Primitive Prime Divisors for Unicritical Polynomials

BY

HOLLY KRIEGER

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Chicago, 2013

Chicago, Illinois

Defense Committee:

Ramin Takloo-Bighash, Chair and Coadvisor
Laura DeMarco, Coadvisor
Izzet Coskun
Majid Hadian-Jazi
Sarah Koch, Harvard University

ACKNOWLEDGMENTS

I am privileged to have worked with two advisors who were uncommonly generous with their time and support. Laura DeMarco contributed significantly to the development of this thesis with her thoughtful guidance and inspiring talent, as well as her personal support and enthusiasm. Ramin Takloo-Bighash provided invaluable teaching and mathematical insight throughout the work of this thesis, in addition to his excellent advice and advocacy during the last few years.

Conversations with many others contributed to this thesis, and among them I thank Mike Bennett, Yann Bugeaud, Xander Faber, Patrick Ingram, Joe Silverman, and Tom Tucker. For my mathematical development I owe thanks especially to Izzet Coskun, an enthusiastic teacher who provided many hours of valuable discussion; to Dave Marker, for his encouragement and thoughtful instruction; and to Mihnea Popa, a superb teacher who gave generously of his time and talents.

Special thanks are due to Rick Laugesen - without his advice and example I would never have become a mathematician. I also owe special thanks to my office-mate, collaborator, and dear friend James Freitag, as well as to Paul Reschke and Karen Zaya, for the hours of great conversation, mathematical and otherwise.

Finally, my thanks to those for whom superlatives cannot suffice: Bill Krieger, Amy Evans, Michael Drago, and Ed Thomson.

TABLE OF CONTENTS

SUMMARY

The present work studies the arithmetic of sequences associated to dynamical systems, with the goal of understanding the number-theoretic properties of forward orbits of dynamical systems over a number field K. Given a morphism $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ and a point $z \in \mathbb{P}^1(K)$, our main object of interest will be the Zsigmondy set associated to the forward orbit of z: roughly speaking, the set of those $n \in \mathbb{N}$ such that $\phi^n(0)$ fails to have a prime divisor which does not appear as a divisor of any previous element of the orbit.

Bang (1) and Zsigmondy (2) proved the finiteness and provided an explicit computation for the Zsigmondy set of $a^n - 1$, $a \in \mathbb{Z}$ a nonzero nonunit. It is known that many other dynamically defined sequences, such as Lucas sequences (3), elliptic divisibility sequences (4), and forward orbits under certain rational maps (5), have finite Zsigmondy set. Under the hypothesis of the *abc*-conjecture, Gratton, Nguyen, and Tucker (6) have shown the finiteness of the Zsigmondy set associated to forward orbits under a general rational map $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$. These results on Zsigmondy sets have been used to prove a dynamical Brauer-Manin criterion for $\mathbb{P}^1(K)$ (7), as well as non-Archimedean convergence of Newton's method (8).

We consider the Zsigmondy set associated to critical orbits of polynomials, deducing both finiteness (independent of abc) and effective bounds of such orbits. We focus in particular on the critical orbit of $z^d + c$ for $c \in \mathbb{Q}$; in this case, the elements of the Zsigmondy set are closely

connected to the location of c in the generalized Mandelbrot set, and the question of hyperbolicity of $z^d + c$. The study of these sets is also closely related to the Diophantine approximation of certain algebraic numbers, and the famous theorems of Mahler, Roth, Thue, and Siegel can be used, with refinement, to great effect in the study of Zsigmondy sets.

We turn to a summary of the content of the chapters of this thesis. The beginning of each chapter contains more detailed background for the explicit problems involved therein, so this should be treated as a preliminary introduction.

After a brief description of the main arithmetic and number theoretic objects involved, given in the first chapter, we begin in Chapter 2 by considering the primitive divisors of a critical orbit of a polynomial $f(z)$ defined over a number field K, and give an arithmetic criterion for the failure of an iterate $f^n(z)$ to have a primitive prime divisor. We use a dynamical Diophantine approximation theorem of Silverman (9) to deduce that the Zsigmondy set associated to the orbit is finite.

In Chapter 3, we consider the more detailed problem of an effective computation of the size of the Zsigmondy set associated to the critical orbit of $z^d + c$, focusing our attention on $c \in \mathbb{Q}$. We connect the Zsigmondy question to a question in Diophantine approximation, and use a result of Mahler (10) to bound the size of the Zsigmondy set independent of choice of d and c. Chapter 4 improves this bound by improving the Diophantine approximation result, and

also provides a bound on the largest element of the Zsigmondy set via an effective Diophantine approximation using linear forms in logarithms due to Bennett and Bugeaud (11).

In Chapter 5, we consider the Zsigmondy question from a complex-dynamical point of view, and produce a bound on the recurrence of the critical orbit for $z^d + c$ in terms of the proximity of c in the generalized Mandelbrot set to any center of a hyperbolic component. This bound is then utilized to effectively compute the Zsigmondy set of the critical orbit of $z^d + c$ for a large class of $c \in \mathbb{Q}$.

As a final remark to the reader, we note that the content of Chapters 3, as well as an outline of Chapter 5 in the case $d = 2$, appears in (12). The related question of S-units in forward orbits is considered by the author in joint work with Levin, Scherr, and Tucker (13).

CHAPTER 1

INTRODUCTION

In this chapter, we review the basic definitions and fundamental results concerning the arithmetic of rational maps of $\mathbb{P}^1$. We recall the canonical height associated to a dynamical system over a number field, and discuss the Zsigmondy set associated to a sequence. Chapter 3 of Silverman (14) is an excellent reference for the material of Section 1.1, and we follow this notation.

1.1 Arithmetic of dynamical systems

Given a number field K, write M_K for the set of places of K, with M_∞ denoting the infinite places. Given $v \in M_K$, we write $n_v = [K_v : \mathbb{Q}_v]$ for the local degree of v. Given $P = [x_0 : x_1] \in \mathbb{P}^1(K)$ we define the **height** of P by

$$H(P) := \left(\prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v\}^{n_v} \right)^{\frac{1}{[K:\mathbb{Q}]}}.$$

The height is independent of choice of coordinates of P (and the choice of number field containing P), and invariant under the action of $\mathrm{Gal}(\bar{K}/K)$. We define the **logarithmic height** of P to be

$$h(P) := \log H(P).$$

Given a rational map $\phi \in K(z)$ of degree d, we consider ϕ as a degree d morphism $\mathbb{P}^1(K) \to \mathbb{P}^1(K)$. We define the **canonical height function (associated to ϕ)**:

$$\hat{h}_\phi(P) := \lim_{n\to\infty} \frac{1}{d^n} h(\phi^n(P)).$$

Theorem 1.1.1 (Call and Silverman (15))**.** *Suppose $\phi : \mathbb{P}^1(\bar{\mathbb{Q}}) \to \mathbb{P}^1(\bar{\mathbb{Q}})$ has degree $d \geq 2$. Then the canonical height $\hat{h}_\phi(P)$ exists for all $P \in \mathbb{P}^1(\bar{\mathbb{Q}})$, and is the unique function $\hat{h}_\phi : \mathbb{P}^1(\bar{\mathbb{Q}}) \to \mathbb{R}$ satisfying*

(1) $\hat{h}_\phi(P) = h(P) + \mathcal{O}(1)$; and

(2) $\hat{h}_\phi(\phi(P)) = d\hat{h}_\phi(P)$.

We will occasionally abuse notation, and write $h(\alpha)$ or $\hat{h}_\phi(\alpha)$ for $\alpha \in K$ by taking the restriction with the usual point at infinity of $\mathbb{P}^1(K)$. The canonical height decomposes as a sum of local height functions; in the case of polynomials $\phi(z) \in K[z]$, the decomposition can be explicitly written for all $P \neq \infty$ as

$$\hat{h}_\phi(P) = \sum_{v\in M_K} n_v \hat{h}_{\phi,v}(P),$$

where

$$\hat{h}_{\phi,v}(P) = \lim_{n\to\infty} \frac{1}{d^n} \log\max\{|\phi^n(P)|_v, 1\}.$$

For $n \in \mathbb{N}$, we denote by ϕ^n the nth iterate under composition of ϕ with itself, and write ϕ^0 for the identity map by convention. We define the **forward orbit of** P to be the (ordered) sequence $\mathcal{O}_\phi(P) = \{\phi^n(P)\}_{n\geq 1}$. $P \in \mathbb{P}^1(K)$ is **periodic** if $\phi^n(P) = P$ for some $n \geq 1$, and **preperiodic** some element of the forward orbit is periodic (and so the values of the forward orbit are a finite set). The canonical height provides an arithmetic criterion for preperiodicity:

Proposition 1.1.2. *With ϕ and P as above, we have P preperiodic if and only if $\hat{h}_\phi(P) = 0$.*

Note that when ϕ is the power map, the canonical height is the usual Weil height, and so this is the well-known theorem of Kronecker that points of zero height are roots of unity. Additionally, this tells us that for any non-preperiodic point P, the height of the elements of the forward orbit will eventually grow like d^n, an important idea which will be made more precise for our use in Chapters 2 and 3.

1.2 Primitive prime divisors and Zsigmondy sets

Given a number field K, we write $\mathcal{O}_K$ for the ring of integers of K, and recall that any fractional ideal $\mathfrak{o}$ of K can be written uniquely in the form

$$\mathfrak{o} = \mathfrak{a}\mathfrak{b}^{-1},$$

where $\mathfrak{a}$ and $\mathfrak{b}$ are coprime ideals of $\mathcal{O}_K$, each with a unique factorization into prime ideals. Given a sequence $\{\mathfrak{a}_n\}$ of ideals of $\mathcal{O}_K$, we say that a prime ideal $\mathfrak{p}$ is a **primitive prime**

divisor of an element $\mathfrak{a}_n$ if $\mathfrak{p} \mid \mathfrak{a}_\mathfrak{n}$, and $\mathfrak{p} \nmid \mathfrak{a}_k$ for all $k < n$. We define the **Zsigmondy set** of the sequence to be

$$\mathcal{Z}(\{\mathfrak{a}_n\}) = \{n \in \mathbb{N} : \mathfrak{a}_n \text{ fails to have a primitive prime divisor}\}.$$

In the case when $\mathcal{O}_K$ is a principal ideal domain (in particular, for $K = \mathbb{Q}$), we will often refer to the Zsigmondy set of a sequence of integral elements, referring to prime divisors in the obvious sense.

A final remark: in our case, we will be concerned with the Zsigmondy set of the sequence of ideals

$$\mathfrak{a}_n \mathfrak{b}_n^{-1} = (f^n(\alpha) - \alpha)\mathcal{O}_K$$

associated to iteration of some polynomial map $f \in K[z]$. In this setting, a primitive prime divisor can be understood in the following geometric sense: a prime $\mathfrak{p}$ is a primitive prime divisor of $\mathfrak{a}_\mathfrak{n}$ if and only if $\mathfrak{p}$ is a prime of good reduction for f such that the reduced map $\tilde{f}$ has the reduced point $\tilde{\alpha}$ as a point of exact period n. This geometric interpretation leads to interesting questions generalizing this work of this thesis to settings other than $\mathfrak{P}^1$, but will not be expanded upon here.

CHAPTER 2

INEFFECTIVE RESULTS

2.1 Introduction

In this chapter, we consider the question of primitive prime divisors of critical orbits of polynomial maps over a number field K. We relate the existence of these primitive prime divisors to an arithmetic inequality, and utilize results on dynamical height functions, dependent on Roth's theorem, to prove that the Zsigmondy set of a critical orbit of a polynomial is finite. In particular, we show:

Theorem 2.1.1. *Let K be a number field, $f \in K[z]$, and $\alpha \in K$ with $f'(\alpha) = 0$ and infinite forward orbit. Write*

$$(f^n(\alpha) - \alpha) = \mathfrak{a}_n \mathfrak{b}_n^{-1}$$

with $\mathfrak{a}_n$ and $\mathfrak{b}_n$ coprime ideals. Then $\mathcal{Z}(\mathfrak{a}_n)$ is a finite set.

We first note that without loss of generality, we can by conjugation take the critical point to be 0:

Lemma 2.1.2. *Let $f \in K[z]$, $\alpha \in K$ such that $f'(\alpha) = 0$, and α has infinite forward orbit. Then for all $n \geq 1$,*

$$f^n(\alpha) - \alpha = g^n(0),$$

where $g(z) = f(z + \alpha) - \alpha$, and 0 is a critical point of g with infinite forward g-orbit.

Therefore throughout we will assume the critical point is 0, and so we consider the sequence

$$f^n(0) = \mathfrak{a}_n \mathfrak{b}_n^{-1};$$

and we will denote the associated Zsigmondy set by $\mathcal{Z}(f)$.

The idea of the proof is the following: firstly, as we know by 1.1.1, the arithmetic complexity (height) of the iterates $f^n(0)$ grows quickly. Secondly, once a prime divides some $\mathfrak{a}_k$ with positive order $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_k)$, then $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_n) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_k)$ for all n (in particular, the sequence has rigid divisibility). Therefore, to account for the growing arithmetic complexity, new prime divisors must appear. We make the notion of rigid divisibility clear and use it to find an arithmetic description of $n \in \mathcal{Z}(f)$ in Section 2.2, and make precise the growth of the arithmetic complexity to prove Theorem 2.1.1 in Section 2.3.

2.2 An arithmetic criterion

Let $\{\mathfrak{a}_n\}_{n\in\mathbb{N}}$ be a sequence of integral ideals of $\mathcal{O}_K$, and S a finite set of places, including all archimedean ones. We say that the sequence is an S**-rigid divisibility sequence** if it satisfies the following conditions:

(1) $\forall \mathfrak{p} \notin S$ and all $m, n \in \mathbb{N}$, $\mathfrak{p} \mid \gcd(\mathfrak{a}_n, \mathfrak{a}_m) \Rightarrow \mathfrak{p} \mid \mathfrak{a}_{\gcd(m,n)}$.

(2) $\forall \mathfrak{p} \notin S$ and all $m \in \mathbb{N}$ with $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_m) > 0$, we have $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_{km}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_m)$ for all $k \geq 1$.

Since $f(z) \in K[z]$ is a polynomial, the prime divisors of the sequence $\mathfrak{b}_n$ lie in a finite set; let S be the collection of these finite primes, along with the archimedean places.

