LIMITING DENSITY OF THE FIBONACCI SEQUENCE MODULO POWERS OF A PRIME

NICHOLAS BRAGMAN AND ERIC ROWLAND

Abstract. For a given prime p, we determine the limit, as $\lambda \to \infty$, of the density of residues modulo p^λ attained by the Fibonacci sequence. In particular, we show that this limiting density is related to zeros in the sequence of Lucas numbers modulo p. The proof uses a piecewise interpolation of the Fibonacci sequence to the p-adic numbers and a characterization of Wall–Sun–Sun primes p in terms of the p-adic absolute value of a number related to the p-adic golden ratio.

1. Introduction

The Fibonacci sequence $F(n)_{n\geq 0}$ is defined by the initial conditions $F(0) = 0$ and $F(1) = 1$ and the recurrence

$$F(n+2) = F(n+1) + F(n) \tag{1}$$

for $n \geq 0$. It is well known that $F(n)_{n\geq 0}$ is periodic modulo m. For example, the Fibonacci sequence modulo 7 is

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, 2, 3, 5, 1, 6, \dots$$

with period length 16.

Not every residue modulo m is attained by $F(n)_{n\geq 0}$. For example, no Fibonacci number is congruent to 4 modulo 11. This suggests the following question. What is the density

$$\frac{|\{F(n) \bmod m : n \geq 0\}|}{m}$$

of residues that the Fibonacci sequence attains modulo m? Burr [3] completed the characterization of integers $m \geq 2$ for which this density is 1 (that is, every residue is attained): The sequence $(F(n) \bmod m)_{n\geq 0}$ contains all residues modulo m if and only if $m = 5^k m'$ for some $k \geq 0$ and some $m' \in \{2, 4, 6, 7, 14\} \cup \{3^j : j \geq 0\}$. More recently, Dubickas and Novikas [4] showed that for every $k \geq 1$ there exists a modulus m and a sequence satisfying the Fibonacci recurrence that attains exactly k residues modulo m. Sanna [10] studied this question for other second-order recurrences. For a constant-recursive sequence satisfying a general second-order recurrence, Bumby [2] characterized the moduli for which the residues are uniformly distributed.

In this article we study the density of residues attained by the Fibonacci sequence modulo prime powers. Specifically, we are interested in the following.

Date: August 22, 2025.

Definition. Let p be a prime. The *limiting density* of the Fibonacci sequence modulo powers of p is

$$\operatorname{dens}(p) := \lim_{\lambda\to\infty} \frac{|\{F(n) \bmod p^\lambda : n \geq 0\}|}{p^\lambda}.$$

This limit exists since the density of residues attained modulo p^λ is bounded above by the density of residues attained modulo $p^{\lambda-1}$. For example, the fact that no Fibonacci number is congruent to 4 modulo 11 implies that no Fibonacci number is congruent to any of $4, 15, 26, \dots, 114$ modulo 11^2. By Burr's characterization, $\operatorname{dens}(3) = 1$ and $\operatorname{dens}(5) = 1$.

Rowland and Yassawi [9] provided a framework for determining $\operatorname{dens}(p)$ using a piecewise interpolation of $F(n)$ to $\mathbb{Z}_p$ and proved that $\operatorname{dens}(11) = \frac{145}{264}$. In this article we generalize this result to give an algorithm for computing $\operatorname{dens}(p)$, given a prime p. Our main result is Theorem 1 below. Before stating it, we need some definitions and notation.

Definition. The *period length* of the Fibonacci sequence modulo p, denoted $\pi(p)$, is the smallest integer $m \geq 1$ such that $F(n+m) \equiv F(n) \mod p$ for all $n \geq 0$. The *restricted period length* of the Fibonacci sequence modulo p, denoted $\alpha(p)$, is the smallest integer $m \geq 1$ such that $F(m) \equiv 0 \mod p$.

Let $L(n)_{n\geq 0}$ be the sequence of Lucas numbers, defined by $L(0) = 2$, $L(1) = 1$, and $L(n+2) = L(n+1) + L(n)$ for $n \geq 0$.

Definition. Let p be a prime. We say that $i \in \{0, 1, \dots, \pi(p) - 1\}$ is a *Lucas zero* (with respect to p) if $L(i) \equiv 0 \mod p$ and a *Lucas non-zero* if $L(i) \not\equiv 0 \mod p$.

For example, let $p = 7$. We have $\pi(7) = 16$ and $\alpha(7) = 8$. Moreover, the Lucas zeros are $i = 4$ and $i = 12$; indeed, $L(4) = 7$ and $L(12) = 322$. In Section 2 we will explicitly identify the Lucas zeros with respect to p. In particular, we will show that there are at most 2.

Let $\nu_p(n)$ denote the p-adic valuation of n; that is, $\nu_p(n)$ is the exponent of the highest power of p dividing n. Let

$$\epsilon = \begin{cases} 1 & \text{if } p \equiv 1, 4 \mod 5 \\ -1 & \text{if } p \equiv 2, 3 \mod 5 \\ 0 & \text{if } p = 5. \end{cases}$$

Theorem 1 shows that $\operatorname{dens}(p)$ depends on the integer $e = \nu_p(F(p - \epsilon))$. One can show that $\alpha(p)$ divides $p - \epsilon$, so $e \geq 1$. As we discuss in Section 3, there are no known examples of primes for which $e \geq 2$.

Theorem 1. *Let $p \neq 2$ be a prime, and define $e = \nu_p(F(p - \epsilon))$. Let*

$$N(p) = |\{F(i) \bmod p^e : i \text{ is a Lucas non-zero}\}|,$$

and let $Z(p)$ be the number of Lucas zeros i such that $F(i) \not\equiv F(j) \mod p^e$ for all Lucas non-zeros j. Then

$$\operatorname{dens}(p) = \frac{N(p)}{p^e} + \frac{Z(p)}{2p^{2e-1}(p+1)}.$$

In particular, $\mathrm{dens}(p) \in \mathbb{Q}$ and $\mathrm{dens}(p) \neq 0$. In the case that there are no Lucas zeros with respect to p, we have

$$\mathrm{dens}(p) = \frac{N(p)}{p^e} = \frac{|\{F(i) \bmod p^e : 0 \leq i \leq \pi(p) - 1\}|}{p^e}.$$

We refer to the expression for $\mathrm{dens}(p)$ in Theorem 1 as an algorithm rather than a formula because we do not have a way to compute $N(p)$ and $Z(p)$ without essentially computing $F(i) \bmod p^e$ for each $i \in \{0, 1, \ldots, \pi(p) - 1\}$.

Next we give several examples to show the variety of behavior that occurs.

Example 2. Let $p = 13$. The period length is $\pi(13) = 28$, and the restricted period length is $\alpha(13) = 7$. There are no Lucas zeros. The set $\{F(0), \ldots, F(27)\} \bmod 13$ is $\{0, 1, 2, 3, 5, 8, 10, 11, 12\}$. Therefore $N(13) = 9$, and $\mathrm{dens}(13) = \frac{9}{13}$. In fact, $\frac{9}{13}$ is the density of residues attained by the Fibonacci sequence modulo 13^λ for every $\lambda \geq 1$.

Example 3. Let $p = 19$, for which $\pi(19) = 18 = \alpha(19)$. The only Lucas zero is 9. The set

$$\{F(i) \bmod 19 : 0 \leq i \leq 17 \text{ and } i \neq 9\} = \{0, 1, 2, 3, 5, 8, 11, 13, 16, 17, 18\}$$

has size $N(19) = 11$ and does not contain $(F(9) \bmod 19) = 15$. Therefore $Z(19) = 1$, and $\mathrm{dens}(19) = \frac{11}{19} + \frac{1}{760} = \frac{441}{760}$. This density is the limit of the decreasing sequence $1, \frac{12}{19}, \frac{210}{361}, \frac{3981}{6859}, \frac{75621}{130321}, \ldots$ of densities of residues attained modulo 19^λ for $\lambda \geq 0$.

Example 4. Let $p = 31$, for which $\pi(31) = 30 = \alpha(31)$. The only Lucas zero is 15, but $F(15) \equiv 21 = F(8) \mod 31$. Therefore $Z(31) = 0$ and $\mathrm{dens}(31) = \frac{N(31)}{31} = \frac{19}{31}$.

Example 5. Let $p = 7$, for which $\pi(7) = 16$ and $\alpha(7) = 8$. The Lucas zeros are 4 and 12. The set

$$\{F(i) \bmod 7 : 0 \leq i \leq 15 \text{ and } i \neq 4, 12\} = \{0, 1, 2, 5, 6\}$$

has size $N(7) = 5$ and does not contain $(F(4) \bmod 7) = 3$ or $(F(12) \bmod 7) = 4$. Therefore $Z(7) = 2$ and $\mathrm{dens}(7) = \frac{5}{7} + \frac{2}{112} = \frac{41}{56}$. Figure 1 encodes the residues attained by the Fibonacci sequence modulo 7^λ for $0 \leq \lambda \leq 6$. Level λ in the tree contains the residues modulo 7^λ. Dotted edges from a residue class m on level λ indicate an omitted full 7-ary tree rooted at that vertex; that is, for every $\gamma \geq \lambda$ and for every integer $k \equiv m \mod 7^\lambda$ there exists $n \geq 0$ such that $F(n) \equiv k \mod 7^\gamma$. On level $\lambda = 1$ the residue classes $0, 1, 2, 5, 6$ modulo 7 are roots of full 7-ary trees; these trees contribute $\frac{5}{7}$ to the measure of $\overline{F(\mathbb{N})}$. We describe how to build additional levels of the tree quickly in Section 5.

For $p = 2$, we have the following analogue of Theorem 1.

Theorem 6. *The limiting density of the residues attained by the Fibonacci sequence modulo powers of* 2 *is* $\mathrm{dens}(2) = \frac{21}{32}$.

