p-ADIC ASYMPTOTIC PROPERTIES OF CONSTANT-RECURSIVE SEQUENCES

ERIC ROWLAND AND REEM YASSAWI

Abstract. In this article we study p-adic properties of sequences of integers (or p-adic integers) that satisfy a linear recurrence with constant coefficients. For such a sequence, we give an explicit approximate twisted interpolation to $\mathbb{Z}_p$. We then use this interpolation for two applications. The first is that certain subsequences of constant-recursive sequences converge p-adically. The second is that the density of the residues modulo p^α attained by a constant-recursive sequence converges, as $\alpha \to \infty$, to the Haar measure of a certain subset of $\mathbb{Z}_p$. To illustrate these results, we determine some particular limits for the Fibonacci sequence.

1. Introduction

Many integer sequences $s(n)_{n\geq 0}$ that arise in combinatorial and number theoretic settings have the property that $(s(n) \bmod p^\alpha)_{n\geq 0}$ is a p-automatic sequence for each $\alpha \geq 0$ [9, 11]. As α varies, automata that produce these sequences have natural relationships to each other; namely, an automaton for a sequence modulo p^α necessarily contains all information about the sequence modulo smaller powers of p. However, there has not been a satisfactory way of letting $\alpha \to \infty$ and capturing information about all powers p^α simultaneously. The inverse limit of these automata is a *profinite automaton* [10]. In this paper we study properties of this profinite automaton for a sequence $s(n)_{n\geq 0}$ satisfying a linear recurrence with constant coefficients, by interpolating subsequences to the p-adic integers $\mathbb{Z}_p$. Namely, we are interested in p-adic limits of certain subsequences of $s(n)_{n\geq 0}$, as well as the limiting density of attained residues of $s(n)_{n\geq 0}$ modulo powers of p.

For example, let $F(n)$ be the nth Fibonacci number. Figure 1 shows the first 40 base-p digits of $F(p^n)$ for $p \in \{2, 5, 11\}$ and $0 \leq n \leq 10$. The digits 0 through $p-1$ are rendered in grey levels ranging from white to black. The $p = 2$ array suggests that $\lim_{n\to\infty} F(2^n)$ does not exist in $\mathbb{Z}_2$ but that $\lim_{n\to\infty} F(2^{2n})$ and $\lim_{n\to\infty} F(2^{2n+1})$ do. The $p = 5$ array suggests that $\lim_{n\to\infty} F(5^n) = 0$ in $\mathbb{Z}_5$, and the $p = 11$ array suggests that $\lim_{n\to\infty} F(11^n)$ exists in $\mathbb{Z}_{11}$ and is non-zero.

Date: May 3, 2017.

The first author was supported by a Marie Curie Actions COFUND fellowship.

Figure 1. Base-p digits of $F(p^n)$ for $p = 2$ (left), $p = 5$ (center), and $p = 11$ (right), for n in the interval $0 \leq n \leq 10$.

Other limits of this nature appear elsewhere in the literature. For example, analogous limits for binomial coefficients were shown to exist by Davis [4], and limits of subsequences of the *gyration* sequence were used by Boyle, Lind, and Rudolph [2, Section 8] to obtain information about the automorphism group of a symbolic dynamical system.

Regarding the Fibonacci sequence, Lenstra [7] showed that $F(n)_{n\geq 0}$ can be interpolated by an analytic function on the *profinite integers*. For $p \neq 2$, Bihani, Sheppard, and Young [1] showed that $(a^n F(bn))_{n\geq 0}$ can be interpolated to $\mathbb{Z}_p$ by a hypergeometric function for some integers a, b.

A constant-recursive sequence cannot generally be interpolated to $\mathbb{Z}_p$. Namely, since $\mathbb{N}$ is dense in $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is compact, a sequence $s(n)_{n\geq 0}$ can be interpolated to $\mathbb{Z}_p$ if and only if $(s(n) \bmod p^\alpha)_{n\geq 0}$ is purely periodic with period length equal to a power of p for every α. However, we show in Theorem 7 that every constant-recursive sequence has an *approximate* twisted interpolation to $\mathbb{Z}_p$, as defined in Section 3. In Theorem 10, we show that in general this is the best we can hope for. We identify in Corollary 8 a large family of constant-recursive sequences that have twisted interpolations to $\mathbb{Z}_p$.

Interpolation of this kind has been used previously to study arithmetic properties of constant-recursive sequences. For example, the Skolem–Mahler–Lech theorem [5, Theorem 2.1] for integer-valued constant-recursive sequences can be proved using interpolation. More recently, Shu and Yao [12, Theorem 3] implicitly used interpolation to characterize constant-recursive sequences of order 2 whose sequence of p-adic valuations is p-regular. In this article we pay particular attention to the constants one must introduce, which allows us to make explicit the number of functions that comprise the twisted interpolation.

In Section 2 we give the necessary background in p-adic analysis. In Section 3 we discuss twisted interpolations to $\mathbb{Z}_p$ of a sequence satisfying a linear recurrence with constant coefficients. In Section 4 we apply interpolations to the computation of p-adic limits and limiting densities of attained residues. In particular, we show in Theorem 13 that the limiting density of attained residues is the Haar measure of a certain set. In Section 5 we give a twisted interpolation for the Fibonacci sequence to $\mathbb{Z}_p$, we establish the limits suggested by Figure 1, and, in Theorem 20, we determine the limiting density of residues attained by the Fibonacci sequence modulo powers of 11.

2. Roots of unity in extensions of $\mathbb{Q}_p$

We use several results about finite extensions of the field $\mathbb{Q}_p$ of p-adic numbers. A complete exposition of the following results can be found in [6, Chapter 5].

If $a_i \in \{0, 1, \ldots, p-1\}$ for all $i \geq k$ and $a_k \neq 0$, recall that the p-adic absolute value is defined on $\mathbb{Q}_p$ by $|\sum_{i=k}^{\infty} a_i p^i|_p = p^{-k}$.

Theorem 1. *Let $K/\mathbb{Q}_p$ be a finite extension of degree d. For $x \in K$, let M_x be the matrix that corresponds to multiplication by x in K, and define the multiplicative function $N_{K/\mathbb{Q}_p} : K \to \mathbb{Q}_p$ as $N_{K/\mathbb{Q}_p}(x) := \det M_x$.*

(1) [6, Corollary 5.3.2 and Theorem 5.3.5] *There is exactly one non-Archimedean absolute value $|\ |_p$ on K extending the p-adic absolute value $|\ |_p$ on $\mathbb{Q}_p$, defined as*

$$|x|_p := \sqrt[d]{|N_{K/\mathbb{Q}_p}(x)|_p}.$$

(2) [6, Proposition 5.4.2] *Define the p-adic valuation $\nu_p : K \setminus \{0\} \to \mathbb{Q}$ as the unique number satisfying*

$$|x|_p = p^{-\nu_p(x)}.$$

Then the image of ν_p is $\frac{1}{e}\mathbb{Z}$, where e is a divisor of d.

The value e in Part (2) of Theorem 1 is called the *ramification index* of the extension $K/\mathbb{Q}_p$. Akin to the special role of p in $\mathbb{Z}_p$, we say $\pi \in K$ is a *uniformizer* if $\nu_p(\pi) = 1/e$.

Given an extension $K/\mathbb{Q}_p$ with absolute value $|\ |_p$, let

$$\mathcal{O}_K := \{x \in K : |x|_p \leq 1\}$$

denote the unit ball in K, and let

$$\mathcal{U}_K := \{x \in K : |x|_p < 1\}$$

denote its interior. Let $f := d/e$.

