New York Journal of Mathematics

New York J. Math. **23** (2017) 1045–1063.

Index divisibility in dynamical sequences and cyclic orbits modulo p

Annie S. Chen, T. Alden Gassert and Katherine E. Stange

Abstract. Let $\phi(x) = x^d + c$ be an integral polynomial of degree at least 2, and consider the sequence $(\phi^n(0))_{n=0}^{\infty}$, which is the orbit of 0 under iteration by ϕ. Let $D_{d,c}$ denote the set of positive integers n for which $n \mid \phi^n(0)$. We give a characterization of $D_{d,c}$ in terms of a directed graph and describe a number of its properties, including its cardinality and the primes contained therein. In particular, we study the question of which primes p have the property that the orbit of 0 is a single p-cycle modulo p. We show that the set of such primes is finite when d is even, and conjecture that it is infinite when d is odd.

Contents

1. Introduction

A dynamical sequence is the orbit $\alpha, \phi(\alpha), \phi^2(\alpha), \ldots$ of some α in a ring R under iteration of a map $\phi\colon R \to R$. In arithmetic dynamics, one often

Received September 1, 2016.

2010 *Mathematics Subject Classification.* Primary: 37P05, 37P25, 11Y55, Secondary: 11B37, 11B39, 11B50, 11G99.

Key words and phrases. arithmetic dynamics, dynamical portrait, index divisibility, cycle, orbit, functional digraph, dynamical sequence, polynomial map, iteration, quadratic map, divisibility sequence, integer sequence, post-critical orbit.

The third author's work was supported by the National Security Agency grant H98230-16-1-0040 and National Science Foundation grant DMS-1643552.

ISSN 1076-9803/2017

takes ϕ to be a rational map defined over a number field and α to be an algebraic number. Such dynamical sequences have many properties in common with their more well-known cousins: recurrence sequences and algebraic divisibility sequences arising from algebraic groups, such as Lucas sequences and elliptic divisibility sequences. In particular, all such sequences a_n are *divisibility sequences*, i.e., whenever $n \mid m$, then $a_n \mid a_m$.

The study of the primes appearing in such sequences has a centuries-long history dating back at least to Fermat's study of primes of the form $2^{2^n}+1$, which is a dynamical sequence with $\alpha = 3$ and $\phi(x) = (x-1)^2 + 1$. The primes appearing in a dynamical sequence encode information about the dynamical system in residue fields. For example, taking $R = \mathbb{Z}$, if $p \mid \phi^n(0)$, then 0 has period dividing n in the dynamical system $\phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. (The period of 0 is the smallest positive integer k for which $\phi^k(0) = 0$.) In particular, $p \mid \phi^p(0)$ if and only if the dynamical system given by ϕ on $\mathbb{Z}/p\mathbb{Z}$ consists of a single orbit of size 1 or p. Silverman studied the statistics of orbit sizes for rational maps modulo a varying prime p [27] (see also [8]).

In this paper, we restrict ourselves to the study of the maps

$$\phi(x) = x^d + c \in \mathbb{Z}[x],$$

where $d \geq 2$. The orbit structure for $x^2 + c$ is of particular interest for primality testing, integer factorization and pseudo-random number generation [6, 20, 22]. Silverman collected some numerical data on quadratic maps $x^2 + c$ [27], while Peinado, Montoya, Muñoz and Yuste give explicit upper bounds for the cycle sizes of $x^2 + c$ in a finite field [21]; more explicit structure is known for the exceptional maps x^2 and $x^2 - 2$ [33]. Jones [18] found that the natural density of primes dividing at least one nonzero term of a dynamical sequence is zero for four infinite families of quadratic functions, including $\phi(x) = x^2 + c$, where $c \in \mathbb{Z}$ and $c \neq 1$. Hamblen, Jones, and Madhu [13] later generalized the results to $\phi(x) = x^d + c$ (see also [5]). In other words, the primes p for which 0 is periodic (instead of pre-periodic) are of density zero. These results imply that the primes p for which the dynamical system consists of a single p-cycle modulo p are of density zero.

Let $S_{d,c}$ be the set of primes p such that the dynamical system

$$\phi\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

consists of a single p-cycle. We show the following.

Theorem 1.1. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Then whenever d is even and c is odd, $S_{d,c} = \{2\}$; while if d is even and c is even, then $S_{d,c} = \emptyset$.*

Based on numerical data and heuristics, we conjecture that there are infinitely many such primes otherwise.

Conjecture 1.2. $S_{d,c}$ is infinite whenever d is odd.

Using an analysis of the cycle structure of the permutation $x \mapsto x^d$ on $\mathbb{Z}/p\mathbb{Z}$, we are able to somewhat restrict the set $S_{d,c}$ as follows.

Theorem 1.3. *If $d \equiv 3 \pmod 4$, and $p \equiv 1 \pmod 4$ is prime, then $p \notin S_{d,c}$.*

For example, when d is an odd power of 3, we conclude that $S_{d,c}$ contains only primes congruent to $11 \pmod{12}$ (Corollary 4.4).

A related question arises naturally by reversing the roles of p and c: fix p and ask which maps ϕ_c in some varying family such as $\phi_c = x^d + c$ have a single p-cycle modulo p. Hutz and Towsley consider a generalization of this question for the families $x^d + c$ [15]; see [25, Section 6.1] for an overview of the setting. We touch on this problem in Sections 5 and 6.

Theorem 1.1 is a consequence of our study of *index divisibility* in dynamical sequences. The question of index divisibility for a sequence $(a_n)_{n=0}^{\infty}$ seeks to characterize those integers $n \geq 1$ such that $n \mid a_n$. It has a substantial history for Fibonacci and Lucas sequences [3, 14, 17, 24, 30, 31, 32, 34], and has also been studied for elliptic divisibility sequences [12, 29] and general linear recurrences [2]. As another example, composite integers n for which $n \mid a^n - a$ are called pseudoprimes to the base a.

Throughout, let $\phi(x) = x^d + c \in \mathbb{Z}[x]$ where $d \geq 2$, let (W_n) denote the orbit of 0 under ϕ, i.e., $W_n = \phi^n(0)$, and define

$$D_{d,c} := \{n \in \mathbb{Z} : n \geq 1, n \mid W_n\}, \quad \text{and} \quad P_{d,c} := \{p \in D_{d,c} : p \text{ is prime}\}.$$

We show that except in a few restricted cases, $D_{d,c}$ is infinite.

Theorem 1.4. *The set $D_{d,c}$ is finite if and only if either*

(1) *d is even and $c = 1$, or*
(2) *$d = 2$ and $c = -2$.*

Moreover, if $D_{d,c}$ is finite, then $D_{d,c} = \{1, 2\}$.

In the spirit of Smyth and of Silverman and Stange [29, 30], we represent $D_{d,c}$ by a directed graph that connects each element to its minimal multiples. To construct this *index divisibility graph* G, initially let 1 be in the vertex set G_V, then add vertices and edges to G iteratively according to the following rules.

Let $v_p(x)$ denote the p-adic valuation of an integer x. For each $n \in G_V$, adjoin the vertex np and the directed edge (n, np) if

(1) p is a prime satisfying $v_p(\phi^n(0)) > v_p(n)$ (edge of *type* 1), or
(2) $p \in P_{d,c}$ satisfies $v_p(n) = 0$ (edge of *type* 2).

We prove Theorem 1.4 via a characterization of $D_{d,c}$ and $P_{d,c}$ in terms of this graph.

Theorem 1.5. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Let G be the index divisibility graph corresponding to ϕ, and let G_V be the vertex set of G. Then $G_V = D_{d,c}$.*

As for $P_{d,c}$, we obtain a partial characterization.

