ABC Implies Bang-Zsigmondy Results In Arithmetic Dynamics

by

Chad Gratton

Submitted in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Supervised by

Thomas J. Tucker

Department of Mathematics
Arts, Sciences and Engineering
School of Arts and Sciences

University of Rochester
Rochester, New York

2013
Biographical Sketch

The author was a student at SUNY Albany from September 2000 to May 2003. In May 2003 he earned a B.S. in mathematics (and a minor in computer science) from SUNY Albany, graduating Summa Cum Laude with a grade point average of 3.99 out of 4.00. In addition, Mr. Gratton has been a student in the Ph.D. Mathematics program at the University of Rochester from September 2003 through August 2013. He was awarded a M.A. in mathematics in May 2005 at the University of Rochester after passing the preliminary qualifying exams. Mr. Gratton’s thesis advisor is Thomas Tucker. The University of Rochester awarded him the Dean’s Teaching Fellowship from 2003 to 2008, and the author was a teaching assistant during his time at the University. He worked as an adjunct math instructor teaching calculus and discrete math at the Rochester Institute of Technology (RIT) from 2006 to 2010. In addition, the author has taught calculus, differential equations, and linear algebra at the University of Rochester.

Mr. Gratton has been working under the supervision of Professor Tom Tucker in the Math Department at the University of Rochester since 2010. His main field of study is arithmetic dynamics. Specifically, he is studying Bang-Zsigmondy type problems. The author interested in examining dynamical sequences generated by polynomial or rational functions over number fields or function fields, and determining those functions that generate primitive prime divisors for all but finitely many terms in the sequence. T. Tucker, K. Nguyen and C. Gratton published the paper “ABC Implies Primitive Prime Divisors in Arithmetic Dynamics” in the
Acknowledgments

Thanks to Professor Tucker for all of his patience and helpful suggestions during my time as a student in the Math Department. I would also like to thank my parents for all their support during my time as a graduate student at the University of Rochester.
I have shown in recent work with T. Tucker and K. Nguyen that if \( \varphi \) is a rational function over a number field \( K \) for which the abc-conjecture holds of degree \( d \geq 2 \), then for sufficiently large \( n \), \( \varphi^n(\alpha) \) has a primitive prime divisor for \( \alpha \in K \) that is \( \varphi \)-wandering. The same results holds unconditionally for function fields \( K \), with the caveat that \( \varphi \) is not isotrivial. In my thesis, this work is extended to obtain results about the 2-parameter Bang-Zsigmondy problem.
Contributors and Funding Sources

The core results of this thesis appeared in a paper that I wrote with Tom Tucker and Khoa Nguyen, [Gratton et al., 2012]. The author was funded by NSF Grants DMS-0854839 and DMS-1200749.
# Table of Contents

Biographical Sketch ........................................ ii

Acknowledgments ............................................. iv

Abstract .................................................................. v

Contributors and Funding Sources ............................. vi

1 Introduction ...................................................... 1
   1.1 Exploring the Bang-Zsigmondy Problem ................. 1
   1.2 Basic Concepts In Dynamics ............................... 4
   1.3 Ramification and the Riemann-Hurwitz Formula ...... 10

2 Statement of the Main Theorems ............................ 12
   2.1 One Parameter Bang-Zsigmondy .......................... 12
   2.2 Ingram-Silverman Two Parameter Bang-Zsigmondy Conjecture . 16
   2.3 Ramification Counterexample to Ingram - Silverman Two Parameter Bang - Zsigmondy ............................... 18
   2.4 Reinterpreting the Faber-Granville One-Parameter Bang-Zsigmondy Result .................................................. 19
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5</td>
<td>The Two Parameter Bang-Zsigmondy Theorems</td>
<td>21</td>
</tr>
<tr>
<td>2.6</td>
<td>A Few More Preliminaries</td>
<td>21</td>
</tr>
<tr>
<td>2.7</td>
<td>A Brief Introduction to Heights</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>Roth-$abc$</td>
<td>32</td>
</tr>
<tr>
<td>3.1</td>
<td>Roth-$abc$ for number fields</td>
<td>32</td>
</tr>
<tr>
<td>3.2</td>
<td>Roth-$abc$ for function fields</td>
<td>36</td>
</tr>
<tr>
<td>4</td>
<td>Proofs of the Main Theorems</td>
<td>40</td>
</tr>
<tr>
<td>4.1</td>
<td>Proofs Of One Parameter Bang-Zsigmondy Theorems</td>
<td>40</td>
</tr>
<tr>
<td>4.2</td>
<td>The $v$-adic Chordal Metric</td>
<td>47</td>
</tr>
<tr>
<td>4.3</td>
<td>Two Parameter Bang-Zsigmondy for Bounded Preperiod $m$</td>
<td>52</td>
</tr>
<tr>
<td>4.4</td>
<td>2-Paramter Bang-Zsigmondy for Bounded Period $n$</td>
<td>58</td>
</tr>
<tr>
<td>4.5</td>
<td>Kisaka’s Classification of Exceptions to Baker’s Theorem</td>
<td>63</td>
</tr>
<tr>
<td>5</td>
<td>Further Research Questions</td>
<td>65</td>
</tr>
<tr>
<td>Bibliography</td>
<td></td>
<td>68</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Exploring the Bang-Zsigmondy Problem

Let \((a_n)_{n\geq 0}\) be a sequence of integers. We say that the prime \(p_n\) is a \textbf{primitive prime divisor of} \(a_n\) if \(p_n \mid a_n\), and \(p_n \nmid a_m\) for all \(m < n\). In other words, \(p_n\) divides \(a_n\), and \(p_n\) does not divide any earlier terms in the sequence. Mathematicians have been studying primitive prime divisors since the late 1800s. More recently a number of authors have studied the question of primitive prime factors arising from the iteration of polynomial or rational functions. Letting \(K\) be a number field or a characteristic 0 function field of transcendence degree 1, let \(\varphi(x) \in K(x)\) be a rational function of degree \(d > 1\), and let \(\alpha \in K\). The \(n\)-fold composition of \(\varphi\) is denoted by \(\varphi^n\). It is frequently the case that \(\varphi^n(\alpha)\) has a primitive prime divisor for all but finitely many \(n\). This primitive prime divisor problem was considered by Bang [Bang, 1886], Zsigmondy [Zsigmondy, 1892], and Schinzel [Schinzel, 1974] in the context of the multiplicative group. More recently, many authors have considered the problem in other cases. Most of these results apply either when 0 is preperiodic under \(\varphi\) (see [Faber and Granville, 2011] and [Ingram and Silverman, 2009], for example) or when 0 is a ramification point of \(\varphi\) (see [Doerksen and Haensch, 2012], [Krieger, 2012], and [Rice, 2007]). Much work has been done on this problem in the setting of elliptic curves (refer to [Ingram,
2007] and [Everest et al., 2006], for example). However, here we do not have an underlying algebraic group.

A few examples of primitive prime divisors are given below.

Example 1.1.1. Consider the Fibonacci sequence \((a_n)_{n\geq0}\), where \(a_0 = 0\), \(a_1 = 1\), and \(a_{n+2} = a_{n+1} + a_n\). Then it is known that \(a_n\) has a primitive prime factor \(p_n\) for all \(n > 12\) (see [Faber and Granville, 2011]).

Example 1.1.2. Define \(F_n = 2^{2^n} + 1\). Then \((F_n)_{n\geq0}\) is known as the sequence of Fermat numbers. Notice that the sequence of Fermat numbers are pairwise coprime (refer to [Faber and Granville, 2011]), hence each term \(F_n\) has a (super) primitive prime factor \(p_n\) (by super primitive, we mean that the prime \(p_n\) only divides \(F_n\), and no other terms in the sequence). Notice that

\[
F_{n+1} - 2 = 2^{2^{n+1}} - 1 = (2^{2^n} + 1)(2^{2^n} - 1) = F_n(F_n - 2).
\]

This implies that

\[
F_{n+1} = F_n^2 - 2F_n + 2.
\]

Letting \(\varphi(z) = z^2 - 2z + 2\), we have \(F_0 = 3\) and \(F_{n+1} = \varphi(F_n)\) for \(n \geq 0\). So the Fermat numbers \(F_n\) arise from iteration of this polynomial \(\varphi\).

Given a sequence of integers \((a_n)_{n\geq0}\), define the Zsigmondy set \(Z((a_n)_{n\geq0})\) to be

\[
Z((a_n)_{n\geq0}) = \{n \geq 0 : a_n \text{ does not have a primitive prime divisor}\}.
\]

Example 1.1.3. Let \(a, b \in \mathbb{Z}\) such that \(a > b > 0\). A theorem of Bang and Zsigmondy stated in [Ingram and Silverman, 2009] says that \#\(Z(a^n - b^n) < \infty\). Bang covered the case where \(b = 1\), and Zsigmondy completed the general case. Moreover, if \(a\) and \(b\) are coprime, then for \(n > 6\), we have \(n \notin \mathcal{Z}(a^n - b^n)\), yielding a strong uniform upper bound.

Let \(\varphi \in K(x)\) of degree \(d \geq 2\), \(\alpha, \beta \in K\), \(h_\varphi(\alpha) > 0\), and \(\beta \notin \text{Orb}_\varphi(\alpha)\). We say \(\gamma \in K\) is exceptional if \(\varphi^{-2}(\gamma) = \{\gamma\}\). Further suppose \(\beta\) is not exceptional
for $\varphi$, and define $\Lambda = (\lambda_n)_{n \geq 0}$, where $\lambda_n = \varphi^n(\alpha) - \beta$. Then the main theorem from our paper [Gratton et al., 2012] states that $\# \mathcal{Z}(\Lambda) < \infty$. This result can be reinterpreted to say that for all but finitely many $n$, one can find a prime $p_n$ of $\mathfrak{o}_K$ such that $\varphi^n(\alpha)$ meets $\beta$ modulo $p_n$, but $\varphi^m(\alpha)$ does not meet $\beta$ modulo $p_n$ if $m < n$. And in the case where $\beta = \alpha$, the result can be interpreted as saying that for all but finitely many $n$, one can find a prime $p_n$ of $\mathfrak{o}_K$ such that modulo $p_n$, the point $\alpha$ has exact period $n$, under the map $\varphi$.

Observe that a simple change of variables allows us to reduce to the case where $\beta = 0$. There are two main components to the proof of this result. First, the establishment of a “Roth-abc” result that provides a lower bound on the product of the magnitudes of the primes that occur in $\varphi^n(\alpha)$. The proof of this Roth-abc result is broken up into two cases. Case (I) is when $K$ is a number field. This case uses the abc-Conjecture for number fields together with the existence of Belyi maps (for number fields) in order to establish the lower bound. Case (II) is when $K$ is a function field. Since Belyi maps do not exist over function fields, it is necessary in this case to use a recent result from Yamanoi to establish the desired lower bound. The second component of the proof establishes an upper bound on the size of non-primitive primes. We find that the non-primitive primes occur either from a bounded set or from a relatively low iterate of $\varphi$. Breaking this up into several cases and using the elementary properties of height functions yield the desired upper bound. The case-by-case analysis of this uses the fact that we can find a factor polynomial factor $F$ of degree at least 4 of $\varphi^i$ (for large enough $i$) such that the roots $\gamma_j$ of $F$ are not zeros of previous iterates of $\varphi^j$ (where $j < i$), and all these roots are non-periodic. And in order to guarantee the existence of such a polynomial factor $F$ of the numerator of $\varphi^i$, we use the fact that $\beta$ is non-exceptional to repeatedly take a sufficiently large number of inverse images of $\alpha$ under $\varphi$. In fact, since $\beta$ is non-exceptional, $\varphi^{-3}(\alpha)$ contains at least one point
non-periodic point that is not infinity (we would like to rule out infinity to avoid having to deal with homogenous polynomials). Taking additional third inverse images as necessary until we obtain at least 4 non-periodic (non-infinite) points, then $F$ is chosen to be the minimal polynomial factor of the numerator of $\varphi^i$ that makes these non-periodic inverse images vanish. Finally, since $h_\varphi(\alpha) > 0$, for all sufficiently large $n$, the lower bound of the product of the sizes of the primes occurring in the $n$-iterate exceeds the upper bound of the product of the magnitudes of the non-primitive primes. Hence these inequalities, when combined, produce a primitive prime divisor $p_n$ for all but finitely many $n$.

Notice that our one-parameter Bang-Zsigmondy result is quite general — in fact, we can remove the requirement that $\beta \notin \text{Orb}_\varphi(\alpha)$ if we include the caveat that $m \neq M$ in the statement of the theorem.

1.2 Basic Concepts In Dynamics

A dynamical system consists of a set $A$ and a function $\varphi : A \rightarrow A$. Thus we can define $\varphi^n$ to be the $n$-fold composition of $\varphi$. We let $\varphi^0$ denote the identity map on $A$. Given $\alpha \in A$, define the (forward) orbit of $\alpha$ under $\varphi$ to be

$$\mathcal{O}_\varphi(\alpha) = \{\varphi^n(\alpha) : n \geq 0\} = \bigcup_{n=0}^{\infty}\{\varphi^n(\alpha)\}$$

A point $\alpha \in A$ is periodic if $\varphi^n(\alpha) = \alpha$ for some $n > 0$. We say that $\alpha$ is preperiodic if $\mathcal{O}_\varphi(\alpha)$ is finite. On the other hand, if $\mathcal{O}_\varphi(\alpha)$ is infinite, then we say that $\alpha$ is wandering. Note that $\alpha$ is preperiodic if $\varphi^n(\alpha) = \varphi^m(\alpha)$ for some integers $n > m \geq 0$. Equivalently, $\alpha$ is preperiodic if $\varphi^m(\alpha)$ is periodic for some $m \geq 0$. We define the smallest such $m$ to be the preperiod of $\alpha$. And it is clear from the definitions that any periodic $\alpha \in A$ is preperiodic. If $\alpha$ is preperiodic but not periodic, we will say that $\alpha$ is strictly preperiodic. Let $\text{Per}(\varphi, A)$ denote the set of periodic points of $\varphi$, and $\text{PrePer}(\varphi, A)$ denote the set of preperiodic
points of $\varphi$. The main goal of the discipline of dynamics is to classify the points $\alpha \in A$ according to the behavior of their orbits $O_{\varphi}(\alpha)$. Typical problems are to describe the sets $\text{Per}(\varphi, A)$ and $\text{PrePer}(\varphi, A)$. It is also of interest to describe the periods of the periodic points. Sometimes the set $A$ will have some additional structure (topological, analytic, algebraic, etc.), so it may be possible to describe the interaction of the orbits with that structure. Below are a few examples to acquaint the reader with these definitions. These examples are found in, or are adapted from examples and exercises that appear in Silverman’s book [Silverman, 2007].

**Example 1.2.1.** Consider $\varphi(x) = x^4 - 1$, looking at its action on $\mathbb{Z}$. Observe that

As a result, 1 is strictly preperiodic, while 0 and $-1$ are periodic. Also, all other $z \in \mathbb{Z}$ are wandering, because if $|z| \geq 2$, then $\lim_{n \to \infty} \varphi^n(z) = \infty$.

**Example 1.2.2.** Let $\varphi(z) = z^2 - 1$ on $\mathbb{F}_5$, the field with 5 elements. Then

and
We can see immediately since $F_5$ is a finite set, every $\alpha \in F_5$ must be preperiodic. And from what is written above, it follows that 1 and 2 are strictly preperiodic, while 0, 4, and 3 are periodic.

Let $G$ be an abelian group. Recall that the torsion subgroup of $G$, denoted $G_{\text{tors}}$, is the subgroup of $G$ consisting of precisely those elements of $G$ of finite order. In other words,

$$G_{\text{tors}} = \{ g \in G : g^n = e \text{ for some } n \geq 1 \}.$$ 

**Example 1.2.3.** Let $G$ be an abelian group, let $d \geq 2$ be an integer, and define the map $\varphi : G \to G$ by $\varphi(g) = g^d$. Clearly $\varphi^i(g) = g^{di}$. One can deduce quickly that the set of points preperiodic under $\varphi$ is exactly the torsion subgroup of $G$. For suppose $g$ is preperiodic. Then $\varphi^i(g) = \varphi^j(g)$ for some $i > j \geq 0$. Then

$$g^{di} = g^{dj}$$

Since $G$ is a group, both sides of the above equation can be multiplied by $g^{-dj}$ to obtain

$$g^{di-dj} = e.$$ 

Note that the exponent is positive, therefore $g \in G_{\text{tors}}$.

Now suppose $g \in G_{\text{tors}}$. Then $g^m = e$ for some positive integer $m$. Of course for some positive integers $n > k \geq 0$, we have $d^n \equiv d^k \pmod{m}$. Consequently,

$$\varphi^n(g) = g^{dn} = g^{dk} = \varphi^k(g),$$

since $a^m = e$ and $d^n \equiv d^k \pmod{m}$. Hence $g$ is preperiodic.

**Proposition 1.2.4.** Let $A$ be a finite set. There exists an integer $N$ such that

$$\Per(\varphi, A) = \varphi^n(A) \text{ for all } n \geq N.$$
Proof. Let $N$ be the maximum of the preperiods of all the elements of $A$. It is clear that

$$\text{Per}(\varphi, A) = \bigcup_{l \in L} C_l,$$

where the union is taken over the cycles. Clearly $\bigcup_{l \in L} C_l \subset A$, $\varphi^j(C_l) = C_l$ for any $j \geq 0$, and $\varphi^n(A) \subset \bigcup_{l \in L} C_l$ for all $n \geq N$. In fact, for each cycle $C_l$, the map $\varphi^n$ simply permutes the elements of $C_l$. So $\bigcup_{l \in L} C_l \subset \varphi^n(A)$. Therefore it follows that

$$\text{Per}(\varphi, A) = \bigcup_{l \in L} C_l = \varphi^n(A).$$

\[ \Box \]

**Proposition 1.2.5.** Let $A$ be a set and $\varphi : A \to A$ be a function.

(a) If $A$ is a finite set, $\varphi$ is bijective if and only if $\text{Per}(\varphi, A) = A$.

(b) In general, if $\text{Per}(\varphi, A) = A$, then $\varphi$ is bijective.

(c) If $\varphi$ is injective, then $\text{PrePer}(\varphi, A) = \text{Per}(\varphi, A)$.

**Proof.** (b) We have $\text{Per}(\varphi, A) = A = \bigcup_{l \in L} C_l$. Take $\alpha \in A$. Then $\alpha \in C_{l_0}$ for some $l_0 \in L$. So let $\beta$ be the element in the cycle before $\alpha$, i.e., $\beta = \varphi^{-1}(\alpha)$. Then $\varphi(\beta) = \alpha$, so $\varphi$ is surjective. Now suppose $\varphi(\alpha_1) = \varphi(\alpha_2)$. Then $\alpha_1$ and $\alpha_2$ are being mapped to the same element, hence $\alpha_1$ and $\alpha_2$ belong to the same cycle. Thus these two elements are in the same cycle and are mapped to the same element, hence it must be the case that $\alpha_1 = \alpha_2$. Therefore $\varphi$ is injective, and it is a bijection.

(a) Now that part (b) has been shown, it just remains to prove that in the case that $A$ is finite, that if $\varphi$ is bijective, then $\text{Per}(\varphi, A) = A$. We note that $\varphi$ is just a permutation of the finite set $A$, and therefore the permutation $\varphi$ partitions $A$ up into a disjoint union of cycles. Each $\alpha \in A$ belongs to a cycle, and it follows immediately that each element of $A$ is periodic.