Lemma 2.2.1. *Let $f(z) \in K[z]$ such that $f'(0) = 0$, and 0 has infinite forward orbit. Define S as above. Then $\mathfrak{a}_n$ is an S-rigid divisibility sequence.*

Proof. By choice of S, note that for all $\mathfrak{p} \notin S, \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}_n) = \operatorname{ord}_{\mathfrak{p}}(f^n(0))$. Suppose then that $\mathfrak{p} \notin S$, and $\mathfrak{p}$ appears as a divisor of some $\mathfrak{a}_n$. Write $k = k(\mathfrak{p})$ for the minimal k such that $\mathfrak{p} \mid \mathfrak{a}_k$. For $m \geq 1$, let $g_m(z)$ be the polynomial defined by $f^m(z) = z g_m(z) + f^m(0)$, noting that $g_m(0) = (f^m)'(0) = 0$ for all m.

For all $q \geq 1$, we have

$$f^{qk}(0) = f^{(q-1)k}(0) g_k(f^{k(q-1)}(0)) + f^k(0),$$

so by induction, we have $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}_{qk}) = \operatorname{ord}_{\mathfrak{p}}(\mathfrak{a}_k)$, and the second condition is satisfied. Similarly, for all $q \geq 1$ and $0 < r < k$, we have

$$f^{qk+r}(0) = f^{qk}(0) g_r(f^{qk}(0)) + f^r(0),$$

so $\mathfrak{p} \nmid \mathfrak{a}_{qk+r}$. Therefore, if $\mathfrak{p} \notin S$ and $\mathfrak{p} \mid \gcd(\mathfrak{a}_n, \mathfrak{a}_m)$, we have $k(\mathfrak{p}) \mid m$ and $k(\mathfrak{p}) \mid n$, so $k(\mathfrak{p}) \mid \gcd(m, n)$, and so $\mathfrak{p} \mid \mathfrak{a}_{\gcd(m,n)}$.

$\square$

As in (5), we define the **prime-to-S norm** of an ideal $\mathfrak{a}$ to be

$$\mathcal{N}_S(\mathfrak{a}) = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})}.$$

The S-rigid divisibility of the sequence $\{\mathfrak{a}_n\}$ yields a nice characterization of $n \in \mathcal{Z}(f)$ in terms of the prime-to-S norms of the sequence:

Corollary 2.2.2. *Suppose $n \in \mathbb{N}$ such that $\mathfrak{a}_n$ has no primitive prime divisor; i.e. $n \in \mathcal{Z}(f)$. Then*

$$\mathcal{N}_S(\mathfrak{a}_n) \leq \prod_{q|n} \mathcal{N}_S(\mathfrak{a}_{\frac{n}{q}}), \tag{2.1}$$

where the product is taken over all distinct primes q dividing n.

Proof. Suppose $\mathfrak{p} \notin S$ is a prime dividing $\mathfrak{a}_n$. Choose k minimal such that $\mathfrak{p} \mid \mathfrak{a}_k$. Since $\mathfrak{p}$ is not a primitive prime divisor, $k < n$, and so by S-rigid divisibility, k divides $\frac{n}{q}$ for some prime q dividing n. Furthermore, S-rigid divisibility guarantees that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_n) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_k) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}_{\frac{n}{q}})$. Taking the product over all primes $\mathfrak{p} \notin S$ yields the corollary. $\square$

2.3 Finiteness of critical Zsigmondy sets

In order to prove Theorem 2.1.1 via inequality (2.1), we must find both lower and upper bounds for $\mathcal{N}_S(\mathfrak{a}_n)$. This is done in (5), though we mention a few details of the proof, since they are the fundamentals that will be expanded upon in Chapters 3 and 4.

Proposition 2.3.1. *[Ingram-Silverman, (5)] Let K, f, $\mathfrak{a}_n$, and S be defined as above. Then there exists a constant C such that*

$$\frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n) \leq d^n \hat{h}_f(0) + C.$$

Additionally, given $\epsilon > 0$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$,

$$\frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n) \geq (1-\epsilon) d^n \hat{h}_f(0).$$

Sketch of the proof. Note that by definition, we have

$$h(f^n(0)) = h(f^n(0)^{-1}) = \frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n) + \sum_{v\in S}\frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}\log\max\{1, |f^n(0)|_v^{-1}\}.$$

The first bound is then immediate by Theorem 1.1.1. For the second bound, we must show that $\log|f^n(0)|_v$ is not very small in comparison to d^{-n}; in other words, $f^{n-1}(0)$ is not a very good approximate in the v-adic topology of any root of f. This is essentially the statement of Roth's theorem (and related theorems in Diophantine approximation), and is shown precisely by Silverman in (9), Theorem E, noting that for our choice of f, 0 is not a dynamically exceptional point for f (here a point is **dynamically exceptional** for a rational map if it is periodic and totally ramified for f^2.) $\square$

Together with rigid divisibility, the result of Ingram and Silverman is sufficient to prove Theorem 2.1.1:

proof of Theorem 2.1.1. Taking logs and dividing by $[K:\mathbb{Q}]$, by inequality (2.1), we must show that

$$\frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n) \leq \sum_{q|n} \frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_{\frac{n}{q}})$$

holds for only finitely many $n \in \mathbb{N}$, where the product is over distinct primes q dividing n. Suppose towards contradiction that this inequality holds for infinitely many n. Applying Proposition 2.3.1 with $\epsilon = \frac{d-1}{d}$, there exists $n_0 \in \mathbb{N}$ such that for all $n \geq n_0$, we have

$$d^{n-1}\hat{h}_f(0) \leq \frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n).$$

Therefore by the first part of Proposition 2.3.1, we have infinitely many values of n such that

$$d^{n-1}\hat{h}_f(0) \leq \frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_n) \leq \sum_{q|n} \frac{1}{[K:\mathbb{Q}]}\log \mathcal{N}_S(\mathfrak{a}_{\frac{n}{q}}) \leq \sum_{q|n} d^{\frac{n}{q}}\hat{h}_f(0) + C.$$

Since $q \geq 2$, coarsely bounding the number of prime divisors of n by n yields

$$d^{n-1}\hat{h}_f(0) \leq n d^{\frac{n}{2}}\hat{h}_f(0) + nC. \tag{2.2}$$

Recall that since 0 has infinite order, $\hat{h}_f(0) > 0$. Therefore inequality (2.2) is false for large values of n, yielding the desired contradiction.

□

CHAPTER 3

EFFECTIVE RESULTS IN THE CASE $K = \mathbb{Q}$

3.1 Introduction

As a particular case of the results of Chapter 2, the Zsigmondy set of the critical orbit of $f_c(z) = z^d + c$ is finite for any c in a number field K and any $d \geq 2$ for any infinite critical orbit. In this important family of unicritical polynomials, one might ask for more:

Question 3.1.1. *Fix number field K and $d \geq 2$, and write $f_c(z) = z^d + c$. Does there exist a constant C such that*

$$\#\mathcal{Z}(f_c) \leq C$$

for all $c \in K$ with $\hat{h}_{f_c}(0) \neq 0$?

Here we might ask C to depend on K, or perhaps only on the degree $[K : \mathbb{Q}]$. It is clear that C must depend at least on the degree of the extension; for example, if we let p be a prime, $b > 1$ an integer, and $c = \frac{x}{b}$, then $f_c^p(0)$ will fail to have a primitive prime divisor if $b^{d^{p-1}} \cdot f_c^p(0) = x$. After cancellation, this is a monic integral polynomial in x, and therefore has a solution $x \in \mathcal{O}_K$ for some number field K of degree at most d^{p-1}.

In this chapter we prove a stronger uniformity result for $K = \mathbb{Q}$; in particular, C is shown to be independent of both d and c (Theorem 3.3.2). We do this by constructing effective bounds on the size of the Zsigmondy set, utilizing the canonical height function and Diophantine approximation. In the case $c = \frac{a}{b} \in \mathbb{Q}$ in lowest terms, the ideals $\mathfrak{a}_n$ and $\mathfrak{b}$ are principal, and by induction, we can write

$$f_c^n(0) = \frac{a_n}{b^{d^{n-1}}},$$

where a_n and $b^{d^{n-1}}$ are coprime integers. In particular, if $b > 1$, the critical orbit is infinite. The case $b = 1$ has been considered by Doerksen and Haensch:

Theorem 3.1.2. *(16) Suppose $c \in \mathbb{Z}$ with infinite critical orbit. Then $n \in \mathcal{Z}(f_c) \Rightarrow n \leq 2$.*

Thus for the remainder of this chapter, we will assume $b \geq 2$. In the case of $c \in \mathbb{Q}$, inequality (2.1) applied to this case says that if a_n fails to have a primitive prime divisor, then

$$\log |f_c^n(0)| + d^{n-1} \log b \leq \sum_q (\log |f_c^{\frac{n}{q}}(0)| + d^{\frac{n}{q}-1} \log b). \tag{3.1}$$

where the sum is taken (without multiplicity) over the primes q which divide n.

We will also show that for any $c \in \mathbb{Q}$, there exists an effectively computable constant $M(c)$ such that $n \geq M(c) \Rightarrow n \notin \mathcal{Z}(f_c)$. We will be slightly loose with notation and write $M(c)$ for any such bound, since it is not always possible to compute the minimal such.

We distinguish in the following between those $f_c(z) = z^d + c$ for which the critical orbit is **recurrent** or **non-recurrent**. For our purposes, this difference is explicit; c is recurrent if and only if d is even and $c \in (-2^{\frac{1}{d-1}}, -1)$. However, the dynamical interpretation is that the critical orbit is recurrent if there is no obvious obstruction in the d-Mandelbrot set to $|f_c^n(0)|$

being small (see Chapter 5). The non-recurrent case is straightforward, and uses a similar idea to that of Chapter 2, while the recurrent case requires a more delicate analysis.

3.2 The non-recurrent case

In this section we demonstrate that often $M(c)$ is quite small; in fact, if the critical orbit is non-recurrent, we have $M(c) = 2$:

Theorem 3.2.1. *Let $f_c(z) = z^d + c$ with $d \geq 2$ and $c = \frac{a}{b} \in \mathbb{Q}$ in lowest terms. If d is odd, or d is even and $c \notin (-2^{\frac{1}{d-1}}, -1)$, then we can take $M(c) = 2$.*

Remark 3.2.2. *Note that $2 \in \mathcal{Z}(f_c) \Leftrightarrow a^{d-1} + b = \pm 1$. In particular, $2 \in \mathcal{Z}(f_c) \Rightarrow |c| < 2^{\frac{1}{d-1}}$.*

Recall our assumption that $c \notin \mathbb{Z}$. In order to utilize inequality (3.1) we connect the elements of the sequence $\{a_n\}$ to the corresponding Weil heights $h(f_c^n(0))$, or find bounds on the modulus of the critical orbit, respectively. In the case when $|c| > 2^{\frac{d}{d-1}}$, we can successfully use the former approach.

Lemma 3.2.3. *Suppose that c satisfies $|c| > 2^{\frac{d}{d-1}}$. Then $|f_c^n(0)| > |c| > 1$ for all $n \geq 2$.*

Proof. Since

$$|f_c^n(0)| = |f_c^{n-1}(0)^d + c| = |c| \cdot |\frac{f_c^{n-1}(0)}{c} \cdot f_c^{n-1}(0)^{d-1} + 1|,$$

the lemma is immediate by induction. $\square$

Denote by h the standard logarithmic Weil height $h(P)$ on $\mathbb{P}^1(\mathbb{Q})$. We will abuse notation and use h as a height on $\mathbb{Q}$ as well; by the lemma above, when $|c| > 2^{\frac{d}{d-1}}$, the inequality (2.1) becomes the following:

$$h(a_n) \leq \sum_q h(a_{\frac{n}{q}}). \tag{3.2}$$

Recall that there exists a constant C such that for all $\alpha \in \mathbb{Q}$,

$$|h(\alpha) - \hat{h}_{f_c}(\alpha)| < C. \tag{3.3}$$

We make the constant C explicit in the following lemma:

Lemma 3.2.4. *Let $f_c(z) = z^d + c$ be as above. Then we can take the constant C of inequality (3.3) to be $h(c) + \log(2)$.*

Proof. We use the methods of Theorems 3.11 and 3.20 of (14). Consider f_c as a morphism $[\phi_z : \phi_w]$ on $\mathbb{P}^1$ given by $[z : w] \mapsto [z^d + cw^d : w^d]$. Let h denote the logarithmic Weil height as above, and for each place v of $\mathbb{Q}$, h_v the local height at v. Since

$$|z^d + c|_v \leq \delta_v \max\{|z|_v^d, |c|_v\},$$

where $\delta_v = 1$ for v non-archimedean and $\delta_v = 2$ for the archimedean place, we have

$$h_v(\phi(P)) \leq \log \delta_v + dh_v(P) + h_v(c).$$

Similarly, we have

$$|z^d|_v \leq |z^d + c - c|_v \leq \delta_v \max\{|z^d + c|_v, |c|_v\},$$

so

$$dh_v(P) \le \log \delta_v + h_v(\phi(P)) + h_v(c).$$

Combining these estimates and taking the sum over all places of $\mathbb{Q}$, we see that

$$-\log 2 - h(c) + h(\phi(P)) \le dh(P) \le \log 2 + h(\phi(P)) + h(c),$$

and so

$$|h(\phi(P)) - dh(P)| \le h(c) + \log(2).$$

Taking a telescoping sum, we see that

$$|\hat{h}_{f_c}(P) - h(P)| \le \frac{h(c) + \log(2)}{d-1} \le h(c) + \log(2),$$

as desired. □

We can now prove an effective Zsigmondy result:

Proposition 3.2.5. *Suppose* $|c| > 2^{\frac{d}{d-1}}$. *Then* $\mathcal{Z}(f_c) = \emptyset$.

Remark. The case of this proposition is (nearly) also a corollary of the methods in Chapter 4. However, for convenience in that chapter, we assumed c was recurrent, and so we provide the following proof.

Proof. First note that by Remark 3.2.2 and the assumption $|c| > 2^{\frac{d}{d-1}} > 2$, it suffices to prove that $n \notin \mathcal{Z}(f_c)$ for all $n \geq 3$.

Suppose $n \geq 3$ and $n \in \mathcal{Z}(f_c)$. By inequality (3.2) and Lemma 3.2.4, we have

$$\frac{d^n - s_d(n)}{\omega(n) + 1} \leq \frac{h_{f_c}(c) + \log 2}{\hat{h}_{f_c}(0)},$$

noting that $\hat{h}_{f_c}(0)$ is non-zero.

