EXCEPTIONAL POINTS IN ARITHMETIC DYNAMICS

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAI'I AT MĀNOA IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

MAY 2015

By

Bianca Thompson

Dissertation Committee:

Michelle Manes, Chairperson
Pavel Guerzhoy
Tom Craven
Sarah Post
Erik Guentner
Linda Furuto

ACKNOWLEDGMENTS

I would like to thank the Institute for Computational and Experimental Research in Mathematics and my coauthors Alon Levy and Michelle Manes for a productive and enjoyable semester during which much of Chapter 2 was completed. I benefited greatly from productive conversations with workshop participants, including Holly Krieger, William Gignac, Frank Paladino, Chi-hao Wang, Andrew Bridy, Kevin Doerksen, Jacqueline Anderson, Jan-Li Lin, Katherine Stange and especially Mike Zieve, who suggested the full strength of Theorem 2.2.7. Thanks also to Joseph Silverman, Xander Faber, and Bianca Viray for numerous helpful comments.

The three questions on page 27 grew out of Joe Silverman's lectures and problems at the 2010 Arizona Winter School, which the authors were both lucky to attend. I was very grateful for the opportunity to attend Sage Days 42, where Chapter 3 was begun in earnest. Thanks especially to my working group for helpful conversations and computations: Michelle Manes, Alina Bucur, Anna Haensch, Adriana Salerno, Lola Thompson, and Stephanie Treneer. Thanks also to Tom Tucker and Kalyani Madhu for help with pictures.

I would like to thank Xander Faber profusely for proposing the question in the final chapter as well as the many helpful conversations and guidance given while working on it. Thank you to Rachel Pries for naming the critically reducible objects as well as this dissertation.

I would like to thank Glazer's where much of the last chapter was written. Thanks to Jared Mukai, Jamal Hassan, Allan Wong, Jean Verrette, and Eric Reckwerdt for letting me spout off ideas and write all over their chalkboards whenever I was stumped.

Finally, I would like to thank my family for always pushing me to greater heights.

ABSTRACT

Let ϕ be a morphism of $\mathbb{P}^N$ defined over a field K. We prove three main results:

When K is a number field, we prove that there is a bound B depending only on ϕ such that every twist of ϕ has no more than B K-rational preperiodic points. (This result is analagous to a result of Silverman for abelian varieties.) For two specific families of quadratic rational maps over $\mathbb{Q}$, we find the bound B explicitly.

When K is a finite field, we find the limiting proportion of periodic points in towers of finite fields for polynomial maps associated to algebraic groups, namely pure power maps $\phi(z) = z^d$ and Chebyshev polynomials.

When K is a number field or $\mathbb{Q}_p$ for $p \neq 3$, and L/K is an extension we prove that K fails to be critically reducible at 3. Meanwhile, $\mathbb{Q}_3$ is critically reducible at 3.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

The field of arithmetic dynamics lies in the intersection of holomorphic (discrete) dynamical systems and number theory. It asks number-theoretic questions arising from discrete dynamical systems. My work has been in three areas, each of which I will describe in more detail below: the study of families of twists of dynamical systems and uniform bounds on the number of rational preperiodic points for these families (Chapter 2); the study of dynamics over finite fields and proportions of strictly periodic points (Chapter 3); and the study of dynamical systems with K rational critical points where K is a number field or $\mathbb{Q}_p$ (Chapter 4).

Dynamical systems are systems which change over time, where the next state depends on the current state. Population growth models are examples of dynamical systems: the number of people in the next generation depends on the current population. Starting in the 1910s, Julia and Fatou explored discrete dynamical systems; the field saw a resurgence of interest in the 1970s with the advent of computing technology.

In number theory, we want to discover interesting and unexpected relationships between different sorts of numbers and to prove these relationships are true. For example, in the 1700s, Goldbach conjectured that every even number $n \geq 4$ was the sum of two prime numbers and every odd integer $m \geq 7$ was the sum of three primes. Computers have checked numbers up to 4×10^{18} while many mathematicians have worked to prove the conjecture in full generality. In 2014, Harold Halfgalt proved the ternary Goldbach Conjecture, but the even case remains open.

We set the following notation:

K	a field with fixed algebraic closure $\overline{K}$.
$\mathbb{P}^N(K)$	projective N space over field K, write $\mathbb{P}^n$ for $\mathbb{P}^n(\overline{K})$.
$\mathrm{Per}\left(\phi, \mathbb{P}^N(K)\right)$	$= \{P \in \mathbb{P}^N(K) \colon P \text{ is periodic under } \phi\}$.
$\mathrm{PrePer}\left(\phi, \mathbb{P}^N(K)\right)$	$= \{P \in \mathbb{P}^N(K) \colon P \text{ is preperiodic under } \phi\}$.
$\mathrm{Crit}(\phi)$	$= \{\gamma \in \mathbb{P}^N \colon \gamma \text{ is a critical point of } \phi\}$
$\mathrm{PGL}_{N+1}(K)$	projective linear group over field K, i.e. $\mathrm{Aut}(\mathbb{P}^N)$, we write PGL_{N+1} for $\mathrm{PGL}_{N+1}(\overline{K})$.

1.1 Periodic points

Dynamics concerns itself with a set S and self mapping function $\phi : S \to S$. This allows for iteration

$$\phi^n = \underbrace{\phi \circ \phi \circ ... \circ \phi}_{n \text{ terms}}.$$

One goal of arithmetic dynamics is to classify a point α according to its behaviour in the *orbit*, defined to be $\{\phi^n(\alpha) : n \geq 0\}$.

Example 1.1.1. Consider $\phi(z) = z^2 - 1$. With $\alpha = 0$,

$$0 \overset{\phi}{\mapsto} -1 \overset{\phi}{\mapsto} 0.$$

The orbit in this case is the finite set $\{0, -1\}$.

The point 1 also has a finite orbit, but is not contained in a cycle:

$$1 \overset{\phi}{\mapsto} 0 \overset{\phi}{\mapsto} -1 \overset{\phi}{\mapsto} 0.$$

The orbit of 2 is infinite:

$$2 \overset{\phi}{\mapsto} 3 \overset{\phi}{\mapsto} 8 \overset{\phi}{\mapsto} 63 \overset{\phi}{\mapsto} \dots$$

In this thesis we let $S = \mathbb{P}^N(K)$, and we let $\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K)$ be a morphism on projective space of dimension N. In the case of $N = 1$, we may write $\phi = \frac{f}{g}$, a rational map where f and g have no common zeros. The degree of ϕ is $d = \max\{\deg(f), \deg(g)\} > 1$.

Definition 1.1.2. We define $\alpha \in \mathbb{P}^N(K)$ to be *periodic* (with period n) if there exists an integer $n > 0$ such that $\phi^n(\alpha) = \alpha$, the smallest such n is called the *primitive period* n. The point α is *preperiodic* if there exist integers $n > m \geq 0$ such that $\phi^m(\alpha) = \phi^n(\alpha)$. If α is not preperiodic, then we call α a *wandering point*.

Example 1.1.3. We revisit our earlier example $\phi(z) = z^2 - 1$. We now can say that the point 0 is periodic since $\phi^2(0) = 0$. The point 1 is a preperiodic point because $\phi(1) = \phi^3(1)$. And the point 2 is wandering.

Let

$$\mathrm{PrePer}\left(\phi, \mathbb{P}^N(K)\right) = \{P \in \mathbb{P}^N(K) \colon P \text{ is preperiodic under } \phi\}.$$

A motivating problem in the field of arithmetic dynamics is the uniform boundedness conjecture of Morton and Silverman [17].

Conjecture 1. *Let $K/\mathbb{Q}$ be a number field of degree D, and let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over K. There is a constant $\kappa(D, N, d)$ such that*

$$\#\,\mathrm{PrePer}(\phi, \mathbb{P}^N(K)) \leq \kappa(D, N, d).$$

This is a deep and difficult problem. It implies, for example, uniform boundedness for torsion points on abelian varieties over number fields (see [3]). Even the special case $N = 1$ and $d = 4$ is enough to imply Merel's uniform boundedness of torsion points on elliptic curves [14]. Though much work has been done on this problem for nearly 20 years, to date only non-uniform bounds are known.

1.2 Ramification points

A guiding principle in complex dynamics is that the orbits of critical (ramification) points are closely tied to the behavior of the dynamical system. Here we define what it means for a point to be ramified.

Definition 1.2.1. Assuming $\alpha \neq \infty$ and $\phi(\alpha) \neq \infty$, we define the *ramification index* to be

$$e_\phi(\alpha) = \mathrm{ord}_\alpha(\phi(z) - \phi(\alpha)).$$

If $e_\phi(\alpha) = \deg(\phi)$, then we say ϕ is *totally ramified at* α.

Example 1.2.2. Let $\phi(z) = z^2 + 2$.

$$e_\phi(0) = \mathrm{ord}_0(\phi(z) - \phi(0)) = \mathrm{ord}_0(\phi(z) - 2) = \mathrm{ord}_0(z^2).$$

We see that $z | z^2$ twice, hence $\mathrm{ord}_0(z^2) = 2 = \deg(\phi)$. So 0 is a totally ramified critical point. Now

consider $z = 4$.

$$e_\phi(4) = \mathrm{ord}_4(\phi(z) - \phi(4)) = \mathrm{ord}_4(\phi(z) - 18) = \mathrm{ord}_4(z^2 - 16) = 1.$$

The last equality comes from the fact $(z-4)|(z^2-16)$ exactly once.

Remark. The ramification index $e_\phi(\alpha) \leq \deg(\phi)$. Also ϕ is locally $e_\phi(\alpha)$-to-1 in a neighbourhood of α.

Definition 1.2.3. The point $\alpha \in \mathbb{P}^N$ is a *critical point* or *ramification point* for ϕ if and only if $e_\phi(\alpha) \geq 2$. For $N = 1$, $\alpha < \infty$, and $\phi(\alpha) < \infty$, this is just the usual definition that $\phi'(\alpha) = 0$. We denote the set of critical points of ϕ by $\mathrm{Crit}(\phi)$.

Definition 1.2.4. The point $\alpha \in \mathbb{P}^1(K)$ is a *critical value* of ϕ if $\alpha = \phi(\gamma)$ for some $\gamma \in \mathrm{Crit}(\phi)$.

Theorem 1.2.5. (Riemann-Hurwitz Formula for $\mathbb{P}^1$, [23, pg 13]) *Let K be a field of characteristic 0 and $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ a rational map of degree d. Then*

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

Hence, a rational map of degree d has exactly $2d-2$ critical points, counted with appropriate multiplicity.

Corollary 1.2.6. ([23, pg 15]) *Let ϕ be a rational map of degree $d \geq 1$. Let $\alpha \in \mathbb{P}^1(K)$. Then*

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

Proposition 1.2.7. ([24, pg 24]) *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a nonconstant rational map and let $\psi : \mathbb{P}^1 \to \mathbb{P}^1$ be another nonconstant rational map. The for all $\alpha \in \mathbb{P}^1$*

$$e_{\psi \circ \phi}(\alpha) = e_\phi(\alpha) e_\psi(\phi(\alpha)).$$

Definition 1.2.8. A set E satisfying $\phi(E) = E = \phi^{-1}(E)$ is called an *exceptional set.*

Example 1.2.9. Consider $\phi(z) = z^3$. Let $E = \{0, \infty\}$. Then we see that $\phi(E) = E = \phi^{-1}(E)$ since $\phi(0) = 0$, $\phi(\infty) = \infty$, $\phi^{-1}(0) = \{0\}$, and $\phi^{-1}(\infty) = \{\infty\}$.

Theorem 1.2.10. ([23, pg 16]) *Let ϕ be a rational map of degree $d \geq 2$ and let $E \subset \mathbb{P}^1$ be an exceptional set. Then $\#E \leq 2$.*

1.3 Good Reduction

It is common in number theory to work modulo a prime p. We continue with the notation above and add to it $\widetilde{\ }$ which means reduction modulo a prime p.

Definition 1.3.1. A rational map ϕ has *good reduction* at prime p if $\deg(\phi) = \deg(\widetilde{\phi})$.

