PRIMITIVE PRIME DIVISORS IN POLYNOMIAL ARITHMETIC DYNAMICS

Brian Rice
brice@hmc.edu

Received: 7/18/06, Revised: 4/10/07, Accepted: 4/20/07, Published: 5/22/07

Abstract

The question of which terms of a recurrence sequence fail to have primitive prime divisors has been significantly studied for several classes of linear recurrence sequences and for elliptic divisibility sequences. In this paper, we consider the question for sequences generated by the iteration of a polynomial. For two classes of polynomials $f(x) \in \mathbb{Z}[x]$ and initial values $a_1 \in \mathbb{Z}$, we show that the sequence (a_n) given by $a_{n+1} = f(a_n)$ for $n \geq 1$ has only finitely many terms which have no primitive prime divisor.

1. Introduction and Statement of Results

Given a sequence $(a_n) = (a_1, a_2, \dots)$ of integers, we say that a term a_n of the sequence has a *primitive prime divisor* if there exists a prime p such that $p | a_n$, but $p \nmid a_i$ for $i < n$. For a given sequence (a_n), we can ask a natural question: which terms of the sequence have primitive prime divisors?

This question has received a lot of attention in the case where (a_n) is a sequence generated by a binary linear recurrence $a_{n+2} = c_1 a_{n+1} + c_2 a_n$. Results going back to Zsigmondy [17] show that for a certain class of such sequences, including the Mersenne numbers $a_n = 2^n - 1$, every term in the sequence past the 6th must have a primitive prime divisor. Recently, the problem has been solved in its entirety for a class of second-order linear recurrence sequences known as Lucas sequences. The result, proved by Bilu, Hanrot, and Voutier in [4], is the culmination of years of work on the topic by a number of mathematicians, including Carmichael [7] and Schinzel [15].

These results, though very important, are far from the whole story. Even within linear recurrences, when one departs from Lucas sequences the situation can become very different. For example, in [9], Everest, Stevens, Tamsett, and Ward examine the problem for the sequences $a_n = n^2 + \beta$, which can be represented as ternary linear recurrences. They show, among other results, that infinitely many terms of (a_n) fail to have primitive prime divisors.

In the case of nonlinear recurrence sequences, however, only elliptic divisibility sequences (see [10, Chapter 10], and [8]) seem to have received any attention. In particular, the subject of primitive prime divisors in recurrence sequences generated by the iteration of nonlinear polynomials appears not to have been studied. The topic of the current paper is the simplest case of such sequences. We consider first-order polynomial recurrence sequences: those generated by iterating a polynomial $f \in \mathbb{Z}[x]$ of degree ≥ 2 on initial input $a_1 \in \mathbb{Z}$.

The material explored in this paper falls under the general category of arithmetic dynamics. In particular, the material in section 3 on rigid divisibility sequences is connected with questions about the topology of orbits in certain p-adic dynamical systems. For more information in this direction, see, for example, [11], [5], [6], [3], [2], and [1].

We use the following terminology throughout the paper: if f is a polynomial in x, and (a_n) satisfies $a_{n+1} = f(a_n)$ for $n \geq 1$, we say that (a_n) is the *sequence generated by f starting at a_1*, denoted by (f, a_1). A polynomial f has integer coefficients and (a_n) is integral unless stated otherwise.

In Section 2, we consider monic polynomials $f \in \mathbb{Z}[x]$ where $(f, 0)$ is finite. (That is, the orbit of 0 under f is preperiodic.) We prove the following theorem.

Theorem 1.1. *Suppose $f(x)$ is a monic polynomial of degree $d \geq 2$, such that $f(x) \neq x^d$ and $(f, 0)$ is finite. If $(a_n) = (f, a_1)$ is unbounded, then only finitely many terms of (a_n) do not have a primitive prime divisor.*

We also give stronger results for some explicit families of polynomials f; for example, we show that if $f(x) = x^2 - kx + k$, (f, a_1) is unbounded, and $4 \nmid v_p(k)$ for all $p|k$, then at most one term of (f, a_1) has no primitive prime divisor (we let v_p denote the p-adic valuation).

In Section 3, we consider sequences $(a_n) = (f, f(0))$ for monic $f \in \mathbb{Z}[x]$. An easy induction shows that such sequences satisfy $a_{n+k} \equiv a_k \pmod{a_n}$ and thus $\gcd(a_n, a_m) = a_{\gcd(m,n)}$ for all $m, n \in \mathbb{N}$. Such a sequence is known as a *strong divisibility sequence.* We call such a sequence a *rigid divisibility sequence* if, additionally, $a_n \neq 0$ for all n, and there is associated to each prime p an integer i_p such that $v_p(a_n) = i_p$ for all n such that $p|a_n$. We prove the following theorem.

Theorem 1.2. *Let $f(x)$ be a monic polynomial of degree ≥ 2. If $(a_n) = (f, f(0))$ is an unbounded rigid divisibility sequence, then only finitely many terms of (a_n) have no primitive prime divisor.*

We also give methods which allow us to prove that many polynomials f generate rigid divisibility sequences. For example, our methods allow us to show that if
$f(x) = x^3 + 3kx^2 + 3k^2x - k$ for some integer $|k| \geq 2$, then every term of $(f, -k)$ has a primitive prime divisor.

Remark: It follows from our methods that the set of n for which a_n has no primitive prime divisor is effectively computable when (a_n) satisfies the hypotheses of Theorem 1.1 or of Theorem 1.2. However, the method of computation is essentially brute force and is not of interest here.

Acknowledgments

The author would to thank Rafe Jones, Ken Ono, Jeremy Rouse, and an anonymous referee for helpful comments. Thanks also goes to the NSF for their generous funding of the REU at which the research for this paper took place.

2. Polynomials f for which $(f, 0)$ is Finite

2.1. Classification and General Results

In order to prove Theorem 1.1, we will first classify all possible $(f, 0)$ such that $(f, 0)$ is finite. Then, we will prove the theorem in several parts.