Proposition 2 ([6, Propositions 5.4.5 and 5.4.6])**.** *Let $K/\mathbb{Q}_p$ be a finite extension of degree d, with ramification index e, and $f = d/e$. Let $\pi \in K$ be a uniformizer. Then the following hold.*

(1) *$\mathcal{U}_K$ is a principal ideal of $\mathcal{O}_K$, and $\mathcal{U}_K = \pi\mathcal{O}_K$.*
(2) *The residue field $\mathcal{O}_K/\mathcal{U}_K$ is a finite field with p^f elements.*
(3) *If $\beta \in K$ is a root of a monic polynomial with coefficients in $\mathbb{Z}_p$, then $\beta \in \mathcal{O}_K$.*
(4) *Let $D = \{0, c_1, \ldots, c_{p^f-1}\}$ be a fixed set of representatives for the cosets of $\mathcal{U}_K$ in $\mathcal{O}_K$. Then any $x \in K$ has a unique expansion $x = \sum_{j=-k}^{\infty} a_j \pi^j$ with each $a_i \in D$.*

Part (4) of Proposition 2 indicates that elements of K have a structure analogous to those of $\mathbb{Q}_p$, with π playing the role of p.

Given an extension $K/\mathbb{Q}_p$, the p-adic logarithm

$$\log_p x := \sum_{m \geq 1} (-1)^{m+1} \frac{(x-1)^m}{m}$$

converges for $x \in 1 + \mathcal{U}_K$, i.e. for x belonging to $\{x \in \mathcal{O}_K : |x-1|_p < 1\}$. The p-adic exponential function

$$\exp_p x := \sum_{m \geq 0} \frac{x^m}{m!}$$

converges for x belonging to $\{x \in \mathcal{O}_K : |x|_p < p^{-1/(p-1)}\}$. If $|x-1|_p < p^{-1/(p-1)}$ then

$$x = \exp_p \log_p x.$$

For details, see [6, Section 5.5].

The next proposition guarantees the existence of certain roots of unity in $\mathcal{O}_K$.

Proposition 3 ([6, Corollary 5.4.9])**.** *Let $K/\mathbb{Q}_p$ be a finite extension of degree d, with ramification index e, and $f = d/e$. Then $\mathcal{O}_K^\times$ contains the cyclic group of $(p^f - 1)$-st roots of unity.*

The proof of Proposition 3 involves the appropriate version of Hensel's lemma, and in particular it implies that each (p^f-1)-st root of unity belongs to a distinct residue class modulo π. Since there are precisely p^f residue classes modulo π, it follows that, for each $x \in \mathcal{O}_K$ such that $x \not\equiv 0 \mod \pi$, there is a unique (p^f-1)-st root of unity congruent to x modulo π; we define $\omega(x)$ to be this root of unity. Note that $\omega(x)$ is independent of the choice of uniformizer. For $p \neq 2$ and a p-adic integer $x \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, $\omega(x)$ coincides with the *Teichmüller representative* of x, the $(p-1)$-st root of unity congruent to x modulo p.

3. Interpolation of a constant-recursive sequence

Let $\mathbb{N} = \{0, 1, \ldots\}$ be the set of natural numbers. Let $s(n)_{n\geq 0}$ be a sequence of p-adic integers satisfying a linear recurrence

$$s(n+\ell) + a_{\ell-1}s(n+\ell-1) + \cdots + a_1 s(n+1) + a_0 s(n) = 0 \tag{1}$$

with constant coefficients $a_i \in \mathbb{Z}_p$. As discussed in Section 1, in general $s(n)$ cannot be interpolated to $\mathbb{Z}_p$.

Definition 4. Let p be a prime, and let $q \geq 1$ be a power of p. Let $s(n)_{n\geq 0}$ be a sequence of p-adic integers. Suppose $\mathbb{N} = \bigcup_{j\in J} A_j$ is a finite partition of $\mathbb{N}$, with each A_j dense in $r + q\mathbb{Z}_p$ for some $0 \leq r \leq q-1$. Let K be a finite extension of $\mathbb{Q}_p$, and for each $j \in J$ let $s_j : \mathbb{Z}_p \to K$ be a continuous function.

- If $s(n) = s_j(n)$ for all $n \in A_j$ and $j \in J$, then we say that the family $\{(s_j, A_j) : j \in J\}$ is a *twisted interpolation* of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$.
- If there are non-negative constants C, D, with $D < 1$, such that $|s(n) - s_j(n)|_p \leq CD^n$ for all $n \in A_j$ and $j \in J$, then we say that $\{(s_j, A_j) : j \in J\}$ is an *approximate twisted interpolation* of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$.

In the case of a twisted interpolation, since A_j is dense in $r + q\mathbb{Z}_p$, the function $s_j(x)$ is the unique continuous function which agrees with $s(n)$ on A_j. Note that some authors refer to each of the functions s_j as a twisted interpolation. If all the functions s_j are the same then we have an *interpolation*. In this section we identify conditions that guarantee the existence of a twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$. If $s(n)_{n\geq 0}$ does not satisfy these conditions, we show that it can only be approximately interpolated. The sets A_j we will obtain are all of the form

$$A_{i,r} := \{m \geq 0 : m \equiv i \mod p^f - 1 \text{ and } m \equiv r \mod q\} \tag{2}$$

for some fixed f. The proof of the following lemma follows directly from the Chinese remainder theorem.

Lemma 5. *Let p be a prime, let $q \geq 1$ be a power of p, and let $f \geq 1$. For each $0 \leq i \leq p^f - 2$ and $0 \leq r \leq q-1$, the set $A_{i,r}$ is dense in $r + q\mathbb{Z}_p$.*

We recall the classical interpolation of the Fibonacci numbers to $\mathbb{R}$. Let $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. Using the generating function of the Fibonacci sequence, the nth Fibonacci number $F(n)$ can be written using Binet's formula

$$F(n) = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}}.$$

Thus to obtain an interpolation of $F(n)_{n\geq 0}$ to $\mathbb{R}$, it suffices to interpret

$$\frac{\phi^x - \bar{\phi}^x}{\sqrt{5}}$$

for $x \in \mathbb{R}$. We can write $\phi^n = (\exp\log\phi)^n = \exp(n\log\phi)$ since ϕ is positive, and it follows that ϕ^n is interpolated by $\exp(x\log\phi)$.

Because $\bar{\phi}$ is negative, we write

$$\bar{\phi}^n = (-1)^n(-\bar{\phi})^n = (-1)^n(\exp\log(-\bar{\phi}))^n = (-1)^n\exp(n\log(-\bar{\phi})),$$

and it remains to interpolate $(-1)^n$ to $\mathbb{R}$. A common, but not unique, choice is $\cos(\pi x)$. Therefore $F(n)_{n\geq 0}$ is interpolated to $\mathbb{R}$ by the analytic function

$$F(x) = \frac{\exp(x\log\phi) - \cos(\pi x)\exp(x\log(-\bar{\phi}))}{\sqrt{5}}.$$

The main idea of this section is to carry out such an interpolation to $\mathbb{Q}_p$ instead of $\mathbb{R}$. The nth term of the constant-recursive sequence $s(n)_{n\geq 0}$ can be written as a linear combination of terms of the form $n^j\beta^n$ in a suitable field extension, where β runs over the roots of the characteristic polynomial $g(x) = x^\ell + \cdots + a_1x + a_0$, and j runs over the integers from 0 to $m_\beta - 1$, where m_β is the multiplicity of β. In other words, we can write

$$s(n) = \sum_\beta c_\beta(n)\beta^n$$

for some polynomials $c_\beta(x) \in K[x]$, where we sum over all roots β of $g(x)$. The key step is to be able to legitimately write $x = \exp_p\log_p x$ for some modified version of the roots β. Lemma 6 tells us how to do this.

