Math. Proc. Camb. Phil. Soc. (2009), **146**, 289 © 2008 *Cambridge Philosophical Society*
doi:10.1017/S0305004108001795 *Printed in the United Kingdom*
First published online 30 September 2008

Primitive divisors in arithmetic dynamics

BY PATRICK INGRAM

Department of Mathematics, University of Toronto, Toronto, Ontario M5S 2E4, Canada.
e-mail: pingram@math.utoronto.ca

AND JOSEPH H. SILVERMAN†

Mathematics Department, Box 1917 Brown University, Providence, RI 02912, U.S.A.
e-mail: jhs@math.brown.edu

(*Received* 15 *November* 2007; *revised* 2 *February* 2008)

Abstract

Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geqslant 2$ with $\varphi(0) = 0$ and such that φ does not vanish to order d at 0. Let $\alpha \in \mathbb{Q}$ have infinite orbit under iteration of φ and write $\varphi^n(\alpha) = A_n/B_n$ as a fraction in lowest terms. We prove that for all but finitely many $n \geqslant 0$, the numerator A_n has a primitive divisor, i.e., there is a prime p such that $p \mid A_n$ and $p \nmid A_i$ for all $i < n$. More generally, we prove an analogous result when φ is defined over a number field and 0 is a preperiodic point for φ.

Introduction

Let $\mathcal{A} = (A_n)_{n \geqslant 1}$ be a sequence of integers. A prime p is called a *primitive divisor of* A_n if

$$p \mid A_n \quad \text{and} \quad p \nmid A_i \quad \text{for all } 1 \leqslant i < n.$$

The *Zsigmondy set of* $\mathcal{A}$ is the set

$$\mathcal{Z}(\mathcal{A}) = \{n \geqslant 1 : A_n \text{ does not have a primitive divisor}\}.$$

A classical theorem of Bang [**3**] (for $b = 1$) and Zsigmondy [**33**] in general says that if $a, b \in \mathbb{Z}$ are integers with $a > b > 0$, then

$$\mathcal{Z}((a^n - b^n)_{n \geqslant 1}) \text{ is a finite set.}$$

Indeed assuming that $\gcd(a, b) = 1$, they prove that $\mathcal{Z}((a^n - b^n)_{n \geqslant 1})$ contains no integer $n > 6$, which is a strong uniform bound. This useful result has been extended and generalized in many ways, for example to more general linear recursions, to number fields, to elliptic curves, and to Drinfeld modules, see [**7**, **8**, **10**, **11**, **13**, **15**, **16**, **17**, **23**, **26**, **28**]. For applications of Zsigmondy sets to Diophantine equations, computability theory, and group theory, see for example [**1**, **22**, **24**].

In this paper we prove a Bang–Zsigmondy result for sequences associated to iteration of rational functions. For ease of exposition, we state here a special case of our main result for dynamical systems over $\mathbb{Q}$. See Theorem 7 for the general statement.

† The second author's research supported by NSA H98230-04-1-0064 and NSF DMS-0650017

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

THEOREM 1. *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geqslant 2$ such that $\varphi(0) = 0$, but φ does not vanish to order d at $z = 0$. Let $\alpha \in \mathbb{Q}$ be a point with infinite orbit under iteration of φ. For each $n \geqslant 1$, let φ^n denote the nth iterate of φ and write*

$$\varphi^n(\alpha) = \frac{A_n}{B_n} \in \mathbb{Q}$$

as a fraction in lowest terms. Then the dynamical Zsigmondy set $\mathcal{Z}((A_n)_{n \geqslant 0})$ is finite.

Remark 2. Rice [**25**] investigates primitive divisors in the case that $\varphi(z) \in \mathbb{Z}[z]$ is a monic polynomial and $\alpha \in \mathbb{Z}$. (See also [**12**] for some similar results.) For example, Rice proves that if $\varphi(z) \neq z^d$, if 0 is preperiodic for φ, and if $\alpha \in \mathbb{Z}$ has infinite φ-orbit, then $\mathcal{Z}((\varphi^n(\alpha))_{n \geqslant 0})$ is finite. Our Theorems 1 and 7 are generalizations of [**25**] to arbitrary rational maps over number fields.

A key tool in the proof of Theorem 1 is a dynamical analog [**30**] of Siegel's theorem [**29**, IX·3·1] for integral points on elliptic curves. Continuing with the notation from Theorem 1, we define the dynamical canonical height [**31**, section 3·4] of α to be the limit

$$\lim_{n \to \infty} \frac{\log \max\{|A_n|, |B_n|\}}{d^n} = \hat{h}_\varphi(\alpha) > 0.$$

This limit exists by the usual telescoping sequence argument, and the usual proof also shows that positivity is equivalent to the fact that α has infinite orbit. The dynamical analog of Siegel's theorem, which is a far deeper result whose proof uses Roth's theorem, says that A_n and B_n grow at approximately the same rate. More precisely, it is proven in [**30**] that

$$\lim_{n \to \infty} \frac{\log |A_n|}{d^n} = \hat{h}_\varphi(\alpha). \tag{0·1}$$

It is an estimate of the form (0·1) that is needed to prove Theorems 1 and 7.

Of course, there are many situations in which it is easy to prove that (0·1) holds, for example if $\varphi(z) \in \mathbb{Z}[z]$ and $\alpha \in \mathbb{Z}$. In such cases the exact determination of the Zsigmondy set often becomes an elementary exercise, see Example 14 and some of the examples in [**12**, **25**].

Remark 3. The first question that one asks about the Zsigmondy set of a sequence is whether it is finite. Theorems 1 and 7 give an affirmative answer for certain sequences defined by iteration of rational maps on $\mathbb{P}^1$. Assuming that the Zsigmondy sets under consideration are finite, it is also natural to ask for explicit upper bounds for

$$\#\mathcal{Z}(\mathcal{A}) \quad \text{and} \quad \max \mathcal{Z}(\mathcal{A}),$$

where one hopes that the bounds depend only minimally on the sequence. For example, Zsigmondy's original theorem says that for coprime integers $a > b > 0$, we have $\max \mathcal{Z}(a^n - b^n) \leqslant 6$. A recent deep result of Bilu, Hanrot and Voutier [**7**] extends this to the statement the $\max \mathcal{Z}(\mathcal{L}) \leqslant 30$ for any nontrivial Lucas or Lehmer sequence $\mathcal{L}$. In this paper we are content to prove the finiteness of certain dynamical Zsigmondy sets. We leave the question of explicit and/or uniform bounds as a problem for future study.