(c) Let $\varphi : A \to A$ be injective. Suppose that $\alpha \in A$ is a point that is preperiodic, but not periodic. Let $m$ be the preperiod of $\alpha$, and let $n$ be the
period of $\varphi^m(\alpha)$. Then $\varphi^{m-1}(\alpha)$ and $\varphi^{m+n-1}(\alpha)$ are distinct elements that map to the same point, namely $\varphi^m(\alpha)$. Thus two distinct points are being mapped to the same image, contradicting the injectivity of $\varphi$. \qed

Example 1.2.6. Consider the infinite set $A = \mathbb{Z}$, and the function

$$\varphi : \mathbb{Z} \to \mathbb{Z} \text{ defined by } \varphi(x) = x + 1.$$  

In this case, $\varphi$ is bijective, but $\text{Per}(\varphi, A) \neq A$. In fact, here $\text{Per}(\varphi, A) = \{\}$. This shows that the converse of (b) does not hold.

We say that a point $P \in A$ is an isolated preperiodic point of $\varphi$ if there are integers $n > m$ such that $\varphi^n(P) = \varphi^m(P)$ and such that the set

$$\{Q \in A : \varphi^n(Q) = \varphi^m(Q)\}$$

is finite.

Proposition 1.2.7. Let $A$ be a set, let $\varphi : A \to A$ and $\psi : A \to A$, and suppose that $\varphi$ and $\psi$ commute, i.e., $\varphi \circ \psi = \psi \circ \varphi$.

(a) $\psi(\text{PrePer}(\varphi)) \subset \text{PrePer}(\varphi)$.

(b) Suppose that $\psi$ is a finite-to-one surjective map. Then $\psi(\text{PrePer}(\varphi)) = \text{PrePer}(\varphi)$.

(c) Suppose every point of $\varphi$ is isolated. Then

$$\text{PrePer}(\varphi) \subset \text{PrePer}(\psi).$$

If the commuting maps $\varphi$ and $\psi$ both have preperiodic points that are all isolated, then

$$\text{PrePer}(\varphi) = \text{PrePer}(\psi).$$

Proof. (a) Let $\alpha \in \text{PrePer}(\varphi)$. So for some integers $m$ and $n$, $\varphi^{m+n}(\alpha) = \varphi^m(\alpha)$. Thus

$$\varphi^{m+n}(\psi(\alpha)) = \psi(\varphi^{m+n}(\alpha)) = \psi(\varphi^m(\alpha)) = \varphi^m(\psi(\alpha)).$$
(b) First suppose that \( B \) is an infinite set, and \( f : B \to B \) is a finite-to-one surjective map. Let \( B' \subset B \), where \( B' \) is also an infinite set. Then \( f(B') \) can not be a finite set. For suppose \( f(B') \) were finite. We have \( B' \subset f^{-1}(f(B')) \). Then by the fact that \( f \) is finite-to-one, \( f^{-1}(f(B')) \) is finite, hence \( B' \) is finite, which is a contradiction. Consequently a finite-to-one surjection \( f : B \to B \) maps infinite sets to infinite sets.

We will need to show \( \text{PrePer}(\varphi) \subset \psi(\text{PrePer}(\varphi)) \). Let \( \alpha \in \text{PrePer}(\varphi) \). So \( \varphi^{m+n}(\alpha) = \varphi^m(\alpha) \). Take \( \beta \in \psi^{-1}(\alpha) \). Suppose that \( O_{\varphi}(\beta) \) is indeed infinite. Consider

\[
\psi(O_{\varphi}(\beta)) = \{\psi(\beta), \psi(\varphi(\beta)), \psi(\varphi^2(\beta)), \ldots\} = \{\psi(\beta), \varphi(\psi(\beta)), \varphi^2(\psi(\beta)), \ldots\}
\]

But \( O_{\varphi}(\alpha) \) is given to be finite, as \( \alpha \) is preperiodic under \( \varphi \). By the equation above, \( \psi(O_{\varphi}(\beta)) \) is also finite, yet this set is the image of an infinite set under the finite-to-one surjection \( \psi \), which yields the desired contradiction. Therefore \( O_{\varphi}(\beta) \) must have been finite, which means that \( \beta \) was indeed preperiodic under \( \varphi \). And \( \varphi(\beta) = \alpha \) since \( \beta \) is in the preimage of \( \alpha \), concluding the proof.

(c) Take an isolated \( \alpha \in \text{PrePer}(\varphi) \). Let \( m \) be the preperiod of \( \alpha \), and let \( n \) be the period. Now consider the equation

\[
\varphi^{m+n}(\psi(\alpha)) = \varphi^m(\psi(\alpha)),
\]

as \( \alpha \) varies over all elements of \( A \). Letting \( \psi(\alpha) = Q \) and noting that there are only finitely many such \( Q \) because \( \alpha \) is isolated, we see that \( \psi(\alpha) \) can only take on finitely many values as \( \alpha \) ranges over all of \( S \). Hence \( O_{\psi}(\alpha) \) is finite, so \( \alpha \) is preperiodic under \( \psi \), i.e., \( \alpha \in \text{PrePer}(\psi) \).

If all of the preperiodic points of \( \psi \) are also isolated, then we obtain (by symmetry) \( \text{PrePer}(\psi) \subset \text{PrePer}(\varphi) \). Combining this with \( \text{PrePer}(\varphi) \subset \text{PrePer}(\psi) \), the equality \( \text{PrePer}(\psi) = \text{PrePer}(\varphi) \) is immediate. \( \square \)
1.3 Ramification and the Riemann-Hurwitz Formula

The material in this section is covered in more detail in [Silverman, 2007]. Suppose a rational function $\varphi(z) = F(z)/G(z)$ is given. Then the formal derivative

$$\varphi'(z) = \frac{G(z)F'(z) - F(z)G'(z)}{G(z)^2}$$

is defined at any point $\alpha$ satisfying $\alpha \neq \infty$ and $G(\alpha) \neq 0$.

Expanding around $z = \alpha$, the conclusion of Taylor’s theorem yields

$$\varphi(z) = \varphi(\alpha) + \varphi'(\alpha)(z - \alpha) + O((z - \alpha)^2).$$

The rational function $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ is ramified at $\alpha$ if $\varphi'(\alpha) = 0$. We say in this case that $\alpha$ is a ramification point of $\varphi$.

Assume $\alpha \neq \infty$ and $\varphi(\alpha) \neq \infty$. Then the ramification index of $\varphi$ at $\alpha$ is

$$e_\alpha(\varphi) = \text{ord}_\alpha(\varphi(z) - \varphi(\alpha)).$$

So $\varphi$ is ramified at $\alpha$ if and only if $e_\alpha(\varphi) \geq 2$. Locally, there exists a constant $c \neq 0$ such that

$$\varphi(z) = \varphi(\alpha) + c(z - \alpha)^{e_\alpha(\varphi)} + O((z - \alpha)^{e_\alpha(\varphi)+1}),$$

and $\varphi$ is locally $e_\alpha(\varphi)$-to-one in a neighborhood of $\alpha$. Notice $e_\alpha(\varphi) \leq \deg(\varphi)$. In the case that $e_\alpha(\varphi) = \deg(\varphi)$, we say that $\varphi$ is totally ramified at $\alpha$.

**Theorem 1.3.1** (Riemann-Hurwitz Formula for $\mathbb{P}^1$).

$$2 \deg(\varphi) - 2 = \sum_{\alpha \in \mathbb{P}^1} (e_\alpha(\varphi) - 1).$$

And we have the following corollary to Theorem 1.3.1 that is often useful.

**Corollary 1.3.2.** Let $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ be a rational map.
(i) Let $\alpha \in \mathbb{P}^1(\mathbb{C})$. Then

$$\sum_{\beta \in \varphi^{-1}(\alpha)} e_{\beta}(\varphi) = \deg(\varphi).$$

(ii) Weak Riemann-Hurwitz Formula:

$$2 \deg(\varphi) - 2 = \sum_{\alpha \in \mathbb{P}^1(\mathbb{C})} (d - \# \varphi^{-1}(\alpha)).$$

One immediate consequence of part (i) of Corollary 1.3.2 is the following. The map $\varphi$ is totally ramified at $\alpha$ if and only if

$$\varphi^{-1}(\{\varphi(\alpha)\}) = \{\alpha\}.$$

In other words, the preimage of $\varphi(\alpha)$ under the map $\varphi$ is just the set containing the point $\alpha$. So $\varphi$ is totally ramified at $\alpha$ if and only if $\alpha$ is the only point in $\mathbb{P}^1(\mathbb{C})$ that is mapped to $\varphi(\alpha)$ by $\varphi$. 
2 Statement of the Main Theorems

2.1 One Parameter Bang-Zsigmondy

We will say that a field $K$ is an \textbf{abc-field} if $K$ is a number field satisfying the abc-conjecture [Vojta, 1987] or a characteristic zero function field of transcendence degree 1. We define the \textbf{strict forward orbit} $\text{Orb}_\varphi(\alpha)$ of a point $\alpha$ under a map $\varphi$ to be $\text{Orb}_\varphi(\alpha) = \bigcup_{i=1}^{\infty}\{\varphi^i(\alpha)\} = \mathcal{O}_\varphi(\alpha)\setminus\{\alpha\}$. If we had changed the definition of orbit in the paper to start with $\alpha$, then the condition that $\beta \notin \text{Orb}_\varphi(\alpha)$ in Theorems 2.1.1 and 2.1.2, and Corollaries 2.1.3 and 2.1.4 would need to be changed to $\beta \notin (\text{Orb}_\varphi(\alpha)\setminus\{\alpha\})$. Starting the orbit with $\varphi(\alpha)$ makes the statement of the theorems and corollaries easier to interpret, so we have left the orbit starting with $\varphi(\alpha)$. The most general results here are most naturally stated in terms of the canonical height $h_\varphi$ of Call and Silverman [Call and Silverman, 1993] (see Section 2 for its definition and a few of its basic properties).

In keeping with the terminology of [Ingram and Silverman, 2009] and [Schinzel, 1974], we say that $p$ is a \textbf{primitive prime factor} of $\varphi^n(\alpha) - \beta$ if $v_p(\varphi^n(\alpha) - \beta) > 0$ and $v_p(\varphi^m(\alpha) - \beta) \leq 0$ for all $m < n$. We say that $p$ is a \textbf{square-free primitive prime factor} if $v_p(\varphi^n(\alpha) - \beta) = 1$ and $v_p(\varphi^m(\alpha) - \beta) \leq 0$ for all $m < n$.

With this notation and terminology, the main theorem of our paper is the
Theorem 2.1.1. Let $K$ be an abc field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $h_\varphi(\alpha) > 0$ and $\beta \notin \text{Orb}_\varphi(\alpha)$. Suppose that $\beta$ is not exceptional for $\varphi$. Then for all but finitely many positive integers $n$, there is a prime $p$ of $K$ such that $p$ is a primitive prime factor of $\varphi^n(\alpha) - \beta$.

We will say that $\varphi$ is dynamically unramified over $\beta$ if there are infinitely many $\tau \in K$ such that $\varphi^n(\tau) = \beta$ and $e_{\varphi^n}(\tau/\beta) = 1$ for some $n$, where $e_{\varphi^n}(\tau/\beta)$ is the ramification index of $\varphi^n$ at $\tau$ over $\beta$. Since $\varphi$ has only finitely many critical points, saying $\varphi$ is dynamically unramified over $\beta$ means that there is at least one infinite backward orbit that contains no critical points.

Theorem 2.1.2. Let $K$ be an abc field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $h_\varphi(\alpha) > 0$ and $\beta \notin \text{Orb}_\varphi(\alpha)$. Suppose $\varphi$ is dynamically unramified over $\beta$. Then for all but finitely many positive integers $n$, there is a prime $p$ of $K$ such that $p$ is a square-free primitive prime factor of $\varphi^n(\alpha) - \beta$.

In fact, the conclusion of Theorem 2.1.2 is false for any $\varphi$ that fails to be dynamically unramified over $\beta$; see Remark 4.1.5. This is most easily seen in the case of maps such as $\varphi(x) = (x - a)^2$, which have the property that $\varphi^n(\alpha)$ is always a perfect square because $\varphi^n$ itself is a perfect square in the field of rational functions.

Theorem 2.1.2 shows that the abc-conjecture implies what Jones and Boston call the “Strong Dynamical Wieferich Prime Conjecture” [Boston and Jones, 2009, Conjecture 4.5] . Silverman [Silverman, 1988] had earlier shown that the abc-conjecture implies a logarithmic lower bound on the growth of the number of Wieferich primes; a Wieferich prime is a prime $p$ for which $2^{p-1} \not\equiv 1 \pmod{p^2}$.

Theorems 2.1.1 and 2.1.2 may also be stated in terms of wandering $\alpha$. We say that $\alpha$ is wandering if $\varphi^n(\alpha) \neq \varphi^m(\alpha)$ for all $n > m > 0$; this is equivalent to
saying that $\text{Orb}_\varphi(\alpha)$ is infinite. It follows immediately from Northcott’s theorem (as stated on page 94 of [Silverman, 2007]) that $h_\varphi(\alpha) \neq 0$ if and only if $\alpha \in K$ is wandering for $\varphi \in K(x)$, where $K$ is a number field and $\deg \varphi > 1$ (see [Call and Silverman, 1993]). By work of Benedetto and Baker [Benedetto, 2005] and [Baker, 2009], one has the same result for non-isotrivial rational functions over a function field. A rational function over a function field $K$ is said to be isotrivial if it cannot be defined over a finite extension of the field of constants of $K$, up to change of coordinates; more precisely we say that $\varphi$ is isotrivial if there exists $\psi \in \overline{K}(x)$ of degree 1 such that $(\psi^{-1} \circ \varphi \circ \psi) \in \overline{k}(x)$, where $\psi^{-1}$ is the compositional inverse of $\psi$ (i.e., $\psi^{-1}(\psi(x)) = x$ in $\overline{K}(x)$).

Baker’s result says that if $K$ is a function field and $\varphi \in K(x)$ is a non-isotrivial map with $\deg \varphi > 1$, then $\alpha \in K$ is wandering if and only if $h_\varphi(\alpha) \neq 0$.

Thus, the following are immediate corollaries of Theorem 2.1.1 and 2.1.2.

**Corollary 2.1.3.** Let $K$ be an abc field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $\alpha$ is wandering and $\beta \notin \text{Orb}_\varphi(\alpha)$. Suppose that $\beta$ is not exceptional for $\varphi$ and $\varphi$ is non-isotrivial if $K$ is a function field. Then for all but finitely many positive integers $n$, there is a prime $p$ of $K$ such that $p$ is a primitive prime factor of $\varphi^n(\alpha) - \beta$.

**Corollary 2.1.4.** Let $K$ be an abc field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $\alpha$ is wandering and $\beta \notin \text{Orb}_\varphi(\alpha)$. Suppose $\varphi$ is dynamically unramified over $\beta$ and that $\varphi$ is non-isotrivial if $K$ is a function field. Then for all but finitely many positive integers $n$, there is a prime $p$ of $K$ such that $p$ is a square-free primitive prime factor of $\varphi^n(\alpha) - \beta$.

The strategy of the proofs of Theorems 2.1.1 and 2.1.2 is fairly simple. First, we show, in Propositions 3.1.4 and 3.2.2, that if $F$ is a polynomial of reasonably high degree without repeated roots, then for any $\tau$ of large height, the product of the distinct prime factors of $F(\tau)$ is large, assuming the abc-conjecture in the
number field case (following Granville [Granville, 1998], we call these “Roth-abc” theorems). We then apply this to an appropriate factor $F$ of the numerator of a power $\varphi^i$ of $\varphi$, after proving, in Proposition 4.1.1, that the product of the distinct factors of $\prod_{\ell=1}^{n-1} \varphi^\ell(\alpha)$ that are also factors of $F(\varphi^{n-i}(\alpha))$ must be very small. With at most finitely many exceptions, any prime that divides $F(\varphi^{n-i}(\alpha))$ also divides $\varphi^n(\alpha)$, so $\varphi^n(\alpha)$ must then have a factor that is not a factor of $\varphi^m(\alpha)$ for any $m < n$. This finishes the proof when $\beta = 0$, and a simple coordinate change argument, Lemma 4.1.3, gives the case of arbitrary $\beta \in K$.

An outline of the proof of the one-parameter Bang-Zsigmondy results is as follows. We begin by setting our notation and terminology in Section 2.6. In Section 3.1 we modify a result of Granville [Granville, 1998] that enables us to say, roughly, that polynomials without repeated factors take on “reasonably square-free” values in general, assuming the abc-conjecture; this is Proposition 3.1.4. Then, in Section 3.2, we derive the same result for function fields, unconditionally, using recent work of Yamanoi [Yamanoi, 2004]; this is Proposition 3.2.2. This enables us to give a proof of our main results in Section 4.1, using Proposition 4.1.1.

For the sake of completeness, I have included material from Sections 2, 3, 4, and 5 of the paper that I wrote with Tom Tucker and Khoa Nguyen, “ABC Implies Primitive Prime Divisors In Arithmetic Dynamics” ([Gratton et al., 2012]). This appears in Sections 2.6, 3.1, 3.2, and 4.1 of the thesis. I have modified the content of these sections to add further explanations, diagrams, and to enhance readability.
2.2 Ingram-Silverman Two Parameter Bang-Zsigmondy Conjecture

Let
\[(U_{m,n})_{m \geq 0, n \geq 1}\]
be a doubly indexed sequence of ideals. Following [Ingram and Silverman, 2009], we say that \(p\) is a \textbf{primitive prime divisor} of \((U_{m,n})\) if

\[p \mid U_{m,n} \text{ and } p \nmid U_{i,j} \text{ for all } i, j \text{ with } 0 \leq i < m \text{ or } 1 \leq j < n.\]

Notice that the above condition can be rephrased as

\[p \mid U_{m,n} \text{ and } p \mid U_{r,s} \text{ implies } r \geq m \text{ and } s \geq n.\]

Then define the \textbf{Zsigmondy set} \(Z(U_{m,n})\) to be

\[Z(U_{m,n}) = \{(m, n) | n \geq 1, m \geq 0 \text{ and } U_{m,n} \text{ has no primitive prime divisors}\}\]

Ingram and Silverman in [Ingram and Silverman, 2009] state the following:

\textbf{Conjecture 2.2.1. (Ingram - Silverman)} Let \(K\) be a number field, let \(\varphi(z) \in K(z)\) be a rational function of degree \(d \geq 2\), and let \(\alpha \in K\) be a \(\varphi\)-wandering point. For each \(n \geq 1\) and \(m \geq 0\), write the ideal

\[(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = U_{m,n}B_{m,n}^{-1}\]

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

Unfortunately there are a number of counterexamples to this conjecture of Ingram and Silverman. Indeed, Faber and Granville, in [Faber and Granville,
detail the cases in which this conjecture fails. Define $\mathcal{F}_1$ to be those $\phi(t) \in \mathbb{Q}(t)$ of the form $\sigma^{-1} \circ \psi \circ \sigma$ for some linear $\sigma(t) = \lambda t + \beta$ with $\lambda \neq 0$, where

$$\psi(t) = \frac{t^2}{t+1} \text{ or } \frac{t^2}{2t+1}.$$  

Then Faber and Granville prove in [Faber and Granville, 2011] that the numerator of $x_{m+1} - x_m$ have the same prime factors for all $m$, and for all sufficiently large $m$ the denominator of $x_m$ has a primitive prime factor, which also divides the denominator of $x_{m+1}$. Define $\mathcal{B}_{n,d}$ to be the set of all $\varphi(t) \in \mathbb{C}(t)$ of degree $d$ such that $\varphi$ has no periodic point of exact period $n$. Then a theorem of Baker shows that $\mathcal{B}_{n,d}$ is non-empty if and only if \((n, d) \in \{(2, 2), (2, 3), (2, 4), (3, 2)\}\). So define $\mathcal{F}_2 = \bigcup_{d=2}^3 \mathcal{B}_{2,d}$ along with with set of all rational maps $\varphi(t)$ of the form $\varphi = \sigma^{-1} \circ \psi \circ \sigma$ for some $\sigma(t) = \frac{\alpha t - \beta}{\gamma t - \delta}$ with $\alpha \delta - \beta \gamma \neq 0$ and $\psi(t) = \frac{1}{t^2}$. Let $\mathcal{F}_3 = \mathcal{B}_{3,2}$. Then the classes $\mathcal{F}_1, \mathcal{F}_2$, and $\mathcal{F}_3$ all provide counterexamples to the 2-parameter Bang-Zsigmondy conjecture of Ingram and Silverman. We call $p_{n,m}$ a **doubly primitive prime factor** if $p_{n,m}$ divides the numerator of $x_{m+n} - x_m$, and if $M \geq m$ and $D \geq n$ whenever $p_{n,m}$ divides the numerator of $x_{M+D} - x_M$. Then [Faber and Granville, 2011] give the following modified conjecture, taking into account the counterexamples listed above:

**Conjecture 2.2.2.** (Faber - Granville) Suppose that $\varphi(t) \in \mathbb{Q}(t)$ has degree $d \geq 2$. Let $x_0 \in \mathbb{Q}$ and define $x_{m+1} = \varphi(x_m)$ for each $n \geq 0$, and suppose that the sequence $(x_m)_{m \geq 0}$ is not eventually periodic. The numerator of $x_{m+n} - x_m$ has a doubly primitive prime factor for all $m \geq 0$ and $n \geq 1$, except for those pairs with $n = 1, 2, \text{ or } 3$ when $\varphi \in \mathcal{F}_1, \mathcal{F}_2$, or $\mathcal{F}_3$, respectively, as well as for finitely many other exceptional pairs $(n, m)$.