Proposition 2.1. *Let $f(x)$ be a monic polynomial such that $(f, 0)$ is finite. Then one of the following is true.*

i: *$f(0) = 0$, and $f(x) = xP(x)$ for some monic polynomial $P(x)$.*

ii: *$f(0) = k$ and $f(k) = 0$ for some nonzero $k \in \mathbb{Z}$, thus*
$f(x) = (x - k)[xP(x) - 1]$ for some monic $P(x)$.

iii: *$f(0) = k$ and $f(k) = k$ for some nonzero $k \in \mathbb{Z}$, thus*
$f(x) = (x - k)xP(x) + k$ for some monic $P(x)$.

iv: *$f(0) = 1$, $f(1) = k$, and $f(k) = 1$ for some nonzero $k \in \mathbb{Z}$, thus*
$f(x) = x(x - k)[(x - 1)P(x) - 1] + 1$ for some monic $P(x)$.

v: *$f(0) = -1$, $f(-1) = k$, and $f(k) = -1$ for some nonzero $k \in \mathbb{Z}$, thus*
$f(x) = x(x - k)[(x + 1)P(x) + 1] - 1$ for some monic (or zero) $P(x)$.

vi: *All iterates $f^n(0)$, $n \geq 1$, are ± 1 or ± 2.*

Proof. We first observe the following.

Lemma 2.2. *An integer, under iteration of a monic integer-coefficient polynomial, cannot belong to a cycle of length greater than two.*

Proof. This is a special case of Theorem 12.9 in [14]. □

Since $(f, 0)$ is finite, 0 must eventually be periodic. By Theorem 2 in [13], if $(f, 0)$ contains a cycle of length one, it contains at most three distinct terms, and if it contains a cycle of length two, it contains at most four distinct terms. Using these facts we can proceed to systematically characterize all polynomials f such that $(f, 0)$ is finite. Each of the possible cases can be analyzed with straightforward algebra; we only include one such case as an example as the others proceed similarly.

Suppose $f(0) = a$, $f(a) = b$, and $f(b) = a$, with $a \neq b$. In this case, 0 and b are both roots of $f(x) - a$, so $f(x) = x(x - b)P(x) + a$. Since $f(a) = b$, we substitute a into the equation to obtain $b = f(a) = a(a - b)P(a) + a$, or equivalently, $(b - a) = a(a - b)P(a)$. Since $a \neq b$, we obtain $-1 = aP(a)$, from which $a = \pm 1$ and $P(a) = -a$. Renaming b as k, we can write the polynomials given by these two cases. In the case $a = 1$,

$$f(x) = x(x - k)[(x - 1)Q(x) - 1] + 1$$

for a monic $Q(x)$, which gives case **iv**. In the case $a = -1$, we have

$$f(x) = x(x - k)[(x + 1)Q(x) + 1] - 1,$$

where $Q(x)$ is either 0 or a monic polynomial; this is case **v**. □

We may now begin to prove Theorem 1.1 for each of the cases of Proposition 2.1. We first do this for case **i**, then for case **ii**, and finally for cases **iii-vi** together. We then follow by giving explicit bounds on the number of terms in (a_n) with no primitive prime divisors for sequences generated by polynomials falling into each of the cases **iii-vi**.

In all that follows, we will use the standard notation $v_p(a)$ to mean the p-adic valuation of a; so that $p^{v_p(a)} \| a$.

Proposition 2.3. *Suppose that $f(x)$ satisfies **i** of Proposition 2.1, and that $f(x) \neq x^d$. If $(a_n) = (f, a_1)$ is unbounded, then only finitely many terms of (a_n) do not have a primitive prime divisor.*

Proof. Since $f(x) \neq x^d$, we may write $f(x) = x^k P(x)$, where $d > k \geq 1$ and $P(x) = \sum_{i=0}^{d-k} c_i x^i$ is a monic polynomial of degree $d - k$ such that $c_0 \neq 0$. Call $b = c_0$.

One important property of the polynomial f is that $a_k | f(a_k)$, so that $a_1 | a_2 | \cdots | a_n$ for all n. It therefore suffices to show that, for all but finitely many n, a_{n+1} has a prime factor which is not a prime factor of a_n. In particular, since $P(a_n) | a_{n+1}$, it suffices to show that $P(a_n)$ shares all its prime factors with a_n for only finitely many a_n.

Now suppose that $p | a_n$. Examining $P(a_n)$ modulo p, we see that $P(a_n) \equiv b \pmod{p}$, so it follows that if $p | P(a_n)$ as well, then $p | b$. Therefore, if $P(a_n)$ has all of its prime factors in common with a_n, it also has all of its prime factors in common with b. There are only two ways that this can happen: either $P(a_n)|b$, or $v_p(P(a_n)) > v_p(b)$ for some $p|b$. Since $|P(x)| > b$ for all but finitely many integers x, there are only finitely many x such that $P(x)$ is a divisor of b, so in particular there are only finitely many a_n such that $P(a_n)|b$.

We next show that, for each $p|b$, there is at most one a_n such that $v_p(a_n) > v_p(b)$. To do this, consider $v_p(a_i)$ as i increases. We have $v_p(a_{i+1}) = kv_p(a_i) + v_p(P(a_i)) \geq v_p(a_i)$, so that $v_p(a_i)$ is nondecreasing. Now suppose that $v_p(P(a_n)) > v_p(b)$. Then we have $v_p(a_m) \geq v_p(a_{n+1}) \geq v_p(P(a_n)) > v_p(b)$ for all $m > n$. Since $P(a_m) \equiv b \pmod{p^{v_p(a_m)}}$, it follows that $v_p(P(a_m)) = v_p(b)$. Thus, the first a_n such that $v_p(P(a_n)) > v_p(b)$ is also the last, and there is at most one such a_n for each p. In particular, this means that there are only finitely many a_n such that $v_p(P(a_n)) > v_p(b)$ for some $p|b$.

