Khayyam J. Math. 8 (2022), no. 1, 115-119
DOI: 10.22034/kjm.2022.261184.2086

Khayyam Journal of Mathematics
emis.de/journals/KJM
kjm-math.org

THE ZSIGMONDY SET FOR ZERO ORBIT OF A RIGID POLYNOMIAL

KHOSRO MONSEF SHOKRI

Communicated by H.R. Ebrahimi Vishki

Abstract. For a monic polynomial f with integer coefficients such that zero is a critical point of f, we consider the zero orbit, namely the sequence $(f^n(0))_{n\geq 1}$. If this sequence contains an infinite number of integer numbers, then we show that the Zsigmondy set of this sequence is either empty or it has at most two elements.

1. Introduction

For a sequence of integers $\mathcal{A} = (a_n)_{n\geq 1}$, a prime divisor p of a_n is called primitive if there is no $m < n$ such that $p|a_m$. The Zsigmondy set of $\mathcal{A}$ denoted by $\mathcal{Z}(\mathcal{A})$ is the set of those n for which a_n has no primitive prime divisor. In recent years, the study of Zsigmondy sets has been the subject of many articles (see, for example, [1, 3, 4]).

For a set S and a function $f : S \to S$, we recall that the orbit of $x \in S$ under f is the set of all iterations of x under f, that is,

$$\mathcal{O}_f(x) = \{f^n(x) : n \geq 1\},$$

where $f^1(x) = f(x)$ and for $n \geq 2$, $f^n(x) = f \circ f^{n-1}(x)$. We say that an element $x \in S$ is preperiodic if its orbit is finite, otherwise x is wandering. Now consider a monic integral polynomial f of the form $f(x) = x^2 g(x) + c$, where $g(x)$ is a polynomial. Rice [5] proved the finiteness of the Zsigmondy set (without giving a uniform bound) of the zero orbit $\mathcal{O}_f(0)$ when 0 is a wandering point. The proof is elementary, and it is based on the property of rigid divisibility of the polynomial f. In [2], the authors completely determined the Zsigmondy set of the wandering

Date: Received: 8 December 2020; Revised: 11 January 2022; Accepted: 17 January 2022.
2020 *Mathematics Subject Classification.* Primary 37P35; Secondary 11B37, 11C08.
Key words and phrases. Zsigmondy set, Zero orbit, Primitive prime. Rigid divisibility.

zero orbit of $f(z) = z^d + c$, where $c \in \mathbb{Z}$ and $d \geq 2$, and for $c \in \mathbb{Q}$, Krieger [4] found a uniform bound. She showed that $\mathcal{Z}$ has at most 23 elements.

Ingram and Silverman [3] generalized the result of Rice to rational functions. They showed that, under mild assumptions for a rational function $\phi(z) \in \mathbb{Q}(z)$ and $\alpha \in \mathbb{Q}$, the Zsigmondy set of the sequence of the numerators $\mathcal{O}_\phi(\alpha)$ is finite. The proof is based on Roth's theorem, which is ineffective. Hence finding a uniform bound (if such bound exists) is challenging. So far, only few cases have been characterized.

The motivation of this article is to generalize the work of [2] to the class of rigid polynomials and classify the Zsigmondy set of zero orbit of such polynomials. More precisely, we obtain the following result.

Theorem 1.1. *Let $f(x) \in \mathbb{Z}[x]$ be a rigid polynomial, that is, $f(x) = x^2 g(x) + c$, where $g(x) \in \mathbb{Z}[x]$. If $x = 0$ is a wandering point, that is, the set $\mathcal{O}_f(0) = \{f^n(0) : n \geq 1\}$ is infinite, then the Zsigmondy set of $\mathcal{O}_f(0)$ has at most two elements. Indeed, we have the following properties:*

(1) *If $|c| = 1$, then $\{1\} \subseteq \mathcal{Z}(\mathcal{O}_f(0)) \subseteq \{1, 2\}$.*
(2) *If $|c| = 2$, then $\mathcal{Z}(\mathcal{O}_f(0)) \subseteq \{2\}$.*
(3) *If $|c| > 2$, then $\mathcal{Z}(\mathcal{O}_f(0))$ is empty.*

From now, for simplicity, we set $\mathcal{O} := \mathcal{O}_f(0)$ and $\mathcal{Z} := \mathcal{Z}(\mathcal{O})$. The idea behind this theorem is that the element of the orbit $\mathcal{O}$ rapidly grows and the rigid divisibility property (see Definition 2.1) implies that $f^n(0)$ has a primitive prime divisor.

Remark 1.2. For $|c| = 1$, the case $\mathcal{Z} = \{1, 2\}$ can occur. For example, let $f(x) = x^2(x-3) + 1$; then $f(0) = 1$ and $f \circ f(0) = -1$. Also for $|c| = 2$ and $f(x) = x^2(x^2 - 5x + 5) + 2$, we have $\mathcal{Z} = \{2\}$.