Remark 4. Tom Tucker has pointed out to the authors that the results of this paper should be valid also for iteration of non-split functions over $\mathbb{C}(T)$, and more generally over one-dimensional function fields of characteristic 0, since in this setting Benedetto [**5**] (for polynomial maps) and Baker [**2**] (for rational maps) have recently proven that points with infinite

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

orbit have strictly positive canonical height. (The Benedetto and Baker results are true in arbitrary characteristic, but we restrict to characteristic 0 because the required Diophantine approximation result [**30**] uses Roth's theorem.)

The material in this paper is divided into two sections. In Section 1 we state and prove our main theorem via a sequence of lemmas, some of which may be of independent interest. Section 2 discusses variants of our main theorem and raises questions, makes conjectures, and indicates directions for further research.

1. *A dynamical Zsigmondy theorem*

In this section we state and prove our main theorem concerning primitive divisors in sequences defined by iteration of certain types of rational functions. We start by recalling that primitive divisors in number fields are most appropriately defined using ideals, rather than elements.

Definition. Let K be a number field and let $\mathcal{A} = (\mathfrak{A}_n)_{n\geqslant 1}$ be a sequence of nonzero integral ideals. A prime ideal $\mathfrak{p}$ is called a *primitive divisor of* $\mathfrak{A}_n$ if

$$\mathfrak{p} \mid \mathfrak{A}_n \qquad \text{and} \qquad \mathfrak{p} \nmid \mathfrak{A}_i \quad \text{for all } 1 \leqslant i < n.$$

The *Zsigmondy set of* $\mathcal{A}$ is the set

$$\mathcal{Z}(\mathcal{A}) = \{n \geqslant 1 : \mathfrak{A}_n \text{ does not have a primitive divisor}\}.$$

We also recall some basic definitions from dynamical systems.

Definition. Let $\varphi(z) \in K(z)$ be a rational function of degree $d \geqslant 2$, which we may view as a morphism $\varphi : \mathbb{P}^1_{\bar{K}} \to \mathbb{P}^1_K$.

A point $\gamma \in \mathbb{P}^1(\bar{K})$ is *periodic for* φ if $\varphi^n(\gamma) = \gamma$ for some $n \geqslant 1$. The smallest such n is called the *φ-period of* γ. A point of φ-period 1 is called a *fixed point*.

Similarly, we say that γ is *preperiodic* if $\varphi^{m+n}(\gamma) = \varphi^m(\gamma)$ for some $n \geqslant 1$ and $m \geqslant 0$. Equivalently, γ is preperiodic if its *φ-orbit* $\{\alpha, \varphi(\alpha), \varphi^2(\alpha), \ldots\}$ is finite.

A point that is not preperiodic, i.e., that has infinite φ-orbit, is called a *wandering point*.

Let γ be a point of φ-period k. We say that φ is *of polynomial type at* γ if there is some $k \geqslant 1$ such that

$$\varphi^k(z) = \gamma + \frac{(z-\gamma)^d}{\psi(z)} \quad \text{for some } \psi(z) \in K[z] \text{with } \psi(\gamma) \neq 0. \tag{1·1}$$

Remark 5. A more intrinsic algebro-geometric definition is that φ is of polynomial type at γ if the map $\varphi^k : \mathbb{P}^1 \to \mathbb{P}^1$ is totally ramified at γ. Equivalently, if $\varphi(z)$ has the form (1·1) and if we move γ to ∞ by conjugating φ by the linear fractional transformation $f(z) = 1/(z-\gamma)$, then the following calculation shows that φ^k becomes a polynomial:

$$\begin{aligned}(f \circ \varphi^k \circ f^{-1})(z) &= \frac{1}{\varphi^k(f^{-1}(z)) - \gamma} = \frac{1}{(f^{-1}(z)-\gamma)^d/\psi(f^{-1}(z))} \\ &= \frac{1}{z^{-d}/\psi(z^{-1}+\gamma)} = z^d\psi(z^{-1}+\gamma) \in K[z].\end{aligned}$$

Remark 6. It is an easy exercise using the Riemann-Hurwitz genus formula to show that if φ is of polynomial type at γ, then the φ-period of γ is at most 2, cf. [**31**, Theorem 1·7]. We will not need to use this fact, but mention it because it provides an easy way to check if there exist any points at which a given map φ is of polynomial type.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

THEOREM 7. *Let K be a number field and let $\varphi(z) \in K(z)$ be a rational function of degree $d \geqslant 2$. Let $\gamma \in K$ be a preperiodic point for φ such that φ is not of polynomial type at γ. Let $\alpha \in K$ be a wandering point, i.e., a point with infinite φ-orbit, and for each $n \geqslant 1$, write the ideal*

$$(\varphi^n(\alpha) - \gamma) = \mathfrak{A}_n \mathfrak{B}_n^{-1}$$

as a quotient of relatively prime integral ideals. (If $\varphi^n(\alpha) = \infty$, we set $\mathfrak{A}_n = (1)$ and $\mathfrak{B}_n = (0)$.) Then the dynamical Zsigmondy set $\mathcal{Z}\big((\mathfrak{A}_n)_{n\geqslant 1}\big)$ is finite.

Remark 8. The assumption in Theorem 7 that φ is not of polynomial type at γ is a necessary condition. For example, let $F(z) \in \mathbb{Z}[z]$ be any polynomial of degree at most d with $F(0) = 1$ and consider the rational map

$$\varphi(z) = z^d / F(z).$$

Then φ is of polyomial type at $\gamma = 0$, and an easy calculation shows that for any starting value $\alpha = A_1/B_1 \in \mathbb{Q}$, we have $A_n = A_1^{d^n}$ for all $n \geqslant 0$. Hence A_n has no primitive divisors for any $n \geqslant 2$.

Proof. We first prove Theorem 7 under the assumption that γ is a periodic point. This is the hardest case. At the end of the proof, we briefly indicate how to modify the argument to handle points that are preperiodic, but not periodic. The proof of Theorem 7 is structured as a series of lemmas that provide the necessary tools.

LEMMA 9. *If Theorem 7 is true when γ is a fixed point of φ, then it is true when γ is a periodic point of φ.*

Proof. Suppose that γ has φ-period $k \geqslant 2$, so $\varphi^k(\gamma) = \gamma$ and no smaller iterate of φ fixes γ. For each $0 \leqslant i < k$ we consider the subsequence

$$(\varphi^{nk+i}(\alpha) - \gamma) = \mathfrak{A}_{nk+i} \mathfrak{B}_{nk+i}^{-1} \quad \text{for } n = 0, 1, 2, \ldots .$$

We claim that these subsequences have very few common prime divisors. More precisely, define the set of good primes $\mathcal{P} = \mathcal{P}_{\varphi,\alpha,\gamma}$ to be primes satisfying the following two conditions:

(A) φ has good reduction at $\mathfrak{p}$. (See [**31**, chapter 2] for the definition and basic properties of maps with good reduction.)