We now use a remark following Lemma 6 of (17) to get a lower bound for $\hat{h}_{f_c}(0)$:

Lemma 3.2.6 (Ingram (17))**.** *Suppose* $|c| > 2^{\frac{d}{d-1}}$*, and* $f_c(z) = z^d + c$*. Then*

$$\hat{h}_{f_c}(c) \geq \frac{1}{d} h(c).$$

Consequently, we have

$$\hat{h}_{f_c}(0) \geq \frac{1}{d^2} h(c).$$

Thus if a_n has no primitive prime divisor, n must satisfy

$$\frac{d^n - s_d(n)}{\omega(n) + 1} \leq d^2 \frac{h(c) + \log 2}{h(c)} = d^2 (1 + \frac{\log 2}{h(c)}) < 1.5 d^2,$$

where the right-hand inequality holds because $b \geq 2$ and $|c| > 2^{\frac{d}{d-1}} > 2$ together imply that $h(c) = \log |a| \geq \log 4$.

Since $d^n - s_d(n)$ grows very quickly with n, this gives a strong restriction on n; in fact, one can use the bounds $s_d(n) \leq d^{\frac{n}{2}} \log_2(n)$ and $\omega(n) \leq \log_2(n)$ to see that

$$\frac{d^n - s_d(n)}{(\omega(n)+1)} > 1.8d^2$$

if $d \geq 4, n \geq 3$, or $d \geq 3, n \geq 4$, or $d \geq 2, n \geq 5$.

Thus the only cases that remain are $d = 3$ and $n = 3$, or $d = 2$ and $n = 3, 4$, which we check by hand.

If $d = 3$ and $n = 3$, we compute

$$f_c^3(0) = \frac{a}{b^9}(a^2(a^2+b^2)^3 + b^8).$$

Since a and b are coprime, the term $(a^2(a^2+b^2)^3 + b^{26})$ can have no common divisors with a; but since it is a sum of positive integers and $b \geq 2$, $(a^2(a^2+b^2)^3 + b^{26}) \geq 2$ and so is divisible by some prime.

Therefore a_3 has a primitive prime divisor for $d = 2$ or 3.

Finally we turn to the case when $d = 2$ and $n = 4$. If $d = 2$ and $4 \in \mathcal{Z}(f, 0)$, then we have

$$\frac{16-4}{4} \leq (1+\frac{\log 2}{h(c)})(\omega(4)+1),$$

and so

$$\frac{1}{2} \leq \frac{\log 2}{h(c)},$$

and so $a \leq 9$. But by assumption, we have $\frac{a}{b} > 2^{\frac{2}{1}} = 4$, so the only possibility is $a = \pm 9$ and $b = 2$. One can check by hand that for these values of c, a_3 has a primitive prime divisor, and the proposition is proved. $\square$

In the remainder of this section, we cannot necessarily utilize height functions, but non-recurrence of the critical orbit will provide upper and lower bounds on $|f_c^n(0)|$ for all n, which can be used in conjuction with inequality (3.1).

We have straightforward bounds when c is positive; the proof of the following lemma is an easy induction:

Lemma 3.2.7. *Suppose $c > 0$. Write $C(n) = \max\{c, c^{d^{n-1}}\}$. Then for all $n \geq 1$, we have*

$$C(n) \leq f_c^n(0) \leq 2^{\frac{d^{n-1}-1}{d-1}} C(n).$$

Proposition 3.2.8. *Suppose $c > 0$, or $c < 0$ and d is odd. Then $\mathcal{Z}(f_c) = \emptyset$.*

Proof. First note that it is sufficient to prove the proposition for $c > 0$, since if $c < 0$ and d is odd, we may replace c with $-c$ and the forward orbit of 0 will be unchanged, modulo sign. Therefore we assume that $c > 0$ (and thus the forward orbit consists of positive numbers). In light of the remark following Remark 3.2.2, we must prove that $n \notin \mathcal{Z}(f_c)$ for all $n \geq 3$ and all $d \geq 2$.

We recall that if $n \in \mathcal{Z}(f_c)$, then we have

$$\log f_c^n(0) + d^{n-1} \log b \leq \sum_q (\log f_c^{\frac{n}{q}}(0) + d^{\frac{n}{q}-1} \log b),$$

with the sum over distinct primes q dividing n. Multiplying by d and applying the preceding lemma, we have:

$$d \log C(n) + d^n \log b \leq \sum_q \left[\frac{d^{\frac{n}{q}} - d}{d-1} \log 2 + d \log C(\frac{n}{q}) + d^{\frac{n}{q}} \log b \right];$$

rearranging, we have

$$d \left[\log C(n) - \sum_q \log C(\frac{n}{q}) \right] + [d^n - s_d(n)] \log b \leq \frac{1}{d-1} s_d(n) \log 2.$$

Checking by cases, we see that the left-most term is always non-negative, and therefore we have the inequality

$$[d^n - s_d(n)] \log b \leq \frac{1}{d-1} s_d(n) \log 2.$$

By assumption, c is non-integral and so $b \geq 2$, and therefore

$$[d^n - s_d(n)] \log 2 \leq \frac{1}{d-1} s_d(n) \log 2,$$

and so

$$d^n - \frac{d}{d-1} s_d(n) \leq 0,$$

which is impossible for any $d \geq 2$, $n \geq 3$.

$\square$

Next we consider the situation when $-1 < c < 0$ and d is even:

Proposition 3.2.9. *Suppose $-1 < c < 0$ and d is even. Then $\mathcal{Z}(f_c) = \emptyset$, unless $d = 2$ and $a + b = 1$, in which case $\mathcal{Z}(f_c) = \{2\}$.*

Proof. By Remark 3.2.2, we must prove $n \notin \mathcal{Z}(f_c)$ for all $n \geq 3$. We utilize the following bounds, which by assumption on c and d hold for all $n \geq 0$:

$$|c|(1 - |c|^{d-1}) \leq |f_c^n(c)| \leq |c|.$$

Together inequality (3.1) and these bounds imply that we have $n \in \mathcal{Z}(f_c)$ only if

$$\log(|c|(1-|c|^{d-1})) + d^{n-1}\log b \leq \omega(n)\log|c| + \log b \sum_q d^{\frac{n}{q}-1}.$$

Multiplying by d and rearranging, we have

$$\begin{aligned}
(d^n - s_d(n))\log b &\leq d(\omega(n)-1)\log|c| - d\log(1-|c|^{d-1}) \\
&\leq -d\log(1-|c|^{d-1}) \\
&= d(d-1)\log b - d\log(b^{d-1} - |a|^{d-1}) \\
&\leq d(d-1)\log b.
\end{aligned}$$

We conclude that

$$d^n - s_d(n) - d^2 + d \leq 0,$$

which is impossible for all $d \geq 2$, $n \geq 3$. Thus the proposition is proved. $\square$

The final non-recurrent case tightens the bound on $|c|$:

Proposition 3.2.10. *Suppose* $2^{\frac{1}{d-1}} < |c| < 2^{\frac{d}{d-1}}$ *Then* $\mathcal{Z}(f_c) = \emptyset$, *unless* $d = 2$ *and* $a+b = -1$, *in which case* $\mathcal{Z}(f_c) = \{2\}$.

Proof. If d is odd this follows from Proposition 3.2.8, so we assume d is even. Again it is easy to bound the critical orbit by induction; since $2^{\frac{1}{d-1}} < |c| < 2^{\frac{d}{d-1}}$, we have

$$\log|c| \leq \log|f_c^n(0)| \leq (3d^{n-1} - 1)\log 2$$

for all $n \in \mathbb{N}$.

Suppose $n \in \mathcal{Z}(f_c)$. Then combining the above bounds with inequality (3.1), we have

$$d\log|c| + d^n \log b \leq \sum_q ((3d^{\frac{n}{q}} - d)\log 2 + d^{\frac{n}{q}} \log b),$$

and so

$$(d^n - s_d(n))\log b \leq 3s_d(n)\log 2 - \omega(n)d\log 2,$$

which is impossible for $b \geq 2, d \geq 2$ and $n \geq 3$.

□

Proof of Theorem 3.2.1. The Theorem follows immediately from Propositions 3.2.5, 3.2.8, 3.2.9 and 3.2.10. □

3.3 Mahler and the size of the Zsigmondy set

The case when the critical orbit possibly recurs requires more sophisticated techniques. In general, the idea is that by inequality (3.1), $n \in \mathcal{Z}(f_c)$ only if $|f_c^n(0)|$ is extremely small, or rather that $f_c^{n-1}(0)$ is a very good rational approximate of the real dth root of $-c$. The famous Diophantine approximation theorem of Roth tells us that real algebraic numbers can have only finitely many good rational approximations (see e.g. (18) for statement and a nice proof exposition):

Theorem 3.3.1 (Roth for $\mathbb{Q}$)**.** *Let α be a real algebraic number of degree $d \geq 3$. Let $\epsilon > 0$. Then only finitely many rational numbers $\frac{p}{q}, q \geq 1$, satisfy*

$$|\frac{p}{q} - \alpha| \leq \frac{1}{q^{2+\epsilon}}.$$

Since we are seeking a uniform (and effective) bound on the number of elements of $\mathcal{Z}(f_c)$, Roth's theorem is not quite the right tool for our task. We will see that the exponent of $2+\epsilon$ is much stronger than what we require for a Zsigmondy result, and we will instead utilize a precursor of Roth's theorem which can be more easily be made effective in our setting. In this section, we use an approximation theorem of Mahler to show:

Theorem 3.3.2. *Let $f_c(z) = z^d + c$ and $c \in \mathbb{Q}$ such that the critical orbit is infinite. Then $\#\mathcal{Z}(f_c) \leq 23$.*

By the previous section, we can and will assume that d is even, and $c \in (-2^{\frac{1}{d-1}}, -1)$ throughout this section. We then have the following easy upper bound:

Lemma 3.3.3. *Suppose d is even and $-2^{\frac{1}{d-1}} < c < -1$. Then we have*

$$|f_c^n(0)| \leq |c|$$

for all $n \geq 1$.

Thus supposing that $n \in \mathcal{Z}(f_c)$, inequality (3.1) implies

$$\log|f_c^n(0)| + d^{n-1}\log b \leq \omega(n)\log|c| + \sum_q d^{\frac{n}{q}-1}\log b, \tag{3.4}$$

where we define $\omega(n)$ to be the number of distinct prime factors of n. To use this inequality to bound n, we require a lower bound on $|f^n(0)|$ that is reasonably better than $b^{-d^{n-1}}$. In order to use Mahler's approximation theorem, we treat separately the cases of $x^d + c$ irreducible or reducible.

3.3.1 $x^d + c$ irreducible over $\mathbb{Q}$

Throughout this subsection, we assume that d is even, $c \in \mathbb{Q} \cap (-2^{\frac{1}{d-1}}, -1)$, and for all $m \mid d$, $m > 1$, c is not an mth power of a rational number.

Under this assumption, we achieve the following bound on the recurrence of the critical point:

Theorem 3.3.1.1. *For each even* $d \geq 2$, *there exist positive integers* $1 \leq N_d \leq 6$ *and* $1 \leq m_d \leq 6$ *such that there are at most* N_d *values of* $n \in \mathbb{N}$ *satisfying both*

$$n \geq 2m_d + 6$$

and

$$|f_c^n(0)| \leq (b^{d^{n-2}})^{-d(1-d^{-m_d})}.$$

Further, for $d \geq 6$, the result holds with $m_d = 1$ and $N_d = 2$, and for $d = 4$, the result holds with $m_d = 2$ and $N_d = 3$.

For those c satisfying the assumptions, Theorem 3.3.2 is an immediate consequence of Theorem 3.3.1.1:

Proof of Theorem 3.3.2. If $n \in \mathcal{Z}(f_c)$, inequality (3.4) says

$$\log|f_c^n(0)| + d^{n-1}\log b \leq \frac{1}{d}s_d(n)\log b + \omega(n)\log|c|,$$

where (as above)

$$s_d(n) := \sum_q d^{\frac{n}{q}}$$

is a sum over primes q dividing n, and $\omega(n)$ is the number of distinct primes dividing n.

Thus applying Theorem 3.3.1.1, for all but at most N_d values of n with $n \geq 2m_d + 6$, we have

$$d^{n-m_d-1} - \frac{1}{d}s_d(n) \leq \frac{\omega(n)\log|c|}{\log b}.$$

Since $\frac{a}{b} = c \in (-2,-1)$, we have $|c| < b$; also we have $\frac{1}{d}s_d(n) < d^{\frac{n}{2}}$. Thus

$$d^{n-m_d-1} - d^{\frac{n}{2}} \leq \omega(n).$$

By assumption, $n - m_d - 1 \geq \frac{n}{2} + 2$, and so

$$d^{\frac{n}{2}} \leq \omega(n);$$

since $\omega(n) \leq \log_2(n)$, this is false for all $d \geq 2, n \geq 2$.

Therefore the size of the Zsigmondy set satisfies

$$\#\mathcal{Z}(f_c) \leq 2m_d + 6 - 1 + N_d \leq 23$$

for all values of $d \geq 2$, with improved bound for $d = 4$ of

$$\#\mathcal{Z}(f_c) \leq 2m_d + 6 - 1 + N_d = 12,$$

and for $d \geq 6$ we have

$$\#\mathcal{Z}(f_c) \leq 2m_d + 6 - 1 + N_d = 9.$$

□

The remainder of this section will be devoted to the proof of Theorem 3.3.1.1, which relies on the proof of Mahler's quantitative result (10) on restricted rational approximation of real algebraic numbers. Examining the proof of Theorem 3 of (10), we extract the following quantitative statement bounding the good rational approximates of real algebraic numbers:

Theorem 3.3.1.2. *[Mahler] Let S be a finite set of primes, ζ a real algebraic number of degree $d \geq 2$, and $\mu > \sqrt{d}$. Let R be the maximal absolute value of the coefficients of the minimal integral polynomial of ζ. Suppose $\epsilon > 0$ is sufficiently small so that*

$$\kappa := \left(\sqrt{\frac{1-2\epsilon}{d}} - 2\sqrt{\epsilon}\right)\mu - (1+\epsilon)^2 > 0.$$

Then there do not exist rational S-integers $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ satisfying

$$\left|\frac{p_i}{q_i} - \zeta\right| < q_i^{-\mu}, \tag{3.5}$$

which also satisfy

- $q_1^{\kappa} \geq (16R)^{\frac{4}{\epsilon}}$,
- $q_2 \geq q_1^{\frac{5d^2}{2\epsilon}}$.