In fact, [Faber and Granville, 2011] show that the above conjecture becomes a theorem when the period $n$ is uniformly bounded. The precise statement is given below:
Theorem 2.2.3. (Faber - Granville) Suppose that \( \varphi(t) \in \mathbb{Q}(t) \) has degree \( d \geq 2 \). Let \( x_0 \in \mathbb{Q} \) and define \( x_{m+1} = \varphi(x_m) \) for each \( n \geq 0 \), and suppose that the sequence \((x_m)_{m\geq0}\) is not eventually periodic. For any given \( N \geq 1 \), the numerator of \( x_{m+n} - x_m \) has a doubly primitive prime factor for all \( m \geq 0 \) and \( N \geq n \geq 1 \), except for those pairs with \( n = 1, 2, \) or \( 3 \) when \( \varphi \in \mathcal{F}_1, \mathcal{F}_2, \) or \( \mathcal{F}_3 \), respectively, as well as for finitely many other exceptional pairs \((n, m)\).

2.3 Ramification Counterexample to Ingram - Silverman Two Parameter Bang - Zsigmondy

Let \( K \) be a number field or a characteristic 0 function field of transcendence degree 1. Let \( k_p \) denote the residue field of \( p \). Assume that \( \varphi \) is a rational function over \( K \) of degree \( d \geq 2 \), and \( z \in K \). Define the reduction map \( r_p : \mathbb{P}^1(K) \to \mathbb{P}^1(k_p) \) as follows: \( r_p(z) = z \) (mod \( p \)) if \( z \in K \) and \( v_p(z) \geq 0 \), and let \( r_p(z) = \infty \) otherwise. Notice that this definition of “reduction modulo \( p \)” of an element of \( \mathbb{P}^1(K) \) is consistent with Silverman’s definition (on pages 48 - 49 of [Silverman, 2007]) of the reduction map modulo \( p \) on projective space. If \( r_p(z) = r_p(z') \), then we say that \( z \) meets \( z' \) modulo \( p \).

We say \( p_{m,n} \) is a two-primitive meeting prime of the pair \((\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))\) if \( \varphi^{m+n}(\alpha) \) meets \( \varphi^{m}(\alpha) \) modulo \( p_{m,n} \), and \( \varphi^{m'}+n'(\alpha) \) does not meet \( \varphi^{m'}(\alpha) \) modulo \( p_{m,n} \) for all integers \( m' \) and \( n' \) satisfying \( 0 \leq m' < m \) or \( 1 \leq n' < n \). In other words, \( p_{m,n} \) is a two-primitive meeting prime of the pair \((\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))\) if modulo \( p_{m,n} \), the element \( \varphi^{m}(\alpha) \) has exact period \( n \) and no previous iterate \( \varphi^{j}(\alpha) \) (for \( j < m \)) is periodic modulo \( p_{m,n} \). The above definition can also be modified in the case where the second coordinate of the pair is fixed. Specifically, we say \( p_n \) is a primitive meeting prime of the pair \((\varphi^n(\alpha), \beta)\) if \( \varphi^n(\alpha) \) meets \( \beta \) modulo \( p_n \), but \( \varphi^{j}(\alpha) \) does not meet \( \beta \) modulo \( p \) for any \( j < n \). Similarly, we say that \( p_n \)
is a \textbf{primitive meeting prime} of the pair $(\varphi^{m+n}(\alpha), \varphi^m(\alpha))$ if $\varphi^{m+n}(\alpha)$ meets $\varphi^m(\alpha)$ modulo $p_n$, and $\varphi^{m+j}(\alpha)$ does \textit{not} meet $\varphi^m(\alpha)$ for $1 \leq j < n$. Thus $\varphi^m(\alpha)$ has \textit{exact} period $n$ modulo the prime $p_n$. Observe that here it may be the case that previous iterates $\varphi^{m'}(\alpha)$ (where $0 \leq m' < m$) are periodic modulo $p_n$.

Next we define the Zsigmondy set $Z$ as follows: $Z((\varphi^{m+n}(\alpha), \varphi^m(\alpha)))$ is

$\{(m, n)|n \geq 1, m \geq 0, \text{ and } (\varphi^{m+n}(\alpha), \varphi^m(\alpha)) \text{ has no two-primitive meeting primes}\}$.

With the above notation, and assuming that $\alpha$ is a $\varphi$-wandering point, the two parameter Bang-Zsigmondy conjecture of Silverman and Ingram says that the Zsigmondy set $Z((\varphi^{m+n}(\alpha), \varphi^m(\alpha)))$ is finite.

Below we provide a simple counterexample to this two parameter Bang-Zsigmondy conjecture. Suppose that $\varphi$ is totally ramified at $\varphi^{m-1}(\alpha)$. Then the \textit{only} point in the preimage of $\varphi^m(\alpha)$ under $\varphi$ is $\varphi^{m-1}(\alpha)$. Then clearly $\varphi^{m-1}(\alpha)$ is periodic if and only if $\varphi^{m}(\alpha)$ is periodic. But then for every $n$, the pair $(m, n) \in Z((\varphi^{m+n}(\alpha), \varphi^m(\alpha)))$. Hence the Zsigmondy set is infinite in this case.

### 2.4 Reinterpreting the Faber-Granville One-Parameter Bang-Zsigmondy Result

The one-parameter Bang-Zsigmondy result of [Faber and Granville, 2011] is as follows.

\textbf{Theorem 2.4.1. (Faber-Granville)} Suppose $\varphi(t) \in \mathbb{Q}(t)$ has degree $d \geq 2$, and that a positive integer $n$ is given. Let $x_0 \in \mathbb{Q}$ and define $x_{m+1} = \varphi(x_m)$ for each $m \geq 0$. If the sequence $\{x_m\}_{m \geq 0}$ is not eventually periodic, then the numerator of $x_{m+n} - x_m$ has a \textit{primitive} prime divisor for all sufficiently large $m$, except if $\varphi \in \mathcal{F}_1$ and $n = 1$. In the case $\varphi \in \mathcal{F}_1$ and $n = 1$, the numerator of $x_{m+1} - x_m$ has the same prime factors for all $m$, and for all sufficiently large $m$ the denominator of $x_m$ has a \textit{primitive} prime factor, which also divides the denominator of $x_{m+1}$. 
Notice that the set of exceptions $\mathcal{F}_1$ is comprised of two affine conjugacy classes that are characterized by the fact that the point $\infty$ is fixed, and all other fixed points are totally ramified. So the $\varphi \in \mathcal{F}_1$ are exceptions for dynamical reasons.

**Remark 2.4.2.** If $n = 1$ and $\varphi \in \mathcal{F}_1$, then from Theorem 2.4.1 we can find a prime $p$ of $\mathbb{Q}$ such that $r_p(x_{m+1}) = r_p(x_m) = \infty$ while $r_p(x_j) \neq \infty$ for any $0 \leq j < m$. Modulo the prime $p$ under the map $\varphi$, the point $x_m \equiv \infty$ is a fixed point, and no previous iterates $x_j$ are periodic modulo $p$.

**Remark 2.4.3.** The conclusion of Theorem 2.4.1 can be restated more simply using the reduction map $r_p$: There exists a prime $p$ of $\mathbb{Q}$ such that $r_p(x_{m+n}) = r_p(x_m)$, and for all $0 \leq j < m$, we have $r_p(x_{j+n}) \neq r_p(x_j)$.

**Remark 2.4.4.** The conclusion of Theorem 2.4.1 also says that there exists a prime $p$ of $\mathbb{Q}$ such that $x_{m+n}$ meets $x_m$ modulo $p$, and for all $0 \leq j < m$, the point $x_{j+m}$ does not meet $x_j$. Equivalently, modulo the prime $p$ under the map $\varphi$, the point $x_m$ is periodic with period dividing $n$, while no previous iterates $x_j$ are periodic modulo $p$.

Thus we see that defining primitive prime divisors in terms of the reduction map $r_p$ allows us to more simply state Bang-Zsigmondy results, whereas the Faber-Granville focus on finding primitive prime divisors of numerators of differences of terms in dynamical sequences introduces complications when $\varphi \in \mathcal{F}_1$ and $n = 1$. Specifically, in this case the complication is that we do not have primitive prime divisors occurring in the numerator of $x_{m+1} - x_m$. Rather, the denominator of $x_m$ has a primitive prime divisor that also divides the denominator of $x_{m+1}$, and this can be interpreted via the reduction map $r_p$, as shown in the above remarks.
2.5 The Two Parameter Bang-Zsigmondy Theorems

Theorem 2.5.1. Let $\varphi(x)$ be a rational function over the $abc$-field $K$ of degree $d \geq 2$. Suppose no point in the orbit of $\alpha$ is totally ramified for $\varphi$, and furthermore suppose that the parameter $m$ is bounded. If $K$ is a function field, assume that $\varphi$ is non-isotrivial. If $K$ is a number field, assume that the $abc$-conjecture holds over all number fields. Then for all but finitely many $(m, n)$, the pair $(\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))$ has a two-primitive meeting prime.

Theorem 2.5.2. Let $K$ be a number field or a characteristic 0 function field of transcendence degree 1. If $K$ is a function field, assume that $\varphi$ is non-isotrivial. Suppose that $\varphi(t) \in K(t)$ has degree $d \geq 2$. Let $x_0 \in K$ be $\varphi$-wandering. For any given $L \geq 1$, the pair $(\varphi^{m+n}(x_0), \varphi^{m}(x_0))$ has a two-primitive meeting prime for all $m \geq 0$ and $L \geq n \geq 1$, except for the following cases:

- $(n, d) = (2, 2)$ and $\varphi \in B_{2,2}$; or
- $(n, d) = (2, 3)$ and $\varphi \in B_{2,3}$; or
- $(n, d) = (2, 4)$ and $K$ is a number field and $\varphi \in B_{2,4}$; or
- $(n, d) = (3, 2)$ and $K$ is a number field and $\varphi \in B_{3,2}$; or
- finitely many other exceptional $(m, n)$.

2.6 A Few More Preliminaries

We set the following:

- $K$ is a number field or one-dimensional function field of characteristic 0;
• if $K$ is a function field, we let $k$ denote its field of constants;

• $p$ is a finite prime of $K$;

• $k_p$ is the residue field of $p$;

• if $K$ is a number field, then we let $N_p = \frac{\log(\#k_p)}{[K : \mathbb{Q}]}$;

• if $K$ is a function field, then we let $N_p = [k_p : k]$;

• $\varphi \in K(x)$ is a rational function of degree $d > 1$.

All of this is completely standard with one exception: the quantity $N_p$ has been normalized in the case of number fields. We divide by $[K : \mathbb{Q}]$ in our definition so that we can use the same proofs (without reference to possible normalization factors) for number fields and function fields in Section 4.1.

When $K$ is a number field, we let $\mathfrak{o}_K$ denote the ring of algebraic integers of $K$ as usual. When $K$ is a function field, we choose a prime $r$, and let $\mathfrak{o}_K$ denote the set $\{ z \in K \mid v_p(z) \geq 0 \text{ for all primes } p \neq r \text{ in } K \}$.

If $K$ is a number field, the height of $\alpha \in K$ is

$$
 h(\alpha) = - \sum_{\text{primes } p \text{ of } \mathfrak{o}_K} \min(v_p(\alpha), 0) N_p + \frac{1}{[K : \mathbb{Q}]} \sum_{\sigma : K \hookrightarrow \mathbb{C}} \max(\log |\sigma(\alpha)|, 0).
$$

(2.6.0.1)

(Note that the $\sigma : K \hookrightarrow \mathbb{C}$ is simply all maps from $K$ to $\mathbb{C}$; in particular, we do not identify complex conjugate embeddings in any way.) We extend our definition of $h(\alpha)$ to the point at infinity by setting $h(\infty) = 0$.

If $K$ is a function field, the height of $\alpha \in K$ is

$$
 h(\alpha) = - \sum_{\text{primes } p \text{ of } K} \min(v_p(\alpha), 0) N_p.
$$

In either case, for $\alpha \neq 0$ the product formula gives the inequality

$$
 \sum_{v_p(\alpha) > 0} v_p(\alpha) N_p \leq h(\alpha).
$$

(2.6.0.2)
We will work with the canonical height $h_{\varphi}$, which is defined as
\[
h_{\varphi}(z) = \lim_{n \to \infty} \frac{h(\varphi^n(z))}{d^n}
\] (2.6.0.3)
The convergence of the right-hand side follows from a telescoping series argument due to Tate. The canonical height has the following important properties:

\[
h_{\varphi}(\varphi(z)) = dh_{\varphi}(z) \text{ for all } z \in K; \tag{2.6.0.4}
\]

there is a constant $C_{\varphi}$ such that $|h(z) - h_{\varphi}(z)| < C_{\varphi}$ for all $z \in K$. (2.6.0.5)

It follows immediately from (2.6.0.4) and (2.6.0.5) that

\[
h_{\varphi}(\alpha) \neq 0 \iff \lim_{s \to \infty} h(\varphi^s(\alpha)) = \infty. \tag{2.6.0.6}
\]

We refer the readers to the work of Call and Silverman [Call and Silverman, 1993] for details on the proofs of the various properties of $h_{\varphi}$.

We say that a point $\alpha$ is preperiodic if there exist $n > m > 0$ such that $\varphi^m(\alpha) = \varphi^n(\alpha)$; we will say that $\alpha$ is periodic if there is an $n > 0$ such that $\varphi^n(\alpha) = \alpha$. Note that a point is wandering if and only if it is not preperiodic.

We write $\varphi(x) = P(x)/Q(x)$ for $P, Q \in \mathfrak{o}_K[x]$ having no common roots in $\overline{K}$. Then we may write $\varphi^i(x) = P_i(x)/Q_i(x)$, where $P_i$ and $Q_i$ are defined recursively in terms of $P$ and $Q$. This is most easily explained by passing to homogeneous coordinates. We let $p(x, y)$ and $q(x, y)$ be the degree $d$ homogenizations of $P$ and $Q$ respectively. Set $p_0(x, y) = x$ and $q_0(x, y) = y$. Then we define recursively

\[
p_i(x, y) = p(p_{i-1}(x, y), q_{i-1}(x, y)),
\]

and

\[
q_i(x, y) = q(p_{i-1}(x, y), q_{i-1}(x, y))
\]

for all $i \geq 1$. Letting $P_i = p_i(x, 1)$ and $Q_i = q_i(x, 1)$ then gives our $P_i$ and $Q_i$. We will say that $p$ is a prime of weak good reduction if $P(x)$ and $Q(x)$
have no common root modulo $p$ and the polynomials $p(1,y)$ and $q(1,y)$ have no common roots modulo $p$. The reason this notion is called weak good reduction is because we are only ruling out common roots in the residue field $k_p$. Note that we are allowing common roots in $k_p$. When $p$ is a prime of weak good reduction, $\phi$ induces a well-defined map from $k_p \cup \infty$ to itself. To describe this, let $r_p$ be the reduction map $r_p : K \rightarrow k_p \cup \infty$ given by $r_p(z) = z \pmod{p}$ if $v_p(z) \geq 0$, and let $r_p(z) = \infty$ otherwise. Then letting $\phi(r_p(z)) = r_p(\phi(z))$ defines a well-defined map on residue classes and thus gives the desired map. So if $r_p(z_1) = r_p(z_2)$, then $r_p(\phi(z_1)) = r_p(\phi(z_2))$. Thus $\phi$ takes residue classes to residue classes. We will make use of this in Proposition 4.1.1.

It turns out that the condition of a rational map having weak good reduction at $p$ is required in order for a rational map $\phi$ to be well-defined on $k_p \cup \infty$. Included below is a counterexample to show why weak good reduction is needed.

**Example 2.6.1.** Let $p$ be a prime integer, and let $p$ be a prime of $K$ such that $p | p$. Define

$$\phi(z) = \frac{z(z-1)}{z-p}.$$  

First note that this map $\phi$ does not have weak good reduction at $p$, because modulo $p$, $0$ is a common root of the numerator and denominator of $\phi$. Observe that $\phi(0) = 0$, while $\phi(p+p^2) = \frac{-1 + 2p^2 + p^3}{p}$. Thus the image of $0$ under $\phi$ modulo $p$ is $0 = [0 : 1]$, while the image of $p+p^2$ under the map $\phi$ modulo $p$ is $\infty = [-1 : 0]$. Yet $r_p(0) = r_p(p+p^2)$. Therefore this map $\phi$ is not well-defined on $k_p \cup \infty$.

When $K$ is a function field, we say that $\phi$ is isotrivial if $\phi = \sigma^{-1} \psi \sigma$ for some $\sigma \in \overline{K}(x)$ with $\deg \sigma = 1$ and some $\psi \in \overline{k}(x)$, where $k$ is the field of constants in $K$. Here $\sigma^{-1}$ is the compositional inverse of $\sigma$; we have $\sigma(\sigma^{-1}(x)) = \sigma^{-1}(\sigma(x)) = x$ in the field $\overline{K}(x)$.

Finally, a few words on notation and conventions. The zeroth iterate of any map is taken to be the identity. Since our maps $\phi$ are rational, rather than
polynomials, they induce maps from \( K \cup \{ \infty \} \) to \( K \cup \{ \infty \} \). When \( \varphi^a(\alpha) = \infty \) and \( \beta \in K \), we say that for any prime \( p \), we have \( v_p(\infty - \beta) = 0 \) if \( v_p(\beta) \geq 0 \) and \( v_p(\infty - \beta) = -v_p(\beta) \) if \( v_p(\beta) < 0 \).