The values of $\mathrm{dens}(p)$ for several primes are given in the following table.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43
$\mathrm{dens}(p)$	$\frac{21}{32}$	1	1	$\frac{41}{56}$	$\frac{145}{264}$	$\frac{9}{13}$	$\frac{13}{17}$	$\frac{441}{760}$	$\frac{409}{552}$	$\frac{541}{1740}$	$\frac{19}{31}$	$\frac{29}{37}$	$\frac{715}{1722}$	$\frac{33}{43}$

Additional values can be found in the OEIS [12, A350999 and A351000]. Among the first 2000 primes, the smallest density that occurs is $\mathrm{dens}(9349) = \frac{504901}{174826300} \approx$

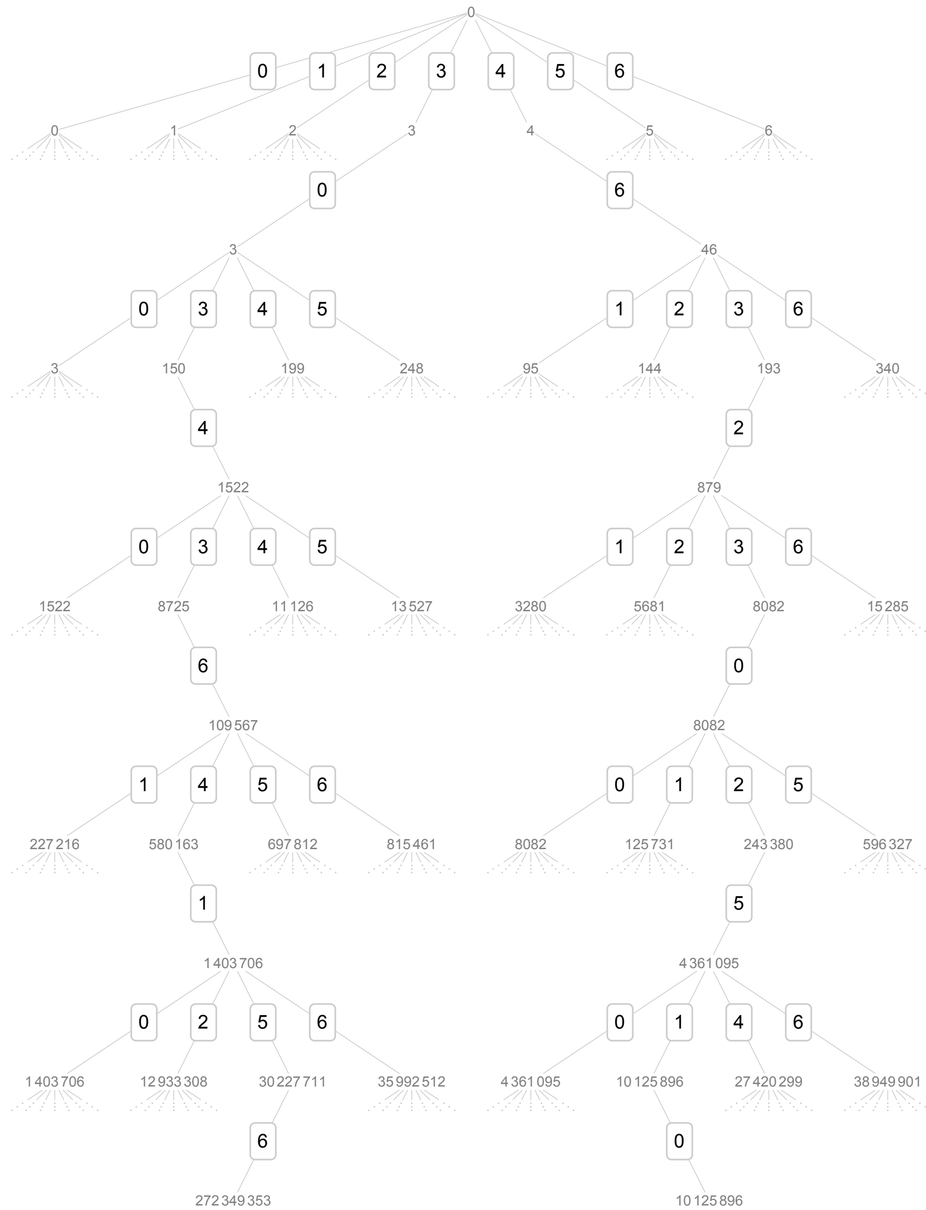

Figure 1. The tree of residues attained by the Fibonacci sequence modulo small powers of 7. The edges are labeled with base-7 digits. Full 7-ary subtrees are not shown but are indicated by dotted edges.

.002888. This low density can be partly explained by the fact that $F(38) \equiv 0 \mod 9349$. An even smaller density occurs for the prime $F(29) = 514229$; here $\operatorname{dens}(514229) = \frac{53}{514229} \approx .000103$. A natural question, which we do not address here, is whether there exist primes p with arbitrarily small $\operatorname{dens}(p)$. More generally, what are the limit points of the set $\{\operatorname{dens}(p) : p \text{ is prime}\}$?

The proofs of Theorems 1 and 6 make use of p-adic analytic functions; see for example Gouvêa's text [5] for the relevant background. In Section 2 we identify the Lucas zeros with respect to p. In Section 3 we give a more convenient characterization of the exponent e that appears in Theorem 1; this allows us to account for the possible existence of Wall–Sun–Sun primes. We also give an additional characterization of e as $\nu_p(L(i))$ where i is a Lucas zero. In Section 4 we interpolate the Fibonacci sequence to the field of p-adic numbers for $p \neq 2$. In Section 5 we prove Theorem 1, and in Section 6 we treat the case $p = 2$.

2. Lucas zeros

In this section we identify the Lucas zeros for the Fibonacci sequence with respect to p, in terms of $\alpha(p)$. First we recall the following special case of a theorem of Vinson [13, Theorem 2], which relates the period length to the restricted period length.

Theorem 7. *Let $p \neq 2$ be a prime. Then*

$$\frac{\pi(p)}{\alpha(p)} = \begin{cases} 4 & \text{if } \alpha(p) \text{ is odd} \\ 1 & \text{if } \alpha(p) \text{ is even but not divisible by } 4 \\ 2 & \text{if } \alpha(p) \text{ is divisible by } 4. \end{cases}$$

(For $p = 2$ we have $\pi(2) = 3 = \alpha(2)$.)

Remark 8. The primes for which $\frac{\pi(p)}{\alpha(p)} = 4$ are

$$5, 13, 17, 37, 53, 61, 73, 89, 97, 109, 113, 137, 149, \ldots \qquad [12,\ \text{A053028}].$$

Excluding 2, the primes for which $\frac{\pi(p)}{\alpha(p)} = 1$ are

$$11, 19, 29, 31, 59, 71, 79, 101, 131, 139, \ldots \qquad [12,\ \text{A053032}].$$

The primes for which $\frac{\pi(p)}{\alpha(p)} = 2$ are

$$3, 7, 23, 41, 43, 47, 67, 83, 103, 107, 127, \ldots \qquad [12,\ \text{A053027}].$$

This "trichotomy" was described by Ballot and Elia [1].

The number of Lucas zeros depends on the 2-adic valuation of $\alpha(p)$ and corresponds to the three cases of Theorem 7.

Proposition 9. *Let $p \neq 2$ be a prime. The set of Lucas zeros with respect to p is*

$$\begin{cases} \{\} & \text{if } \alpha(p) \text{ is odd} \\ \{\frac{\alpha(p)}{2}\} & \text{if } \alpha(p) \text{ is even but not divisible by } 4 \\ \{\frac{\alpha(p)}{2}, \frac{3\alpha(p)}{2}\} & \text{if } \alpha(p) \text{ is divisible by } 4. \end{cases}$$

Moreover, if $\alpha(p)$ is divisible by 4 then $F(\frac{\alpha(p)}{2}) \not\equiv F(\frac{3\alpha(p)}{2}) \mod p$.

Throughout the article we denote $\phi = \frac{1+\sqrt{5}}{2}$ and $\bar{\phi} = \frac{1-\sqrt{5}}{2} = -\frac{1}{\phi}$. Recall Binet's formula

$$F(n) = \frac{\phi^n - \bar{\phi}^n}{\sqrt{5}} \tag{2}$$

and the analogous formula $L(n) = \phi^n + \bar{\phi}^n$. Together these imply $2\phi^n = L(n) + \sqrt{5}F(n)$ and $2\bar{\phi}^n = L(n) - \sqrt{5}F(n)$ as well as the fundamental identity $L(n)^2 - 5F(n)^2 = (-1)^n 4$. In Section 3 we will assume $p \neq 5$ and interpret $\sqrt{5}$ as a p-adic number or p-adic algebraic number, depending whether $\mathbb{Z}_p$ contains a square root of 5. For the proof of Proposition 9, it suffices to work modulo p, so we work in the residue field

$$\begin{cases} \mathbb{Z}/(p\mathbb{Z}) & \text{if } x^2 \equiv 5 \mod p \text{ has an integer solution} \\ \mathbb{Z}[\sqrt{5}]/(p\mathbb{Z}[\sqrt{5}]) & \text{otherwise.} \end{cases}$$

Proof of Proposition 9. The statement holds for $p = 5$, since $\alpha(5) = 5$ and no Lucas number is divisible by 5. Assume $p \neq 5$.

By Binet's formula, $F(n) \equiv 0 \mod p$ if and only if $\phi^n - \bar{\phi}^n \equiv 0 \mod p$, which can be rewritten $(-\phi^2)^n \equiv 1 \mod p$ since $\phi\bar{\phi} = -1$. Since $F(\alpha(p)) \equiv 0 \mod p$ by definition, we have $(-\phi^2)^{\alpha(p)} \equiv 1 \mod p$. Moreover, $\alpha(p)$ is the smallest positive integer with this property. In other words, $\alpha(p)$ is the order of $-\phi^2$ modulo p.

Similarly, $L(i) = \phi^i + \bar{\phi}^i = \frac{\phi^{2i}+(-1)^i}{\phi^i}$, so i is a Lucas zero if and only if $(-\phi^2)^i \equiv -1 \mod p$. Therefore the Lucas zeros are precisely the values of $i \in \{0, \dots, \pi(p) - 1\}$ for which the order of $(-\phi^2)^i$ is 2. If $\alpha(p)$ is odd, then there are none. If $\alpha(p)$ is even, then the Lucas zeros are the solutions to $i \equiv \frac{\alpha(p)}{2} \mod \alpha(p)$. If $\alpha(p)$ is even but not divisible by 4, then $\pi(p) = \alpha(p)$ by Theorem 7, so the only solution is $i = \frac{\alpha(p)}{2}$. If $\alpha(p)$ is divisible by 4, then $\pi(p) = 2\alpha(p)$, so the solutions are $i = \frac{\alpha(p)}{2}$ and $i = \frac{\alpha(p)}{2} + \alpha(p)$.

It remains to show that $F(\frac{\alpha(p)}{2}) \not\equiv F(\frac{3\alpha(p)}{2}) \mod p$ when $\alpha(p)$ is divisible by 4. Vinson [13, Lemma 1] established that the order of $F(\alpha(p) - 1)$ modulo p is $\frac{\pi(p)}{\alpha(p)}$. Since $\frac{\pi(p)}{\alpha(p)} = 2$, this implies that $F(\alpha(p) - 1) \equiv -1 \mod p$. We have $F(\alpha(p)) \equiv 0 = -F(0) \mod p$, so it follows from $F(\alpha(p) + 1) = F(\alpha(p)) + F(\alpha(p) - 1)$ that

$$F(\alpha(p) + 1) \equiv F(\alpha(p) - 1) \equiv -1 = -F(1) \mod p.$$

Now the Fibonacci recurrence (1) inductively implies $F(\alpha(p)+n) \equiv -F(n) \mod p$ for all $n \geq 0$. In particular, $F(\frac{3\alpha(p)}{2}) \equiv -F(\frac{\alpha(p)}{2}) \mod p$. By the minimality of $\alpha(p)$, we have $F(\frac{\alpha(p)}{2}) \not\equiv 0 \mod p$, so $F(\frac{3\alpha(p)}{2}) \not\equiv F(\frac{\alpha(p)}{2}) \mod p$. □

3. The Wall exponent

In this section we give two additional characterizations of the exponent $e = \nu_p(F(p - \epsilon))$ that appears in Theorem 1. We will need these characterizations for the proof of Theorem 1 in Section 5, since we will want to express e in terms of the p-adic absolute value of a certain p-adic number involving ϕ. First we introduce some notation. As in Section 1, for $p \neq 5$, let

$$\epsilon = \begin{cases} 1 & \text{if } p \equiv 1, 4 \mod 5 \\ -1 & \text{if } p \equiv 2, 3 \mod 5. \end{cases}$$

Equivalently, we can write $\epsilon = (\frac{p}{5})$ using the Legendre symbol.