To apply this theorem to our setting, let ζ be the positive dth root of $|c|$, and $\mu = d(1-d^{-m})$, with m to be chosen later. Since $\zeta > 1$, we have

$$|\frac{|a_{n-1}|}{b^{d^{n-2}}} - \zeta| < |f_c^{n-1}(0)^d - |c|| = |f_c^n(0)|,$$

so if

$$|f_c^n(0)| \leq (b^{d^{n-2}})^{-d(1-d^{-m})},$$

then $|f_c^{n-1}(0)|$ is a good approximate of ζ in the sense of inequality (3.5).

So we will apply Mahler's theorem to the iterates $f^{n-1}(0)$; to do so, we rewrite the last three conditions of Theorem 3.3.1.2 in our setting. Suppose that $|f_c^{n_1-1}(0)|$ and $|f_c^{n_2-1}(0)|$ are both good approximates to ζ; i.e., satisfy inequality (3.5). Since the denominator of $|f_c^{n_i-1}(0)|$ is $q_i = b^{d^{n_i-2}}$, we have

$$q_1^{\kappa} \geq (16R)^{\frac{4}{\epsilon}} \Leftrightarrow d^{n_1-2}\log b \geq \frac{4}{\kappa\epsilon}\log 16R.$$

Since $|c| \in (1,2)$, we have $R = |a| < 2b$; also we have $b \geq 2$, so

$$n_1 \geq \log_d(\frac{24}{\kappa\epsilon}) + 2 \Rightarrow (b^{d^{n_1-2}})^{\kappa} \geq (b^6)^{\frac{4}{\epsilon}} \Rightarrow d^{n_1-2} \geq \frac{24}{\kappa\epsilon} \Rightarrow q_1^{\kappa} \geq (16R)^{\frac{4}{\epsilon}}.$$

Similarly, we have

$$n_2 \geq n_1 + \log_d(\frac{5d^2}{2\epsilon}) \Rightarrow q_2 \geq q_1^{\frac{5d^2}{2\epsilon}}.$$

Therefore we have shown that Theorem 3.3.1.2 implies the following:

Proposition 3.3.1.3. *Suppose that $|f_c^{n_1-1}(0)|$ and $|f_c^{n_2-1}(0)|$ satisfy inequality (3.5), with $n_1 \geq \log_d(\frac{24}{\kappa\epsilon}) + 2$. Then we have*

$$n_2 < n_1 + \log_d(\frac{5d^2}{2\epsilon}).$$

Proof of Theorem 3.3.1.1. According to Proposition 3.3.1.3, in order to prove Theorem 3.3.1.1, we must show that we can choose ϵ and $\mu = d(1 - d^{-m_d})$ such that $\kappa > 0$, and

- $1 \leq m_d \leq 6$,
- $2m_d + 6 \geq \log_d(\frac{24}{\kappa\epsilon}) + 2$, and
- $\log_d(\frac{5d^2}{2\epsilon}) \leq 6$.

Remark 3.3.1.4. *In fact, we can weaken this last inequality; since* $|f_c^n(0)| < \frac{1}{2} \Rightarrow |f_c^{n+1}(0)| > \frac{1}{2}$*, we cannot have consecutive good approximates, and so we have* $N_d \leq \frac{1}{2}\log_d(\frac{5d^2}{2\epsilon})$*.*

Suppose $d \geq 6$. Let $m_d = 1$ and $\epsilon = \frac{1}{d^3}$ (note $\mu = d - 1$). Then one can compute that $\kappa > \frac{24}{d^3} > 0$, and therefore

$$\log_d(\frac{24}{\kappa\epsilon}) < 6.$$

Therefore

$$2m_d + 6 = 8 \geq \log_d(\frac{24}{\kappa\epsilon}) + 2.$$

By choice of ϵ, we have

$$\log_d(\frac{5d^2}{2\epsilon}) = 5 + \log_d(\frac{5}{2}) < 6,$$

and by Remark 3.3.1.4, we conclude that $N_d \leq \frac{1}{2}\log_d(\frac{5d^2}{2\epsilon}) < 3$.

For $d = 2$, we simply note that the smallest m_2 and N_2 that can be achieved are found when $\epsilon = .004$ and $m_2 = 6$. In this case we have

$$2m_2 + 6 = 18 \geq \log_2(\frac{24}{\kappa\epsilon}) + 2,$$

and

$$\log_2(\frac{5d^2}{2\epsilon}) = \log_2(15000) < 14,$$

so we can take $N_2 = 6$.

Similarly for $d = 4$, we achieve optimal values at $m_4 = 2$ and $\epsilon = \frac{1}{128}$. In this case we have

$$2m_4 + 6 = 10 \geq \log_4(\frac{24}{\kappa\epsilon}) + 2,$$

and

$$\log_2(\frac{5d^2}{2\epsilon}) = \frac{11}{2} + \log_4(\frac{5}{2}) < 7,$$

so we can take $N_4 = 3$.

$\square$

3.3.2 $x^d + c$ reducible over $\mathbb{Q}$

In the case when c is a power dividing d over $\mathbb{Q}$ we have a stronger result:

Proposition 3.3.2.1. *Suppose that d is even, and $c = \frac{a}{b} \in (-2^{\frac{1}{d-1}}, -1)$ such that there exists $m \mid d$, $m \neq 1$, and positive integers k, l with $a = -k^m, b = l^m$. Then $\mathcal{Z}(f_c) = \emptyset$.*

In order to prove the proposition, we find a lower bound for $|f_c^n(0)|$:

Lemma 3.3.2.2. *Suppose d and c are as above. Then we have*

$$|f_c^n(0)| \geq \frac{1}{db^{\frac{1}{2}d^{n-1}}}$$

for all $n \geq 2$.

Proof. By assumption, we have

$$\begin{aligned} |f_c^n(0)| &= |f_c^{n-1}(0)^d - \left(\frac{k}{l}\right)^m | \\ &= ||f_c^{n-1}(0)|^{\frac{d}{m}} - \frac{k}{l}| \cdot | \left(|f_c^{n-1}(0)|^{\frac{d}{m}}\right)^{m-1} + \left(|f_c^{n-1}(0)|^{\frac{d}{m}}\right)^{m-2} \cdot \left(\frac{k}{l}\right) + \cdots + \left(\frac{k}{l}\right)^{m-1} | \\ &\geq ||f_c^{n-1}(0)|^{\frac{d}{m}} - \frac{k}{l}|, \end{aligned}$$

since the right-hand factor is a sum of positive numbers, one of which is $\left(\frac{k}{l}\right)^{m-1}$, which is > 1 by assumption.

Write β for the positive $\frac{d}{m}$th root of $\frac{k}{l}$ - for notational convenience we will set $r = \frac{d}{m}$, so that $\beta^r = \frac{k}{l}$. From the above, we have

$$\begin{aligned}
|f_c^n(0)| &\geq ||f_c^{n-1}(0)|^{\frac{d}{m}} - \frac{k}{l}| \\
&= ||f_c^{n-1}(0)| - \beta| \cdot ||f_c^{n-1}(0)|^{\frac{d}{m}-1} + |f_c^{n-1}(0)|^{\frac{d}{m}-2} \cdot \beta + \cdots + \beta^{\frac{d}{m}-1}| \\
&> ||f_c^{n-1}(0)| - \beta|,
\end{aligned}$$

since $\beta > 1$. But we know that $|f_c^{n-1}(0)|$ is a rational number whose denominator is $b^{d^{n-2}}$ and therefore a power of l. Therefore we have

$$\begin{aligned}
\frac{1}{b^{r \cdot d^{n-2}}} &\leq |(\frac{|a_{n-1}|}{b^{d^{n-2}}})^r - \frac{k}{l}| \\
&= ||f_c^{n-1}(0) - \beta| \cdot ||f_c^{n-1}(0)|^{r-1} + ... + \beta^{r-1}| \\
&\leq ||f_c^{n-1}(0)| - \beta| \cdot r \max\{|f_c^{n-1}(0)|, \beta\},
\end{aligned}$$

noting that the first inequality is valid because the right-hand term divides $f_c^n(0)$ and thus cannot be 0, since 0 is not periodic. By Lemma 3.3.3, we then have

$$\begin{aligned}
\frac{1}{b^{r \cdot d^{n-2}}} &\leq ||f_c^{n-1}(0)| - \beta| \cdot \frac{d}{2} \cdot |c| \\
&\leq ||f_c^{n-1}(0)| - \beta| \cdot d;
\end{aligned}$$

Since $r = \frac{d}{m} \leq \frac{d}{2}$, we conclude that

$$|f_c^n(0)| > ||f_c^{n-1}(0)| - \beta| \geq \frac{1}{d \cdot b^{r \cdot d^{n-2}}} \geq \frac{1}{d \cdot b^{\frac{1}{2}d^{n-1}}},$$

as desired. $\square$

Having achieved a lower bound for $|f_c^n(0)|$, we can now prove the proposition.

Proof. Suppose $n \geq 3$ with $n \in \mathcal{Z}(f_c)$, so that

$$\log|f_c^n(0)| + d^{n-1}\log b \leq \omega(n)\log|c| + \sum_q d^{\frac{n}{q}-1}\log b.$$

By the lemma, we then have

$$d\log\left(\frac{1}{d \cdot b^{\frac{1}{2}d^{n-1}}}\right) + d^n \log b < d\omega(n)\log|c| + s_d(n)\log b,$$

and so

$$-d\log d + \frac{1}{2}d^n \log b < d\omega(n)\log|c| + s_d(n)\log b.$$

Since $|c| < 2$,

$$\frac{1}{2}d^n - s_d(n) < \frac{d\omega(n)\log 2 + d\log d}{\log b}.$$

Since c is an mth power of a rational number, $m > 1$, we have $b \geq 9$, so

$$\frac{1}{2}d^n - s_d(n) < \frac{d}{3}\omega(n) + \frac{1}{2}d\log d,$$

and so

$$\frac{1}{2}d^{n-1} - \frac{1}{2}\log d - \frac{1}{d}s_d(n) \leq \frac{1}{3}\omega(n).$$

Utilizing the bounds $s_d(n) \leq d^{\frac{n}{2}}\log_2(n)$ and $\omega(n) \leq \log_2(n)$, we see that this is false for all $d \geq 2$ and all $n \geq 3$.

Since from Remark 3.2.2 we know that $2 \in \mathcal{Z}(f_c)$ only if $d = 2$ and $a = -(b \pm 1)$, our assumption that c is an mth power guarantees that $2 \notin \mathcal{Z}(f_c)$, and the proposition is proved.

$\square$

Remark 3.3.2.3. *These methods could be easily generalized for any polynomial maps for which the proximity of the roots of f to the rational numbers can be nicely bounded; for example, Mahler's results would apply with minimal modification to any f with all real roots.*

CHAPTER 4

IMPROVING THE BOUND

4.1 Introduction

It is clear that the bound $\#\mathcal{Z}(f_c) \leq 23$ of Theorem 3.3.2 above is an artifact of the proof, and not sharp. In light of the results of Chapter 5, one might speculate that the sharp bound is 2 or 3, depending whether $d > 2$. We cannot with these methods achieve quite this sharpness; however, we can do better for $d > 2$ by refining the Mahler/Thue method.

Theorem 4.1.1. *Let $f_c(z) = z^d + c$ with $d \geq 3$ and $c \in \mathbb{Q}$. Then for $n \geq 8$, there is at most one n such that a_n fails to have a primitive prime divisor.*

Remark 4.1.2. *Though this theorem would be more satisfying if the small ($3 \leq n \leq 7$) values of n were ruled out, this is quite difficult; for example, $f_c^7(0)$ has a primitive prime divisor for all $c \in \mathbb{Q}$ if and only if two particular auxiliary affine Thue curves of degree $d^7 - 1$ have no integral solutions. Note also that for $d = 2$, $n = 3$ actually does appear as an element of $\mathcal{Z}(f_{-7/4})$; in this case, a corresponding auxiliary curve is $a^3 + 2a^2b + ab^2 + b^3 = 1$, which is nonsingular of genus 1. After a change of variables, the integral solutions of this Thue equation are due to Nagell (19), and we see that $c = \frac{-7}{4}$ is the only non-critically-finite parameter for $d = 2$ with $3 \in \mathcal{Z}(f_c)$.*

The heart of this result is a refinement of Thue's precursor to Roth's theorem on the approximation of dth roots of integers. Utilizing the rapid growth of the denominator of $f_c^n(0)$, two sufficiently large elements of the Zsigmondy set would give rise to a pair of which rationals contradict the refinement of Thue's theorem.

In this chapter we prove Theorem 4.1.1, which is applicable to any value $c \in \mathbb{Q}$. Since the result of Theorem 4.1.1 is superseded by that of Theorem 3.2.1 if applicable, we will assume throughout this section that c is recurrent, i.e. d is even and $c \in (-2^{\frac{1}{d-1}}, -1)$. Additionally we must assume $d \geq 3$ as in the statement of Theorem 4.1.1. Our goal is to achieve a bound on the size of the Zsigmondy set, though we do not necessarily have nice bounds on the critical orbit, or the tool of height functions. We do have a upper bound on the critical orbit, whose proof is a straightfoward induction:

Lemma 4.1.3. *Suppose d is even and $-2^{\frac{1}{d-1}} < c < -1$. Then we have*

$$|f_c^n(0)| \leq |c|$$

for all $n \geq 1$.

Thus supposing that $n \in \mathcal{Z}(f_c)$, we have by inequality (3.1):

$$\log|f_c^n(0)| + d^{n-1} \log b \leq \omega(n) \log|c| + \sum_q d^{\frac{n}{q}-1} \log b; \tag{4.1}$$

to utilize this towards contradiction, we require a lower bound on $|f^n(0)|$ reasonably better than $b^{-d^{n-1}}$. By definition and assumption on c,

$$|f_c^n(0)| = |f_c^{n-1}(0)^d - |c||,$$

so this is easily accomplished when $|c|^{\frac{1}{d}}$ is poorly approximated by rationals, as seen in Subsection 3.3.2. In general, we cannot with these methods achieve such an explicit expression of the Zsigmondy set. However, we can still use the idea of $|c|^{\frac{1}{d}}$ being poorly approximated by rationals to draw the conclusion of Theorem 4.1.1. As this is a diophantine approximation argument, we require the additional assumption that for all $m \mid d$, we do not have $a, b \in \mathbb{Z}^m$; i.e., c is not an mth power of a rational number, which case was dealt with in Subsection 3.3.2.

