# INDEX DIVISIBILITY IN THE ORBIT OF 0 FOR INTEGRAL POLYNOMIALS

**T. Alden Gassert**
*Department of Mathematics and Computer Science, Hobart and William Smith Colleges, Geneva, New York*
gassert@hws.edu

**Michael T. Urbanski**
*Department of Mathematics, University of Connecticut, Storrs, Connecticut*
michael.urbanski@uconn.edu

*Received: 9/25/17, Revised: 12/25/19, Accepted: 2/6/20, Published: 2/14/20*

**Abstract**

Let $f(x) \in \mathbb{Z}[x]$ and consider the index divisibility set $D = \{n \in \mathbb{N} : n \mid f^n(0)\}$. We present a number of properties of $D$ in the case that $(f^n(0))_{n=1}^{\infty}$ is a rigid divisibility sequence, generalizing a number of results of Chen, Stange, and the first author. We then study the polynomial $x^d + x^e + c \in \mathbb{Z}[x]$, where $d > e \geq 2$ and determine all cases where this map has a finite index divisibility set.

## 1. Introduction

Let $f(x) \in \mathbb{Z}[x]$, and consider the orbit of 0 under iteration by this function:

$$(f^n(0)) = (f^n(0))_{n=1}^{\infty} = (f(0), f^2(0), f^3(0), \ldots).$$

Here $f^n(x)$ denotes the $n$-fold composition of $f$ with itself, and we also set $f^0(x) = x$. If this sequence is unbounded, then 0 is a *wandering point*. Otherwise 0 is *preperiodic*, and there exist integers $m \geq 1$ and $n \geq 0$ such that $f^{m+n}(0) = f^n(0)$. If $n = 0$, then 0 is *periodic*, and the smallest positive integer $m$ for which $f^m(0) = 0$ is the *exact period* of 0.

In this dynamical setting, the orbit of 0 is a *divisibility sequence*. That is, $f^m(0) \mid f^n(0)$ whenever $m \mid n$. If $f(x)$ has no linear term (i.e. its linear coefficient is 0) and 0 is a wandering point, then $(f^n(0))$ is a *superrigid divisibility sequence* [15, Proposition 3.2]. However, in this paper, we will only make use of the weaker condition that $(f^n(0))$ is a *rigid divisibility sequence*. A divisibility sequence $(a_n)$ is a rigid divisibility sequence if it satisfies the following properties.

1. If $v_p(a_n) \geq 1$, then $v_p(a_{nk}) = v_p(a_n)$ for all $k \geq 1$.

2. If $v_p(a_n) \geq 1$ and $v_p(a_m) \geq 1$, then $v_p(a_n) = v_p(a_m) = v_p(a_{\gcd(n,m)})$.

Here, $v_p(n)$ denotes the $p$-adic valuation of $n$.

Given any sequence, it is natural to ask if the position of a value in the sequence reveals any information about the value itself. In our case, we focus on the terms that are multiples of their indices. These terms are captured by the *index divisibility set*

$$D = D(f) = \{n \in \mathbb{N} : n \mid f^n(0)\},$$

where $\mathbb{N}$ is the set of positive integers.

Historically, index divisibility has been studied in a variety of contexts. For example, if $f(x) = a(x + a) - a$, then $f^n(0) = a^n - a$, and the question of index divisibility is analogous to the Fermat primality test. Namely, if $n \nmid f^n(0)$, then $n$ is composite. Otherwise if $n$ is relatively prime to $a$ and $n \mid f^n(0)$, then either $n$ is prime, or $n$ is a *pseudoprime to base a*. As another example, if one takes $f(x) = (x - 1)^2 + 1$, then $f^n(a + 1) = a^{2^n} + 1$ is a generalized Fermat number, with $a = 2$ being the original case studied by Fermat. The literature on index divisibility in Fibonacci and Lucas numbers (which are divisibility sequences) is extensive—see [2, 8, 11, 16, 20, 21] as a sampling—and for general linear recurrences, see [1]. Silverman and Stange [19] and Gottschlich [6] have studied this question for elliptic divisibility sequences, and Kim [12] considers the case where the $n$-th term in an elliptic divisibility sequence shares a fixed gcd with $n$. In the dynamical setting, the index divisibility set for the polynomial $x^d + c \in \mathbb{Z}[x]$ was analyzed by Chen, Stange, and the first author [3].

In [3], the authors describe a graph whose vertex set is exactly the divisibility set for $f(x) = x^d + c$. This *index divisibility graph* $G$ is constructed iteratively as follows. Start with 1 as a vertex in $G$. Then build out the rest of the graph by continuously looping through the vertices of $G$ and applying the rule: for each vertex $n$ in $G$ and each prime $p$, extend the graph by adding the vertex $np$ and the directed edge $(n, np)$ if either

1. $v_p(n) < v_p(f^n(0))$ (in which case $(n, np)$ is a *type 1* edge), or
2. $v_p(n) = 0$ and $p \in D$ (and $(n, np)$ is a *type 2* edge).

We note that given any function $f$, such a graph may be constructed, and that leads us to the following generalization of [3, Theorem 1.5].

**Theorem 1.** *Let $f(x) \in \mathbb{Z}[x]$ and suppose $(f^n(0))$ is a rigid divisibility sequence. Let $D$ be its divisibility set and $G_V$ be the vertex set of its index divisibility graph. Then $G_V = D$.*

A proof of this theorem is given in Section 2 along with generalizations of other statements from [3].