For primes $p \equiv 1, 4 \mod 5$, the set of p-adic integers $\mathbb{Z}_p$ contains a square root of 5; this can be shown using quadratic reciprocity and Hensel's lemma. For other primes, $\mathbb{Z}_p$ does not contain a square root of 5, so we consider the extension $\mathbb{Q}_p(\sqrt{5})$. Throughout the article, we denote

$$K = \mathbb{Q}_p(\sqrt{5}) = \begin{cases} \mathbb{Q}_p & \text{if } p \equiv 1,4 \mod 5 \\ \mathbb{Q}_p(\sqrt{5}) & \text{if } p \equiv 2,3 \mod 5 \\ \mathbb{Q}_5(\sqrt{5}) & \text{if } p = 5. \end{cases}$$

The p-adic absolute value of $x \in K$ is denoted $|x|_p$; it extends the p-adic absolute value on $\mathbb{Q}$ [5, Definition 2.1.4 and Theorem 5.3.5]. The p-adic valuation $\nu_p(x)$ of $x \in \mathbb{Q}_p$ is related to its p-adic absolute value by $|x|_p = p^{-\nu_p(x)}$. The ring of integers of K is

$$\mathcal{O}_K = \{x \in K : |x|_p \leq 1\} = \begin{cases} \mathbb{Z}_p & \text{if } p \equiv 1,4 \mod 5 \\ \mathbb{Z}_p[\sqrt{5}] & \text{if } p \equiv 2,3 \mod 5 \text{ and } p \neq 2 \\ \mathbb{Z}_2[\phi] & \text{if } p = 2 \\ \mathbb{Z}_5[\sqrt{5}] & \text{if } p = 5. \end{cases}$$

We now consider ϕ and $\bar{\phi}$ as elements of $\mathcal{O}_K$.

Let d be the degree of the extension K of $\mathbb{Q}_p$, and let p^f be the size of the residue field $\mathcal{O}_K/\{x \in K : |x|_p < 1\}$. Namely,

$$d = \begin{cases} 1 & \text{if } p \equiv 1,4 \mod 5 \\ 2 & \text{if } p \equiv 2,3 \mod 5 \\ 2 & \text{if } p = 5 \end{cases} \qquad \text{and} \qquad f = \begin{cases} 1 & \text{if } p \equiv 1,4 \mod 5 \\ 2 & \text{if } p \equiv 2,3 \mod 5 \\ 1 & \text{if } p = 5. \end{cases}$$

The quotient d/f is the *ramification index* of the extension.

To obtain another description of $e = \nu_p(F(p - \epsilon))$, we will use the fact that the ring of integers $\mathcal{O}_K$ contains the cyclic group of $(p^f - 1)$th roots of unity [5, Corollary 5.4.9]. Moreover, for each $x \in K$ such that $|x|_p = 1$, there is a unique $(p^f - 1)$th root of unity congruent to x modulo p (or, in the case $p = 5$, modulo a uniformizer). This is because there are precisely p^f residue classes modulo p (or modulo the uniformizer) and each $(p^f - 1)$th root of unity belongs to a distinct residue class.

Notation. If $|x|_p = 1$ and $p \neq 5$, define $\omega(x)$ to be the $(p^f - 1)$th root of unity satisfying $\omega(x) \equiv x \mod p$. In particular, $\frac{x}{\omega(x)} \equiv 1 \mod p$. For $p = 5$, we use the uniformizer $\sqrt{5}$ and define $\omega(x)$ to be the 4th root of unity satisfying $\omega(x) \equiv x \mod \sqrt{5}$.

The first main result of this section is that the Wall exponent $e = \nu_p(F(p - \epsilon))$ can also be defined by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$.

Theorem 10. *Let p be a prime such that $p \neq 2$ and $p \neq 5$. Then $|F(p - \epsilon)|_p = \left|\frac{\phi}{\omega(\phi)} - 1\right|_p$.*

The prime p is a *Wall–Sun–Sun prime* if $\nu_p(F(p-\epsilon)) \geq 2$. Wall–Sun–Sun primes are also known as *Fibonacci–Wieferich primes*. Wall [14] verified that there are none $< 10^4$. No Wall–Sun–Sun primes are known, although a heuristic argument suggests there are infinitely many [8, Section 4]. For $p \notin \{2, 5\}$, Theorem 10 implies that p is a Wall–Sun–Sun prime if and only if $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p \leq \frac{1}{p^2}$.

We split the proof of Theorem 10 into the following two propositions. The first is a straightforward generalization of the statement that p is a Wall–Sun–Sun prime if and only if $L(p-\epsilon) \equiv 2\epsilon \mod p^4$, which is one of several characterizations of Wall–Sun–Sun primes given by McIntosh and Roettger [8, Theorem 1] (in a more general form).

Proposition 11. *Let p be a prime such that $p \neq 2$ and $p \neq 5$. Then $|F(p-\epsilon)|_p = \sqrt{|L(p-\epsilon) - 2\epsilon|_p}$.*

Proof. We use the identity $5F(n)^2 = L(n)^2 - (-1)^n 4$. Note that $p-\epsilon$ is even and $(-1)^{(p-\epsilon)/2} = \epsilon$. Therefore

$$5F(p-\epsilon)^2 = \left(L(p-\epsilon) + 2\epsilon\right)\left(L(p-\epsilon) - 2\epsilon\right).$$

McIntosh and Roettger [8, Equation (5)] show that $L(p-\epsilon) - 2\epsilon \equiv 0 \mod p^2$. Since $4\epsilon \not\equiv 0 \mod p$, this implies $L(p-\epsilon) + 2\epsilon \not\equiv 0 \mod p$. It follows that $|F(p-\epsilon)|_p^2 = |L(p-\epsilon) - 2\epsilon|_p$ as desired. □

To prove the second proposition, we use the following lemma.

Lemma 12. *Let p be a prime, and let $x \in K$ such that $|x|_p = 1$. Then $|x^{p^f} - x|_p = |x - \omega(x)|_p$.*

Proof. We use the factorization $x^{p^f} - x = x \prod_r (x - r)$ in $\mathcal{O}_K[x]$, where r ranges over the $(p^f - 1)$th roots of unity. Since $|x|_p = 1$, there is precisely one root of unity r such that $|x - r|_p \neq 1$, namely $r = \omega(x)$. Therefore $|x^{p^f} - x|_p = |x - \omega(x)|_p$. □

Proposition 13. *Let p be a prime such that $p \neq 2$ and $p \neq 5$. Then $\sqrt{|L(p-\epsilon) - 2\epsilon|_p} = \left|\frac{\phi}{\omega(\phi)} - 1\right|_p$.*

Proof. First we note that $\left|\bar{\phi}^{p-\epsilon} - \epsilon\right|_p = \left|\phi^{p-\epsilon} - \epsilon\right|_p$, since

$$\left|\bar{\phi}^{p-\epsilon} - \epsilon\right|_p = \left|\left(-\frac{1}{\phi}\right)^{p-\epsilon} - \epsilon\right|_p = \left|(-1)^{p-\epsilon} - \epsilon\phi^{p-\epsilon}\right|_p = \left|1 - \epsilon\phi^{p-\epsilon}\right|_p = \left|\phi^{p-\epsilon} - \epsilon\right|_p$$

(using the fact that $p - \epsilon$ is even). Since $L(n) = \phi^n + \bar{\phi}^n$, we have

$$\begin{aligned} -\epsilon(\phi^{p-\epsilon} - \epsilon)(\bar{\phi}^{p-\epsilon} - \epsilon) &= -\epsilon(-1)^{p-\epsilon} + \phi^{p-\epsilon} + \bar{\phi}^{p-\epsilon} - \epsilon \\ &= L(p-\epsilon) - 2\epsilon. \end{aligned}$$

Taking the p-adic absolute value of both sides gives $\left|\phi^{p-\epsilon} - \epsilon\right|_p^2 = \left|L(p-\epsilon) - 2\epsilon\right|_p$. Therefore it suffices to show that $\left|\phi^{p-\epsilon} - \epsilon\right|_p = \left|\frac{\phi}{\omega(\phi)} - 1\right|_p$.

If $p \equiv 1, 4 \mod 5$, then $\epsilon = 1$ and $f = 1$. It follows from Lemma 12 that $|\phi^{p-1} - 1|_p = |\phi^p - \phi|_p = |\phi - \omega(\phi)|_p = \left|\frac{\phi}{\omega(\phi)} - 1\right|_p$.

If $p \equiv 2, 3 \mod 5$, then $\epsilon = -1$ and $f = 2$. The geometric series formula gives

$$\frac{\phi^{p^2-1} - 1}{\phi^{p+1} + 1} = \sum_{j=0}^{p-2} (-1)^{j+1} \phi^{(p+1)j} \equiv \sum_{j=0}^{p-2} (-1)^{j+1} (-1)^j \equiv 1 \mod p.$$

It follows that $|\phi^{p+1} + 1|_p = |\phi^{p^2-1} - 1|_p = |\phi^{p^2} - \phi|_p$. By Lemma 12, $|\phi^{p+1} + 1|_p = |\phi - \omega(\phi)|_p = \left|\frac{\phi}{\omega(\phi)} - 1\right|_p$. □

This concludes the proof of Theorem 10.

The second main result of this section is that the Wall exponent is also the p-adic valuation of certain Lucas numbers.

Theorem 14. *Let p be a prime such that $p \neq 2$, $p \neq 3$, and $p \neq 5$. If i is a Lucas zero with respect to p, then $|L(i)|_p = |F(p-\epsilon)|_p$.*

For $p = 3$, the Lucas zeros are 2 and 6. The Lucas zero 2 does satisfy the conclusion, since $L(2) = 3 = F(4)$. However, 6 does not, since $|L(6)|_3 = |18|_3 = \frac{1}{9} < \frac{1}{3} = |F(4)|_3$.

Proof of Theorem 14. We show that $|L(i)|_p = |F(\alpha(p))|_p$. The result will then follow from $|F(\alpha(p))|_p = |F(p-\epsilon)|_p$.

Since i is a Lucas zero, Proposition 9 implies that $\alpha(p)$ is even. Therefore

$$|F(\alpha(p))|_p = \left|\frac{\phi^{\alpha(p)} - (-\phi^{-1})^{\alpha(p)}}{\sqrt{5}}\right|_p = \left|\frac{\phi^{\alpha(p)} - \phi^{-\alpha(p)}}{\sqrt{5}}\right|_p = \left|\phi^{2\alpha(p)} - 1\right|_p.$$

We consider two cases.

If $\alpha(p)$ is not divisible by 4, then $i = \frac{\alpha(p)}{2}$ is odd. Therefore

$$|L(i)|_p = \left|\phi^i + (-\phi^{-1})^i\right|_p = \left|\phi^i - \phi^{-i}\right|_p = \left|\phi^{\alpha(p)} - 1\right|_p = \frac{\left|\phi^{2\alpha(p)} - 1\right|_p}{\left|\phi^{\alpha(p)} + 1\right|_p}.$$

Since i is a Lucas zero, we have $\phi^{\alpha(p)} \equiv 1 \not\equiv -1 \mod p$, which implies $\left|\phi^{\alpha(p)} + 1\right|_p = 1$. It follows that $|L(i)|_p = |F(\alpha(p))|_p$.