There are therefore only finitely many a_n such that $P(a_n)$ shares all of its prime factors with b, and thus only finitely many a_{n+1} such that $a_{n+1} = a_nP(a_n)$ shares all of its prime factors with a_n. It follows that only finitely many terms of (a_n) have no primitive prime divisor. □

Many interesting sequences are given by recursions of this form. For instance, the sequence $(x^2+x, 1)$ appears in the Online Encyclopedia of Integer Sequences ([16]), as A007018. The sequence $2^{2^n} - 1$ (A051179 in [16]) is also of this form, as it is $(x^2 + 2x, 1)$. For both of these, we can see, going through the above proof for the specific case, that every term past the first has a primitive prime divisor.

We now proceed to case **ii**, making use of Proposition 2.3 in the proof.

Proposition 2.4. *Suppose $f(x)$ falls into case **ii** in Proposition 2.1. If the sequence $(a_n) = (f, a_1)$ is unbounded, then only finitely many terms of (a_n) do not have a primitive prime divisor.*

Proof. Since $f(f(0)) = 0$, it follows that $f(f(x))$ falls into case **i** of Proposition 2.1. Since (a_{2n}) and (a_{2n-1}) are unbounded by hypothesis, it follows by Proposition 2.3 that the sequences (a_{2n}) and (a_{2n-1}), considered separately, each have only finitely many terms which are not primitive prime divisors. Furthermore, $a_1|a_3|\cdots|a_{2n-1}|\cdots$, and $a_2|a_4|\cdots|a_{2n}|\cdots$.

Now, let us consider $\gcd(a_{2r}, a_{2s-1})$. Suppose without loss of generality (the other case is identical) that $2r > 2s-1$. Then, since $a_{2s-1}|a_{2r-1}$, it follows that $\gcd(a_{2r}, a_{2s-1})|\gcd(a_{2r}, a_{2r-1})$. But since $f(0) = k$, we see that $a_{2r} = f(a_{2r-1}) \equiv k \pmod{a_{2r-1}}$. It follows that $\gcd(a_{2r}, a_{2r-1})|k$, and hence that $\gcd(a_{2r}, a_{2s-1})|k$, for any $r, s \geq 1$.

Now suppose that a_{2r}, considered as part of the sequence (a_{2n}), has a primitive prime divisor p. Then a_{2r}, considered as part of the sequence (a_n), can only fail to have a primitive prime divisor if $p|\gcd(a_{2r}, a_{2s-1})$ for some $s \leq r$. But by the above this can only happen if $p|k$, and since only finitely many primes divide k, there are only finitely many terms a_{2r} which have a primitive prime divisor considered as part of (a_{2n}), but fail to have one when considered as part of (a_n). The same follows for terms of the form a_{2s-1}. Since we know by the above that there are only finitely many terms in (a_{2n}) and in (a_{2n-1}) with no primitive prime divisor, the number of terms of (a_n) with no primitive prime divisor is finite, as required. □

One interesting sequence in this category is $(x^2-4x+3, 2) = 2, -1, 8, 35, \ldots$. The second and third terms (but no others) fail to have primitive prime divisors.

Proposition 2.5. *Suppose that $f(x)$ satisfies one of the cases* ***iii-vi*** *of Proposition 2.1. If the sequence $(a_n) = (f, a_1)$ is unbounded, then the number of terms of (a_n) which have no primitive prime divisor is finite.*

Proof. We begin by observing that $a_{n+1} = f(a_n) \equiv f(0) \pmod{a_n}$, and by induction, $a_{n+m} \equiv f^m(0) \pmod{a_n}$. It follows that $\gcd(a_{n+m}, a_n) | f^m(0)$. By hypothesis, $f^m(0)$ takes on only finitely many distinct values, and all of these values are nonzero. Letting c be the product of these distinct values, it follows that $\gcd(a_r, a_s) | c$ for all $r \neq s$. There are only finitely many n such that $a_n | c$, so consider a_n, having no primitive prime divisor, with $a_n \nmid c$. Since $\gcd(a_n, a_r) | c$ for all r, if a_n has no primitive prime divisor, then all of the primes dividing it must also divide c. Thus, since $a_n \nmid c$, there must be some prime p such that $v_p(a_n) > v_p(c) \geq 1$. Now since $\gcd(a_n, a_r) | c$ for all $r \neq n$, it follows that $v_p(a_r) \leq v_p(c)$ for all $r \neq n$. Hence, for each $p | c$, there is at most one n such that $v_p(a_n) > v_p(c)$. This means that the number of n for which $a_n \nmid c$ but a_n has no primitive prime divisor is bounded above by the number of prime factors of c, and is thus finite. Hence the total number of n such that a_n has no primitive prime divisor is finite, as required. □

Propositions 2.1, 2.3, 2.4, and 2.5 together comprise a proof of Theorem 1.1.

2.2. Stronger Bounds in Specific Cases

The proof of Proposition 2.5 suggests that in some cases we may be able to give better bounds than mere finiteness on the number of terms in (f, a_1) with no primitive prime divisor.

Proposition 2.6. *Suppose that $f(x)$ satisfies case* ***vi*** *in Proposition 2.1. If $(a_n) = (f, a_1)$ is unbounded, then at most two terms of (a_n) have no primitive prime divisor.*

Proof (sketch). In this case, $(f, 0)$ contains only the initial 0 and numbers from the set $\{\pm 1, \pm 2\}$. It follows that $\gcd(a_n, a_m) | 2$, so if a_n has no primitive prime divisor, then $a_n = \pm 2^k$ for some $k \geq 0$, and there can be at most one such a_n with $k > 1$. Considering each possible $(f, 0)$ separately (we leave the details to the reader), we see that in each case, if $\pm 2^k$ $(k > 1)$ occurs, it must be the first time 2 occurs as a divisor of some a_n, and so that term has a primitive prime divisor. Thus, the terms with no primitive prime divisors must be ± 1 or ± 2. However, similar casewise consideration shows that at most two of the numbers $\{\pm 1, \pm 2\}$ can occur in the sequence. □

One such sequence is $(x^2-2,3)$ (A001566 in [16]), in which the terms are in fact relatively prime (they are all odd and $\gcd(a_n,a_m)|2$ as noted above).