**Remark.** The index divisibility graph is a rooted directed graph with the vertex 1 as its root. We expect that the graph is infinite in most cases. The edge types in the index divisibility graph are not mutually exclusive. That is to say that there may be edges which are both type 1 and type 2. The outdegree of each vertex depends on the number of primes in $D$ and hence may be finite or infinite.

In Section 3, we study the trinomial $f(x) = x^d + x^e + c \in \mathbb{Z}[x]$, where $d > e \geq 2$, and its divisibility set $D_{d,e,c}$. In particular, we determine all cases where this set is finite.

**Theorem 2.** *The divisibility set $D_{d,e,c}$ is finite if and only if $c \in \{1, -1\}$. Moreover, $D_{d,e,\pm 1} = \{1\}$.*

Given a sequence $(a_n)$, a prime $p$ is a *primitive prime divisor* of $a_n$ if $p \mid a_n$ and $p \nmid a_k$ for all $1 \leq k < n$. The terms in the sequence that do not have primitive prime divisors form the *Zsigmondy set* of $(a_n)$:

$$Z((a_n)) = \{n \in \mathbb{N} : a_n \text{ has no primitive prime divisors}\}.$$

In the construction of a divisibility graph, the main sources of edges emanating from a vertex $n$ are the primitive prime divisors of $f^n(0)$. Hence part of our strategy for proving Theorem 2 is to show that the divisibility set $D_{d,e,c}$ is contained in the Zsigmondy set of $(f^n(0))$ as this significantly restricts the potential for the divisibility set to be large. We compute the Zsigmondy set of $f(x) = x^d + x^e + c$ explicitly in Proposition 6. Our proof is modeled after the argument of Doerksen and Haensch [4], who computed the Zsigmondy set for $x^d + c$. It was already known to Rice that the Zsigmondy set for $x^d + x^e + c$ would be finite [15, Theorem 1.2], and since then the finiteness of Zsigmondy sets has been established in more general contexts [7, 10, 18].

In the final section of the paper, we consider the primes in $D_{d,e,c}$. For a prime $p$ to be in the divisibility set, it must be that 0 is periodic modulo $p$, and that the period of 0 is a divisor of $p$. That is, either 0 is fixed, in which case $p \mid c$, or the period of 0 is $p$, in which case $f(x)$ is a cyclic permutation of $\mathbb{Z}/p\mathbb{Z}$. Therefore the primes of most interest are those for which $f$ is a permutation polynomial with a prescribed cycle type. For a survey of results on permutation polynomials, see Hou [9], and see [5, 13, 17] for more on cycle structures of polynomials over finite fields.

In general it is difficult to guarantee the existence of specific primes in the index divisibility set. For the map $x^d + x^e + c$, we find that if either $d$ or $e$ is even, then the only primes in $D_{d,e,c}$ are those dividing $c$ (Proposition 4). When both $d$ and $e$ are odd, it is not uncommon for $D_{d,e,c}$ to contain other primes. In this case, we give conditions that would prevent primes from being in the divisibility set.

## 2. Properties of the Divisibility Set

In this section we identify properties of the index divisibility set for the polynomial $f(x) \in \mathbb{Z}[x]$. We then prove Theorem 1, showing that the divisibility graph defined in [3] yields the divisibility set for any $f(x) \in \mathbb{Z}[x]$ where $(f^n(0))$ is a rigid divisibility sequence. A number of these statements are more general versions of statements found in [3], and for the most part, few changes are needed to adapt the arguments for our purposes. We finish this section with a discussion on the divisibility graph in the case that $(f^n(0))$ is not a rigid divisibility sequence.

**Proposition 1.** *Suppose $f(x) \in \mathbb{Z}[x]$, and let $D$ be its index divisibility set.*

1. *If $n \mid f(0)$, then $n \in D$.*
2. *If $f(x)$ is an even function, then the only primes in $D$ are the primes dividing $f(0)$.*
3. *If $n \in D$ and $v_p(n) < v_p(f^n(0))$, then $np \in D$.*
4. *If $m, n \in D$ and $\gcd(m, n) = 1$, then $mn \in D$.*
5. *Suppose $m, n \in D$ and $m \mid n$. Let $p$ be the smallest prime divisor of $n/m$. If $p \nmid m$, then $mp \in D$. In particular, if $n \in D$ and $p$ is the smallest prime divisor of $n$, then $p \in D$.*

*Proof.* (1) Suppose that $n \mid f(0)$. Since $(f^n(0))$ is a divisibility sequence, it follows that $f(0) \mid f^n(0)$, and thus $n \mid f^n(0)$.

(2) Suppose $f(x)$ is even and $p \in D$. Necessarily, 0 is periodic modulo $p$, and its period divides $p$. If the period of 0 is 1, then $f(0) = c \equiv 0 \pmod{p}$, and hence $p \mid c$.

Otherwise, if the period of 0 is $p$, then $f(f^{p-1}(0)) \equiv 0 \pmod{p}$, where $f^{p-1}(0) \not\equiv 0 \pmod{p}$. However, since $f$ is even, it is also the case that $f(-f^{p-1}(0)) \equiv 0 \pmod{p}$. Therefore 0 has at least two preimages modulo $p$, and so the period of 0 is strictly less than $p$ (a contradiction).

(3) Suppose that $n \in D$ and $v_p(n) < v_p(f^n(0))$. Then $np \mid f^n(0)$. Since $(f^n(0))$ is a divisibility sequence, $f^n(0) \mid f^{np}(0)$, and hence $np \mid f^{np}(0)$. Therefore, $np \in D$.