Our goal now is to use a modification of Thue's Diophantine approximation theorem to prove the 'nearly' effective statement of Theorem 4.1.1. The proof relies on finding a lower bound for $|f^n(0)|$ in terms of its denominator; in particular, Theorem 4.1.1 is a corollary of the following theorem:

Theorem 4.1.4 (Approximation Theorem)**.** *For all but possibly one $n \geq 8$, we have*

$$|f_c^n(0)| \geq \frac{1}{b^{\frac{15}{16}d^{n-1}+\frac{1}{16}d}}.$$

To see why this implies Theorem 4.1.1, recall inequality (4.1) above that if a_n fails to have a primitive prime divisor, then

$$\log|f_c^n(0)| + d^{n-1}\log b \le \sum_{q|n}(\log|f_c^{\frac{n}{q}}(0)| + d^{\frac{n}{q}-1}\log b),$$

where the sum is taken over distinct primes q dividing n.

We combine the Approximation Theorem with this bound and inequality to deduce Theorem 4.1.1:

Proof of Theorem 4.1.1. Suppose $n \ge 8$, and $n \in \mathcal{Z}(f_c)$. By the above inequality and Lemma 4.1.3, we have

$$\log|f_c^n(0)| + d^{n-1}\log b \le \frac{1}{d}s_d(n)\log b + \omega(n)\log|c|,$$

where

$$s_d(n) = \sum_q d^{\frac{n}{q}}$$

is a sum over primes q dividing n, and $\omega(n)$ is the number of distinct primes dividing n.

Thus applying the Approximation Theorem, for all but at most one such n, we have

$$\frac{1}{16}d^{n-1} - \frac{1}{16}d - \frac{1}{d}s_d(n) \le \frac{\omega(n)\log|c|}{\log b}.$$

Since $\frac{a}{b} = c \in (-2, -1)$, we have $|c| < b$. In addition, $d \geq 4$ and the left-hand side is increasing in d for $n \geq 8$, so we conclude that

$$4^{n-3} - \frac{1}{4} - \frac{1}{4}s_4(n) \leq \frac{\omega(n) \cdot \log |c|}{\log b} < \omega(n),$$

which is false for all $n \geq 8$.

$\square$

The remainder of this chapter will be devoted to the proof of the Approximation Theorem. For the proof, we will modify Thue's classical result on Diophantine approximation, which provides an improvement on Liouville's theorem on the exponent $\tau(d)$ such that for any $C > 0$,

$$|\frac{p}{q} - \beta| < \frac{C}{q^{\tau(d)}}$$

has only finitely many rational solutions for a given algebraic integer β of degree d.

In Thue's (and subsequent related) arguments, the crucial assumption which leads to ineffectivity is the necessity of producing two good approximates $\frac{p_1}{q_1}, \frac{p_2}{q_2}$ with q_1 large, and q_2 large compared to q_1. This can be exploited for elements of forward orbit of 0 under $z^d + c$ precisely because the denominators of the iterates grow very rapidly in n. We will thus modify Thue's argument so that it is enough to assume towards contradiction that $q_2 \geq q_1^{16}$, which for $d \geq 4$

is sufficient to prove the 'at most one' statement of the Approximation Theorem.

Once the proper values to consider to achieve this are found, the argument is a straightforward modification of the original proof. For clarity, we will mimic the notation and terminology of Chapter V of (20), which presents the necessary theorems and result for Thue's general argument in the case $d = 3$. All of their expositions and theorems must be generalized and tightened for our purposes to achieve the necessary constants.

4.2 Preliminary Theorems

Throughout we fix $d \geq 4$ and a positive integer B which is not an mth root for any $m \mid d$, and define

$$\alpha = \frac{d-2}{2} + \frac{1}{2d}.$$

In order to simplify notation, for a polynomial $F(x, y) = P(x) + Q(x)y \in \mathbb{Z}[x, y]$, we define

$$F^{(k)}(x, y) := \frac{1}{k!} \frac{\partial^k}{\partial x^k} F(x, y)$$

to be the coefficients of the Taylor expansion at (x, y), noting that $F^{(k)}(x, y)$ will then have integer coefficients as well.

Theorem 4.2.1 (Auxiliary Polynomial Theorem)**.** *Let B be an integer, let $\beta = B^{\frac{1}{d}}$ be the positive dth root of B, and let $m, n \geq 3$ be integers satisfying*

$$m + 1 > \alpha n \geq m.$$

Then there is a non-zero polynomial with integer coefficients of degree at most $m+n$ *in* x*,*

$$F(x, y) = P(x) + Q(x)y,$$

such that for all $0 \leq k < n$*, we have*

$$F^{(k)}(\beta, \beta) = 0,$$

and the coefficients of F *are bounded above in absolute value by*

$$2(8^d B)^{d(m+n)}.$$

Note that α was chosen precisely to be the minimal value so that this theorem is an immediate consequence of Siegel's lemma applied to a system of $M = dn$ equations in $N = 2(m+n+1)$ variables, along with an estimate of the coefficients of the system that is sufficient to deduce the Approximation Theorem.

Proof. The proof follows (20), modified here to achieve the desired constant. We write $F(x, y) = P(x) + Q(x)y$ as:

$$F(x,y) = \sum_{i=0}^{m+n} u_i x^i + \sum_{i=0}^{m+n} v_i x^i y.$$

Since by assumption on B, $1, \beta, ..., \beta^{d-1}$ are linearly independent over $\mathbb{Q}$, the restriction

$$F(\beta,\beta) = F^{(1)}(\beta,\beta) = ... = F^{(n-1)}(\beta,\beta) = 0$$

imposes exactly dn conditions on the coefficients of F. Since F is determined by two polynomials of degree at most $m+n$, finding an F which satisfies this requirement is equivalent to solving $M = dn$ equations in $N = 2(m+n+1)$ variables. By hypothesis, we have

$$m \leq n\alpha < m+1,$$

with

$$\alpha = \frac{d-2}{2} + \frac{1}{2d}.$$

Therefore

$$\begin{aligned} N - M &= 2(m+n+1) - dn \\ &= n(2(\frac{m+1}{n}) + 2 - d) \\ &> n(2(\frac{d-2}{2} + \frac{1}{2d}) + 2 - d) \\ &= \frac{n}{d} > 0, \end{aligned}$$

so the system has solutions.

Siegel's lemma then guarantees that we have an nonzero integer solution for the u_i and v_j, with

$$\max_{i,j}\{|u_i|, |v_j|\} < 2(4N\mu)^{\frac{M}{N-M}},$$

where μ is the maximum absolute value of coefficients in the system. Thus we must estimate μ; i.e., the coefficients of the equations $F^{(k)}(\beta,\beta) = 0$. We have

$$F^{(k)}(\beta,\beta) = \sum_{i=0}^{m+n-k+1} \{\binom{i+k}{k}\beta^i u_{i+k} + \binom{i+k-1}{k}\beta^i v_{i+k-1}\};$$

writing $i = dj + l$,

$$F^{(k)}(\beta,\beta) = \sum_{l=0}^{d-1}\{\sum_j \binom{dj+l+k}{k} B^j u_{dj+l+k} + \binom{dj+l+k-1}{k} B^j v_{dj+l+k-1}\}\beta^l.$$

Therefore

$$\begin{aligned}
\mu &\leq \max_{0\leq dj+l\leq m+n, 0\leq k<n} \binom{dj+l+k}{k} B^j \\
&\leq \max_{0\leq i\leq m+n, 0\leq k<n} \binom{i+k}{k} B^{\frac{i}{d}} \\
&\leq \max_{0\leq i\leq m+n, 0\leq k<n} 2^{i+k} B^{\frac{i}{d}} \\
&= 2^{m+2n-1} B^{\frac{m+n}{d}} \\
&< (4^d B)^{\frac{m+n}{d}}
\end{aligned}$$

Therefore, recalling that $N - M \geq \frac{n}{d}$ and $m, n \geq 3$, we have an integer solution for the u_i, v_j such that

$$\begin{aligned}
\max_{i,j}\{|u_i|, |v_j|\} &< 2(4N\mu)^{\frac{M}{N-M}} \\
&< 2(8(m+n+1)(4^d B)^{\frac{m+n}{d}})^{d^2} \\
&\leq 2(8^d B)^{d(m+n)},
\end{aligned}$$

as desired.

□

We have the following modification of the Smallness Theorem:

Theorem 4.2.2 (Smallness Theorem)**.** *Let $F(x, y)$ be an auxiliary polynomial as described in the previous theorem. Then there is a constant $c_1 > 0$, depending only on B, so that for any real numbers x, y such that $|x - \beta| \leq 1$ and any integer $0 \leq t < n$, we have*

$$|F^{(t)}(x, y)| \leq c_1^n(|x - \beta|^{n-t} + |y - \beta|).$$

Further, we can take the constant c_1 to be

$$c_1 = (2^{4d^2+2} B^{d+\frac{1}{d}})^{1+\alpha}$$

Proof. Again we follow [Si-Ta], with the necessary modifications. We use the Taylor expansion of $F(x, y)$ about (β, β); since the first n derivatives vanish, we have

$$F(x, y) = \sum_{k=n}^{m+n} F^{(k)}(\beta, \beta)(x - \beta)^k + \sum_{k=0}^{m+n} Q^{(k)}(\beta)(x - \beta)^k(y - \beta).$$

Since we want to estimate $F^{(t)}(x, y)$, we differentiate the above t times with respect to x and divide by $t!$:

$$F^{(t)}(x,y) = \{\sum_{k=n}^{m+n} F^{(k)}(\beta,\beta)\binom{k}{t}(x-\beta)^{k-n}\}(x-\beta)^{n-t} + \{\sum_{k=0}^{m+n} Q^{(k)}(\beta)\binom{k}{t}(x-\beta)^{k-t}\}(y-\beta).$$

Since $|x-\beta| < 1$ and $|y-\beta| < 1$, the triangle inequality implies

$$|F^{(t)}(x,y)| \leq \sum_{k=n}^{m+n} |F^{(k)}(\beta,\beta)|\binom{k}{t}|x-\beta|^{n-t} + \sum_{k=0}^{m+n} |Q^{(k)}(\beta)|\binom{k}{t}|y-\beta|.$$

For the binomial coefficient, we will use the easy bound

$$\binom{k}{t} \leq 2^{m+n}.$$

For the rest, we have, by differentiating and applying the Auxiliary Polynomial Theorem:

$$\begin{aligned}
|F^{(k)}(\beta,\beta)| &= |\sum_{i=k}^{m+n}\binom{i}{k}(u_i\beta^{i-k} + v_i\beta^{i-k-1})| \\
&\leq (m+n+1)2^{m+n+1}\max_{i,j}\{|u_i|,|v_j|\}\beta^{m+n} \\
&\leq 2^{2m+2n+2}(8^dB)^{d(m+n)}B^{\frac{m+n}{d}} \\
&\leq (16^{d^2}B^{d+\frac{1}{d}})^{m+n}.
\end{aligned}$$

Therefore

$$\begin{aligned}
\sum_{k=n}^{m+n} |F^{(k)}(\beta,\beta)| \binom{k}{t} &\leq (m+1)(16^{d^2} B^{d+\frac{1}{d}})^{m+n} 2^{m+n} \\
&\leq 2^{m+n}(16^{d^2} B^{d+\frac{1}{d}})^{m+n} 2^{m+n} \\
&\leq (4 \cdot 16^{d^2} B^{d+\frac{1}{d}})^{m+n} \\
&\leq \{(4 \cdot 16^{d^2} B^{d+\frac{1}{d}})^{1+\alpha}\}^{n}.
\end{aligned}$$

For the other sum, we have

$$\begin{aligned}
|Q^{(k)}(\beta)| &= |\sum_{i=k}^{m+n} \binom{i}{k} v_i \beta^{i-k}| \\
&\leq (m+n+1)2^{m+n} \max_{i,j}\{|u_i|, |v_j|\}\beta^{m+n} \\
&\leq (16^{d^2} B^{d+\frac{1}{d}})^{m+n},
\end{aligned}$$

by comparison with the previous estimate. Therefore,

$$\begin{aligned}
\sum_{k=0}^{m+n} |Q^{(k)}(\beta)| \binom{k}{t} &\leq (m+n+1)(16^{d^2} B^{d+\frac{1}{d}})^{m+n} 2^{m+n} \\
&\leq 2^{m+n}(16^{d^2} B^{d+\frac{1}{d}})^{m+n} 2^{m+n} \\
&\leq \{(4 \cdot 16^{d^2} B^{d+\frac{1}{d}})^{1+\alpha}\}^{n},
\end{aligned}$$

again by comparing to the first estimate.

Therefore for

$$c_1 = (2^{4d^2+2} B^{d+\frac{1}{d}})^{1+\alpha},$$

we have the desired result.

□

Finally, we modify the Non-Vanishing Theorem:

Theorem 4.2.3 (Non-Vanishing Theorem)**.** *Let $F(x, y)$ be an auxiliary polynomial as described in the theorem above. Let p_1/q_1 and p_2/q_2 be rational numbers in lowest terms. Then there is a constant c_2, depending only on B, and an integer*

$$0 \leq t \leq 1 + \frac{c_2 n}{\log q_1},$$

so that

$$F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2}) \neq 0.$$

Further, we can take the constant c_2 to be $c_2 = \log c_3$, where

$$c_3 = (2^{6d^2+3}B^{2d})^{1+\alpha}.$$

Proof. Let $W(x) = P(x)Q'(x) - Q(x)P'(x)$, and let T be the largest integer such that

$$F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2}) = 0$$

for all $0 \leq t < T$.