Lemma 6. *Let p be a prime. Let $g(x) \in \mathbb{Z}_p[x]$ be a monic polynomial, and let β be a root of $g(x)$ in a splitting field K of $g(x)$ over $\mathbb{Q}_p$, with $|\beta|_p = 1$. Let e be the ramification index of $K/\mathbb{Q}_p$. Let*

$$q = \begin{cases} 1 & \text{if } e < p-1 \\ p^{\lceil \log_p(e+1)\rceil} & \text{if } e \geq p-1, \end{cases} \tag{3}$$

where here $\log_p$ is the real logarithm to base p. Then $|(\frac{\beta}{\omega(\beta)})^q - 1|_p < p^{-1/(p-1)}$.

Proof. Let π be a uniformizer. Since $|\beta|_p = 1$, by Proposition 3 there exists a root of unity $\omega(\beta) \in \mathcal{O}_K$ which is congruent to β modulo π. We have

$$\left|\frac{\beta}{\omega(\beta)} - 1\right|_p = \frac{|\beta - \omega(\beta)|_p}{|\omega(\beta)|_p} = |\beta - \omega(\beta)|_p.$$

First suppose $e < p-1$, so that $q = 1$. Since $\beta \equiv \omega(\beta) \mod \pi$, we have

$$|\beta - \omega(\beta)|_p \leq |\pi|_p = p^{-1/e} < p^{-1/(p-1)}$$

as desired. Now suppose $e \geq p-1$, so that $q = p^{\lceil\log_p(e+1)\rceil}$. Since $\log_p(e+1) \leq \lceil\log_p(e+1)\rceil$, our choice of q implies $\pi^q \equiv 0 \mod p\pi$. Since $\beta \equiv \omega(\beta) \mod \pi$, Kummer's theorem then implies $\beta^q \equiv \omega(\beta)^q \mod p\pi$, so

$$|\beta^q - \omega(\beta)^q|_p \leq |p\pi|_p = p^{-1-1/e} < p^{-1/(p-1)}$$

since $1 + \frac{1}{e} > 1 \geq \frac{1}{p-1}$. □

We make two remarks regarding Lemma 6. The first is that the case $e \geq p-1$ in Equation (3) does occur. For example, consider the sequence defined by $s(n+3) = 2s(n)$ and $s(0) = s(1) = s(2) = 1$. Let $p = 3$. Then $K = \mathbb{Q}_3(\sqrt[3]{2})$, $e = 3 \geq 2 = p-1$, and $q = 9$.

The second remark is that the value of q given by Lemma 6 is not necessarily optimal. For example, the extension $K = \mathbb{Q}_2$ of degree 1 contains the square root of unity -1. This root of unity is not included in those guaranteed by Proposition 3, but allowing $\beta \in \mathbb{Z}_2 \setminus 2\mathbb{Z}_2$ to be divided by 1 or -1 allows us to reduce the value of q from 2 to 1.

We now state the main result of this section.

Theorem 7. *Let p be a prime, and let $s(n)_{n\geq 0}$ be a constant-recursive sequence of p-adic integers with monic characteristic polynomial $g(x) \in \mathbb{Z}_p[x]$. Then there exists an analytic approximate twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$.*

Proof. As in Lemma 6, let K be a degree-d splitting field of $g(x)$ over $\mathbb{Q}_p$ with ramification index e, and $f = d/e$. Let q be defined as in Equation (3). We have $s(n) = \sum_\beta c_\beta(n)\beta^n$ for some $c_\beta(x) \in K[x]$.

We mimic what is done to interpolate the Fibonacci numbers to $\mathbb{R}$. By Proposition 2, all roots of $g(x)$ lie in $\mathcal{O}_K$. Let $n \geq 0$ and $0 \leq r \leq q-1$. For each root β such that $|\beta|_p = 1$, we have

$$\begin{aligned}\beta^{qn+r} &= \omega(\beta)^{qn}\beta^r \left(\tfrac{\beta}{\omega(\beta)}\right)^{qn} \\ &= \omega(\beta)^{qn}\beta^r \left(\exp_p \log_p \left(\tfrac{\beta}{\omega(\beta)}\right)^{qn}\right) \\ &= \omega(\beta)^{qn}\beta^r \exp_p \left(n \log_p \left(\tfrac{\beta}{\omega(\beta)}\right)^{q}\right)\end{aligned}$$

by Lemma 6. Therefore

$$\begin{aligned}s(qn+r) &= \sum_\beta c_\beta(qn+r)\beta^{qn+r} \\ &= \sum_{|\beta|_p<1} c_\beta(qn+r)\beta^{qn+r} + \sum_{|\beta|_p=1} c_\beta(qn+r)\omega(\beta)^{qn}\beta^r \exp_p \left(n \log_p \left(\tfrac{\beta}{\omega(\beta)}\right)^{q}\right).\end{aligned}$$

We discard terms involving β^{qn+r} where $|\beta|_p < 1$ since these tend to 0 quickly. For the remaining terms, we must replace $\omega(\beta)^{qn}$ with a function defined on $\mathbb{Z}_p$.

When n is restricted to a fixed residue class modulo $p^f - 1$, the expression $\omega(\beta)^{qn}$ is constant, and we can now define, for each $0 \leq i \leq p^f - 2$ and $0 \leq r \leq q-1$,

$$s_{i,r}(qx+r) := \sum_{|\beta|_p=1} c_\beta(qx+r)\omega(\beta)^{i-r}\beta^r \exp_p \left(x \log_p \left(\tfrac{\beta}{\omega(\beta)}\right)^{q}\right)$$

for $x \in \mathbb{Z}_p$.

Recall $A_{i,r} = \{m \geq 0 : m \equiv i \mod p^f - 1 \text{ and } m \equiv r \mod q\}$ for $0 \leq i \leq p^f - 2$ and $0 \leq r \leq q-1$. Then for $m \in A_{i,r}$, $s_{i,r}(m)$ agrees with the second sum in the expression for $s(m)$.

We claim that $\{(s_{i,r}, A_{i,r}) : 0 \leq i \leq p^f - 2 \text{ and } 0 \leq r \leq q-1\}$ is an analytic approximate twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$. By Lemma 5, each set $A_{i,r}$ has the correct density property. Since $|\log_p(\frac{\beta}{\omega(\beta)})^q|_p < p^{-1/(p-1)}$ for each β satisfying $|\beta|_p = 1$, the expression

$$\exp_p \left(x \log_p \left(\tfrac{\beta}{\omega(\beta)}\right)^{q}\right)$$

is well defined for $x \in \mathbb{Z}_p$. Therefore the function $x \mapsto s_{i,r}(qx+r)$ is analytic on $\mathbb{Z}_p$. Since each c_β is continuous, and $\mathbb{Z}_p$ is compact, we can define $C =$

$\max_{|\beta|<1} \max_{x\in\mathbb{Z}_p} |c_\beta(x)|_p$. Then for $n \in A_{i,r}$ we have

$$|s(n) - s_{i,r}(n)|_p = \left| \sum_{|\beta|_p<1} c_\beta(n)\beta^n \right|_p \leq \max_{|\beta|_p<1} |c_\beta(n)\beta^n|_p \leq C \left(\max_{|\beta|_p<1} |\beta|_p \right)^n,$$

where we interpret a maximum over the empty set to be 0, and 0^0 to be 0. □

Remark. We do not use the fact that the functions c_β are polynomials, but only that they are continuous. Hence the proof of Theorem 7 works more generally for any sequence $s(n)_{\geq 0}$ which can be written $s(n) = \sum_\beta c_\beta(n)\beta^n$ as a sum over a finite set $B \subset \mathcal{O}_K$, where the functions c_β are arbitrary continuous functions.

Example. Let $s(0) = s(1) = s(2) = 1$, and $s(n+3) = 3s(n+2)+2s(n+1)-6s(n)$. Let $p = 2$. Then the roots of the characteristic polynomial are 3 and $\pm\sqrt{2}$. Because of these last two roots, $s(n) \neq s_{i,r}(n)$, and Theorem 7 gives only an approximate twisted interpolation.