(B) $\varphi^i(\gamma) \not\equiv \gamma \pmod{\mathfrak{p}}$ for all $0 < i < k$.

It is clear that $\mathcal{P}$ contains all but finitely many primes. Now suppose that some $\mathfrak{p} \in \mathcal{P}$ divides terms in different subsequences, say

$$\mathfrak{p} \mid \mathfrak{A}_{nk+i} \quad \text{and} \quad \mathfrak{p} \mid \mathfrak{A}_{mk+j} \quad \text{for some } 0 \leqslant j < i < k. \tag{1·2}$$

Note that the good reduction assumption means that $(\varphi \bmod \mathfrak{p})^n = (\varphi^n) \bmod \mathfrak{p}$, i.e., reduction modulo $\mathfrak{p}$ commutes with composition of φ (see [**31**, Theorem 2·18]). Hence if $\mathfrak{p}$ is a prime of good reduction for φ, then we have

$$\mathfrak{p} \mid \mathfrak{A}_n \iff \varphi^n(\alpha) \equiv \gamma \pmod{\mathfrak{p}}.$$

So we can rewrite assumption (1·2) as

$$\varphi^{nk+i}(\alpha) \equiv \varphi^{mk+j}(\alpha) \equiv \gamma \pmod{\mathfrak{p}}.$$

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

Suppose first that $nk+i > mk+j$. Since $0 \leqslant j < i \leqslant k$ by assumption, this implies that $n \geqslant m$. We compute

$$\begin{aligned}
\gamma &\equiv \varphi^{nk+i}(\alpha) \pmod{\mathfrak{p}} \\
&= \varphi^{(nk+i)-(mk+j)}(\varphi^{mk+j}(\alpha)) \\
&\equiv \varphi^{(nk+i)-(mk+j)}(\gamma) \pmod{\mathfrak{p}} \\
&= \varphi^{i-j}((\varphi^k)^{n-m}(\gamma)) \\
&= \varphi^{i-j}(\gamma) \qquad \text{since } \varphi^k(\gamma) = \gamma.
\end{aligned}$$

But $0 < i - j < k$, so this contradicts Property (B) of $\mathcal{P}$.

Similarly, if $nk + i < mk + j$, then $m > n$ (since $i > j$), so we have

$$\begin{aligned}
\gamma &\equiv \varphi^{mk+j}(\alpha) \pmod{\mathfrak{p}} \\
&= \varphi^{(mk+j)-(nk+i)}(\varphi^{nk+i}(\alpha)) \\
&\equiv \varphi^{(mk+j)-(nk+i)}(\gamma) \pmod{\mathfrak{p}} \\
&= \varphi^{j-i+k}((\varphi^k)^{m-n-1}(\gamma)) \\
&= \varphi^{j-i+k}(\gamma) \qquad \text{since } \varphi^k(\gamma) = \gamma.
\end{aligned}$$

This is again a contradiction of Property (B), since $0 < j - i + k < k$.

We have now proven that for primes $\mathfrak{p} \in \mathcal{P}$, at most one of the subsequences

$$(\mathfrak{A}_{nk+i})_{n\geqslant 0}, \qquad i = 0, 1, \ldots, k-1,$$

has a term divisible by $\mathfrak{p}$.

We are assuming that Theorem 7 is true if γ is a fixed point. It follows that for each $0 \leqslant i < k$, the Zsigmondy set $\mathcal{Z}((\mathfrak{A}_{nk+i})_{n\geqslant 0})$ is finite, since $(\mathfrak{A}_{nk+i})_{n\geqslant 0}$ is the sequence associated to the map φ^k, the initial point $\varphi^i(\alpha)$, and the fixed point γ of φ^k. (Note that the condition that φ is not a polynomial at γ is equivalent to the condition that φ^k is not of polynomial type at γ.)

It follows that we can find a number N so that for all $n \geqslant N$ and all $0 \leqslant i < k$ there is a prime ideal $\mathfrak{p}_{n,i}$ satisfying

$$\mathfrak{p}_{n,i} \mid \mathfrak{A}_{nk+i} \quad \text{and} \quad \mathfrak{p}_{n,i} \nmid \mathfrak{A}_{mk+i} \quad \text{for all } 0 \leqslant m < n.$$

In other words, for a fixed i, the ideals $\mathfrak{p}_{n,i}$ are primitive divisors in the subsequence $(\mathfrak{A}_{nk+i})_{n\geqslant 0}$. Increasing N if necessary, we may assume that $\mathfrak{p}_{n,i} \in \mathcal{P}$ for all n and all i, since the complement of $\mathcal{P}$ is finite.

It is now clear that for $n > N$ and $0 \leqslant i < k$, the prime $\mathfrak{p}_{n,i}$ is a primitive divisor of $\mathfrak{A}_{nk+i}$ in the full sequence $(\mathfrak{A}_m)_{m\geqslant 0}$. This is true because it is a primitive divisor in its own subsequence, and we proved above that it does not divide any of the terms in any of the other subsequences.

We next reduce to the case $\gamma = 0$, which will simplify our later computations.

LEMMA 10. *It suffices to prove Theorem* 7 *under the assumption that* $\gamma = 0$.

Proof. Let $f(z) = z + \gamma$. Then we have

$$\varphi^n(\alpha) - \gamma = f^{-1}(\varphi^n(\alpha)) = (f^{-1} \circ \varphi \circ f)^n(f^{-1}(\alpha)).$$

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

Hence replacing φ by $f^{-1} \circ \varphi \circ f$ and replacing α by $f^{-1}(\alpha)$ allows us to replace γ wtih $f^{-1}(\gamma) = 0$. Finally, we note that φ is of polynomial type at γ if and only if $f^{-1} \circ \varphi \circ f$ is of polynomial type at $f^{-1}(\gamma) = 0$, so the conjugated map has the required property. □

We are now reduced to the case that $\gamma = 0$ is a fixed point of $\varphi(z)$. This means that we can write φ in the form

$$\varphi(z) = \frac{a_e z^e + a_{e+1} z^{e+1} + \cdots + a_d z^d}{b_0 + b_1 z + b_2 z^2 + \cdots + b_d z^d}, \tag{1·3}$$

with

$$a_e \neq 0, \quad b_0 \neq 0, \quad \text{and} \quad e \geqslant 1.$$

Further, without loss of generality, we may assume that all a_i and b_i are in the ring of integers R of K, and since $\deg \varphi = d$, we know that at least one of a_d and b_d is nonzero. Finally, our assumptions that $\varphi(0) = 0$ and that φ is not of polynomial type at 0 imply that

$$0 < e < d. \tag{1·4}$$

Note the strict inequalities on both sides.