Theorem 1.6. *Let $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Then $P_{d,c}$ satisfies the following.*

(1) $2 \in P_{d,c}$.
(2) *Every divisor of c is an element of $D_{d,c}$. In particular, if p is prime and $p \mid c$, then $p \in P_{d,c}$.*
(3) *If p is prime and $d \equiv 1 \pmod{p-1}$, then $p \in P_{d,c}$.*

If d is even, then we are able to fully characterize $P_{d,c}$.

Theorem 1.7. *If d is even, then*

$$P_{d,c} = \{2\} \cup \{p \text{ prime} : p \mid c\}.$$

Theorem 1.1 is an immediate consequence.

Two main tools we use in our investigation are the notions of a *rigid divisibility sequence* and of a *primitive prime divisor*.

An integer sequence (a_n) is a *rigid divisibility sequence* if for every prime p the following two properties hold:

(1) if $v_p(a_n) > 0$, then $v_p(a_{nk}) = v_p(a_n)$ for all $k \geq 1$, and
(2) if $v_p(a_n) > 0$ and $v_p(a_m) > 0$, then $v_p(a_n) = v_p(a_m) = v_p(a_{\gcd(m,n)})$.

In particular, rigid divisibility sequences are divisibility sequences.

Rice [23] showed that for any polynomial $\phi \in \mathbb{Z}[x]$ of degree $d \geq 2$ where 0 is a wandering point (i.e., of infinite orbit), the integer sequence $(\phi^n(0))$ is a rigid divisibility sequence if and only if the coefficient of the linear term of ϕ is zero. In particular, this means that the orbit of zero under $\phi(x) = x^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$, is a rigid divisibility sequence.

Given a sequence (a_n) of integers, the term a_n contains a *primitive prime divisor* if there exists a prime p such that $p \mid a_n$, but $p \nmid a_i$ for all $0 < i < n$. The study of primitive prime divisors dates back to Bang and Zsigmondy, who showed that every term of the sequence $(a^n - b^n)$, where $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$, has a primitive prime divisor [4, 35]. Carmichael's Theorem asserts that the same is true for the Fibonacci numbers beyond the 12th term [7]. The *Zsigmondy set* is the set of terms not having a primitive prime divisor; for the Fibonacci numbers, it is $\{1, 2, 6, 12\}$. Similarly, Silverman has shown that elliptic divisibility sequences have finite Zsigmondy sets [28].

Turning to dynamical sequences, Rice [23] showed that if $\phi(x) \in \mathbb{Z}[x]$ is a monic polynomial of degree $d \geq 2$, and $(\phi^n(0))$ is an unbounded rigid divisibility sequence, then all but finitely many terms contain a primitive prime divisor. Ingram and Silverman [16] generalized the results to rational functions over number fields (see also [10, 11]). Doerksen and Haensch [9] extended upon this by finding explicit upper bounds on the Zsigmondy set for certain polynomial maps.

The following examples illustrate our results.

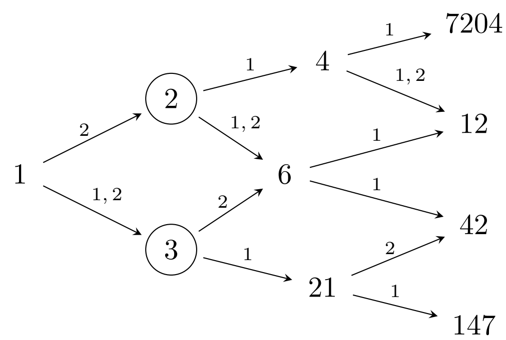

FIGURE 1. A portion of the index divisibility graph for $\phi(x) = x^2 + 3$. The circled vertices are elements of $P_{2,3}$, and edges are labeled by their type.

Example 1.8. Suppose $\phi(x) = x^2 + 3$. Then the orbit of 0 is

$$0, 3, 12, 147, 21612, 467078547, \ldots.$$

Here,

$$D_{2,3} = \{1, 2, 3, 4, 6, 12, 21, 42, \ldots\} \quad \text{and} \quad P_{2,3} = \{2, 3\}$$

by Theorems 1.6 and 1.7. The index divisibility graph is shown in Figure 1.

Notice in Figure 1 that all type 2 edges are also type 1 edges. However, this is not always the case, as shown in Figure 2.

Example 1.9. Suppose $\phi(x) = x^3 + 4$. Then the orbit of 0 is:

$$0, 4, 68, 314436, \ldots.$$

The index divisibility graph is illustrated in Figures 2 and 3.

In Section 2, we study index divisibility and prove Theorems 1.1, 1.5, 1.6, and 1.7.

In Section 3, we prove Theorem 1.4.

In Section 4, we study $P_{d,c}$ and its subset $S_{d,c}$ in the case where d is odd, and prove Theorem 1.3.

In Section 5, we ask the question, for a fixed n, of which pairs (d, c) satisfy $n \in D_{d,c}$.

Finally, in Section 6, as a computational experiment, we find all pairs (p, c), where $0 < c < p/2$ and $p \leq 37619$, for which p is in $S_{3,c}$ (see Figure 4). We combine this data with heuristics to support Conjecture 1.2.

Acknowledgements. The authors would like to thank the Boulder Valley School District's Science Research Seminar program for making this research project possible, and would like to thank the first author's teacher in that program, Ryan O'Block, for his support. The authors also wish to thank

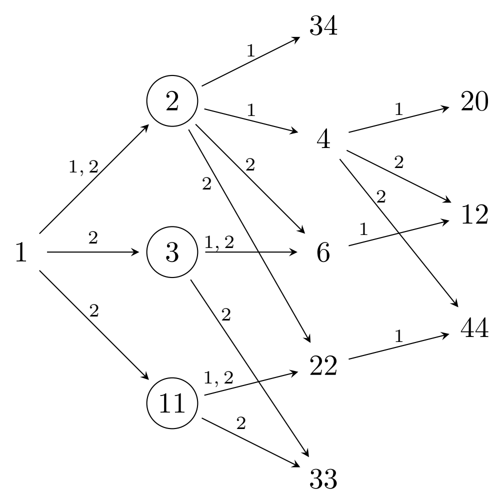

FIGURE 2. A portion of the index divisibility graph for $\phi(x) = x^3 + 4$. The circled vertices are elements of $P_{3,4}$, and edges are labeled by their type.

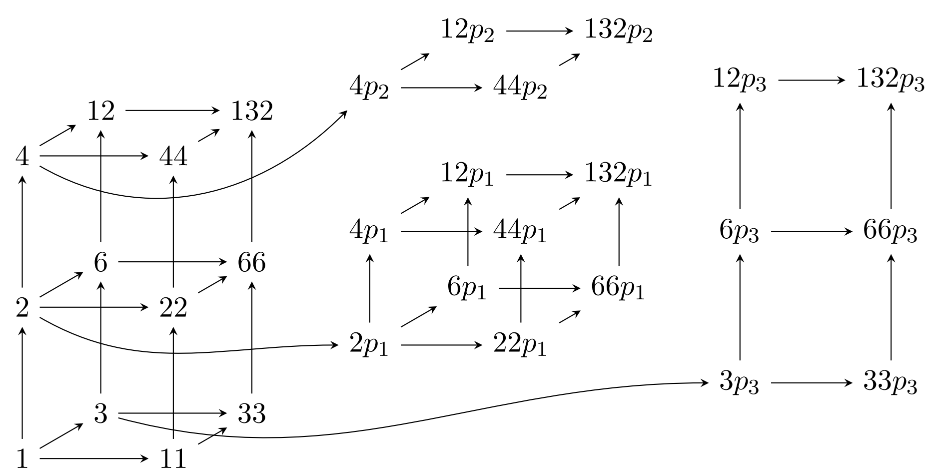

FIGURE 3. A graphical representation of a portion of $D_{3,4}$. Here $p_1 = 17$, $p_2 = 5$, and $p_3 = 26203$. To avoid clutter, not every edge between the vertices shown here is depicted.