The proof of Theorem 7 gives us sufficient conditions for a constant-recursive sequence $s(n)_{n\geq 0}$ to have an analytic twisted interpolation to $\mathbb{Z}_p$. If $g(x) = x^\ell + \cdots + a_1x + a_0 \in \mathbb{Z}_p[x]$ is a monic characteristic polynomial for $s(n)_{n\geq 0}$, with $s(n) = \sum_\beta c_\beta(n)\beta^n$ and

$$\{\beta : |\beta|_p < 1 \text{ and } c_\beta \text{ is not the 0 polynomial}\} = \emptyset,$$

then there exists an analytic twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$. In particular, since, up to a unit, $a_0 = \prod_\beta \beta$, we have the following corollary.

Corollary 8. *Let p be a prime, and let $s(n)_{n\geq 0}$ be a constant-recursive sequence of p-adic integers with monic characteristic polynomial $x^\ell + \cdots + a_1x + a_0 \in \mathbb{Z}_p[x]$. If $|a_0|_p = 1$, then there exists a twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$.*

If all roots of $g(x)$ satisfy $|\beta|_p = 1$, then we can extend $s(n)_{n\geq 0}$ to a two-sided sequence $s(n)_{n\in\mathbb{Z}}$ of p-adic integers satisfying Recurrence (1). In this case, Theorem 7 implies that $s(n) = s_{i,r}(n)$ for all $n \in \mathbb{Z}$ such that $n \equiv i \mod p^f - 1$ and $n \equiv r \mod q$. Additionally, we obtain the following corollary. We continue to assume the hypotheses of Theorem 7.

Corollary 9. *If $e < p - 1$ and all roots of $g(x)$ satisfy $\beta \equiv 1 \mod \pi$, then $s(n)$ can be interpolated to $\mathbb{Z}_p$.*

Proof. Since $\beta \equiv 1 \mod \pi$, we have $\omega(\beta) = 1$. It follows from Theorem 7 that, for a fixed r, the functions $s_{i,r}(qx + r)$ coincide for all i. Since $e < p - 1$, we have $q = 1$, and therefore the only value of r is $r = 0$, so $s(n) = s_{0,0}(n)$ for all $n \geq 0$. □

Example. Let $p \geq 5$. Let $s(0) = s(1) = 1$, and let $s(n+2) = 2s(n+1)+(p-1)s(n)$. Then $e \leq 2 < p - 1$, and the roots of $x^2 - 2x - (p - 1)$ are congruent to 1 modulo π. Therefore $s(n)_{n\geq 0}$ can be interpolated to $\mathbb{Z}_p$.

Our next result tells us that Theorem 7 is the best that we can hope for.

Theorem 10. *Let p be a prime and K a finite extension of $\mathbb{Q}_p$. Suppose that B is a nonempty finite set of elements of K such that $|\beta|_p < 1$ for each $\beta \in B$. For each $\beta \in B$, let $c_\beta : \mathbb{Z}_p \to K$ be a continuous function. For $n \in \mathbb{N}$, define $s(n) = \sum_{\beta\in B} c_\beta(n)\beta^n$, and suppose that there is a twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$. Then $s(n) = 0$ for all $n \geq 0$.*

Proof. Let (s_j, A_j) be a twisted interpolation for $s(n)_{n\geq 0}$. Let $x \in \mathbb{Z}_p \setminus \mathbb{N}$, and define $k_n \in \mathbb{N}$ by $k_n = (x \bmod p^n)$. Fix j. The closure $\overline{A}_j$ of each partition element A_j in $\mathbb{Z}_p$ satisfies $\overline{A}_j = r + q\mathbb{Z}_p$ for some $0 \leq r \leq q-1$, where q is as in Definition 4; this implies that there exists $x \in \mathbb{Z}_p \setminus \mathbb{N}$ such that $k_n \in A_j$ for sufficiently large n. Now fix any such $x \in \overline{A}_j \setminus A_j$. As $n \to \infty$, the continuity of s_j implies that $s(k_n) = s_j(k_n) \to s_j(x)$. On the other hand, as $n \to \infty$, $\beta^{k_n} \to 0$ for each β, and we have that $s(k_n) \to 0$. Thus s_j is identically zero on $\overline{A}_j \setminus A_j$. Since $\overline{A}_j = r + q\mathbb{Z}_p$, if $k \in A_j$ then there exists a sequence of elements $(x_n)_{n\geq 0}$ in $\overline{A}_j \setminus A_j$, such that $x_n \to k$, and now continuity of s_j again tells us that $s(k) = 0$. □

Example. Consider the sequence defined by $s(n+2) = 2s(n)$ and $s(0) = s(1) = 1$. Let $p = 2$. The roots of the characteristic polynomial are $\pm\sqrt{2}$. Since $\sqrt{2}$ is a uniformizer of $\mathbb{Q}_2(\sqrt{2})/\mathbb{Q}_2$, Theorem 10 tells us that there is no twisted interpolation of $s(n)_{n\geq 0}$ to $\mathbb{Z}_p$.

4. Limits and distribution of residues

In this section we describe two applications of Theorem 7. The first concerns p-adic limits of subsequences of constant-recursive sequences, such as the limits suggested by Figure 1. The second concerns the density of residues modulo p^α attained by a constant-recursive sequence.

Using the power series of Theorem 7, we can compute limits of $s(n)$ along sequences of points in $A_{i,r}$.

Corollary 11. *Let $a, b \in \mathbb{Z}$ with $a \geq 1$. Under the hypotheses of Theorem 7, the limit $\lim_{n\to\infty} s(ap^{fn} + b)$ exists in $\mathbb{Z}_p$ and is equal to*

$$\lim_{n\to\infty} s(ap^{fn} + b) = \sum_{|\beta|_p = 1} c_\beta(b)\omega(\beta)^a \beta^b$$

In particular, the value of this limit is algebraic over $\mathbb{Q}_p$.

We note that if the coefficients $a_{\ell-1}, \ldots, a_0$ in Recurrence (1) are integers and $s(n)_{n\geq 0}$ is integer-valued, then the limit above is algebraic over $\mathbb{Q}$.

Proof. For sufficiently large n, we have $ap^{fn}+b \equiv a+b \mod p^f-1$ and $ap^{fn}+b \equiv b \mod q$. Therefore

$$|s(ap^{fn} + b) - s_{a+b,(b \bmod q)}(ap^{fn} + b)|_p \leq C \left(\max_{|\beta|_p \neq 1} |\beta|_p \right)^{ap^{fn}+b}.$$

As $n \to \infty$, the right side of the inequality tends to 0, so we have

$$\begin{aligned} \lim_{n\to\infty} s(ap^{fn} + b) &= \lim_{n\to\infty} s_{a+b,(b \bmod q)}(ap^{fn} + b) \\ &= s_{a+b,(b \bmod q)}(b) \\ &= \sum_{|\beta|_p = 1} c_\beta(b)\omega(\beta)^a \beta^b \end{aligned}$$

by continuity of $s_{i,r}(qx + r)$. □

Corollary 11 is a generalization of the fact that if $\beta \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ then $\lim_{n\to\infty} \beta^{p^n} = \omega(\beta)$. This can be seen since $s(n) = \beta^n$ satisfies the recurrence $s(n+1) = \beta s(n)$ of order 1. For example, see [8].

It also follows from Corollary 11 that the sequence

$$\left(\lim_{n\to\infty} s(ap^{fn}+b)\right)_{b\geq 0}$$

of p-adic integers satisfies Recurrence (1), the original recurrence satisfied by $s(n)_{n\geq 0}$. Other limits, such as $\lim_{n\to\infty} s(a_2p^{2fn}+a_1p^{fn}+b)$, can be computed similarly.