Though we cannot prove a constant bound for all polynomials falling under any one of the other cases of Proposition 2.1, we can still produce an explicit bound when $f(x)$ falls under one of the cases **iii-v** of Proposition 2.1.

Theorem 2.7. *Suppose that $f(x)$ falls under one of the cases **iii-v** of Proposition 2.1. The orbit of 0 in those cases depends on a parameter $k \neq 0$. If the sequence $(a_n) = (f, a_1)$ is unbounded, then the number of terms of (a_n) which have no primitive prime divisor is bounded above by $\log_2 |k| + 3$.*

Proof. By the same argument as in the proof of Proposition 2.5, we know $\gcd(a_n,a_m)|k$, and thus the number of n such that $a_n \nmid k$ but a_n has no primitive prime divisor is bounded above by the number of distinct prime factors of k. Let α be the number of distinct prime factors of k.

Now consider the n such that $a_n|k$. We have two cases: either $f(x)$ falls under case **iii**, or it falls under one of the cases **iv** or **v**. In the former case, we see from the characterization given in Proposition 2.1 that the linear coefficient of $f(x)$ is divisible by k, call it ck. Suppose that $p|k$ and $v_p(k) > v_p(a_n) = j > 0$; then $a_{n+1} = f(a_n) \equiv cka_n + k \equiv 0 \pmod{p^{j+1}}$, so that $v_p(a_{n+1}) \geq j+1 > v_p(a_n)$. Therefore, for each $0 < i < v_p(k)$, there is at most one $a_n|k$ such that $v_p(a_n) = i$.

The latter case proceeds similarly. From the characterization of the polynomials for cases **iv** and **v** given in Proposition 2.1 it follows that the linear coefficient of $f(f(x))$ must be divisible by k. It follows as in the previous paragraph that $v_p(a_{n+2}) \geq j+1 > v_p(a_n)$. Furthermore, if $p|k$ and $p|a_n$, we have by induction that $a_{n+2s+1} \equiv \pm 1 \pmod{p}$, and thus $p \nmid a_{n+2s+1}$, for $s \geq 0$. Thus, for each $0 < i < v_p(k)$, there is at most one n such that $v_p(a_n) = i$: if there is one of the form a_{2n}, there are none of the form a_{2n+1}, and vice-versa.

Furthermore, in all cases there are at most two $a_n|k$ such that $v_p(a_n) = 0$ for all $p|k$ (namely ± 1), and at most one $a_n|k$ such that $v_p(a_n) = v_p(k)$ for all $p|k$ (since k itself cannot be in an unbounded (f, a_1)). It follows that the number of n such that $a_n|k$ is at most

$$\left[\sum_{p|k}(v_p(k)-1)\right] + 3 = \left[\sum_{p|k} v_p(k)\right] - \alpha + 3 \leq \log_2 \left[\prod_{p|k} p^{v_p(k)}\right] - \alpha + 3 = \log_2 |k| - \alpha + 3.$$

Therefore, the total number of a_n which have no primitive prime divisor is bounded above by $\log_2 |k| + 3$, as required. □

We note that the bound $\log_2 |k| + 3$ can be reduced to $\log_2 |k| + 2$ by more detailed case analysis. It is doubtful, however, that this better bound is sharp either, and in any case such tightenings are less interesting than the much stronger result which can be obtained in the following special case.

Theorem 2.8. *Let $f(x) = x^2 - kx + k$, with $k \neq 0$, and suppose that $(a_n) = (f, a_1)$ is unbounded. For $n \geq 1$, let $B_n = \{p : v_2(v_p(k)) = n\}$, and for $n \geq 0$, define β_n by $\beta_0 = 0$ and $\beta_n = \min\{\beta_{n-1} + |B_n|, n\}$. Since $B_n = \emptyset$ for all sufficiently large n, we may define $\beta = \max \beta_n$. Then the number of terms of (a_n) with no primitive prime divisor is bounded above by $\max\{1, \beta\}$. In particular, this means that if $v_p(k)$ is not divisible by 4 for any $p|k$, then at most one term of (a_n) has no primitive prime divisor.*

We note that several well-known sequences fall into this class. Sylvester's sequence (number A000058 in [16]) is the sequence $(x^2 - x + 1, 2)$, while $(x^2 - 2x + 2, 3)$ is the sequence of Fermat numbers. It is not hard to see that these sequences, and in general all sequences in the family $(x^2 - kx + k, k + 1)$, have all terms coprime. Theorem 2.8 can be seen as a generalization that gives us partial results even when the starting point is changed. For instance, the sequence $(x^2 - 4x + 4, 6)$ begins $6, 16, 196, \cdots$, and the second term fails to have a primitive prime divisor. Theorem 2.8 tells us that this is the only such term in the sequence.

Proof. We begin with a lemma.

Lemma 2.9. *Let $n \geq 2$, and suppose that $a_n \nmid k$ but that a_n has no primitive prime divisor. Then there is some prime $p|k$ such that $v_p(k) = 2^{n-1}v_p(a_1)$.*

Proof. As in Theorem 2.7, $\gcd(a_n, a_m)|k$, so that if a_n has no primitive prime divisor, then a_n shares all its prime factors with k. Thus, if additionally $a_n \nmid k$, then $v_p(a_n) > v_p(k)$ for some prime $p|k$.