(4) Suppose $m, n \in D$ and $\gcd(m, n) = 1$. Further assume $f^{mn}(0)$ is nonzero as otherwise the statement is trivial. Since $(f^n(0))$ is a divisibility sequence, we have that $f^m(0) \mid f^{mn}(0)$ and $f^n(0) \mid f^{mn}(0)$. Therefore, $m \mid f^{mn}(0)$ and $n \mid f^{mn}(0)$. Since $\gcd(m, n) = 1$ it follows that $mn \in D$.

(5) Suppose $m, n \in D$ and $m \mid n$. Let $p$ be the smallest prime divisor of $n/m$, and suppose $p \nmid m$. Since $p \mid n$ and $n \mid f^n(0)$, we have that 0 is periodic modulo $p$. Let $b$ denote the period of 0 modulo $p$. Note that $\gcd(b, n/m) \mid p$ since $\gcd(b, n/m)$ is a divisor of $n/m$ that is less than or equal to $p$. Therefore, $b$ is either a divisor of $m$ or a divisor of $p$. In the former case, $p \mid f^m(0)$. Therefore $v_p(m) = 0 < v_p(f^m(0))$,

and $mp \in D$ by part (3). In the latter case, it follows that $p \mid f^p(0)$, and hence $p \in D$. Thus $mp \in D$ by part (4) since $\gcd(m, p) = 1$. □

We now prove Theorem 1. For the benefit of the reader, we recall that the edges in the divisibility graph are all of the form $(n, np)$, where $p$ is prime. The edge is type 1 if $v_p(n) < v_p(f^n(0))$, and it is type 2 if $p \in D$ and $v_p(n) = 0$.

*Proof of Theorem 1.* We begin by showing that $G_V \subseteq D$. Certainly $1 \in D$, and it suffices to show that if $n \in D$ and $(n, np)$ is an edge in the divisibility graph, then $np \in D$.

Suppose that $n \in D$ and $(n, np)$ is an edge in the divisibility graph. If $(n, np)$ is type 1, then $v_p(f^n(0)) > v_p(n)$. Hence $np \in D$ by Proposition 1.(3). Otherwise $(n, np)$ is type 2, so $p \in D$ and $p \nmid n$. By Proposition 1.(4), $np \in D$.

To show $D \subseteq G_V$, it suffices to show that for each $n \in D$, the divisibility graph contains a path from 1 to $n$. Write $n = \prod_{i=1}^{k} p_i^{\beta_i}$ for the prime factorization of $n$, and order the primes so that $p_1 < p_2 < \cdots < p_k$.

Consider $m_j = \prod_{i=1}^{j-1} p_i^{\beta_i}$ for each $1 \leq j \leq k$, where we take $m_1 = 1$. If $m_j \in D$, then following the proof of Proposition 1.(5), either $p_j \mid f^{m_j}(0)$ or $p_j \in D$. If $m_j \in G_V$ and $p_j \mid f^{m_j}(0)$, then $(m_j, m_j p_j)$ is a type 1 edge. Otherwise if $m_j \in G_V$ and $p_j \in D$, then $(m_j, m_j p_j)$ is a type 2 edge.

Moreover, if $m_j \in G_V$, then $(m_j p_j^t, m_j p_j^{t+1})$ is a type 1 edge for $1 \leq t < \beta_j$ since

$$v_p(f^{m_j p_j^t}(0)) = v_p(f^n(0)) \geq \beta_j > t = v_p(m_j p_j^t).$$

Thus if $m_j \in G_V$, then $m_{j+1} \in G_V$. Since $m_1 \in G_V$, the divisibility graph contains a path from 1 to $n$. □

Consequently, we may expand our list of properties for the divisibility set in the case of rigid divisibility sequences.

**Proposition 2.** *Suppose $f \in \mathbb{Z}[x]$ and $(f^n(0))$ is a rigid divisibility sequence. Let $D$ be its index divisibility set.*

1. *If $m, n \in D$, $m \mid n$, and $p$ is the smallest prime divisor of $n/m$, then $mp \in D$.*
2. *If $n \in D$ and $p$ is the largest prime divisor of $n$, then $n/p \in D$.*

*Proof.* Part (1) differs from Proposition 1.(5) in that we allow for $p$ to divide $m$. If $p \mid m$, then by rigid divisibility, $v_p(f^m(0)) = v_p(f^n(0)) \geq v_p(n) > v_p(m)$. Thus $mp \in D$ by Proposition 1.(3). We note that if $(f^n(0))$ is only a divisibility sequence, then it may be that $v_p(f^m(0)) = v_p(f^{mp}(0))$, in which case $mp \nmid f^{mp}(0)$.

Part (2) comes directly from the construction of the path from 1 to $n$ in the proof of Theorem 1. Namely, if $p$ is the largest prime divisor of $n$, the edge $(n/p, n)$ is the last edge in the path. □

We also note that one may recover a divisibility graph directly from a divisibility set.