In the following section, we review some basic properties of rigid polynomials, and in section 3, we give a proof of Theorem 1.1

2. Rigid divisibility property

In this section, first we review basic definitions and results from [5].

Definition 2.1. A sequence $(\sigma_n)_{n\geq 1}$ of integers is a rigid divisible sequence if for every prime p, the following two properties hold:

(1) If $v_p(\sigma_n) > 0$, then $v_p(\sigma_{kn}) = v_p(\sigma_n)$ for all $k \geq 1$.

(2) If $v_p(\sigma_n) > 0$ and $v_p(\sigma_m) > 0$, then $v_p(\sigma_{(n,m)}) > 0$.

Here v_p denotes the p-adic valuation with respect to p and (m, n) means the greatest common divisor of m and n.

Remark 2.2. It follows from Definition 2.1 that for a sequence $(\sigma_n)_{n\geq 1}$ with rigid divisibility, if $v_p(\sigma_n) > 0$ and $v_p(\sigma_m) > 0$, then $v_p(\sigma_n) = v_p(\sigma_{(n,m)})$.

Definition 2.3. A monic polynomial defined over $\mathbb{Z}$ is called rigid if $x = 0$ is a critical value for f. In other words, $f \in \mathbb{Z}[x]$ is rigid if $f(x) = x^2 g(x) + c$ for some $c \in \mathbb{Z}$ and a monic polynomial $g(x) \in \mathbb{Z}[x]$.

Proposition 2.4. *Let $f(x)$ be a rigid polynomial and let $f(0) \neq 0$. Then the sequence $(f^n(0))_{n\geq 1}$ has the rigid divisibility property.*

Proof. We write $f(x) = x^2 g(x) + c$, where $c \neq 0$ and $g(x) \in \mathbb{Z}[x]$. Let $c_n = f^n(0)$, for fixed $n \geq 1$, and let $v_p(c_n) = i > 0$. We have

$$c_{n+1} = f(c_n) = c_n^2 g(c_n) + c \equiv c \pmod{p^{i+1}},$$

and by induction

$$c_{n+m} = f(c_{n+m-1}) \equiv f(c_{m-1}) = c_m \pmod{p^{i+1}}.$$

In particular, for $m = (k-1)n + r$ with $1 \leq r < n$, we have

$$c_{kn+r} \equiv c_{(k-1)n+r} \equiv \cdots \equiv c_r \pmod{p^{i+1}}.$$

This identity shows two properties of rigid divisibility. □

Corollary 2.5. *Let f be a polynomial as before and let $\mathcal{O} = (c_n)_{n\geq 1} = (f^n(0))_{n\geq 1}$. If n belongs to $\mathcal{Z}(\mathcal{O})$, then*

$$c_n | \prod_{\substack{m|n \\ m\neq n}} c_m.$$

Proof. Let p be a prime such that $p|c_n$ and let $v_p(c_n) = i > 0$. Since $n \in \mathcal{Z}(\mathcal{O})$, there exists some $m < n$ such that $p|c_m$ and $v_p(c_m) = i$. The sequence (c_n) is a rigid sequence, so $p|c_{(n,m)}$, $v_p(c_{(n,m)}) = i$, and (n, m) is a proper divisor of n. Hence p^i divides the above product. □

3. Proof

Now we are ready to prove Theorems 1.1. We start with the following lemma.

Lemma 3.1. *Let $f(x) = x^2 g(x) + c$ be a rigid polynomial of degree $d \geq 2$ such that zero is a wandering point. Let $c_n = f^n(0)$ for $n \geq 1$.*

(1) *If $|c| > 2$, then the sequence $(|c_n|)_{n\geq 1}$ is strictly increasing. Furthermore, for $n \geq 2$, we have $|c_{n+1}| > |c_n|(|c_n| - 1)$.*

(2) *If $|c| = 1, 2$, then the sequence $(c_n)_{n\geq 2}$ is strictly increasing. Furthermore, for $n \geq 3$, we have $|c_{n+1}| > |c_n|(|c_n| - 1)$.*

Proof. We prove by induction on n. We note that since zero is wandering so for all $k \geq 1$, $g(c_k) \neq 0$. Now, for $|c| > 2$, we have

$$\begin{aligned} |c_2| = |f(c)| = |c^2 g(c) + c| &\geq |c^2 g(c)| - |c| \\ &\geq c^2 - |c| > |c| = |c_1|. \end{aligned}$$