We next prove an elementary, but useful, lemma that bounds how rapidly the $\mathfrak{p}$-divisibility of $\mathfrak{A}_n$ can grow, where recall that $\mathfrak{A}_n$ is the integral ideal obtained by writing

$$(\varphi^n(\alpha)) = \mathfrak{A}_n \mathfrak{B}_n^{-1}$$

as a quotient of relatively prime integral ideals. In order to state the result, we need one definition.

Definition. For each prime ideal $\mathfrak{p}$, we define the *rank of apparition* (*of φ and α*) *at* $\mathfrak{p}$ to be the integer

$$r_{\mathfrak{p}} = \min\{r \geqslant 0 : \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_r) > 0\}.$$

(If no such r exists, we set $r_{\mathfrak{p}} = \infty$.) Notice that this is a direct analog of Ward's definition [**32**] of the rank of apparition for elliptic divisibility sequences.

LEMMA 11. *With notation as above, let*

$$S = \{\mathfrak{p} : \operatorname{ord}_{\mathfrak{p}}(a_e b_0) \neq 0\}.$$

Then, for all primes $\mathfrak{p} \notin S$,

$$k \leqslant r_{\mathfrak{p}} \Longrightarrow \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{k-1}) = 0, \tag{1·5}$$

$$k > r_{\mathfrak{p}} \Longrightarrow \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_k) = e \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{k-1}), \tag{1·6}$$

where e is the order of vanishing of $\varphi(z)$ at $z = 0$, see (1·3).

Proof. We note that (1·5) is true by the definition of $r_{\mathfrak{p}}$, so we only need to prove (1·6), which we do by induction on k. Since $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{r_{\mathfrak{p}}}) > 0$ by definition, the inductive hypothesis implies that

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_i) > 0 \quad \text{for all } r_{\mathfrak{p}} \leqslant i < k. \tag{1·7}$$

In particular, $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{k-1}) > 0$.

For notational convenience, we let $\beta = \varphi^{k-1}(\alpha)$. The fact that $\mathfrak{A}_{k-1}$ has positive valuation implies that

$$\operatorname{ord}_{\mathfrak{p}}(\beta) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{k-1}) > 0.$$

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

Further, the assumption that $\mathfrak{p} \notin S$ means that

$$\operatorname{ord}_{\mathfrak{p}}(a_e) = \operatorname{ord}_{\mathfrak{p}}(b_0) = 0,$$

so when we evaluate the numerator and denominator of $\varphi(\beta)$, the lowest degree terms have the strictly smallest $\mathfrak{p}$-adic valuation. Hence the ultrametric triangle inequality gives

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_k) &= \operatorname{ord}_{\mathfrak{p}}(\varphi(\beta)) \\
&= \operatorname{ord}_{\mathfrak{p}}(a_e\beta^e + a_{e+1}\beta^{e+1} + \cdots + a_d\beta^d) \\
&\quad - \operatorname{ord}_{\mathfrak{p}}(b_0 + b_1\beta + \cdots + b_d\beta^d) \\
&= e \operatorname{ord}_{\mathfrak{p}}(\beta) \qquad \text{since } \operatorname{ord}_{\mathfrak{p}}(a_e b_0) = 0 \text{ and } \operatorname{ord}_{\mathfrak{p}}(\beta) > 0. \\
&= e \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{k-1}).
\end{aligned}$$

This completes the proof of Lemma 11.

We next consider the height functions that are needed for proving our main results. In general, if $\beta \in K^*$ and if we write the ideal (β) as a quotient of relatively prime integral ideals $(\beta) = \mathfrak{A}\mathfrak{B}^{-1}$, then the (*normalized logarithmic*) *height* of β is given by the formula

$$h(\beta) = \frac{1}{[K:\mathbb{Q}]} \left(\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{B} + \sum_{v \in M_K^\infty} [K_v : \mathbb{Q}_v] \log \max\{1, |\beta|_v\} \right). \tag{1·8}$$

See for example [**19**, section 3·1]. Using this, we next recall the definition and basic properties of the canonical height associated to φ.

LEMMA 12. *The* canonical height associated to φ *is the function* $\hat{h}_\varphi : \mathbb{P}^1(\bar{K}) \to \mathbb{R}$ *defined by the limit*

$$\hat{h}_\varphi(\beta) = \lim_{n\to\infty} \frac{1}{d^n} h(\varphi^n(\beta)).$$

It satisfies, and is characterized by, the two following properties:

$$\hat{h}_\varphi(\beta) = h(\beta) + O(1) \quad \text{for all } \beta \in \mathbb{P}^1(\bar{K}). \tag{1·9}$$

$$\hat{h}_\varphi(\varphi(\beta)) = d\hat{h}_\varphi(\beta) \quad \text{for all } \beta \in \mathbb{P}^1(\bar{K}). \tag{1·10}$$

The $O(1)$ *constant in* (1·9) *depends on* φ, *but is independent of* β.

The values $\hat{h}_\varphi(\beta)$ *are nonnegative, and*

$$\hat{h}_\varphi(\beta) > 0 \iff \beta \text{ has infinite } \varphi\text{-orbit}.$$

Proof. See [**9**], [**14**, section B·4], or [**31**, section 3·4].

Definition. Let S be a finite set of places of K, including all archimedean places, and let $\mathfrak{A}$ be an integral ideal. The *prime-to-S norm of* $\mathfrak{A}$ is the quantity

$$\mathsf{N}_S\mathfrak{A} = \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}}\mathfrak{A}}.$$

As the name suggests, $\mathsf{N}_S\mathfrak{A}$ is the part of $\mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}$ that is relatively prime to all of the primes in S.

We next apply the main result of [**30**] to show that $\log(\mathsf{N}_S\mathfrak{A}_n)$ grows like a constant multiple of d^n. We observe that the proof of [**30**, theorem E] requires some sort of nontrivial theorem on Diophantine approximation such as Roth's theorem, so despite its simple statement,

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

the following lemma conceals the deepest part of the proof of Theorem 7. For our purposes, we require the general number field version proven in [**30**], but see [**31**, section 3·8] for a more leisurely exposition of the same result over $\mathbb{Q}$ with $S = \{\infty\}$.

We remind the reader that we continue with the assumptions stated in Theorem 7. In particular, the inequality (1·12) in part (b) of the next result is certainly not true if φ is of polynomial type at 0. However, the elementary estimate (1·11) in (a) is a souped-up version of the triangle inequality and is true for all rational maps.