If $\alpha(p)$ is divisible by 4, then $i \in \{\frac{\alpha(p)}{2}, \frac{3\alpha(p)}{2}\}$, so i is even. Therefore

$$|L(i)|_p = \left|\phi^i + (-\phi^{-1})^i\right|_p = \left|\phi^i + \phi^{-i}\right|_p = \left|\phi^{2i} + 1\right|_p.$$

If $i = \frac{\alpha(p)}{2}$, then

$$|L(i)|_p = \left|\phi^{\alpha(p)} + 1\right|_p = \frac{\left|\phi^{2\alpha(p)} - 1\right|_p}{\left|\phi^{\alpha(p)} - 1\right|_p} = |F(\alpha(p))|_p$$

since $|L(i)|_p < 1$ implies $\left|\phi^{\alpha(p)} - 1\right|_p = 1$. On the other hand, if $i = \frac{3\alpha(p)}{2}$, then

$$|L(i)|_p = \left|\phi^{3\alpha(p)} + 1\right|_p = \left|\phi^{\alpha(p)} + 1\right|_p \left|\phi^{2\alpha(p)} - \phi^{\alpha(p)} + 1\right|_p.$$

Since $\phi^{\alpha(p)} \equiv -1 \mod p$, we have $\phi^{2\alpha(p)} - \phi^{\alpha(p)} + 1 \equiv 3 \not\equiv 0 \mod p$ since $p \neq 3$. It follows that $|L(i)|_p = |F(\alpha(p))|_p$. □

4. Piecewise interpolation to the p-adic numbers

In this section we interpolate $F(n)$ to $\mathbb{Z}_p$ so that we can work with continuous functions in Section 5. This same approach was used to prove the celebrated Skolem–Mahler–Lech theorem concerning the set of zeros of a constant-recursive sequence [11, 7, 6].

The Fibonacci sequence cannot be interpolated to $\mathbb{Z}_p$ by a single continuous function, but there exists a finite set of continuous functions that comprise a piecewise interpolation to $\mathbb{Z}_p$. These functions come from Binet's formula (2) interpreted in $\mathbb{Q}_p(\sqrt{5})$. For this, we need the p-adic logarithm and exponential functions, which are defined by their usual power series

$$\log_p(1+x) := \sum_{m \geq 1} (-1)^{m+1} \frac{x^m}{m} \qquad \text{and} \qquad \exp_p x := \sum_{m \geq 0} \frac{x^m}{m!}.$$

The series $\log_p(1+x)$ converges if $|x|_p < 1$, and $\exp_p x$ converges if $|x|_p < p^{-1/(p-1)}$. Moreover, $\log_p$ is an isomorphism from the multiplicative group $\{x : |x-1|_p < p^{-1/(p-1)}\}$ to the additive group $\{x : |x|_p < p^{-1/(p-1)}\}$, and its inverse map is $\exp_p$ [5, Proposition 4.5.9 and Section 6.1]. In particular, if $|x-1|_p < p^{-1/(p-1)}$, then $x = \exp_p \log_p x$.

To interpolate $F(n)$, we use this last identity to rewrite ϕ^n and $\bar{\phi}^n$. There are several ways to do this. We use an approach that directly involves the root of unity $\omega(\phi)$, which plays a major role in the structure of the set $F(\mathbb{Z}_p)$. Since $e \geq 1$ and $p \neq 2$, we have $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p < p^{-1/(p-1)}$; this also follows from a more general result [9, Lemma 6]. Therefore, for all $n \geq 0$, we have $\left(\frac{\phi}{\omega(\phi)}\right)^n = \exp_p \log_p\left(\left(\frac{\phi}{\omega(\phi)}\right)^n\right) = \exp_p\left(n \log_p \frac{\phi}{\omega(\phi)}\right)$.

Theorem 15 (Rowland–Yassawi [9, Theorem 15])**.** *Let $p \neq 2$ be a prime, and let p^f be the size of the residue field $\mathcal{O}_K/\{x \in K : |x|_p < 1\}$. For each $i \in \{0, 1, \ldots, p^f - 2\}$, define the function $F_i \colon \mathbb{Z}_p \to K$ by*

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

Then $F_i(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$, and $F(n) = F_{n \bmod (p^f-1)}(n)$ for all $n \geq 0$.

To see that $F_i(x) \in \mathbb{Z}_p$ if $x \in \mathbb{Z}_p$, take a sequence of integers $(x_m)_{m \geq 0}$ that converges to x such that $x_m \equiv i \mod p^f - 1$ for each $m \geq 0$; since $F_i(x_m) = F(x_m) \in \mathbb{Z}$, it follows by continuity that $F_i(x) \in \mathbb{Z}_p$.

Note we have not defined F_i for $p = 2$; the definition requires modification and will be discussed in Section 6.

Recall the observation in the proof of Proposition 9 that $\alpha(p)$ is the order of $-\phi^2$ modulo p. Along with Theorem 7, this implies that $\omega(\phi)^{\pi(p)} = 1$ and $\omega(\bar{\phi})^{\pi(p)} = 1$; Ballot and Elia give an alternate proof of this fact [1, Proposition 1.2]. Therefore $F_{i+\pi(p)}(x) = F_i(x)$ for all $x \in \mathbb{Z}_p$, so we can reduce the number of functions in the piecewise interpolation. Namely, the functions $F_i(x)$ for $i \in \{0, 1, \ldots, \pi(p) - 1\}$ comprise an interpolation.

In Section 5, we will use Proposition 18 below, which refines the isomorphism $\log_p$. To prove it, we need two lemmas, whose proofs we include for completeness. The first is the lifting-the-exponent lemma.

Lemma 16. *Let $e \geq 0$ be an integer. If $a, b \in \mathcal{O}_K$ such that $|a-b|_p < p^{-1/(p-1)}$, then $\left|a^{p^e} - b^{p^e}\right|_p < p^{-e-1/(p-1)}$.*

Proof. Assume $i \geq 0$ and $|a-b|_p < p^{-i-1/(p-1)}$; we show that this implies $|a^p - b^p|_p < p^{-(i+1)-1/(p-1)}$. The statement will then follow inductively. Write $a = b + O(p^i)$. We have

$$\begin{aligned}\frac{a^p - b^p}{a-b} &= \sum_{j=0}^{p-1} a^{p-1-j} b^j = \sum_{j=0}^{p-1} \left(b + O(p^i)\right)^{p-1-j} b^j \\ &= \sum_{j=0}^{p-1} \left(b^{p-1} + O(p^i)\right) = p b^{p-1} + O(p^i).\end{aligned}$$

Therefore

$$\begin{aligned}|a^p - b^p|_p &= |a-b|_p \cdot \left|pb^{p-1} + O(p^i)\right|_p \\ &< p^{-i-1/(p-1)} \cdot p^{-1}. \end{aligned}$$ □

The second is a special case of the isometry property of the p-adic logarithm.

Lemma 17. *If $x \in \mathcal{O}_K$ and $|x|_p < p^{-1/(p-1)}$, then $\left|\log_p(1+x)\right|_p = |x|_p$.*

Proof. The power series for $\log_p$ gives

$$\left|\log_p(1+x)\right|_p = |x|_p \cdot \left|1 + \sum_{m \geq 2} (-1)^{m+1} \frac{x^{m-1}}{m}\right|_p.$$

Since $|m|_p \geq p^{-\frac{m-1}{p-1}}$ for each $m \geq 1$, for $m \geq 2$ we have $\left|\frac{x^{m-1}}{m}\right|_p < \frac{1}{|m|_p} p^{-\frac{m-1}{p-1}} \leq 1$. Therefore

$$\left|1 + \sum_{m \geq 2} (-1)^{m+1} \frac{x^{m-1}}{m}\right|_p = 1$$

by the ultrametric inequality. □

Proposition 18. *For each integer $e \geq 0$, $\exp_p$ is a group isomorphism from $\{x : |x|_p < p^{-e-1/(p-1)}\}$ to $\{x : |x-1|_p < p^{-e-1/(p-1)}\}$.*

Proof. Since $\exp_p$ is a group isomorphism from $\{x : |x|_p < p^{-1/(p-1)}\}$ to $\{x : |x-1|_p < p^{-1/(p-1)}\}$, to prove the proposition it suffices to show that

$$\left\{\exp_p(x) : |x|_p < p^{-e-1/(p-1)}\right\} = \left\{x : |x-1|_p < p^{-e-1/(p-1)}\right\}.$$

To show $\subseteq$, let $x \in \mathcal{O}_K$ such that $|x|_p < p^{-e-1/(p-1)}$; then $|\frac{x}{p^e}|_p < p^{-1/(p-1)}$, so $\frac{x}{p^e}$ is in the domain of $\exp_p$. We have

$$\exp_p(x) = \exp_p(\underbrace{\tfrac{x}{p^e} + \tfrac{x}{p^e} + \cdots + \tfrac{x}{p^e}}_{p^e}) = \left(\exp_p(\tfrac{x}{p^e})\right)^{p^e}.$$

Since $|\exp_p(\frac{x}{p^e}) - 1|_p < p^{-1/(p-1)}$, Lemma 16 implies $\left|(\exp_p(\frac{x}{p^e}))^{p^e} - 1\right|_p < p^{-e-1/(p-1)}$.

To show $\supseteq$, let $y \in \mathcal{O}_K$ such that $|y-1|_p < p^{-e-1/(p-1)}$. Let $x = \log_p y$. By Lemma 17, $|x|_p < p^{-e-1/(p-1)}$, and x satisfies $\exp_p(x) = y$. □

5. Proof of the main result

In this section we prove Theorem 1, which establishes the value of $\text{dens}(p)$ for $p \neq 2$. This density is equal to the measure of the closure of the set of Fibonacci numbers in the p-adic integers $\mathbb{Z}_p$. That is, let μ be the Haar measure on $\mathbb{Z}_p$ defined by $\mu(m + p^\lambda \mathbb{Z}_p) = p^{-\lambda}$; then $\text{dens}(p) = \mu(\overline{F(\mathbb{N})})$.

As an illustrative warm-up example, we determine the limiting density of residues attained by the set of squares modulo powers of p for $p \neq 2$. Let $z \in \mathbb{Z}_p$, and define $\lambda \in \mathbb{Z}$ by $|z|_p = \frac{1}{p^\lambda}$. If λ is odd, then z does not have a square root in $\mathbb{Z}_p$. If λ is even, then z has a square root in $\mathbb{Z}_p$ (more precisely, in $p^{\lambda/2}\mathbb{Z}_p$) if and only if

$\frac{z}{p^\lambda}$ mod p is a quadratic residue, by Hensel's lemma. Since there are $\frac{p-1}{2}$ nonzero quadratic residues modulo p, the image of $\mathbb{Z}_p$ under $x \mapsto x^2$ has measure

$$\sum_{\substack{\lambda \geq 0 \\ \lambda \text{ even}}} \frac{p-1}{2} \cdot \frac{1}{p^{\lambda+1}} = \frac{p}{2(p+1)}.$$

The term $\frac{Z(p)}{2p^{2e-1}(p+1)}$ in Theorem 1 will arise in a similar way, since the Fibonacci sequence satisfies a second-order recurrence.

Notation. For $p \neq 2$, we write the function $F_i(x)$ in Theorem 15 as the composition $F_i(x) = g_i(h_i(x))$ where $g_i(y) = \frac{y-(-1)^i y^{-1}}{\sqrt{5}}$ and $h_i(x) = \omega(\phi)^i \exp_p\left(x \log_p \frac{\phi}{\omega(\phi)}\right)$. We use this notation throughout this section. The function g_i is close enough to a polynomial that we will be able to apply Hensel's lemma.