If all roots of $g(x)$ satisfy $|\beta|_p = 1$, then we can relax the hypotheses of Corollary 11 and allow a to be an arbitrary integer, obtaining the same conclusion. Additionally, we have the following.

Corollary 12. *Under the hypotheses of Theorem 7, if $a \in (p^f-1)\mathbb{Z}$ and all roots of $g(x)$ satisfy $|\beta|_p = 1$, then we obtain the integer limit*

$$\lim_{n\to\infty} s(ap^{fn}+b) = s(b).$$

Proof. The computation in the proof of Corollary 11 shows that

$$\lim_{n\to\infty} s(ap^{fn}+b) = \sum_{\beta} c_\beta(b)\omega(\beta)^a\beta^b = \sum_{\beta} c_\beta(b)\beta^b = s(b). \qquad \square$$

Our second application of the power series of Theorem 7 is determining the value of the limiting density

$$\lim_{\alpha\to\infty} \frac{|\{s(n) \bmod p^\alpha : n\geq 0\}|}{p^\alpha}$$

of attained residues. This limit exists since the sequence of densities modulo powers of p is a non-increasing sequence bounded below by 0. Let μ be the Haar measure on $\mathbb{Z}_p$ defined by $\mu(m+p^\alpha\mathbb{Z}_p) = p^{-\alpha}$. For $f\geq 1$ and $q\geq 1$ a power of p, recall the definition of the family of sets $A_{i,r}$ in Equation (2).

Theorem 13. *Let $s(n)_{n\geq 0}$ be a sequence of p-adic integers with an approximate twisted interpolation $\{(s_{i,r}, A_{i,r}) : 0\leq i\leq p^f-2$ and $0\leq r\leq q-1\}$. Then*

$$\lim_{\alpha\to\infty} \frac{|\{s(n) \bmod p^\alpha : n\geq 0\}|}{p^\alpha} = \mu\left(\mathbb{Z}_p \cap \bigcup_{i,r} s_{i,r}(r+q\mathbb{Z}_p)\right).$$

Proof. First, note that

$$|\{s(n) \bmod p^\alpha : n\geq 0\}| = \left|\overline{s(\mathbb{N})} \bmod p^\alpha\right|.$$

For $n\in A_{i,r}$, define $t(n) = s_{i,r}(n)$. Let the extension K and the constants C, D be as in Definition 4. For all $n\geq 0$, we have $|s(n)-t(n)|_p \leq CD^n$, so $\overline{s(\mathbb{N})} = \mathbb{Z}_p\cap\overline{t(\mathbb{N})}$. Since $\frac{\left|\overline{s(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha}$ and $\frac{\left|\mathbb{Z}_p\cap\overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha}$ are non-increasing functions of α, the limits exist and

$$\lim_{\alpha\to\infty} \frac{\left|\overline{s(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} = \lim_{\alpha\to\infty} \frac{\left|\mathbb{Z}_p\cap\overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha}.$$

Therefore it suffices to work with $t(n)$. Note that in the case of a twisted interpolation, $s(n) = t(n)$ and we work in $\mathbb{Z}_p$, but in general $t(n)$ is an element of $\mathcal{O}_K$.

By Lemma 5, we have $r+q\mathbb{Z}_p = \overline{A_{i,r}}$ for each i and r, so

$$\overline{t(\mathbb{N})} = \bigcup_{i,r} \overline{s_{i,r}(A_{i,r})} = \bigcup_{i,r} s_{i,r}(r+q\mathbb{Z}_p).$$

Note that $\overline{t(\mathbb{N})} = t(\mathbb{Z}_p)$ is compact, and hence closed, in K. It follows that $\mathbb{Z}_p \cap \overline{t(\mathbb{N})}$ is closed in $\mathbb{Z}_p$. The set $\mathbb{Z}_p \setminus \overline{t(\mathbb{N})}$ is open, so it is a countable union of cylinder sets, i.e. sets of the form $k + p^\beta \mathbb{Z}_p$, where $k \in \mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a countable union of cylinder sets, it follows that $\mathbb{Z}_p \cap \overline{t(\mathbb{N})}$ is also a countable union of cylinder sets and is therefore measurable. It follows that

$$\mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big) = \mu\left(\mathbb{Z}_p \cap \bigcup_{i,r} s_{i,r}(r + q\mathbb{Z}_p)\right).$$

It remains to show that

$$\lim_{\alpha\to\infty} \frac{\left|\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} = \mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big).$$

Let

$$S_\alpha := \bigcup_{k \in \left(\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right)} k + p^\alpha \mathbb{Z}_p.$$

Since $\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \subset S_\alpha$, it follows that $\frac{\left|\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} \geq \mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big)$ for each α, and so $\lim_{\alpha\to\infty} \frac{\left|\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} \geq \mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big)$.

To establish the other inequality, we fix $\epsilon > 0$ and we suppose that for some α, $\frac{\left|\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} > \mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big) + \epsilon$, i.e. $\mu\Big(S_\alpha \setminus \overline{t(\mathbb{N})}\Big) > \epsilon$. Since $S_\alpha \setminus \overline{t(\mathbb{N})}$ is open, there exists a set $T \subset S_\alpha \setminus \overline{t(\mathbb{N})}$, which is a finite union of cylinder sets, and whose μ-mass is at least $\frac{\epsilon}{2}$. There exists $\beta > \alpha$ such that T is a union of cylinder sets all of which are of the form $k + p^\beta \mathbb{Z}_p$. Then $\mu(S_\beta) \leq \mu(S_\alpha) - \frac{\epsilon}{2}$. If $\mu\Big(S_\beta \setminus \overline{s(\mathbb{N})}\Big) > \epsilon$, we iterate this procedure until we find a γ with $\mu\Big(S_\gamma \setminus \overline{s(\mathbb{N})}\Big) < \epsilon$, and hence $\lim_{\alpha\to\infty} \frac{\left|\mathbb{Z}_p \cap \overline{t(\mathbb{N})} \bmod p^\alpha\right|}{p^\alpha} \leq \mu\Big(\mathbb{Z}_p \cap \overline{t(\mathbb{N})}\Big) + \epsilon$. As this is true for any $\epsilon > 0$, this completes the proof. □

We apply Theorem 13 to compute the limiting density of residues attained by the Fibonacci sequence modulo 11^α in Theorem 20. We suspect that the method we use there generalizes to any p and any constant-recursive sequence.

5. The Fibonacci sequence

In this section we apply the results from Sections 3 and 4 to the Fibonacci sequence $F(n)_{n\geq 0}$, which satisfies

$$F(n+2) - F(n+1) - F(n) = 0$$

with initial conditions $F(0) = 0$ and $F(1) = 1$. Accordingly, we take $K = \mathbb{Q}_p(\phi)$, where ϕ is a root of $x^2 - x - 1$. Let $\bar{\phi}$ be the other root. Note that $\sqrt{5} := 2\phi - 1 \in \mathbb{Q}_p(\phi)$, and in fact $\mathbb{Q}_p(\sqrt{5}) = \mathbb{Q}_p(\phi)$. The ramification index of the extension $\mathbb{Q}_p(\phi)/\mathbb{Q}_p$ is as follows.

Lemma 14. *Let p be a prime, and let d be the degree of the extension $\mathbb{Q}_p(\phi)/\mathbb{Q}_p$.*

- *If $p \equiv 1, 4 \mod 5$, then $\phi \in \mathbb{Q}_p$, so $e = d = 1$.*
- *If $p \equiv 2, 3 \mod 5$, then $\phi \notin \mathbb{Q}_p$ and $e = 1$ and $d = 2$.*
- *If $p = 5$, then $\phi \notin \mathbb{Q}_5$ and $e = d = 2$.*

For $p = 5$ we take the uniformizer to be $\pi = \sqrt{5}$. For other primes we take $\pi = p$. Throughout this section, e denotes the ramification index of $\mathbb{Q}_p(\phi)/\mathbb{Q}_p$, as determined in Lemma 14, and $f = d/e$.