Suppose that the sequence is strictly increasing for all $k \leq n$. Then

$$\begin{aligned} |c_{n+1}| = |f(c_n)| = |c_n^2 g(c_n) + c| &\geq |c_n^2 g(c_n)| - |c| \\ &\geq |c_n^2| - |c|, \end{aligned}$$

$$> 2|c_n| - |c| > |c_n| \qquad\qquad (|c_n| > |c| > 2).$$

This completes the induction step. Now, for the second claim, we have $|c_n| > |c|$ for $n > 1$. Hence from the above inequality, we have

$$|c_{n+1}| \geq c_n^2 - |c| > c_n^2 - |c_n|.$$

The proof of the second part is similar and we omit it. The only point is that it might be $|c_1| = |c_2|$, but then certainly $|c_3| > |c_2|$, otherwise $x = 0$ is a preperiodic point and is not wandering. □

Lemma 3.2. *With the same assumptions as in Lemma 3.1, we have*

(1) *if $|c| > 2$, for $n \geq 2$, then $|c_n| > \prod_{k=1}^{n-1} |c_k|$;*

(2) *if $|c| = 1, 2$, for $n \geq 3$, then $|c_n| > \prod_{k=1}^{n-1} |c_k|$.*

Proof. We prove by induction. For $|c| > 2$, according to Lemma 3.1, $|c_2| > |c_1|$. If $|c_n| > \prod_{k=1}^{n-1} |c_k|$, then $|c_n| - 1 \geq \prod_{k=1}^{n-1} |c_k|$. Hence from Lemma 3.1, we have

$$|c_{n+1}| > |c_n||(c_n| - 1) \geq \prod_{k=1}^{n} |c_k|.$$

For the second part, if $|c_2| > |c_1|$, then the above argument holds without a change, otherwise $|c_3| > |c_2|$. Now if $|c| = 1$, then $|c_3| > |c_1 c_2|$, and we can continue the inductive argument as before. If $|c| = 2$, then $| c_3 | \neq 2$ is of the form $| c_3 | = 4m + 2$ with $m \neq 0$. Hence $|c_3| > |c_1 c_2| = 4$ and the proof can be repeated as before. □

Proof of Theorem 1.1. First we show that independent of the value of c, there is no $n \geq 3$ in the Zsigmondy set $\mathcal{Z}$ of zero orbit of f. Suppose that $n \geq 3$ belongs to $\mathcal{Z}$. Then from Corollary 2.5, we have

$$c_n | \prod_{\substack{m|n \\ m \neq n}} c_m.$$

In particular, we have

$$|c_n| \leq \prod_{\substack{m|n \\ m \neq n}} c_m \leq \prod_{k=1}^{n-1} |c_k|.$$

This is a contradiction, according to Lemma 3.2, which shows that $n \notin \mathcal{Z}$.
For $n = 1, 2$, we distinguish three cases. If $|c| > 2$, then $|c_1| = |c| \neq 1$, which implies that $1 \notin \mathcal{Z}$. For $n = 2$, from Lemma 3.1, we have $|c_2| > |c_1|$ and $| c_2 | = | c^2 g(c) + c | = |c|.|c\, g(c) + 1|$. Since $|c\, g(c) + 1|$ is greater than 1 and is coprime to c, it has a primitive prime divisor. Hence $2 \notin \mathcal{Z}$. Therefore $\mathcal{Z}$ is empty for $|c| > 2$.
For $|c| = 2$, evidently $1 \notin \mathcal{Z}$. If $|c_2| \neq |c_1|$, the the previous argument can be repeated and we find that the Zsigmondy set $\mathcal{Z}$ is empty in this case. For $|c_1| = |c_2| = 2$, we have $2 \in \mathcal{Z}$. Hence we conclude that for $|c| = 2$, we have $\mathcal{Z} \subseteq \{2\}$.

Finally for $|c| = 1$, we have $1 \in \mathcal{Z}$. Now if $|c_2| > |c_1|$, in a similar vein, then we find that $\mathcal{Z} = \{1\}$, otherwise $\mathcal{Z} = \{1, 2\}$, and the proof is complete. □

Acknowledgment. I would like to thank The Research Institute for Fundamental Sciences (IPM) for its support, and the referees for their valuable suggestions.

References

1. Y. Bilu, G. Hanrot and P.M. Voutier, *Existing of primitive divisors of Lucas and Lehmer numbers,* J. Reine. Angew. Math. **539** (2001) 75–122.
2. K. Doerksen and A. Haensch, *Primitive prime divisors in zero orbits of polynomials,* Integers, **12** (2012), no. 3, 465–472.
3. P. Ingram and J.H. Silverman, *Primitive divisors in arithmetic dynamics,* Math. Proc. Cambridge Philos. Soc. **146** (2009), no.2, 289–302.
4. H. Krieger, *Primitive prime divisors in the critical orbit of* $z^d + c$, Int. Math. Res. Not. IMRN **2013** (2013), no. 23, 5498–5525.
5. B. Rice. *Primitive prime divisors in polynomial arithmetic dynamics*, Integers,**7** (2007), no. A26, 16 pp.

Department of Mathematics, Faculty of Mathematical Sciences, University of Shahid Beheshti, Tehran, Iran.
Email address: k_shokri@sbu.ac.ir