PRIMITIVE PRIME DIVISORS IN ZERO ORBITS OF POLYNOMIALS

Kevin Doerksen
Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada
kdoerkse@gmail.com

Anna Haensch
Department of Mathematics and Computer Science, Wesleyan University, Middletown, Connecticut
ahaensch@wesleyan.edu

Received: 9/20/10, Revised: 6/2/11, Accepted: 1/1/12, Published: 1/13/12

Abstract

Let $(b_n) = (b_1, b_2, \dots)$ be a sequence of integers. A primitive prime divisor of a term b_k is a prime which divides b_k but does not divide any of the previous terms of the sequence. A zero orbit of a polynomial $\varphi(z)$ is a sequence of integers (c_n) where the n-th term is the n-th iterate of φ at 0. We consider primitive prime divisors of zero orbits of polynomials. In this note, we show that for c, d in $\mathbb{Z}$, where $d \geq 2$ and $c \neq \pm 1$, every iterate in the zero orbit of $\varphi(z) = z^d + c$ contains a primitive prime divisor whenever zero has an infinite orbit. If $c = \pm 1$, then every iterate after the first contains a primitive prime divisor.

1. Introduction

A *dynamical system* is a pair (φ, S) where S is a set and φ is a map from S to itself. Given such a pair, the *orbit* of an element $\alpha \in S$ under φ is the set

$$\{\varphi(\alpha), \varphi^2(\alpha), \dots, \varphi^n(\alpha), \dots\}$$

where

$$\varphi^n(z) = \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{n \text{ times}}(z).$$

Such an element α can classified according to the size of the orbit. If the orbit contains only finitely many values, then α is a *preperiodic point*. If the orbit contains infinitely many values, then α is a *wandering point*. If we restrict to the case where $S = \mathbb{Z}$ and $\varphi \in \mathbb{Z}[z]$, the orbit of a wandering point α, will yield an infinite sequence

of integers. Some very natural questions about prime factorization and divisibility in these sequences arise. In particular, one can ask which iterates in the orbit contain prime divisors not dividing any previous term.

Definition 1. Let $(b_n) = (b_1, b_2, \dots)$ be a sequence of integers. We say that the term b_n contains a *primitive prime divisor* if there exists a prime p such that $p \mid b_n$, but $p \nmid b_i$ for $i < n$.

Questions about terms containing primitive prime divisors have been asked for a number of different recurrence sequences. Classical results by Bang [1] (for $b = 1$) and Zsigmondy [11] showed that for any $a, b \in \mathbb{N}$, every term in the sequence $a^n - b^n$ has a primitive prime divisor past the sixth term. The question of primitive prime divisors in second-order linear recurrence sequences was completely solved by Bilu, Hanrot, and Voutier in [2].

Recent papers have addressed the question of primitive prime divisors in nonlinear recurrence sequences. Elliptic divisibility sequences, for example, were considered by Silverman in [8], and later by Everest, Mclaren, and Ward in [3] and Yabuta in [10]. In our paper, we consider recurrence sequences generated by the orbit of wandering points of non-linear polynomials. This question was first addressed by Rice [7].

Theorem 2. (Rice 2007) *Let $\varphi(z) \in \mathbb{Z}[z]$ be a monic polynomial of degree $d \geq 2$. Suppose that $(b_n) = \varphi^n(0)$ has infinite orbit under iteration of φ such that (b_n) is a rigid divisibility sequence. Then all but finitely many terms of the sequence $(\alpha, \varphi(\alpha), \varphi^2(\alpha), \dots)$ contain a primitive prime divisor.*

See Section 2 for a definition of rigid divisibility sequences. Rice also showed that if zero is a preperiodic point of a monic polynomial of degree ≥ 2, then the orbit of any wandering point has finitely many terms which contain no primitive prime divisor. Silverman and Ingram [5] later generalized this result to arbitrary rational maps over number fields. Faber and Granville [4] also considered rational maps, ϕ, over number fields, but they looked at primitive prime divisors in the sequence generated by $\left(\phi^{n+\Delta}(\alpha) - \phi^n(\alpha)\right)$ for a wandering point α and a fixed integer $\Delta \geq 1$.