Now, suppose that $v_p(a_m) = i$, and $v_p(k) = j$. Write $a_m = c_a p^i$ and $k = c_k p^j$. Then

$$a_{m+1} = c_a^2 p^{2i} + c_a c_k p^{i+j} + c_k p^j. \tag{1}$$

If $2i < j$, we can factor out p^{2i} from (1) to obtain $v_p(a_{m+1}) = 2i$; similarly, if $2i > j$, we can factor out p^j to obtain $v_p(a_{m+1}) = j$. It follows that

$$v_p(a_{m+1}) > v_p(k) \text{ is only possible if } v_p(k) = 2v_p(a_m). \tag{2}$$

Additionally, we obtain by induction on m that

$$v_p(a_m) = 2^{m-1}v_p(a_1) \text{ provided that } v_p(a_m) < v_p(k). \tag{3}$$

Now suppose that $v_p(a_n) > v_p(k)$ for some $p|k$. Then by (2), $v_p(k) = 2v_p(a_{n-1})$. It follows that $v_p(a_{n-1}) < v_p(k)$, so by (3) we have $v_p(a_{n-1}) = 2^{n-2}v_p(a_1)$. Therefore, $v_p(k) = 2^{n-1}v_p(a_1)$ as required. □

We now return to the proof of Theorem 2.8. Since (a_n) is unbounded, $1 \notin (a_n)$. Hence if a_1 has no primitive prime divisor, then $a_1 = -1$, in which case it follows by induction on n that $v_p(a_n) = 0$ for all $p|k$. It follows that in this case, all other terms of (a_n) have a primitive prime divisor.

Straightforward computation reveals that $a_n > k$ for $n \geq 3$ and $\left|\frac{k}{a_2}\right| < 4$. If $a_2|k$ and a_n has no primitive prime divisor for some $n \geq 3$, then $a_n \nmid k$ and by Lemma 2.9,

$$v_p(k) = 2^{n-1}v_p(a_1) = 2^{n-2}v_p(a_2) \text{ for some prime } p|k. \tag{4}$$

Now $v_p(k) - v_p(a_2) \leq 1$ since $4 > \left|\frac{k}{a_2}\right| \in \mathbb{N}$, and $v_p(a_2) = 2v_p(a_1)$ is even if $v_p(a_2) < v_p(k)$, so (4) cannot hold for $n \geq 3$. It follows that if $a_2|k$, then a_n has a primitive prime divisor for $n \geq 3$.

Therefore, when either a_1 has no primitive prime divisor or $a_2|k$, the number of terms of (a_n) with no primitive prime divisor is at most 1. Now, suppose that neither of the above cases holds.

Define $A = \{n : a_n \text{ has no primitive prime divisor}\}$. Suppose that $n \in A$; then $n \geq 2$. Since $a_n \nmid k$, by Lemma 2.9 there is some prime $p|k$ such that $v_p(k) = 2^{n-1}v_p(a)$. For each $n \in A$, choose one such prime p_n. Then $v_2(v_{p_n}(k)) \geq n-1$, so that there is some $m \geq n-1$ such that $p_n \in B_m$.

Define $A_p = \{p_n : n \in A\}$. It follows that

$$A_p \subset \bigcup_{i=1}^{n} B_i \text{ for all sufficiently large } n. \tag{5}$$

Similarly,

$$\left|A_p \cap \bigcup_{i=1}^{n} B_i\right| \leq n, \tag{6}$$

since only p_2 through p_{n+1} could be in this intersection.

We therefore have $|A_p \cap B_1| \leq \min\{|B_1|, 1\} = \beta_1$, and by induction together with (6),

$$\left|A_p \cap \bigcup_{i=1}^{n} B_i\right| = \left|A_p \cap \bigcup_{i=1}^{n-1} B_i\right| + |A_p \cap B_n| \leq \min\{\beta_{n-1} + |B_n|, n\} = \beta_n. \tag{7}$$

By (5), there exists an n such that $A_p \cap \bigcup_{i=1}^{n} B_i = A_p$. It follows from this and (7) that

$$|A_p| = \left|A_p \cap \bigcup_{i=1}^{n} B_i\right| \leq \beta_n \leq \max_{n \geq 0} \beta_n = \beta. \tag{8}$$

Recall that (8) covers all cases except where $a_2|k$ or $1 \in A$; as noted above these other cases yield at most one a_n with no primitive prime divisor. Since $|A_p| = |A|$ is the number of terms of (a_n) with no primitive prime divisor, it follows that the number of such terms is bounded above by $\max\{1, \beta\}$ as required. □

A slight weakening of this result gives a bound which is easier to evaluate.

Corollary 2.10. *Let (a_n) be as in Theorem 2.8. Then the number of terms of (a_n) with no primitive prime divisor is bounded above by $\max\{1, \log_2 \log_2 |k|\}$.*

Proof. Write $m = \max\{n|B_n \neq \emptyset\}$. Then $\beta = \beta_m \leq m$. By definition of B_n,
$m = \max\limits_{p|k}\{v_2(v_p(k))\}$. It follows that $v_2(v_p(k)) \leq \log_2(v_p(k)) \leq \log_2 \log_2 |k|$, so
$m \leq \log_2 \log_2 |k|$. The result then follows by Theorem 2.8. □

3. Sequence Factorization and Rigid Divisibility Sequences

We now turn to another class of iterated polynomial recurrence sequences: those that are rigid divisibility sequences (see p. 2 for a definition). A special case of such sequences and a special case of the sequence factorization discussed in section 3.2 appear in section 5 of [12].

It turns out that it is often more convenient and useful to consider sequences satisfying a stronger condition than rigid divisibility. Accordingly, we say that a strong divisibility sequence (a_n) is a *superrigid divisibility sequence* if $a_n \neq 0$ for all n, and
$a_{cn+k} \equiv a_k \pmod{p^{v_p(a_n)+1}}$ for any integers $c, k \geq 1$ whenever $p|a_n$.

3.1. Basic Results on Rigid Divisibility Sequences

We begin by showing that all superrigid divisibility sequences are rigid divisibility sequences.