For primes $p \neq 2$ we obtain the following.

Theorem 15. *Let $p \neq 2$ be a prime, and let $0 \leq i \leq p^f - 2$. Define the function $F_i : \mathbb{Z}_p \to \mathbb{Z}_p$ by*

$$F_i(x) = \sum_{m \geq 0} \frac{\left(\omega(\phi)^i - (-1)^m \omega(\bar{\phi})^i\right) \left(\log_p \frac{\phi}{\omega(\phi)}\right)^m}{m!\sqrt{5}} x^m,$$

and let $A_i = \{n \geq 0 : n \equiv i \mod p^f - 1\}$. Then $\{(F_i, A_i) : 0 \leq i \leq p^f - 2\}$ is a twisted interpolation of $F(n)_{n \geq 0}$ to $\mathbb{Z}_p$.

Proof. Since $p \neq 2$, we have $q = 1$ by Equation (3). We have

$$F(n) = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}}$$

for each integer $n \geq 0$. The roots of $x^2 - x - 1$ satisfy $|\phi|_p = |\bar{\phi}|_p = 1$. By Theorem 7,

$$\frac{\omega(\phi)^i \exp_p\left(x \log_p \frac{\phi}{\omega(\phi)}\right) - \omega(\bar{\phi})^i \exp_p\left(x \log_p \frac{\bar{\phi}}{\omega(\bar{\phi})}\right)}{\sqrt{5}}$$

defines an analytic function on $\mathbb{Z}_p$ which agrees with $F(n)$ on A_i. Expanding the power series for $\exp_p$ gives

$$\sum_{m \geq 0} \frac{\omega(\phi)^i \left(\log_p \frac{\phi}{\omega(\phi)}\right)^m - \omega(\bar{\phi})^i \left(\log_p \frac{\bar{\phi}}{\omega(\bar{\phi})}\right)^m}{m!\sqrt{5}} x^m.$$

We claim that $\log_p \frac{\bar{\phi}}{\omega(\bar{\phi})} = -\log_p \frac{\phi}{\omega(\phi)}$. Since $p \neq 2$, we have $-1 = \phi \cdot \bar{\phi} \equiv \omega(\phi)\omega(\bar{\phi}) \mod \pi$; since -1 and $\omega(\phi)\omega(\bar{\phi})$ are both $(p^f - 1)$-st roots of unity, this implies $\omega(\phi)\omega(\bar{\phi}) = -1$. Therefore

$$\log_p \frac{\phi}{\omega(\phi)} + \log_p \frac{\bar{\phi}}{\omega(\bar{\phi})} = \log_p 1 = 0,$$

and

$$F_i(x) = \sum_{m \geq 0} \frac{\left(\omega(\phi)^i - (-1)^m \omega(\bar{\phi})^i\right) \left(\log_p \frac{\phi}{\omega(\phi)}\right)^m}{m!\sqrt{5}} x^m. \qquad \square$$

For $p = 2$ one can also state a version of Theorem 15, where there are 6 functions in the twisted interpolation since $q = p = 2$.

For $p = 5$ it turns out that $F_i(x)$ simplifies somewhat, allowing us to interpolate a twisted Fibonacci sequence to $\mathbb{Z}_5$. Define the p-adic hyperbolic sine by

$$\sinh_p(x) := \frac{\exp_p(x) - \exp_p(-x)}{2} = \sum_{m \geq 0} \frac{1}{(2m+1)!} x^{2m+1}.$$

Corollary 16. *Let $p = 5$. The function $F(n)/\omega(3)^n$ can be extended to an analytic function on $\mathbb{Z}_5$, namely*

$$\frac{2}{\sqrt{5}} \sinh_5\left(x \log_5 \frac{\phi}{\omega(3)}\right).$$

Proof. One checks that $\phi \equiv \bar{\phi} \equiv 3 \mod \sqrt{5}$ in $\mathcal{O}_{\mathbb{Q}_5(\phi)}$, so that $\omega(\phi) = \omega(\bar{\phi}) = \omega(3)$, and the coefficient of x^m is 0 for even m. Therefore, for every integer n, we have

$$F(n) = \sum_{m \geq 0} \frac{2\,\omega(3)^n \left(\log_5 \frac{\phi}{\omega(3)}\right)^{2m+1}}{(2m+1)!\sqrt{5}} n^{2m+1} = \frac{2\,\omega(3)^n}{\sqrt{5}} \sinh_5\left(n \log_5 \tfrac{\phi}{\omega(3)}\right). \quad \square$$

Bihani, Sheppard, and Young [1] similarly showed that $2^n F(n)$ can be extended to an analytic function on $\mathbb{Z}_5$, in this case by a hypergeometric series.

Since $\omega(3)^{5^n} = \omega(3)$ in $\mathbb{Z}_5$ for all $n \geq 0$, from Corollary 16 we see that the coefficient of x^0 in the power series expansion of $\frac{2}{\sqrt{5}} \sinh_5\left(x \log_5 \frac{\phi}{\omega(3)}\right)$ is $\lim_{n\to\infty} F(5^n) = 0$. Moreover, the coefficient of x^1 is

$$\lim_{n\to\infty} \frac{F(5^n)}{5^n} = \frac{2\,\omega(3)}{\sqrt{5}} \log_5 \tfrac{\phi}{\omega(3)},$$

the 5-adic digits of which comprise the diagonal stripes seen in Figure 1. Other coefficients of this power series can be obtained as limits similarly.

Corollary 11 allows us to establish the other limits suggested by Figure 1. For a prime p and $a, b \in \mathbb{Z}$, we have

$$\lim_{n\to\infty} F(ap^{fn} + b) = \frac{\omega(\phi)^a \phi^b - \omega(\bar{\phi})^a \bar{\phi}^b}{\sqrt{5}}.$$

For $p = 2$ one computes that $\lim_{n\to\infty} F(p^{2n})$ and $\lim_{n\to\infty} F(p^{2n+1})$ are equal to $\pm\sqrt{-\frac{3}{5}}$. For $p = 11$ the limit $\lim_{n\to\infty} F(p^n)$ is a root of $5x^2 + 5x + 1$.

We now turn to an application of Theorem 13. A number of authors have studied the distribution of residues of the Fibonacci sequence modulo m. Burr [3] characterized the integers m such that $(F(n) \bmod m)_{n\geq 0}$ contains all residue classes modulo m. In particular, the Fibonacci numbers attain all residues modulo 3^α and all residues modulo 5^α.

The limiting densities of attained residues modulo powers of other primes can be determined by Theorem 13. We conclude the paper by determining the limiting density of residues for $p = 11$. In this case, $f = d = 1$, so the twisted interpolation of the Fibonacci sequence to $\mathbb{Z}_{11}$ consists of 10 functions $F_0, \ldots, F_9$. By Theorem 13,

$$\lim_{\alpha\to\infty} \frac{|\{F(n) \bmod 11^\alpha : n \geq 0\}|}{11^\alpha} = \mu\left(\bigcup_{i=0}^{9} F_i(\mathbb{Z}_{11})\right).$$

Therefore it suffices to determine $F_i(\mathbb{Z}_{11})$ for each i in the interval $0 \leq i \leq 9$.