A useful tool in determining if a map has good reduction is the resultant. We define it as follows:

Definition 1.3.2. Let $\phi = \frac{f}{g}$ be a rational map where

$$f = a_0x^n + a_1x^{n-1} + ... + a_{n-1}x + a_n$$
$$g = b_0x^m + b_1x^{m-1} + ... + b_{m-1}x + b_m.$$

Then the *resultant of* ϕ is defined to be

$$\mathrm{Res}(\phi) = \mathrm{Res}(f,g) = \det \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_n & & & & \\ & a_0 & a_1 & a_2 & \cdots & a_n & & & \\ & & a_0 & a_1 & a_2 & \cdots & a_n & & \\ & & & \ddots & & & \ddots & & \\ & & & a_0 & a_1 & a_2 & \cdots & a_n & \\ b_0 & b_1 & b_2 & \cdots & b_m & & & & \\ & b_0 & b_1 & b_2 & \cdots & b_m & & & \\ & & b_0 & b_1 & b_2 & \cdots & b_m & & \\ & & & \ddots & & & \ddots & & \\ & & & & b_0 & b_1 & b_2 & \cdots & b_m \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ \} \, m \text{ times} \\ \\ \\ \\ \\ \\ \} \, n \text{ times} \end{matrix}$$

Theorem 1.3.3. ([23, pg 58]) *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map defined over K. Then ϕ has good reduction at a prime $\mathfrak{p}$ if and only if* $\mathrm{Res}(\widetilde{\phi}) = \widetilde{\mathrm{Res}(\phi)} \neq 0$.

Proposition 1.3.4. ([23, pg 59]) *If ϕ has good reduction and $\phi(\alpha) = \beta$, then $\widetilde{\phi(\alpha)} = \widetilde{\phi}(\widetilde{\alpha}) = \widetilde{\beta}$.*

1.4 p-adic dynamics

In this thesis, we study dynamics on fields of number theoretic interest: number fields, finite fields, and p-adic rationals. This section develops some of the background for dynamics on p-adic fields.

Definition 1.4.1. If an absolute value satisfies the strong triangle inequality

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\} \text{ for all } \alpha \in K,$$

then the absolute value is *nonarchimedean.* A *value field* is a pair $(K, |\ .\ |_K)$ consisting of a field K and an absolute value on K. Let $(K, |\ .\ |_K)$ be a value field equipped with nonarchimedean absolute value. Then K is a said to be a *nonarchimedean valued field.*

Definition 1.4.2. Fix a prime p. The *p-adic absolute value* $|\ .\ |_p$ on $\mathbb{Q}$ is defined as follows: let $\alpha = p^m \frac{a}{b} \in \mathbb{Q}$, with $p \nmid ab$, $m \in \mathbb{Z}$, is

$$|\alpha|_p = p^{-m}.$$

In Chapter 3, we use the related idea of *valuation*: $v_p(\alpha) = v(\alpha) = m$.

It is easy to check the p-adic absolute value satisfies the strong triangle inequality: $|\ x + y\ |_p \leq \max\{|x|_p, |y|_p\}$.

Lemma 1.4.3. ([6, pg 31]) *Let* $|\ .\ |_p$ *be the p-adic absolute value. If* $|a|_p \neq |b|_p$, *then for* $a, b \in \mathbb{Q}$, $|a + b|_p = \max\{|a|_p, |b|_p\}$.

Example 1.4.4. Consider $\left|9 + \frac{1}{12}\right|_3$. Note that $|9|_3 = 3^{-2}$ and $\left|\frac{1}{12}\right|_3 = 3^1$.

$$\left|9 + \frac{1}{12}\right|_3 = \left|\frac{109}{12}\right|_3 = 3 = \max\{3^{-2}, 3\} = \max\left\{|9|_3, \left|\frac{1}{12}\right|_3\right\}$$

Example 1.4.5. Now consider $\left|12 + \frac{28}{3}\right|_2$. Here $|12|_2 = 2^{-2}$ and $\left|\frac{28}{3}\right|_2 = 2^{-2}$. So $\left|12 + \frac{28}{3}\right|_2 \leq \max\{|12|_2, \left|\frac{28}{3}\right|_2\} = 2^{-2}$. In fact $\left|12 + \frac{28}{3}\right|_2 = \left|\frac{36+28}{3}\right|_2 = \left|\frac{64}{3}\right|_2 = 2^{-6}$.

Remark. The ring of integers in a nonarchimedean valued field K is defined by $\alpha \in \mathcal{O}_K$ if and only if $|\alpha| \leq 1$. Equivalently, $v_p(\alpha) \geq 0$.

Theorem 1.4.6. Ostrowski, ([19])*Every non-trivial absolute value on* $\mathbb{Q}$ *is equivalent to one of the absolute values* $|\ .\ |_p$, *where either p is prime or* $p = \infty$.

When we complete $\mathbb{Q}$ with respect to the standard absolute value, this gives us $\mathbb{R}$. If we complete $\mathbb{Q}$ with respect to a p-adic absolute value, we get the field $\mathbb{Q}_p$. Many analytical properties that hold for $\mathbb{R}$ will still hold for $\mathbb{Q}_p$. For example, by construction every Cauchy sequence will converge in $\mathbb{Q}_p$. The algebraic closure of $\mathbb{R}$ is $\mathbb{C}$ and $[\mathbb{C} : \mathbb{R}] = 2$. The algebraic closure of $\mathbb{Q}_p$, denoted $\overline{\mathbb{Q}}_p$, is an infinite degree extension and is no longer complete. The complete and alebraically closed extension of $\mathbb{Q}_p$ is denoted $\mathbb{C}_p$.

It is natural to take theorems in $\mathbb{R}$ and ask to what extent they hold in $\mathbb{Q}_p$. Unfortunately, $\mathbb{Q}_p$ is totally disconnected and is homeomorphic to a fractal. This can make proofs more difficult. On the other hand, $\mathbb{Q}_p$ has nice properties that are not true for $\mathbb{R}$. For exmple, Hensel's Lemma below gives us a means to test for $\mathbb{Q}_p$ roots of polynomials.

Theorem 1.4.7. (Hensel's Lemma,[6, pg 68]) *Let $\phi(x) = a_0 + a_1x + ...a_nx^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Suppose that there exists a p-adic integer $\alpha_1 \in \mathbb{Z}_p$ such that*

$$\phi(\alpha_1) \equiv 0 \pmod{p\mathbb{Z}_p}$$
$$\phi'(\alpha_1) \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

where $\phi'(x)$ is the (formal) derivative of $\phi(x)$. Then there exists an integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1 \pmod{p\mathbb{Z}_p}$ and $\phi(\alpha) = 0$.

1.5 Dynamical Heights

Let K be a number field and $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ a morphism. A *height* is a function that measures the arithmetic complexity of a point.

Definition 1.5.1. We define the *logarithmic height of $\alpha \in K$* to be

$$h(\alpha) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \log \max\{|\alpha|_v, 1\}$$

where M_K is the standard set of absolute values on K.

The function has nice properties:

(i) If $K \subset L$, $h(\alpha)$ is unchanged if we consider $\alpha \in L$.

(ii) $h(\phi(\alpha)) = dh(\alpha) + \mathcal{O}(1)$, where d is the degree of ϕ.

(iii) The Northcott property: For every $B \in \mathbb{R}_{\geq 0}$, $|\{\alpha \in K : h(\alpha) < B\}| < \infty$.

Proposition 1.5.2. ([23, pg 97]) *Let S be a set, let $d > 1$ be a real number, and let $\phi : S \to S$ and $h : S \to \mathbb{R}$ be functions satisfying:*

$$h(\phi(\alpha)) = dh(\alpha) + O(1)$$

for all $\alpha \in S$. Then the limit

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

exists and satisfies:

(i) $\hat{h}_\phi(\alpha) = h(\alpha) + O(1)$, and

(ii) $\hat{h}_\phi(\phi(\alpha)) = d\hat{h}_\phi(\alpha)$.

The function $\hat{h} : S \to \mathbb{R}$ is uniquely determined by the above properties.

Definition 1.5.3. Inspired by canonical heights for elliptic curves we can define the *canonical height for a rational fuction*

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

The proposition above says this limit exists and $\hat{h}$ is well defined.

Canonical height functions are useful because they can detect if a point $\alpha \in K$ is preperiodic. The *canonical height* $\widehat{h}_\phi(\alpha)$ is zero precisely when α is a preperiodic point.

Theorem 1.5.4. ([23, pg 99]) *Let $\phi : \mathbb{P}^N \to \mathbb{P}^N$ be a morphism of degree $d \geq 2$ defined over $\overline{\mathbb{Q}}$ and let $\alpha \in \mathbb{P}^N(\overline{\mathbb{Q}})$. Then $\alpha \in \mathrm{PrePer}(\phi)$ iff $\hat{h}_\phi = 0$.*

Theorem 1.5.5. (Northcott, [18]) *Let $\phi \in \mathrm{Hom}_d^N(K)$. Then the set of preperiodic points $\mathrm{PrePer}(\phi, \mathbb{P}^N(\overline{K}))$ is a set of bounded height. In particular, $\mathrm{PrePer}(\phi, \mathbb{P}^N(K))$ is a finite set, and more generally, for any $D > 1$ the set*

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

is finite.

CHAPTER 2
UNIFORM BOUNDS FOR PREPERIODIC POINTS IN FAMILIES OF TWISTS

This is joint work with Alon Levy and Michelle Manes. The results appear in [10].

2.1 Introduction

As a first step towards proving the uniform boundedness conjecture, one might ask if Conjecture 1 holds in interesting families of dynamical systems. For example, in [21] Poonen conjectures a precise bound for quadratic polynomials over $\mathbb{Q}$, which can be viewed as a one-parameter family $f_c(z) = z^2 + c$:

Conjecture 2. *If $z_0, c \in \mathbb{Q}$ such that z_0 has primitive period n for $f_c(z) = z^2 + c$, then $n \leq 3$.*

Even this special form of Conjecture 1 remains very much open. Morton [16] has shown that $n \neq 4$. Flynn, Poonen, Schaefer [4] showed that $n \neq 5$. And Stoll [26] proved that the Birch and Swinnerton-Dyer Conjecture implies $n \neq 6$. Given the difficulty of the question for quadratic polynomials, our Theorem 2.4.1 regarding a different one-parameter family of quadratic functions appears surprisingly strong.

Theorem. *The rational map $\phi_b(z) = z + \frac{b}{z}$ where $b \in \mathbb{Q}$ has no rational points with primitive period $n \geq 5$.*

It turns out that these two one-parameter families are different in a dynamically significant way. The quadratic functions ϕ_b considered above are all quadratic twists of the function $\phi(z) = z + 1/z$. This is not the case for the quadratic polynomials f_c considered by Poonen and others.

In Theorem 2.2.7, we show that Conjecture 1 holds for families of twists of rational maps. More precisely, for any twist ψ of a morphism of projective space ϕ defined over a number field K, the number of K-rational preperiodic points is uniformly bounded by a constant depending only on the map ϕ, but independent of the twist. This statement and its proof are similar to a result for abelian varieties in [22]. There, Silverman shows that given an abelian variety A, for all but finitely many twists A_ξ of A the set of K-rational torsion points $A_\xi(K)_{\text{tors}}$ is contained in

$$\{P \in A_\xi(\overline{K}) \colon \text{for some } f \in \operatorname{Aut} A_\xi, f \neq \mathrm{id}, f(P) = P\}.$$

We conclude with an outline of the chapter and a survey of the techniques used.

Section 2.2 We provide background on Northcott's Theorem and twists of rational maps. We conclude with a proof of our main result, Theorem 2.2.7, which combines this background material with Galois-theoretic methods.

Section 2.3 We introduce the primary tool for understanding periodic points for morphisms of the projective line: dynatomic polynomials. We use arithmetic functions and elementary number theory to prove several lemmas about the coefficients of these polynomials for the family of maps $\phi_{k,b}(z) = k(z + b/z)$.