Proposition 3.1. *If (a_n) is a superrigid divisibility sequence, then (a_n) is also a rigid divisibility sequence.*

Proof. Let m be minimal such that the prime p divides a_m. Then, since (a_n) is a strong divisibility sequence, it follows that $p|a_n$ if and only if $m|n$. It therefore suffices to show that $v_p(a_{cm}) = v_p(a_m)$; we will then choose $i_p = v_p(a_m)$. Since (a_n) is a superrigid divisibility sequence, $a_{cm} \equiv a_m \pmod{p^{v_p(a_m)+1}}$, from which it follows that $v_p(a_{cm}) = v_p(a_m)$. This holds for all primes p dividing some element of the sequence, so (a_n) is a rigid divisibility sequence. □

Next, we exhibit a class of polynomials f such that $(f, f(0))$ is a superrigid divisibility sequence, and thus a rigid divisibility sequence.

Proposition 3.2. *Suppose that $f(x)$ is a monic polynomial with linear coefficient 0; i.e., $f(x) = x^2P(x) + k$. Let $(a_n) = (f, f(0))$, and suppose that $a_1, a_2 \neq 0$ (this always occurs if $|k| \geq 2$). Then (a_n) is a superrigid divisibility sequence.*

Proof. We first show that $a_n \neq 0$ for all n. By hypothesis, $a_1 = f(0)$ and $a_2 = f^2(0)$ are nonzero. Hence if $a_n = f^n(0) = 0$, then 0 is contained in a cycle of length greater than two. This is impossible by Lemma 2.2, so it follows that $a_n \neq 0$ for all n.

Now suppose that $p|a_n$ and write $v_p(a_n) = i \geq 1$. We can thus write $a_n = \ell p^i$ for some ℓ not divisible by p. Then $a_{n+1} = \ell^2 p^{2i} P(\ell p^i) + k \equiv k \equiv a_1 \pmod{p^{i+1}}$, since $i + 1 \leq 2i$. Inducting on m, we see that $a_{n+m} = f(a_{n+m-1}) \equiv f(a_{m-1}) \equiv a_m \pmod{p^{i+1}}$. In particular, choosing $m = (c-1)n + r$ gives $a_{cn+r} \equiv a_{(c-1)n+r} \equiv \cdots \equiv a_r \pmod{p^{i+1}}$. Since this holds for all n and all $p|a_n$, (a_n) is a superrigid divisibility sequence. □

We now prove our key result about rigid divisibility sequences, Theorem 1.2.

Proof of Theorem 1.2. We prove this theorem by showing that the sequence (a_n) eventually grows too quickly to be divisible only by primes occurring earlier. Suppose that a_n is a term with no primitive prime divisor. Then $p|a_n$ implies that $p|a_m$ for some $m < n$. Since (a_n) is a rigid divisibility sequence, this means that $v_p(a_n) = v_p(a_{\gcd(n,m)})$. Therefore, for any $p|a_n$, $v_p(a_n) = v_p(a_d)$ for some $d|n$. It follows that

$$a_n \mid \prod_{d|n,\ d<n} a_d. \tag{9}$$

We next prove a lemma.

Lemma 3.3. *Let $f(x)$ be a monic polynomial of degree ≥ 2, and suppose that $(a_n) = (f, a_1)$ is unbounded. Then there exists some positive integer N such that $|a_N| > |a_m|$ for all $m < N$, and for all $n > N$,*

$$|a_n| > \prod_{i=N}^{n-1} |a_i|. \tag{10}$$

Proof. It suffices to prove this lemma when $a_n \to +\infty$, as the proof in the case $a_n \to -\infty$ is identical.

Let r be the degree of $f(x)$ and b be the coefficient of x^{r-1} in $f(x)$. Choose some positive $c > -b$. Then there is some X such that for all $x > X$, $f(x) > x(x-c) + c$. Now, let N be minimal such that $a_N > X$, $a_N > c$, and $a_N > |a_m|$ for all $m < N$. We will show the stronger statement that

$$a_n > \left[\prod_{i=N}^{n-1} |a_i|\right] + c. \tag{11}$$

Certainly, $a_{N+1} = f(a_N) > a_N + c = |a_N| + c$, so the inequality (11) is true for $n = N + 1$. We now prove (11) by induction on n:

$$a_n > a_{n-1}(a_{n-1} - c) + c > a_{n-1}\left(\left[\prod_{i=N}^{n-2} |a_i|\right] + c - c\right) + c = \left[\prod_{i=N}^{n-1} |a_i|\right] + c.$$

Since (11) is strictly stronger than (10), this completes the proof of the lemma. □

Next, we note that if $d|n$ and $d < n$, then $d \leq \frac{n}{2}$. Let N be as in Lemma 3.3 and choose $n \geq 2N$. Then we have that

$$\prod_{d|n,\, d<n} |a_d| < \prod_{d|n,\, d<n} |a_{N+d-1}| < \prod_{i=N}^{n-1} |a_i| < |a_n|.$$

It follows that a_n cannot satisfy (9), so a_n must have a primitive prime divisor. Since this holds for all $n \geq 2N$, it follows that only finitely many terms of (a_n) have no primitive prime divisor, as required. □

It is worth noting why we proved Lemma 3.3 in above manner, rather than appealing to a general growth rate for sequences generated by iterating polynomials. (The growth rate is doubly exponential.) The reason is that the above proof can be easily adapted in special cases to yield bounds on the last term which could fail to have a primitive prime divisor – see, for instance, Corollaries 3.7 and 3.8 below. Appealing to a general growth rate result instead would make this adaptation more difficult.

There are some well-known rigid divisibility sequences, to which the above theorem applies. For instance, the sequence $(x^2 + 1, 1)$ (number A003095 in [16]) is a rigid divisiblity sequence by Proposition 3.2. Thus by the Theorem 1.2 it has only a finite number of terms with no primitive prime divisor. Indeed, every term but the first has a primitive prime divisor, as we can see by the argument above together with the fact that every term is strictly greater than the product of all the previous ones. (This fact is a stronger version of Lemma 3.3 for this sequence.)