To prove Theorem 1, we describe the set $F_i(\mathbb{Z}_p)$. In Proposition 23 we show that this set is contained in $F(i) + p^e\mathbb{Z}_p$, where e is defined by $|\frac{\phi}{\omega(\phi)} - 1|_p = \frac{1}{p^e}$. For Lucas non-zeros i, Proposition 24 shows that in fact $F_i(\mathbb{Z}_p) = F(i) + p^e\mathbb{Z}_p$. It follows that the Lucas non-zeros contribute measure $\frac{N(p)}{p^e}$ in Theorem 1. Moreover, they account for the full subtrees rooted at level 1 in Figure 1 and analogous trees for other primes.

When i is a Lucas zero, the description of the set $F_i(\mathbb{Z}_p)$ is more complicated, since it is not a cylinder set. We will show that partial branching of the kind pictured in Figure 1 occurs through the tree along edges corresponding to the p-adic digits of $\omega(\phi)^i \frac{2}{\sqrt{5}}$. For $p = 7$, there are two such paths, for the 7-adic numbers

$$\omega(\phi)^4 \tfrac{2}{\sqrt{5}} = 3 + \frac{0}{7^{-1}} + \frac{3}{7^{-2}} + \frac{4}{7^{-3}} + \frac{3}{7^{-4}} + \frac{6}{7^{-5}} + \frac{4}{7^{-6}} + \frac{1}{7^{-7}} + \cdots$$
$$\omega(\phi)^{12} \tfrac{2}{\sqrt{5}} = 4 + \frac{6}{7^{-1}} + \frac{3}{7^{-2}} + \frac{2}{7^{-3}} + \frac{3}{7^{-4}} + \frac{0}{7^{-5}} + \frac{2}{7^{-6}} + \frac{5}{7^{-7}} + \cdots$$

(where we place each power of 7 in the denominator to make the digits easier to read). This partial branching is due to a double root of $y^2 - \sqrt{5}zy - (-1)^i = 0$ (equivalently, $g_i(y) = z$) when $z = \omega(\phi)^i \frac{2}{\sqrt{5}}$. By computing digits of $\omega(\phi)^i \frac{2}{\sqrt{5}}$, we can use the set of quadratic residues modulo p to quickly construct levels $\lambda \geq 2$ of the tree of attained residues. The construction follows from Lemma 26, and Proposition 27 establishes $\mu(F_i(\mathbb{Z}_p))$ for Lucas zeros i.

We begin the proof of Theorem 1 with a lemma allowing us to conclude that certain numbers belong to $\exp_p(p\sqrt{5}\mathbb{Z}_p)$. As before, let $\bar{\phi} = \frac{1-\sqrt{5}}{2}$. In the case $p \equiv 2, 3 \mod 5$, we generalize this notation as follows. If $x = a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}_p$, define $\bar{x} = a - b\sqrt{5}$.

Lemma 19. *Let $p \equiv 2, 3 \mod 5$. If $x \in \mathcal{O}_K$ such that $x\bar{x} = 1$ and $|x - 1|_p < p^{-1/(p-1)}$, then $\log_p x \in p\sqrt{5}\mathbb{Z}_p$.*

Proof. In addition to $|x-1|_p < p^{-1/(p-1)}$, we have $|\bar{x} - 1|_p = \left|\frac{1}{x} - 1\right|_p = |1-x|_p < p^{-1/(p-1)}$. Since $\log_p$ is a group isomorphism from $\{x : |x-1|_p < p^{-1/(p-1)}\}$ to $\{x : |x|_p < p^{-1/(p-1)}\}$, it follows that $\log_p x + \log_p \bar{x} = \log_p(x\bar{x}) = \log_p 1 = 0$. Write $\log_p x = a + b\sqrt{5}$ where $a, b \in \mathbb{Z}_p$. Then

$$a - b\sqrt{5} = \overline{a + b\sqrt{5}} = \log_p \bar{x} = -\log_p x = -a - b\sqrt{5},$$

so $a = 0$. Finally, $b \equiv 0 \mod p$ because $\left|\log_p x\right|_p = |x-1|_p < p^{-1/(p-1)}$ by Lemma 17. $\square$

Next we use Lemma 19 to describe the image of $\mathbb{Z}_p$ under h_i.

Lemma 20. *Let p be a prime such that $p \neq 2$ and $p \neq 5$, and define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$. If $i \in \{0, 1, \ldots, \pi(p)-1\}$, then $h_i(\mathbb{Z}_p) = \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$.*

Proof. It follows from Lemma 17 that $\left|\log_p \frac{\phi}{\omega(\phi)}\right|_p = \frac{1}{p^e}$. In particular, $x \log_p \frac{\phi}{\omega(\phi)}$ is in the domain of $\exp_p$ for all $x \in \mathbb{Z}_p$. If $p \equiv 1, 4 \mod 5$, then

$$\begin{aligned} h_i(\mathbb{Z}_p) &= \omega(\phi)^i \exp_p\Big(\mathbb{Z}_p \log_p \tfrac{\phi}{\omega(\phi)}\Big) \\ &= \omega(\phi)^i \exp_p(p^e \mathbb{Z}_p) \\ &= \omega(\phi)^i \exp_p(p^e \sqrt{5}\mathbb{Z}_p) \end{aligned}$$

since $|\sqrt{5}|_p = 1$. If $p \equiv 2, 3 \mod 5$, then $\log_p \frac{\phi}{\omega(\phi)} \in p^e\sqrt{5}\mathbb{Z}_p$ by Lemma 19, since $\frac{\phi}{\omega(\phi)} \cdot \frac{\bar{\phi}}{\omega(\bar{\phi})} = \frac{-1}{-1} = 1$. Therefore

$$\begin{aligned} h_i(\mathbb{Z}_p) &= \omega(\phi)^i \exp_p\Big(\mathbb{Z}_p \log_p \tfrac{\phi}{\omega(\phi)}\Big) \\ &= \omega(\phi)^i \exp_p(p^e \sqrt{5}\mathbb{Z}_p). \end{aligned}$$ $\square$

We will not describe the set $h_i(\mathbb{Z}_p) = \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$ more explicitly. Instead, the next lemma gives conditions under which $g_i(y) = z$ has a solution $y \in h_i(\mathbb{Z}_p)$ when $p \equiv 2, 3 \mod 5$. We will apply it for Lucas non-zeros i as well as Lucas zeros.

Lemma 21. *Let $p \equiv 2, 3 \mod 5$. If $p \neq 2$, define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$; if $p = 2$, let $e = 2$. Let $z, w \in \mathbb{Z}_p$ and $y_0 \in \mathcal{O}_K \setminus \{0\}$ such that $w^2 = 5z^2 + 4y_0\overline{y_0}$ and $\left|\frac{w+\sqrt{5}z}{2} - y_0\right|_p \leq \frac{1}{p^e}$. Then $\frac{w+\sqrt{5}z}{2} \in y_0 \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$.*

Proof. We have

$$\frac{\frac{w+\sqrt{5}z}{2}}{y_0} \cdot \frac{\frac{w-\sqrt{5}z}{2}}{\overline{y_0}} = 1.$$

Since $\left|\frac{w+\sqrt{5}z}{2} - y_0\right|_p \leq p^{-e} < p^{-1/(p-1)}$, Lemma 19 implies $\log_p \frac{w+\sqrt{5}z}{2y_0} \in p\sqrt{5}\mathbb{Z}_p$. Moreover, Lemma 17 implies $\left|\log_p \frac{w+\sqrt{5}z}{2y_0}\right|_p = \left|\frac{w+\sqrt{5}z}{2} - y_0\right|_p \leq \frac{1}{p^e}$, so in fact $\log_p \frac{w+\sqrt{5}z}{2y_0} \in p^e\sqrt{5}\mathbb{Z}_p$, and this implies $\frac{w+\sqrt{5}z}{2} \in y_0 \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$. $\square$

Now we begin to consider $F_i(\mathbb{Z}_p)$. We will use the following as a partial converse of Lemma 21 to prove Propositions 23 and 27 concerning $F_i(\mathbb{Z}_p)$.

Lemma 22. *Let p be a prime such that $p \neq 2$ and $p \neq 5$, and define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$. Let $i \in \{0, 1, \ldots, \pi(p)-1\}$. If $y \in h_i(\mathbb{Z}_p)$, then $|y - \omega(\phi)^i|_p \leq \frac{1}{p^e}$.*

Proof. Since $F_i(x) = g_i(h_i(x))$, it suffices to show $g_i(y) \in F(i) + p^e\mathbb{Z}_p$. By Lemma 20, $y = \omega(\phi)^i \exp_p(p^e\sqrt{5}t)$ for some $t \in \mathbb{Z}_p$. Since $p \neq 2$, we have $1 > \frac{1}{p-1}$ and

$$\left|p^e\sqrt{5}t\right|_p \leq p^{-e} < p^{-e+1-1/(p-1)}.$$

By Proposition 18, this implies

$$\left|y - \omega(\phi)^i\right|_p = \left|\exp_p(p^e\sqrt{5}t) - 1\right|_p < p^{-e+1-1/(p-1)}.$$

Since $p \neq 5$, we have $|y - \omega(\phi)^i|_p \in p^{\mathbb{Z}}$ (because the ramification index is 1); therefore $|y - \omega(\phi)^i|_p \leq p^{-e}$. □

Proposition 23. *Let p be a prime such that $p \neq 2$ and $p \neq 5$, and define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$. If $i \in \{0, 1, \ldots, \pi(p) - 1\}$, then $F_i(\mathbb{Z}_p) \subseteq F(i) + p^e\mathbb{Z}_p$.*

Proof. Let $y \in h_i(\mathbb{Z}_p)$. By Lemma 22, $|y - \omega(\phi)^i|_p \leq p^{-e}$. We also have $|\phi^i - \omega(\phi)^i|_p \leq p^{-e}$ since $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = p^{-e}$. Therefore

$$\begin{aligned}
|g_i(y) - F(i)|_p &= \left|\frac{y - (-1)^i y^{-1}}{\sqrt{5}} - \frac{\phi^i - (-1)^i\phi^{-i}}{\sqrt{5}}\right|_p \\
&= \left|\left(y - \phi^i\right) - (-1)^i\left(y^{-1} - \phi^{-i}\right)\right|_p \\
&\leq \max\Big(\left|y - \phi^i\right|_p, \left|y^{-1} - \phi^{-i}\right|_p\Big) \\
&= \left|y - \phi^i\right|_p \\
&\leq \max\Big(\left|y - \omega(\phi)^i\right|_p, \left|\omega(\phi)^i - \phi^i\right|_p\Big) \\
&\leq p^{-e}
\end{aligned}$$

after two applications of the ultrametric inequality. It follows that $g_i(y) \in F(i) + p^e\mathcal{O}_K$. By Theorem 15, $g_i(y) \in F_i(\mathbb{Z}_p) \subseteq \mathbb{Z}_p$, so $g_i(y) \in F(i) + p^e\mathbb{Z}_p$. □

If i is a Lucas non-zero, the $\subseteq$ in Proposition 23 can be strengthened to $=$ as follows; this establishes that $\mu(F_i(\mathbb{Z}_p)) = \frac{1}{p^e}$.

Proposition 24. *Let p be a prime such that $p \neq 2$ and $p \neq 5$, and define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$. If i is a Lucas non-zero, then $F_i(\mathbb{Z}_p) = F(i) + p^e\mathbb{Z}_p$.*

Proof. As a result of Proposition 23, it suffices to show

$$g_i\Big(\omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)\Big) \supseteq F(i) + p^e\mathbb{Z}_p.$$

Let $z \in F(i) + p^e\mathbb{Z}_p$. We first show that there exists $y \in \omega(\phi)^i + p^e\mathcal{O}_K$ such that $g_i(y) = z$, and then we show $y \in \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$.