Section 2.4 Using the background in Section 2.3 and an application of the rational root theorem, we get the surprisingly strong Theorem 2.4.1 described above. Combining this Theorem with results from [12], we give all possible graphs associated to rational preperiodic points for maps of the form $\phi_b(z) = z + b/z$; there are at most 6 rational preperiodic points for such maps.

Section 2.5 Using the same techniques, we get a similar theorem and graphical description of rational preperiodic point structures for the family of maps $\psi_b(z) = -(z + b/z)$.

2.2 Uniform Bounds for Families of Twists

We begin with some background in arithmetic dynamics. Throughout, K will be a number field, and we will state explicitly when results hold for more general fields.

Definition 2.2.1. We define

$$\mathrm{Hom}_d^N(K) = \{\phi : \mathbb{P}^N(K) \to \mathbb{P}^N(K) \colon \phi \text{ is a morphism of degree } d^N\}.$$

That is, ϕ is defined in each coordinate by homogeneous polynomials of degree d with coefficients in K. (We follow the convention that Hom_d^N refers to $\mathrm{Hom}_d^N(\overline{K})$.)

The primary tool in our proof is the classic theorem of Northcott, see Theorem 1.5.5.

Let $f \in \mathrm{PGL}_{N+1}$ act on the points of $\mathbb{P}^N$ as a fractional linear transformation in the usual way. Then we define the morphism

$$\phi^f = f \circ \phi \circ f^{-1}.$$

Definition 2.2.2. Let $\phi, \psi \in \mathrm{Hom}_d^N(K)$. We say the morphisms are *conjugate* if there is some $f \in \mathrm{PGL}_{N+1}$ such that $\phi^f = \psi$. They are *conjugate over* K if there is some $f \in \mathrm{PGL}_{N+1}(K)$ such that $\phi^f = \psi$.

If P is a point of period n for ϕ, then $f(P)$ has the same property for ϕ^f, and similarly for preperiodic points. It is also easily seen that $(\phi^n)^f = \left(\phi^f\right)^n$. So conjugate maps have essentially the same dynamical behavior. However, if we are concerned with the arithmetic of the (pre)periodic points, we must be a bit more careful. For a map $\phi \in \mathrm{Hom}_d^N(K)$,

$$\mathrm{Twist}(\phi/K) = \left\{ \begin{array}{c} K\text{-equivalence classes of maps } \psi \in \mathrm{Hom}_d^N(K) \\ \text{such that } \psi \text{ is } \overline{K}\text{-equivalent to } \phi \end{array} \right\}.$$

An element $\psi \in \mathrm{Twist}(\phi/K)$ is called a twist of ϕ.

Example 2.2.3. Let

$$\phi(z) = z - \frac{2}{z} \text{ and } \psi(z) = z - \frac{1}{z}.$$

Also let $f(z) = z\sqrt{2}$. One may check that $\phi^f(z) = \psi(z)$. So ψ is a (quadratic) twist of ϕ. Solving $\phi^2(z) = z$ gives the $\mathbb{Q}$-rational two-cycle $\{\pm 1\}$. But ψ does not have rational points of primitive period 2; solving $\psi^2(z) = z$ gives $\{\pm 1/\sqrt{2}\}$.

Definition 2.2.4. For any $\phi \in \mathrm{Hom}_d^N(\overline{K})$ define $\mathcal{A}_\phi$ to be the *automorphism group* of ϕ, i.e.,

$$\mathcal{A}_\phi = \{f \in \mathrm{PGL}_{N+1} \mid \phi^f = \phi\}.$$

From [9, 20], $\mathcal{A}_\phi$ is well-defined as a finite subgroup of PGL_{N+1}.

We introduce some notation to make the statement and proof of Lemma 2.2.6 more succinct. Let $\phi \in \mathrm{Hom}_d^N(K)$, and $\psi \in \mathrm{Twist}(\phi/K)$, meaning there is an $f \in \mathrm{PGL}_{N+1}$ with $\phi^f = \psi$. Write $f = (a_{ij})$, a matrix. At least one of the a_{ij} is nonzero, say $a_{lm} \neq 0$. So we may also write $f = (a'_{ij})$ where $a'_{ij} = \frac{a_{ij}}{a_{lm}}$, since this represents the same element of PGL_{N+1}.

Definition 2.2.5. Let $K_f = K(a'_{ij})$ be the minimal field of definition for a given $f \in \mathrm{PGL}_{N+1}$ such that $\phi^f = \psi$, and let L_f be the Galois closure of K_f.

Lemma 2.2.6. *For any $\psi \in \mathrm{Twist}(\phi/K)$ and any f satisfying $\phi^f = \psi$,*

$$[K_f : K] \leq \#\mathcal{A}_\phi.$$

Proof. Choose $f \in \mathrm{PGL}_{N+1}$ such that $\phi^f = \psi$, and let $\sigma \in \mathrm{Gal}(L_f/K)$. Since ψ is defined over K,

$$\begin{aligned} f\phi f^{-1} = (f\phi f^{-1})^\sigma &= f^\sigma \phi^\sigma (f^{-1})^\sigma \\ &= f^\sigma \phi (f^{-1})^\sigma. \\ \phi &= f^{-1} f^\sigma \phi (f^\sigma)^{-1} f. \end{aligned}$$

Hence $f^{-1}f^\sigma \in \mathcal{A}_\phi$. Define the map

$$\begin{aligned} \rho : \mathrm{Gal}(L_f/K) &\to \mathcal{A}_\phi \\ \sigma &\mapsto f^{-1}f^\sigma \end{aligned}$$

Then

$$\begin{aligned} \rho(\sigma) = \rho(\tau) &\Leftrightarrow f^{-1}f^\sigma = f^{-1}f^\tau \\ &\Leftrightarrow f^\sigma = f^\tau \\ &\Leftrightarrow f = f^{\tau\sigma^{-1}}. \end{aligned}$$

So $\tau\sigma^{-1} \in \mathrm{Gal}(L_f/K_f)$ since it fixes f. Clearly if $\tau_1\sigma^{-1} = \tau_2\sigma^{-1}$ as elements of $\mathrm{Gal}(L_f/K_f)$, then they are equal as elements of $\mathrm{Gal}(L_f/K)$, and $\tau_1 = \tau_2$. Hence ρ is $[L_f : K_f]$-to-1, and we conclude that

$$[L_f : K_f][K_f : K] = [L_f : K] \leq [L_f : K_f](\#\mathcal{A}_\phi),$$

which gives the result since all of the extensions are finite. □

Remark. If all elements of $\mathcal{A}_\phi$ are defined over K, then ρ is in fact a group anti-homomorphism; that is, it is a homomorphism with the direction of group multiplication reversed. This is because

$\sigma\tau \mapsto f^{-1}f^{\sigma\tau}$ but now $(f^{-1}f^{\tau})^{\sigma} = f^{-1}f^{\tau}$. So we have,

$$\begin{aligned}\rho(\sigma)\rho(\tau) &= f^{-1}f^{\sigma}f^{-1}f^{\tau} = f^{-1}f^{\sigma}(f^{-1}f^{\tau})^{\sigma} \\ &= f^{-1}f^{\sigma}(f^{-1})^{\sigma}f^{\tau\sigma} = f^{-1}f^{\tau\sigma} \\ &= \rho(\tau\sigma).\end{aligned}$$

Inversion is also an anti-homomorphism, so the map ρ^{-1}, which maps each $\sigma \in \mathrm{Gal}(L_f/K)$ to $\rho^{-1}(\sigma)$, is a homomorphism. Since the map is injective, we conclude that $\mathrm{Gal}(L_f/K)$ is a subgroup of $\mathcal{A}_{\phi}$.

The following is now a straightforward consequence of Northcott's Theorem.

Theorem 2.2.7. *Let K be a number field and let $\phi \in \mathrm{Hom}_d^N(K)$. Then there is a uniform bound B_{ϕ} such that for all $\psi \in \mathrm{Twist}(\phi/K)$,*

$$\#\,\mathrm{PrePer}(\psi, \mathbb{P}^N(K)) \leq B_{\phi}.$$

Proof. Given $\psi \in \mathrm{Twist}(\phi/K)$ and $f \in \mathrm{PGL}_{N+1}$ such that $\phi^f = \psi$, every K-rational preperiodic point for ψ corresponds to a K_f-rational preperiodic point for ϕ. From Lemma 2.2.6, $[K_f : K] \leq \#\mathcal{A}_{\phi} := D$. By Northcott's Theorem,

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

is finite; call the cardinality of this set B_{ϕ}. Then for every $\psi \in \mathrm{Twist}(\phi/K)$,

$$\#\,\mathrm{PrePer}(\psi, \mathbb{P}^N(K)) \leq B_{\phi}.$$

□

Remark. In fact Lemma 2.2.6 holds over an arbitrary field K; hence Theorem 2.2.7 also holds when K is a function field over a finite field.

Example 2.2.8. Suppose that $\phi(z) : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is a degree-2 morphism with a unique fixed point $P \in \mathbb{P}^1(\overline{K})$. Applying any Galois action to the equation $\phi(P) = P$ shows that any Galois conjugate of P is also fixed by ϕ. Hence, $P \in \mathbb{P}^1(K)$. Choose a change of coordinates $f \in \mathrm{PGL}_2(K)$

moving P to infinity. Then we may write

$$\phi^f(z) = \frac{z^2 + az + b}{z + a} \text{ for some } a, b \in K \text{ with } b \neq 0.$$

The critical points of ϕ^f are $a \pm \sqrt{b}$, so conjugate by $g \in \mathrm{PGL}_2(K)$ which fixes infinity and moves the critical points to $\pm\sqrt{b}$, and we see that ϕ is conjugate over K to a map of the form $\phi_b(z) = z + \frac{b}{z}$.

For any $b \in K^*$, ϕ_b is a quadratic twist of $\phi(z) = z + \frac{1}{z}$ with conjugating map $f_b = z\sqrt{b}$. So $f_b \in \mathrm{PGL}_2(L)$ with $[L : K] \leq 2$. Let $Q \in \mathbb{P}^1(K)$ be a K-rational preperiodic point for ϕ_b. Then $f_b(Q)$ is an L-rational preperiodic point for ϕ.

By Theorem 2.2.7, $\#\,\mathrm{PrePer}(\phi_b, \mathbb{P}^1(K)) \leq B$ for some absolute bound B, independent of the parameter b. In Section 2.4, we show that for this twisted family of quadratic rational maps when $K = \mathbb{Q}$, the bound is actually 6.

2.3 Main Tool: Dynatomic Polynomials

In this section, we will write rational maps using homogeneous coordinates:

$$\phi : \mathbb{P}^1 \to \mathbb{P}^1$$
$$[X : Y] \mapsto [F(X, Y) : G(X, Y)],$$

where F and G are homogeneous polynomials of the same degree with no common factor. Then for $n > 1$,

$$\phi^n[X : Y] = [F_n(X, Y) : G_n(X, Y)],$$

where F_n and G_n are given recursively by

$$F_n(X, Y) = F_{n-1}(F(X, Y), G(X, Y)) \text{ and } G_n(X, Y) = G_{n-1}(F(X, Y), G(X, Y)).$$

Definition 2.3.1. The n-period polynomial of ϕ is

$$\Phi_{\phi,n}(X, Y) = YF_n(X, Y) - XG_n(X, Y).$$

The n^{th} *dynatomic polynomial of* ϕ is the polynomial

$$\Phi^*_{\phi,n}(X,Y) = \prod_{d|n} \Phi_{\phi,d}(X,Y)^{\mu(\frac{n}{d})},$$

where μ is the Mobius function. When the function ϕ is clear, we will suppress it from the notation, writing simply Φ^*_n.

See [23, p.151] for a proof that $\Phi^*_n(X,Y)$ is indeed a polynomial. Clearly it is then a homogeneous polynomial in X and Y. Further, we let

$$\nu_2(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d = \text{ degree of } \Phi^*_n \text{ for a quadratic rational map.}$$

By construction, all points of period $d \mid n$ are roots of the n-period polynomial Φ_n. One might hope that the roots of Φ^*_n are the points of primitive period n (eliminating as roots points with period $d < n$). This isn't quite the case, but it is true that every point with primitive period n is a root of Φ^*_n, and that fact is enough for our purposes. See [23, Chapter 4] for details about dynatomic polynomials and their properties.