Lemma 17. *Let $p = 11$, and let $0 \leq i \leq 9$ such that $i \neq 5$. Then $F_i(\mathbb{Z}_{11}) = (F(i) \bmod 11) + 11\mathbb{Z}_{11}$.*

Proof. We determine the set $F_i(\mathbb{Z}_{11})$ by decomposing $F_i(x)$ as the composition of two simpler functions. Using $\omega(\phi)\omega(\bar{\phi}) = -1$ and $\log_{11} \frac{\bar{\phi}}{\omega(\bar{\phi})} = -\log_{11} \frac{\phi}{\omega(\phi)}$, we

have from the proof of Theorem 15 that

$$\begin{aligned} F_i(x) &= \frac{\omega(\phi)^i \exp_{11}\left(x \log_{11} \frac{\phi}{\omega(\phi)}\right) - \omega(\bar{\phi})^i \exp_{11}\left(-x \log_{11} \frac{\phi}{\omega(\phi)}\right)}{\sqrt{5}} \\ &= \frac{\omega(\phi)^i \exp_{11}\left(x \log_{11} \frac{\phi}{\omega(\phi)}\right) - (-1)^i \omega(\phi)^{-i} \exp_{11}\left(-x \log_{11} \frac{\phi}{\omega(\phi)}\right)}{\sqrt{5}} \\ &= \frac{h_i(x) - (-1)^i h_i(x)^{-1}}{\sqrt{5}} \end{aligned}$$

where $h_i(x) = \omega(\phi)^i \exp_{11}\left(x \log_{11} \frac{\phi}{\omega(\phi)}\right)$.

One computes $\left|\log_{11} \frac{\phi}{\omega(\phi)}\right|_{11} = \frac{1}{11}$, so $\left(\log_{11} \frac{\phi}{\omega(\phi)}\right) \mathbb{Z}_{11} = 11\mathbb{Z}_{11}$. Since $\exp_{11}$ is an isomorphism from the additive group $11\mathbb{Z}_{11}$ to the multiplicative group $1 + 11\mathbb{Z}_{11}$, we have

$$h_i(\mathbb{Z}_{11}) = \omega(\phi)^i(1 + 11\mathbb{Z}_{11}) = (\phi^i \bmod 11) + 11\mathbb{Z}_{11}.$$

It remains to show that the image of $(\phi^i \bmod 11) + 11\mathbb{Z}_{11}$ under the function $y \mapsto \frac{1}{\sqrt{5}}(y - (-1)^i y^{-1})$ is $(F(i) \bmod 11) + 11\mathbb{Z}_{11}$. Let

$$z \in \left(\frac{\phi^i - (-1)^i \phi^{-i}}{\sqrt{5}} \bmod 11\right) + 11\mathbb{Z}_{11} = (F(i) \bmod 11) + 11\mathbb{Z}_{11}.$$

We apply Hensel's lemma to show that there exists $y \in (\phi^i \bmod 11) + 11\mathbb{Z}_{11}$ such that $\frac{1}{\sqrt{5}}(y - (-1)^i y^{-1}) = z$, or, equivalently, $y^2 - \sqrt{5}zy - (-1)^i = 0$. From our choice of z, it is clear that $y_0 = \phi^i$ satisfies this polynomial equation modulo 11. Then we must check that $2y_0 - \sqrt{5}z \not\equiv 0 \mod 11$. The ring $\mathbb{Z}_{11}$ contains two square roots of 5; without loss of generality, choose $\sqrt{5} \equiv 7 \mod 11$. Then $\phi \equiv 4 \mod 11$, so $2y_0 - \sqrt{5}z \not\equiv 0 \mod 11$ if and only if $2 \cdot 4^i - (4^i - (-1)^i 4^{-i}) \not\equiv 0 \mod 11$, which is true since $i \neq 5$. □

Figure 2 shows the first several levels of the infinite rooted tree in which the vertices at level α consist of all residues m modulo 11^α such that $F(n) \equiv m \mod 11^\alpha$ for some $n \geq 0$. Two vertices at consecutive levels α and $\alpha + 1$ are connected by an edge if the residue at level $\alpha + 1$ projects to the residue at level α, and the edge is labeled with the extra base-11 digit in the residue at level $\alpha + 1$. Framed residues represent full infinite 11-ary subtrees: to simplify the diagram we suppress these full subtrees.

It follows from Lemma 17 that

$$\bigcup_{i \neq 5} F_i(\mathbb{Z}_{11}) = \bigcup_{i \neq 5} (F(i) \bmod 11) + 11\mathbb{Z}_{11} = \bigcup_{m \in \{0,1,2,3,8,10\}} m + 11\mathbb{Z}_{11}.$$

Accordingly, level $\alpha = 1$ of Figure 2 contains the residues $\{0, 1, 2, 3, 8, 10\}$, and the outgoing edges from these vertices are suppressed since they consist of full 11-ary subtrees. Level $\alpha = 1$ also contains the residue 5; we will see that this residue has a unique residue modulo 11^2 that projects onto it.

It remains to determine $F_5(\mathbb{Z}_{11})$. We continue to choose $\sqrt{5} \equiv 7 \mod 11$. We need to determine for which $z \in \mathbb{Z}_{11}$ the equation $y^2 - \sqrt{5}zy + 1 = 0$ has a solution in $\phi^5 + 11\mathbb{Z}_{11} = 1 + 11\mathbb{Z}_{11}$. If $z = \frac{2}{\sqrt{5}}$, the equation becomes $(y - 1)^2 = 0$, which clearly has a solution in $1 + 11\mathbb{Z}_{11}$. Consequently, the tree in Figure 2 contains an

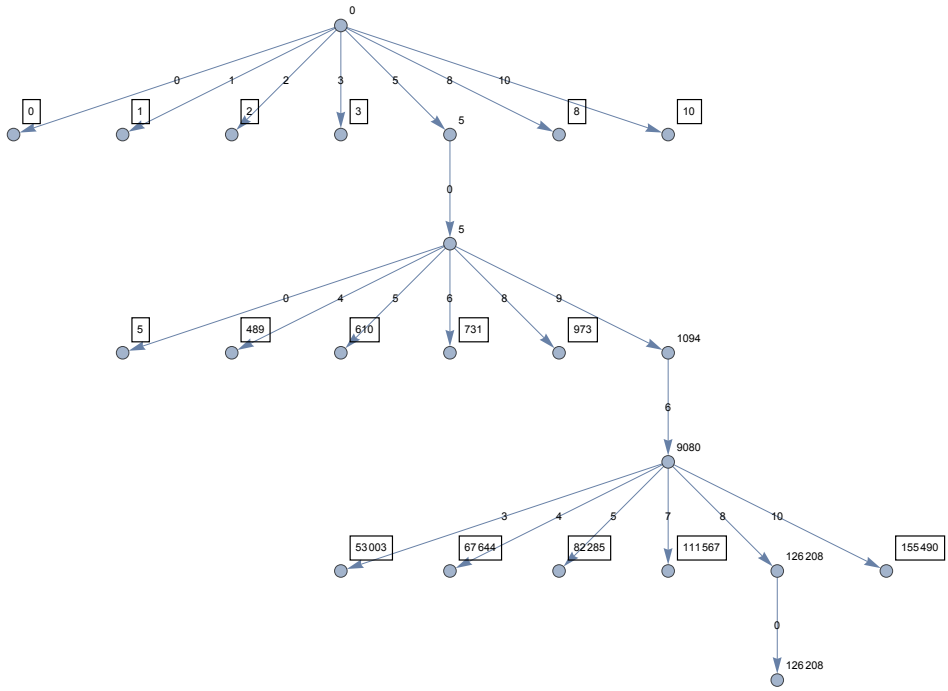

FIGURE 2. The tree of the residues attained by the Fibonacci sequence modulo small powers of 11.

infinite path corresponding to the 11-adic expansion of $\frac{2}{\sqrt{5}}$, and it is precisely along this path that more complicated branching occurs.