**Proposition 3.** *If $D$ is the divisibility set for a rigid divisibility sequence, then the associated divisibility graph has vertex set $G_V = D$ and edge set*

$$G_E = \{(m, n) : m, n \in D \text{ and } n/m \text{ is prime}\}.$$

*Proof.* Certainly $G_V = D$ and $G_E \subseteq \{(m, n) : m, n \in D \text{ and } n/m \text{ is prime}\}$. For the reverse inclusion, the argument is identical to the final paragraphs in the proof of Theorem 1. Briefly, suppose $m, n \in D$, and let $p = n/m$ be prime. If $p \nmid m$, then $(m, mp)$ is an edge of type 1 or type 2 depending on whether the period of 0 modulo $p$ divides $m$ or divides $p$. If $p \mid m$, then $(m, mp)$ is type 1. □

To conclude this section, we consider possibilities for the divisibility graph of $f(x) \in \mathbb{Z}[x]$ in the case that $(f^n(0))$ is not a rigid divisibility sequence. We point out that at a glance, the definition of the divisibility graph presented above seems inadequate for divisibility sequences. For instance, if one uses the definition above to construct the divisibility graph for the sequence of natural numbers $(1, 2, 3, \ldots)$, then one quickly finds that there are no type 1 edges and that the graph contains infinitely many components. If one uses Proposition 3 to define the divisibility graph, then the graph for the sequence of natural numbers will be connected. However, this too has its shortcomings. For one, what independence the graph had from $D$, it now loses. Nor does the statement in Proposition 3 guarantee that the graph is rooted, much less connected. That is, even if the graph is comprised of a single component, it may not be possible to reach every vertex in the graph from 1 via a sequence of directed edges.

Experimentally, however, the current definition of the divisibility graph appears to be robust. As a small survey, we computed

$$\{n \in \mathbb{N} : n \mid f^n(0) \text{ and } n \leq 5000\}$$

for the maps $x^3 + x + c$ and $x^4 + x + c$, where $c \in \{1, 2, 3, \ldots, 100\}$. We then constructed their divisibility graphs and verified that every edge in these graphs were either type 1 or type 2. This begs the following question.

**Question 3.** Does Theorem 1 apply to all $f(x) \in \mathbb{Z}[x]$? Otherwise, is there an $f(x) \in \mathbb{Z}[x]$ whose index divisibility set contains values $n$ and $np$, but $(n, np)$ is neither type 1 nor type 2?

Recalling Rice [15, Proposition 3.2], if $f\colon \mathbb{Z} \to \mathbb{Z}$ and $(f^n(0))$ is not a rigid divisibility sequence, then the coefficient of its linear term is nonzero. Writing $f(x) = x^2 g(x) + bx + c$ where $g(x) \in \mathbb{Z}[x]$, it is straightforward to verify that

$$f^n(0) = c^2 h(c) + c \sum_{i=0}^{n-1} b^i$$

for some $h(x) \in \mathbb{Z}[x]$. Note that for all primes $p$,

$$\sum_{i=0}^{p-1} b^i \equiv \begin{cases} 0 & \text{if } b \equiv 1 \pmod{p} \\ 1 & \text{otherwise.} \end{cases}$$

Thus for the primes dividing $c$, either $b \not\equiv 1 \pmod{p}$ and $v_p(f^n(0)) = v_p(c)$ for all $n \in \mathbb{N}$, or $b \equiv 1 \pmod{p}$ and $v_p(f^{np}(0)) > v_p(np)$ for all $n \in \mathbb{N}$. Therefore all the edges in the divisibility graph that result from primes dividing $c$ are type 1. The question is still open for primes that do not divide $c$.

## 3. The Polynomial $x^d + x^e + c$

In this section, we restrict our attention to the polynomial $f(x) = x^d + x^e + c \in \mathbb{Z}[x]$, where $d > e \geq 2$. We begin with a pair of propositions regarding primes in the index divisibility set for $f(x)$. We then turn to the topic of primitive primes divisors, and in Proposition 6, show that the Zsigmondy set for $f(x)$ is a subset of $\{1\}$. Following that, we determine all cases where the index divisibility set of $f(x)$ is finite, proving Theorem 2.

Throughout this section, we let $D_{d,e,c}$ denote the index divisibility set for $f(x) = x^d + x^e + c$, and for convenience, we set $O_{d,e,c} = (f^n(0))$ and $O^+_{d,e,c} = (|f^n(0)|)$.

**Proposition 4.** *If $d$ or $e$ is even and $p \in D_{d,e,c}$, then $p \mid c$.*

*Proof.* If $d$ and $e$ are both even, then $f(x)$ is an even function and Proposition 1.(2) applies.

In the case that exactly one of $d$ or $e$ is even, we have $f(-1) = f(0) = c$. Therefore, $c$ has two preimages in $\mathbb{Z}/p\mathbb{Z}$ for every prime $p$. Hence, 0 can not have period $p$ modulo $p$. Thus $p \in D_{d,e,c}$ only if 0 is fixed modulo $p$, i.e. $p \mid c$. □

**Corollary 1.** *If $d$ or $e$ is even, then every edge in the index divisibility graph associated to $f(x) = x^d + x^e + c$ is type 1.*

*Proof.* Suppose $(n, np)$ is a type 2 edge in the index divisibility graph for $f(x)$. Then $p \in D_{d,e,c}$ and $v_p(n) = 0$. If $d$ or $e$ is even, then by Proposition 4, $p \mid c$. Since $O_{d,e,c}$ is a divisibility sequence, $p \mid f^n(0)$. Therefore $v_p(f^n(0)) > v_p(n)$, and we have that $(n, np)$ is a type 1 edge. □

**Proposition 5.** *If $p \in D_{d,e,c}$, then $p \in D_{d+k_1(p-1),e+k_2(p-1),c}$ for all $k_1, k_2 \in \mathbb{Z}$, where $d + k_1(p-1) \geq 3$, and $e + k_2(p-1) \geq 2$.*

*Proof.* Let $p \in D_{d,e,c}$ and consider the polynomial $g(x) = x^{d+k_1(p-1)} + x^{e+k_2(p-1)} + c$. Then

$$\begin{aligned} g(x) &= x^{d+k_1(p-1)} + x^{e+k_2(p-1)} + c \\ &= x^d \cdot x^{k_1(p-1)} + x^e x^{k_2(p-1)} + c \\ &\equiv x^d + x^e + c \pmod{p}. \end{aligned}$$

So $g^p(0) \equiv f^p(0) \equiv 0 \pmod{p}$. Thus, $p \in D_{d+k_1(p-1),e+k_2(p-1),c}$. □

We now give several technical lemmas, which will be useful for determining the Zsigmondy set of $O_{d,e,c}$.