Anna Haensch, Rafe Jones, Michelle Manes and Joseph Silverman for helpful conversations. The authors are also indebted to the anonymous referee for useful and thought-provoking comments.

2. Index divisibility

For the remainder of the paper, we maintain the notation presented in the introduction, namely $\phi(x) = x^d + c$ is an integral polynomial of degree at least 2, $W_n = \phi^n(0)$, $D_{d,c} = \{n \in \mathbb{Z} : n \geq 1, n \mid W_n\}$, and $P_{d,c}$ is the set of primes in $D_{d,c}$.

Before proceeding to the proofs, we identify two significant properties of $D_{d,c}$.

Lemma 2.1. *Suppose $n \in D_{d,c}$ and let p be the smallest prime divisor of n. Then $p \in D_{d,c}$.*

Proof. Let $n \in D_{d,c}$, and write $n = pm$, where p is the smallest prime factor of n. Then $p \mid W_n$ as $p \mid n$ and $n \mid W_n$. In particular, 0 is periodic modulo p, so letting b denote the period of 0, it follows that $0 < b \leq p$, $p \mid W_b$, and $b \mid n$. However, since p is the smallest factor of n greater than 1, either $b = 1$ or $b = p$. If $b = p$, then $p \mid W_p$ as desired. Otherwise, if $b = 1$, then $p \mid W_1$, and hence $p \mid W_p$ since $W_1 \mid W_p$. □

Lemma 2.2. *If $a, b \in D_{d,c}$ are relatively prime, then $ab \in D_{d,c}$.*

Proof. Let a and b be relatively prime numbers in $D_{d,c}$. Since (W_n) is a rigid divisibility sequence, we have that $a \mid ab$ implies $W_a \mid W_{ab}$, and $b \mid ab$ implies $W_b \mid W_{ab}$. Then because $a \mid W_a$, $a \mid W_{ab}$. Similarly, because $b \mid W_b$, we have $b \mid W_{ab}$. Since a and b are relatively prime, $ab \mid W_{ab}$, and so $ab \in D_{d,c}$. □

Proof of Theorem 1.5. First we show $G_V \subseteq D_{d,c}$. To begin, we have $1 \mid W_1$, and so $1 \in D_{d,c}$.

Next we show that if $n \in D_{d,c}$ and $(n, np) \in G_E$ (the edge set of G), then $np \in D_{d,c}$. We examine edges of type 1. Suppose there exist $n \in D_{d,c}$ and a prime p such that $v_p(W_n) > v_p(n)$. Since $n \mid W_n$ and $v_p(W_n) > v_p(n)$, we see that $np \mid W_n$. Then since (W_n) is a rigid divisibility sequence, $n \mid np$ implies $W_n \mid W_{np}$. Thus $np \mid W_{np}$, and so $np \in D_{d,c}$.

For edges of type 2, if $p \in P_{d,c}$ and $p \nmid n$, then $np \in D_{d,c}$ by Lemma 2.2. Thus we have shown that $G_V \subseteq D_{d,c}$.

We now proceed to show $D_{d,c} \subseteq G_V$. Suppose $n \in D_{d,c}$. To prove that $n \in G_V$, we show that G contains a path from 1 to n. If $n = 1$, there is nothing to show, so let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ be the prime factorization of n, where $p_1 < p_2 < p_3 < \cdots < p_k$. From Lemma 2.1, we know that $p_1 \in D_{d,c}$, hence $(1, p_1)$ is an edge of type 2 in G.

Now suppose $1 \leq i \leq k$ and m is the largest divisor of n supported on primes p_j, where $j < i$. If $p_i \in P_{d,c}$, then (m, mp_i) is an edge of type 2. For the case $p_i \notin P_{d,c}$, we note the following.

(1) If 0 is periodic modulo ℓ for some integer ℓ, and $\ell' \mid \ell$, then 0 is periodic modulo ℓ'. Moreover, the period of 0 modulo ℓ' divides the period of 0 modulo ℓ.

(2) Since $n \mid W_n$, we have 0 is periodic modulo n. Moreover, the period of 0 modulo n is a divisor of n.

From these observations, we see that 0 is periodic modulo p_i, and the period of 0 is a divisor of n. Therefore if $p_i \notin P_{d,c}$, then the period of 0 modulo p_i is a divisor of n that is strictly less than p_i. In particular, the period of 0 modulo p_i divides m, and hence $p_i \mid W_m$. Thus $v_{p_i}(W_m) > v_{p_i}(m)$, and so (m, mp_i) is an edge of type 1.

We have now established that $mp_i \in D_{d,c}$, and hence $p_i \mid W_{mp_i} \mid W_{mp_i^t}$ for each $1 \leq t < \alpha_i$. By rigid divisibility,

$$v_{p_i}(W_{mp_i^t}) = v_{p_i}(W_n) \geq \alpha_i > t = v_{p_i}(mp_i^t).$$

Therefore, we also have an edge of type 1: (mp_i^t, mp_i^{t+1}). All told, we have the following path of directed edges in G from 1 to n:

$$\begin{aligned}
&1 \xrightarrow{2} p_1 \xrightarrow{1} p_1^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} \\
&\xrightarrow{1or2} p_1^{\alpha_1} p_2 \xrightarrow{1} p_1^{\alpha_1} p_2^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \\
&\xrightarrow{1or2} \cdots \\
&\xrightarrow{1or2} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^2 \xrightarrow{1} \cdots \xrightarrow{1} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n.
\end{aligned}$$

Thus, $D_{d,c} \subseteq G_V$. □

Proof of Theorem 1.6. First, $W_2 = c^d + c = c^{d-1}(c+1)$. It follows that $2 \mid W_2$, and thus $2 \in P_{d,c}$. Second, $W_1 = c$, and therefore $c \mid W_n$ for all n since (W_n) is a divisibility sequence.

For the third property, we show that if p is prime, then $p \in P_{d,c}$ if $d \equiv 1 \pmod{p-1}$. Let $d = (p-1)k + 1$, where $k \in \mathbb{Z}$. We have

$$\phi(x) = x^d + c = x^{(p-1)k+1} + c \equiv x + c \pmod{p},$$

so $\phi^p(x) \equiv x + pc \equiv x \pmod{p}$. In particular, this means that $W_p = \phi^p(0) \equiv 0 \pmod{p}$, so $p \in P_{d,c}$. □

Proof of Theorem 1.7. Let d be even. We show that if p is an odd prime, then $p \in P_{d,c}$ only if $p \mid c$.

Suppose that $p \in P_{d,c}$. Then $p \mid W_p$, and the period of 0 modulo p is a divisor of p. If the period of 0 is 1, then $p \mid W_1 = c$. Otherwise if the period of 0 is p, then 0 has a unique preimage modulo p. In particular, $\sqrt[d]{-c} \equiv -\sqrt[d]{-c} \pmod{p}$. Therefore $\sqrt[d]{-c} \equiv 0 \pmod{p}$, so $c \equiv 0 \pmod{p}$. □

In conjunction with Theorem 1.6, Theorem 1.7 provides a full characterization for $P_{d,c}$ when d is even. In particular, we can now prove Theorem 1.1.