LEMMA 13. (a) *There is a constant $C = C(\varphi, \alpha)$ so that*

$$\frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_n \leqslant d^n \hat{h}_\varphi(\alpha) + C \qquad \text{for all } n \geqslant 0. \tag{1·11}$$

(b) *Let S be a finite set of places, including all archimedean places, and let $\epsilon > 0$. There is an $n_0 = n_0(\epsilon, S, \varphi, \alpha)$ so that*

$$\frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}_S\mathfrak{A}_n \geqslant (1-\epsilon) d^n \hat{h}_\varphi(\alpha) \qquad \text{for all } n \geqslant n_0. \tag{1·12}$$

Proof. (a) We begin by applying the formula (1·8) for the height of an algebraic number β. We take $\beta = \varphi^n(\alpha)^{-1}$, so writing β as a quotient of relatively prime integral ideals $(\beta) = \mathfrak{A}\mathfrak{B}^{-1}$, we have $\mathfrak{B} = \mathfrak{A}_n$. We use the fact that all of the terms in the sum (1·8) are non-negative and the fact that $h(\beta) = h(\beta^{-1})$ for any nonzero β to deduce that

$$h(\varphi^n(\alpha)) \geqslant \frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_n. \tag{1·13}$$

Finally, we use Lemma 12 to compute

$$h(\varphi^n(\alpha)) = \hat{h}_\varphi(\varphi^n(\alpha)) + O(1) = d^n \hat{h}_\varphi(\alpha) + O(1). \tag{1·14}$$

Combining (1·13) and (1·14) completes the proof of (a).

(b) Our assumption that φ is not of polynomial type at 0 allows us to apply [**30**, theorem E]. This theorem implies that for each $v \in S$ we have

$$\lim_{n\to\infty} \frac{\delta_v(\varphi^n(\alpha), 0)}{d^n} = 0, \tag{1·15}$$

where δ_v is a logarithmic v-adic distance function on $\mathbb{P}^1(K_v)$. Since we are measuring the distance to 0, we may take δ_v to be the function

$$\delta_v(\beta, 0) = 1 + \log\left(\frac{\max\{|\beta|_v, 1\}}{|\beta|_v}\right) = 1 + \log \max\{1, |\beta|_v^{-1}\}.$$

(See [**30**, section 3].) Substituting this into (1·15), we obtain the equivalent statement

$$\lim_{n\to\infty} \frac{\log \max\{1, |\varphi^n(\alpha)|_v^{-1}\}}{d^n} = 0. \tag{1·16}$$

We now rewrite (1·8), moving the part of the norm coming from primes in S into the sum. Using our notation for the prime-to-S norm, formula (1·8) becomes

$$h(\beta) = \frac{1}{[K:\mathbb{Q}]}\left(\log \mathsf{N}_S\mathfrak{B} + \sum_{v\in S} [K_v:\mathbb{Q}_v] \log \max\{1, |\beta|_v\}\right). \tag{1·17}$$

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

We apply (1·17) with $\beta = \varphi^n(\alpha)^{-1}$, so $\mathfrak{B} = \mathfrak{A}_n$. Again using $h(\beta) = h(\beta^{-1})$, this gives

$$h(\varphi^n(\alpha)) = \frac{1}{[K:\mathbb{Q}]} \log \mathsf{N}_S \mathfrak{A}_n + \sum_{v \in S} \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]} \log \max\left\{1, |\varphi^n(\alpha)|_v^{-1}\right\}. \tag{1·18}$$

We now divide both sides of (1·18) by d^n and let $n \to \infty$. The limit formula (1·16) tells us that the sum over the places in S goes to 0. On the other hand, the left-hand side of (1·18) is exactly the limit that defines the canonical height. Hence we obtain

$$\hat{h}_\varphi(\alpha) = \lim_{n\to\infty} \frac{1}{[K:\mathbb{Q}]} \frac{\log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{A}_n}{d^n}.$$

This limit implies the lower bound (1·12) that we are trying to prove, which completes the proof of Lemma 13. (It also implies an upper bound, but a weaker upper bound than we obtained by the elementary argument in (a).)

We have assembled all of the tools needed to complete the proof of Theorem 7 in the case that γ is a periodic point. Our goal is to show that $\mathfrak{A}_n$ has a primitive prime divisor for all sufficiently large n. In order to do this, we let S be the union of the set of primes described in Lemma 11 and the set of primes dividing the resultant of the numerator and the denominator of (1·3). (In particular, the rational function φ as defined by (1·3) has good reduction at all $\mathfrak{p} \notin S$.) For this set S we define an ideal

$$\mathfrak{E}_{n,S} := \prod_{\substack{\text{primes } \mathfrak{p} \notin S \text{ that divide} \\ \text{one of } \mathfrak{A}_0, \mathfrak{A}_1, \ldots, \mathfrak{A}_{n-1}}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_n}. \tag{1·19}$$

Similarly, we let $\mathfrak{A}_{n,S}$ be the prime-to-S part of $\mathfrak{A}_n$, thus

$$\mathfrak{A}_{n,S} = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_n}.$$

We will prove that for all sufficiently large n, the ideal $\mathfrak{A}_{n,S}$ is strictly larger than the ideal $\mathfrak{E}_{n,S}$. This will imply the desired result, since it will show that $\mathfrak{A}_n$ has a primitive prime divisor, and indeed a primitive prime divisor not lying in S.

Suppose that $\mathfrak{p} \notin S$ divides $\mathfrak{A}_i$ for some $i < n$. Then $r_{\mathfrak{p}} \leqslant i < n$, so Lemma 11 tells us that

$$\operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_{n-1} > 0 \qquad \text{and} \qquad \operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_n = e \operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_{n-1}.$$

Thus in the product (1·19) defining $\mathfrak{E}_{n,S}$, it suffices to multiply over the primes dividing $\mathfrak{A}_{n-1}$, and we find that

$$\mathfrak{E}_{n,S} = \prod_{\mathfrak{p} \notin S,\ \mathfrak{p} \mid \mathfrak{A}_{n-1}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_n} = \prod_{\mathfrak{p} \notin S,\ \mathfrak{p} \mid \mathfrak{A}_{n-1}} \mathfrak{p}^{e \operatorname{ord}_{\mathfrak{p}} \mathfrak{A}_{n-1}} = \mathfrak{A}_{n-1,S}^e.$$

The upper bound in Lemma 13(a), applied to $\mathfrak{A}_{n-1}$, gives the estimate

$$\begin{aligned} \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{E}_{n,S} &= e \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{A}_{n-1,S} \\ &\leqslant e \log \mathsf{N}_{K/\mathbb{Q}} \mathfrak{A}_{n-1} \\ &\leqslant [K:\mathbb{Q}] e d^{n-1} \hat{h}_\varphi(\alpha) - O(1), \end{aligned} \tag{1·20}$$

where the $O(1)$ depends only on φ, α, and K.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

To obtain the complementary lower bound, we apply Lemma 13(b) to $\mathfrak{A}_n$ with $\epsilon = 1/2d$. This gives

$$\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_{n,S} = \log \mathsf{N}_S\mathfrak{A}_n \geqslant [K:\mathbb{Q}]\left(1-\frac{1}{2d}\right)d^n\hat{h}_\varphi(\alpha), \tag{1·21}$$

valid for $n \geqslant n_0(S,\varphi,\alpha,\gamma)$.