One can show (see (20)) that the definition of T guarantees the existence of a polynomial $V(x) \in \mathbb{Z}[x]$ such that

$$W(x) = (q_1 x - p_1)^{T-1} V(x).$$

Since $V(x)$ is an integral polynomial, $W(x)$ is either identically zero, or has a coefficient of absolute value at least as large as q_1^{T-1}. Assume for the moment that $W(x)$ is not identically zero. Then we can utilize this, along with an upper bound on the coefficients of W, to find an upper bound for T. Since

$$W(x) = \sum_{i,j} j(u_i v_j - v_i u_j)x^{i+j-1},$$

the largest coefficient of $W(x)$ is bounded above by

$$\begin{aligned}
\max_{i,j\leq m+n} |j(u_i v_j - v_i u_j)| &\leq 2(m+n)(\max_{i\leq m+n}\{|u_i|,|v_i|\})^2 \\
&\leq 2(m+n)4(8^d B)^{2d(m+n)} \\
&\leq (8^{d+\frac{1}{2d}}B)^{2d(m+n)} \\
&\leq (2^{6d^2+3}B^{2d})^{(1+\alpha)n}.
\end{aligned}$$

Therefore if we let $c_3 = (2^{6d^2+3}B^{2d})^{1+\alpha}$, and $c_2 = \log c_3$, we have

$$q_1^{T-1} \leq c_3^n,$$

and so

$$T \leq 1 + \frac{c_2 n}{\log q_1}.$$

So by our definition of T, there exists an integer $0 \leq t \leq 1 + \frac{c_2 n}{\log q_1}$ such that

$$F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2}) \neq 0.$$

It remains to prove our assumption that $W(x)$ is not identically 0. Suppose otherwise; since $W(x)$ is the numerator of the derivative of $P(x)/Q(x)$, there exists a constant A such that

$$P(x) = AQ(x),$$

and so

$$F(x, y) = (A + y)Q(x).$$

Note that since $P(x), Q(x) \in \mathbb{Z}[x]$, $A \in \mathbb{Q}$. By the Auxiliary Polynomial Theorem, we have for all $0 \leq k < n$,

$$0 = F^{(k)}(\beta, \beta) = (A + \beta)Q^{(k)}(\beta);$$

since A is rational and β irrational, $A + \beta \neq 0$, so we have $Q^{(k)}(\beta) = 0$ for all $0 \leq k < n$. Thus the minimal polynomial $x^d - B$ of β divides $Q(x)$ with multiplicity at least n. Hence the degree of $Q(x)$ is at least dn; but we have specified that the degree of $Q(x)$ is at most

$$m + n \leq (1 + \alpha)n = (1 + \frac{d-2}{2} + \frac{1}{2d})n = (\frac{d}{2} + \frac{1}{2d})n.$$

Since d is a positive integer, we have

$$\frac{d}{2} + \frac{1}{2d} < d,$$

yielding a contradiction. Therefore $W(x)$ cannot be identically 0. $\square$

4.3 Proof of the Approximation Theorem.

As a corollary of the preceding results, we have the modification of Thue's theorem that we will need to prove the Approximation Theorem:

Theorem 4.3.1. *With c_1, c_2, c_3 as above, there do not exist two rational numbers $\frac{p_1}{q_1}$ and $\frac{p_2}{q_2}$ which satisfy all of the following:*

$$q_1 > c_3^9,$$

$$q_1 > (2^{\frac{1}{17}} c_1)^{22},$$

$$q_2 \geq q_1^{16},$$

and

$$|\frac{p_i}{q_i} - \beta| \leq \frac{1}{q_i^{\frac{15}{16}d}}.$$

Proof. Suppose to the contrary that we have such a pair $\frac{p_1}{q_1}, \frac{p_2}{q_2}$. Let n be the positive integer satisfying

$$q_1^{\frac{8}{9}n} \leq q_2 < q_1^{\frac{8}{9}(n+1)}.$$

Note that by hypothesis, we then have

$$n > \frac{9 \log q_2}{8 \log q_1} - 1 \geq 17.$$

Using this value of n, and the corresponding choice of m so that

$$m \leq \alpha n < m + 1,$$

apply the Auxiliary Polynomial Theorem and Non-Vanishing Theorem to find a polynomial

$$F(x, y) = P(x) + Q(x)y \in \mathbb{Z}[x, y]$$

of degree at most $m + n$ in x, and integer t, such that

$$0 \leq t \leq 1 + \frac{c_2 n}{\log q_1},$$

and

$$F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2}) \neq 0.$$

Note that since $\log q_1 > 9 \log c_3 = 9c_2$, we have

$$n - t \geq n - (1 + \frac{c_2 n}{\log q_1}) \geq \frac{8}{9}n - 1.$$

Now we work towards the desired contradiction by finding upper and lower bounds for $|F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2})|$.

Since $F^{(t)}(x,y)$ is nonzero, has integer coefficients, and is degree at most $m+n$ in x, degree 1 in y, we have

$$|F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2})| \geq \frac{1}{q_1^{m+n} q_2}.$$

Since $m \leq \alpha n$ and $q_2 < q_1^{\frac{8}{9}(n+1)}$, we have

$$\begin{aligned} |F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2})| &> \frac{1}{q_1^{(1+\alpha)n} q_1^{\frac{8}{9}(n+1)}} \\ &= \frac{1}{q_1^{(\frac{d}{2}+\frac{1}{2d}+\frac{8}{9})n+\frac{8}{9}}} \end{aligned}$$

On the other hand, by the Smallness Theorem and our hypotheses,

$$\begin{aligned}
|F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2})| &\leq c_1^n(|\frac{p_1}{q_1} - \beta|^{n-t} + |\frac{p_2}{q_2} - \beta|) \\
&\leq c_1^n\{(\frac{1}{q_1^{\frac{15}{16}d}})^{n-t} + (\frac{1}{q_2^{\frac{15}{16}d}})\} \\
&\leq c_1^n\{\frac{1}{q_1^{\frac{15}{16}d(\frac{8}{9}n-1)}} + \frac{1}{q_1^{\frac{15}{16}d(\frac{8}{9}n)}}\} \\
&\leq \frac{2c_1^n}{q_1^{\frac{15}{16}d(\frac{8}{9}n-1)}}.
\end{aligned}$$

Since $n \geq 17$ and $q_1 > (2^{\frac{1}{17}}c_1)^{22}$, we have

$$2c_1^n \leq (2^{\frac{1}{17}}c_1)^n \leq q_1^{\frac{n}{22}},$$

and so

$$|F^{(t)}(\frac{p_1}{q_1}, \frac{p_2}{q_2})| \leq \frac{1}{q_1^{\frac{15}{16}d(\frac{8}{9}n-1)-\frac{n}{22}}} = \frac{1}{q_1^{(\frac{5}{6}d-\frac{1}{22})n-\frac{15}{16}d}}.$$

Combining these upper and lower bounds, we see that

$$\frac{1}{q_1^{(\frac{d}{2}+\frac{1}{2d}+\frac{8}{9})n+\frac{8}{9}}} < \frac{1}{q_1^{(\frac{5}{6}d-\frac{1}{22})n-\frac{15}{16}d}}.$$

Since $q_1 > 1$, we must then have

$$(\frac{d}{2}+\frac{1}{2d}+\frac{8}{9})n+\frac{8}{9}>(\frac{5}{6}d-\frac{1}{22})n-\frac{15}{16}d,$$

and so

$$\frac{15}{16}d+\frac{8}{9}>(\frac{1}{3}d-\frac{1}{22}-\frac{8}{9}-\frac{1}{2d})n.$$

Since $d \geq 4$, the quantity in the parenthesis is positive, and so we can conclude that

$$n<\frac{\frac{15}{16}d+\frac{8}{9}}{\frac{1}{3}d-\frac{1}{22}-\frac{8}{9}-\frac{1}{2d}}.$$

But the right-hand side of this inequality is less than 17 for all $d \geq 4$, and $n > 17$ as noted above, providing our contradiction. $\square$

Now we return to the setting of the Approximation theorem. We require two lemmas to connect our dynamical sequence to the Diophantine Approximation just proved. We write $B = |a|b^{d-1}$, recalling that a and b are coprime, so because of our assumption that $\frac{a}{b}$ is not an mth power for any $m \mid d$, neither is B.

Lemma 4.3.2. *Suppose that $n \in \mathbb{N}$ satisfies*

$$|f_c^n(0)|<\frac{1}{b^{\frac{15}{16}d^{n-1}+\frac{1}{16}d}}.$$

Then $\frac{p}{q} := |f_c^{n-1}(0)b| = \frac{|a_{n-1}|}{b^{d^{n-2}-1}}$ is a fraction in lowest terms which satisfies

$$|\frac{p}{q} - \beta| < \frac{1}{q^{\frac{15}{16}d}}.$$

Proof. Note that

$$|f_c^n(0)| = |\frac{a_{n-1}^d}{b^{d^{n-1}}} - \frac{a}{b}| = \frac{1}{b^d}|(\frac{|a_{n-1}|}{b^{d^{n-2}-1}})^d - B| \geq \frac{1}{b^d}|\frac{|a_{n-1}|}{b^{d^{n-2}-1}} - \beta|;$$

the second equality holds because d is even, and the inequality holds because $\beta > 1$ and so for all $x > 0$, we have

$$|x^d - B| = |x - \beta| \cdot |x^{d-1} + x^{d-2}\beta + ... + x\beta^{d-2} + \beta^{d-1}| \geq |x - \beta| \cdot |\beta^{d-1}| > |x - \beta|.$$

So if $n \in \mathbb{N}$ satisfies

$$|f_c^n(0)| < \frac{1}{b^{\frac{15}{16}d^{n-1}+\frac{1}{16}d}},$$

then we have

$$|\frac{p}{q} - \beta| = |\frac{|a_{n-1}|}{b^{d^{n-2}-1}} - \beta| < b^d|f_c^n(0)| \leq \frac{1}{b^{\frac{15}{16}d^{n-1}-\frac{15}{16}d}} = \frac{1}{(b^{d^{n-2}-1})^{\frac{15}{16}d}} = \frac{1}{q^{\frac{15}{16}d}}.$$

□

Lemma 4.3.3. *Suppose that $q_1 \geq b^{d^6-1}$. Then for all $d \geq 4$, q_1 satisfies the bounds*

$$q_1 > c_3^9,$$

$$q_1 > (2^{\frac{1}{17}} c_1)^{22},$$

where these constants are determined with $B = |a| b^{d-1}$.

Proof. Recall that we chose

$$c_1 = (2^{4d^2+2} B^{d+\frac{1}{d}})^{1+\alpha}$$

and

$$c_3 = (2^{6d^2+3} B^{2d})^{1+\alpha}.$$

Since $c_3 < c_1^2$, we need only show that q_1 satisfies the second bound. Since $|c| = \frac{|a|}{b} < 2$, we have $B = |a| b^{d-1} < 2b^d$. Therefore we have

$$\begin{aligned} c_1 &\leq (2^{4d^2+2} 2^{d+\frac{1}{d}} b^{d^2+1})^{\frac{d}{2}+\frac{1}{2d}} \\ &= 2^{2d^3+\frac{1}{2}d^2+3d+1+\frac{1}{d}+\frac{1}{2d^2}} b^{\frac{1}{2}d^3+d+\frac{1}{2d}}, \end{aligned}$$

and so

$$(2^{\frac{1}{17}}c_1)^{22} \leq 2^{44d^3+11d^2+66d+22+\frac{22}{17}+\frac{22}{d}+\frac{11}{d^2}}b^{11d^3+22d+\frac{11}{d}}.$$

Since $b \geq 2$, it suffices to show that

$$q_1 \geq b^{55d^3+11d^2+88d+23+\frac{33}{d}+\frac{11}{d^2}}.$$

But by assumption, $q_1 \geq b^{d^6-1}$, and

$$d^6 - 1 \geq 55d^3 + 11d^2 + 88d + 23 + \frac{33}{d} + \frac{11}{d^2}$$

for all $d \geq 4$, so the lemma is proved.

$\square$

Finally, we note that if $n < m$ is such that

$$|f_c^n(0)| < \frac{1}{b^{\frac{15}{16}d^{n-1}+\frac{1}{16}d}}.$$

and

$$|f_c^m(0)| < \frac{1}{b^{\frac{15}{16}d^{m-1}+\frac{1}{16}d}}.$$

then we cannot have $m = n + 1$, since for all $\epsilon < 1/2$,

$$f_c(\epsilon) = \epsilon^d + c > |c| - \frac{1}{2} > \frac{1}{2}.$$

Therefore if $q_1 = b^{d^{n-2}-1}$ and $q_2 = b^{d^{m-2}-1}$, we have

$$\frac{\log q_2}{\log q_1} \geq \frac{d^{n+2}-1}{d^n - 1} \geq d^2 \geq 16.$$

We can now see the proof of the Approximation Theorem:

Proof of the Approximation Theorem. Suppose towards contradiction that we have $n_2 > n_1 \geq 8$ such that

$$|f_c^{n_i}(0)| < \frac{1}{b^{\frac{15}{16}d^{n_i-1}+\frac{1}{16}d}}.$$

By the above, we have $n_2 > n_1 + 1$. So for $i = 1, 2$, we let

$$\frac{p_i}{q_i} := \frac{|a_{n_i-1}|}{b^{d^{n_i-2}-1}};$$

so that by Lemma 4, $\frac{p_i}{q_i}$ satisfy the first three inequalities of Theorem 4.3.1. Therefore Theorem 4.3.1 implies that for at least one of $i = 1, 2$ we have

$$|\frac{p_i}{q_i} - \beta| > \frac{1}{q_i^{\frac{15}{16}d}}.$$

But by lemma 3, we also have

$$|\frac{p_i}{q_i} - \beta| < \frac{1}{q_i^{\frac{15}{16}d}},$$

which is a contradiction.