Proof of Theorem 1.1. For c odd, the orbit of 0 has period 2. For c even, the orbit of 0 has period 1. When $p \mid c$, the orbit of 0 has period 1. □

3. Cardinality of $D_{d,c}$

In this section, we prove Theorem 1.4, which identifies all pairs (d, c) for which $D_{d,c}$ is finite. First, we note some simple infinite cases where $D_{d,c}$ is explicit.

Lemma 3.1.

(1) *For all d, $D_{d,0}$ is the set of positive integers.*
(2) *If d is even, then $D_{d,-1}$ is the set of even positive integers.*

Proof. If $c = 0$, then $W_n = 0$ for all n. When $c = -1$, then

$$W_n = \begin{cases} 0 & \text{if } n \text{ is even} \\ -1 & \text{if } n \text{ is odd.} \end{cases}$$

In both cases, the result is immediate. □

We now provide a simple yet sufficient condition for $D_{d,c}$ to be infinite.

Lemma 3.2. *If there exists $n \in D_{d,c}$ such that $n \geq 3$, then $D_{d,c}$ is infinite.*

Proof. Suppose that $n \in D_{d,c}$ for some $n \geq 3$. From [9], W_n contains a primitive prime divisor p. Therefore, 0 is periodic modulo p, with some period $r \leq p$. Therefore $p \mid W_r$, and primitivity then ensures that $n \leq r \leq p$. Hence either $p = n$, or p and n are coprime. If the latter holds, then, by Theorem 1.5, there is an edge of type 2: (n, np). This implies that n is not the largest element of $D_{d,c}$. Therefore it suffices to consider the case $p = n$.

First, suppose that d is even and $p = n$. Then, by Theorem 1.7, we have $p \mid c$, so that $p \mid W_n$ for all n. This contradicts primitivity, so d must be odd.

Therefore, suppose that d is odd and $p = n$. In this case, write $W_p = pm$ for some integer m. If $|m| > 1$, then for each prime divisor q of m, the index divisibility graph contains the edge (p, pq), hence p is not the largest element of $D_{d,c}$.

Thus we are left considering the case d is odd, $p = n$, and $W_p \in \{0, \pm p\}$. However, we claim that this is not possible, by the growth of W_n. For, since d is odd, the signs of W_n, W_n^d, and c are all the same by induction. This implies that $|W_{n+1}| = |W_n^d + c| = |W_n^d| + |c| \geq |W_n|^d$. In particular, since $|W_2| \geq 2$, we have $|W_n| > 2^{d^{n-2}}$. (Here we use that $|c| \geq 1$. The case $c = 0$ is covered by Lemma 3.1.) This rules out $|W_p| \leq p$ for any $p \geq 3$. □

Consequently, $D_{d,c}$ is infinite in most cases.

Proof of Theorem 1.4. By Theorem 1.6, $c \in D_{d,c}$, hence it follows from Lemma 3.2 that $D_{d,c}$ is infinite whenever $|c| \geq 3$. Similarly, if d is odd, then $3 \in P_{d,c}$ by Theorem 1.6, and again $D_{d,c}$ is infinite.

For the remainder of the proof, assume that d is even. The cases $c = 0$ and $c = -1$ are handled by Lemma 3.1, leaving only the cases $c = 1$ and $c = -2$ to consider.

Suppose $c = 1$. In this case $W_1 = 1$ and $W_2 = 2$, and by Theorem 1.7, we have $P_{d,1} = \{2\}$. Following the construction of the index divisibility graph, we have a single edge of type 2 emanating from the vertex 1 (the edge $(1, 2)$), and there are no edges emanating from the vertex 2. Thus $D_{d,1} = \{1, 2\}$.

Suppose $c = -2$. If $d = 2$, then $W_1 = -2$ and $W_2 = 2$. Similar to the previous case, the index divisibility graph only contains a single edge—the edge $(1, 2)$—and hence $D_{2,-2} = \{1, 2\}$.

Otherwise suppose $d \geq 4$. Then $W_2 = (-2)^d - 2 = -2((-2)^{d-1} + 1)$, where $|(-2)^{d-1} + 1| > 1$ and is odd. Hence W_2 has an odd prime divisor p, and therefore $(2, 2p)$ is an edge of type 1 in the index divisibility graph. Since $2p \in D_{d,-2}$, it follows that $D_{d,-2}$ is infinite. □

4. $S_{d,c}$ and p-cycles modulo p

In Theorem 1.6, we give a description of the set $P_{d,c}$. In the case that d is even, Theorem 1.7 concludes that Theorem 1.6 completely determines $P_{d,c}$. However, when d is odd, the conditions in Theorem 1.6 are insufficient to completely describe the set. This insufficiency is illustrated in Example 1.9 where we see that $11 \in P_{3,4}$, yet 11 does not satisfy any of the conditions in Theorem 1.6.

Suppose then that $p \in P_{d,c}$ where both p and d are odd. As we have previously noted, if $p \in P_{d,c}$, then the period of 0 in $\mathbb{Z}/p\mathbb{Z}$ is a divisor of p. If that period is 1, then $p \mid c$, which Theorem 1.6 already accounts for. Therefore, the primes that are the exceptions are the odd primes for which 0 has period p modulo p. In other words, the primes of interest are the odd primes p for which $x^d + c$ induces a single cycle of size p in $\mathbb{Z}/p\mathbb{Z}$.

It is well known that $\pi(x) = x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $\gcd(d, p - 1) = 1$. Hence under the same conditions, it follows that $x^d + c$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$. In particular, we have $\phi = \tau^c \circ \pi$ (over $\mathbb{Z}/p\mathbb{Z}$), where $\tau(x) = x + 1$. Since every p-cycle is an even permutation, we see that ϕ is a p-cycle only if π is an even permutation. Equivalently, if π is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$, then $p \notin P_{d,c}$.

We now use this observation to prove Theorem 1.3. For the remainder of this section, let $\operatorname{ord}_n m$ denote the order of m in $(\mathbb{Z}/n\mathbb{Z})^*$.

In order to understand the sign of π as a permutation, we consider its cycle structure, which is given thusly.

Lemma 4.1. *Suppose $\pi(x) = x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$. Then π has a cycle of length m if and only if there exists a divisor k of $p - 1$ such that $\operatorname{ord}_k d = m$. Moreover, the number of cycles N_m of length m satisfies*

$$mN_m = \sum_{i|m, i<m} iN_i.$$

Proof. See Lidl and Mullen [19, Theorem 1], as well as Ahmad [1, Theorem 1] for a more general statement. □

In particular, letting φ denote the Euler totient function, the theory of cyclic groups gives the following cycle structure.

Lemma 4.2. *Let p be prime, and suppose $\gcd(d, p-1) \neq 1$. Then $x \mapsto x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ with the following cycle structure:*

(1) 0 *is fixed, and*
(2) *for each divisor k of $p-1$, there are $\varphi(k)$ elements of $(\mathbb{Z}/p\mathbb{Z})^*$ of order $\operatorname{ord}_k d$, i.e., the permutation contains $\varphi(k)/(\operatorname{ord}_k d)$ cycles of length $\operatorname{ord}_k d$ for each divisor k of $p-1$.*

The following Lemma will also prove useful.