Lemma 2.3.2. *The following products are positive powers of* k *for* $n > 1$:

(1) $\displaystyle\prod_{d|n} \left(k^{2^d-d-1}\right)^{\mu(\frac{n}{d})}$.

(2) $\displaystyle\prod_{d|n} \left(k^{2^d-1}\right)^{\mu(\frac{n}{d})}$.

(3) $\displaystyle\prod_{d|n} \left(k^{2^{d-1}}\right)^{\mu(\frac{n}{d})}$.

(4) $\displaystyle\prod_{d|n} \left(k^{b(d)}\right)^{\mu(\frac{n}{d})}$ *where* $b(d) = \left\lceil \frac{2(2^{d-1}-1)}{3} \right\rceil$.

Proof. Proofs will rely on facts about the properties of the arithmetic functions φ and μ, as well as the connection between them. We refer the interested reader to [15, Chapter 2] for these facts.

(1) Consider

$$\begin{aligned}\prod_{d|n} \left(k^{2^d-d-1}\right)^{\mu(\frac{n}{d})} &= k^{\sum_{d|n} \mu(\frac{n}{d})(2^d-d-1)} \\ &= k^{\sum_{d|n} \mu(\frac{n}{d})(2^d-d)}.\end{aligned}$$

The last step follows from the fact that when $n > 1$ the $\sum_{d|n} \mu\left(\frac{n}{d}\right) = 0$. Recall that $\sum_{d|n} \mu(\frac{n}{d})d = \varphi(n)$ where $\varphi(n)$ is the Euler totient function.

Also,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d \quad \geq \quad 2^n - \sum_{d|n \ d\neq n} 2^d \quad \geq \quad 2^n - 2^{n-1} \quad = \quad 2^{n-1}. \tag{2.3.1}$$

Hence

$$\begin{aligned}
\sum_{d|n} \mu\left(\frac{n}{d}\right)(2^d - d) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d - \sum_{d|n} \mu\left(\frac{n}{d}\right) d \\
&= \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d - \varphi(n) \\
&\geq \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d - n \\
&\geq 2^{n-1} - n.
\end{aligned}$$

After taking the derivative of $2^{x-1} - x$, we see that the fuction is increasing as long as $x > 1$. Hence $\sum_{d|n} \mu(\frac{n}{d})(2^d - d) > 0$.

(2) follows immediately from (1).

(3) follows immediately from equation (2.3.1), replacing d by $d-1$ and using the fact that $n > 1$.

(4) Now consider

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) b(d) \geq \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{2}{3}(2^{d-1} - 1).$$

Multiplying the result from (3) by $\frac{2}{3}$ and using the fact that $\sum_{d|n} \mu(n/d) = 0$ for $n > 1$, we see that (4) is also positive. □

Let K be a number field and let

$$\begin{aligned}
\phi_{k,b} : \mathbb{P}^1 &\to \mathbb{P}^1 \\
[X : Y] &\mapsto [k(X^2 + bY^2) : XY]
\end{aligned}$$

for some $b, k \in K^*$. *A priori* Φ_n^* is a polynomial in X and Y. However, if we view k and b as

parameters, we may ask if $\Phi_n^* \in \mathbb{Z}[k, b, X, Y]$. The following Lemma will help us address this question.

Lemma 2.3.3. *For every $n > 1$,*

(1) *The coefficient of $X^{\nu_2(n)}$ in $\Phi^*_{\phi_{k,b};n}(X, Y)$ is a positive power of k times $C_n(k)$, where $C_n(k)$ refers to the n^{th} cyclotomic polynomial in the variable k.*

(2) *The coefficient of $Y^{\nu_2(n)}$ in $\Phi^*_{\phi_{k,b};n}(X, Y)$ is a positive power of k times a positive power of b.*

(3) *Each monomial of Φ_n^* is divisible by k.*

Proof. We have

$$\begin{aligned} F_1(X,Y) &= k(X^2 + bY^2) & G_1(X,Y) &= XY \\ F_n(X,Y) &= k(F_{n-1}^2 + bG_{n-1}^2) & G_n(X,Y) &= F_{n-1}G_{n-1}. \end{aligned} \tag{2.3.2}$$

A simple induction argument shows that for $n > 1$, we have

$$\deg_X(F_n) = \deg_X(G_n) + 1, \quad \text{and in fact } \deg_X(F_n) = 2^n \text{ and } \deg_X(G_n) = 2^n - 1.$$

(The same arguments hold for $\deg_Y F_n$ and $\deg_Y G_n$.) Now,

$$\text{coefficient of } X^{2^n} \text{ in } F_n = k\left(\text{coefficient of } X^{2^{n-1}} \text{ in } F_{n-1}\right)^2,$$

so inductively this coefficient is k^{2^n-1}. Similarly,

$$\begin{aligned} \text{coeff. of } X^{2^n-1} \text{ in } G_n &= \left(\text{coeff. of } X^{2^{n-1}} \text{ in } F_{n-1}\right)\left(\text{coeff. of } X^{2^{n-1}-1} \text{ in } G_{n-1}\right) \\ &= Y\prod_{i=0}^{n-1} k^{2^i-1} = Yk^{2^n-n-1}. \end{aligned}$$

Let c_d be the coefficient of X^{2^d} in $\Phi_d = YF_d - XG_d$ and c_d^* be the coefficient of $X^{\nu_2(d)}$ in Φ_d^*.

So that

$$\begin{aligned} c_d &= Y\left(k^{2^d-1} - k^{2^d-d-1}\right) = Yk^{2^d-d-1}\left(k^d-1\right) \\ c_n^* &= \prod_{d|n} c_d^{\mu\left(\frac{n}{d}\right)} = \prod_{d|n}\left(Yk^{2^d-d-1}\left(k^d-1\right)\right)^{\mu\left(\frac{n}{d}\right)} \\ &= \prod_{d|n} Y^{\mu\left(\frac{n}{d}\right)} \prod_{d|n}\left(k^{2^d-d-1}\right)^{\mu\left(\frac{n}{d}\right)} \prod_{d|n}\left(k^d-1\right)^{\mu\left(\frac{n}{d}\right)}. \end{aligned}$$

(Here, we use the definition of Φ_n^* and the fact that we know it is a polynomial in X and Y.) When $n > 1$, the first term is 1, the second is a positive power of k by Lemma 2.3.2, and the third is $C_n(k)$ exactly as claimed.

Also,

$$\begin{aligned} \text{coefficient of } Y^{2^n+1} \text{ in } \Phi_n = &\text{ coefficient of } Y^{2^n} \text{ in } F_n \\ &= k\left(\text{coefficient of } Y^{2^{n-1}} \text{ in } F_{n-1}\right)^2, \end{aligned}$$

so inductively this coefficient is $k^{2^n-1}b^{2^{n-1}}$. So then

$$\text{coefficient of } Y^{\nu_2(n)} \text{ in } \Phi_n^* = \prod_{d|n}\left(k^{2^d-1}b^{2^{d-1}}\right)^{\mu\left(\frac{n}{d}\right)},$$

which is a positive power of k times a positive power of b by Lemma 2.3.2.

The proof for the final claim is similar, but the algebraic details are messier. We sketch the main points here and leave the details for the reader. Inductively one may show that

$$F_n(X,Y) = k^{a(n)} f_n(X,Y) \text{ and } G_n(X,Y) = k^{b(n)} g_n(X,Y),$$

where

$$a(n) = \frac{2^n - (-1)^n}{3}, \quad b(n) = \left\lceil \frac{2(2^{n-1}-1)}{3} \right\rceil$$

and $f_n, g_n \in \mathbb{Z}[k,b,X,Y]$. So then

$$\Phi_n(X,Y) = k^{b(n)} \Psi_n(X,Y),$$

where $\Psi_n \in \mathbb{Z}[k,b,X,Y]$. Then exactly as above, it follows that a positive power of k divides each

dynatomic polynomial Φ_n^*. $\square$

Since $\Phi_n^*(X,Y)$ is homogeneous, we may dehomogenize in the usual way. We will write $\Phi_n^*(z)$ for the dehomogenized dynatomic polynomial. Note that the lead coefficient of $\Phi_1^*(z) = k-1 = C_1(k)$ and the constant term is bk.

Mobius inversion gives $\prod_{d|n} \Phi^*_{\phi_{k,b},d}(z) = \Phi_{\phi_{k,b},n} \in \mathbb{Z}[k,b,z]$. In other words, $\Phi_{\phi_{k,b},n}(z)$ factors over $\mathbb{Q}(k,b)$, so by Gauss's Lemma it factors over $\mathbb{Z}[k,b]$. Lemma 2.3.3 and the remark above show that the polynomials $\Phi^*_{\phi_{k,b},d}(z)$ in the product each have content a non-negative power of k, meaning that $\Phi^*_{\phi_{k,b},n}(z) \in \mathbb{Z}[k,b,z]$.

Lemma 2.3.4. *Let $n > 1$. Then each monomial of the n^{th} dynatomic polynomial $\Phi_n^*(X,Y)$ has the form $c_i X^{2i} Y^{\nu_2(n)-2i} b^{\frac{\nu_2(n)-2i}{2}}$ where $c_i \in \mathbb{Z}[k]$.*

Proof. We first show that for all $n \geq 1$,

$$F_n(X,Y) = \sum_{i=0}^{2^{n-1}} c_i X^{2i} Y^{2^n-2i} b^{2^{n-1}-i}, \text{ and} \tag{2.3.3}$$

$$G_n(X,Y) = Y \sum_{j=1}^{2^{n-1}} d_j X^{2j-1} Y^{2^n-2j} b^{2^{n-1}-j}, \tag{2.3.4}$$

where $c_i, d_j \in \mathbb{Z}[k]$.

From equation (2.3.2), we see that F_1 and G_1 have the correct form. Assume F_{n-1} and G_{n-1} satisfy the claim above.

Consider

$$F_n = k\left(\sum_{i=0}^{2^{n-2}} c_i X^{2i} Y^{2^{n-1}-2i} b^{2^{n-2}-i}\right)^2 + kb\left(Y\sum_{j=1}^{2^{n-2}} d_j X^{2j-1} Y^{2^{n-1}-2j} b^{2^{n-2}-j}\right)^2.$$

If we look at the first term monomial by monomial we get

$$\left(c_i X^{2i} Y^{2^{n-1}-2i} b^{2^{n-2}-i}\right)\left(c_j X^{2j} Y^{2^{n-1}-2j} b^{2^{n-2}-j}\right)$$
$$= c_i c_j X^{2(i+j)} Y^{2^n-2(i+j)} b^{2^{n-1}-(i+j)},$$

so each monomial has the correct form. Now consider monomials from the second term:

$$kbY^2\left(d_iX^{2i-1}Y^{2^{n-1}-2i}b^{2^{n-2}-i}\right)\left(d_jX^{2j-1}Y^{2^{n-1}-2j}b^{2^{n-2}-j}\right)$$
$$= kd_id_jX^{2(i+j-1)}Y^{2^n-2(i+j-1)}b^{2^{n-1}-(i+j-1)},$$

which has the correct form. This completes the proof for F_n, and the proof for G_n is similar.

It follows immediately from equations (2.3.3) and (2.3.4) that

$$\Phi_n(X,Y) = YF_n - XG_n = Y\sum_{i=0}^{2^n} e_iX^{2i}Y^{2^n-2i}b^{2^{n-1}-i}.$$

We now compute the dynatomic polynomial:

$$\begin{aligned}\Phi_n^*(X,Y) &= \prod_{d|n}\left(Y\sum e_iX^{2i}Y^{2^d-2i}b^{2^{d-1}-i}\right)^{\mu\left(\frac{n}{d}\right)}\\ &= \prod_{d|n}Y^{\mu\left(\frac{n}{d}\right)}\prod_{d|n}\left(\sum e_iX^{2i}Y^{2^d-2i}b^{2^{d-1}-i}\right)^{\mu\left(\frac{n}{d}\right)}\\ &= \prod_{d|n}\left(\sum e_iX^{2i}Y^{2^d-2i}b^{2^{d-1}-i}\right)^{\mu\left(\frac{n}{d}\right)},\end{aligned}$$

where the last step follows because $n > 1$.