The equation $g_i(y) = z$ is equivalent to $y^2 - \sqrt{5}zy - (-1)^i = 0$. Let $y_0 = \omega(\phi)^i$. Binet's formula (2) shows that $\frac{y_0 - (-1)^i y_0^{-1}}{\sqrt{5}} \equiv \frac{\phi^i - (-1)^i\phi^{-i}}{\sqrt{5}} = F(i) \equiv z \mod p^e$, so $y_0^2 - \sqrt{5}zy_0 - (-1)^i \equiv 0 \mod p^e$. The discriminant of $y^2 - \sqrt{5}zy - (-1)^i$ is $5z^2 + (-1)^i 4 \equiv 5F(i)^2 + (-1)^i 4 = L(i)^2 \mod p^e$. Therefore $(5z^2 + (-1)^i 4) \bmod p$ is a quadratic residue. Since i is a Lucas non-zero, we have $5z^2 + (-1)^i 4 \not\equiv 0 \mod p$, so $\mathbb{Z}_p$ contains two distinct square roots of $5z^2 + (-1)^i 4$. The two solutions to $y^2 - \sqrt{5}zy - (-1)^i = 0$ are $y = \frac{\pm w + \sqrt{5}z}{2}$, where $w \in \mathbb{Z}_p$ is a square root of $5z^2 + (-1)^i 4$. Choose w such that $\frac{w + \sqrt{5}z}{2} \in \omega(\phi)^i + p^e\mathcal{O}_K$. It remains to show that $\frac{w + \sqrt{5}z}{2} \in \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$.

If $p \equiv 1, 4 \mod 5$, then $\sqrt{5} \in \mathbb{Z}_p$ and Proposition 18 implies that $\exp_p$ is an isomorphism from $p^e\mathbb{Z}_p$ to $1 + p^e\mathbb{Z}_p$, so

$$\omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p) = \omega(\phi)^i(1 + p^e\mathbb{Z}_p) = \omega(\phi)^i + p^e\mathbb{Z}_p.$$

Therefore $\frac{w+\sqrt{5}z}{2} \in \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$.

Let $p \equiv 2,3 \mod 5$. We have $y_0\overline{y_0} = \omega(\phi)^i\omega(\bar{\phi})^i = (-1)^i$, so $w^2 = 5z^2 + 4y_0\overline{y_0}$. By Lemma 21, $\frac{w+\sqrt{5}z}{2} \in \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$. □

The last major step in the proof of Theorem 1 is to establish the measure of $F_i(\mathbb{Z}_p)$ for Lucas zeros i. We do this in Proposition 27, using the following two lemmas.

Lemma 25. *Let p be a prime such that $p \neq 2$ and $p \neq 5$. Let i be a Lucas zero, and define $\zeta = \omega(\phi)^i$. Then $\zeta \in \sqrt{5}\mathbb{Z}_p$.*

Proof. Since i is a Lucas zero and $L(i) = \frac{\phi^{2i}+(-1)^i}{\phi^i}$, we have $\zeta^2 = \omega(\phi^{2i}) = -(-1)^i$. (In particular, $\zeta^4 = 1$.)

If $p \equiv 1,4 \mod 5$, then $\sqrt{5} \in \mathbb{Z}_p$, so it follows that $\zeta \in \sqrt{5}\mathbb{Z}_p$ as desired. If $p \equiv 2,3 \mod 5$, write $\zeta = a + b\sqrt{5}$ where $a, b \in \mathbb{Z}_p$. Since $a^2 + 2ab\sqrt{5} + 5b^2 = \zeta^2 \in \mathbb{Z}_p$, this implies $a = 0$ or $b = 0$, so $\zeta \in \mathbb{Z}_p$ or $\zeta \in \sqrt{5}\mathbb{Z}_p$. Vinson [13, Theorem 4] showed that $\frac{\pi(p)}{\alpha(p)} = 2$ if $p \equiv 3,7 \mod 20$ and $\frac{\pi(p)}{\alpha(p)} = 4$ if $p \equiv 13,17 \mod 20$. These two cases include all primes $p \equiv 2,3 \mod 5$ such that $p \neq 2$, so Theorem 7 and Proposition 9 imply that i is even. Therefore $\zeta^2 = -(-1)^i = -1$. If $p \equiv 3 \mod 4$, then one of the supplements to quadratic reciprocity implies $\zeta \notin \mathbb{Z}_p$, so $\zeta \in \sqrt{5}\mathbb{Z}_p$. If $p \equiv 1 \mod 4$, then $p \equiv 13,17 \mod 20$, so $\frac{\pi(p)}{\alpha(p)} = 4$ and there are no Lucas zeros, so the statement is vacuously true. □

Since $\zeta \in \sqrt{5}\mathbb{Z}_p$ by Lemma 25, for a given $j \in \mathbb{Z}_p$ the residue $\zeta\sqrt{5}j \bmod p$ is either a quadratic residue or a quadratic non-residue. This allows us, for a given z, to characterize the Lucas zeros i for which $y^2 - \sqrt{5}zy - (-1)^i = 0$ has a solution $y \in \mathbb{Z}_p$.

Lemma 26. *Let p be a prime such that $p \neq 2$ and $p \neq 5$. Let i be a Lucas zero, and define $\zeta = \omega(\phi)^i$. Let $z \in \mathbb{Z}_p$. Define $\lambda \in \mathbb{Z}$ by $\left|z - \zeta\frac{2}{\sqrt{5}}\right|_p = \frac{1}{p^\lambda}$, and define $j \in \{1, 2, \ldots, p-1\}$ by $z \equiv \zeta\frac{2}{\sqrt{5}} + jp^\lambda \mod p^{\lambda+1}$.*

1. *The equation $y^2 - \sqrt{5}zy - (-1)^i = 0$ has a solution $y \in \mathbb{Z}_p$ if and only if λ is even and $\zeta\sqrt{5}j \bmod p$ is a quadratic residue.*
2. *If $y^2 - \sqrt{5}zy - (-1)^i = 0$ has a solution $y \in \mathbb{Z}_p$, then $|y - \zeta|_p = \frac{1}{p^{\lambda/2}}$.*

To prove Lemma 26, we use the following version of Hensel's lemma in $\mathcal{O}_K$.

Hensel's lemma. *Let $f(x) \in \mathcal{O}_K[x]$. If there exists $y_0 \in \mathcal{O}_K$ such that $|f(y_0)|_p < |f'(y_0)|_p^2$, then there is a unique $y \in \mathcal{O}_K$ satisfying $|y - y_0|_p < |f'(y_0)|_p$ such that $f(y) = 0$.*

Proof of Lemma 26. Let $f_z(y) := y^2 - \sqrt{5}zy - (-1)^i$. As in the proof of Lemma 25, $\zeta^2 = \omega(\phi^{2i}) = -(-1)^i$. Therefore we can write $f_z(y) = y^2 - \sqrt{5}zy + \zeta^2$.

To prove Assertion (1), first assume λ is even and $\zeta\sqrt{5}j \bmod p$ is a quadratic residue. Let $a \in \{1, \ldots, p-1\}$ such that $a^2 \equiv \zeta\sqrt{5}j \mod p$. We now check that $y_0 := \zeta + p^{\lambda/2}a$ satisfies the condition of Hensel's lemma. Using $\sqrt{5}z \equiv 2\zeta + \sqrt{5}jp^\lambda$

mod $p^{\lambda+1}$, we have

$$\begin{aligned} f_z(y_0) &= y_0^2 - \sqrt{5}zy_0 + \zeta^2 \\ &\equiv \left(\zeta + p^{\lambda/2}a\right)^2 - \left(2\zeta + \sqrt{5}jp^\lambda\right)\left(\zeta + p^{\lambda/2}a\right) + \zeta^2 \mod p^{\lambda+1} \\ &\equiv \left(a^2 - \zeta\sqrt{5}j\right)p^\lambda \mod p^{\lambda+1} \\ &\equiv 0 \mod p^{\lambda+1}. \end{aligned}$$

Therefore $|f_z(y_0)|_p \leq \frac{1}{p^{\lambda+1}}$. It remains to bound $|f_z'(y_0)|_p^2$. Since $z \equiv \zeta\frac{2}{\sqrt{5}} \mod p^{\lambda/2}$, we have $f_z'(y_0) \equiv 2y_0 - 2\zeta \equiv 0 \mod p^{\lambda/2}$, but $f_z'(y_0) \not\equiv 0 \mod p^{\lambda/2+1}$ since $a \not\equiv 0 \mod p$. Therefore

$$|f_z(y_0)|_p \leq p^{-\lambda-1} < p^{-\lambda} = |f_z'(y_0)|_p^2,$$

so Hensel's lemma implies that $f_z(y)$ has a unique root $y \in \mathbb{Z}_p$ satisfying $|y - (\zeta + p^{\lambda/2}a)|_p < \frac{1}{p^{\lambda/2}}$. It follows that $|y - \zeta|_p = \frac{1}{p^{\lambda/2}}$. This proves one direction of Assertion (1) and also Assertion (2).

Conversely, assume $y^2 - \sqrt{5}zy + \zeta^2 = 0$ and $y \in \mathbb{Z}_p$. Since $z \equiv \zeta\frac{2}{\sqrt{5}} \mod p^\lambda$, we have

$$\begin{aligned} 0 &= y^2 - \sqrt{5}zy + \zeta^2 \\ &\equiv y^2 - 2\zeta y + \zeta^2 \mod p^\lambda \\ &= (y-\zeta)^2. \end{aligned}$$

There are two cases.

If λ is even, this implies $y \equiv \zeta \mod p^{\lambda/2}$. Write $y = \zeta + p^{\lambda/2}a$ for some $a \in \mathbb{Z}_p$. Expanding $f_z(y)$ as above shows that $0 = f_z(y) \equiv \left(a^2 - \zeta\sqrt{5}j\right)p^\lambda \mod p^{\lambda+1}$. Therefore $\zeta\sqrt{5}j \bmod p$ is a quadratic residue.