Lemma 4.3. *Let d be an odd integer, let $\mu = v_2(d-1)$, and let $\nu = v_2(d^2-1) - 1$ (i.e., $\nu = \max\{v_2(d-1), v_2(d+1)\}$). Then*

$$\operatorname{ord}_{2^k} d = \begin{cases} 1 & 0 \leq k \leq \mu \\ 2 & \mu < k \leq \nu \\ 2^{k-\nu} & \nu < k. \end{cases}$$

Proof. If $v_2(d-1) \geq k$, then $d \equiv 1 \pmod{2^k}$, hence $\operatorname{ord}_{2^k} d = 1$. If $v_2(d+1) \geq k > 1$, then $d \equiv -1 \pmod{2^k}$, hence $\operatorname{ord}_{2^k} = 2$. Otherwise $v_2(d^{2^j} - 1) = \nu + j$, and it follows that $2^{k-\nu}$ is the order of d. $\square$

Proof of Theorem 1.3. Let p be a prime where $p \equiv 1 \pmod 4$. We will show that $\pi(x) = x^d$ is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $d \equiv 3 \pmod 4$, which by the discussion at the start of this section is sufficient to prove the theorem. Moreover, we assume that $\gcd(d, p-1) = 1$, as this is both necessary and sufficient for π to be a permutation.

The cycle type of π is given in Lemma 4.2. Let $N_k = \varphi(k)/(\operatorname{ord}_k d)$ be the number of cycles of length $\operatorname{ord}_k d$ in π. Since a k-cycle is the product of $k-1$ transpositions, we see that π may be written as a product of the following number of transpositions:

$$\begin{aligned} \sum_{k|p-1} N_k((\operatorname{ord}_k d) - 1) &= \sum_{k|p-1} \varphi(k) - \sum_{k|p-1} N_k \\ &= p - 1 - \sum_{k|p-1} N_k. \end{aligned}$$

It now suffices to determine when $\sum_{k|p-1} N_k$ is odd.

To count the cycles, write $p - 1 = 2^\lambda \omega$, where ω is odd. Then

$$\sum_{k|p-1} N_k = \sum_{\delta|\omega} \sum_{0 \leq i \leq \lambda} N_{2^i \delta}.$$

Consider first the sum over $\delta > 1$; we will show that this is even. Using the same notation as in Lemma 4.3, let $\mu = v_2(d-1)$ and $\nu = v_2(d^2-1) - 1$.

Then for each δ, we have

$$\sum_{0\le i\le\lambda} N_{2^i\delta} = N_\delta + N_{2\delta} + \sum_{2\le i\le\mu} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d} + \sum_{\mu<i\le\nu} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d} + \sum_{\nu<i\le\lambda} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d}.$$

Note that $N_\delta + N_{2\delta} = 2N_\delta$ since

$$N_{2\delta} = \frac{\varphi(2\delta)}{\operatorname{lcm}(\operatorname{ord}_2 d, \operatorname{ord}_\delta d)} = \frac{\varphi(\delta)}{\operatorname{ord}_\delta d} = N_\delta.$$

Next, $\operatorname{ord}_{2^i\delta} d = \operatorname{lcm}(\operatorname{ord}_{2^i} d, \operatorname{ord}_\delta d)$ by the Chinese remainder theorem. Moreover, $\operatorname{ord}_\delta d \mid \varphi(\delta)$ because $\varphi(\delta) = \#(\mathbb{Z}/\delta\mathbb{Z})^*$, and $\operatorname{ord}_\delta d$ is the order of d in $(\mathbb{Z}/\delta\mathbb{Z})^*$. Hence

$$\sum_{2\le i\le\mu} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d} = \sum_{2\le i\le\mu} \frac{2^{i-1}\varphi(\delta)}{\operatorname{ord}_\delta d} \equiv 0 \pmod 2.$$

Now since $i \ge 2$,

$$\sum_{\mu<i\le\nu} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d} = \sum_{\mu<i\le\nu} \frac{2^{i-1}\varphi(\delta)}{\operatorname{lcm}(2, \operatorname{ord}_\delta d)} \equiv 0 \pmod 2,$$

and similarly,

$$\sum_{\nu<i\le\lambda} \frac{\varphi(2^i\delta)}{\operatorname{ord}_{2^i\delta} d} = \sum_{\nu<i\le\lambda} \frac{2^{i-1}\varphi(\delta)}{\operatorname{lcm}(2^{k-\nu}, \operatorname{ord}_\delta d)} \equiv 0 \pmod 2.$$

We conclude that the portion of the sum where $\delta > 1$ is even.

We are left to consider the contribution from $\delta = 1$. Here,

$$\begin{aligned}\sum_{0\le i\le\lambda} N_{2^i} &= \sum_{0\le i\le\lambda} \frac{\varphi(2^i)}{\operatorname{ord}_{2^i} d}\\ &= 2 + \sum_{2\le i\le\lambda} \frac{2^{i-1}}{\operatorname{ord}_{2^i} d}\\ &\equiv \begin{cases} 1 \pmod 2 & \text{if } v_2(d-1) = 1\\ 0 \pmod 2 & \text{otherwise.}\end{cases}\end{aligned}$$

Therefore, π is odd if and only if $d \equiv 3 \pmod 4$, concluding the proof. □

Corollary 4.4. *If $p \in P_{3^k,c}$ and k is odd, then either $p = 2$, $p \mid c$, or $p \equiv 11 \pmod{12}$.*

Proof. The cases $p = 2$ and $p \mid c$ are due to Theorem 1.6. Otherwise, if $p \in P_{3^k,c}$, k is odd, and $p \nmid c$, then $x^{3^k} + c$ is a cyclic permutation of $\mathbb{Z}/p\mathbb{Z}$, and hence $p \not\equiv 1 \pmod 3$. Finally, $p \not\equiv 5 \pmod{12}$ by Theorem 1.3. □

As evidenced in Example 1.9, primes $p \in P_{3^k,c}$ with $p \equiv 11 \pmod{12}$ do exist.

5. Fixed n and variable c, d

In this section, we investigate $D_{d,c}$ from a different perspective: for a fixed $n \in \mathbb{Z}$, in which $D_{d,c}$ does n appear? Let $H_n = \{(d, c) : n \in D_{d,c}\}$.

Proposition 5.1. *For any integers $d, c \in \mathbb{Z}$, where $d \geq 2$, we have the following.*

(1) *If $n \mid c$, then $(d, c) \in H_n$.*
(2) *If $d \equiv 1 \pmod{n-1}$ and n is prime, then $(d, c) \in H_n$.*
(3) *If $(d, c_0) \in H_n$, then $(d, c) \in H_n$ whenever $c \equiv c_0 \pmod n$. Additionally, if d is odd, then $(d, -c) \in H_n$ whenever $(d, c) \in H_n$.*

Proof. The first two properties are immediate from Theorem 1.6. For the third, set $\phi_c(x) = x^d + c$. If $c \equiv c_0 \pmod n$, then ϕ_c and ϕ_{c_0} are identical over $\mathbb{Z}/n\mathbb{Z}$. Hence $(d, c) \in H_n$ if and only if $(d, c_0) \in H_n$. Moreover, if d is odd, then $\phi_{-c}(x) = -\phi_c(-x)$. Thus if $\phi_c^n(0) \equiv 0 \pmod n$, then $\phi_{-c}^n(0) \equiv 0 \pmod n$. $\square$

Finally, we have a result regarding the powers of d when d is prime.