Let

$$\alpha = \sum e_iX^{2i}Y^{D_\alpha-2i}b^{\frac{D_\alpha}{2}-i} \text{ and } \beta = \sum f_jX^{2j}Y^{D_\beta-2j}b^{\frac{D_\beta}{2}-j}.$$

Clearly the form is not affected if we add or subtract two such monomials. It is then easy to check that $\alpha\beta$ and $\frac{\alpha}{\beta}$ also have the correct form. □

Lemma 2.3.5. *For all $n \geq 1$, there exists a homogeneous polynomial $\psi_n(w,b) \in \mathbb{Z}[w,b]$ such that $\psi_n(z^2,b) = \Phi_n^*(z,b)$.*

Proof. From Lemma 2.3.4, when $n > 1$ each monomial of $\Phi_n^*(z)$ has the form $c_iz^{2i}b^{\frac{\nu_2(n)-2i}{2}}$. A straightforward calculation shows that $\Phi_1^*(z)$ also has this form.

Now substitute $w = z^2$ to get $\Phi_n^*(w)$ with monomials of the form $c_iw^ib^{\frac{\nu_2(n)}{2}-i}$, which is homogeneous in w and b, with degree $\frac{\nu_2(n)}{2}$. □

Definition 2.3.6. Let $F(X,Y)$ be a homogeneous polynomial. We define $\ell(F)$ to be the leading coefficient of the dehomogenized polynomial $F(z,1)$ and $c(F)$ to be the constant term of $F(z,1)$.

Lemma 2.3.7. *Let*

$$\begin{aligned}\phi_b(X,Y)\colon \mathbb{P}^1 &\to \mathbb{P}^1\\ (X,Y) &\mapsto (X^2+bY^2, XY).\end{aligned}$$

Then

$$\ell(\Phi_n^*(X,Y)) = \begin{cases} p & \text{if } n = p^e, e \geq 1 \\ b & \text{if } n = 1 \\ 1 & \text{otherwise,} \end{cases}$$

and $c(\Phi_n^*)$ is a non-negative power of b.

Proof. The result for $n = 1$ follows from the remark after Lemma 2.3.3.

For $n > 1$, we see from Lemma 2.3.3 part (1) that $\ell(\Phi_n^*)$ is a non-negative power of k times $C_n(k)$, where $C_n(k)$ is the n^{th} cyclotomic polynomial in the variable k. The result follows from evaluating this at $k = 1$. Similarly, the result for $c(\Phi_n^*)$ follows from part (2) of Lemma 2.3.3 and evaluating at $k = 1$. (See, for example, [8, p. 280 points **2.** and **4.**] to evaluate the cyclotomic polynomials at $k = 1$.) □

2.4 The Explicit Bound

In this section, we find an explicit uniform bound for the number of $\mathbb{Q}$ preperiodic points for a one-parameter family of quadratic rational maps; namely, the quadratic maps with a unique fixed point. The existence of such a bound follows immediately from Theorem 2.2.7, so the content of this work is in finding the bound explicitly. By construction, a rational point (z_0, b_0) on the variety $V(\Phi_n^*(z,b))$ corresponds to a quadratic rational map $\phi(z) = z + \frac{b_0}{z}$, and a rational point z_0 of period n for ϕ. Note that $b_0 \neq 0$, since that value does not give a degree 2 rational map.

By Lemma 2.3.5, we may substitute $w = z^2$ in Φ_n^*, and the resulting polynomial $\psi_n(w,b) \in \mathbb{Z}[w,b]$ is homogeneous in w and b. So if $V(\Phi_n^*(z,b))$ has a rational point (z_0, b_0) with $b_0 \neq 0$, then $V(\psi_n(w,b))$ has a rational point $\left(z_0^2, b_0\right)$. Since $\psi_n(w,b)$ is homogeneous, we may equivalently ask if $\psi_n(w,1)$ has a rational root.

Theorem 2.4.1. *The rational map $\phi(z) = z + \frac{b}{z}$ where $b \in \mathbb{Q}$ has no rational points with primitive period $n \geq 5$.*

Proof. From Lemma 2.3.7, we know that for $n > 1$ the lead coefficient of $\psi_n(w, 1) \in \mathbb{Z}[w]$ is either 1 (if n is not a prime power) or p (if $n = p^e$) and the constant term is 1. The only rational roots of such a polynomial are ± 1 when n is not a prime power, and ± 1 or $\pm\frac{1}{p}$ when n is a power of a prime.

In either case, we can have no more than four rational roots of ψ_n, which means no more than four rational points are on any given cycle, and this is independent of the parameter b. □

We now combine Theorem 2.4.1 with earlier work on the two-parameter family $\phi(z) = kz + \frac{b}{z}$ to find exactly what primitive periods are possible for rational periodic points.

Corollary 2.4.2. *If $P \in \mathbb{P}^1(\mathbb{Q})$ is a periodic point for $\phi(z) = z + \frac{b}{z}$ where $b \in \mathbb{Q}$, then P is either the point at infinity or a point of primitive period* 2*.*

Proof. From Theorem 2.4.1, we know that the primitive period of P must be less than 5.

From [12, Theorem 4], a map of the form $\phi(z) = kz + \frac{b}{z}$ with $k, b \in \mathbb{Q}^*$ has a rational point of primitive period 4 if there is some $m \in \mathbb{Q} \setminus \{0, \pm 1\}$ such that $k = 2m/(m^2-1)$ and $b = -m/(m^4-1)$. In the proof of that theorem, we see that the map has a rational point of primitive period 4 if and only if we can find a rational point on a certain algebraic curve. The parameterization of the curve given in the proof shows that in fact the condition $k = 2m/(m^2 - 1)$ is necessary. However, there is no such m with $1 = 2m/(m^2 - 1)$. We conclude that P has primitive period less than 4.

Similarly, [12, Theorem 3] says that if $\phi(z) = kz + \frac{b}{z}$ with $k, b \in \mathbb{Q}^*$, then $\phi(z)$ has no rational point of primitive period 3. Hence, P has primitive period one or two.

Solving $\phi(z) = z$, we see that P is a fixed point if and only if P is the point at infinity. The only other possibility is a rational point of primitive period 2. □

To finish finding the exact bound on the number of rational preperiodic points for a map of the form $\phi(z) = z + \frac{b}{z}$, we introduce a bit more notation.

Definition 2.4.3. Let m and n be positive integers. Given a rational map ϕ and a point P that is strictly preperiodic for ϕ (in other words, P is preperiodic but not periodic), we say that P has type m_n if P enters a cycle of primitive period m after n iterations. That is, $\phi^{n+m}(P) = \phi^n(P)$, where $m \geq 1$ and $n \geq 1$ are the smallest such integers.

Corollary 2.4.4. *Let $\phi(z) = z + \frac{b}{z} \in \mathbb{Q}(z)$ with $b \neq 0$. Then ϕ has either* 2*,* 4*, or* 6 *rational preperiodic points.*

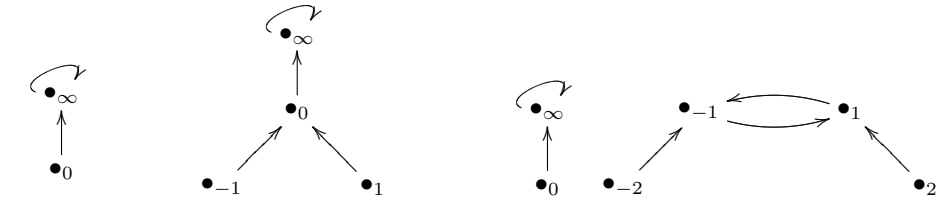
Proof. First note that for every nonzero $b \in \mathbb{Q}$, the point at infinity is fixed, and $\phi(0)$ is infinity. Hence, every ϕ_b has a rational fixed point and a rational point of type 1_1.

Applying [12, Proposition 6], we see that ϕ has a rational points of type 1_2 if and only if $b = -c^2$ for some $c \in \mathbb{Q}^*$. However, all of these maps are conjugate over $\mathbb{Q}$, so take $b = -1$ as a representative. From [12, Propositions 7 and 8], we conclude that ϕ has no rational points of type 1_n for $n > 2$.

Applying [12, Proposition 2], we see that ϕ has a rational point of primitive period 2 if and only if $b = -2c^2$ for some $c \in \mathbb{Q}^*$. Again, all such maps are conjugate over $\mathbb{Q}$, so we take $b = -2$ as a representative. It is a simple matter to check that in this case, ϕ_b has two rational points of type 2_1. (See Figure 2.1.) From [12, Proposition 8], we conclude that ϕ_b has no rational points of type 2_n for $n > 1$.

Finally, [12, Proposition 9] says that ϕ_b has both rational points of type 1_2 and rational points of primitive period 2 if and only if we can solve $1 = 1/(x^2 - 1)$ with $x \in \mathbb{Q} \smallsetminus \{0, \pm 1\}$. Evidently, this is not possible. Hence for $b = -1$ (and all $\mathbb{Q}$-conjugate maps), ϕ_b has four rational preperiodic points. Similarly, for $b = -2$ (and all $\mathbb{Q}$-conjugate maps), ϕ_b has six rational preperiodic points. There are no b values for which ϕ_b has more than six rational preperiodic points. □

We provide a graphical representation of all possible structures for rational preperiodic points for the family $\phi(z) = z + \frac{b}{z}$. In these graphs, the vertices represent points in $\mathbb{P}^1(\mathbb{Q})$, and an arrow from vertex P to vertex Q indicates $\phi(P) = Q$.



(a) $b = 1$ (b) $b = -1$ (c) $b = -2$

Figure 2.1: All possible rational preperiodic graphs for $\phi_b(z) = z + \frac{b}{z}$.

2.5 Another Family of Twists

We conclude with an abbreviated analysis of the possible preperiodic structures for another family of twists. Lemma 2.3.3 says the lead coefficient of the dynatomic polynomials are powers of k times a cyclotomic polynomial in k. With the help of [7, Proposition 1], we can evaluate cyclotomic

polynomials at roots of unity. Hence, we consider $k = -1$. The proofs are similar to those in Section 2.4, so the details will be sketched here.

We now consider the maps $\psi_b(z) = -\left(z + \frac{b}{z}\right)$. Again, each ψ_b is conjugate to ψ_1 via the map $f(z) = z\sqrt{b}$. The family of twists is distinct from the one already considered, since ψ_b has two finite fixed points at $\pm\sqrt{-b/2}$.

Note that Lemmas 2.3.3, 2.3.4, and 2.3.5 apply to the family ψ_b, as we are taking $k = -1$.

Lemma 2.5.1. *Let*

$$\begin{aligned} \psi_b(X,Y)\colon \mathbb{P}^1 &\to \mathbb{P}^1 \\ (X,Y) &\mapsto \left(-(X^2 + bY^2), XY\right). \end{aligned}$$

Then

$$\ell(\Phi_n^*(X,Y)) = \begin{cases} \pm p & \text{if } n = 2p^e, e \geq 1, p \text{ prime} \\ -2 & \text{if } n = 1 \\ \pm 1 & \text{otherwise,} \end{cases}$$

and $c(\Phi_n^*)$ is a non-negative power of b.

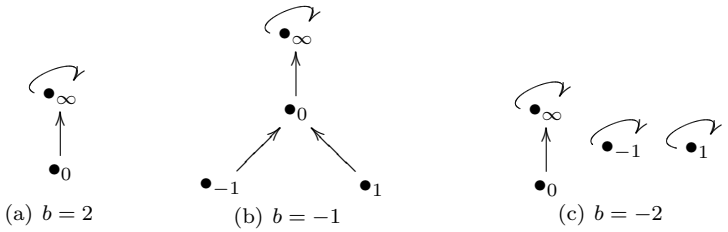
Proof. The case $n = 1$ is found by computation. By Lemma 2.3.3, the lead coefficient of ψ_b is some power of k times a cyclotomic polynomial. We apply [7, Proposition 1] to evaluate the cyclotomic polynomials at $k = -1$, yielding the result. □

Proposition 2.5.2. *Let $\psi_b(z) = -\left(z + \frac{b}{z}\right) \in \mathbb{Q}(z)$ with $b \neq 0$. Then ψ_b has either 2 or 4 rational preperiodic points.*

Proof. A proof identical to Theorem 2.4.1 using Lemma 2.5.1 shows there can be no rational points of primitive period $n \geq 5$, and we apply [12, Theorems 3 and 4] to see that there are no rational points of primitive period 3 or 4. From [12, Proposition 2], we conclude that no value of $b \in \mathbb{Q}^*$ gives a rational map with a rational point of primitive period 2. Hence, we need only consider fixed points and points of type 1_n for $n \geq 1$.