Silverman and Ingram use Roth's theorem to prove their result, and therefore their proof does not give a means to find an effective upper bound on the terms without primitive prime divisors. Rice also remarks that though his bounds are effectively computable, he does not compute them. Silverman [9] proposed that it would be of interest to compute explicit upper bounds on n for the terms which contain no primitive prime divisor, when the polynomial $\varphi(z)$ and α are fixed. In this paper, we answer this question for a certain class of polynomials. We prove

Theorem 3. *Let $\varphi \in \mathbb{Z}[z]$ be the polynomial $\varphi(z) = z^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Suppose that zero is a wandering point of φ and write $b_n = \varphi^n(0)$. Then*

1. *If $c = \pm 1$, then b_n contains a primitive prime for all $n \geq 2$.*

2. *For all other $c \in \mathbb{Z}$, b_n contains a primitive prime for all $n \geq 1$.*

We prove Theorem 3 in two parts. We begin by showing that for the sequence (b_n), defined in the statement of the theorem, there is an upper bound on the size of the product of all prime divisors of a term b_n which are not primitive prime divisors. We then show that the sequence grows too fast for any one term to not contain a primitive prime divisor (other than possibly the first term).

Acknowledgements. The authors would like to thank Joe Silverman for originally drawing their attention to the problem. They would also like to thank Michelle Manes and Rafe Jones for the helpful comments and suggestions. Thanks also goes to the organizers of the NSF-funded Arizona Winter School, at which the initial research for this paper took place.

2. Rigid Divisibility Sequences

In order to prove Theorem 3, we make use of a special type of divisibility sequence, with terminology taken from Jones [6] and Rice [7]. For $\alpha \in \mathbb{Z}$, let $v_p(\alpha)$ denote the valuation at p of α. A sequence (b_n) of integers is said to be a *rigid divisiblity sequence* if for every prime p the following two properties hold:

1. If $v_p(b_n) > 0$ then $v_p(b_{nk}) = v_p(b_n)$ for all $k \geq 1$, and
2. If $v_p(b_n) > 0$ and $v_p(b_m) > 0$ then $v_p(b_n) = v_p(b_m) = v_p(b_{\gcd(m,n)})$.

Lemma 4. (Rice [7]) *Let $\varphi \in \mathbb{Z}[z]$ be the polynomial $\varphi(z) = z^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Let zero be a wandering point of φ and write $b_n = \varphi^n(0)$. Then (b_n) is a rigid divisibility sequence.*

Proof. Let p be a prime and suppose $v_p(b_n) = e > 0$ for some $n, e \in \mathbb{N}$. Then $b_n = p^e m$ for some m where $p \nmid m$. Then

$$b_{n+1} = p^{ed}m^d + c = p^{e+1}\left(p^{e(d-1)-1}m^d\right) + c \equiv c \pmod{p^{e+1}},$$

with the last congruence possible because $d \geq 2$. But $b_1 = c$ so $b_{n+1} \equiv b_1 \pmod{p^{e+1}}$. By induction on t, we have $b_{n+t} \equiv b_t \pmod{p^{e+1}}$, and so in general for $k \geq 1$, $b_{kn+r} \equiv b_r \pmod{p^{e+1}}$, and in particular, for $r = 0$, we get $v_p(b_{kn}) = v_p(b_n)$.

Now suppose $m, n \in \mathbb{N}$ such that $v_p(b_m) > 0$ and $v_p(b_n) > 0$. Without loss of generality, suppose $m < n$ and $m \nmid n$ (the case where $m|n$ has already been covered). Let $s, t \in \mathbb{N}$ such that $t \geq 1$ and $sm + tn = \gcd(m, n)$. Then

$$b_{\gcd(m,n)} = b_{sm+tn} \equiv b_{tn} \equiv b_n \pmod{p^{e+1}},$$

therefore $v_p\big(b_{\gcd(m,n)}\big) = v_p(b_n)$, and since m is a positive multiple of $\gcd(m, n)$, we also conclude $v_p\big(b_{\gcd(m,n)}\big) = v_p(b_m)$. □

Remark 5. Rice actually proves a more general result than Lemma 4. In Propositions 3.1 and 3.2 from [7], he shows that for any polynomial φ of degree $d \geq 2$ that has a wandering orbit at zero, then the sequence b_n as defined in Lemma 4 is a rigid divisibility sequence if and only if the coefficient of the linear term of φ is zero.