**Lemma 1.** *Let $f(x) = x^d + x^e + c$ such that $d > e \geq 2$ and $|c| > 1$. Then, $O^+_{d,e,c}$ is a strictly increasing sequence.*

*Proof.* Suppose $|c| > 1$ and $d > e \geq 2$. We proceed by induction. For the base case, we have $|f^2(0)| = |c^d + c^e + c| > |c|$ since $c^{d-1} + c^{e-1} + 1$ is an integer outside $\{-1, 0, 1\}$.

Now assume $|f^n(0)| > |c|$ for some $n$. We have

$$\begin{aligned} |f^{n+1}(0)| &= |(f^n(0))^d + (f^n(0))^e + c| \\ &\geq |f^n(0)|^e(|f^n(0)|^{d-e} - 1) - |c| \\ &> |f^n(0)|^e \\ &> |f^n(0)| \end{aligned}$$

since $|f^n(0)| > |c|$ and $|f^n(0)| \geq 3$. □

**Lemma 2.** *If $f(x) = x^d + x^e + c$ where $d > e \geq 2$, then either*

1. *0 is a wandering point and $O^+_{d,e,c}$ is a strictly increasing sequence, or*
2. *0 is a preperiodic point, which occurs exactly when*
   (a) *$c = 0$, or*
   (b) *$c = -1$ and either $d$ or $e$ is even.*

*Proof.* The case where $|c| > 1$ is precisely Lemma 1. In the case that $c = 1$, simple induction can be used to show that $O_{d,e,1}$ is an increasing sequence, and a similar argument applies in the case where $d$ and $e$ are both odd and $c = -1$. In fact, $O^+_{d,e,-1} = O_{d,e,1}$.

In the case that $c = 0$, it can easily be seen that $f(0) = 0$. Otherwise, let $c = -1$. If exactly one of $d$ and $e$ is even, then $f^2(0) = -1 = f(0)$. In the case when $d$ and $e$ are both even we find that $f^3(0) = 1 = f^2(0)$. □

Recall that if $a_n$ is a term in the sequence $(a_n)$, the primitive prime divisors of $a_n$ are the primes that do not divide $a_i$ for $1 \leq i < n$. Thus we may distinguish between the primitive and non-primitive primes of $a_n$ and write $a_n = P_n N_n$, where $P_n$ is the primitive part of $a_n$ and $N_n$ is the non-primitive part of $a_n$. That is, $P_n$ is a product of powers of primitive primes of $a_n$, and $N_n$ is a product of powers of non-primitive primes.

**Lemma 3.** *If $(a_n)$ is a rigid divisibility sequence, then*

$$N_n = \prod_{d|n, d\neq n} P_d.$$

*Proof.* See [4, Lemma 6]. □

The following result determines the Zsigmondy set for $f(x)$.

**Proposition 6.** *Let $f(x) = x^d + x^e + c$, where $d > e \geq 2$. If 0 is a wandering point, then*

1. *if $c = \pm 1$, $f^n(0)$ has a primitive prime divisor for all $n \geq 2$, and*
2. *if $c \neq \pm 1$, $f^n(0)$ has a primitive prime divisor for all $n \geq 1$.*

*Proof.* Assume 0 is a wandering point. By Lemma 2, we can eliminate cases where $c = -1$ and where $c = 0$ when either $d$ or $e$ is even. In all other cases, 0 is a wandering point.

Note that if $c = \pm 1$, then $f(0) = \pm 1$, in which case $f(0)$ does not have a primitive prime divisor. If $c \neq \pm 1$, then $f(0) = c$ has at least one primitive prime factor, namely any prime factor of $c$.

For $n = 2$ and $|c| \geq 1$, we have that

$$f^2(0) = c(c^{d-1} + c^{e-1} + 1).$$

From the proof of Lemma 2, the sequence $O^+_{d,e,c}$ is increasing, hence $|c^{d-1} + c^{e-1} + 1| > 1$. Therefore $f^2(0)$ has primitive prime divisors, namely any prime divisor of $c^{d-1} + c^{e-1} + 1$.

Now we proceed to show that $f^n(0)$ has a primitive prime divisor for all $n \geq 3$. Since $O^+_{d,e,c}$ is increasing, we have $|f^n(0)| \geq |f^2(0)| \geq 3$ when $n \geq 2$. We show that

$$\prod_{k=1}^{n-1} |f^k(0)| < |f^n(0)|$$

for $n \geq 2$ by induction. The case $n = 2$ is immediate. Assume the inequality holds for some $N \geq 2$. Then

$$|f^{N+1}(0)| = |(f^N(0))^d + (f^N(0))^e + c| > \frac{1}{3}|f^N(0)|^d \geq \prod_{k=1}^{N} |f^k(0)|$$

since $d \geq 3$, $|f^N(0)| \geq 3$, and the induction hypothesis.