For every $b \in \mathbb{Q}^*$, there is a rational fixed point at ∞ and a rational point of type 1_1 at 0. By [12, Proposition 1], ψ_b has rational finite fixed points if and only if $b = -2c^2$. Since all such maps are conjugate over $\mathbb{Q}$, so we take $b = -2$ as a representative. There are no other type 1_1 rational points.

Applying [12, Proposition 6] we have rational points of type 1_2 if and only if $b = -c^2$. Again, all such maps are conjugate over $\mathbb{Q}$, so we take $b = -1$ as a representative. By [12, Proposition 7 and 8] there are no rational points of type 1_n for $n > 2$. See Figure 2.2. □



(a) $b = 2$ (b) $b = -1$ (c) $b = -2$

Figure 2.2: All possible rational preperiodic graphs for $\psi_b(z) = -\left(z + \frac{b}{z}\right)$.

CHAPTER 3
PERIODIC POINTS IN TOWERS OF FINITE FIELDS FOR POLYNOMIALS ASSOCIATED WITH ALGEBRAIC GROUPS

This paper was in joint work with Michelle Manes and has been submitted for publication [13].

3.1 Introduction

We fix the following notation:

$\phi(z)$	a polynomial.
$\phi^n(z)$	the n^{th} iterate of ϕ under composition; we take $\phi^0(z) = z$.
$\mathcal{O}_\phi(\alpha)$	the (forward) orbit of a point α under ϕ; i.e. $\{\phi^n(z) \mid n \geq 0\}$.
$\text{Per}(\phi, K)$	the set of periodic points for ϕ in the field K; i.e. $\{\alpha \in K \mid \phi^n(\alpha) = \alpha \text{ for some } n > 0\}$.

When iterating a polynomial function ϕ over a finite field, the orbit of any point $\alpha \in \mathbb{F}_{p^n}$ is a finite set. That is, all points are preperiodic, meaning the orbit eventually enters a cycle. But many natural questions about the structure of orbits over finite fields remain:

(i) Fix a finite field $\mathbb{F}_{p^n}$ and look over all polynomials of fixed degree d: On average are there "lots" of periodic points with relatively small tails leading into the cycles? Or do we expect few periodic points with long tails? (See Figures 3.1 and 3.2.)

(ii) Fix a polynomial: How does the proportion of periodic points in $\mathbb{F}_p$ vary as $p \to \infty$?

(iii) Again fix a polynomial: How does the proportion of periodic points in $\mathbb{F}_{p^n}$ vary as $n \to \infty$?

Recent work by Flynn and Garton [5] addresses the first question. Using combinatorial arguments, they bound the average number of periodic points over all polynomials of degree d. For d large (that is, $d \geq \sqrt{p^n}$), their bound of $\frac{5}{6}\sqrt{p^n}$ agrees with earlier heuristic arguments.

In her thesis [11], Madhu tackles the second question in the case $\phi(z) = z^m + c$, using Galois-theoretic methods. With some restrictions on c, she shows that for primes congruent to 1 modulo m, the proportion of points in $\mathbb{F}_p$ that are periodic points for ϕ goes to zero as $p \to \infty$.

In the current work, we focus on the third question in the special case that the polynomial map $\phi(z)$ can be viewed as an endomorphism of an underlying algebraic group. This restriction makes

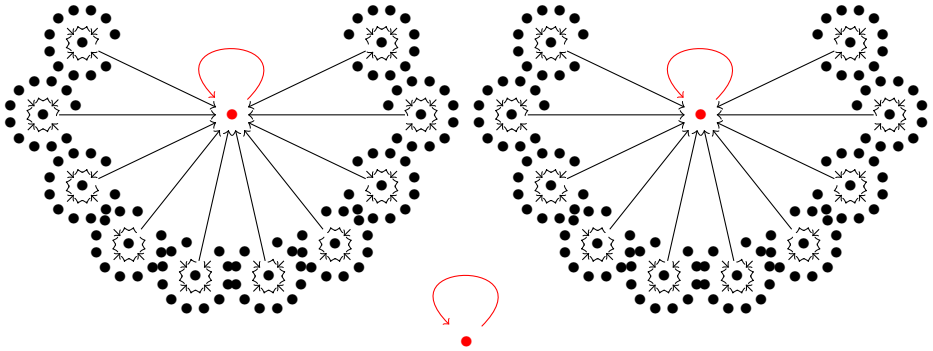


Figure 3.1: Few periodic points: $\phi(z) = z^{11}$ on $\mathbb{F}_{3^5}$ has three fixed points and 240 strictly preperiodic points.

the structure of the periodic points particularly simple and is therefore a natural place to begin a more complete investigation of the question.

We will quickly see that in fact the naïve limit

$$\lim_{n\to\infty} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}$$

does not exist in general, because the map ϕ acts as a permutation polynomial whenever n is relatively prime to the multiplicative order of p modulo the degree of ϕ.

However, we are able to find limiting proportions along towers of finite fields $\mathbb{F}_{p^n}$ with suitable divisibility conditions on n. For example, we have the following two results for q an odd prime. Similar results hold in the case $q = 2$ and for maps of composite degree.

Theorem (Theorems 3.4.5 and 3.5.7)**.** *Fix a prime p and let q be a different odd prime. Define δ to be the multiplicative order of p modulo q and $\mu = v_q(p^\delta - 1) \geq 1$. Let $\phi(z) = z^q$, and let $T_q(z)$ be the q^{th} Chebyshev polynomial. Then we have the following:*

$$\lim_{\substack{n\to\infty \\ \delta|n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \frac{1}{q^{\mu+\nu}}, \text{ and}$$

$$\lim_{\substack{n\to\infty \\ \delta|2n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(T_q, \mathbb{F}_{p^n})}{p^n} = \frac{q^{\mu+\nu}+1}{2q^{\mu+\nu}}.$$

We conclude with an outline of the chapter and a survey of the techniques used.

Section 3.2 We offers a brief overview of the two families of polynomials we consider here: pure

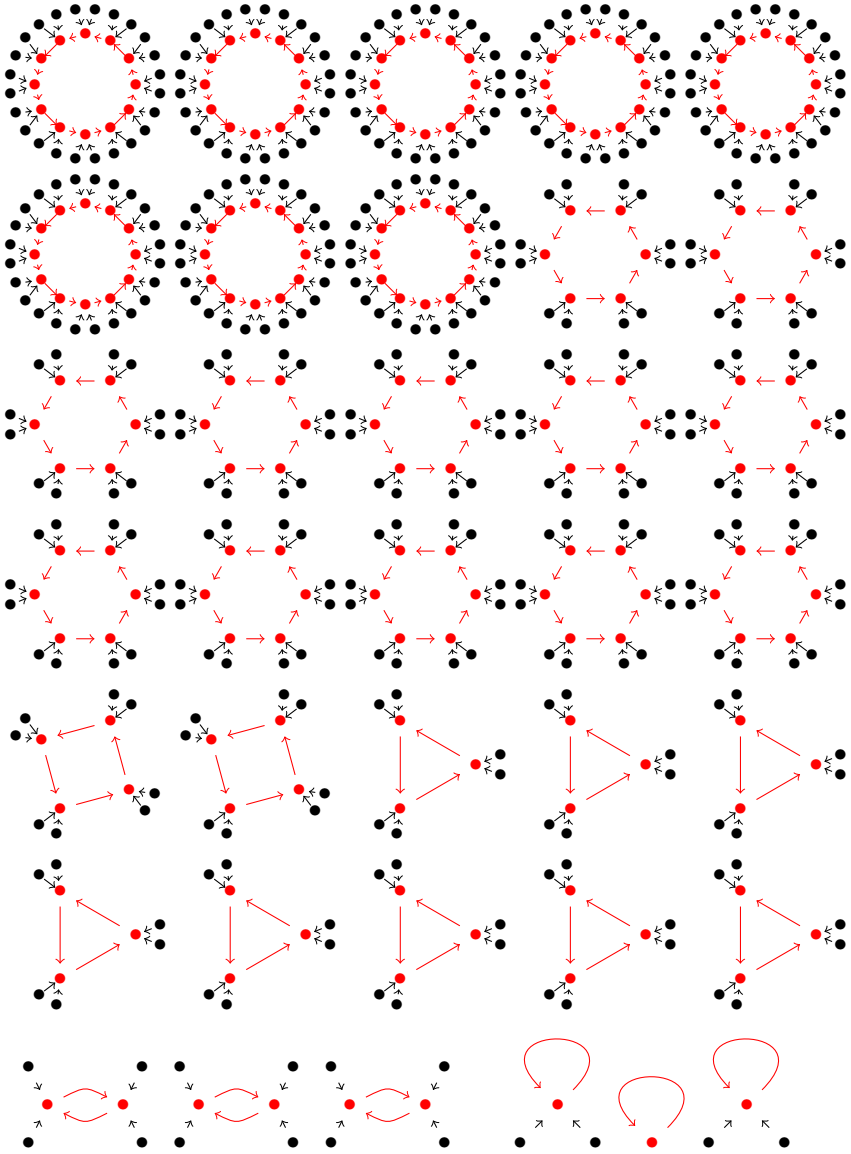


Figure 3.2: Lots of periodic points: $\phi(z) = z^3$ on $\mathbb{F}_{5^4}$ has 209 periodic points and 416 strictly preperiodic points.

power maps and Chebyshev polynomials.

Section 3.3 We prove some useful lemmas concerning q-adic valuations.

Sections 3.4 and 3.5 Here we give our main results for pure power maps and Chebyshev polynomials respectively.

3.2 Polynomials associated to endomorphisms of algebraic groups

We first consider the multiplicative group $\mathbb{G}_m$ where for a field K, the K-valued points are $\mathbb{G}_m(K) = K^*$. The endomorphism ring of $\mathbb{G}_m$ is $\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z} &\to \mathrm{End}(\mathbb{G}_m) \\ d &\mapsto z^d. \end{aligned}$$

So these pure power maps can be viewed as endomorphisms of an underlying group. Iteration of pure power maps is particularly easy to understand, as

$$\phi(z) = z^d \quad \text{means } \phi^n(z) = z^{d^n}.$$

Similarly, we consider the additive group $\mathbb{G}_a$, whose underlying scheme is the affine line $\mathbb{A}^1$, which may be viewed as a quotient of $\mathbb{G}_m$:

$$\begin{aligned} \mathbb{G}_m/\{z = z^{-1}\} &\to \mathbb{A}^1 \\ z &\mapsto z + z^{-1}. \end{aligned}$$

Since the automorphism $z \mapsto z^{-1}$ commutes with the power map $\phi(z) = z^d$, the polynomial ϕ descends to an endomorphism of $\mathbb{A}^1$, which we denote T_d, the d^{th} Chebyshev polynomial.

$$\begin{array}{ccc}
\mathbb{G}_m & \xrightarrow{z\mapsto z^d} & \mathbb{G}_m \\
\downarrow & & \downarrow \\
\mathbb{G}_m/z \sim z^{-1} & \xrightarrow{z\mapsto z^d} & \mathbb{G}_m/z \sim z^{-1} \\
\downarrow{\scriptstyle z\mapsto z+z^{-1}} & & \downarrow{\scriptstyle z\mapsto z+z^{-1}} \\
\mathbb{A}^1 & \xrightarrow{\omega\mapsto T_d(\omega)} & \mathbb{A}^1
\end{array}$$

Taking as a definition the fact that $T_d(w) \in \mathbb{Z}[w]$ satisfies

$$T_d(z + z^{-1}) = z^d + z^{-d}, \tag{3.2.1}$$

one may prove existence and uniqueness of the Chebyshev polynomials along with a simple recursion

$$T_d(w) = \begin{cases} 2 & d = 0 \\ w & d = 1 \\ wT_{d-1}(w) - T_{d-2}(w) & d \geq 2. \end{cases} \tag{3.2.2}$$

A pleasant rule for composition of Chebyshev polynomials arises directly from the definition in (3.2.1):

$$T_d \circ T_e(w) = T_{de}(w) = T_e \circ T_d(w),$$

which in turn gives a simple form of iteration

$$T_d^n(w) = T_{d^n}(w). \tag{3.2.3}$$

We refer the interested reader to [23, Chapter 6] for more on the dynamics of pure power maps, Chebyshev polynomials, and other rational maps arising from algebraic groups, including proofs of some of the statements above.