Theorem 5.2. *If d is prime, there exist d-adic integers $a_1, a_2, \ldots, a_{d-1}$, where $a_1 \equiv 1 \pmod d$, $a_2 \equiv 2 \pmod d, \ldots, a_{d-1} \equiv d-1 \pmod d$, such that if $c \equiv 0, a_1, a_2, \ldots, a_{d-1} \pmod{d^n}$, then $(d, c) \in H_{d^n}$.*

Proof. Let d be prime. From Theorem 1.6, we have $d \in D_{d,c}$ for all $c \in \mathbb{Z}$. In particular, $W_d \equiv 0 \pmod d$ for $c \equiv 0, 1, \ldots, d-1 \pmod d$. Considering W_d as a function in c (e.g. $W_d(c) = (\phi^{d-1}(0))^d + c$), we see that $\frac{d}{dc} W_d(c) \equiv 1 \pmod d$. Thus by Hensel's Lemma, each value modulo d lifts to a unique d-adic solution. Namely, if $a_0, a_1, a_2, \ldots, a_{d-1} \in \mathbb{Z}_d$ are these lifts (where $a_i \equiv i \pmod d$) and $c \equiv a_i \pmod{d^n}$ for one of these a_i, then $W_d(c) \equiv 0 \pmod{d^n}$. It now follows from rigid divisibility that if $d^n \mid W_d$, then $d^n \mid W_{d^n}$. It is straightforward to verify that $a_0 = 0$. $\square$

6. Heuristics and Experiment for the infinitude of $S_{d,c}$

In this section, we consider some data and heuristics to support Conjecture 1.2, that $S_{d,c}$ is infinite, particularly in the case that $d = 3$.

We will find it helpful to generalize the question by allowing both p and c to vary: we begin by considering the pairs (p, c) such that $p \in S_{3,c}$. In Figure 4, we plot all pairs $(p, c) \in [3, 37619] \times [1, p/2]$ for which $p \in S_{3,c}$. When d is odd, if $p \in S_{d,c}$, then $p \in S_{d,c'}$ for any $c' \equiv \pm c \pmod p$ (Proposition 5.1), hence the restriction to the interval $[1, p/2]$. In Corollary 4.4, we observed that for k odd, if $p \in P_{3^k,c}$, then $p = 2$, $p \mid c$ or else $p \equiv 11 \pmod{12}$. Therefore only primes $p \equiv 11 \pmod{12}$ may appear in this data.

The data indicates that these pairs occur somewhat frequently and that the pairs $(p, c/p)$ seem to be distributed randomly in the rectangle

$$[1, 37619] \times [0, 0.5].$$

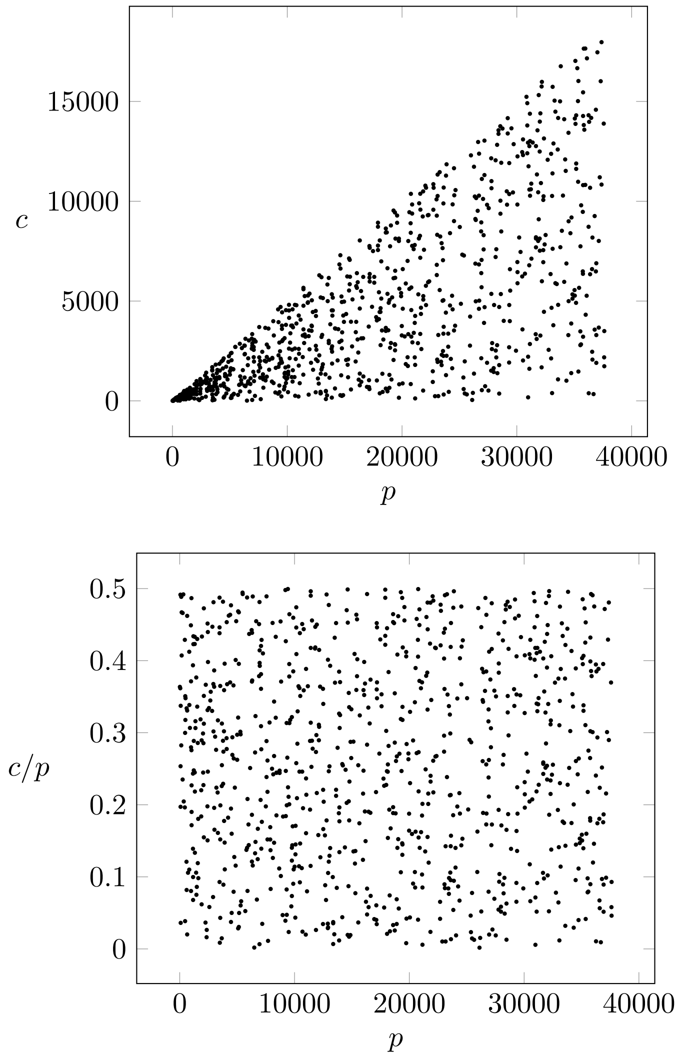

FIGURE 4. The graph on the top shows a scatterplot of pairs (p, c) such that $p \leq 37619$ is prime and $p \in S_{3,c}$. Below, the same scatterplot is scaled so that the pairs are of the form $(p, c/p)$. There are a total of 906 data points. There are 3986 primes ≤ 37619, of which 1000 are $11 \pmod{12}$.

Based on this observation, it seems reasonable to hypothesize that, at least for data in this range (i.e., $p \geq 2|c|$), the pair (p, c) is a Bernoulli random variable that occurs with a probability that is independent of c. Based on the existence of 906 data points for 1000 potential primes (i.e., those $11 \pmod{12}$ and ≤ 37619), we will also hypothesize the following: that, for a given prime $p \equiv 11 \pmod{12}$, there are on average 0.906 values of

$1 \le c \le (p-1)/2$ for which $p \in S_{3,c}$. Under these suppositions, we are led to the following heuristic assumption.

Hypothesis 6.1. *For any fixed c the probability that a prime $p \geq 2|c|$ satisfies $p \in S_{3,c}$ is $0.906 \cdot 2/(p-1)$.*

For small primes (those with $p < 2|c|$), we make no assumption on the behaviour. We remark, for example, that $p = 2, 3$ and $p = c$ have special behaviour, and otherwise the occurrence of (p, c) is determined by the occurrence of $(p, \pm c \bmod p)$ by Proposition 5.1.

Under this hypothesis, we may compute the expected number of pairs (p, c) in the data set for any given c. Namely, the expectation for the number of data points for any fixed c is

$$E_X(c) = \sum_{\substack{p \in [2|c|, X] \\ p \equiv 11 \bmod 12}} \frac{1.812}{p-1}.$$

In particular, $E_X(c) \to \infty$ as $X \to \infty$, which is the statement of Conjecture 1.2.

To test Hypothesis 6.1, the theoretical quantity $E_X(c)$ is compared to the actual count for our data ($X = 37619$) in Figure 5. The closeness of fit verifies that Hypothesis 6.1 is at least plausible, and gives some credence to Conjecture 1.2.

We make one more numerical experiment to verify the validity of Hypothesis 6.1. If it is indeed the case that all 906 pairs (p, c) are uniformly assigned to primes $p \equiv 11 \pmod{12}$, then a standard computation reveals that the expected number of primes which do not receive a pair is ≈ 403. Therefore, we should expect approximately 60% of the primes $p \equiv 11 \pmod{12}$ to have a corresponding c such that $p \in P_{3,c}$. In Figure 6, we see that, indeed, for approximately 60% of 11 (mod 12) primes, there exists a c for which $p \in P_{3,c}$.