Lemma 18. *Let $\alpha \geq 1$ and $j \in \{1, \ldots, 10\}$. Let $z \equiv \frac{2}{\sqrt{5}} + j\,11^{2\alpha} \mod 11^{2\alpha+1}$. Let $f_z(y) := y^2 - \sqrt{5}zy + 1$.*

- *If $j \in \{2, 6, 7, 8, 10\}$ then $f_z(y)$ has a root $y \in \mathbb{Z}_{11}$ satisfying $|y - 1|_{11} < 1/11^{\alpha}$.*
- *If $j \in \{1, 3, 4, 5, 9\}$ then $f_z(y)$ has no root in $\mathbb{Z}_{11}$.*

Proof. We use the following version of Hensel's lemma: If there is an integer a such that $|f_z(a)|_p < |f_z'(a)|_p^2$, then there is a unique p-adic integer y such $f_z(y) = 0$ and $|y - a|_p < |f_z'(a)|_p$.

There are 6 quadratic residues modulo 11, namely 0, 1, 3, 4, 5, and 9. If $j \in \{2, 6, 7, 8, 10\}$ then there exists $a' \in \{1, \ldots, 10\}$ such that $a'^2 - \sqrt{5}j \equiv 0 \mod 11$. We check that $a = 1 + 11^{\alpha}a'$ satisfies the conditions of Hensel's lemma. We have

$$\begin{aligned} f_z(a) &= a^2 - \sqrt{5}za + 1 \\ &\equiv a^2 - \left(2 + \sqrt{5}j\,11^{2\alpha}\right)a + 1 \mod 11^{2\alpha+1} \\ &\equiv \left(a'^2 - \sqrt{5}j\right)11^{2\alpha} \mod 11^{2\alpha+1} \\ &\equiv 0 \mod 11^{2\alpha+1}. \end{aligned}$$

On the other hand, since $z \equiv \frac{2}{\sqrt{5}} \mod 11^\alpha$ we have $f_z'(a) \equiv 2a - 2 \equiv 0 \mod 11^\alpha$, but $f_z'(a) \not\equiv 0 \mod 11^{\alpha+1}$ since $a' \not\equiv 0 \mod 11$. It follows that

$$|f_z(a)|_{11} \le \frac{1}{11^{2\alpha+1}} < \frac{1}{11^{2\alpha}} = |f_z'(a)|_{11}^2.$$

Since $z \equiv \frac{2}{\sqrt{5}} \mod 11^{2\alpha}$, it follows that if $y^2 - \sqrt{5}zy + 1 = 0$ then $y \equiv 1 \mod 11^\alpha$. Write $y = 1 + 11^\alpha a'$ for some $a' \in \mathbb{Z}_{11}$. If $j \in \{1, 3, 4, 5, 9\}$ then $a'^2 - \sqrt{5}j \equiv 0 \mod 11$ has no solution in a', so the computation above shows that $f_z(y) \not\equiv 0 \mod 11^{2\alpha+1}$, which contradicts our assumption that $f_z(y) = 0$. □

Lemma 19. *Let $\alpha \ge 1$ and $j \in \{1, \dots, 10\}$. Let $z \equiv \frac{2}{\sqrt{5}} + j\,11^{2\alpha-1} \mod 11^{2\alpha}$. Then $f_z(y) := y^2 - \sqrt{5}zy + 1$ has no root in $\mathbb{Z}_{11}$.*

Proof. The argument is similar to that of Lemma 18. If $y^2 - \sqrt{5}zy + 1 = 0$ then $y \equiv 1 \mod 11^\alpha$. Write $y = 1 + 11^\alpha a'$ for some $a' \in \mathbb{Z}_{11}$. Then

$$\begin{aligned} f_z(y) &= y^2 - \sqrt{5}zy + 1 \\ &\equiv y^2 - \left(2 + \sqrt{5}j\,11^{2\alpha-1}\right) y + 1 \mod 11^{2\alpha} \\ &\equiv -\sqrt{5}j\,11^{2\alpha-1} \mod 11^{2\alpha} \\ &\not\equiv 0 \mod 11^{2\alpha}, \end{aligned}$$

which contradicts our assumption that $f_z(y) = 0$. □

Lemmas 18 and 19 can be used to verify features of Figure 2. For example, letting $\alpha = 1$ in Lemma 19 shows that the edge labeled 0 is the only edge emanating from the residue 5 modulo 11 on level $\alpha = 1$. The residue 5 modulo 11^2 on level $\alpha = 2$ has an emanating edge labeled 9, since $\frac{2}{\sqrt{5}} \equiv 5 + 9 \cdot 11^2 \mod 11^3$. Letting $\alpha = 1$ in Lemma 18 shows that the other edges emanating from 5 modulo 11^2 are $9 + \{2, 6, 7, 8, 10\} \bmod 11 = \{0, 4, 5, 6, 8\}$.

Theorem 20. *The limiting density of residues attained by the Fibonacci sequence modulo 11^α is*

$$\lim_{\alpha\to\infty} \frac{|\{F(n) \bmod 11^\alpha : n \ge 0\}|}{11^\alpha} = \frac{145}{264}.$$

Proof. It follows from Lemma 17 that

$$\bigcup_{i\ne 5} F_i(\mathbb{Z}_{11}) = \bigcup_{m\in\{0,1,2,3,8,10\}} m + 11\mathbb{Z}_{11},$$

which has measure $\frac{6}{11}$. By Lemmas 18 and 19, $F_5(\mathbb{Z}_{11})$ is a subset of $5 + 11^2\mathbb{Z}_{11}$ and so is disjoint from $F_i(\mathbb{Z}_{11})$ for each $i \ne 5$. Moreover, it follows from these lemmas that $\mu(F_5(\mathbb{Z}_{11})) = \sum_{\alpha=1}^{\infty} \frac{5}{11^{2\alpha+1}} = \frac{1}{264}$, so that

$$\mu\left(\bigcup_{i=0}^{9} F_i(\mathbb{Z}_{11})\right) = \frac{145}{264}.$$ □

Acknowledgments

The authors thank Valérie Berthé for helpful discussions. The second author thanks LIAFA, Université Paris-7 for its hospitality and support.

References

[1] Prerna Bihani, Wendy Pusser Sheppard, and Paul Thomas Young, p-adic interpolation of the Fibonacci sequence via hypergeometric functions, *The Fibonacci Quarterly* **43** (2005) 213–226.

[2] Mike Boyle, Douglas Lind, and Daniel Rudolph, The automorphism group of a shift of finite type, *Transactions of the American Mathematical Society* **306** (1988) 71–114.

[3] Stefan A. Burr, On moduli for which the Fibonacci sequence contains a complete system of residues, *The Fibonacci Quarterly* **9** (1971) 497–504.

[4] Donald M. Davis, Binomial coefficients involving infinite powers of primes, *The American Mathematical Monthly* **121** (2014) 734–737.

[5] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society, 2003.

[6] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction* second edition, Universitext, Springer–Verlag, Berlin, 1997.

[7] Hendrik Lenstra, Profinite Fibonacci numbers, *Nieuw Archief voor Wiskunde* **6** (2005) 297–300.

[8] Eric Rowland, Regularity versus complexity in the binary representation of 3^n, *Complex Systems* **18** (2009) 367–377.

[9] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *Journal de Théorie des Nombres de Bordeaux* **27** (2015) 245–288.

[10] Eric Rowland and Reem Yassawi, Profinite automata, `http://arxiv.org/abs/1403.7659`.

[11] Eric Rowland and Doron Zeilberger, A case study in meta-automation: automatic generation of congruence automata for combinatorial sequences, *Journal of Difference Equations and Applications* **20** (2014) 973–988.

[12] Zhang Shu and Jia-Yan Yao, Analytic functions over $\mathbb{Z}_p$ and p-regular sequences, *Comptes Rendus Mathematique* **349** (2011) 947–952.

Department of Mathematics, University of Liege, 4000 Liège, Belgium

Department of Mathematics, Trent University, Peterborough, Ontario, Canada