3.3 Preliminaries

This section contains a few facts about valuations and periodic points over finite fields which will be useful in the sequel. Throughout this section, p and q represent distinct primes, n is a positive integer, and we use the following additional notation:

$v_q(n)$ q-adic valuation; i.e. if $n = q^\nu d$ with $q \nmid d$, then $v_q(n) = \nu$.

δ the multiplicative order of p modulo q; i.e. the smallest positive integer such that $q \mid \left(p^\delta - 1\right)$.

Since our goal is ultimately to classify periodic points in finite fields, we need to be able to recognize which points are periodic as opposed to strictly preperiodic. Our first result says that any finite set that is *forward invariant under* ϕ contains only periodic points.

Lemma 3.3.1. *Let $\phi(z) \in K[z]$ be a polynomial and let $S \subseteq K$ be finite. If*

$$\phi(S) = S,$$

then $S \subseteq \mathrm{Per}(\phi, K)$.

Proof. Fix $\alpha \in S$. For every $n > 0$ we have $\phi^n(S) = S$. Hence for every n, we can find $\beta_n \in S$ such that $\phi^n(\beta_n) = \alpha$.

Since S is finite, for some $n > m > 0$, we must have $\beta_n = \beta_m$. But this means we have $\beta \in S$ such that

$$\phi^m(\beta) = \alpha \text{ and } \phi^n(\beta) = \alpha, \text{ so } \quad \phi^{n-m}(\alpha) = \alpha$$

and α is periodic. □

The next three lemmas give us the tools to calculate the q-adic valuation of $p^{nd} - 1$ based on the valuations of $p^d - 1$ and n. These will be used to create the towers of finite fields for which we can calculate limiting proportions of periodic points. The results are different enough for $q = 2$ compared to odd primes that we break up the cases along those lines.

Lemma 3.3.2. *Let p and q be distinct primes. Suppose $v_q(p^d - 1) = \mu \geq 1$ and $v_q(n) = 0$. Then $v_q(p^{nd} - 1) = \mu$.*

Proof.

$$\begin{aligned} v_q(p^{nd} - 1) &= v_q(p^d - 1) + v_q(\underbrace{p^{(n-1)d} + p^{(n-2)d} + \cdots + p^d + 1}_{n \text{ terms, all } 1 \bmod q.}) \\ &= \mu + 0 = \mu. \end{aligned}$$

□

Lemma 3.3.3. *Let p be an odd prime with $\max\{v_2(p-1), v_2(p+1)\} = \mu$. Let $v_2(n) = \nu \geq 1$. Then $v_2(p^n - 1) = \mu + \nu$.*

Proof. We proceed by induction on $v_2(n)$. For every odd d, exactly one of $p^d - 1$, $p^d + 1$ is divisible by 4. (In particular, $\mu \geq 2$.) Similar to the proof of Lemma 3.3.2, we have

$$\begin{aligned} v_2(p^{2d} - 1) &= v_2(p^d - 1) + v_2(p^d + 1) \\ &= v_2(p-1) + v_2(\text{odd number}) + v_2(p+1) + v_2(\text{odd number}) \\ &= \mu + 1. \end{aligned}$$

Assume for all n with $v_2(n) = \nu > 1$ we have $v_2(p^n - 1) = \mu + \nu > 1$, in which case $v_2(p^n + 1) = 1$. Consider some n with $v_2(n) = \nu + 1$ and choose d odd such that $n = 2^{\nu+1}d$.

$$\begin{aligned} v_2(p^n - 1) = v_2(p^{2^{\nu+1}d} - 1) &= v_2(p^{2^\nu d} - 1) + v_2(p^{2^\nu d} + 1) \\ &= \mu + \nu + 1. \end{aligned}$$

□

Lemma 3.3.4. *Let q be an odd prime. Suppose $v_q(p^d - 1) = \mu \geq 1$ and $v_q(n) = \nu$. Then $v_q(p^{nd} - 1) = \mu + \nu$.*

Proof. The result for $\nu = 0$ is exactly Lemma 3.3.2. Choose k so that $p^d = 1 + kq^\mu$ (in particular $q \nmid k$). Since $q \geq 3$ and $\mu \geq 1$, we have $q\mu \geq \mu + 2$. Hence

$$p^{qd} = (1 + kq^\mu)^q \equiv 1 + kq^{\mu+1} \pmod{q^{\mu+2}}.$$

The result then follows by a straightforward induction. □

Our main results in Sections 3.4 and 3.5 will be stated for maps of prime degree q. The following Lemma shows that in fact the proportion of periodic points is identical for the maps of degree q and degree q^e. We focus on the prime degree case for ease of exposition.

Lemma 3.3.5. *Let $\phi(z) = z^q$ and $\psi(z) = z^{q^e}$. Then $\mathrm{Per}(\phi, \mathbb{F}_{p^n}) = \mathrm{Per}(\psi, \mathbb{F}_{p^n})$ for every n. Similarly, $\mathrm{Per}(T_q, \mathbb{F}_{p^n}) = \mathrm{Per}(T_{q^e}, \mathbb{F}_{p^n})$*

Proof. Note that $\phi^m(z) = z^{q^m}$ and $\psi^m(z) = z^{q^{em}}$. So if $\phi^m(\alpha) = \alpha$, then likewise $\psi^m(\alpha) = \alpha$. On the other hand, if $\psi^m(\alpha) = \alpha$, then $\phi^{em}(\alpha) = \alpha$. Applying the iteration for Chebyshev polynomials in (3.2.3) gives the result in that case as well. □

3.4 Power maps

Throughout this section, we fix the polynomial

$$\phi(z) = z^q,$$

for q prime. We also take p to be any prime different from q. Our interest is in understanding the proportion of periodic points in $\mathbb{F}_{p^n}$ as n grows. In particular, we consider the following limits.

Definition 3.4.1. We define the following proportions for integers $\nu \geq 0$. Recall that δ is the multiplicative order of p modulo q.

$$P_\nu(\phi) = \lim_{\substack{n \to \infty \\ \delta \mid n \\ v_q(n) = \nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}.$$

We know that $\delta < q$. So if n satisfies

$$\delta \mid n \text{ and } v_q(n) = \nu,$$

then there is n' such that

$$n = \delta n' \text{ and } v_q(n') = \nu.$$

We will implicitly use this fact later when applying Lemma 3.3.4.

We begin by classifying explicitly the periodic points of ϕ in $\mathbb{F}_{p^n}$.

Lemma 3.4.2. *Let $p^n - 1 = q^e d$ with $q \nmid d$. Then*

$$\operatorname{Per}(\phi, \mathbb{F}_{p^n}) = \{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^d = 1\}.$$

Proof. The defining equation for $\mathbb{F}_{p^n}$ is

$$z^{p^n} - z = z(z^d - 1)Q(z), \tag{3.4.1}$$

for some monic $Q(z) \in \mathbb{Z}[z]$. Clearly 0 is fixed by ϕ. Since $q \nmid d$, the roots of $z^d - 1$ form a group of order prime to q. Hence $\phi(z) = z^q$ is a permutation of the group elements, and these roots are forward invariant under ϕ. So we have

$$\{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^d = 1\} \subseteq \mathrm{Per}(\phi, \mathbb{F}_{p^n}).$$

Now let α be a root of $Q(z)$; so in particular $\alpha^{q^e d} = 1$ but $\alpha^d \neq 1$. Hence for some $1 \leq i \leq e$ and some $d' \mid d$, we have $\alpha^{q^i d'} = 1$. In other words, α^{q^i} has order dividing d and is therefore a root of $z^d - 1$. Since roots of $z^d - 1$ are forward invariant under ϕ, α is not periodic for ϕ. □

Remark. We applied Lemma 3.4.2 to create the examples in Figures 3.1 and 3.2. Finding a value of $p^n - 1$ where, in the notation of the Lemma, q^e is much smaller than d gives "lots of periodic points." Similarly, an example where q^e is relatively large compared with d gives few periodic points.

The following Proposition justifies our choice of limit in Definition 3.4.1 because the only interesting proportions of periodic points are those where $\delta \mid n$.

Proposition 3.4.3. *If $\delta \nmid n$, all points of $\mathbb{F}_{p^n}$ are periodic under ϕ.*

Proof. Since $\delta \nmid n$, $q \nmid p^n - 1$. The result follows immediately from Lemma 3.4.2. □

We now prove our main results for pure power maps. The statement is slightly different depending on whether $q = 2$ or q is an odd prime. The difference parallels exactly the difference between the valuation calculations in Lemmas 3.3.3 and 3.3.4.

Theorem 3.4.4. *Let $v_2(p-1) = \lambda$ and $\max\{v_2(p-1), v_2(p+1)\} = \mu$. Then for $\phi(z) = z^2$ we have*

$$P_0(\phi) = \frac{1}{2^\lambda}, \qquad \text{and}$$
$$P_\nu(\phi) = \frac{1}{2^{\mu+\nu}} \qquad \text{for } \nu \geq 1.$$

Proof. First consider n odd. By Lemma 3.3.2, we may choose d_n odd so that $p^n - 1 = 2^\lambda d_n$. By Lemma 3.4.2 the periodic points for ϕ in $\mathbb{F}_{p^n}$ are 0 and roots of $z^{d_n} - 1$. So there are $d_n + 1$ points

in $\mathrm{Per}(\phi, \mathbb{F}_{p^n})$. Then

$$P_0(\phi) = \lim_{\substack{n\to\infty \\ n \text{ odd}}} \frac{\#\mathrm{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{d_n\to\infty} \frac{d_n+1}{2^\lambda d_n + 1} = \lim_{\substack{d\to\infty \\ d \text{ odd}}} \frac{d+1}{2^\lambda d+1} = \frac{1}{2^\lambda}.$$

Now let $v_2(n) = \nu \geq 1$. By Lemma 3.3.3, $p^n - 1 = 2^{\mu+\nu} d_n$ with d_n odd. Again, the periodic points for ϕ in $\mathbb{F}_{p^n}$ are 0 and roots of $z^{d_n} - 1$. Hence

$$P_\nu(\phi) = \lim_{\substack{n\to\infty \\ v_2(n)=\nu}} \frac{\#\mathrm{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{d\to\infty \\ d \text{ odd}}} \frac{d+1}{2^{\mu+\nu} d+1} = \frac{1}{2^{\mu+\nu}}.$$

□

In Tables 3.1–3.2, we illustrate Theorem 3.4.4. The data were calculated using Sage [25].

p	3	5	41	17
$\lambda = v_2(p-1)$	1	2	3	4
$\frac{\#\mathrm{Per}(z^2, \mathbb{F}_p)}{p}$	0.666666667	0.400000000	0.146341463	0.117647059
$\frac{\#\mathrm{Per}(z^2, \mathbb{F}_{p^3})}{p^3}$	0.518518518	0.256000000	0.125012696	0.0626908203
$\frac{\#\mathrm{Per}(z^2, \mathbb{F}_{p^5})}{p^5}$	0.502057613	0.250240000	0.125000008	0.0625006603
$\frac{\#\mathrm{Per}(z^2, \mathbb{F}_{p^7})}{p^7}$	0.500228624	0.250009600	0.125000000	0.0625000023
$\frac{1}{2^\lambda}$	0.5	0.25	0.125	0.0625

Table 3.1: $\dfrac{\#\mathrm{Per}(z^2, \mathbb{F}_{p^n})}{p^n}$ with n odd.