Finally, we combine (1·20) and (1·21) to obtain

$$\begin{aligned}\frac{1}{[K:\mathbb{Q}]}\log\left(\frac{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_{n,S}}{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{E}_{n,S}}\right) &\geqslant \left(1-\frac{1}{2d}\right)d^n\hat{h}_\varphi(\alpha) - ed^{n-1}\hat{h}_\varphi(\alpha) + O(1)\\ &\geqslant \frac{1}{2}d^{n-1}\hat{h}_\varphi(\alpha) + O(1), \quad \text{since } e < d \text{ from (1·4)}.\end{aligned}$$

The right-hand side is positive for all sufficiently large n, which completes the proof that $\mathfrak{A}_n$ has a primitive divisor for all sufficiently large n, and hence that the Zsigmondy set $\mathcal{Z}\big((\mathfrak{A}_n)_{n\geqslant 1}\big)$ is finite.

In order to complete the proof of Theorem 7, it remains to consider the case that γ is preperiodic, but not periodic. This case turns out to be easier to treat, because the terms in the sequence $(\mathfrak{A}_n)_{n\geqslant 1}$ are essentially relatively prime, i.e., there are only finitely many primes dividing more than one term in the sequence.

To see this, let

$$m = \#\{\varphi^i(\gamma) : i \geqslant 0\}$$

be the number of distinct points in the orbit of γ. Thus

$$\gamma, \varphi(\gamma), \varphi^2(\gamma), \ldots, \varphi^{m-1}(\gamma)$$

are distinct, and for every $k \geqslant 1$ there is some $1 \leqslant j < m$ such that $\varphi^k(\gamma) = \varphi^j(\gamma)$. (The assumption that γ is not periodic ensures that j is strictly positive.)

Let S be the union of the set of primes of bad reduction of φ and the primes that occur to a positive power in any of the ideals

$$(\varphi^j(\gamma) - \gamma) \quad \text{for } 1 \leqslant j < m.$$

Clearly S is a finite set of primes. We claim that if $\mathfrak{p}$ is a prime ideal of good reduction for φ and if $\mathfrak{p}$ divides more than one $\mathfrak{A}_i$, then $\mathfrak{p} \in S$. To see this, suppose that $\mathfrak{p} \mid \mathfrak{A}_n$ and $\mathfrak{p} \mid \mathfrak{A}_k$ with $k > n \geqslant 1$. This implies that

$$\varphi^n(\alpha) \equiv \gamma \pmod{\mathfrak{p}} \qquad \text{and} \qquad \varphi^k(\alpha) \equiv \gamma \pmod{\mathfrak{p}},$$

and hence that

$$\gamma \equiv \varphi^k(\alpha) \equiv \varphi^{k-n}\big(\varphi^n(\alpha)\big) \equiv \varphi^{k-n}(\gamma) \pmod{\mathfrak{p}}. \tag{1·22}$$

As indicated earlier, the preperiodicity of γ tells us that we can find some $1 \leqslant j < m$ satisfying $\varphi^j(\gamma) = \varphi^{k-n}(\gamma)$. It follows from (1·22) that $\gamma \equiv \varphi^j(\gamma) \pmod{\mathfrak{p}}$, and hence that $\mathfrak{p} \in S$.

Continuing with this finite set of primes S, we observe that the ideal $\mathfrak{E}_{n,S}$ given by (1·19) satisfies $\mathfrak{E}_{n,S} = (1)$. Hence the lower bound for $\log \mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_{n,S}$ in (1·21) is also a lower bound for

$$\log\left(\frac{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{A}_{n,S}}{\mathsf{N}_{K/\mathbb{Q}}\mathfrak{E}_{n,S}}\right).$$

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

The lower bound in (1·19) is clearly positive, and hence $\mathfrak{A}_n$ has a primitive divisor for all $n \geqslant n_0(S, \varphi, \alpha, \gamma)$.

Remark 14. The proof for preperiodic γ works precisely because there are only finitely many primes for which γ becomes periodic. This fails for wandering points, which are presumably periodic modulo $\mathfrak{p}$ for infinitely many primes.

Example 15. It is easy to construct specific examples, and even families of examples, for which one can find the full dynamical Zsgimondy set by an elementary calculation. We illustrate with one such example, see [**12**, **25**] for others.

Let $\varphi(z) = z^2 + z$, let $\gamma = 0$, and let $\alpha \in \mathbb{Q}$ with $\alpha > 0$. Then for all $n \geqslant 1$ we have $\gcd(A_{n-1}, B_{n-1}) = 1$ and

$$\frac{A_n}{B_n} = \frac{A_{n-1}^2 + A_{n-1}B_{n-1}}{B_{n-1}^2},$$

so $A_n = A_{n-1}^2 + A_{n-1}B_{n-1}$ and $B_n = B_{n-1}^2$. In particular,

$$A_0 \mid A_1 \mid A_2 \mid \cdots$$

so A_n has a primitive prime divisor if and only if there is a prime $p \mid A_n$ with $p \nmid A_{n-1}$. But from $A_n = A_{n-1}(A_{n-1} + B_{n-1})$, this means that A_n has a primitive prime divisor if and only if $A_{n-1} + B_{n-1} > 1$. This is true for every $n \geqslant 1$, so it follows that $\mathcal{Z}\big((A_n)_{n\geqslant 1}\big) = \varnothing$.

2. *Questions and speculations*

It is interesting to ask to what extent one can relax or modify the hypotheses in Theorem 7. We discuss this question in a series of remarks.