Setting $|f^n(0)| = P_n \cdot N_n$ in accordance with Lemma 3, we see that

$$N_n = \prod_{d|n, d\neq n} P_d \leq \prod_{k=1}^{n-1} P_k \leq \prod_{k=1}^{n-1} |f^k(0)| < |f^n(0)|.$$

Hence we see that that $P_n > 1$, and thus $f^n(0)$ has a primitive prime divisor. □

We now prove that $D_{d,e,c}$ is finite if and only if $c = \pm 1$.

*Proof of Theorem 2.* In the forward direction we proceed by contradiction. Assume that $D_{d,e,c}$ is finite and $c \notin \{1, -1\}$. Let $M = \max D_{d,e,c}$. By Proposition 6, we know that every term in $O_{d,e,c}$ has a primitive prime divisor. Suppose that $p$ is a primitive prime divisor of $f^M(0)$. Since $p \mid f^M(0)$, it follows that the period of 0 modulo $p$ is $M$, and thus $M \leq p$. If $M < p$, then $v_p(f^M(0)) > v_p(M)$, and hence $Mp \in D_{d,e,c}$ by Proposition 1.(3). This is a contradiction to the maximality of $M$.

Now consider the case $p = M$. Since $p \mid f^p(0)$, write $f^p(0) = mp$ where $m \in \mathbb{Z}$. As a consequence of Lemma 1, $m > 1$, so there is some prime $q$ such that $q \mid m$. This means that $pq \mid f^p(0)$. Since $O_{d,e,c}$ is a divisibility sequence, $p \mid pq$ implies $f^p(0) \mid f^{pq}(0)$. Therefore $pq \mid f^{pq}(0)$. So $pq \in D_{d,e,c}$, which is a contradiction.

In the reverse direction we show that if $c \in \{1, -1\}$, then $D_{d,e,\pm 1}$ is finite. Our approach is to show that $D_{d,e,\pm 1}$ does not contain any primes. By Proposition 1.(5), this is sufficient to show that $D_{d,e,\pm 1} = \{1\}$ .

If $d$ or $e$ is even, then by Proposition 4 there are no primes in $D_{d,e,c}$ except the divisors of $c$. Since $c = \pm 1$, there are no primes in $D_{d,e,\pm 1}$.

When $d$ and $e$ are both odd and $c = 1$, then $f(-1) = -1$. Since $-1$ is a fixed point, 0 can not have period $p$ modulo any prime $p$. Therefore $D_{d,e,1}$ contains no primes.

When $d$ and $e$ are both odd and $c = -1$, a similar argument can be made. In this case 1 is a fixed point, and once again $D_{d,e,c}$ contains no primes. □

## 4. Restriction of Primes from the Divisibility Set

In this section, we provide conditions that would prevent primes from appearing in the index divisibility set of $f(x) = x^d + x^e + c$. By Proposition 4, we know that when $d$ and $e$ are both odd, the divisibility set $D_{d,e,c}$ may contain primes that do not divide $c$. Indeed, we find examples of this: $31 \in D_{13,3,5}$, $157 \in D_{107,3,60}$, $223 \in D_{77,3,74}$, among many others.

As stated several times previously, for a prime $p$ to be in the index divisibility set, either $p \mid c$ or 0 has period $p$ modulo $p$. In the latter case, the map $f(x)$ is a cyclic permutation of $\mathbb{Z}/p\mathbb{Z}$. The conditions that restrict primes from appearing

in a divisibility set result from showing that $f$ is not a cyclic permutation, either because it is not a permutation or because its permutation type is not a $p$-cycle. All the computations in this section are local and thus apply to any map that is congruent to $f(x)$ modulo $p$.

We also note that if $d \equiv e \pmod{p-1}$, then $x^d + x^e + c \equiv 2x^d + c \pmod{p}$. We treat this as a separate case later in the section.

### 4.1. The Case $d \not\equiv e \pmod{p-1}$

Let $D$ denote the index divisibility set for $f(x) \in \mathbb{Z}[x]$, and let $\mathrm{ord}_p(a)$ denote the multiplicative order $a$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

**Proposition 7.** *Suppose $f(x) \equiv x^d + x^e + c \pmod{p}$, where $0 < e < d < p$ and $p \nmid c$. Then $p \notin D$ if any of the following is true:*

1. *$d$ or $e$ is even;*
2. *$(p-1)/\gcd(d-e, p-1)$ is even;*
3. *$\mathrm{ord}_p(2) \nmid \gcd(d-e, p-1)$;*
4. *$\gcd(d-e, p-1) < \log_2(p)$.*

*Proof.* The first statement is effectively a restatement of Proposition 4.

For the next two cases, we recall that if $p \nmid c$, then $p \in D$ if and only if 0 is $p$-periodic modulo $p$ (that is, $f^p(0) \equiv 0 \pmod{p}$, and $f^k(0) \not\equiv 0 \pmod{p}$ for $1 \leq k < p$). In particular, if $f(x)$ is not injective, then $p \notin D$.