When \( \varphi^n(\tau) = \beta \), we let \( e_{\varphi^n}(\tau/\beta) \) denote the ramification index of \( \varphi^n \) at \( \tau \) over \( \beta \).

### 2.7 A Brief Introduction to Heights

Standard references for the material on heights below include Sections 1.4 - 1.5 and Chapter 2 of [Bombieri and Gubler, 2006] and [Call and Silverman, 1993]. In dynamics, we are interested in studying the arithmetic properties of points in projective space. In order to this, we will need a way to measure the “size” of a point. And it would be quite nice to have the “size” of a point be closely related to the point’s arithmetic complexity. This measure of size or arithmetic complexity will be called the **height**. And it will be extremely helpful if there are only finitely many points of bounded height. In order to get a handle on this issue of size and arithmetic complexity, let’s examine a simple example.

**Example 2.7.1.** Let \( \alpha \in \mathbb{Q} \). Then we could define the height of \( \alpha \), \( H(\alpha) \), to be 

\[
H(\alpha) = |\alpha|.
\]

Unfortunately, this is not a good definition for \( H(\alpha) \), as for any \( \alpha \neq 0 \), there are infinitely many \( \beta \in \mathbb{Q} \) such that \( H(\beta) \) is bounded above by \( \alpha \).

**Example 2.7.2.** Let \( \alpha = a/b \in \mathbb{Q} \), where \( \gcd(a, b) = 1 \). Then we will define the height of \( \alpha \), \( H(\alpha) \), by

\[
H(\alpha) = \max\{|a|, |b|\}.
\]

Notice that this definition of height provides a fine measure of the arithmetic complexity of \( \alpha \), and also if \( B \) is a fixed positive integer, then there are at most
2B + 1 points \( \beta \in \mathbb{Q} \) such that \( H(\beta) \leq B \). Hence with this definition, there are only \textit{finitely} many points of bounded height. As a result, this definition of height is much better than what was proposed in the previous example.

Our next task is to extend this definition of height to projective space. This is done in the next example.

\textbf{Example 2.7.3.} Let \( P \in \mathbb{P}^N(\mathbb{Q}) \). Write \( P = [x_0 : x_1 : \ldots : x_N] \), where \( x_0, \ldots, x_n \in \mathbb{Z} \), and \( \gcd(x_0, x_1, \ldots, x_N) = 1 \). It is always possible to write \( P \in \mathbb{P}^N(\mathbb{Q}) \) in this way, since one can always clear denominators, and cancel out common factors. Then define the height of \( P \), \( H(P) \), to be

\[
H(P) = \max\{|x_0|, |x_1|, \ldots, |x_N|\}.
\]

If \( B \) is a positive integer, then there are at most \((2B + 1)^{N+1}\) points \( \beta \in \mathbb{P}^1(\mathbb{Q}) \) satisfying \( H(\beta) \leq B \), meaning that there are just finitely many points of bounded height.

Next we will want to define the notion of the height of a point for an arbitrary number field \( K \). The only problem is that, in general, the ring of integers \( \mathcal{O}_K \) is not a principal ideal domain. Consequently, there is no uniform way to normalize the homogeneous coordinates of \( P \in \mathbb{P}^N(K) \). However, with a bit of work and terminology, we can use the theory of absolute values to obtain the proper notion of normalization.

- \( \mathcal{M}_\mathbb{Q} \) will denote the set of absolute values on \( \mathbb{Q} \). \( \mathcal{M}_\mathbb{Q} \) contains one absolute value corresponding to the usual absolute value (the archimedean one), and one absolute value for each prime \( p \) (the nonarchimedean ones).

- Similarly, \( \mathcal{M}_K \) will denote the set of absolute values on \( K \). Observe that \( \mathcal{M}_K \) consists of all absolute values that restrict to an absolute value on \( \mathbb{Q} \).

- \( \mathcal{R}_K = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ for all nonarchimedean } v \} \), the usual ring of integers of \( K \).
• Suppose $S$ is a finite set that contains all the archimedean valuations on $K$.
Then the ring of $S$-integers, $R_S$, is defined by

$$R_S = \{ \alpha \in K : |\alpha|_v \leq 1 \text{ for all } v \not\in S \}.$$ 

So $\alpha \in S$ is $S$-integral if $\alpha$ is integral outside of the set $S$.

Given an absolute value $v \in M_K$, let $K_v$ be the completion of $K$ at $v$. The local degree of $v$ is $n_v = [K_v : \Q_v]$. Two important results concerning absolute values from algebraic number theory are listed below for the reader’s convenience.

**Proposition 2.7.4.** (Extension Formula) Let $L/K/\Q$ be a tower of number fields, and let $v \in M_K$ be an absolute value on $K$. Then

$$\frac{1}{[L : K]} \sum_{w \in M_L \text{ such that } w|v} n_w = n_v.$$ 

The notation $w | v$ means that the restriction of $w$ to $K$ is equal to $v$, so the sum is taken over all absolute values on $L$ that extend the absolute value $v$ on $K$.

**Proposition 2.7.5.** (Product Formula) Let $K/\Q$ be a number field. Then

$$\prod_{v \in M_K} |\alpha|_v^{n_v} = 1 \text{ for all } \alpha \in K^*.$$ 

Let $K/\Q$ be a number field, and let $P \in \mathbf{P}^N(K)$ be a point with homogeneous coordinates $P = [x_0 : x_1 : \ldots : x_N]$, where $x_0, x_1, \ldots, x_N \in K$. Then the height of $P$ (relative to $K$) is

$$H_K(P) = \prod_{v \in M_K} \max\{|x_0|_v, |x_1|_v, \ldots, |x_N|_v\}^{n_v}.$$ 

**Proposition 2.7.6.** Suppose we have a fixed coordinate system, and let $K/\Q$ be a number field and $P \in \mathbf{P}^N(K)$ a point. Then

(i) $H_K(P)$ is independent of the choice of homogeneous coordinates for $P$.
(ii) $H_K(P) \geq 1$.
(iii) Let $L/K$ be a finite extension. Then $H_L(P) = H_K(P)^{[L:K]}$. 

Let \( P \in \mathbf{P}^N(\overline{\mathbb{Q}}) \) be a point whose coordinates are algebraic numbers. The \textbf{(absolute) height} of \( P \), denoted by \( H(P) \), is defined by choosing any number field \( K \) such that \( P \in \mathbf{P}^N(K) \) and setting
\[
H(P) = H_K(P)^{1/[K:\mathbb{Q}]},
\]
We see that part (iii) of the previous proposition tells us that this quantity \( H(P) \) is indeed well-defined.

**Theorem 2.7.7.** \( \text{Let } K/\mathbb{Q} \text{ be a number field, let } P \in \mathbf{P}^N(\overline{\mathbb{K}}), \text{ and let } \sigma \in \text{Gal}(\overline{\mathbb{K}}/\mathbb{K}). \text{ Then} \)
\[
H(\sigma(P)) = H(P).
\]

The above theorem says that the height is invariant under the action of the Galois group. The next theorem says that there are only finitely many points on \( \mathbf{P}^N(\overline{\mathbb{Q}}) \) of bounded height and degree — this is one of the most important properties of heights. Specifically,

**Theorem 2.7.8.** \( \text{Let } K/\mathbb{Q} \text{ be a number field, and let } B \text{ be any constant. Then} \)
\[
\#\{P \in \mathbf{P}^N(K) : H_K(P) \leq B\} < \infty.
\]

More generally, for any constants \( B \) and \( D \),
\[
\#\{P \in \mathbf{P}^N(\overline{\mathbb{Q}}) : H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\} < \infty.
\]

And it is also worth noting the following.

**Theorem 2.7.9.** \( \text{(Kronecker) Let } \alpha \in \overline{\mathbb{Q}} \text{ be a nonzero algebraic number. Then} \)
\[
H(\alpha) = 1 \text{ if and only if } \alpha \text{ is a root of unity.}
\]

The next theorem is an importat result. It says that up to a scalar factor, a morphism of degree \( d \) raises the height to the \( d^{\text{th}} \) power.
Theorem 2.7.10. Let $\varphi : \mathbb{P}^N(\overline{K}) \to \mathbb{P}^M(\overline{K})$ be a morphism of degree $d$. Then there are positive constants $C_1$ and $C_2$, depending on $\varphi$, such that

$$C_1 H(P)^d \leq H(\varphi(P)) \leq C_2 H(P)^d$$

for all $P \in \mathbb{P}^N(\overline{K})$.

So the height of $\varphi(P)$ is roughly equal to the $d^{th}$ power of $H(P)$, which means that the height $H$ is a multiplicative type of function. It is usually easier to work with an additive function. We can turn this multiplicative function into an additive function by taking logarithms. Specifically, the **logarithmic height** (relative to $K$) is the function

$$h_K : \mathbb{P}^N(K) \to \mathbb{R}, \text{ defined by } h_K(P) = \log H_K(P).$$

And the **absolute logarithmic height** is the function

$$h : \mathbb{P}^N(\overline{Q}) \to \mathbb{R}, \text{ defined by } h(P) = \log H(P).$$

Rephrasing the result of Theorem 2.7.10, there exists a constant $C_\varphi$ such that

$$|h(\varphi(P)) - dh(P)| \leq C_\varphi.$$

In other words, $h(\varphi(P))$ and $dh(\varphi(P))$ differ by a bounded amount. The following theorem, due to Northcott, can be found in [Northcott, 1950].

**Theorem 2.7.11.** (Northcott) Let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over a number field $K$. Then the set of preperiodic points $\text{PrePer}(\varphi) \subset \mathbb{P}^N(\overline{K})$ is a set of bounded height. In particular,

$$\text{PrePer}(\varphi, \mathbb{P}^N(K)) = \text{PrePer}(\varphi) \cap \mathbb{P}^N(K)$$

is a finite set, and more generally, for any $D \geq 1$, the set

$$\bigcup_{[L:K] \leq D} \text{PrePer}(\varphi, \mathbb{P}^N(L))$$

is finite.
The following construction was originally in [Call and Silverman, 1993], and the convergence of the limit below is due to a telescoping sum argument by Tate.

**Theorem 2.7.12.** Let $S$ be a set, let $d > 1$ be a real number, and let $\varphi : S \to S$ and $h : S \to \mathbb{R}$ satisfying
\[
h(\varphi(P)) = dh(P) + O(1) \text{ for all } P \in S.
\]
Then the limit
\[
h_\varphi(P) = \lim_{n \to \infty} \frac{h(\varphi^n(P))}{d^n}
\]
exists and satisfies:

(i) $h_\varphi(P) = h(P) + O(1)$, and

(ii) $h_\varphi(\varphi(P)) = dh_\varphi(P)$.

The function $h_\varphi : S \to \mathbb{R}$ is uniquely determined by the properties (i) and (ii).

Let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$. The **canonical height function** (associated to $\varphi$) is the unique function $h_\varphi : \mathbb{P}^N(\bar{\mathbb{Q}}) \to \mathbb{R}$ satisfying $h_\varphi(P) = h(P) + O(1)$ and $h_\varphi(\varphi(P)) = dh_\varphi(P)$. The existence and uniqueness of $h_\varphi$ follows immediately from the previous theorem.

It turns out that the canonical height provides a very useful way to identify preperiodic points of $\varphi$, as we shall see below.

**Theorem 2.7.13.** Let $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over $\mathbb{Q}$ and let $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$. Then $P$ is preperiodic if and only if $h_\varphi(P) = 0$.

**Proof.** Assume that $h_\varphi(P) = 0$. We let $K$ be a number field containing the coordinates of $P$ and the coefficients of $\varphi$. So $P \in \mathbb{P}^N(K)$ and $\varphi$ is defined over $K$. Because $h_\varphi(P) = 0$,
\[
h(\varphi^n(P)) = h_\varphi(\varphi^n(P)) + O(1) = d^n h_\varphi(P) + O(1) = O(1) \text{ for all } n \geq 0.
\]
Consequently
\[
O_\varphi(P) = \{P, \varphi(P), \varphi^2(P), \varphi^3(P), \ldots\} \subset \mathbb{P}^N(K)
\]
is a set of bounded height. Therefore the orbit of $P$ under $\varphi$ is finite, implying that $P$ is preperiodic.

Conversely suppose that $P$ is preperiodic. Then $\mathcal{O}_\varphi(P)$ is finite, which means that as $n$ ranges over all of the non-negative integers, $h(\varphi^n(P))$ takes on only finitely many values. So there exists a constant $\kappa$ such that for all $n \geq 0$, $h(\varphi^n(P)) \leq \kappa$. As a result,

$$h_\varphi(P) = \lim_{n \to \infty} \frac{h(\varphi^n(P))}{d^n} \leq \lim_{n \to \infty} \frac{\kappa}{d^n} = 0.$$  

Thus $h_\varphi(P) = 0$. \hspace{1cm} \Box
3 Roth-abc

3.1 Roth-abc for number fields

The main result of this Section, Proposition 3.1.4, is a direct translation of [Granville, 1998, Theorem 5] into the more general setting of number fields. Following Granville, we refer to this as a “Roth-abc” type result, because it can be interpreted as a strengthening of Roth’s theorem [Roth, 1955] (in particular the $-2-\epsilon$ here plays the same role as the the $2+\epsilon$ in Roth’s theorem). The techniques are the same as those of [Granville, 1998]. We include a full proof for the sake of completeness. The methods here are also quite similar to those of [Elkies, 1991] (see especially page 105) and [Bombieri and Gubler, 2006, Theorem 14.4.16].

Let $K$ be a number field. We will be using a version of the “abc-Conjecture for Number Fields”. Recall our definition of $h(z)$ for $z \in K$ from (2.6.0.1). For $n \geq 2$, we may extend this definition to an $n$-tuple $(z_1,\ldots,z_n) \in K^n \setminus \{(0,\ldots,0)\}$ by letting

$$h(z_1,\ldots,z_n) = -\sum_{\text{primes } p \text{ of } s_K} \min(v_p(z_1),\ldots,v_p(z_n)) N_p + \frac{1}{[K:Q]} \sum_{\sigma:K\rightarrow C} \max(\log |\sigma(z_1)|,\ldots,\log |\sigma(z_n)|). \tag{3.1.0.1}$$

Note that when $z_2 \neq 0$, we have $h(z_1,z_2) = h(z_1/z_2,1) = h(z_1/z_2)$. 
For any \((z_1,\ldots,z_n) \in (K^*)^n\), we define

\[ I(z_1,\ldots,z_n) = \{ \text{primes } p \text{ of } \mathcal{O}_K \mid v_p(z_i) \neq v_p(z_j) \text{ for some } 1 \leq i, j \leq n \} \]

and let

\[ \text{rad}(z_1,\ldots,z_n) = \sum_{p \in I(z_1,\ldots,z_n)} N_p. \]

With all of this notation set, the abc-Conjecture for number fields says the following.

**Conjecture 3.1.1.** For any \(\epsilon > 0\), there exists a constant \(C_{K,\epsilon}\) such that for all \(a,b,c \in K^*\) satisfying \(a + b = c\), we have \(h(a,b,c) < (1 + \epsilon) \text{rad}(a,b,c) + C_{K,\epsilon}\).

Following Granville [Granville, 1998], we start by proving a homogeneous form of Roth-abc. Let \(S\) be a finite set of finite primes of \(K\). We will say that a pair \((z_1,z_2) \in \mathcal{O}_K\) is in \(S\)-reduced form if they have no common prime factors outside of \(S\), that is \(\min(v_p(z_1),v_p(z_2)) = 0\) for all \(p \not\in S\). We will use a well-known result of Belyi [Belyï, 1979].

**Lemma 3.1.2.** Given any homogeneous \(f(x,y) \in K[x,y]\), we can determine homogeneous polynomials \(a(x,y),b(x,y),c(x,y) \in \mathcal{O}_K[x,y]\) satisfying \(a(x,y) + b(x,y) = c(x,y)\), all of degree \(D \geq 1\), with no common linear factors, where \(a(x,y)b(x,y)c(x,y)\) has exactly \(D + 2\) non-proportional linear factors (over \(\overline{K}\)), which include all the factors of \(f(x,y)\).

The conclusion of Lemma 3.1.2 ([Belyï, 1979]) can be more cleanly stated as follows: The divisor of \(abc\) in \(\mathbb{P}^1(\overline{K})\) is a sum of \(D + 2\) points, each having multiplicity 1. Now let \(Q(p)\) be a condition involving the prime \(p\). Then when a sum of the following form appears, \(\sum_{Q(p)}\), interpret this to mean that the indicated sum is being taken over all (finite) primes \(p\) satisfying the condition \(Q(p)\). We may then prove the following.
Proposition 3.1.3. Let \( f(x, y) \in \mathfrak{o}_K[x, y] \) be a homogeneous polynomial of degree 3 or more without repeated factors. Let \( \epsilon > 0 \) and let \( S \) be a finite set of finite places of \( K \). Suppose that \( K \) is a number field satisfying the abc Conjecture. Then

\[
(deg f - 2 - \epsilon) h(z_1, z_2) \leq \left( \sum_{v_p(f(z_1, z_2)) > 0} N_p \right) + O_{K,S,\epsilon,f}(1)
\]

for all \((z_1, z_2) \in \mathfrak{o}_K\) in \( S\)-reduced form.

Proof. We begin by applying Lemma 3.1.2 to obtain \( a(x, y), b(x, y), c(x, y) \in \mathfrak{o}_K[x, y] \) of degree \( D \) where \( a(x, y)b(x, y)c(x, y) \) has exactly \( D + 2 \) non-proportional linear factors (over \( \overline{K} \)), which include all the factors of \( f(x, y) \), and \( a(x, y) + b(x, y) = c(x, y) \). Write the product of the factors of \( a(x, y)b(x, y)c(x, y) \) as \( f(x, y)g(x, y) \).

Then applying the abc-Conjecture for number fields, we obtain

\[
(1 - \epsilon/D) h(a(z_1, z_2), b(z_1, z_2)) \leq \left( \sum_{p \in I(a(z_1, z_2), b(z_1, z_2), c(z_1, z_2))} N_p \right) + O_{K,S,\epsilon,f}(1).
\]

Now, \( a, b, \) and \( c \) have no common linear factors and \((z_1, z_2)\) is in \( S\)-reduced form, so, possibly after enlarging \( S \), we have a finite set \( S \) of primes, depending only on \( a, b, c \) and \( K \). Note that

\[
I(a(z_1, z_2), b(z_1, z_2), c(z_1, z_2)) \setminus S = \{ p : v_p(a(z_1, z_2)b(z_1, z_2)c(z_1, z_2)) > 0 \} \setminus S.
\]

Since \( a(x, y)b(x, y)c(x, y) \) has the same prime factors as \( f(x, y)g(x, y) \), we therefore have

\[
\left( \sum_{p \in I(a(z_1, z_2), b(z_1, z_2), c(z_1, z_2))} N_p \right) \leq \left( \sum_{v_p(f(z_1, z_2)) > 0} N_p \right) + \left( \sum_{v_p(g(z_1, z_2)) > 0} N_p \right) + O_{K,S,\epsilon,f}(1),
\]

so

\[
(1 - \epsilon/D) h(a(z_1, z_2), b(z_1, z_2)) \leq \left( \sum_{v_p(f(z_1, z_2)) > 0} N_p \right) + \left( \sum_{v_p(g(z_1, z_2)) > 0} N_p \right) + O_{K,S,\epsilon,f}(1).
\]

(3.1.3.1)
By basic properties of height functions, we have
\[\sum_{v_p(g(z_1,z_2))>0} N_p \leq h(g(z_1,z_2)) \leq (D + 2 - \deg f)h(z_1,z_2) + O_{K,S,\epsilon,f}(1),\]
since \(g\) has degree \(D + 2 - \deg f\). Similarly, using the assumption at \(a(x,y)\) and \(b(x,y)\) have no common factors, we have
\[h(a(z_1,z_2),b(z_1,z_2)) + O_{K,S,\epsilon,f}(1) \geq D(h(z_1,z_2)).\]
Substituting these inequalities into (3.1.3.1) gives
\[(\deg f - 2 - \epsilon)h(z_1,z_2) \leq \left(\sum_{v_p(f(z_1,z_2))>0} N_p\right) + O_{K,S,\epsilon,f}(1)\]
as desired. \(\square\)

**Proposition 3.1.4.** Let \(F(x) \in \mathfrak{o}_K[x]\) be a polynomial of degree 3 or more without repeated factors. Suppose \(K\) is a number field satisfying the abc Conjecture. Then, for any \(\epsilon > 0\), there is a constant \(C_{F,\epsilon}\) such that
\[\sum_{v_p(F(z))>0} N_p \geq (\deg F - 2 - \epsilon)h(z) + C_{F,\epsilon}\]
for all \(z \in K\).