3.2. Sequence Factorization

Theorem 1.2 shows that all rigid divisibility sequences have only finitely many terms a_n which fail to have a primitive prime divisor. While Proposition 3.2 gives one class of polynomials which generate rigid divisibility sequences, it by no means exhausts them. For this reason, as well as independent interest, we introduce the notion of *sequence factorization.*

Proposition 3.4. *Let $f(x)$ be a monic polynomial of degree $d \geq 2$, and let $(a_n) = (f, f(0))$. Let $f(x)$ have roots $r_1, \ldots, r_d$, not necessarily distinct and not necessarily integers. For each*

$1 \leq i \leq d$, *define* $f_i(x) = f(x + r_i) - r_i$, *and let* $(a_{i,n}) = (f_i, f_i(0))$. *Then for every* $n \geq 1$,

$$a_n = \prod_{i=1}^{d} a_{i,n}. \tag{12}$$

Additionally,

$$a_{i,n} = a_{n-1} - r_i \qquad \text{for } n \geq 2. \tag{13}$$

Remark: If a root r_i of $f(x)$ is not an integer, the corresponding polynomial f_i is not in $\mathbb{Z}[x]$, and the sequence $(a_{i,n})$ is not integral.

Proof. We proceed by induction. Since $a_{i,1} = f_i(0) = -r_i$, and $a_1 = f(0) = \prod_i(-r_i)$, (12) holds for $n = 1$. Also, $a_{i,2} = f_i(a_{i,1}) = f_i(-r_i) = f(-r_i + r_i) - r_i = f(0) - r_i = a_1 - r_i$, so (13) holds for $n = 2$. Now suppose that (12) holds for n, and that (13) holds for $n + 1$. Then, writing $f(x) = \prod_i(x - r_i)$, we have

$$a_{n+1} = f(a_n) = \prod_{i=1}^{d}(a_n - r_i) = \prod_{i=1}^{d} a_{i,n+1},$$

so that (12) holds for $n + 1$, and

$$a_{i,n+2} = f_i(a_{i,n+1}) = f_i(a_n - r_i) = f(a_n - r_i + r_i) - r_i = a_{n+1} - r_i,$$

so that (13) holds for $n + 2$. Hence both equations hold by induction. □

If a root r_k of $f(x)$ is an integer, we call the corresponding sequence $(a_{k,n}) = (f_k, f_k(0))$ a factor of the sequence $(a_n) = (f, f(0))$. This definition makes sense even when the other roots r_i of f are not all integers: since all of the r_i must be *algebraic* integers, so are the iterates $a_{i,n}$ of $f_i(x)$ for all i, and thus so is $\dfrac{a_n}{a_{k,n}} = \displaystyle\prod_{i \neq k} a_{i,n}$. It follows that $a_{k,n} | a_n$ for all n.

We can now use the tool of sequence factorization to prove that many more sequences are rigid divisibility sequences.

Proposition 3.5. *Let $f(x)$ be a monic polynomial of degree d. Suppose that all of the roots r_i of $f(x)$ are integers, and let $(a_{i,n}) = (f_i, f_i(0))$ be the corresponding factors of the sequence $(a_n) = (f, f(0))$. If (a_n) is a rigid divisibility sequence, then $(a_{i,n})$ is a rigid divisibility sequence for all $1 \leq i \leq d$.*

Proof. Let p be a prime, and suppose that $p | a_{k,n}$ for some given k and n. Since $a_{k,n} | a_n$, it follows that $p | a_n$. Let m be minimal such that $p | a_m$ (it follows that $m | n$ as in the proof of Proposition 3.1), and set $v_p(a_m) = \alpha$. Let $v_p(a_{i,m}) = \alpha_i$ for all $1 \leq i \leq d$. Then by (12), it follows that $\alpha = \sum \alpha_i$. Since $(a_{i,n})$ is a strong divisibility sequence (see remark preceding

Theorem 1.2), $\gcd(a_{i,n}, a_{i,m}) = a_{i,\gcd(n,m)} = a_{i,m}$ for all i, so $v_p(a_{i,n}) \geq v_p(a_{i,m}) = \alpha_i$. Since (a_n) is a rigid divisibility sequence, $\sum v_p(a_{i,n}) = v_p(a_n) = \alpha = \sum \alpha_i$. It follows that $\alpha_i = v_p(a_{i,n})$ for all i; in particular, $v_p(a_{k,n}) = \alpha_k = v_p(a_{k,m})$. Since this held for all n such that $p|a_{k,n}$, it follows that $\alpha_k = v_p(a_{k,m})$ is the exponent i_p required in the definition of a rigid divisibility sequence. □

A special case of Proposition 3.5, the case of $f(x) = x^2 - k^2$, can be seen in Theorem 5.6 in [12].

In case the roots of $f(x)$ are not all integers, we can still find new rigid divisibility sequences provided that (a_n) is a superrigid divisibility sequence.

Proposition 3.6. *Let $f(x)$ be a monic polynomial. Suppose that $r_i \in \mathbb{Z}$ is a root of $f(x)$, and let $(b_n) = (f_k, f_k(0))$ be the corresponding factor of $(a_n) = (f, f(0))$. If (a_n) is a superrigid divisibility sequence, then (b_n) is a rigid divisibility sequence.*

Proof. Suppose that $p|b_n$. Since $b_n|a_n$, we also have $p|a_n$. Since (a_n) is a superrigid divisibility sequence, it then follows that $a_{cn+k-1} \equiv a_{k-1} \pmod{p^{v_p(a_n)+1}}$ unless $k = 1$ (a_0 is not defined). We then have that $b_{cn+k} = a_{cn+k-1} - r_i \equiv a_{k-1} - r_i = b_k \pmod{p^{v_p(a_n)+1}}$ for $k \neq 1$. Finally, since $b_n|a_n$, $v_p(b_n) \leq v_p(a_n)$, and thus $b_{cn+k} \equiv b_k \pmod{p^{v_p(b_n)+1}}$ unless $k = 1$. Since this held for any n and p, (b_n) satisfies the definition of a superrigid divisibility sequence for all $k \neq 1$. Unfortunately, since this does not necessarily hold for $k = 1$, (b_n) is not necessarily a superrigid divisibility sequence.