Remark 16. If $\mathfrak{A}_n$ is a classical divisibility sequence associated to a (possibly twisted) multiplicative group or to an elliptic curve, then the higher order $\mathfrak{p}$ divisibility can be described quite precisely via properties of the formal group of the group variety. Roughly speaking, if $\mathfrak{A}_r$ is the first term divisible by $\mathfrak{p}$, then

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{kr}) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_r) + \operatorname{ord}_{\mathfrak{p}}(k) \quad \text{for all } k \geqslant 1, \tag{2·1}$$

and no other terms are divisible by $\mathfrak{p}$. The proof of (2·1) (see, e.g., [**28**, equation (13)]) is essentially $\mathfrak{p}$-adic in nature, and indeed it holds for classical divisibility sequences defined over the $\mathfrak{p}$-adic completion $K_{\mathfrak{p}}$ of K. We note that the estimate (2·1) forms an essential, albeit reasonably elementary, component of the proof that classical Zsigmondy sets are finite.

In the proof of our main theorem, Lemma 11 plays the role of (2·1), but note that Lemma 11, which implies that

$$\operatorname{ord}_{\mathfrak{p}}\mathfrak{A}_{\mathfrak{k}} = e^{k-r}\operatorname{ord}_{\mathfrak{p}}\mathfrak{A}_r,$$

is only valid for primes outside a certain bad set S. It is natural to ask if the dynamical analog of (2·1) is true over $K_{\mathfrak{p}}$, since that might lead to a better understanding of the underlying dynamics. The answer is probably not. Rob Benedetto (private communication) has sketched an argument using ideas from [**4**, **6**] which suggests that there are dynamical examples over $\mathbb{Q}_p$ with γ periodic such that $\operatorname{ord}_p\mathfrak{A}_n$ grows extremely rapidly, for example faster than $O(d^n)$, or even faster than $O(2^{d^n})$.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

This is in marked contrast to the situation over a number field, where the elementary height estimate

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}}\varphi^n(\alpha)\log \mathsf{N}\mathfrak{p} \leqslant \log \mathsf{N}\mathfrak{A}_n &\leqslant [K:\mathbb{Q}]h\big(\varphi^n(\alpha)\big)\\ &= [K:\mathbb{Q}]\hat{h}_\varphi(\varphi^n(\alpha)) + O(1) = d^n[K:\mathbb{Q}]\hat{h}_\varphi(\alpha) + O(1)\end{aligned}$$

shows that $\operatorname{ord}_{\mathfrak{p}}\varphi^n(\alpha)$ cannot grow faster than $O(d^n)$.

Remark 17. If we change the assumptions of Theorem 7 to make γ a wandering point, then Zsigmondy-type theorems appear to be more difficult to prove. Note that when stripped to their essentials, proofs of Zsigmondy-type theorems have two main ingredients:

(i) prove that the sequence $\mathfrak{A}_n$ grows very rapidly,

(ii) prove that once a prime $\mathfrak{p}$ divides some term in the sequence, it cannot divide later terms to an extremely high power.

Condition (i) is a global condition, and it is true for both preperiodic and wandering γ. This may be proved using [**30**, theorem E] as we did in the proof of Lemma 13. Indeed, the proof of Lemma 13 only uses the assumption that φ is not of polynomial type at γ, it does not require that γ be a preperiodic point.

Thus the difficulty in proving a Zsigmondy-type theorem for wandering γ is Condition (ii). As noted in Remark 16, classical multiplicative or elliptic divisibility sequences satisfy

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{kr}) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_r) + \operatorname{ord}_{\mathfrak{p}}(k),$$

where r is the rank of apparition at $\mathfrak{p}$. However, in the dynamical setting there is no analogous uniform result with γ wandering, and indeed it is easy to construct examples in which $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_{kr})$ is arbitrarily much larger than $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_r)$. For example, let

$$\gamma = 0, \quad \alpha = p, \quad \text{and} \quad \varphi(z) = z^2 - pz + p^e.$$

Then

$$\operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_0) = \operatorname{ord}_{\mathfrak{p}}(\alpha) = 1 \quad \text{and} \quad \operatorname{ord}_{\mathfrak{p}}(\mathfrak{A}_1) = \operatorname{ord}_{\mathfrak{p}}(p^e) = e.$$

Remark 18. Our main theorem is really about primes $\mathfrak{p}$ such that the reduction modulo $\mathfrak{p}$ of a wandering point α coincides with a given periodic point γ. This is a natural question, but it is possibly not the most natural generalization of the classical multipicative and elliptic divisibility sequences. In the classical case, one studies the order of α modulo $\mathfrak{p}$ for varying primes ideals $\mathfrak{p}$, which means the order of α mod $\mathfrak{p}$ as a torsion point in the underlying group. The dynamical analog of the set of torsion points is the set of preperiodic points, so a natural dynamical analog of the classical Zsigmondy theorems would be to look at primitive prime divisors in the sequence

$$\varphi^n(\alpha) - \alpha, \qquad \text{or, more generally,} \quad \varphi^{m+n}(\alpha) - \varphi^m(\alpha).$$

We formulate two primitive divisor conjectures, analogous to Theorem 7, corresponding to these situations.

CONJECTURE 19. *Let K be a number field, let $\varphi(z) \in K(z)$ be a rational function of degree $d \geqslant 2$, and let $\alpha \in K$ be a φ-wandering point. For each $n \geqslant 1$, write the ideal*

$$(\varphi^n(\alpha) - \alpha) = \mathfrak{A}_n\mathfrak{B}_n^{-1}$$

as a quotient of relatively prime integral ideals. Then the dynamical Zsigmondy set $\mathcal{Z}\big((\mathfrak{A}_n)_{n\geqslant 1}\big)$ is finite.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

Note that as discussed in Remark 17, there is no problem with the growth of $\mathsf{N}\mathfrak{A}_n$. However, there is the potential problem of primes reappearing in the sequence to very high powers. For example, if we take $\varphi(z) = p - z + p^e z^2$ and $\alpha = 0$, then

$$\varphi(\alpha) = p \quad \text{and} \quad \varphi^2(\alpha) = \varphi(p) = p^{e+2}.$$

In order to state the second conjecture, we need to extend the definition of Zsigmondy sets to doubly indexed sequences.

Definition. Let

$$(\mathfrak{A}_{m,n})_{\substack{m\geqslant 1\\ n\geqslant 0}}$$

be a doubly indexed sequence of ideals. We say that $\mathfrak{p}$ is a *primitive prime divisor* of $\mathfrak{A}_{m,n}$ if

$$\mathfrak{p} \mid \mathfrak{A}_{m,n} \quad \text{and} \quad \mathfrak{p} \nmid \mathfrak{A}_{i,j} \quad \text{for all } i \text{ and } j \text{ with } 0 \leqslant i < m \text{ or } 1 \leqslant j < n.$$

The we define the *Zsigmondy set* $\mathcal{Z}(\mathfrak{A}_{m,n})$ to be the set

$$\{(m,n) : n \geqslant 1,\ m \geqslant 0, \text{ and } \mathfrak{A}_{m,n} \text{ has no primitive divisors}\}.$$

CONJECTURE 20. *Let K be a number field, let $\varphi(z) \in K(z)$ be a rational function of degree $d \geqslant 2$, and let $\alpha \in K$ be a φ-wandering point. For each $n \geqslant 1$ and $m \geqslant 0$, write the ideal*

$$(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = \mathfrak{A}_{m,n}\mathfrak{B}_{m,n}^{-1} \tag{2·2}$$

as a quotient of relatively prime integral ideals. Then the dynamical Zsigmondy set $\mathcal{Z}(\mathfrak{A}_{m,n})$ is finite.