**Proof.** For any finite set \(S\) of finite primes, let \(\mathfrak{o}_{K,S}\) denote as usual the ring of \(S\)-integers of \(K\). By the finiteness of the class group, we can (effectively) find an \(S\), depending only on \(K\), so that \(\mathfrak{o}_{K,S}\) is a principal ideal domain. Then we may write any \(z \in K\) as \(z = z_1/z_2\) with \((z_1,z_2)\) in \(S\)-reduced form.

Let \(g(x,y)\) be the homogenization of \(F(x)\) so that \(g(x,1) = F(x)\) and \(g(z_1,z_2) = z_2^{\deg f}F(z_1)\). Let \(f(x,y) = yg(x,y)\). Let
\[T_1 = \{\text{primes } p : \min(v_p(z_1),v_p(z_2)) > 0\}.\]
Note that we can take \(S = T_1\). Let \(T_2\) be the set of primes such that \(|a_n|_p \neq 1\) for some nonzero coefficient \(a_n\) of \(F\) (note that \(T_1\) and \(T_2\) are finite and depend...
only on $K$ and $F$). Then for all $p \notin T_1 \cup T_2$, we have $v_p(F(z)) \neq 0$ if and only if $v_p(f(z_1, z_2)) > 0$. Thus, we have

$$\left( \sum_{v_p(F(z)) \neq 0} N_p \right) + O_{F, \epsilon}(1) \geq \sum_{v_p(f(z_1, z_2)) > 0} N_p.$$ 

Since $h(z) = h(z_1, z_2)$ and $\deg f = \deg F + 1$, applying Proposition 3.1.3 gives

$$\left( \sum_{v_p(f(z_1, z_2)) > 0} N_p \right) + O_{F, \epsilon}(1) \geq (\deg F - 1 - \epsilon)h(z_1, z_2). \quad (3.1.4.1)$$

For $p \notin T_1 \cup T_2$, we have $v_p(F(z)) < 0$ exactly when $v_p(z) < 0$, so

$$\sum_{v_p(F(z)) < 0} N_p \leq h(z) + O_{F, \epsilon}(1).$$

Thus, we have a constant $C_{F, \epsilon}$ such that $\sum_{v_p(F(z)) > 0} N_p \geq (\deg F - 2 - \epsilon)h(z) + C_{F, \epsilon}$, as desired.

\[\square\]

### 3.2 Roth-abc for function fields

Using Yamanoi’s theorem [Yamanoi, 2004, Theorem 5] which establishes a conjecture of Vojta for function fields (see also [Gasbarri, 2009] and [McQuillan, 2012]), we obtain a function field analog of Proposition 3.1.4. Note that a more general implication is proved by Vojta in [Vojta, 1998], see also [Vojta, 2011, p. 202]. In the special case needed here, we include a short proof for the sake of completeness.

Let $V$ be a curve over a function field $K$, and let $\gamma \in V(\overline{K})$. Then we define

$$d(\gamma) = \frac{1}{[K(\gamma) : K]} \sum_{\text{primes } p \text{ of } K} (v_p(\Delta_{K(\gamma)/K}))$$

where $\Delta_{K(\gamma)/K}$ is the relative discriminant of the extension $K(\gamma)/K$.

Since we are working over a function field of characteristic 0 (so that all ramification is tame), we may use the definition

$$d(\gamma) = \frac{1}{[K(\gamma) : K]} \sum_{\text{primes } q \text{ of } K(\gamma)} (e(q/(q \cap o_K)) - 1) N_q$$
where \( e(q/(q \cap o_K)) \) is the ramification index of \( q \) over \( q \cap o_K \).

Let \( K_V \) be a canonical divisor on \( V \), and let \( h_{K_V} \) be a height function for \( K_V \). Yamanoi [Yamanoi, 2004] proves the following result, sometimes called the Vojta \((1 + \epsilon)\)-conjecture.

**Theorem 3.2.1.** (Yamanoi) Let \( K \) be a function field, let \( V \) be a curve over \( K \), let \( M \) be a positive integer, and let \( \epsilon > 0 \). Then there is a constant \( C_{M,\epsilon} \) such that for all \( \gamma \in V(K) \) with \([K(\gamma) : K] \leq M\), we have

\[
h_{K_V}(\gamma) \leq (1 + \epsilon)d(\gamma) + C_{M,\epsilon}.
\]

We will use Theorem 3.2.1 to prove Proposition 3.2.2, the function field analog of Proposition 3.1.4. To do this, we first introduce a little information about height functions and divisors.

The divisor \( K_V \) has degree \( 2g_V - 2 \) where \( g_V \) is the genus of \( V \). By the standard theory of heights on curves (see [Vojta, 1987, Proposition 1.2.9]), for example), if \( D \) is any ample divisor, and \( D' \) is an arbitrary divisor, we have

\[
\lim_{h_D(z) \to \infty} \frac{h_D'(z)}{h_D(z)} = \frac{\deg D'}{\deg D}.
\]

Now, let \( \pi : V \to \mathbb{P}^1 \) be a nonconstant map on a curve. Suppose that \( \pi(\gamma) = z \) for \( z \in \mathbb{P}^1(K) \). The usual height \( h(z) \) comes from a degree 1 divisor on \( \mathbb{P}^1 \) which pulls back to a degree \( \deg \pi \) divisor on \( V \). Furthermore if \( \pi(\gamma) \in \mathbb{P}^1(K) \), then \([K(\gamma) : K] \leq \deg \pi\). Thus, Theorem 3.2.1 and (3.2.1.2) imply that for any \( \epsilon' > 0 \), we have

\[
(1 - \epsilon') \frac{2g_V - 2}{\deg \pi} h(\pi(\gamma)) \leq d(\gamma) + O_{\epsilon'}(1)
\]

for all \( \gamma \in V(K) \) such that \( \pi(\gamma) \in \mathbb{P}^1(K) \).

We will use this to prove a function field analog of Proposition 3.1.4.
Proposition 3.2.2. Let $K$ be a function field and let $F(x) \in K[x]$ be a polynomial of degree 3 or more without repeated factors. Then, for any $\epsilon > 0$, there is a constant $C_{F,\epsilon}$ such that

$$\sum_{v_p(F(z)) > 0} N_p \geq (\deg F - 2 - \epsilon)h(z) + C_{F,\epsilon}$$  \hspace{1cm} (3.2.2.1)

for all $z \in K$.

Proof. For each $n > 0$, let $V_n$ be a nonsingular projective model over $K$ of $y^n = F(x)$. We obtain this by taking plane curve in $\mathbb{P}^2$ obtained by taking the homogenization of $y^n - F(x) = 0$, and the blowing up repeatedly over the point at infinity. Following [Hartshorne, 1977, Chapter V, Section 3], one sees that we obtain a single point at infinity in this way, since $\gcd(n, \deg F) = 1$.

To calculate the genus $g_n$ of $V_n$, we use the morphism $\pi : V_n \rightarrow \mathbb{P}^1$ given by projection onto the $x$-coordinate; that is, $\pi(x, y) = x$.

From now on, we choose $n$ such that it is relatively prime to $\deg F$. This makes the above morphism totally ramified at zeroes and poles of of $F$ and unramified everywhere else. Since $F$ has a single pole at the point at infinity along with $\deg F$ zeros, and $\pi$ has degree $n$, the Riemann-Hurwitz theorem gives

$$2g_n - 2 = (n - 1)(\deg F + 1) - 2n = n(\deg F - 1) - (\deg F + 1).$$  \hspace{1cm} (3.2.2.2)

Suppose that $\pi(\gamma) = z \in K$. Then (3.2.1.3) and (3.2.2.2) together give

$$(1 - \epsilon')(\deg F - 1 - \frac{\deg F + 1}{n})h(z) \leq d(\gamma) + O_{\epsilon', n}(1)$$

Let $\epsilon > 0$. Choosing sufficiently large $n$ and sufficiently small $\epsilon'$ yields

$$(\deg F - 1 - \epsilon)h(z) \leq d(\gamma) + O_{n, \epsilon}(1).$$  \hspace{1cm} (3.2.2.3)

Now, $K(\gamma) = K(\sqrt[n]{F(z)})$, which can only ramify over a prime $p$ when $v_p(F(z)) \neq 0$. Since $e(q/(q \cap o_K)) \leq n - 1$, where $e(q/q \cap o_K)$ is the ramification index of $q$ over $q \cap o_K$, we have

$$d(\gamma) \leq \sum_{v_p(F(z)) \neq 0} N_p .$$
When $v_p(F(z)) < 0$, either $v_p(z) < 0$ or $v_p(a_i) < 0$ for some coefficient $a_i$ of $F(z)$. Since $F$ has only finitely many coefficients and each has negative valuation at only finitely many primes, this means that

$$\sum_{v_p(F(z)) < 0} N_p \leq h(z) + O_F(1).$$

Hence, we have

$$d(\gamma) \leq \sum_{v_p(F(z)) > 0} N_p + h(z) + O_F(1).$$

Combining this inequality with (3.2.2.3) then gives (3.2.2.1).
4 Proofs of the Main Theorems

4.1 Proofs Of One Parameter Bang-Zsigmondy Theorems

We begin with a proposition that allows us to control the size of certain non-primitive factors of \( \varphi^n(\alpha) \). We choose a polynomial factor \( F \) of the numerator \( P_i \) of \( \varphi^i(z) \) and use the fact that, outside a finite set of primes, we have \( v_p(\varphi^n(\alpha)) > 0 \) whenever \( v_p(F(\varphi^{n-i}(\alpha))) > 0 \). If \( m < n \), the condition

\[
\min(v_p(F(\varphi^{n-i}(\alpha))), v_p(\varphi^m(\alpha))) > 0
\]

forces some root of \( F \) to be periodic modulo \( p \), with period at most \( n-m \). If all of the roots of \( F \) are non-periodic, then, for bounded \( n-m \), there are at most finitely many such \( p \). Thus, any \( p \) such that \( \min(v_p(F(\varphi^{n-i}(\alpha))), v_p(\varphi^m(\alpha))) > 0 \) comes from either a bounded set or from a relatively low order iterate \( \varphi^\ell(\alpha) \) of \( \alpha \). Since \( h(\varphi^\ell(\alpha)) \) is very small relative to \( h(\varphi^n(\alpha)) \) when \( \ell \) is small relative to \( n \), this allows for a strong upper bound on the product of all such \( p \).

**Proposition 4.1.1.** Let \( \delta > 0 \), let \( K \) be an abc-field, let \( \alpha \in K \) such that \( h_{\varphi}(\alpha) > 0 \), and let \( F \) be a factor of the numerator of \( \varphi^i \) such that every root \( \gamma_j \) of \( F \) is non-periodic and satisfies \( \varphi^\ell(\gamma_j) \neq 0 \) for \( \ell = 0, \ldots, i-1 \). Let \( Z \) be the set of
prime \( p \) such that \( \min(v_p(\varphi^m(\alpha)), v_p(F(\varphi^{n-i}(\alpha)))) > 0 \) for some positive integer \( m < n \). Then there is a constant \( C_\delta \) such that for all positive integers \( n \), we have
\[
\sum_{p \in \mathbb{Z}} N_p \leq \delta h(\varphi^n(\alpha)) + C_\delta.
\]

**Proof.** Let \( L \) be a finite extension of \( K \) over which \( F \) splits completely as \( F(x) = a(x - \gamma_1) \ldots (x - \gamma_s) \), for \( \gamma_j \in L \). Then, for all but finitely many primes \( p \) of \( K \), we have \( v_p(F(z)) > 0 \) if and only if \( v_q(z - \gamma_j) > 0 \) for some prime \( q \) of \( L \) with \( q | p \). Thus, it suffices to show that for each \( \gamma_j \), there is a \( C_\delta \) such that for all \( n \) we have
\[
\sum_{p \in Y} N_p \leq \delta h(\varphi^n(\alpha)) + C_\delta,
\]
where \( Y \) is the set of primes \( p \) such that \( \min(v_q(\varphi^m(\alpha)), v_q(\varphi^{n-i}(\alpha) - \gamma_j)) > 0 \) for some positive integer \( m < n \) and some prime \( q \) of \( L \) with \( q | p \).

Let \( Y_1 \) be the set of primes of \( L \) at which \( \varphi \) does not have weak good reduction, as defined in Section 2.6. Write \( P_i = FR \), and let \( Y_2 \) be the finite set of primes \( q \) at which some \( |b_s|_q \neq 1 \) for some nonzero coefficient of \( F \) or \( R \). Then, for all \( q \) outside of \( Y_1 \cup Y_2 \), we have \( \varphi(z) \equiv 0 \pmod{q} \) whenever \( F(z) \equiv 0 \pmod{q} \).

If \( \min(v_q(\varphi^m(\alpha)), v_q(\varphi^{n-i}(\alpha) - \gamma_j)) > 0 \) for \( n-i \leq m < n \), then \( v_q(\varphi^{m-(n-i)}(\gamma_j)) > 0 \). The picture for this situation modulo the prime \( q \) is given below.

\[
\begin{array}{c}
\alpha \rightarrow \varphi^{n-i}(\alpha) \equiv \gamma_j \rightarrow \varphi^{m-(n-i)}(\gamma_j) \equiv \varphi^m(\alpha) \equiv 0
\end{array}
\]

The set \( Y_3 \) of primes for which this can happen is therefore finite since \( \varphi^\ell(\gamma_j) \neq 0 \) for \( \ell = 0, \ldots, i-1 \).
For any $B$, let $W_B$ be the set of primes outside $Y_1 \cup Y_2 \cup Y_3$ such that 
\[ \min(v_q(\varphi^m(\alpha)), v_q(\varphi^{n-i}(\alpha) - \gamma_j)) > 0 \]
for some positive integers $m$ and $n$ with $n - i > m > n - i - B$. If $q \in W_B$, then $\varphi^m(\alpha) \equiv \varphi^n(\alpha) \equiv 0 \pmod{q}$, so $0$ is in a cycle of period at most $n - m$ modulo $q$. Since $\gamma_j \equiv \varphi^{n-i}(\alpha) \equiv \varphi^{(n-i)-m}(0) \pmod{q}$, we see that $\gamma_j$ is in the same cycle modulo $q$. This implies that $\gamma_j$ has period $n - m < B + i$ modulo $q$. The diagram below illustrates the situation, modulo $q$.

\[
\begin{array}{cccccc}
\alpha & \varphi^m & \equiv 0 & \varphi^{n-i} & \equiv \varphi^{(n-i)-m}(0) \\
\varphi^n(\alpha) & \varphi^i & \gamma_j
\end{array}
\]

Since $\gamma_j$ is not periodic, there are only finitely many such $q$, so $W_B$ must be finite. (Note that $\varphi$ induces a well-defined map from $k_q \cup \infty$ to itself, because $q$ is a prime of weak good reduction for $\varphi$.)

Note that $v_p(\varphi^j(\alpha)) > 0$ if and only if $v_q(\varphi^j(\alpha)) > 0$ for some $q \mid p$. Let $Z_B$ be the set \{primes $p \in \mathfrak{c}_K \mid q \mid p$ for some $q \in W_B$\}. Let $Y_i'$ (for $i = 1, 2, 3$) be the set \{primes $p \in \mathfrak{c}_K \mid q \mid p$ for some $q \in Y_i$\}. When $p \notin Z_B \cup Y_1' \cup Y_2' \cup Y_3'$, we see then that if $\min(v_p(F(\varphi^{n-i}(\alpha))), v_p(\varphi^n(\alpha))) > 0$ then $v_p(\varphi^m(\alpha)) > 0$ for some positive integer $m \leq n - i - B$. Since $Y_1'$, $Y_2'$, and $Y_3'$ are finite, and $Z_B$ is finite for any positive integer $B$, there is a constant $C_B$ such that

\[ \sum_{p \in Y} N_p \leq \sum_{\ell=1}^{n-i-B} \sum_{v_p(\varphi^j(\alpha))>0} N_p + C_B \leq \sum_{\ell=1}^{n-B-i} h(\varphi^\ell(\alpha)) + C_B \]  

(4.1.1.3)

where $Y$ is the set of primes $p$ where $\min(v_q(\varphi^m(\alpha)), v_q(\varphi^{n-i}(\alpha) - \gamma_j)) > 0$ for some positive integer $m < n$ and some prime $q$ of $L$ with $q \mid p$.

So it suffices to show that for any $\delta$, we have

\[ \sum_{\ell=1}^{n-B-i} h(\varphi^\ell(\alpha)) < \delta(h(\varphi^n(\alpha))) \]  

(4.1.1.4)
for all sufficiently large $n$. We will use the canonical height of Call and Silverman [Call and Silverman, 1993] here. Recall that by (2.6.0.4), we have $h_\varphi(\varphi(z)) = dh_\varphi(z)$ for all $z \in K$ and that by (2.6.0.5), there is a constant $C_\varphi$ such that $|h(z) - h_\varphi(z)| < C_\varphi$ for all $z \in K$.

Choose $B_\delta$ such that $1/d^{B_\delta+i} < \delta/4$ and $d^n(h_\varphi(\alpha)) > (n+1)C_\varphi^{\delta/2}$ for all $n > B_\delta$. Then for all $n > B_\delta$, we have

$$\sum_{\ell=1}^{n-B_\delta-i} h(\varphi^\ell(\alpha)) \leq \sum_{\ell=1}^{n-B_\delta-i} h_\varphi(\varphi^\ell(\alpha)) + nC_\varphi$$

$$= \frac{1}{d^{B_\delta+i}} \sum_{r=0}^{n-B_\delta-i-1} \frac{h_\varphi(\varphi^n(\alpha))}{d^r} + nC_\varphi \quad \text{(by (2.6.0.4))}$$

$$\leq \left( \frac{1}{d^{B_\delta+i}} \sum_{r=0}^{\infty} \frac{1}{d^r} \right) h_\varphi(\varphi^n(\alpha)) + nC_\varphi \quad \text{(4.1.1.5)}$$

$$\leq \frac{\delta}{2} h_\varphi(\varphi^n(\alpha)) + nC_\varphi$$

$$\leq \frac{\delta}{2} h(\varphi^n(\alpha)) + (n + 1)C_\varphi \quad \text{(by (2.6.0.5))}$$

$$\leq \delta h(\varphi^n(\alpha)).$$

Thus, (4.1.1.4) holds, and our proof is complete. \qed

**Lemma 4.1.2.** Let $K$ be an abc-field. If $\gamma \in \overline{K}$ is not exceptional, then $\varphi^{-3}(\gamma)$ contains at least two distinct points in $\mathbb{P}^1(\overline{K})$.