Choosing $k = n > 1$ and $p|b_n$, we obtain $b_{cn} \equiv b_n \pmod{p^{v_p(b_n)+1}}$, so that $v_p(b_{cn}) = v_p(b_n)$. Furthermore, when $n = 1$, $c \geq 3$, and $p|b_1$, $b_c = b_{(c-2)+2} \equiv b_2 \pmod{p^{v_p(b_1)+1}}$, so that $v_p(b_c) \geq \min\{v_p(b_2), v_p(b_1) + 1\}$. Since $\gcd(b_c, b_{c+1}) = b_1$, we therefore have $v_p(b_1) = v_p(\gcd(b_c, b_{c+1})) \geq \min\{v_p(b_2), v_p(b_1) + 1\}$. It follows that $v_p(b_2) \leq v_p(b_1)$, and since $b_1|b_2$, $v_p(b_1) = v_p(b_2)$. Therefore, $b_c \equiv b_2 \not\equiv 0 \pmod{p^{v_p(b_2)+1}}$, and we obtain $v_p(b_c) = v_p(b_2) = v_p(b_1)$ for $p|b_1$. Hence if m is minimal such that $p|b_m$, we may choose $i_p = v_p(a_m)$, so (b_n) is a rigid divisibility sequence. □

To demonstrate the utility of these results, we give two families of sequences all of whose terms have primitive prime divisors.

Corollary 3.7. *Let k be an integer, $|k| \geq 2$. Let $f(x) = x^2+2kx-k$, and let $(a_n) = (f, f(0))$. Then if $k \neq -2$, every term of (a_n) has a primitive prime divisor, and if $k = -2$, only a_2 fails to have a primitive prime divisor.*

Proof. We first check that (a_n) is a factor of the sequence (c_n) generated by $g(x) = x^2 - k^2$ starting at $g(0) = -k^2$. By Proposition 3.2, (c_n) is a rigid divisibility sequence. Since the roots of $g(x)$ are both integers, it follows from Proposition 3.5 that (a_n) is a rigid divisibility sequence as well. It follows immediately from Theorem 1.2 that at most finitely many terms of (a_n) have no primitive prime divisor; a proof like that in Lemma 3.3 shows that if $k \neq 2$, then $|a_n| > \prod_{i=1}^{n-1} |a_i|$ for $n \geq 3$, and if $k = 2$, this is true for all $n \geq 4$. In all cases except $k = -2$, we can check that a_2 has a primitive prime divisor. (In the case $k = 2$, we also check a_3.) The fact that all other terms have a primitive prime divisor then follows as in Theorem 1.2, completing the proof. □

Another example demonstrates the usefulness of Proposition 3.6 in a case where Proposition 3.5 does not apply.

Corollary 3.8. *Let k be an integer, $|k| \geq 2$. Let $f(x) = x^3 + 3kx^2 + 3k^2x - k$, and let $(a_n) = (f, f(0))$. Then every term of (a_n) has a primitive prime divisor.*

Proof. We observe that (a_n) is a factor of the sequence (c_n) generated by $g(x) = x^3 - k^3$ starting at $g(0) = -k^3$ (corresponding to the only integer root k of $g(x)$). By Proposition 3.2, (c_n) is a superrigid divisibility sequence. Then by Proposition 3.6, (a_n) is a rigid divisibility sequence. Calculations along the lines of Lemma 3.3 show that for $n \geq 2$, $|a_n| > \prod_{i=1}^{n-1} |a_i|$; it follows as in Theorem 1.2 that a_n has a primitive prime divisor for $n \geq 2$, completing the proof. □

References

[1] David K. Arrowsmith and Franco Vivaldi. Geometry of p-adic Siegel discs. *Phys. D*, 71(1-2):222–236, 1994.

[2] Robert L. Benedetto. p-adic dynamics and Sullivan's no wandering domains theorem. *Compositio Math.*, 122(3):281–298, 2000.

[3] Robert L. Benedetto. Components and periodic points in non-Archimedean dynamics. *Proc. London Math. Soc. (3)*, 84(1):231–256, 2002.

[4] Yu. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[5] Gregory S. Call and Susan W. Goldstine. Canonical heights on projective space. *J. Number Theory*, 63(2):211–243, 1997.

[6] Gregory S. Call and Joseph H. Silverman. Canonical heights on varieties with morphisms. *Compositio Math.*, 89(2):163–205, 1993.

[7] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):30–48, 1913/14.

[8] Graham Everest, Gerard Mclaren, and Thomas Ward. Primitive divisors of elliptic divisibility sequences. *J. Number Theory*, 118(1):71–89, 2006.

[9] Graham Everest, Shaun Stevens, Duncan Tamsett, and Tom Ward. Primes generated by recurrence sequences. arXiv: math.NT/0412079, 2006. To appear in Amer. Math. Monthly.

[10] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward. *Recurrence sequences*, Volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[11] Liang-Chung Hsia. Closure of periodic points over a non-Archimedean field. *J. London Math. Soc. (2)*, 62(3):685–700, 2000.

[12] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. arXiv: math.NT/0612415, 2006. Preprint.

[13] W. Narkiewicz and T. Pezda. Finite polynomial orbits in finitely generated domains. *Monatsh. Math.*, 124(4):309–316, 1997.

[14] Władysław Narkiewicz. *Polynomial mappings*, Volume 1600 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1995.

[15] Andrzej Schinzel. The intrinsic divisors of Lehmer numbers in the case of negative discriminant. *Ark. Mat.*, 4:413–416 (1962), 1962.

[16] N.J.A. Sloane. The on-line encyclopedia of integer sequences. Published electronically at http://www.research.att.com/~njas/sequences/, 2007.

[17] K. Zsigmondy. Zur theorie der potenzreste. *Monatsh. Math.*, 3:265–284, 1892.