Suppose (b_n) is a rigid divisibility sequence. For every n, we can write

$$b_n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} q_1^{f_1} \dots q_\ell^{f_\ell}$$

where p_i are the primitive prime divisors of b_n and q_j are the prime divisors of b_n which are not primitive. Let

$$P_n = p_1^{e_1} \dots p_k^{e_k} = \text{the } \textit{primitive part} \text{ of } b_n \text{ and}$$
$$N_n = q_1^{f_1} \dots q_\ell^{f_\ell} = \text{the } \textit{non-primitive part} \text{ of } b_n.$$

Lemma 6. *Let (b_n) be a rigid divisibility sequence and let P_n and N_n be as above. Then*

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

Proof. Let p be a prime divisor in the non-primitive part of b_n. Then there exists some positive integer $d < n$ such that p is a primitive prime divisor of b_d. By Property 2 of rigid divisibility sequences, $v_p(b_n) = v_p(b_d) = v_p(b_{\gcd(d,n)})$. Since p is a primitive prime divisor of b_d, we must have $\gcd(d, n) \geq d$ and so $d \mid n$. Therefore N_n divides $\prod_{d|n, d\neq n} P_d$.

Now suppose $d \mid n$ and suppose q is a primitive prime divisor of b_d. Then by Property 1, $v_q(b_d) = v_q(b_n)$. Therefore the product $\prod_{d|n,d\neq n} P_d$ divides N_n, completing the proof. □

Armed with these two results, we are now able to proceed with the main theorem of this paper.

3. Proof of Main Result

We begin this section with two useful lemmas.

Lemma 7. *Let $\varphi \in \mathbb{Z}[z]$ be the polynomial $\varphi(z) = z^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Let $a \in \mathbb{Z}$, and for nonnegative $n \in \mathbb{Z}$, define the sequence $(b_{a,n})$ by*

$$b_{a,0} = a \quad \textit{and} \quad b_{a,n+1} = \varphi(b_{a,n})$$

and let $B_{a,n} = |b_{a,n}|$. If $|a| \geq |c|$ and $|a| > 2$ then $(B_{a,n})$ is an increasing sequence.

Proof. We prove this by induction. For the base case,

$$B_{a,1} = |\varphi(a)| = \left|a^d + c\right| > |2a| - |c| \geq |a|\,.$$

Now suppose $(B_{a,n})$ is increasing on $n \leq N$. Then

$$B_{a,N+1} = |\varphi(b_{a,N})| = \left|(b_{a,N})^d + c\right| > |2b_{a,N}| - |c| > B_{a,N} + |a| - |c| \geq B_{a,N},$$

completing the proof. □

The statement of Theorem 3 requires zero to be a wandering point of φ. In the next lemma, we characterize all polynomials over $\mathbb{Z}$ of the form $z^d + c$ for which zero is a preperiodic point. Rice proves a more general result by giving a complete classification of monic polynomials for which the orbit of zero is finite (see [7, Proposition 2.1]). Nevertheless, the special case where $\varphi(z) = z^d + c$ is a relevant lemma with a straightforward proof. We therefore provide a full proof.

Lemma 8. *Let $\varphi \in \mathbb{Z}[z]$ be the polynomial $\varphi(z) = z^d + c$, where $c, d \in \mathbb{Z}$ and $d \geq 2$. Then either*

1. *Zero is a wandering point and the sequence (B_n), defined by $B_n = |\varphi^n(0)|$, is an increasing sequence, or*
2. *Zero is a preperiodic point and exactly one of the following is true*
   (a) *$c = 0$,*
   (b) *$c = -1$ and d is even, or*
   (c) *$c = -2$ and $d = 2$.*

Proof. Note that $\varphi(0) = c$, so if $c \notin \{0, \pm 1, \pm 2\}$, then (B_n) is an increasing sequence by Lemma 7, and so zero must be a wandering point.

For $c > 0$, a simple induction shows that $(\varphi^n(0))$ is an increasing sequence, and so zero is a wandering point.

If $c = 0$ then $\varphi(0) = 0$ and zero is a preperiodic point.

Now suppose $c = -1$. If d is even, then $\varphi(0) = -1$ and $\varphi(-1) = 0$ and therefore zero is a preperiodic point. If d is odd then $\varphi(0) = -1$, $\varphi(-1) = -2$, and $\varphi(-2) = (-2)^d - 1$. Since $|\varphi(-2)| > 2$, we can apply Lemma 7 to show that all subsequent iterates grow in absolute value.