*Proof.* If $\varphi^{-3}$ contains only one point, $\tau$, then $\varphi$ is totally ramified at $\tau$, $\varphi(\tau)$, and $\varphi^2(\tau)$. By Riemann-Hurwitz, $\varphi$ can have at most two totally ramified points, so this means that $\tau$, $\varphi(\tau)$, and $\varphi^2(\tau)$ are not distinct, so we must have $\varphi^2(\tau) = \tau$, so $\tau$ is exceptional. But then $\gamma$ must be exceptional too. \qed

Now, we prove a very simple lemma that allows us to reduce the proofs of Theorems 2.1.1 and 2.1.2 to the case where $\beta = 0$. In the statement below $\sigma^{-1}$ denotes the compositional inverse of a linear polynomial $\sigma$. 

Lemma 4.1.3. Let $K$ be an abc-field. Let $\beta \in K$, let $\sigma$ be the linear polynomial $\sigma(x) = x + \beta$, let $\varphi \in K(x)$, and let $\varphi^\sigma = \sigma^{-1} \circ \varphi \circ \sigma$. Then we have the following:

(i) $(\varphi^\sigma)^n(\sigma^{-1}(\alpha)) = \varphi^n(\alpha) - \beta$ for any $\alpha \in K$ and any positive integer $n$; and

(ii) the map $\varphi^\sigma$ is dynamically unramified over 0 if and only if $\varphi$ is dynamically unramified over $\beta$.

Proof. We have $(\varphi^\sigma)^n = (\sigma^{-1} \circ \varphi \circ \sigma)^n = \sigma^{-1} \circ \varphi^n \circ \sigma$ for any positive integer $n$. Since $\sigma^{-1}(x) = x - \beta$, statement (i) above is immediate. To verify (ii), note that for any $\tau \in \overline{K}$ such that $\varphi^n(\tau) = \beta$, we therefore have $(\varphi^\sigma)^n(\sigma(\tau)) = 0$ and $e_{\varphi^n}(\tau/\beta) = e_{(\varphi^\sigma)^n}(\sigma(\tau)/0)$.

With the tools that we have assembled, the remainder of the proof of Theorem 2.1.1 is a short computation.

Proof of Theorem 2.1.1. Lemma 4.1.3 allows us to immediately reduce to the case that $\beta = 0$.

There is an $i$ such that $P_i$ has a factor $F \in K[x]$ of degree 4 or more such that every root $\gamma_j$ of $F$ is non-periodic and satisfies $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \ldots, i - 1$ (see Remark 4.1.4). To see this, note that since Lemma 4.1.2 tells us that $\varphi^{-3}(0)$ contains two points, we see that at least one of these points is not periodic. Taking the third inverse image of this point yields at least four non-periodic points; if one of these is the point at infinity, then three further inverse images yields eight points, at none of which is the point at infinity. Let $i$ be the smallest integer such that $\varphi^i(z) = 0$ for these points $z$ (this $i$ is the same for all of them since they are all inverse images of the same non-periodic point), and let $F \in K[x]$ be a factor of $P_i$ that vanishes at all of these $z$. Then $\deg F \geq 4$ by construction.
By Propositions 3.1.4 and 3.2.2, with $\epsilon = 1$, there is a nonzero constant $C_1$ such that

$$
\sum_{v_p(F(\varphi^{n-i}(\alpha))) > 0} N_p > (\deg F - 3) h(\varphi^{n-i}(\alpha)) \geq h(\varphi^{n-i}(\alpha)) + C_1.
$$

Applying Proposition 4.1.1 with $\delta = 1/(2d)$ and using the fact that $h(\varphi^i(z)) \leq d^i h(z) + O(1)$ for all $z \in K$, we see that there is a constant $C_2$ such that

$$
\sum_{p \in \mathbb{Z}} N_p \leq \frac{1}{2} h(\varphi^{n-i}(\alpha)) + C_2,
$$

where $Z$ is the set of primes $p$ such that $\min(v_p(F(\varphi^{n-i}(\alpha))), v_p(\varphi^m(\alpha))) > 0$ for some positive integer $m < n$. Thus, when $h(\varphi^{n-i}(\alpha)) > 2(C_2 - C_1)$, we have

$$
\sum_{v_p(F(\varphi^{n-i}(\alpha))) > 0} N_p > \sum_{p \in \mathbb{Z}} N_p
$$

so there is a prime $p$ such that $v_p(F(\varphi^{n-i}(\alpha))) > 0$ but $v_p(\varphi^m(\alpha)) \leq 0$ for all $m < n$. Now, writing $\varphi^i(x) = F(x)R(x)/T(x)$, where $FR$ and $T$ are coprime, we see that for all but finitely many $p$, we have $v_p(\varphi^i(z)) > 0$ whenever $v_p(F(z)) > 0$. Since $\lim_{n \to \infty} h(\varphi^{n-i}(\alpha)) = \infty$ (by (2.6.0.6)), we see then that for all but finitely many $n$, there is a prime $p$ such that $v_p(\varphi^n(\alpha)) > 0$ and $v_p(\varphi^m(\alpha)) \leq 0$ for all $1 \leq m < n$.

Theorem 2.1.2 is proved in the same manner as Theorem 2.1.1. The only significant difference is that we use a square-free factor $F$ of $P_i$, which is possible because $\varphi$ is dynamically unramified over $\beta$.

Proof. As in the proof of Theorem 2.1.1, we may assume that $\beta = 0$, using Lemma 4.1.3. By Remark 4.1.4, there is an $i$ such that $P_i$ has a factor $F$ of degree 8 or more such that every root $\gamma_j$ of $F$ is non-periodic, satisfies $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \ldots, i-1$, and has multiplicity 1 as a root of $P_i$. To see this note that since $\varphi$ is dynamically unramified over 0, there are infinitely many points $\tau$ such that
\( \varphi^n(\tau) = 0 \) and \( e_{\varphi^n}(\tau/0) = 1 \) for some \( n \). Thus, we may choose such a \( \tau \) that is not periodic and which is not in the forward orbit of any ramification points or the point at infinity. Then \( \varphi^{-3}(\tau) \) contains at least 8 points (since \( d \geq 2 \)) in \( \varphi^{-(n+3)}(0) \) none of which are ramification points of \( \varphi^{n+3} \). None of this points can be periodic since \( \tau \) is not periodic. Let \( i \) be the smallest \( i \) such that \( \varphi^i(z) = 0 \) for these points \( z \) (this \( i \) is the same for all of them since they are all inverse images of the same non-periodic point), and let \( F \in K[x] \) be a factor of \( P_i \) that vanishes at all of these \( z \). Then \( \deg F \geq 8 \) by construction.

Applying Roth-abc to \( F \) with \( \epsilon = 1 \), we obtain

\[
\sum_{v_p(F(\varphi^{n-i}(\alpha))) \geq 0} N_p > (\deg F - 3)h(\varphi^{n-i}(\alpha)) + C_3
\]

for some constant \( C_3 \), depending only on \( F \). Since

\[
\sum_{v_p(F(\varphi^{n-i}(\alpha))) > 0} v_p(F(\varphi^{n-i}(\alpha))) N_p \leq (\deg F)h(\varphi^{n-i}(\alpha)) + O(1),
\]

we see that there is a constant \( C_4 \) such that

\[
\sum_{v_p(F(\varphi^{n-i}(\alpha))) \geq 2} N_p > \frac{\deg F}{2}h(\varphi^{n-i}(\alpha)) + C_4.
\]

Since \( \deg F \geq 8 \), we have \( (\deg F)/2 - 3 \geq 1 \), so there is a constant \( C_5 \) such that

\[
\sum_{v_p(F(\varphi^{n-i}(\alpha))) = 1} N_p > h(\varphi^{n-i}(\alpha)) + C_5.
\]

Applying Theorem 4.1.1 with \( \delta = 1/(2d^i) \) and using the fact that \( h(\varphi^i(z)) \leq d^i h(z) + O(1) \) for all \( z \in K \), we see that there is a constant \( C_6 \) such that

\[
\sum_{p \in Z} N_p \leq \frac{1}{2}h_\varphi(\varphi^n(\alpha)) + C_6
\]

where \( Z \) is the set of primes \( p \) such that \( \min(v_p(F(\varphi^{n-i}(\alpha)), v_p(\varphi^m(\alpha))) > 0 \) for \( 1 \leq m < n \). Thus, when \( h(\varphi^{n-i}(\alpha)) > 2(C_6 - C_4) \), there is prime \( p \) such that \( v_p(F(\varphi^{n-i}(\alpha))) = 1 \) but \( v_p(\varphi^m(\alpha)) \leq 0 \) for all \( m < n \). Now, writing \( \varphi^i(x) = \)
$F(x)R(x)/T(x)$, where $F$, $R$, and $T$ are pairwise coprime, we see that for all but finitely many $p$, we have $v_p(\varphi^i(z)) = v_p(F)$ whenever $v_p(F(z)) > 0$. Since $\lim_{n \to \infty} h(\varphi^n-\varphi^i) = \infty$ (by (2.6.0.6)), we see then that for all but finitely many $n$, there is a prime $p$ such that $v_p(\varphi^n(\alpha)) = 1$ and $v_p(\varphi^m(\alpha)) \leq 0$ for all $1 \leq m < n$.

Remark 4.1.4. In the proofs of Theorems 2.1.1 and 2.1.2, the degree of the polynomial $F$ could be taken as large as one likes. Degrees 4 and 8, respectively, are simply convenient for the estimates. We wish to avoid the point at infinity so that we can take a polynomial $F(x)$ that vanishes at all of the points (without introducing homogenous coordinates). The reason we do not take $\deg F$ to be exactly 4 or 8 is that doing so might require passing to a finite extension of $K$, and we do not wish to assume the $abc$-conjecture for extensions of $K$ when $K$ is a number field.

Remark 4.1.5. When $\varphi$ is not dynamically unramified over $\beta$, there are at most finitely many $p$ that appear as square-free factors of any $\varphi^n(\alpha) - \beta$. To see this, note that by Lemma 4.1.3, it suffices to check what happens when $\beta = 0$ and $\varphi$ is not dynamically unramified over 0. In this case, there are at most finitely many polynomials that appear as factors of any $P_n$, where $P_n$ is the numerator of $\varphi$. Thus, for any $\alpha$, there are only finitely many $p$ such that $v_p(\varphi^n(\alpha)) = 1$ for some $n$. Thus, the conclusion of Theorem 2.1.2 will never hold for a rational function that is not dynamically unramified over $\beta$.

4.2 The $v$-adic Chordal Metric

Throughout this section (unless otherwise noted), $K$ will be a valued field with a nonarchimedean absolute value $|\cdot|_v$. Please note that the results stated in this section can be found in Silverman’s arithmetic dynamics book, [Silverman, 2007].
I refer the reader to examine Chapter 2 of [Silverman, 2007] for proofs of the results stated below. In order to state the results for the 2-parameter Bang-Zsigmondy problem for bounded period \( n \), it will be useful to define and state a few basic facts about the \( v \)-adic chordal metric. Let \( P_1 = [X_1 : Y_1] \) and \( P_2 = [X_2 : Y_2] \) be points in \( \mathbb{P}^1(\mathbb{C}) \). First let’s recall the chordal metric on \( \mathbb{P}^1(\mathbb{C}) \), denoted by \( \rho_\infty \), is defined by

\[
\rho_\infty(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|}{\sqrt{|X_1|^2 + |Y_1|^2} \sqrt{|X_2|^2 + |Y_2|^2}}
\]

It will be necessary to use a slightly different definition for the chordal metric in the event that we use a nonarchimedean absolute value \( |\cdot|_v \). Letting \( P_1 = [X_1 : Y_1] \) and \( P_2 = [X_2 : Y_2] \) be points in \( \mathbb{P}^1(K) \) (where \( K \) is a number field), the \( v \)-adic chordal metric on \( \mathbb{P}^1(K) \) is

\[
\rho_v(P_1, P_2) = \frac{|X_1Y_2 - X_2Y_1|_v}{\max\{|X_1|_v, |Y_1|_v\} \max\{|X_2|_v, |Y_2|_v\}}
\]

**Proposition 4.2.1.** The \( v \)-adic chordal metric satisfies the following properties.

(i) \( 0 \leq \rho_v(P_1, P_2) \leq 1 \).

(ii) \( \rho_v(P_1, P_2) = 0 \) if and only if \( P_1 = P_2 \).

(iii) \( \rho_v(P_1, P_2) = \rho_v(P_2, P_1) \).

(iv) \( \rho_v(P_1, P_3) \leq \max\{\rho_v(P_1, P_2), \rho_v(P_2, P_3)\} \).

So the previous proposition means that \( \rho_v \) is a true metric. Indeed, because it satisfies property (iv), which is stronger than the usual triangle inequality (due to the fact that \( v \) is nonarchimedean), \( \rho_v \) is in fact an ultrametric.

**Lemma 4.2.2.** Let \( R \) be the ring of integers of \( K \), and let \( f \in \text{PGL}_2(R) \). Then

\[
\rho_v(f(P_1), f(P_2)) = \rho_v(P_1, P_2) \text{ for all } P_1, P_2 \in \mathbb{P}^1(K)
\]

The above lemma is quite useful as it means that \( f \in \text{PGL}_2(R) \) preserve \( v \)-adic distances between points. We shall see a bit later that this will imply that changing coordinates via an element of \( \text{PGL}_2(R) \) does not change the underlying \( v \)-adic dynamics.
Before proceeding, let’s fix some notation that will be used in the remainder of this section.

- $K$ is a field with normalized discrete valuation $v : K^* \to \mathbb{Z}$.
- $| \cdot |_v = c^{-v(x)}$ for some $c > 1$, an absolute value associated to $v$.
- $R = \{ \alpha \in K : v(\alpha) \geq 0 \}$, the ring of integers of $K$.
- $p = \{ \alpha \in K : v(\alpha) \geq 1 \}$, the maximal ideal of $R$.
- $R^* = \{ \alpha \in K : v(\alpha) = 0 \}$, the group of units of $R$.
- $k_p = R/p$, the residue field of $R$.
- $r_p : R \to k_p$ is the reduction modulo $p$ map, i.e., $a \mapsto r_p(a)$.

**Lemma 4.2.3.** Let $P_1$ and $P_2$ be points in $\mathbb{P}^1(K)$. Then

$$r_p(P_1) = r_p(P_2) \text{ if and only if } \rho_v(P_1, P_2) < 1.$$ 

**Remark 4.2.4.** Let $f$ be a linear fractional transformation (i.e., $f \in \text{PGL}_2(\mathbb{C})$), and define $\varphi^f = f^{-1} \circ \varphi \circ f$. We say that $\varphi^f$ is the linear conjugate of $\varphi$ by $f$. Note that linear conjugation corresponds to a change of variables on $\mathbb{P}^1$ as can be seen in the commutative diagram that follows.

\[
\begin{array}{c}
\mathbb{P}^1 \xrightarrow{\varphi^f} \mathbb{P}^1 \\
\downarrow f \quad \quad \downarrow f
\end{array}
\]

Fractional linear transformations in $\text{PGL}_2(R)$ respect reduction modulo $p$, as we see below.
Proposition 4.2.5. Let $P, Q \in \mathbb{P}^1(K)$ and $f \in \text{PGL}_2(R)$. Then

$$r_p(P) = r_p(Q) \text{ if and only if } r_p(f(P)) = r_p(f(Q)).$$

Proof. $r_p(P) = r_p(Q)$ if and only if $\rho_v(P, Q) < 1$ (by Lemma 4.2.3) if and only if $\rho_v(f(P), f(Q)) < 1$ (by Lemma 4.2.2) if and only if $r_p(f(P)) = r_p(f(Q))$ (by Lemma 4.2.3). \qed

It is elementary to see that given 3 distinct points in $\mathbb{P}^1(K)$, there exists an $f \in \text{PGL}_2(K)$ that maps these points to 0, 1, and $\infty$, respectively. The following proposition provides an even stronger result.

Proposition 4.2.6. Let $P_1, P_2, P_3 \in \mathbb{P}^1(K)$ be points whose reductions $r_p(P_1), r_p(P_2), r_p(P_3)$ are distinct. Then there exists a linear fractional transformation $f \in \text{PGL}_2(R)$ such that

$$P_1 \mapsto 0, \quad P_2 \mapsto 1, \quad P_3 \mapsto \infty.$$  

The above lemma is extremely useful since Lemma 4.2.2 tells us the $v$-adic chordal metric is invariant for maps $f \in \text{PGL}_2(R)$. Consequently, changing coordinates by an element of $\text{PGL}_2(R)$ does not change the system’s $v$-adic dynamics.

Proposition 4.2.7. Let

$$f = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{PGL}_2(K),$$

with $a, b, c, d \in R$, at least one of $a, b, c, d \in R^*$, and $ad \equiv bc \pmod{p}$. Then there exist points $P, Q \in \mathbb{P}^1(K)$ satisfying

$$r_p(P) = r_p(Q) \text{ and } r_p(f(P)) \neq r_p(f(Q)).$$

Therefore the above result shows that Proposition 4.2.5 is false if $f \notin \text{PGL}_2(R)$. The following two theorems appear on page 59 of [Silverman, 2007].
Theorem 4.2.8. Let \( \varphi : \mathbb{P}^1 \to \mathbb{P}^1 \) be a rational map that has good reduction at the finite prime \( p \). Let \( v \) be the finite valuation corresponding to \( p \). Then the map \( \varphi \) is everywhere non-expanding. In other words,

\[
\rho_v(\varphi(P_1), \varphi(P_2)) \leq \rho_v(P_1, P_2) \text{ for all } P_1, P_2 \in \mathbb{P}^1(K).
\]

Lemma 4.2.9. Let \( \varphi : \mathbb{P}^1 \to \mathbb{P}^1 \) be a rational map that has good reduction at the finite prime \( p \). Let \( v \) be the finite valuation corresponding to \( p \). Let \( P_1, P_2 \in \mathbb{P}^1(K) \). If \( r_p(P_1) = r_p(P_2) \), then \( r_p(\varphi(P_1)) = r_p(\varphi(P_2)) \).

Proof. Assume \( r_p(P_1) = r_p(P_2) \). Then \( \rho_v(P_1, P_2) < 1 \) by Lemma 4.2.3. Using the result from Theorem 4.2.8,

\[
\rho_v(\varphi(P_1), \varphi(P_2)) \leq \rho_v(P_1, P_2) < 1.
\]

So \( \rho_v(\varphi(P_1), \varphi(P_2)) < 1 \), which implies by Lemma 4.2.3 that \( r_p(\varphi(P_1)) = r_p(\varphi(P_2)) \).

\( \square \)

Theorem 4.2.10. Let \( \varphi : \mathbb{P}^1 \to \mathbb{P}^1 \) be a rational map that has good reduction at \( p \). And let \( \widehat{\varphi} \) denote the result of reducing the coefficients of \( \varphi \) modulo \( p \).

(a) \( r_p(\varphi(P)) = \widehat{\varphi}(r_p(P)) \) for all \( P \in \mathbb{P}^1(K) \).

(b) Let \( \psi : \mathbb{P}^1 \to \mathbb{P}^1 \) be another rational map with good reduction at \( p \). Then the composition \( \varphi \circ \psi \) has good reduction, and

\[
\widehat{\varphi \circ \psi} = \widehat{\varphi} \circ \widehat{\psi}.
\]

And finally we have a proposition that implies linear conjugation of \( \varphi \) by the linear fractional transformation \( f \) preserves reduction modulo \( p \) at all but finitely many places.