We finish this section with a brief discussion of a relationship to certain polynomials arising in the study of portraits for post-critically finite polynomials. We will observe that, fixing p, the number of $1 \le c \le p-1$ for which $p \in S_{3,c}$ is the number of non-zero roots of a certain polynomial, as follows. Given a family of maps ϕ_c (for us, $\phi_c(x) = x^3 + c$), write $\Psi_{n,0}(c) \in \mathbb{Z}[c]$ for the polynomial whose roots are those c for which 0 has period n, i.e.,

$$\Psi_{n,0}(c) = \phi_c^n(0).$$

(In the case that $\phi_c(x) = x^2 + c$, these are sometimes called Gleason polynomials.) Then define $\Phi_{n,0}(c)$ so that

$$\Psi_{n,0} = \prod_{d|n} \Phi_{d,0}.$$

In particular, $\Phi_{n,0}$ has as roots those c such that 0 has formal period n under the map $x^3 + c$. (Our polynomials $\Psi_{n,0}(c)$ are specializations at $z = 0$

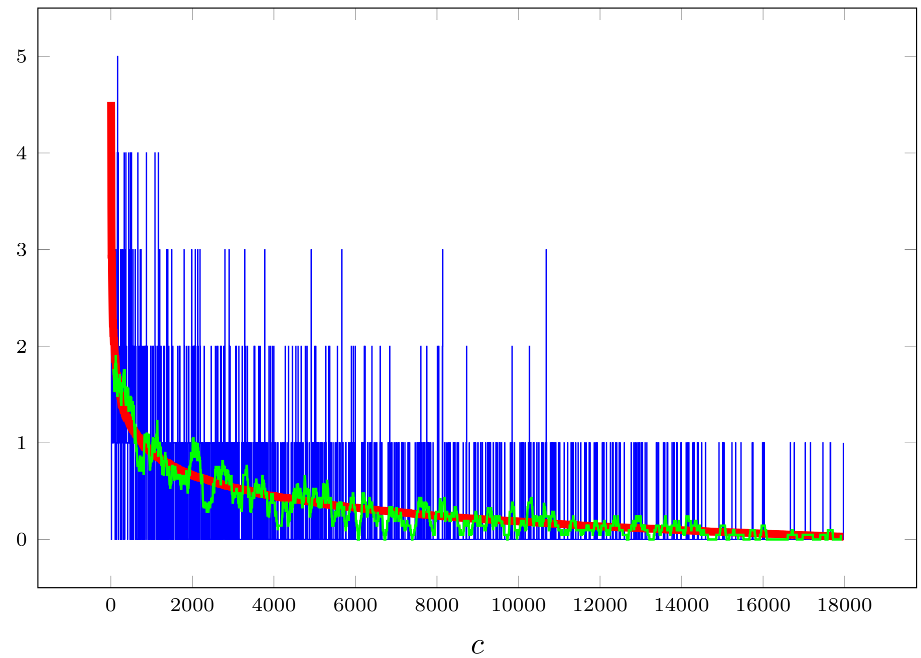

FIGURE 5. The data in Figure 4 is collected by c value in bins of size six. For each $k \in \mathbb{N}$, the value of the blue graph on the interval $[6(k-1), 6k)$ is the number of pairs (p, c) in the data for which $6(k-1) \leq c < 6k$. At each point x, the green line is the average of the blue function over the interval $(x - 60, x + 60)$. The red line is the theoretical expectation under the assumption that the data is random, i.e., it is the graph of $E_{37619}(x)$.

of the two-variable polynomial $\Psi_{n,z}(c) \in \mathbb{Z}[z, c]$, which is called the n-th dynatomic polynomial. Dynatomic curves are obtained by considering such polynomials; here we are taking the slice $z = 0$, allowing c to vary. For more on these standard definitions, see [26, Section 4.1–2].)

With this setup, for a fixed p, the number of $1 \leq c \leq p-1$ for which $p \in S_{3,c}$ is equal to the number of non-zero roots of $\Phi_{p,0}(c)$ modulo p. This raises an interesting general question.

Question 6.2. *As the integer n and prime p vary, what is the splitting behaviour of $\Phi_{n,0}(c)$ modulo p?*

These polynomials fall into a more general family of polynomials whose roots include the values of c for which 0 has a given finite portrait (i.e., a given preperiodic length, following by a given period). As 0 is the only critical point for $x^d + c$, the study of these polynomials is the study of $\phi_{c,d}$ which are post-critically finite; for example, in the case that 0 is strictly

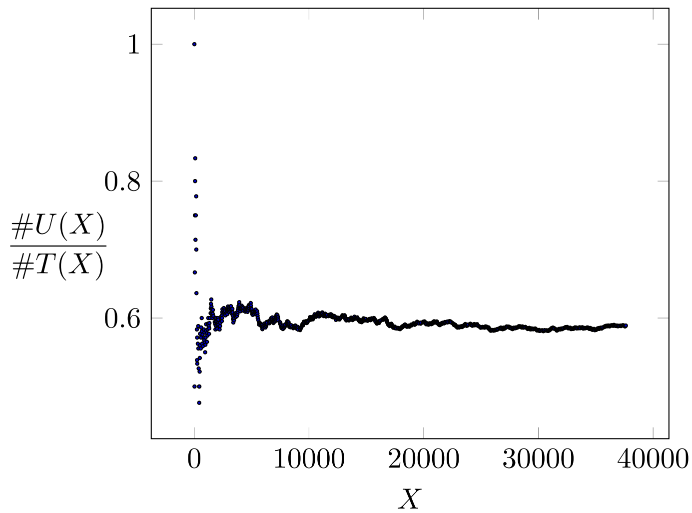

FIGURE 6. Let $T(X) = \{p \leq X : p \text{ prime}, p \equiv 11 \pmod{12}\}$ and $U(X) = \{p \in T(X) : p \in P_{3,c} \text{ for some } c\}$. The plot shows the ratio $\#U/\#T$ for $X \leq 37619$.

pre-periodic, the value c is called a *Misiurewicz point.* It is known that for $x^d + c$, the points c where 0 has a given portrait are the roots of a polynomial in $\mathbb{Z}[c]$, all of whose roots are simple [15, Theorem 1.1]. It is unknown if these polynomials are irreducible, or what their Galois groups are.

References

[1] Ahmad, Shair. Cycle structure of automorphisms of finite cyclic groups. *J. Combinatorial Theory* **6** (1969), 370–374. MR0240184, Zbl 0169.34101, doi: 10.1016/S0021-9800(69)80032-3.

[2] Alba González, Juan José; Luca, Florian; Pomerance, Carl; Shparlinski, Igor E. On numbers n dividing the nth term of a linear recurrence. *Proc. Edinb. Math. Soc.* (2) **55** (2012), no. 2, 271–289. MR2928495, Zbl 1262.11015, doi: 10.1017/S0013091510001355.

[3] André-Jeannin, Richard. Divisibility of generalized Fibonacci and Lucas numbers by their subscripts. *Fibonacci Quart.* **29** (1991), no. 4, 364–366. MR1131414, Zbl 0737.11003.

[4] Bang, A. S. Taltheoretiske undersøgelser. *Tidsskrift Mat.* **4** (1886), 70–80. `http://www.jstor.org/stable/24539988`.

[5] Benedetto, Robert L.; Ghioca, Dragos; Hutz, Benjamin; Kurlberg, Pär; Scanlon, Thomas; Tucker, Thomas J. Periods of rational maps modulo primes. *Math. Ann.* **355** (2013), no. 2, 637–660. MR3010142, Zbl 1317.37111, arXiv:1107.2816, doi: 10.1007/s00208-012-0799-8.

[6] Blum, Lenore; Blum, Manuel; Shub, Michael. A simple unpredictable pseudo-random number generator. *SIAM J. Comput.* **15** (1986), no. 2, 364–383. MR837589, Zbl 0602.65002, doi: 10.1137/0215025.