If λ is odd, then $0 \equiv (y-\zeta)^2 \mod p^\lambda$ implies $y \equiv \zeta \mod p^{(\lambda+1)/2}$. Write $y = \zeta + p^{(\lambda+1)/2}a$ for some $a \in \mathbb{Z}_p$. Then

$$\begin{aligned} 0 &= y^2 - \sqrt{5}zy + \zeta^2 \\ &\equiv \left(\zeta + p^{(\lambda+1)/2}a\right)^2 - \left(2\zeta + \sqrt{5}jp^\lambda\right)\left(\zeta + p^{(\lambda+1)/2}a\right) + \zeta^2 \mod p^{\lambda+1} \\ &\equiv -\zeta\sqrt{5}jp^\lambda \mod p^{\lambda+1}, \end{aligned}$$

which contradicts $j \in \{1, 2, \ldots, p-1\}$. Therefore there is no solution $y \in \mathbb{Z}_p$ when λ is odd. □

Proposition 27. *Let p be a prime such that $p \neq 2$ and $p \neq 5$, and define $e \geq 1$ by $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$. If i is a Lucas zero, then $\mu(F_i(\mathbb{Z}_p)) = \frac{1}{2p^{2e-1}(p+1)}$.*

Proof. Let i be a Lucas zero. We would like to determine the measure of the set

$$F_i(\mathbb{Z}_p) = \{z \in \mathbb{Z}_p : g_i(y) = z \text{ for some } y \in h_i(\mathbb{Z}_p)\}.$$

Let $z \in \mathbb{Z}_p$. As in the proof of Proposition 24, $g_i(y) = z$ if and only if $y^2 - \sqrt{5}zy - (-1)^i = 0$. Let $\zeta = \omega(\phi)^i$. Define $\lambda \in \mathbb{Z}$ by $\left|z - \zeta\frac{2}{\sqrt{5}}\right|_p = \frac{1}{p^\lambda}$, and define $j \in \{1, 2, \ldots, p-1\}$ by $z \equiv \zeta\frac{2}{\sqrt{5}} + jp^\lambda \mod p^{\lambda+1}$. By Lemma 26, if λ is odd then $g_i(y) = z$ has no solution $y \in \mathbb{Z}_p$. Furthermore, if λ is even then $g_i(y) = z$ has a unique solution $y \in \mathbb{Z}_p$ if $\zeta\sqrt{5}j \bmod p$ is a quadratic residue and no solution otherwise. In the case that there is a unique solution, we will show that $y \in h_i(\mathbb{Z}_p)$

if and only if $\lambda \geq 2e$. Since there are $\frac{p-1}{2}$ nonzero quadratic residues modulo p and the set $\zeta\frac{2}{\sqrt{5}} + jp^\lambda + p^{\lambda+1}\mathbb{Z}_p$ has measure $\frac{1}{p^{\lambda+1}}$, it will then follow that

$$\mu(F_i(\mathbb{Z}_p)) = \sum_{\substack{\lambda \geq 2e \\ \lambda \text{ even}}} \frac{p-1}{2} \cdot \frac{1}{p^{\lambda+1}} = \frac{1}{2p^{2e-1}(p+1)}.$$

To that end, assume that λ is even and $\zeta\sqrt{5}j \bmod p$ is a quadratic residue. Let $y \in \mathbb{Z}_p$ be the unique solution of $g_i(y) = z$, which is guaranteed by Lemma 26. In particular, $|y - \omega(\phi)^i|_p = \frac{1}{p^{\lambda/2}}$.

If $\lambda < 2e$, then $|y - \omega(\phi)^i|_p = \frac{1}{p^{\lambda/2}} > p^{-e}$. By Lemma 22, $y \notin h_i(\mathbb{Z}_p)$.

For the other direction, assume $\lambda \geq 2e$. Then $|y - \omega(\phi)^i|_p = \frac{1}{p^{\lambda/2}} \leq p^{-e}$. We show that $y \in h_i(\mathbb{Z}_p)$. There are two cases.

If $p \equiv 1, 4 \mod 5$, then $h_i(\mathbb{Z}_p) = \omega(\phi)^i + p^e\mathbb{Z}_p$ (again by Lemma 20 and the proof of Proposition 24), so $y \in h_i(\mathbb{Z}_p)$.

Let $p \equiv 2, 3 \mod 5$. Let $y_0 = \omega(\phi)^i$. Since i is a Lucas zero, we have $\omega(\phi)^i + (-1)^i\omega(\phi)^{-i} \equiv 0 \mod p$. In fact, we can strengthen this congruence to $\omega(\phi)^i + (-1)^i\omega(\phi)^{-i} \equiv 0 \mod p^e$ by Theorem 14 (along with the fact that $e = 1$ for $p = 3$). Therefore $\frac{y_0 - (-1)^i y_0^{-1}}{\sqrt{5}} = \frac{\omega(\phi)^i - (-1)^i\omega(\phi)^{-i}}{\sqrt{5}} \equiv \zeta\frac{2}{\sqrt{5}} \equiv z \mod p^e$, so $y_0^2 - \sqrt{5}zy_0 - (-1)^i \equiv 0 \mod p^e$. The discriminant of $y^2 - \sqrt{5}zy - (-1)^i$ is

$$\begin{aligned} 5z^2 + (-1)^i 4 &\equiv 5\left(\zeta\frac{2}{\sqrt{5}} + jp^\lambda\right)^2 + (-1)^i 4 \mod p^{\lambda+1} \\ &\equiv 4\zeta\sqrt{5}jp^\lambda \mod p^{\lambda+1}, \end{aligned}$$

so $\frac{1}{p^\lambda}(5z^2 + (-1)^i 4) \equiv 2^2 \cdot \zeta\sqrt{5}j \mod p$ is a quadratic residue. Let $w \in p^{\lambda/2}\mathbb{Z}_p$ be the square root of $5z^2 + (-1)^i 4$ satisfying $\frac{w+\sqrt{5}z}{2} \in \omega(\phi)^i + p^e\mathcal{O}_K$. The two solutions to $y^2 - \sqrt{5}zy - (-1)^i = 0$ are $y = \frac{\pm w + \sqrt{5}z}{2}$. By Lemma 21, $\frac{w+\sqrt{5}z}{2} \in \omega(\phi)^i \exp_p(p^e\sqrt{5}\mathbb{Z}_p)$. Therefore $\frac{w+\sqrt{5}z}{2} \in h_i(\mathbb{Z}_p)$. $\square$

Putting together the previous results now allows us to prove the main result of the article.

Proof of Theorem 1. As mentioned in Section 1, for $p = 5$ it follows from Burr's characterization [3] that $\text{dens}(5) = 1$. We compute $N(5) = 5$ and $Z(5) = 0$, so $\text{dens}(5) = 1 = \frac{N(5)}{5} + \frac{Z(5)}{10 \cdot (5+1)}$ as desired.

Let p be a prime such that $p \neq 2$ and $p \neq 5$. Let $e = \nu_p(F(p - \epsilon))$. By Theorem 10, $\left|\frac{\phi}{\omega(\phi)} - 1\right|_p = \frac{1}{p^e}$.

By Theorem 15 and the discussion following it,

$$\text{dens}(p) = \mu\left(\bigcup_{i=0}^{p^f-2} F_i(\mathbb{Z}_p)\right) = \mu\left(\bigcup_{i=0}^{\pi(p)-1} F_i(\mathbb{Z}_p)\right).$$

By Proposition 24, if i is a Lucas non-zero, then $F_i(\mathbb{Z}_p) = F(i) + p^e\mathbb{Z}_p$. The number of distinct images is $N(p)$, so together the Lucas non-zeros contribute measure $\frac{N(p)}{p^e}$.

Let i be a Lucas zero. By Proposition 23, $F_i(\mathbb{Z}_p) \subseteq F(i) + p^e\mathbb{Z}_p$. If $F(i) \equiv F(j) \mod p^e$ for some Lucas non-zero j, then $F_i(\mathbb{Z}_p) \subseteq F(j) + p^e\mathbb{Z}_p = F_j(\mathbb{Z}_p)$, so $\mu(F_i(\mathbb{Z}_p) \cup F_j(\mathbb{Z}_p)) = \mu(F_j(\mathbb{Z}_p))$ and $F_i(\mathbb{Z}_p)$ makes no additional contribution to $\text{dens}(p)$. Otherwise, $F_i(\mathbb{Z}_p)$ is disjoint from $F_j(\mathbb{Z}_p)$ for all Lucas non-zeros j, so

$\mu(F_i(\mathbb{Z}_p) \cup F_j(\mathbb{Z}_p)) = \mu(F_i(\mathbb{Z}_p)) + \mu(F_j(\mathbb{Z}_p))$. There are $Z(p)$ Lucas zeros i such that $F(i) \not\equiv F(j) \mod p^e$ for all Lucas non-zeros j. If $Z(p) \geq 2$ then Proposition 9 implies that $Z(p) = 2$ and that the two images $F_i(\mathbb{Z}_p)$ are disjoint. Therefore the Lucas zeros contribute measure $\frac{Z(p)}{2p^{2e-1}(p+1)}$ by Proposition 27. $\square$

6. The prime $p = 2$

In this section we prove Theorem 6, which states that $\operatorname{dens}(2) = \frac{21}{32}$. For the prime $p = 2$, the period length is $\pi(2) = 3 = \alpha(2)$. There is one Lucas zero, namely $i = 0$. It is convenient to write elements of $\mathbb{Q}_2(\sqrt{5})$ as elements of $\mathbb{Q}_2(\phi)$ instead since the denominator of $\frac{1+\sqrt{5}}{2}$ obscures the fact that ϕ is a 2-adic algebraic integer. Recall that if $|x|_2 = 1$ then $\omega(x)$ is the 3rd root of unity satisfying $\omega(x) \equiv x \mod 2$. The roots of unity congruent modulo 2 to ϕ and $\bar{\phi}$ are

$$\begin{aligned}
\omega(\phi) &= \left(0 + \frac{1}{2^{-1}} + \frac{0}{2^{-2}} + \frac{0}{2^{-3}} + \cdots\right) + \left(1 + \frac{1}{2^{-1}} + \frac{0}{2^{-2}} + \frac{1}{2^{-3}} + \cdots\right)\phi \\
\omega(\bar{\phi}) &= \left(1 + \frac{0}{2^{-1}} + \frac{1}{2^{-2}} + \frac{1}{2^{-3}} + \cdots\right) + \left(1 + \frac{0}{2^{-1}} + \frac{1}{2^{-2}} + \frac{0}{2^{-3}} + \cdots\right)\phi.
\end{aligned}$$

Their product is $\omega(\phi)\omega(\bar{\phi}) = 1$ (since $\rho = \omega(\phi)\omega(\bar{\phi})$ is a root of unity satisfying $\rho^3 = 1$ and $\rho \equiv \phi\bar{\phi} = -1 \mod 2$).

The outline of the proof of Theorem 6 is the same as for other primes, but several details are different. First we need a version of Theorem 15. We compute $|\frac{\phi}{\omega(\phi)} - 1|_2 = \frac{1}{2}$ and $|\log_2 \frac{\phi}{\omega(\phi)}|_2 = \frac{1}{2} = p^{-1/(p-1)}$. The power series for $\exp_2$ does not converge when evaluated at $\log_2 \frac{\phi}{\omega(\phi)}$; in particular, we cannot replace $\frac{\phi}{\omega(\phi)}$ with $\exp_2 \log_2 \frac{\phi}{\omega(\phi)}$. Consequently the interpolation is comprised of 6 functions rather than 3.

Theorem 28. *For each $i \in \{0, 1, 2\}$ and each $r \in \{0, 1\}$, define the function $F_{i,r}\colon r + 2\mathbb{Z}_2 \to \mathbb{Q}_2(\sqrt{5})$ by*

$$F_{i,r}(r+2x) = \frac{\omega(\phi)^{i-r}\phi^r \exp_2\Big(x \log_2((\frac{\phi}{\omega(\phi)})^2)\Big) - \omega(\bar{\phi})^{i-r}\bar{\phi}^r \exp_2\Big(-x \log_2((\frac{\phi}{\omega(\phi)})^2)\Big)}{\sqrt{5}}.$$

Then $F_{i,r}(r + 2\mathbb{Z}_2) \subseteq \mathbb{Z}_2$, and $F(n) = F_{(n \bmod 3),(n \bmod 2)}(n)$ for all $n \geq 0$.