Proposition 4.2.11. Let \( \varphi : \mathbb{P}^1 \to \mathbb{P}^1 \) be a rational map that has good reduction at \( p \), let \( f \) be a linear fractional transformation and let \( v \) be finite valuation corresponding to \( p \), and suppose \( P_1, P_2 \in \mathbb{P}^1(K) \). Then

\[
r_p(P_1) = r_p(P_2) \text{ implies } r_p(\varphi^f(P_1)) = r_p(\varphi^f(P_2)).
\]
4.3 Two Parameter Bang-Zsigmondy for Bounded Preperiod \( m \)

Let \( \beta \in K \), where \( K \) is an \( abc \)-field. Recall that the conclusion of Theorem 2.1.1 states that \( \varphi^n(\alpha) - \beta \) has a primitive prime divisor \( p \) for all but finitely many \( n \). In this section it will be useful to restate the result of Theorem 2.1.1 using the reduction map \( r_p \), which can be found below.

- For all but finitely many \( n \), there exists a prime \( p \) of \( K \) such that \( r_p(\varphi^n(\alpha)) = r_p(\beta) \), and \( r_p(\varphi^i(\alpha)) \neq r_p(\beta) \) whenever \( i < n \).
- For all but finitely many \( n \), there exists a prime \( p \) of \( K \) such that \( \varphi^n(\alpha) \) meets \( \beta \) modulo \( p \), and \( \varphi^i(\alpha) \) does not meet \( \beta \) modulo \( p \) whenever \( i < n \).
- For all but finitely many \( n \), there is a primitive meeting prime \( p \) of \( K \) for the pair \( (\varphi^n(\alpha), \beta) \).

Remember that Theorem 2.5.1 says the following: Let \( \varphi(x) \) be a rational function over the \( abc \)-field \( K \) of degree \( d \geq 2 \). Suppose no point in the orbit of \( \alpha \) is totally ramified for \( \varphi \), and furthermore suppose that the parameter \( m \) is bounded. If \( K \) is a function field, assume that \( \varphi \) is non-isotrivial. If \( K \) is a number field, assume that the \( abc \)-conjecture holds over all number fields. Then for all but finitely many \( (m, n) \), the pair \( (\varphi^{m+n}(\alpha), \varphi^m(\alpha)) \) has a two-primitive meeting prime.

**Lemma 4.3.1.** Let \( \varphi(x) \) be a rational function over the \( abc \)-field \( K \) of degree \( d \geq 2 \). Assume \( \eta \in K \). Let \( L \) be a finite extension of \( K \). Let \( q \) be a prime of \( L \), and write \( p = q \cap \mathcal{O}_K \). The point \( \eta \) has exact period \( N \) modulo the prime \( q \) if and only if \( \eta \) has exact period \( N \) modulo the prime \( p \).

**Proof.** Suppose that modulo the prime \( q \) of \( L \), the element \( \eta \) has exact period \( N \). Since \( \varphi^j(\eta) \in K \) for all \( j \geq 0 \), it follows immediately that \( \varphi^N(\eta) \) meets \( \eta \) modulo
It just remains to verify the primitivity of \( p \). Suppose not, i.e., suppose that for some \( 0 < i < N \), \( \varphi^i(\eta) \) meets \( \eta \) modulo \( p \). Because \( q \) lies over \( p \), it follows that \( \varphi^i(\eta) \) meets \( \eta \) modulo \( q \), contradicting the fact that modulo the prime \( q \), the point \( \eta \) has exact period \( N \).

Now assume \( \eta \) has exact period \( N \) modulo \( p \). Let \( q \) be a prime of \( L \) lying above \( p \). Because \( p \) factors in \( L \) as \( p \mathfrak{O}_L = q^e q_1^{e_1} \cdots q_j^{e_j} \), for primes \( q, q_1, \ldots, q_j \) of \( L \) and positive integers \( e, e_1, \ldots, e_j \), the element \( \varphi^N(\eta) \) meets \( \eta \) modulo \( q \). Say that \( \eta \) has period \( k < N \) modulo \( q \). Because \( \varphi^j(\eta) \in K \) for all \( j \geq 0 \) and \( q \) lies over \( p \), the element \( \varphi^k(\eta) \) meets \( \eta \) modulo \( p \), contradicting the fact that \( \eta \) has exact period \( N \) modulo \( p \).

**Lemma 4.3.2.** Let \( \varphi(x) \) be a rational function over the abc-field \( K \) of degree \( d \geq 2 \). Let \( m \) be fixed, and suppose that \( \varphi^{m-1}(\alpha) \) is not a totally ramified point for \( \varphi \). If \( K \) is a function field, assume that \( \varphi \) is non-isotrivial. If \( K \) is a number field, assume that the abc-conjecture holds over all number fields. Then for all but finitely many \( n \), there exists a prime \( p \) of \( K \) such that modulo \( p \), \( \varphi^m(\alpha) \) has exact period \( n \), and for \( m' < m \), \( \varphi^{m'}(\alpha) \) is not periodic modulo \( p \).

Rephrasing the conclusion of Lemma 4.3.2, for fixed preperiod \( m \) and all sufficiently large \( n \), we can find a prime \( p \) of \( K \) such that modulo \( p \), the point \( \varphi^m(\alpha) \) has exact period \( n \), and modulo the prime \( p \), no previous iterate is periodic. The proof of Lemma 4.3.2 is reasonably straightforward. First we take a \( \gamma \neq \varphi^{m-1}(\alpha) \) in the preimage of \( \varphi^m(\alpha) \) under \( \varphi \), and let \( L \) be a finite extension of \( K \) that contains \( \gamma \). Since \( \varphi^{m-1}(\alpha) \) is not a totally ramified point of \( \varphi \), we are guaranteed to have at least two points in the preimage of \( \varphi^m(\alpha) \). Note that \( \gamma \) can not be an exceptional point for \( \varphi \). For if \( \gamma \) were exceptional, then \( \varphi^{-1}(\{\gamma\}) = \{\gamma\} = \varphi(\{\gamma\}) \). But then \( \varphi^m(\alpha) = \gamma \), and of course \( \varphi^{m-1}(\alpha) \in \varphi^{-1}(\{\gamma\}) \). Hence \( \varphi^{m-1}(\alpha) = \gamma \), implying that \( \alpha \) is preperiodic under \( \varphi \). This contradicts the fact that \( \alpha \) is \( \varphi \)-wandering, so
γ must not be an exceptional point for ϕ. This means we can use Theorem 2.1.1 and Corollary 2.1.3. Using the aforementioned one parameter Bang-Zsigmondy result, we obtain (for all but finitely many n) a primitive meeting prime q in L of the pair (ϕ^{n-1}(ϕ^m(α)), γ). Of course, γ in general will be in some extension L of K, so some care must be taken in the proof to account for this. Applying ϕ to ϕ^{n-1}(ϕ^m(α)) and γ yields a primitive meeting prime p = q ∩ O_K of the pair (ϕ^n(ϕ^m(α)), ϕ(γ)) = (ϕ^n(ϕ^m(α)), ϕ^m(α)). And finally we observe that only finitely of these primes p could possibly make previous iterates periodic modulo p, so by taking n to be larger if necessary, these “bad” primes can be discarded.

It will be convenient to assume that p and q be primes of good reduction for ϕ, as it will be useful in the proof below to use the fact that reduction modulo a prime with good reduction commutes with composition of functions. But there are only finitely many primes that fail to have good reduction, so this is a relatively mild assumption, as we can just take a larger n if necessary to exclude these finitely many primes.

**Lemma 4.3.3.** Suppose that the point γ ∈ ϕ^{-1}(ϕ^{-1}(ϕ^m(α))) is ∞. Let σ(z) = 1/z. Define ϕ^σ = σ^{-1} ◦ ϕ ◦ σ. Then for all finite primes p of K,

\[ r_p(ϕ^j(ϕ^m(α))) = r_p(∞) = ∞ ⇐⇒ r_p((ϕ^σ)^j(σ^{-1}(ϕ^m(α)))) = r_p(σ^{-1}(∞)) = r_p(0). \]

**Proof.** Recall that for linear conjugation of ϕ^j by ρ, we have the commutative diagram below:

\[
\begin{array}{ccc}
\mathbb{P}^1 & \overset{(ϕ^j)^σ}{\longrightarrow} & \mathbb{P}^1 \\
\sigma \downarrow & & \sigma \downarrow \\
\mathbb{P}^1 & \overset{ϕ^j}{\longrightarrow} & \mathbb{P}^1 \\
\end{array}
\]
The above diagram tells us that $\varphi^m(\alpha)$ is mapped to $\varphi^i(\varphi^m(\alpha))$ by $\varphi^i$ if and only if $\sigma^{-1}(\varphi^m(\alpha))$ is mapped to $(\varphi^i)^{(\sigma^{-1}(\varphi^m(\alpha)))}$ by $(\varphi^i)^{(\sigma^{-1}(\varphi^m(\alpha)))}$. Observing that

$$(\varphi^i)^{(\sigma^{-1}(\varphi^m(\alpha)))} = (\varphi^i)^{(\sigma^{-1}(\varphi^m(\alpha)))} = \sigma^{-1}(\varphi^i(\varphi^m(\alpha))),$$

it follows that

$$r_p(\varphi^i(\varphi^m(\alpha))) = r_p(\infty) = \infty \iff r_p((\varphi^i)^{(\sigma^{-1}(\varphi^m(\alpha)))}) = r_p(\sigma^{-1}(\infty)) = r_p(0)$$

for all primes $p$ of $K$. \hfill \Box

**Lemma 4.3.4.** Suppose that the point $\gamma \in \varphi^{-1}(\{\varphi^m(\alpha)\})$ is $\infty$. Let $\sigma(z) = 1/z$. Define $\varphi^\sigma = \sigma^{-1} \circ \varphi \circ \sigma$. Then the pair $((\varphi^\sigma)^{(n^{-1}(\sigma^{-1}(\varphi^m(\alpha)))})$, $0)$ has a primitive meeting prime $p$ if and only if $p$ is a primitive meeting prime of the pair $(\varphi^{n^{-1}}(\varphi^m(\alpha)), \infty)$.

**Proof.** Immediate from Lemma 4.3.3 and the definition of a primitive divisor of a pair of elements via the reduction map $r_p$. \hfill \Box

**Proof of Lemma 4.3.2.** Let $\gamma$ be an element in the preimage of $\varphi^m(\alpha)$ under $\varphi$, where $\gamma$ is not $\varphi^{m-1}(\alpha)$. Observe that such a $\gamma$ exists because $\varphi^{m-1}(\alpha)$ is not totally ramified. The picture below illustrates the situation.

$$\begin{array}{ccccccc}
\alpha & \varphi^{m-1} & \varphi^{m-1}(\alpha) & \varphi & \varphi^{m}(\alpha) & \varphi & \varphi^{m+1}(\alpha) & \varphi & \cdots \\
\gamma & \varphi & \varphi^m(\alpha) & \varphi & \varphi^{m+1}(\alpha) & \varphi & \varphi^{m+2}(\alpha) & \varphi & \cdots \\
\end{array}$$

Now replace $\alpha$ with $\varphi^m(\alpha)$, and replace $\beta$ with $\gamma$ in the arguments from [Gratton et al., 2012]. So we are applying the arguments of [Gratton et al., 2012] to the pair $(\varphi^{n-1}(\varphi^m(\alpha)), \gamma)$. Let $L$ be a finite extension of $K$ that contains $\gamma$. If $\gamma = \infty$, apply the change of coordinates given in Lemma 4.3.3 and Lemma 4.3.4. In this case, as a result of the change of coordinates, we replace $\varphi^{n-1}$ with its linear conjugate by $\rho(z) = 1/z$, and $\gamma = \infty$ is replaced with $\gamma = 0$. Then Theorem 2.1.1
implies that for all sufficiently large \( n \), there exists a primitive meeting prime \( q \) in \( L \) of the pair \((\varphi^{n-1}(\varphi^m(\alpha)), \gamma)\). Applying \( \varphi \) to \( \varphi^{n-1}(\varphi^m(\alpha)) \) and \( \gamma \), we see that \( q \) is a meeting prime of the pair \((\varphi^n(\varphi^m(\alpha)), \varphi(\gamma)) = (\varphi^n(\varphi^m(\alpha)), \varphi^m(\alpha))\). Modulo \( q \), we obtain a cycle of the following form:

\[
\begin{array}{c}
\varphi^{m-1}(\alpha) \\
\varphi \\
\varphi^m(\alpha) \\
\varphi \\
\varphi^{n-2}(\varphi^m(\alpha))
\end{array}
\]

Thus modulo \( q \), the element \( \varphi^m(\alpha) \) is periodic with period dividing \( n \). If the period of \( \varphi^m(\alpha) \) were \( i < n \), then \( \varphi^{i-1}(\alpha) \) is mapped to \( \varphi^m(\alpha) \) modulo \( q \). If this were the case, we would have the following picture modulo \( q \).

\[
\begin{array}{c}
\varphi^{m-1}(\alpha) \\
\varphi \\
\varphi^m(\alpha) \\
\varphi \\
\varphi^{i-2}(\varphi^m(\alpha))
\end{array}
\]

But \( \varphi^{n-1}(\varphi^m(\alpha)) \equiv \gamma \) is in the same cycle, and is also mapped to \( \varphi^m(\alpha) \) modulo \( q \). Hence \( \varphi^{i-1}(\varphi^m(\alpha)) \equiv \gamma \) modulo \( q \). This contradicts the fact that \( q \) is a primitive meeting prime of the pair \((\varphi^{n-1}(\varphi^m(\alpha)), \gamma)\). As a consequence, modulo the prime \( q \) of \( L \), the point \( \varphi^m(\alpha) \) is periodic with period exactly \( n \).

Let \( p = q \cap O_K \), and observe that \( \varphi^n(\varphi^m(\alpha)) \) and \( \varphi(\gamma) = \varphi^m(\alpha) \) are both in \( K \). Therefore \( \varphi^n(\varphi^m(\alpha)) \) meets \( \varphi^m(\alpha) \) modulo \( p \). Combining the discussion in the previous paragraph with Lemma 4.3.1 (letting \( \eta = \varphi^m(\alpha) \)), for all but finitely many \( n \), there exists a prime \( p \) of \( K \) such that modulo \( p \), the element \( \varphi^m(\alpha) \) has exact period \( n \).
Suppose an earlier iterate $\varphi^r(\alpha)$ is periodic modulo $p$, where $r < m$. Then for all $r' \geq r$, modulo the prime $p$, the points $\varphi^{r'}(\alpha)$ must be periodic. In particular, $\varphi^{m-1}(\alpha)$ would be periodic modulo $p$. So showing that an earlier iterate is not periodic modulo $p$ reduces to verifying that $\varphi^{m-1}(\alpha)$ is not periodic modulo $p$.

Assume that $\varphi^{m-1}(\alpha)$ is in fact periodic modulo $p$. For all of the (finitely many) primes $q_i$ of $L$ lying above $p$, by Lemma 4.3.1, $\varphi^{m-1}(\alpha)$ is periodic modulo $q_i$. Because $\varphi^{m-1}(\alpha)$ and $\gamma$ are both mapped into $\varphi^{m}(\alpha)$ and $\gamma$ is in the cycle containing $\varphi^{m}(\alpha)$, it follows that $\varphi^{m-1}(\alpha)$ meets $\gamma$ modulo $q_i$. But $\varphi^{m-1}(\alpha) \neq \gamma$, so there are at most finitely many primes $r$ of $L$ such that these two points meet modulo $r$. Hence there are only finitely many primes $p$ of $K$ such that $\varphi^{m-1}(\alpha)$ could be periodic modulo $p$. By taking $n$ larger if necessary, these finitely many primes can be excluded from further consideration. We conclude that one can produce a primitive meeting prime $p$ for which $\varphi^{m}(\alpha)$ has exact period $n$ modulo $p$, and no previous iterate $\varphi^r(\alpha)$ is periodic modulo $p$, thereby completing the proof. \[\square\]

Suppose $\varphi^{m+n}(\alpha)$ meets $\varphi^{m}(\alpha)$ modulo $p$. As we have seen earlier in this section, $p$ would fail to be a two-primitive meeting prime of the pair $(\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))$ if a previous iterate $\varphi^i(\alpha)$ (for some $i < m$) is periodic modulo $p$, or if the exact period of $\varphi^{m}(\alpha)$ modulo $p$ is strictly less than $n$. Define $S_m$ to be the set of all $(m, n)$ such that for some $n \geq 1$, the pair $(\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))$ does not have a primitive meeting prime. Let $M$ be a given non-negative integer. Define $S$ to be the set of all $(m, n)$ such that for some $0 \leq m \leq M$ and some $n \geq 1$, the pair $(\varphi^{m+n}(\alpha), \varphi^{m}(\alpha))$ does not have a two-primitive meeting prime. Theorem 2.5.1 will be proven if it can be shown that $\# S < \infty$.

Proof of Theorem 2.5.1. Clearly

$$S = \bigcup_{m=0}^{M} S_m,$$
and

\[ \#S = \sum_{m=0}^{M} \#S_m. \]

By the discussion in the above paragraph, it will suffice to show that for each \(0 \leq m \leq M\), \(\#S_m < \infty\). But \(S_m\) contains precisely one ordered pair \((m,n)\) for each positive integer \(n\) for which we fail to find a prime \(p\) of \(K\) such that \(\varphi^m(\alpha)\) has exact period \(n\) modulo \(p\). But the conclusion of Lemma 4.3.2 tells us that there are only finitely many such \(n\). Consequently \(\#S_m < \infty\). Therefore \(\#S < \infty\) too, completing the proof.

\[\square\]

### 4.4 2-Parameter Bang-Zsigmondy for Bounded Period \(n\)

Throughout this section, unless otherwise noted, \(K\) will be a number field or a characteristic 0 function field of transcendence degree 1. Let \(x_0 \in K\). Also throughout this section we will assume that \(x_0\) is \(\varphi\)-wandering. We begin with a proposition and two lemmas, adapted from [Faber and Granville, 2011].

**Proposition 4.4.1.** Suppose that \(\varphi(x) \in K(x)\) has degree \(d \geq 2\). If \(K\) is a number field, assume that 0 is a strictly preperiodic point. If \(K\) is a characteristic 0 function field of transcendence degree 1, suppose \(\varphi\) is non-isotrivial, 0 is non-exceptional for \(\varphi\), and \(0 \notin \cup_{i=1}^{\infty}\{\varphi^i(x_0)\}\). Then \(\varphi^n(x_0)\) has a primitive prime factor \(p_n\) for all sufficiently large \(n\).

Proposition 4.4.1 was originally just stated over number fields. The proof of Proposition 4.4.1 in [Faber and Granville, 2011] uses the Thue-Mahler Theorem, which is valid over number fields. And by Corollary 2.1.3, the point \(\varphi^n(\alpha) - \beta\) has a primitive prime divisor for all sufficiently large \(n\), assuming the following: \(\varphi\) is non-isotrivial when \(K\) is a function field, \(\alpha\) is \(\varphi\)-wandering, and \(\beta \notin \text{Orb}_\varphi(\alpha)\).
Replacing $\alpha$ with $x_0$, and $\beta$ with 0 yields the function field part of Proposition 4.4.1.