□

4.4 Bounding the maximal element of the Zsigmondy set

Theorem 3.2.1 guarantees a maximal element of 2 in the Zsigmondy set except in the possibly recurrent case of d even and $c \in (-2^{\frac{1}{d-1}}, -1)$. However, it is possible regardless of choice of c to use effective Diophantine approximation to bound the maximal element of the Zsigmondy set. In this section, we prove:

Theorem 4.4.1. *Let $f_c(z) = z^d + c$ with $d \geq 2$ and $c \in \mathbb{Q}$ so that the critical orbit is infinite. Then there exists an effectively computable bound $M(c)$ such that $n \in \mathcal{Z}(f_c) \Rightarrow n \leq M(c)$.*

Theorem 4.4.1 follows from an improvement of Schinzel's result (21) on approximation of quadratic irrationals due to Bennett and Bugeaud (11):

Theorem 4.4.2. *[Theorem 1.2 of (11)] Let $||x||$ denote the distance from x to the nearest integer. For every integer $b \geq 2$ and every quadratic real number ξ, there exist positive effectively computable constants $\epsilon(\xi, b)$ and $\tau(\xi, b)$ such that for all $n \geq 1$,*

$$||b^n \xi|| > \frac{\epsilon(\xi, b)}{b^{-(1-\tau(\xi,b))n}}.$$

Proof of Theorem 4.4.1. We may by Theorem 3.2.1 simplify our argument by assuming $c = \frac{a}{b} \in (-2^{\frac{1}{d-1}}, -1)$ and d even, so write $c = -\xi^2$, choosing positive square root ξ. For notational convenience, we denote the constants of Theorem 4.4.2 by ϵ and τ respectively, so that for all $n \geq 1$, we have

$$||b^n \xi|| > \frac{\epsilon}{b^{-(1-\tau))n}}.$$

Then for any $n \geq 1$, we have the following lower bound for $|f_c^n(0)|$:

$$\begin{aligned}
|f_c^n(0)| &> \left| \left(\frac{|a_{n-1}|}{b^{d^{n-2}}} \right)^{\frac{d}{2}} - \xi \right| \\
&= b^{-\frac{1}{2}d^{n-1}} \left| |a_{n-1}| - \xi b^{-\frac{1}{2}d^{n-1}} \right| \\
&\geq b^{-\frac{1}{2}d^{n-1}} ||\xi b^{\frac{1}{2}d^{n-1}}|| \\
&\geq b^{-\frac{1}{2}d^{n-1}} \frac{\epsilon}{b^{\frac{1}{2}(1-\tau)d^{n-1}}} \\
&= \frac{\epsilon}{b^{d^{n-1} - \frac{\tau}{2} d^{n-1}}}
\end{aligned}$$

Suppose now that $n \notin \mathcal{Z}(f_c)$, so that by inequality (2.1) and Lemma 3.3.3, we have

$$d \log |f_c^n(0)| + d^n \log b \leq s_d(n) \log b + d\omega(n) \log |c|,$$

where as before $s_d(n) := \sum_q d^{\frac{n}{q}}$ and $\omega(n) := \sum_q 1$ are sums over the distinct prime factors q of n. Our lower bound on $|f_c^n(0)|$ then implies

$$\log \epsilon + \frac{\tau}{2} d^{n-1} \log b \leq \frac{1}{d} s_d(n) \log b + \omega(n) \log |c|,$$

so

$$(\frac{\tau}{2} d^{n-1} - \frac{1}{d} s_d(n)) \log b \leq \log \frac{1}{\epsilon} + \omega(n) \log |c|.$$

Since τ is a constant, the left-hand side growth will be exponential in n for n sufficiently large, while the right-hand side is $\mathcal{O}(\log n)$. Thus for $n \geq M(c)$ for some sufficiently large $M(c)$, we have a contradiction. Further, since τ and ϵ are effectively computable, $M(c)$ is as well. $\square$

Remark 4.4.3. *The existence of the constant τ is a consequence of an effective linear forms in logarithms bound and is not computed in (11), but has a complicated dependence on ξ. Working through the proof of Bennett and Bugeaud's theorem, τ can be seen to be generally too small for a useful effective bound on the maximal element of the Zsigmondy set; in fact, it is on the order of the reciprocal of the logarithm of the fundamental unit of $\mathbb{Q}(\sqrt{c})$, so $M(c)$ is comparable to the logarithm of the regulator of $\mathbb{Q}(\sqrt{c})$ plus a constant which is large for dynamical purposes. For example, for $f_{-\frac{3}{2}}(z) = z^2 - \frac{3}{2}$ (the minimal height recurrent example) the process gives a value of $M(c)$ close to 80, and computationally checking primitive divisors for 80 iterates is an infeasible task.*

CHAPTER 5

CRITICAL RECURRENCE AND THE GENERALIZED MANDELBROT SET

5.1 Introduction

In Chapter 3 we showed that if $c \notin (-2^{\frac{1}{d-1}}, -1)$, then there is a norm-based obstruction to critical orbit recurrence, and so $M(c)$ is quite small. This is a coarse statement of a more subtle dynamical phenomenon: namely, if c is a parameter which is not close (as a complex number) to any parameter c_n with a period n critical orbit, then $f_c^n(0)$ cannot be close to 0. In this chapter, we provide a bound on critical recurrence of $z^d + c$, which we use to bound $M(c)$ for those $c \in \mathbb{Q}$ which are not too close to centers of hyperbolic components of the Mandelbrot set.

The **Mandelbrot set** $\mathcal{M}$ is the set of parameters c such that the critical orbit of $f_c(z) = z^2 + c$ remains bounded under iteration. We generalize this definition for any $d \geq 2$, and define the **d-Mandelbrot set** $\mathcal{M}_d$ to be the set of complex parameters c such that the critical orbit of $f_c(z) = z^d + c$ remains bounded under iteration. By induction, if $|c| > 2^{\frac{1}{d-1}}$, then $|f_c^n(0)| \geq |c|(|c|^{d-1} - 1)^n \to \infty$, and so

Lemma 5.1.1. *Suppose $|c| > 2^{\frac{1}{d-1}}$. Then $c \notin \mathcal{M}_d$.*

We note the following facts on the multibrot set, which can be found in (22) and (23). If a point z has exact period n, we say the **multiplier** of the periodic cycle is $(f_c^n)'(z)$, and that the cycle is **attracting** if the multiplier has modulus less than 1. Since any attracting basin must contain a critical point, if c is a parameter so that $f_c(z) = z^d + c$ has an attracting cycle, then $c \in \mathcal{M}_d$. A parameter c is **hyperbolic** if $f_c(z) = z^d + c$ has an attracting cycle. The connected components of the set of hyperbolic parameters are known to be open connected components of the interior of the d-Mandelbrot set, and each of these **hyperbolic components** has a unique period n and center c_n so that $f_c(z) = z^d + c_n$ has critical orbit of exact period n. Given a hyperbolic component $\mathcal{H}$ of period n, we define the multiplier map $\rho : \mathcal{H} \to \mathbb{D}$ which sends a parameter c to the multiplier of the unique attracting cycle. The multiplier map is a proper, holomorphic map of degree $d-1$ from $\mathcal{H}$ to the unit disk, and so by the maximum-modulus principle, for any hyperbolic component $\mathcal{H}$ and any $r < 1$, $\{c \in \mathcal{H} : |\rho(c)| < r\}$ is simply connected. Therefore, the maximum-modulus principle yields the following preliminary proposition:

Proposition 5.1.2. *Fix a degree $d \geq 2$, a period n, and $r < 1$. Let $D_{n,r} := \{c \in \mathbb{C} : f_c(z) = z^d + c$ has an attracting cycle of exact period n and multiplier $|\rho(c)| < r\}$. Then $\mathbb{C} \setminus \overline{D_{n,r}}$ is a domain.*

In this chapter, our goal is to achieve a Zsigmondy result for values of c that are not close to hyperbolic centers of the d-Mandelbrot set, by bounding the recurrence of the critical orbit.

5.2 Bounds on critical recurrence

Our goal in this section is to understand critical recurrence in terms of the d-Mandelbrot set. In particular, we find a lower bound for $|f_c^n(0)|$ in terms of the distance from c to a center of a hyperbolic component of period $k \mid n$ that depends on the multiplier $r = \rho(c)$.

Theorem 5.2.1. *Fix $d \geq 2$ and $n \geq 1$ and $0 < r < \frac{1}{4^{d-1}}$, and define $D_{n,r}$ as above. Then for all $c \in \mathbb{C} \setminus (\bigcup_{k|n} D_{k,r})$, we have*

$$|f_c^n(0)| \geq r \cdot \frac{1}{d^{2n+2}}.$$

Proof. Throughout we write $f_c(z) = z^d + c$. Choose a radius R sufficiently large so that $|f_c^n(0)| \gg 1$ for all $|c| \geq R$, and consider the set

$$D(n) = \mathbb{D}(0, R) \cap (\mathbb{C} \setminus \bigcup_{k|n} D_{k,r}).$$

By Proposition 5.1.2, since each $D_{k,r}$ is disjoint, this is a domain in $\mathbb{C}$ which contains no c with $f_c^n(0) = 0$, and so we can apply the maximum-modulus principle to the reciprocal of $f_c^n(0)$ as a function of c on this domain, and we see that the minimum value of $|f_c^n(0)|$ must be obtained on the boundary of $D(n)$. By our choice of R, this minimum is in fact obtained on the boundary of some $D_{k,r}$; i.e. $|f_c^n(0)|$ as a function of c is bounded below on $D(n)$ by the value of $|f_c^n(0)|$ when c is chosen such that 0 lies in an attracting basin of a point a with period k dividing n, with multiplier of modulus r. Thus it suffices to provide a bound for these boundary c.

Suppose c is a parameter such that 0 is in the basin of attraction of a point a of exact period n and multiplier r, and denote the immediate basin of attraction of a by V. Since $f_c(z)$ is a polynomial, the basin V is simply connected, so by uniformization we have a conformal isomorphism $\phi : \mathbb{D} \to V$. Choose coordinates so that $\phi(0) = 0$, and so that the fixed point s of $g(z) := \phi^{-1} \circ f_c^n \circ \phi$ is a positive real number. Note that $f_c^n(z)$ is a proper map on V and has well-defined degree. By the chain rule, 0 is the only critical point of $f_c^n(z)$ which lies inside of V, and it has ramification index d. Therefore, since V is simply connected, the Riemann-Hurwitz formula implies that f_c^n is a degree d self-map of V. So $g(z)$ is a proper, holomorphic, degree d map of the unit disk to itself. Therefore g is a Blaschke product. In fact, g can be made more explicit:

Lemma 5.2.2. *Let s be the unique fixed point of g, and write $\beta := \frac{s-s^d}{1-s^{d+1}}$ and $h(z) := \frac{\beta+z^d}{1+\beta z^d}$. Then there exists $|\theta| = 1$ such that*

$$g = \alpha_s \circ R_\theta \circ \alpha_s \circ h$$

on $\mathbb{D}$, where R_θ is the rotation $z \mapsto e^{i\theta} z$, and $\alpha_s := \frac{z-s}{sz-1}$.

Proof. By (24), since g and h are Blaschke products with the same critical set with multiplicity, there exists some disk automorphism τ with $g = \tau \circ h$. Since both g and h fix the point s (the latter by definition of β), τ fixes s as well, and so $\alpha_s^{-1} \circ \tau \circ \alpha_s$ is a disk automorphism fixing 0; i.e., a rotation by some $|\theta| = 1$. Since $\alpha_s^{-1} = \alpha_s$ by definition, we have

$$\tau = \alpha_s \circ R_\theta \circ \alpha_s,$$

as desired. $\square$

We will prove Theorem 5.2.1 by bounding the recurrence of the Blaschke product g - which we know is quite explicit - then utilizing a double application of de Branges' famous theorem, which controls the distorting effects of the uniformization map ϕ. In order to use de Branges' theorem, we normalize ϕ, by defining $\psi : \mathbb{D} \to \mathbb{C}$ to be

$$\psi(z) = \frac{\phi(z)}{\phi'(0)}.$$

We will bound the following quantity:

$$\frac{|a|}{|f_c^n(0)|} \cdot \frac{|g(0)|}{|s|} = \frac{|\phi(s)|}{|s|} \cdot \frac{|g(0)|}{|\phi(g(0))|} = \frac{|\psi(s)|}{|s|} \cdot \frac{|g(0)|}{|\psi(g(0))|} \tag{5.1}$$

with the deep theorem of de Branges (see (25) or the excellent expository article (26)):

Theorem 5.2.3. *[de Branges] Suppose $\psi(w) : \mathbb{D} \to \mathbb{C}$ is one-to-one, with $\psi(0) = 0$ and $\psi'(0) = 1$. Then the coefficients of the power series expansion*

$$\psi(w) = z + a_2 z^2 + a_3 z^3 + ...$$

satisfy $|a_n| \leq n$ for all $n \geq 2$.

As a consequence of de Branges' theorem, we have:

Corollary 5.2.4.

$$\frac{|\psi(s)|}{|s|} \cdot \frac{|g(0)|}{|\psi(g(0))|} \leq \frac{(1 - |g(0)|)^2}{(1 - s)^2}.$$

Proof. Considering the power series expansion of ψ, we have

$$\frac{|\psi(g(0))|}{|g(0)|} \geq 1 - \sum_{n \geq 2} |a_n||g(0)|^{n-1} \geq 1 - \sum_{n \geq 2} n|g(0)|^{n-1} = \frac{1}{(1 - |g(0)|)^2}.$$

On the other hand,

$$\frac{|\psi(s)|}{|s|} \leq \sum_{n \geq 1} |a_n| s^{n-1} \leq \sum_{n \geq 1} n s^{n-1} = \frac{1}{(1 - s)^2},$$

and combining the two inequalities completes the proof of the corollary. $\square$

By the chain rule, we have

$$r = |(f_c^n)'(a)| = d^n \prod_{0 \leq k < n} |f_c^k(a)|.$$

Since 0 is in the basin of attraction of a, c lies in the d-Mandelbrot set and thus has modulus at most $2^{\frac{1}{d-1}}$. Consequently, $|z| > 2^{\frac{1}{d-1}} \Rightarrow |f_c(z)| = |z| \cdot |z^{d-1} + \frac{c}{z}| > |z|$, and so since a is periodic, each iterate of a has modulus bounded above by $2^{\frac{1}{d-1}}$. So we conclude that

$$|a| \geq r \cdot \frac{1}{d^n 2^{\frac{n-1}{d-1}}} \geq \frac{r}{d^{2n-1}}.$$

Combining this bound with the inequality (5.1) and Corollary 5.2.4 yields

$$|f_c^n(0)| \geq \frac{r}{d^{2n-1}} \cdot \frac{(1-s)^2}{(1-|g(0)|)^2} \cdot \frac{|g(0)|}{s}. \tag{5.2}$$

To complete the proof, we must bound the right hand term below, done in the following lemma:

Lemma 5.2.5. *Suppose $r < \frac{1}{4^{d-1}}$. Then*

$$\frac{(1-s)^2}{(1-|g(0)|)^2} \cdot \frac{|g(0)|}{s} \geq \frac{1}{8}$$

Proof. A straightforward derivative computation yields

$$r = \frac{ds^{d-1}(1-s^2)}{1-s^{2d}} > s^{d-1},$$

so our assumption $r < \frac{1}{4^{d-1}}$ yields $s < \frac{1}{4}$. Similarly, we can compute

$$g(0) = \alpha_s(e^{i\theta}s^2 \cdot \frac{s^d + s^{d-1} - s^2 - 1}{s^d + s^2 - s - 1}).$$

For any $y \in \mathbb{D}$ with $s^2 y \in \mathbb{D}$, we have

$$|\alpha_s(s^2 y)| = \frac{|s^2 y - s|}{|s^3 y - 1|} \geq s \cdot \frac{1 - |sy|}{1 + |s^3 y|}.$$

Since $d \geq 2$ and $s < \frac{1}{4}$, we have $|\frac{s^d + s^{d-1} - s^2 - 1}{s^d + s^2 - s - 1}| < 2$, and so letting

$$y = e^{i\theta} \frac{s^d + s^{d-1} - s^2 - 1}{s^d + s^2 - s - 1},$$

we have

$$\frac{|g(0)|}{s} \geq \frac{1 - s|y|}{1 + s^3|y|} \geq \frac{1 - 2s}{1 + 2s^3} \geq \frac{1}{4},$$

where the last inequality holds because $s > \frac{1}{4}$.