Proof. Let $p = 2$. We rewrite ϕ^n and $\bar{\phi}^n$ in Binet's formula (2) as functions that are defined on $\mathbb{Z}_2$. We have $|(\frac{\phi}{\omega(\phi)})^2 - 1|_2 = \frac{1}{4} < p^{-1/(p-1)}$ by direct computation (or by [9, Lemma 6]). Therefore $(\frac{\phi}{\omega(\phi)})^2 = \exp_2 \log_2((\frac{\phi}{\omega(\phi)})^2)$. For $m \geq 0$ and $r \in \{0, 1\}$, write

$$\begin{aligned}
\phi^{r+2m} &= \omega(\phi)^{2m}\phi^r (\tfrac{\phi}{\omega(\phi)})^{2m} \\
&= \omega(\phi)^{2m}\phi^r \exp_2 \log_2((\tfrac{\phi}{\omega(\phi)})^{2m}) \\
&= \omega(\phi)^{2m}\phi^r \exp_2\Big(m \log_2((\tfrac{\phi}{\omega(\phi)})^2)\Big),
\end{aligned}$$

and similarly for $\bar{\phi}$. For all $x \in \mathbb{Z}_2$, define

$$F_{i,r}(r+2x) := \frac{\omega(\phi)^{i-r}\phi^r \exp_2\Big(x \log_2((\frac{\phi}{\omega(\phi)})^2)\Big) - \omega(\bar{\phi})^{i-r}\bar{\phi}^r \exp_2\Big(x \log_2((\frac{\bar{\phi}}{\omega(\bar{\phi})})^2)\Big)}{\sqrt{5}}.$$

Then $F_{i,r}$ is an analytic function on $r+2\mathbb{Z}_2$ that agrees with F on $A_{i,r} := \{n \geq 0 : n \equiv i \mod 3 \text{ and } n \equiv r \mod 2\}$. Finally, since $\phi\bar{\phi} = -1$,

$$\begin{aligned}\log_2((\tfrac{\phi}{\omega(\phi)})^2) + \log_2((\tfrac{\bar{\phi}}{\omega(\phi)})^2) &= \log_2((\tfrac{\phi}{\omega(\phi)})^2 \cdot (\tfrac{\bar{\phi}}{\omega(\phi)})^2) \\ &= \log_2 1 \\ &= 0,\end{aligned}$$

so $\log_2((\frac{\bar{\phi}}{\omega(\phi)})^2) = -\log_2((\frac{\phi}{\omega(\phi)})^2)$. This gives the expression for $F_{i,r}(r+2x)$ stated in the theorem. By construction, $F(n) = F_{(n \bmod 3),(n \bmod 2)}(n)$ for all $n \geq 0$.

To see that $F_{i,r}(r+2x) \in \mathbb{Z}_2$ if $x \in \mathbb{Z}_2$, take a sequence of integers $(x_m)_{m\geq 0}$ that converges to x such that $r + 2x_m \equiv i \mod 3$ for each $m \geq 0$; since $F_{i,r}(r+2x_m) = F(r+2x_m) \in \mathbb{Z}$, it follows by continuity that $F_{i,r}(r+2x) \in \mathbb{Z}_p$. □

As in the proof of Theorem 28, let

$$A_{i,r} = \{n \geq 0 : n \equiv i \mod 3 \text{ and } n \equiv r \mod 2\}.$$

By the Chinese remainder theorem, $A_{i,r}$ is dense in $r + 2\mathbb{Z}_2$. Theorem 28 implies

$$\operatorname{dens}(2) = \mu\left(\bigcup_{i=0}^{2} \left(F_{i,0}(2\mathbb{Z}_2) \cup F_{i,1}(1+2\mathbb{Z}_2)\right)\right).$$

An upper bound on dens(2) can be obtained easily. Namely, the set of residues modulo 32 attained by the Fibonacci sequence is

$$\{0, 1, 2, 3, 5, 7, 8, 9, 11, 13, 15, 16, 17, 19, 21, 23, 24, 25, 27, 29, 31\}.$$

This set has size 21, so $\operatorname{dens}(2) \leq \frac{21}{32}$. Proposition 30 below implies that $\frac{21}{32}$ is also a lower bound on dens(2).

Write $F_{i,r}(r+2x) = g_r(h_{i,r}(x))$ where $g_r(y) = \frac{y-(-1)^r y^{-1}}{\sqrt{5}}$ and

$$h_{i,r}(x) = \omega(\phi)^{i-r}\phi^r \exp_2\Big(x \log_2((\tfrac{\phi}{\omega(\phi)})^2)\Big).$$

We next determine $h_{i,r}(\mathbb{Z}_2)$; this is analogous to Lemma 20.

Lemma 29. *For all $i \in \{0,1,2\}$ and $r \in \{0,1\}$, we have $h_{i,r}(\mathbb{Z}_2) = \omega(\phi)^{i-r}\phi^r \exp_2(4\sqrt{5}\mathbb{Z}_2)$.*

Proof. It follows from $|\log_2((\frac{\phi}{\omega(\phi)})^2)|_2 = \frac{1}{4}$ that $x\log_2((\frac{\phi}{\omega(\phi)})^2)$ is in the domain of $\exp_2$ for all $x \in \mathbb{Z}_2$. Since $(\frac{\phi}{\omega(\phi)})^2 \cdot (\frac{\bar{\phi}}{\omega(\bar{\phi})})^2 = (-1)^2 = 1$, Lemma 19 implies that $\log_2((\frac{\phi}{\omega(\phi)})^2) \in 4\sqrt{5}\mathbb{Z}_2$. Therefore

$$\begin{aligned}h_{i,r}(\mathbb{Z}_2) &= \omega(\phi)^{i-r}\phi^r \exp_2\Big(\mathbb{Z}_2 \log_2((\tfrac{\phi}{\omega(\phi)})^2)\Big) \\ &= \omega(\phi)^{i-r}\phi^r \exp_2(4\sqrt{5}\mathbb{Z}_2).\end{aligned}$$

□

The following proposition is analogous to Propositions 24 and 27. For the Lucas zero $i = 0$ there is no partial branching, but the images have smaller measure than the images for the Lucas non-zeros.

Proposition 30. *Let $i \in \{0,1,2\}$ and $r \in \{0,1\}$. The image of $r+2\mathbb{Z}_2$ under $F_{i,r}$ satisfies*

$$\begin{aligned} F_{1,0}(0+2\mathbb{Z}_2) &\supseteq 3+4\mathbb{Z}_2 \\ F_{i,r}(r+2\mathbb{Z}_2) &\supseteq 1+4\mathbb{Z}_2 \text{ for all } (i,r) \in \{(1,1),(2,0),(2,1)\} \\ F_{0,0}(0+2\mathbb{Z}_2) &\supseteq 8\mathbb{Z}_2 \\ F_{0,1}(1+2\mathbb{Z}_2) &\supseteq 2+32\mathbb{Z}_2. \end{aligned}$$

Proof. There are six cases. Let $z \in 3+4\mathbb{Z}_2$ if $(i,r)=(1,0)$ and $z \in 1+4\mathbb{Z}_2$ if $(i,r) \in \{(1,1),(2,0),(2,1)\}$. In these four cases, $z^2 \equiv 1 \mod 8$, so $5z^2+(-1)^r 4 \equiv 1 \mod 8$; therefore $\mathbb{Z}_2$ contains square roots of $5z^2+(-1)^r 4$. Similarly, if $(i,r)=(0,0)$ and $z \in 8\mathbb{Z}_2$, then $2\mathbb{Z}_2$ contains square roots of $5z^2+(-1)^r 4 = 5z^2+4 \equiv 4 \mod 64$. If $(i,r)=(0,1)$ and $z \in 2+32\mathbb{Z}_2$, then $4\mathbb{Z}_2$ contains square roots of $5z^2+(-1)^r 4 = 5z^2-4 \equiv 16 \mod 128$.

As in the proof of Proposition 24, $g_r(y)=z$ is equivalent to $y^2-\sqrt{5}zy-(-1)^r=0$, the solutions of which are $y=\frac{\pm w+\sqrt{5}z}{2}$, where $w \in \mathbb{Z}_2$ is a square root of $5z^2+(-1)^r 4$. Let $y_0=\omega(\phi)^{i-r}\phi^r$; then $\overline{y_0}=\omega(\bar{\phi})^{i-r}\bar{\phi}^r$ and $y_0\overline{y_0}=(-1)^r$. One checks that in all six cases $g_r(y_0) \equiv z \mod 4$. Choose w such that $\frac{w+\sqrt{5}z}{2} \equiv y_0 \mod 4$. Then the conditions of Lemma 21 are satisfied, so $\frac{w+\sqrt{5}z}{2} \in \omega(\phi)^{i-r}\phi^r \exp_2(4\sqrt{5}\mathbb{Z}_2)$. By Lemma 29, there exists $x \in \mathbb{Z}_2$ such that $F_{i,r}(r+2x)=z$. □

Proposition 30 implies that $\operatorname{dens}(2) \geq \frac{1}{4}+\frac{1}{4}+\frac{1}{8}+\frac{1}{32}=\frac{21}{32}$. Theorem 6 now follows. In particular, the superset relations for $F_{1,0}(0+2\mathbb{Z}_2)$, $F_{0,0}(0+2\mathbb{Z}_2)$, and $F_{0,1}(1+2\mathbb{Z}_2)$ in Proposition 30 are equalities.

Acknowledgment

We thank Genevieve Maalouf for productive discussions.

Data availability statement

Data generated during this study can be found in the OEIS [12, A350999 and A351000].

References

[1] Christian Ballot and Michele Elia, Rank and period of primes in the Fibonacci sequence: a trichotomy, *The Fibonacci Quarterly* **45** (2007) 56–63.
[2] Richard T. Bumby, A distribution property for linear recurrence of the second order, *Proceedings of the American Mathematical Society* **50** (1975) 101–106.
[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] Artūras Dubickas and Aivaras Novikas, Recurrence with prescribed number of residues, *Journal of Number Theory* **215** (2020) 120–137.
[5] Fernando Q. Gouvêa, *p-adic Numbers: An Introduction* second edition, Universitext, Springer–Verlag, Berlin, 1997.
[6] Christer Lech, A note on recurring series, *Arkiv för Matematik* **2** (1953) 417–421.
[7] Kurt Mahler, Eine arithmetische Eigenschaft der Taylor-koeffizienten rationaler Funktionen, *Koninklijke Nederlandse Akademie van Wetenschappen Proceedings* **38** (1935) 50–60.
[8] Richard J. McIntosh and Eric L. Roettger, A search for Fibonacci–Wieferich and Wolstenholme primes, *Mathematics of Computation* **76** (2007) 2087–2094.
[9] Eric Rowland and Reem Yassawi, p-adic asymptotic properties of constant-recursive sequences, *Indagationes Mathematicae* **28** (2017) 205–220.

[10] Carlo Sanna, On the number of residues of linear recurrences, *Research in Number Theory* **8** (2022) Article 7.

[11] Thoralf Skolem, Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, *Comptes rendus du huitième Congrès des Mathématiciens Scandinaves* (1934) 163–188.

[12] Neil Sloane et al., The On-Line Encyclopedia of Integer Sequences, `http://oeis.org`.

[13] John Vinson, The relation of the period modulo to the rank of apparition of m in the Fibonacci sequence, *The Fibonacci Quarterly* **1** (2) (1963) 37–45.

[14] Donald Dines Wall, Fibonacci series modulo m, *The American Mathematical Monthly* **67** (1960) 525–532.

Department of Mathematics, Hofstra University, Hempstead, NY, USA