Notice that there are several exceptional cases in [Faber and Granville, 2011] that occur when $\varphi(\mu) = \infty$. Faber and Granville in [Faber and Granville, 2011] must be very careful to deal with these exceptional classes because they are looking for primitive primes dividing the differences of numerators of the dynamical sequence. The consideration of these exceptional classes of functions considerably complicates their proofs. However, our definition of primitive prime factors, using valuations and the idea of two elements of a dynamical sequence meeting modulo $p$ is stable under change of coordinates (since the reduction modulo $p$ map, $r_p$, is respected by applying an $\sigma \in \text{PGL}_2(R)$ to move the point $\infty$), unlike Faber and Granville’s notion in [Faber and Granville, 2011]. To nail this down, if it turns out that if $\varphi(\mu) = \infty$, by the work of the last section, simply take $\sigma \in \text{PGL}_2(R)$ that moves $\infty$ to 0. We take $\sigma(t) = \frac{1}{t}$. Then replacing $\varphi$ with $\sigma^{-1} \circ \varphi \circ \sigma$ and replacing $x_0$ with $\sigma^{-1}(x_0)$ will do the trick. As we’ve seen, this does not change the $v$-adic dynamics of the system. Specifically, recall that $r_p(P) = r_p(Q)$ if and only if $r_p(\sigma(P)) = r_p(\sigma(Q))$ from Proposition 4.2.5. So the action of $\text{PGL}_2(R)$ on $\mathbb{P}^1(K)$ preserves congruence classes modulo $p$.

Now we define $\mathcal{E}$ to be the class of rational functions $\varphi(t) \in \mathbb{C}(t)$ of degree $d \geq 2$ satisfying one of the following:

- $\varphi(t) = t + \frac{1}{g(t)}$ for some polynomial $g(t)$ with $\deg(g) = d - 1$;
- $\varphi = \sigma^{-1} \circ \psi \circ \sigma$ for some linear transformation $\sigma(t) = \lambda t + \beta$ with $\gamma \neq 0$, where $\psi(t) = \frac{t^n}{t^{d-1} - 1}$; or
- $\varphi = \sigma^{-1} \circ \psi \circ \sigma$ with $\sigma$ as above and $\psi(t) = \frac{t^2}{2t+1}$.

By arguments presented in [Faber and Granville, 2011], the only time that $\varphi(\mu)$ could be $\infty$ is when $n = 1$ and $\varphi \in \mathcal{E}$. By doing the change of coordinates
listed above in this case, we can dispense with consideration of the exceptional cases comprising $\mathcal{E}$, which greatly simplifies the proof of the two parameter Bang-Zsigmondy problem in the case where the period $n$ is bounded.

**Lemma 4.4.2. (Faber-Granville)** Let $\varphi(t) \in \mathbb{C}(t)$ be a rational function of degree $d \geq 2$ and $n$ a positive integer. There exists $\mu \in \mathbb{P}^1(\mathbb{C})$ such that $\varphi^n(\varphi(\mu)) = \varphi(\mu)$ and $\varphi^n(\mu) \neq \mu$. If $n > 1$ or $n = 1$ and $\varphi \not\in \mathcal{E}$, we have $\varphi(\mu) \neq \infty$ as well. In the case where $n = 1$ and $\varphi \in \mathcal{E}$, let $\sigma(t) = 1/t$, and replace $\varphi(t)$ with $\varphi^\sigma(\sigma^{-1}(t))$ to guarantee that $\varphi$ does not send $\mu$ to $\infty$.

Write $\mathcal{B}_{n,d}$ for the set of rational functions of degree $d$ with no point of exact period $n$. Then Baker's Theorem, as stated in [Faber and Granville, 2011], says the following.

**Theorem 4.4.3. (Baker)** A rational map of degree $d \geq 2$ defined over $\mathbb{C}$ has a periodic point in $\mathbb{P}^1(\mathbb{C})$ of exact period $n \geq 2$ except perhaps when $n = 2, d = 2, 3, 4$, or when $n = 3, d = 2$. There exist exceptional maps in each of these four cases.

**Lemma 4.4.4. (Faber-Granville)** Suppose $\varphi(t) \in \mathbb{C}(t)$ is a rational function of degree $d \geq 2$, and let $n \geq 1$ be an integer. Then there exists a point $\mu \in \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ such that $\varphi(\mu)$ has exact period $n$, $\varphi(\mu) \neq \infty$, and $\varphi^n(\mu) \neq \mu$ unless

- $n = 2$ and $\varphi \in \mathcal{B}_{2,d}$ for some $d = 2, 3, 4$; or
- $n = 3$ and $\varphi \in \mathcal{B}_{3,2}$.

Observe that the exceptions to Lemma 4.4.4 are precisely the exceptional maps in Theorem 4.4.3. In other words, the exceptions are the maps without a periodic point of period 2 or 3, respectively.

**Theorem 4.4.5.** Suppose $\varphi(t) \in \mathbb{K}(t)$ has degree $d \geq 2$, and a positive integer $n$ is given. Then for all sufficiently large $m$, there exists a prime $p_m$ of $\mathbb{K}$ such that
\[ \varphi^{m+n}(x_0) \text{ meets } \varphi^m(x_0) \text{ modulo } p_m, \text{ but } \varphi^{j+n}(x_0) \text{ does not meet } \varphi^j(x_0) \text{ modulo } p_m \]

for any \( j < m \).

The proof of the theorem has four steps.

- First, choose \( \mu \in \mathbf{P}^1(\mathbb{C}) \) such that \( \varphi^n(\varphi(\mu)) = \varphi(\mu) \), but \( \varphi^n(\mu) \neq \mu \) by Lemma 4.4.2. Set up an auxiliary function \( \psi = \varphi^\sigma \). If \( \mu \in \mathbb{C} \), take \( \sigma(t) = t + \mu \). Otherwise let \( \sigma(t) = 1/t \). Then \( \psi \) has been defined such that 0 is strictly preperiodic for \( \psi \). Note that \( \psi(t) \in K'(t) \) for some finite Galois extension \( K'/K(\mu) \). This allows us to derive a primitive prime factor \( P_m \) in \( K' \) of the pair \( (\varphi^m(x_0), \mu) \).

- Second, exclude finitely many “bad” primes from consideration. In particular, we will exclude primitive primes \( P_m \) from Step 1 that are not of good reduction for \( \varphi \), and primes \( P_m \) such that \( \varphi^n(\mu) \) meets \( \mu \) will also be discarded. Also we exclude primes \( P_m \) dividing the denominator of \( \varphi(\mu) \). By choosing \( m \) to be sufficiently large, we can assume without loss of generality that these bad primes will not occur.

- Third, show that \( \varphi^{m+1}(x_0) \) meets \( \varphi^{m+1+n}(x_0) \) modulo \( p_m \). This follows almost immediately from the fact that \( \varphi^m(x_0) \) meets \( \mu \) modulo \( P_m \) and \( \varphi^n(\varphi(\mu)) = \varphi(\mu) \), so we obtain \( \varphi^{m+1}(x_0) \) meets \( \varphi^{m+1+n}(x_0) \) modulo \( P_m \) immediately. If \( p_m \) is the prime of \( K \) divisible by \( P_m \), then \( \varphi^{m+1+n}(x_0) \) meets \( \varphi^{m+1}(x_0) \) modulo \( p_m \) since \( \varphi^{m+1+n}(x_0) \) and \( \varphi^{m+1}(x_0) \) are both in \( K \).

- Fourth, verify the primitivity of \( p_m \). For if \( p_m \) failed to be primitive, then \( \varphi^n(\mu) \) would meet \( \mu \) modulo \( p_m \), contradicting the fact that such primes were previously excluded in Step 2 by choosing \( m \) to be sufficiently large.

**Lemma 4.4.6.** Suppose \( \varphi(t) \in K(t) \) is a rational function of degree \( d \geq 2 \), and that there exists a point \( \mu \in \mathbf{P}^1(\overline{K}) \) such that \( \varphi(\mu) \) has exact period \( n \geq 1 \), \( \varphi(\mu) \neq \infty \), and \( \varphi^n(\mu) \neq \mu \). Suppose \( p \) is a prime of good reduction for \( \varphi \). If
\( \varphi^m(x_0) \) meets \( \mu \) modulo \( p \), and \( \varphi^n(\mu) \) does not meet \( \mu \) modulo \( p \), and \( \varphi'(\varphi(\mu)) \) does not meet \( \varphi(\mu) \) modulo \( p \) for any \( 1 \leq l < n \), then \( \varphi^{M+D}(x_0) \) meets \( \varphi^M(x_0) \) modulo \( p \) if and only if \( M \geq m + 1 \) and \( n \mid D \).

We recall Theorem 2.5.2. Let \( K \) be a number field or a characteristic 0 function field of transcendence degree 1. If \( K \) is a function field, assume that \( \varphi \) is non-isotrivial. Suppose that \( \varphi(t) \in K(t) \) has degree \( d \geq 2 \). Let \( x_0 \in K \) be \( \varphi \)-wandering. For any given \( L \geq 1 \), the pair \( (\varphi^{m+n}(x_0), \varphi^m(x_0)) \) has a two-primitive meeting prime for all \( m \geq 0 \) and \( L \geq n \geq 1 \), except for the following cases:

- \( (n, d) = (2, 2) \) and \( \varphi \in B_{2,2} \); or
- \( (n, d) = (2, 3) \) and \( \varphi \in B_{2,3} \); or
- \( (n, d) = (2, 4) \) and \( K \) is a number field and \( \varphi \in B_{2,4} \); or
- \( (n, d) = (3, 2) \) and \( K \) is a number field and \( \varphi \in B_{3,2} \); or
- finitely many other exceptional \((m, n)\).

Proof of Theorem 2.5.2. The proof will proceed by induction on \( L \), with the case of \( L = 1 \) following immediately as a consequence of Theorem 4.4.5. We now proceed to the induction step. Directly from the induction hypothesis, the pair \((\varphi^{m+n}(x_0), \varphi^m(x_0))\) has a two-primitive meeting prime \( p_{n,m} \) for \( m \geq 0 \) and \( L - 1 \geq n \geq 1 \) except for finitely many \((m, n)\). Now let \( n = L \).

Choose \( \mu \in \mathbb{P}^1(K) \) so that \( \varphi(\mu) \) has exact period \( n \), \( \varphi(\mu) \neq \infty \), and \( \varphi^n(\mu) \neq \mu \). We then obtain a sequence of prime ideals \( \{P_{n,m}\} \) of the Galois closure of \( K(\mu) \) such that \( P_{n,m} \) is a primitive meeting prime of the pair \((\varphi^m(x_0), \mu)\) for all \( m \) large enough. Moreover, if \( p_{n,m} \) is the prime of \( K \) divisible by \( P_{n,m} \), then by Lemma 4.4.6, \( p_{n,m} \) is a two-primitive meeting prime of \((\varphi^{m+1+n}(x_0), \varphi^{m+1}(x_0))\), provided that \( p_{n,m} \) is not one of the finitely primes that must be excluded by Lemma 4.4.6.

\( \square \)
It is worth observing that the original theorem, as it appeared in [Faber and Granville, 2011], contained the caveat that certain exceptional classes must be avoided. Of course, since we’ve moved $\infty$ in case $\varphi(\mu) = \infty$, we are free to drop this reservation.

### 4.5 Kisaka’s Classification of Exceptions to Baker’s Theorem

In this section we give Kisaka’s classification [Kisaka, 1995] of the exceptions to Baker’s Theorem. Below we summarize Appendix B of [Faber and Granville, 2011] which states Kisaka’s result.

We say two rational maps $\varphi(t), \psi(t) \in \mathbb{C}(t)$ are **conjugate** if $\varphi = \sigma^{-1} \circ \psi \circ \sigma$ for some fractional linear transformation $\sigma(t) = (at + b)/(ct + d)$ with $ad - bc \neq 0$. In [Kisaka, 1995], Theorem 1, Kisaka showed that if $\varphi(t) \in \mathbb{C}(t)$ is a rational map of degree $d \geq 2$ with no periodic point of exact period $n$, then $\varphi$ is conjugate to one of the following:

1. $(n, d) = (2, 2)$.

   $$\varphi(t) = \frac{t^2 - t}{at + 1}, \text{ where } a \neq -1.$$ 

2. $(n, d) = (2, 3)$.

   $$\psi(t) = \frac{t^3 + at^2 - t}{(a^2 - 1)t^2 - 2at + 1}, \text{ where } a \neq 0; \text{ or}$$

   $$\psi(t) = \frac{t^3 - t}{-t^2 + at + 1}, \text{ where } a \neq 0; \text{ or}$$

   $$\psi(t) = \frac{t^3 + \frac{4}{a}t^2 - t}{-t^2 + at + 1}, \text{ where } a \neq 0, \pm 2i.$$

(3) \((n, d) = (2, 4)\).

\[\psi(t) = \frac{t^4 - t}{-2t^3 + 1} \text{ or } \frac{t^4 + t^3 + t^2 - t}{-t^3 + t^2 - 3t + 1} \text{ or } \frac{t^4 - 3^{1/3}t^3 + 3^{2/3}t^2 - t}{-t^3 + 3^{4/3}t^2 - (5)(3^{-1/3})t + 1}\]

\[\text{or } \frac{t^4 + \overline{c_0}t^3 + \overline{b_0}t^2 - t}{-t^3 + b_0 t^2 + c_0 t + 1},\]

where \((x - b_0)(x - \overline{b_0}) = x^2 - 3x + 1\) and \((x - c_0)(x - \overline{c_0}) = x^2 + 5x + 5\).

(4) \((n, d) = (3, 2)\):

\[\psi(t) = \frac{t^2 + \omega t}{\omega + t} \text{ or } \frac{t^2 + \omega t}{\omega t + 1},\]

where \(\omega\) is a primitive third root of unity.

Actually, Kisaka’s result holds over any field of characteristic 0. Also notice that if \(K = \mathbb{C}(a)\) is a function field, then \(\psi\) is non-isotrivial in Cases (1) and (2), while \(\psi\) is isotrivial in Cases (3) and (4). Therefore Cases (1) - (4) provide all of the exceptions to Theorem 2.5.2 when \(K\) is a number field, while only Cases (1) and (2) provide exceptions to Theorem 2.5.2 when \(K = \mathbb{C}(a)\) is a function field, because \(\varphi \in K(t)\) is assumed to be non-isotrivial.
5 Further Research Questions

In this thesis, it has been established (for bounded preperiod $m$ or bounded period $n$) that modulo some mild assumptions that appear in Theorem 2.5.1 and Theorem 2.5.2, there is a two-primitive meeting prime $p$ for the pair $(\varphi^{m+n}(\alpha), \varphi^m(\alpha))$. It would be interesting to investigate if there is a Bang-Zsigmondy principle for $\varphi^m(\alpha) - \varphi^n(\beta)$. The issue is as follows. Can we find an ordering $\ll$ of $\mathbb{N}^2$ such that we are always getting a “new” prime $p \mid \varphi^m(\alpha) - \varphi^n(\beta)$ such that $p \nmid \varphi^{m'}(\alpha) - \varphi^{n'}(\beta)$ whenever $(m',n') \ll (m,n)$? If such an ordering $\ll$ can be found, then it may be possible to obtain a Bang-Zsigmondy result here. A related question is to find a Bang-Zsigmondy result for pairs $(\varphi^{m+n}(\alpha), \varphi^m(\beta))$, but again the issue of finding a proper ordering of $\mathbb{N}^2$ arises.

Observe that Corollaries 2.1.3 and 2.1.4 and Theorems 2.5.1 and 2.5.2 include the condition that $\varphi$ is non-isotrivial when $K$ is a function field. This non-isotriviality condition is included so that the requirement $h_{\varphi}(\alpha) > 0$ can be replaced with “$\alpha$ is $\varphi$-wandering”. Can the non-isotriviality requirement be weakened while keeping the condition that $\alpha$ is $\varphi$-wandering? It may be the case that the only such $\varphi$ that must be excluded are those $\varphi$ that are actually trivial when $K$ is a function field. But then the possibility that $\alpha$ is $\varphi$-wandering yet $h_{\varphi}(\alpha) = 0$ when $K$ is a function field would need to be addressed in the Roth-$abc$ section of this thesis. Is there a (not too painful) way to accomplish this?
It would be nice to remove the bound on the preperiod $m$ and the period $n$ in the two-parameter Bang-Zsigmondy theorems in this thesis. Paul Vojta in [Vojta, 1998] has a higher dimensional $abc$ conjecture that may be useful in removing this restriction in certain cases.

**Conjecture 5.0.1. (Vojta’s More General $abc$)** Let $X$ be a smooth complete variety over $k$, let $D$ be a normal crossings divisor on $X$, let $K$ denote the canonical line sheaf on $X$, let $A$ be a big line sheaf on $X$, let $r \in \mathbb{Z}_{>0}$, and let $\epsilon > 0$. Then there exists a proper Zariski-closed subset $Z = Z(k, S, X, D, A, r, \epsilon) \subseteq X$ such that

$$h_K(P) + m(D, P) \leq d_k(P) + \epsilon h_A(P) + O(1),$$

for all $P \in X(\overline{k}) \setminus Z$ with $[k(P) : k] \leq r$.

So the hope here is to utilize Conjecture 5.0.1 to prove a two parameter Bang-Zsigmondy result that does not have any restriction on the preperiod $m$ and the period $n$ of $\alpha$ modulo $p$.

One major goal in complex and arithmetic dynamics is to understand the dynamic moduli spaces that parametrize families of maps. For example, the space of rational maps of degree $d$ modulo conjugation by Mobius maps is

$$\mathcal{M}_d = \text{Rat}_d / \text{Aut}(\mathbb{P}^1).$$

It turns out that the behavior of a rational map $F : \mathbb{P}^1 \to \mathbb{P}^1$ is governed by the forward orbits of the critical points. If we impose the condition that all critical points have finite forward orbits (maps satisfying this condition are called post-critically finite, or PCF) has strong dynamical consequences.

To every PCF map, we associate a ramification portrait — i.e., a finite graph encoding the action of $F$ restricted to its critical and postcritical sets. Then we have an important theorem of Thurston.

**Theorem 5.0.2. (Thurston Rigidity)** Given a ramification portrait (not of Lattès type), there exist at most finitely many conjugacy classes in $\mathcal{M}_d$ which realize it.
Recall that the two-parameter Bang-Zsigmondy results of Theorems 2.5.1 and 2.5.2 state that assuming the restrictions in the hypotheses of these theorems are satisfied, for all but finitely many additional exceptions, assuming either the preperiod $m$ or the period $n$ is bounded, we can find a prime $p$ of $K$ such that modulo $p$, the point $\varphi^m(\alpha)$ has exact period $n$, and $\alpha$ has preperiod $m$ modulo $p$. Consequently, given $\alpha, \varphi, m,$ and $n$ (where one of $m$ and $n$ is bounded), we are obtaining a portrait of the point $\alpha$ modulo $p$ under the map $\varphi$, where $\varphi^m(\alpha)$ has exact period $n$, and no previous iterate $\varphi^i(\alpha)$ (where $0 \leq i < m$) is periodic modulo $p$. The fact that modulo $p$ we are obtaining these portraits means that studying PCF maps and Thurston Rigidity are natural topics to explore further.

One final (probably multi-year) project that I am considering is to make a serious effort to understand Shinichi Mochizuki’s proof of the $abc$-conjecture. This is laid out in Mochizuki’s series of four papers on inter-universal Teichmuller theory, [Mochizuki, 2013a], [Mochizuki, 2013b], [Mochizuki, 2013c], and [Mochizuki, 2013d]. Actually, assuming the proof is correct, it follows from a series of Diophantine inequalities that are proven. Mochizuki develops an arithmetic Teichmuller theory for number fields equipped with an elliptic curve. This would be a longer term project, however, as it will take a considerable investment of time and effort to learn all of the necessary background.
Bibliography


