv 0 \mod p), \\ \mu_p^{(p-1)\cdot p^{k-1}} & \equiv 1 \mod p \ (\mu_p \not\equiv 0 \mod p). \end{cases} \end{aligned} \tag{7}$$

Here the first congruence follows from equalities

$$f^{i\lambda(p)}(t) = f^{i\lambda(p)+K}(a) = f^{i'\lambda(p)+\kappa(p)}(a) \equiv f^{\kappa(p)}(a) \mod p$$

and the fact that f^j and f' are polynomials in $\mathbb{Z}[x]$, in particular, congruence preserving. We also note that the last congruence in Equation (7) for the case $\mu_p \not\equiv 0 \mod p$ follows from Fermat's little theorem. Applying Lemma 4.2 to $g(s) = (f^L)'(t) \cdot s + c$, by Equation (7), we obtain $g^m(s) \equiv g^{m+n}(s) \mod p$ for

$$(m,n) = \begin{cases} (1,1) & (\mu_p \equiv 0 \mod p), \\ (0,p) & (\mu_p \not\equiv 0 \mod p). \end{cases}$$

By substituting the above pair (m,n), $t = f^K(a)$ and Equation (5) into Equation (6), we complete the proof of theorem and hence the one of the theorem. □

Remark 4.4. In [4], Fan and Liao evaluated for $\lambda(n)$ more precisely. In their classification, the first assertion of Theorem 4.3 corresponds to the case "grow tails" and the second assertion corresponds to the cases "grows", "splits" and "partially splits." They gave a precise evaluation of $\lambda(n)$ each case of their classification, and the other assertions of Theorem 4.3 easily follow from their arguments.

Proposition 4.5. *Let p be a prime number. If $\mu_p \equiv 0 \mod p$, then the p-adic part of $f \uparrow_a (s)$ is algebraic number for every $s \in \widehat{\mathbb{Z}}$. Here the p-adic part means the image of an element of $\widehat{\mathbb{Z}}$ by the projection $\widehat{\mathbb{Z}} \to \mathbb{Z}_p$.*

Proof. Let s' be a positive integer such that $s' > \kappa(p)$ and $s' \equiv s \mod \lambda(p)$. By Theorem 4.3, for every $k \in \mathbb{N}$, we have

$$f^{k\lambda(p)+s'}(a) \equiv f^{(k+1)\lambda(p)+s'}(a) \mod p^k.$$

Therefore, the sequence $\{x_k := f^{k\lambda(p)+s'}(a)\}$ converges in $\mathbb{Z}_p$ as $k \to \infty$. Since $x_{k+1} = f^{\lambda(p)}(x_k)$, if we put $x := \lim_{k\to\infty} x_k$, then $f^{\lambda(p)}(x) = x$. We conclude that x is algebraic over $\mathbb{Q}$.

For every increasing sequence of positive integers $\{n_i\}_i$ such that $n_i \to s$ in $\widehat{\mathbb{N}}$ as $i \to \infty$, $\{f^{n_i}(a)\}_i$ is a subsequence of $\{x_k\}$ for $i \gg 0$. Thus, the number $f \uparrow_a (s) = \lim_{i\to\infty} f^{n_i}(a) = x$ is algebraic. □

Proposition 4.6. *Let b be an f-valid number. Then, we have $\lambda_f(b^n) \mid b^n$ for every sufficiently large n.*

Proof. From Lemma 3.13 and Theorem 4.3,

$$\lambda_f(b^n) = \mathrm{lcm}_{p^a \mid b}\{\lambda_f(p^{an})\} \mid \mathrm{lcm}_{p^a \mid b}\{\lambda_f(p) \cdot (p-1) \cdot p^{an}\}.$$

For a p with $p \mid b$, if we write $\lambda_f(p) \cdot (p-1) = \prod q_i^{r_i}$ is the prime factorization, then since b is f-valid, we have $q_i \mid b$ for every q_i. Therefore, if we put $N = \max_p \max_{q_i} r_i$, then we have $\lambda_f(p) \cdot (p-1) \cdot p^{an} \mid b^n$ for every prime power divisor p^a of b and integer $n \geq N$. □