Remark 21. In the classical multiplicative and elliptic Zsigmondy theorems, every prime divides some term of the sequence, but this is (probably) not true for (most) dynamically defined sequences. In some nontrivial dynamical cases, various authors [**18**, **20**, **21**] have proven that

$$\{\mathfrak{p} : \mathfrak{p} \mid \mathfrak{A}_n \text{ for some } n\}$$

is a set of density 0. See also [**27**] for a weak lower bound on the number of primes in this set.

On the other hand, it is clear that every prime divides at least one term in the doubly indexed dynamical sequence $\mathfrak{A}_{m,n}$ defined by (2·2). In particular, if φ has good reduction at $\mathfrak{p}$, then $\mathfrak{p} \mid \mathfrak{A}_{m,n}$ if and only if the orbit of α modulo $\mathfrak{p}$ has a tail of length m and a cycle of length n.

Acknowledgements. The authors would like to thank Rob Benedetto for sketching the construction described in Remark 16, and Graham Everest, Igor Shparlinski and Tom Tucker for their helpful comments on the initial draft of this paper.

REFERENCES

[**1**] S. A. ARIF and F. S. ABU MURIEFAH. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory* **95**(1) (2002), 95–100.
[**2**] M. BAKER. A finiteness theorem for canonical heights attached to rational maps over function fields (2005) `ArXiv:math.NT/0601046`.
[**3**] A. S. BANG. Taltheoretiske Undersogelser. *Tidsskrift Mat.* **4**(5) (1886), 70–80, 130–137.
[**4**] R. L. BENEDETTO. Examples of wandering domains in p-adic polynomial dynamics. *C. R. Math. Acad. Sci. Paris* **335**(7) (2002), 615–620.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press

[5] R. L. BENEDETTO. Heights and preperiodic points of polynomials over function fields. *Int. Math. Res. Not.* **62** (2005), 3855–3866.
[6] R. L. BENEDETTO. Wandering domains in non-Archimedean polynomial dynamics. *Bull. London Math. Soc.* **38**(6) (2006), 937–950.
[7] Y. 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.
[8] G. D. BIRKHOFF and H. S. VANDIVER. On the integral divisors of $a^n - b^n$. *Ann. of Math.* (2) **5**(4) (1904), 173–180.
[9] G. S. CALL and J. H. SILVERMAN. Canonical heights on varieties with morphisms. *Compositio Math.* **89**(2) (1993), 163–205.
[10] R. D. CARMICHAEL. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math.* (2) **15**(1–4) (1913/14), 30–48.
[11] G. EVEREST, G. MCLAREN and T. WARD. Primitive divisors of elliptic divisibility sequences. *J. Number Theory* **118**(1) (2006), 71–89.
[12] A. FLATTERS. Arithmetic dynamics of rational maps. preliminary manuscript (July 9, 2007).
[13] D. GHIOCA and T. TUCKER. Equidistribution and integral points for Drinfeld modules (2006). ArXiv:math.NT.0609120.
[14] M. HINDRY and J. H. SILVERMAN. *Diophantine Geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics* (Springer-Verlag, 2000).
[15] L.-C. HSIA. On the reduction of a non-torsion point of a Drinfeld module (2006). Preprint, NSC 90-2115-M-008-016.
[16] P. INGRAM. Elliptic divisibility sequences over certain curves. *J. Number Theory* **123**(2) (2007), 473–486.
[17] P. INGRAM and J. H. SILVERMAN. Uniform estimates for primitive divisors in elliptic divisibility sequences. Volume in honor of Serge Lang (Springer-Verlag), to appear.
[18] R. JONES. The density of prime divisors in the arithmetic dynamics of quadratic polynomials (2006). ArXiv:math.NT/0612415.
[19] S. LANG. *Fundamentals of Diophantine Geometry* (Springer-Verlag, 1983).
[20] R. W. K. ODONI. The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc.* (3) **51**(3) (1985), 385–414.
[21] R. W. K. ODONI. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. London Math. Soc.* (2) **32**(1) (1985), 1–11.
[22] B. POONEN. Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers. In *Algorithmic number theory (Sydney*, 2002), *Lecture Notes in Comput. Sci.* vol. 2369 (Springer, 2002), pp 33–42.
[23] L. P. POSTNIKOVA and A. SCHINZEL. Primitive divisors of the expression $a^n - b^n$ in algebraic number fields. *Mat. Sb.* (N.S.) **75**(117) (1968), 171–177.
[24] C. E. PRAEGER. Primitive prime divisor elements in finite classical groups. In *Groups St. Andrews* 1997 *in Bath, II. London Math. Soc. Lecture Note Ser.* vol. 261 (Cambridge University Press, 1999), pp 605–623.
[25] B. RICE. Primitive prime divisors in polynomial arithmetic dynamics. *Integers (electronic)*, **7:A26** (2007), 16 pages.
[26] A. SCHINZEL. Primitive divisors of the expression $A^n - B^n$ in algebraic number fields. *J. Reine Angew. Math.* **268/269** (1974), 27–33.
[27] I. E. SHPARLINSKIĬ. The number of different prime divisors of recurrent sequences. *Mat. Zametki* **42**(4) (1987), 494–507, 622.
[28] J. H. SILVERMAN. Wieferich's criterion and the *abc*-conjecture. *J. Number Theory* **30**(2) (1988), 226–237.
[29] J. H. SILVERMAN. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics, vol. 106 (Springer-Verlag, 1992).
[30] J. H. SILVERMAN. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.* **71**(3) (1993), 793–829.
[31] J. H. SILVERMAN. *The Arithmetic of Dynamical Systems*. Graduate Texts in Mathematics, vol. 241 (Springer-Verlag, 2007).
[32] M. WARD. Memoir on elliptic divisibility sequences. *Amer. J. Math.* **70** (1948), 31–74.
[33] K. ZSIGMONDY. Zur Theorie der Potenzreste. *Monatsh. Math. Phys.* **3**(1) (1892), 265–284.

https://doi.org/10.1017/S0305004108001795 Published online by Cambridge University Press