Since $f(x)$ is regarded as a map from $\mathbb{Z}/p\mathbb{Z}$ to itself, injectivity of $f$ is equivalent to surjectivity. By definition, this means $f(x) - a$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for every $a \in \mathbb{Z}/p\mathbb{Z}$. Since $a$ is arbitrary, this means $x^d + x + a$ has a root in $\mathbb{Z}/p\mathbb{Z}$ for every $a \in \mathbb{Z}/p\mathbb{Z}$. The case $a = 0$ is immediate, hence injectivity of $f$ is equivalent to $\mathrm{Res}(x^d + x^e + a, x^{p-1} - 1) \equiv 0 \pmod{p}$ for every $a \in (\mathbb{Z}/p\mathbb{Z})^*$. By [14]Proposition 8.3, let $\zeta$ be a $(p-1)$-st primitive root of unity, the last equation is equivalent to:

$$\prod_{n=1}^{p-1} (\zeta^{nd} + \zeta^{ne} + a) \equiv 0 \pmod{p}$$

for every $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Since the left side of this equation is a monic polynomial in $\mathbb{Z}[a]$ of degree $p-1$, it has to be a congruent to $a^{p-1} - 1$ modulo $p$. Consequently, if the constant term of the expression on the left is not $-1$, then $f$ is not injective

modulo $p$. This constant term is

$$\prod_{n=1}^{p-1} \zeta^{dn} + \zeta^{en} = \prod_{n=1}^{p-1} \zeta^{en} \prod_{n=1}^{p-1} (\zeta^{(d-e)n} + 1)$$
$$= \left( \prod_{n=1}^{p-1} \zeta^n \right)^e \left( \prod_{n=1}^{(p-1)/k} (\zeta^{(d-e)n} + 1) \right)^k,$$

where $k = \gcd(d-e, p-1)$. Note that the first product is the product of the roots of $x^{p-1} - 1$, while the second is the product of the roots of $(x-1)^{(p-1)/k} - 1$, hence

$$\prod_{n=1}^{p-1} \zeta^n = -1 \quad \text{and} \quad \prod_{n=1}^{(p-1)/k} (\zeta^{(d-e)n} + 1) = \begin{cases} 0 & \text{if } (p-1)/k \text{ is even} \\ -2 & \text{if } (p-1)/k \text{ is odd.} \end{cases}$$

Since $e$ is odd, and $k$ is even when $(p-1)/k$ is odd, we have

$$\left( \prod_{n=1}^{p-1} \zeta^n \right)^e \left( \prod_{n=1}^{(p-1)/k} (\zeta^{(d-e)n} + 1) \right)^k = \begin{cases} 0 & \text{if } (p-1)/k \text{ is even} \\ -2^k & \text{if } (p-1)/k \text{ is odd.} \end{cases} \tag{1}$$

Note that $-2^k \equiv -1 \pmod{p-1}$ if and only if $\mathrm{ord}_p(2) \mid k$. Thus if $(p-1)/k$ is even or $\mathrm{ord}_p(2) \nmid k$, then $\mathrm{Res}(f(x), x^{p-1} - 1) \not\equiv c^{p-1} - 1 \pmod{p}$. Therefore $f(x)$ is not injective and $p \notin D$.

Finally, we note that $\log_2(p) < \mathrm{ord}_p(2) \leq p-1$ and $2 \leq k < p-1$. Hence if $k < \log_2(p)$, then $\mathrm{ord}_p(2) \nmid k$, and so $p \notin D$. While this statement only takes advantage of the trivial bounds for $\mathrm{ord}_2(p)$ and $k$, it does not require the exact value of $\mathrm{ord}_2(p)$. □

### 4.2. The Case $d \equiv e \pmod{p-1}$

In the case that $d \equiv e \pmod{p-1}$, we have $x^d + x^e + c \equiv 2x^d + c \pmod{p}$. We obtain a very simple condition in the case $d \equiv 1 \pmod{p-1}$.

**Proposition 8.** *If $f(x) \in \mathbb{Z}[x]$ and $f(x) \equiv ax + c \pmod{p}$, then $p \in D$ only if $a \equiv 1 \pmod{p}$ or $c \equiv 0 \pmod{p}$.*

*Proof.* A simple induction shows that

$$f^p(x) = a^p x + c \left( \sum_{i=0}^{p-1} a^i \right) \equiv \begin{cases} ax & \text{if } a \equiv 1 \pmod{p} \\ ax + c & \text{if } a \not\equiv 1 \pmod{p}. \end{cases}$$

The result follows immediately. □

Returning to the map $2x^d + c$, we note that $\tau(x) = x + 1$ and $\sigma(x) = 2x$ are permutations of $\mathbb{Z}/p\mathbb{Z}$, and the map $x^d$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $\gcd(d, p-1) = 1$. Therefore $f(x) = \tau^c \circ \sigma \circ \pi(x)$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $\gcd(d, p-1) = 1$. Moreover, cyclic permutations of $\mathbb{Z}/p\mathbb{Z}$ are even. Hence if $f(x)$ is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$, then $p$ is not in the divisibility set of $f(x)$.

**Lemma 4.** *If $p \equiv 1 \pmod 4$, then $x^d$ is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$ if and only if $d \equiv 3 \pmod 4$.*

*Proof.* See the proof of [3]Theorem 1.3. □

**Proposition 9.** *Suppose $f(x) \in \mathbb{Z}[x]$ and $f(x) \equiv ax^d + c \pmod p$, where $p \equiv 1 \pmod 4$, $d \equiv 3 \pmod 4$, and $\mathrm{ord}_p(a)$ is odd. Then $p \notin D$.*

*Proof.* The translation map $\tau(x) = x + 1$ is a cyclic permutation of $\mathbb{Z}/p\mathbb{Z}$ and is even. Since $\mathrm{ord}_p(a)$ is odd, the cycle $(a, a^2, a^3, \ldots, a^{\mathrm{ord}_p(a)})$ is an even permutation, hence the scaling map $\sigma(x) = ax$ is an even permutation. Finally, $\pi(x) = x^d$ is an odd permutation by Lemma 4. Thus $f(x)$ is an odd permutation of $\mathbb{Z}/p\mathbb{Z}$. □