Lemma 4.7. *Let κ and λ be positive integers, let p be a prime, let $x \in \mathbb{Z}_p$ be a p-adic integer which is algebraic over $\mathbb{Q}$ and let $\{x_n\}$ be a nondecreasing sequence of positive integers such that $x_n \equiv x \mod p^n$. If $\{x_n\}$ is not eventually constant, then we have*

$$x_n \geq \lambda n + \kappa$$

for every sufficiently large n.

Proof. Let F be a polynomial with integer coefficients such that $F(x) = 0$. Since $x_n \equiv x \mod p^n$, we obtain

$$F(x_n) \equiv F(x) = 0 \mod p^n.$$

We have $F(x_n) \neq 0$ $(n \gg 0)$, because x_n is nondecreasing and not eventually constant. It follows that

$$|F(x_n)| \geq p^n$$

and

$$x_n \geq C_1 \cdot p^{n/\deg F} > C_2 \cdot n \ (n \gg 0)$$

for some constants C_1 and C_2. □

Proof of Theorem 1.5. By Theorem 3.14, we can take the limit

$$x = \lim_{k \to \infty} f \uparrow_a \uparrow_t (k),$$

which satisfies $f \uparrow_a (x) = x$. Write the expansion of the b-adic part of x as

$$x = c_0 + c_1 b + c_2 b^2 + ... + c_n b^n + ... , \text{ where } 0 \leq c_n < b.$$

Let $x_{n|}$ be the positive integers given by the first n digits of the expansion, that is,

$$x_{n|} := c_0 + c_1 b + c_2 b^2 + ... + c_{n-1} b^{n-1}.$$

Then, the sequence $\{x_{n|}\}$ is nondecreasing. We now assume that the sequence $x_{n|}$ is not eventually constant and show the inequality

$$\kappa(b^n) \leq x_{n|} \ (n \gg 0). \tag{8}$$

To see this, we first note that $\kappa(b^n) = \max_{p^a | b}\{\kappa(p^{an})\}$ by a similar argument as one in the proof of Lemma 3.13 (i). By Theorem 4.3, for some integers l, k, we have

$$\kappa(b^n) \leq ln + k \ (n \gg 0). \tag{9}$$

Moreover, if $\mu_p \not\equiv 0 \mod p$ for every $p \mid b$, then Formula (9) holds for $l = 0$ and Formula (8) follows obviously. Now we assume $\mu_p \equiv 0 \mod p$ for some p. By Proposition 4.5, the p-adic component of x is algebraic, and $x_{n|} \equiv x \mod p^n$ by

the definition of $x_{n|}$. Thus, by Lemma 4.7, $x_{n|} > ln + k$ $(n \gg 0)$. Combining this with Formula (9) gives Formula (8).

By Proposition 4.6, $x_{n|} \equiv x \mod b^n$ implies

$$x_{n|} \equiv x \mod \lambda(b^n)\ (n \gg 0). \tag{10}$$

From Formulae (8) and (10),

$$\begin{aligned} f^{x_{n|}}(a) &\equiv f^x(a) \mod b^n\ (n \gg 0) \\ &= x \\ &\equiv x_{n|} \mod b^n. \end{aligned}$$

Therefore, if we fix a sufficiently large N and put

$$x_n := \begin{cases} x_{N|} & (n \le N), \\ x_{n|} & (\text{otherwise}), \end{cases}$$

then we have

$$f^{x_n}(a) \equiv x_n \mod b^n \text{ and } x_n = c'_n b^{n-1} + x_{n-1} \quad (0 \le c'_n < b),$$

which is the required condition in Theorem 1.5.