[7] Carmichael, Robert D. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math.* (2) **15** (1913/14), no. 1–4, 30–48. MR1502458, JFM 44.0216.01, doi: 10.2307/1967797.

[8] Chang, Mei-Chu. On periods modulo p in arithmetic dynamics. *C. R. Math. Acad. Sci. Paris* **353** (2015), no. 4, 283–285. MR3319121, Zbl 1323.37055, doi: 10.1016/j.crma.2015.01.007.

[9] Doerksen, Kevin; Haensch, Anna. Primitive prime divisors in zero orbits of polynomials. *Integers* **12** (2012), no. 3, 465–472. MR2955527, Zbl 1273.37045, arXiv:1009.3971, doi: 10.1515/integers-2011-0117.

[10] Faber, Xander; Granville, Andrew. Prime factors of dynamical sequences. *J. Reine Angew. Math.* **661** (2011), 189–214. MR2863906, Zbl 1290.11019, arXiv:0903.1344, doi: 10.1515/CRELLE.2011.081.

[11] Ghioca, Dragos; Nguyen, Khoa D.; Tucker, Thomas J. Squarefree doubly primitive divisors in dynamical sequences. Preprint, 2016. arXiv:1608.01361.

[12] Gottschlich, Avram. On positive integers n dividing the nth term of an elliptic divisibility sequence. *New York J. Math.* **18** (2012), 409–420. MR2928585, Zbl 1300.11059.

[13] Hamblen, Spencer; Jones, Rafe; Madhu, Kalyani. The density of primes in orbits of $z^d + c$. *Int. Math. Res. Not. IMRN* (2015), no. 7, 1924–1958. MR3335237, Zbl 06435176, arXiv:1303.6513, doi: 10.1093/imrn/rnt349.

[14] Hoggatt, Verner E., Jr.; Bergum, Gerald E. Divisibility and congruence relations. *Fibonacci Quart.* **12** (1974), 189–195. MR0349567, Zbl 0277.10012.

[15] Hutz, Benjamin; Towsley, Adam. Misiurewicz points for polynomial maps and transversality. *New York J. Math.* **21** (2015), 297–319. MR3358544, Zbl 06456673, arXiv:1309.4048.

[16] Ingram, Patrick; Silverman, Joseph H. Primitive divisors in arithmetic dynamics. *Math. Proc. Cambridge Philos. Soc.* **146** (2009), no. 2, 289–302. MR2475968 (2010a:11023), Zbl 1242.11012, arXiv:0707.2505, doi: 10.1017/S0305004108001795.

[17] Jarden, Dov. Divisibility of terms by subscripts in Fibonacci's sequence and associate sequence. *Riveon Lematematika* **13** (1959), 51–56. MR0130205.

[18] Jones, Rafe. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc.* (2) **78** (2008), no. 2, 523–544. MR2439638 (2010b:37239), Zbl 1193.37144, arXiv:math/0612415, doi: 10.1112/jlms/jdn034.

[19] Lidl, Rudolf; Mullen, Gary L. Cycle structure of Dickson permutation polynomials. *Math. J. Okayama Univ.* **33** (1991), 1–11. MR1159877, Zbl 0759.11044.

[20] Lucas, Edouard. Théorie des fonctions numériques simplement périodiques. *Amer. J. Math.* **1** (1878), no. 4, 289–321. MR1505176, JFM 10.0134.05, doi: 10.2307/2369308.

[21] Peinado, A.; Montoya, Fernando; Muñoz, Juan-Guillermo; Yuste, Antonio J. Maximal periods of $x^2 + c$ in $\mathbf{F}_q$. *Applied algebra, algebraic algorithms and error-correcting codes* (Melbourne, 2001), 2227. Lecture Notes in Comput. Sci., 219–228. *Springer-Verlag, Berlin*, 2001. MR2640521, Zbl 1053.11091.

[22] Pollard, John M. A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)* **15** (1975), no. 3, 331–334. MR0392798, Zbl 0312.10006, doi: 10.1007/BF01933667.

[23] Rice, Brian. Primitive prime divisors in polynomial arithmetic dynamics. *Integers* **7** (2007), A26, 16 pp. MR2312276 (2008e:11030), Zbl 1165.11028.

[24] Sanna, Carlo. On numbers n dividing the nth term of a Lucas sequence. *Int. J. Number Theory* **13** (2017), no. 3, 725–734. MR3606950, Zbl 06696676, doi: 10.1142/S1793042117500373.

[25] Silverman, Joseph H. Moduli spaces and arithmetic dynamics. CRM Monograph Series, 30. *Amer. Math. Soc., Providence, RI*, 2012. viii+140 pp. ISBN: 978-0-8218-7582-7. MR2884382, Zbl 1247.37004.

[26] Silverman, Joseph H. The arithmetic of dynamical systems. Graduate Texts in Mathematics, 241. *Springer, New York*, 2007. x+511 pp. ISBN: 978-0-387-69903-5. MR2316407, Zbl 1130.37001, doi: 10.1007/978-0-387-69904-2.

[27] Silverman, Joseph H. Variation of periods modulo p in arithmetic dynamics. *New York J. Math.* **14** (2008), 601–616. MR2448661, Zbl 1153.11028, arXiv:0707.1505.

[28] Silverman, Joseph H. Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture. *J. Number Theory* **133** (2013), no. 9, 2948–2963. MR3057058, Zbl 1297.37046, arXiv:1209.3491, doi: 10.1016/j.jnt.2013.03.005.

[29] Silverman, Joseph H.; Stange, Katherine E. Terms in elliptic divisibility sequences divisible by their indices. *Acta Arith.* **146** (2011), no. 4, 355–378. MR2747036, Zbl 1225.11079, arXiv:1001.5303, doi: 10.4064/aa146-4-4.

[30] Smyth, Chris. The terms in Lucas sequences divisible by their indices. *J. Integer Seq.* **13** (2010), no. 2, Article 10.2.4, 18 pp. MR2592551, Zbl 1210.11025, arXiv:0908.3832.

[31] Somer, Lawrence. Divisibility of terms in Lucas sequences by their subscripts. *Applications of Fibonacci numbers, Vol. 5* (St. Andrews, 1992), 515–525. *Kluwer Acad. Publ., Dordrecht*, 1993. MR1271392, Zbl 0806.11013.

[32] Somer, Lawrence. Divisibility of terms in Lucas sequences of the second kind by their subscripts. *Applications of Fibonacci numbers, Vol. 6* (Pullman, WA, 1994), 473–486. *Kluwer Acad. Publ., Dordrecht*, 1996. MR1393479, Zbl 0861.11010, doi: 10.1007/978-94-009-0223-7_39.

[33] Vasiga, Troy; Shallit, Jeffrey. On the iteration of certain quadratic maps over GF(p). *Discrete Math.* **277** (2004), no. 1–3, 219–240. MR2033734, Zbl 1045.11086, doi: 10.1016/S0012-365X(03)00158-4.

[34] Walsh, Gary. On integers n with the property $n \mid f_n$ (1986), 5 pp. Unpublished, 1986.

[35] Zsigmondy, Karl. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3** (1892), no. 1, 265–284. MR1546236, JFM 24.0176.02, doi: 10.1007/BF01692444.

(Annie S. Chen) Stanford University, 450 Serra Mall, Stanford, CA 94305
asc8@stanford.edu

(T. Alden Gassert) Hobart and William Smith Colleges, 300 Pulteney Drive, Geneva, NY 14456
gassert@hws.edu

(Katherine E. Stange) Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395
kstange@math.colorado.edu

This paper is available via http://nyjm.albany.edu/j/2017/23-45.html.