For our polynomial $2x^d + c$, the conditions $p \equiv 1 \pmod 4$ and $\mathrm{ord}_p(2)$ is odd in Proposition 9, when taken together, are equivalent to $p \equiv 1 \pmod 8$. The reason for this is that 2 is not a quadratic residue if $p \equiv 5 \pmod 8$, and therefore the order of 2 is even. In particular, in order for $\mathrm{ord}_p(2)$ to be odd, it must be that 2 is a $2^v$-th power in $\mathbb{Z}/p\mathbb{Z}$, where $v = v_2(p-1)$. There are $(p-1)/2^v$ values which are $2^v$-th powers modulo $p$, so if $p \equiv 1 \pmod 8$ and we assume the heuristic that all values are equally likely to generate $(\mathbb{Z}/p\mathbb{Z})^*$ (c.f. Artin's conjecture), then the probability that 2 is a $2^v$-th power given that it is already a square is

$$\frac{(p-1)/2^v}{1/2} = \frac{1}{2^{v-1}}.$$

The primes that are congruent to 1 modulo 8 may be partitioned into sets of the form $p \equiv 2^{k-1} + 1 \pmod{2^k}$ for $k \geq 4$. As primes are distributed equally across equivalence classes, the proportion of primes satisfying $p \equiv 2^{k-1} + 1 \pmod{2^k}$ is $1/2^{k-1}$. Thus we expect that the proportion of all primes where $p \equiv 1 \pmod 8$ and $\mathrm{ord}_p(2)$ is odd to be

$$\sum_{k=4}^{\infty} \frac{1}{2^{k-1}} \cdot \frac{1}{2^{k-2}} = \frac{1}{24},$$

and therefore Proposition 9 is only sufficient to remove 1/24-th of all primes from consideration.

Given a sequence $(a_n)$, the rank of apparition function $t(x)$ gives the minimum value $n$ such that $x \mid a_n$. This function plays a key role in the study of Lucas

sequences [12] and elliptic divisibility sequences [16]. In our case, the rank of apparition is the period of 0 modulo $x$. It would be interesting to see if the methods of Sanna and Kim can be translated to the dynamical setting to give more concrete results regarding primes in index divisibility sets.

**Acknowledgements.** The authors thank the anonymous referee for many helpful comments and the suggestions for simplifying our arguments.

## References

[1] J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, On numbers $n$ dividing the $n$th term of a linear recurrence, *Proc. Edinb. Math. Soc. (2)* **55**, no. 2, (2012), 271–289.

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

[3] A. S. Chen, T. A. Gassert, and K. E. Stange, Index divisibility in dynamical sequences and cyclic orbits modulo $p$, *New York J. Math.* **23**, (2017), 1045–1063.

[4] K. Doerksen and A. Haensch, Primitive prime divisors in zero orbits of polynomials, *Integers* **12**, no. 3, (2012), 465–472.

[5] R. Flynn and D. Garton, Graph components and dynamics over finite fields, *Int. J. Number Theory* **10**, no. 3, (2014), 779–792.

[6] A. Gottschlich, On positive integers $n$ dividing the $n$th term of an elliptic divisibility sequence, *New York J. Math.* **18**, (2012), 409–420.

[7] C. Gratton, K. Nguyen, and T. J. Tucker, *ABC* implies primitive prime divisors in arithmetic dynamics, *Bull. Lond. Math. Soc.* **45**, no. 6, (2013), 1194–1208.

[8] V. E. Hoggatt Jr. and G. E. Bergum, Divisibility and congruence relations, *Fibonacci Quart.* **12**, (1974), 189–195.

[9] X.-d. Hou, Permutation polynomials over finite fields—a survey of recent advances, *Finite Fields Appl.* **32**, (2015), 82–119.

[10] P. Ingram and J. H. Silverman, Primitive divisors in arithmetic dynamics, *Math. Proc. Cambridge Philos. Soc.* **146**, no. 2, (2009), 289–302.

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

[12] S. Kim, The density of the terms in an elliptic divisibility sequence having a fixed G.C.D. with their index, *ArXiv e-prints*, (2017-08), arXiv:1708.08357.

[13] S. V. Konyagin, F. Luca, B. Mans, L. Mathieson, M. Sha, and I. E. Shparlinski, Functional graphs of polynomials over finite fields, *J. Combin. Theory Ser. B* **116**, (2016), 87–122.

[14] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[15] B. Rice, Primitive prime divisors in polynomial arithmetic dynamics, *Integers* **7**, (2007), A26, 16 pp.

[16] C. Sanna, On numbers $n$ dividing the $n$th term of a Lucas sequence, *Int. J. Number Theory* **13**, no. 3, (2017), 725–734.

[17] J. H. Silverman, Variation of periods modulo $p$ in arithmetic dynamics, *New York J. Math.* **14**, (2008), 601–616.

[18] J. H. Silverman, Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture, *J. Number Theory* **133**, no. 9, (2013), 2948–2963.

[19] J. H. Silverman and K. E. Stange, Terms in elliptic divisibility sequences divisible by their indices, *Acta Arith.* **146**, no. 4, (2011), 355–378.

[20] C. Smyth, The terms in Lucas sequences divisible by their indices, *J. Integer Seq.* **13**, no. 2, (2010), Article 10.2.4, 18 pp.

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