When $x_{n|}$ is eventually constant, then denoting that constant by x', We replace $x_{n|}$ by $x_{n|} := x' + b^n$ and apply the above argument. (In this case, the argument is easier, because Formula (9) and the definition of $x_{n|}$ induce directly Formula (8).) This shows the desired assertion in this case and completes the proof of the theorem. □

5. Remaining Problems

All problems about the sequences $a \uparrow\uparrow n$ raised in [7] can be generalized to iterated polynomial. The most interesting one might be the following problem concerning

$${}^{\infty}f(a) := \lim_{n\to\infty} f \uparrow_a \uparrow_b (n) \in \widehat{\mathbb{Z}}.$$

Problem 1. Are ${}^{\infty}f(a)$ irrational, and transcendental over $\mathbb{Q}$ except trivial counterexamples such as ${}^{\infty}f(a) \in \mathbb{N}$ and the case $\mu_p \equiv 0 \mod p$ (see Proposition 4.5)? Are there some nontrivial algebraic, or analytic correlations among the number $\{{}^{\infty}f(a)\}_{f,a}$?

Relatively many of polynomials are tower-stable. Theorem 3.14 and Lemma 3.11 (ii) give the ratio C_{tow} of tower-stable function among all congruence preserving

functions as

$$\begin{aligned} C_{tow} &:= \int_{\mathrm{Cong}(\widehat{\mathbb{Z}})} \{f \mid f \text{ is tower-stable}\}\, d\mu \\ &= \prod_p \int_{\mathrm{Cong}(\mathbf{Z}_p)} \{f \mid f \text{ is not a cycle permutation of length } p\}\, d\mu_p \\ &= \prod_p \left(1 - \frac{(p-1)!}{p^p}\right) \sim 0.688, \end{aligned}$$

where $\mathrm{Cong}(\widehat{\mathbb{Z}})$ denotes the set of all congruence preserving functions and $\mathrm{Cong}(\mathbf{Z}_p)$ denotes the set of their reductions. The measures μ and μ_p are the additive Haar probability measures. It would be interesting to ask the following.

Problem 2. Is C_{tow} a transcendental number?

In Section 4, we focused on polynomials f. However, there exist congruence preserving maps on $\mathbb{N}$ which are not polynomial. The map $n \mapsto \lceil e^n n! \rceil$ considered in [2] is such an example. It is natural to consider the following problem.

Problem 3. Does Theorem 1.5 hold for every congruence preserving map?

Acknowledgements. Takao Watanabe encouraged me to try to write this paper and gave helpful comments on drafts of it. Takehiko Yasuda and Seidai Yasuda helped me in proofreading this paper and gave me warm encouragement. Without their contributions, this paper cannot be materialized. I would like to express my greatest appreciation to them. The author also thanks the referee(s) for providing important comments. Especially, Remark 4.4 and the examples below Definition 1.4 are added by incorporating to their suggestions. The author was supported by JSPS KAKENHI Grant-in-Aid for Research Fellow JP202122197.

References

[1] P. Cégielski, Arithmetical congruence preservation: from finite to infinite, in *Fields of Logic and Computation II*, Lecture Notes in Comput. Sci. 9300, Springer, Cham (2015), 210-225.

[2] P. Cégielski, S. Grigorieff and I. Guessarian, Newton representation of functions over natural integers having integral difference ratios, *Int. J. Number Theory* **11(7)** (2015), 2109-2139.

[3] Z. Chen, On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, *Discrete Math.* **137** (1995), 137-145.

[4] A. Fan and L. Liao, On minimal decomposition of p-adic polynomial dynamical systems, *Adv. Math.* **228,** no. 4, (2011), 2116-2144.

[5] J. J. Urroz and J. L. A. Yebra, On the equation $a^x \equiv x(\mod b^n)$, *J. Integer Seq.* **12** (2009), no. 8, Article 09.8.8.

[6] D. E. Knuth, Mathematics and computer science: coping with finiteness, *Science* **194** (1976), 1235-1242.

[7] D. B. Shapiro and S. D. Shapiro, Iterated exponents in number theory, *Integers* **7** (2007), #A23.