As a consequence, we also have

$$\frac{(1-s)^2}{(1 - |g(0)|)^2} \geq \frac{(1-s)^2}{(1 - \frac{s}{4})^2} \geq \frac{1}{2},$$

and the proof of the lemma is complete. □

The Lemma together with estimate 5.2 complete the proof of Theorem 5.2.1. □

5.3 Critical recurrence and Zsigmondy results

Having bounded the critical recurrence for those c away from centers of hyperbolic components, we achieve a tight Zsigmondy bound for these c:

Theorem 5.3.1. *Define $D(n, r_n)$ as above with $r_n = \min\{\frac{1}{4^{d-1}}, \frac{1}{2^{d^{n-2}}}\}$. Write*

$$\mathcal{D} := \mathbb{C} - \bigcup_{n \in \mathbb{N}} D(n, r_n).$$

Then for all $c = \frac{a}{b} \in \mathcal{D}$, we can take $M(c) = 3$.

We note that the choice of $r_n = \frac{1}{2^{d^{n-2}}}$ in the theorem is on the order of the minimal value to achieve the tightest possible Zsigmondy result.

Proof of Theorem 5.3.1. Define $D(n)$ as above for each n with $\rho_n = \frac{1}{2^{d^{n-2}}}$, and write

$$S := \mathbb{C} - \bigcup_{n \in \mathbb{N}} D(n).$$

Theorem 5.3.1 is shown for non-recurrent c in Chapter 3, so suppose that $c = \frac{a}{b} \in S \cap (-2^{\frac{1}{d-1}}, -1)$. Then if a_n fails to have a primitive prime divisor for $n \geq 3$, we have (as shown in preceding sections)

$$d \log |f_c^n(0)| + d^n \log b \leq d\omega(n) \log 2 + \sum_{q|n} d^{\frac{n}{q}} \log b,$$

where the sum is taken over distinct primes q dividing n, and $\omega(n)$ is the number of distinct primes dividing n. Write $s_d(n) = \sum_{q|n} d^{\frac{n}{q}}$. Then $|c| < 2$ and the lower bound for $|f_c^n(0)|$ obtained above yields

$$(d^n - s_d(n)) \log b < (d\omega(n) \log 2 + d(2n+2) \log d + d^{n-1} \log 2.$$

Since $b \geq 2$, this is false for all $n \geq 4$ if $d \geq 4$. If $d = 2$, this fails for all $n \geq 7$, and if $b \geq 6$, for all $n \geq 4$. It remains to check a finite number of cases to complete the proof, which is done in Appendix A. □

5.4 Search for elements of Zsigmondy sets

We conclude this chapter with a remark that the proof of Theorem 5.3.1 makes it clear where to look for possible values of $c \in \mathbb{Q}$ with elements of their Zsigmondy set greater than 3. In particular, these c must be very good rational approximations of the centers of hyperbolic components; more precisely, they must be convergents to some hyperbolic center. This explains why, for example, we have $3 \in \mathcal{Z}(f_{-\frac{7}{4}})$ for $d = 2$; the hyperbolic center is the non-zero real root of

$$f_c^3(0) = (c^2 + c)^2 + c = 0.$$

This value of c is approximately -1.7549, and has $-\frac{7}{4}$ as a convergent of small height.

It is generally unclear whether another sufficiently good convergent of a hyperbolic center exists, and computation is difficult, since the heights of the elements in the forward orbit grow exponentially. However, some computation is possible for small values of n and d. Mathematica and SAGE were used to check that for the n and d in the table below, the first 50 convergents of the centers of hyperbolic components do not provide parameters c with $n \in \mathcal{Z}(f_c)$, and so 3 is still the largest known element of any Zsigmondy set for $z^d + c$ with $c \in \mathbb{Q}$ (recall from Remark 4.1.2 that we need not check $d = 2$, $n = 3$, since $c = -\frac{7}{4}$ is known to be the only convergent with $3 \in \mathcal{Z}(f_c)$ in this case).

d	n	number of real hyperbolic centers
2	4	2
2	5	3
2	6	5
2	7	9
4	3	1
4	4	2
6	3	1
6	4	2
8	3	1
10	3	1

APPENDICES

Appendix A

APPENDIX A

In this Appendix, we list the necessary computations to finish the proof of Theorem 5.3.1. Recall that $n \in \mathcal{Z}(f_c)$ implies

$$(d^n - s_d(n)) \log b < (d\omega(n) \log 2 + d(2n+2) \log d + d^{n-1} \log 2,$$

which is false for $d \geq 4$ and $n \geq 4$. In the $d = 2$ case, we rearrange the above inequality and take exp:

$$b < 2^{\frac{2\omega(n)+4n+4+2^{n-1}}{2^n - s_2(n)}}.$$

As noted above, if $n \geq 7$, this fails for all $b \geq 2$; for $n = 5, 6$ it fails for $b \geq 3$, and for $n = 4$, fails for $b \geq 6$. Therefore it remains to show that $f_c^n(0)$ has a primitive prime divisor for $n = 4$ for c with denominator at most 5, and the same for $n = 5, 6$ for $c = -\frac{3}{2}$. We do this in Table I below; the primitive prime divisors are marked in bold font.

Appendix A (Continued)

TABLE I

c	a_1	a_2	a_3	a_4	a_5	a_6
$-3/2$	$\mathbf{3}$	3	$3 \cdot \mathbf{5}$	$3 \cdot \mathbf{53}$	$3 \cdot \mathbf{101} \cdot \mathbf{241}$	$3 \cdot 5 \cdot \mathbf{74006161}$

c	a_1	a_2	a_3	a_4
$-4/3$	$\mathbf{2^2}$	2^2	$2^2 \cdot \mathbf{23}$	$2^2 \cdot \mathbf{71}$
$-5/3$	$\mathbf{5}$	$\mathbf{2} \cdot 5$	$5 \cdot \mathbf{7}$	$2 \cdot 5 \cdot \mathbf{971}$
$-5/4$	$\mathbf{5}$	5	$5 \cdot \mathbf{59}$	$5 \cdot \mathbf{1021}$
$-7/4$	$\mathbf{7}$	$\mathbf{3} \cdot 7$	7	$3 \cdot 7 \cdot \mathbf{53} \cdot \mathbf{103}$
$-6/5$	$\mathbf{2} \cdot \mathbf{3}$	$2 \cdot 3$	$2 \cdot 3 \cdot \mathbf{7} \cdot \mathbf{17}$	$2 \cdot 3 \cdot \mathbf{6841}$
$-7/5$	$\mathbf{7}$	$\mathbf{2} \cdot 7$	$7 \cdot \mathbf{97}$	$2 \cdot 7 \cdot \mathbf{6131}$
$-8/5$	$\mathbf{2^3}$	$2^3 \cdot \mathbf{3}$	$2^3 \cdot \mathbf{53}$	$2^3 \cdot 3 \cdot \mathbf{13} \cdot \mathbf{1427}$
$-9/5$	$\mathbf{3^2}$	$\mathbf{2^2} \cdot 3^2$	$3^2 \cdot \mathbf{19}$	$2^2 \cdot 3^2 \cdot \mathbf{18719}$

CITED LITERATURE

1. Bang, A. S.: Taltheoretiske undersogelser. Tidsskrift Mat., 4(5):70–80, 130–137, 1886.

2. Zsigmondy, K.: Zur theorie der potenzreste. Monatsh. Math. Phys., 3(1):265–284, 1892.

3. Carmichael, R. D.: On the numerical factors of the arithmetic forms $\alpha^n + \beta^n$. Annals of Mathematics, 15(1/4):30–70, 1913.

4. Silverman, J.: Wieferich's criterion and the abc-conjecture. J. Number Theory, 30(2):226–237, 1988.

5. Ingram, P. and Silverman, J.: Primitive divisors in arithmetic dynamics. Mathematical Proceedings of the Cambridge Philosophical Society, 146(2):289–302, 2009.

6. Gratton, C., Nguyen, K., and Tucker, T.: Abc implies primitive prime divisors in arithmetic dynamics. http://arxiv.org/abs/1208.2989, 2012.

7. Silverman, J. and Voloch, F.: A local-global criterion for dynamics on $\mathbb{P}^1$. Acta Arith., 137(3):285–294, 2009.

8. Faber, X. and Voloch, F.: On the number of places of convergence of newton's method over number fields. Journal de théorie des nombres de Bordeaux, 23(2):387–401, 2011.

9. Silverman, J.: Iteration of rational maps. Duke Mathematical Journal, 71(3), 1993.

10. Mahler, K.: On the continued fractions of quadratic and cubic irrationals. Ann. Mat. Pura Appl., 30(4):147–172, 1949.

11. Bennett, M. and Bugeaud, Y.: Effective results for restricted rational approximation to quadratic irrationals. preprint: http://www.math.ubc.ca/ bennett/BeBu.pdf, 2011.

12. Krieger, H.: Primitive prime divisors in the critical orbit of $z^d + c$. International Math Research Notices (to appear).

13. Krieger, H., Levin, A., Scherr, Z., and Tucker, T.: Uniform boundedness of s-units in orbits. in preparation.

14. Silverman, J.: The Arithmetic of Dynamical Systems. Springer-Verlag New York, Inc., 2007.

15. Call, G. and Silverman, J.: Canonical heights on varieties with morphisms. Compositio Math., 89(2), 1993.

16. Doerksen, K. and Haensch, A.: Primitive prime divisors in zero orbits of polynomials. (to appear in Integers), 2011.

17. Ingram, P.: Lower bounds on the canonical height associated to the morphism $z^d + c$. Monatshefte für Mathematik, 157:69–89, 2009.

18. Bombieri and Gubler: Heights in Diophantine Geometry. Cambridge University Press, 2006.

19. Nagell, T.: Darstellung ganzer zahlen durch binitre kubische formen mit negativer diskrind-nante. Mathematische Zeitschrift, 28(1):10–29, 1928.

20. Silverman, J. and Tate, J.: Rational Points on Elliptic Curves. Springer-Verlag New York, Inc., 1992.

21. Schinzel, A.: On two theorems of gel'fond and some of their applications. Acta Arith., 13:177–236, 1967.

22. Douady, A. and Hubbard, J.: Itération des polynômes quadratiques complexes. Publications Math. d'Orsay, 1984.

23. Eberlein, D.: Rational parameter rays of multibrot sets. Doctoral dissertation, Technische Universität München.

24. Zakeri, S.: On critical points of proper holomorphic maps on the unit disk. Bulletin of the London Mathematical Society, 30(1), 1998.

25. de Branges, L.: A proof of the bieberbach conjecture. Acta Math., 154:137–152, 1985.

26. Zorn, P.: The bieberbach conjecture. Mathematics Magazine, 59(3):131–148, 1986.

27. Faber, X. and Granville, A.: Prime factors of dynamical sequences. J. Reine Angew. Math., 661:189–214, 2011.

28. Rudin, W.: Real and Complex Analysis. McGraw-Hill Inc., 1987.

29. Thue, A.: Über annäherungswerte algebraischer zahlen. J. Reine Angew. Math., 135:284–305, 1909.

30. Schinzel, A.: Primitive divisors of the expression $a^n - b^n$ in algebraic number fields. J. Reine Angew. Math., 268/269:27–33, 1974.

31. Rice, B.: Primitive prime divisors in polynomial arithmetic dynamics. Integers, 7(1), 2007.

32. Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc., 78(2):523–544, 2008.

33. Hindry, M. and Silverman, J.: Diophantine Geometry: An Introduction. Springer-Verlag New York, Inc., 2000.

VITA

Holly Krieger - Curriculum Vitae

Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
851 S. Morgan Street (M/C 249)
Chicago, IL 60607-7045, USA

hkrieger@uic.edu
http://homepages.math.uic.edu/~hkrieger/

Education

UNIVERSITY OF ILLINOIS AT CHICAGO.

Ph.D. in Mathematics, in progress (finishing June 2013).
Thesis co-advisors: Laura DeMarco and Ramin Takloo-Bighash.

MS in Mathematics, 2008.

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN.

B.S. in Mathematics, 2006.
Minor: Computer Science.

Research

Arithmetic and Algebraic Dynamics, Diophantine Geometry.

Papers

Cohomological conditions on endomorphisms of projective varieties, with P. Reschke.
in preparation.

Uniform boundedness of S-units in orbits, with A. Levin, Z. Scherr, and T. Tucker.
in preparation.

Primitive prime divisors in the critical orbit of $z^d + c$
to appear in *International Math Research Notices.*

Some Consequences of Schanuel's Conjecture, with Cheng et al.
J. Number Theory 129 (2009), no. 6, 1464-1467.

Service

Graduate Student Colloquium, Co-organizer
University of Illinois at Chicago, 2012-2013.

Math Circles Volunteer
Mathematics education and enrichment for middle school students in the Chicago Public Schools, 2012.

Graduate Number Theory Seminar, Organizer
University of Illinois at Chicago, 2009-2011.

Faculty Mentoring Award committee,
University of Illinois at Chicago, 2010, 2012.

Putnam Exam Proctor, 2008 and 2010.

Awards

Emily Mann Peck Scholarship in Mathematics,
University of Illinois at Urbana-Champaign, 2005-2006.

Recent Invited Talks

Cohomological conditions on endomorphisms of projective varieties,
Algebraic geometry seminar, University of Michigan, January 2013.

Primitive Prime Divisors in the critical orbit of $z^d + c$,
JMM Special session in complex dynamics, San Diego, January 2013.

Arithmetic of the critical orbit of totally ramified polynomials,
Geometry, topology, and dynamics Seminar, University of Illinois at Chicago, October 2012.

Bounding recurrence on the boundary of the Mandelbrot set,
Graduate student colloquium, University of Illinois at Chicago, September 2012.

Primitive Prime Divisors in the critical orbit of $z^d + c$,
Semester in complex and arithmetic dynamics research seminar, ICERM, April 2012.