Finally, suppose $c = -2$. If $d = 2$ then $\varphi(0) = -2$, $\varphi(-2) = 2$, and $\varphi(2) = 2$. If $d > 2$ then $\varphi(0) = -2$ and $\varphi(-2) = (-2)^d - 2$. But

$$\left|(-2)^d - 2\right| \geq 2^d - 2 \geq 2^3 - 2 = 6.$$

We can therefore apply Lemma 7 to conclude that zero is a wandering point. □

We now are ready to prove Theorem 3.

Proof of Theorem 3. Note first that if $c = 0$, then zero would not be a wandering point, so we must have $c \neq 0$. Also, $b_1 = \varphi(0) = c$, so b_1 will have a primitive prime divisor if and only if $c \neq \pm 1$. For b_2, note that

$$b_2 = \varphi(b_1) = c^d + c = c(c^{d-1} + 1),$$

and since $b_1 = c$, we see that b_2 will contain a primitive prime divisor, except when $c = 0$ or when $c = -1$ and d is even. In both cases, by Lemma 8, zero would not be a wandering point.

Now let $m \in \mathbb{N}$ with $m \geq 3$. We will prove that b_m contains a primitive prime. Let $|\cdot|$ denote the Euclidean absolute value. Then

$$\begin{aligned}
|b_m| &= \left|(b_{m-1})^d + c\right| \\
&\geq \left|(b_{m-1})^d\right| - |c| \\
&\geq |b_{m-1}|^2 - |b_1| && \text{because } b_1 = \varphi(0) = c \text{ and } d \geq 2 \\
&> |b_{m-1}|^2 - |b_{m-1}|\,. && \text{because } (b_n) \text{ is increasing and } m \geq 3.
\end{aligned}$$

We can factor the last line to obtain

$$|b_m| > |b_{m-1}| \cdot (|b_{m-1}| - 1)\,. \tag{1}$$

To complete the proof, we first need to show that for all $m \geq 3$,

$$\prod_{k=1}^{m-1} |b_k| < |b_m|\,.$$

We prove this claim by induction. The base case is trivially true. Now assume that $\prod_{k=1}^{m-2} |b_k| < |b_{m-1}|$. In particular, this implies

$$\prod_{k=1}^{m-2} |b_k| \leq |b_{m-1}| - 1. \tag{2}$$

Combining (2) with (1),

$$\prod_{k=1}^{m-1} |b_k| = |b_{m-1}| \cdot \prod_{k=1}^{m-2} |b_k| \leq |b_{m-1}| \cdot (|b_{m-1}| - 1) < |b_m|\,.$$

Finally, by Lemma 4, we know that (b_n) is a rigid divisibility sequence. For all $m \in \mathbb{N}$, let P_m and N_m denote the primitive part and the non-primitive part of b_m respectively. Then $|b_m| = P_m N_m$ and by Lemma 6

$$N_m = \prod_{d|m, d\neq m} P_d \leq \prod_{k=1}^{m-1} P_k \leq \prod_{k=1}^{m-1} |b_k| < |b_m|$$

Therefore $P_m > 1$ and b_m contains a primitive prime. □

References

[1] A. S. Bang. *Taltheoretiske Undersogelser*. Tidsskrift Mat., 4(5):7080, 130137, 1886.

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

[3] Graham Everest, Gerard Mclaren, and Thomas Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), no. 1, 71–89.

[4] Xander Faber and Andrew Granville, *Prime factors of dynamical sequences*, Journal für die reine und angewandte Mathematik (Crelles Journal) (2011).

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

[6] Rafe Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. (2) **78** (2008), no. 2, 523–544.

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

[8] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237.

[9] Joseph H. Silverman. *Lecture Notes on Arithmetic Dynamics*, Arizona Winter School, 2010. math.arizona.edu/∼swc/aws/10/2010SilvermanNotes.pdf.

[10] Minoru Yabuta, *Primitive divisors of certain elliptic divisibility sequences*, Experiment. Math. **18** (2009), no. 3, 303–310.

[11] K. Zsigmondy. *Zur Theorie der Potenzreste*. Monatsh. Math. Phys. **3(1)** (1892), 265–284.