Theorem 3.4.5. *Let q be an odd prime. We continue with the earlier notation: δ is the multiplicative order of p modulo q and $v_q(p^\delta - 1) = \mu \geq 1$. For $\phi(z) = z^q$, we have*

$$P_\nu(\phi) = \frac{1}{q^{\mu+\nu}}.$$

Proof. Recall that the limit for $P_\nu(\phi)$ is taken over n such that $\delta \mid n$ and $v_q(n) = \nu$. By Lemma 3.3.4, for such n we have $p^n - 1 = q^{\mu+\nu} d_n$ with $q \nmid d_n$, and by Lemma 3.4.2 the periodic points are 0 and

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\dfrac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^2})}{p^2}$	0.222222222	0.0816326530	0.0346020761
$\dfrac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^6})}{p^6}$	0.126200274	0.0625079686	0.0312500401
$\dfrac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^{10}})}{p^{10}}$	0.125014818	0.0625000033	0.0312500000
$\dfrac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^{14}})}{p^{14}}$	0.125000183	0.0625000000	0.0312500000
$\dfrac{1}{2^{\mu+1}}$	0.125	0.0625	0.03125

Table 3.2: $\dfrac{\#\operatorname{Per}(z^2, \mathbb{F}_{p^n})}{p^n}$ with $v_2(n) = 1$.

roots of $z^{d_n} - 1$. So

$$P_\nu(\phi) = \lim_{\substack{n\to\infty \\ \delta\mid n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{n\to\infty \\ \delta\mid n \\ v_q(n)=\nu}} \frac{d_n + 1}{q^{\mu+\nu} d_n + 1}$$
$$= \lim_{\substack{d\to\infty \\ q\nmid d}} \frac{d+1}{q^{\mu+\nu} d + 1} = \frac{1}{q^{\mu+\nu}}.$$

□

Tables 3.3–3.4 illustrate Theorem 3.4.5 for the map $\phi(z) = z^3$. Again, the data were calculated using Sage [25].

We wish to extend our results to polynomials with composite degree. Lemma 3.3.5 takes care of prime power degree, so we are left to consider the case $\phi(z) = z^t$ for $t = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ and $r \geq 2$. For each $1 \leq i \leq r$, let

$$\delta_i \text{ is the multiplicative order of } p_i \text{ modulo } q_i \quad \text{and} \quad \mu_i = v_{q_i}(p^{\delta_i} - 1).$$

We also define

$$\Delta = \operatorname{lcm}\{\delta_i\}_{1\leq i\leq r}.$$

An argument identical to the one in Proposition 3.5.5 shows that if $\gcd(\Delta, n) = 1$, then all points

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^\delta})}{p^\delta}$	0.360000000	0.157894737	0.0373798505
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{2\delta}})}{p^{2\delta}}$	0.334400000	0.113573407	0.0370371591
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{4\delta}})}{p^{4\delta}}$	0.333335040	0.111117932	0.0370370371
$\dfrac{1}{3^\mu}$	0.333333333	0.111111111	0.0370370370

Table 3.3: $\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^n})}{p^n}$ with $v_3(n) = 0$.

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{3\delta}})}{p^{3\delta}}$	0.111168000	0.0371774311	0.0123456791
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{6\delta}})}{p^{6\delta}}$	0.111111115	0.0370370575	0.0123456790
$\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^{12\delta}})}{p^{12\delta}}$	0.111111111	0.0370370370	0.0123456790
$\dfrac{1}{3^{\mu+1}}$	0.111111111	0.0370370370	0.0123456790

Table 3.4: $\dfrac{\#\operatorname{Per}(z^3, \mathbb{F}_{p^n})}{p^n}$ with $v_3(n) = 1$.

of $\mathbb{F}_{p^n}$ will be periodic. Unlike the case of prime degree, however, we need not require $\Delta \mid n$ to have a nontrivial ratio of periodic points.

In order to define the appropriate towers of fields, we need a bit more notation. For each nonempty subset $I \subseteq \{1, 2, \ldots, r\}$, let

$$\delta_I = \operatorname{lcm}\{\delta_i\}_{i \in I}.$$

If $\delta_I = \delta_{I'}$, then $\delta_{I \cup I'} = \delta_I$ as well. Hence to a fixed value of δ we will associate the *maximal* subset $J \subseteq \{1, 2, \ldots, r\}$ such that $\delta_J \mid \delta$. Finally, given an integer n, we define an r-tuple of valuations

$$v(n) = \langle v_{q_i}(n) \rangle_{1 \leq i \leq r}.$$

We now have the tools to define limiting proportions of periodic points along appropriate towers of finite fields. Define

$$P_{\delta,\nu}(\phi) = \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(\phi, \mathbb{F}_{p^n})}{p^n}.$$

Proposition 3.4.6. *Let $\phi(z) = z^t$ where $t = q_1^{f_1} q_2^{f_2} \ldots q_r^{f_r}$, with q_i distinct odd primes for $1 \leq i \leq r$. Then for $J \subseteq \{1, 2, \ldots, r\}$ maximal with $\delta_J \mid \delta$,*

$$P_{\delta,\nu}(\phi) = \prod_{j \in J} \frac{1}{q_j^{\mu_j + \nu_j}}.$$

Remark. If no $\delta_i \mid \delta$, then the maximal set J is empty, and we recover the fact that all points in $\mathbb{F}_{p^n}$ are periodic in this case. This theorem also recovers our result in Theorem 3.4.5 when applied to the case $t = q$ for q an odd prime.

Proof. Since J is maximal such that $\delta_J \mid \gcd(\Delta, n)$, we have

$$p^n - 1 = d_n \prod_{j \in J} q_j^{e_j} \quad \text{with } \gcd(t, d_n) = 1.$$

Lemma 3.3.4 shows that $e_j = v_{q_j}(p^n - 1) = \mu_j + \nu_j$ for each $j \in J$.

The proof of Lemma 3.4.2 extends easily to this case, and we have

$$\operatorname{Per}(\phi, \mathbb{F}_{p^n}) = \{0\} \cup \{\alpha \in \mathbb{F}_{p^n} : \alpha^{d_n} = 1\}.$$

Hence

$$P_{\delta,\nu}(\phi) = \lim_{\substack{n\to\infty \\ \gcd(\Delta,n)=\delta \\ v(n)=\langle\nu_i\rangle}} \frac{\#\operatorname{Per}(\phi,\mathbb{F}_{p^n})}{p^n}.$$
$$= \lim_{\substack{d_n\to\infty \\ \gcd(t,d_n)=1}} \frac{d_n+1}{d_n\prod_{j\in J} q_j^{\mu_j+\nu_j}+1} = \prod_{j\in J}\frac{1}{q_j^{\mu_j+\nu_j}}.$$

□

In Tables 3.5–3.6 we use data from Sage [25] to illustrate Theorem 3.4.6 for the map $\phi(z) = z^{15}$ over fields $\mathbb{F}_{2^n}$. In the notation of the theorem, we have the following:

$$q_1 = 3 \qquad q_2 = 5 \qquad p = 2$$
$$\delta_1 = 2 \qquad \delta_2 = 4 \qquad \Delta = 4$$
$$\mu_1 = v_3(2^2-1) = 1 \qquad \mu_2 = v_5(2^4-1) = 1.$$

The table contains values of n with $\gcd(4,n) = \delta$.

δ	1	2	4
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^\delta})}{2^\delta}$	1.00000000	0.500000000	0.125000000
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^{7\delta}})}{2^{7\delta}}$	1.00000000	0.333374023	0.0666666701
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^{11\delta}})}{2^{11\delta}}$	1.00000000	0.333333492	0.0666666667
$\{q_j : j\in J\}$	$\emptyset$	$\{3\}$	$\{3,5\}$
$\prod_{j\in J}\frac{1}{q_j^{\mu_j}}$	1	0.333333333	0.0666666666

Table 3.5: $\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^n})}{2^n}$ with $\nu = (v_3(n), v_5(n)) = (0,0)$.

Remark. A statement similar to Proposition 3.4.6 holds when t is even, though the bookkeeping is somewhat messier. One must apply the results in Lemma 3.3.3, with the exponent for 2 depending on $\max\{v_2(p-1), v_2(p+1)\}$ and $v_2(n)$. We leave the details to the interested reader.

δ	1	2	4
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^{3\delta}})}{2^{3\delta}}$	1.00000000	0.125000000	0.0224609375
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^{21\delta}})}{2^{21\delta}}$	1.00000000	0.111111111	0.0222222222
$\frac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^{33\delta}})}{2^{33\delta}}$	1.00000000	0.111111111	0.0222222222
$\{q_j : j \in J\}$	$\emptyset$	$\{3\}$	$\{3,5\}$
$\prod_{j\in J} \frac{1}{q_j^{\mu_j+\nu_j}}$	1	0.111111111	0.0222222222

Table 3.6: $\dfrac{\#\operatorname{Per}(z^{15},\mathbb{F}_{2^n})}{2^n}$ with $\nu = (v_3(n), v_5(n)) = (1,0)$.

3.5 Chebyshev polynomials

Throughout this section, we consider $T_q(z)$, the Chebyshev polynomial of prime degree q. We take p to be any prime different from q. The proportions of interest in this case run over slightly different towers of finite fields than in the power map case.

Definition 3.5.1. We define the following proportions for integers $\nu \geq 0$. Recall that δ is the multiplicative order of p modulo q.

$$R_\nu(T_q) = \lim_{\substack{n\to\infty \\ \delta|2n \\ v_q(n)=\nu}} \frac{\#\operatorname{Per}\left(T_q,\mathbb{F}_{p^n}\right)}{p^n}.$$

We begin with an explicit classification of the periodic points of T_q in $\overline{\mathbb{F}_p}$. For any $\omega \in \overline{\mathbb{F}_p}$, we may solve a quadratic to find a nonzero $\zeta \in \overline{\mathbb{F}_p}$ such that $\omega = \zeta + \zeta^{-1}$.

Lemma 3.5.2. *Consider some nonzero $\zeta \in \overline{\mathbb{F}_p}$ and an integer $d \geq 0$. Then*

$$\zeta + \zeta^{-1} = \zeta^d + \zeta^{-d} \qquad \textit{if and only if} \qquad \zeta = \zeta^d \textit{ or } \zeta = \zeta^{-d}.$$

Proof.

$$\zeta + \zeta^{-1} = \zeta^d + \zeta^{-d}$$
$$\zeta^{2d} - \zeta^{d+1} - \zeta^{d-1} + 1 = 0$$
$$(\zeta^{d-1} - 1)(\zeta^{d+1} - 1) = 0.$$

Since $\zeta \neq 0$, the first factor vanishes if and only if $\zeta^d = \zeta$ and the second vanishes if and only if $\zeta^d = 1/\zeta$. □

Lemma 3.5.3. *Let $\omega \in \overline{\mathbb{F}_p}$. Then $\omega \in \mathrm{Per}(T_q, \overline{\mathbb{F}_p})$ if and only if $\omega = \zeta + \zeta^{-1}$ where $\zeta^d = 1$ for some d relatively prime to q.*

Proof. Suppose $\omega \in \overline{\mathbb{F}_p}$ is periodic for T_q, and choose ζ so that $\omega = \zeta + \zeta^{-1}$. Then

$$T_q^n(\omega) = \omega; \quad \text{that is,}$$
$$T_{q^n}(\zeta + \zeta^{-1}) = \zeta^{q^n} + \zeta^{-q^n} = \zeta + \zeta^{-1}.$$

So by Lemma 3.5.2, $\zeta^{q^n - 1} = 1$ or $\zeta^{q^n + 1} = 1$.

Conversely, suppose there is d prime to q such that $\zeta^d = 1$, and let φ be the Euler totient function as in Chapter 2. Since $d \mid \left(q^{\varphi(d)} - 1\right)$,

$$\zeta^{q^{\varphi(d)} - 1} = 1; \quad \text{that is,} \quad \zeta^{q^{\varphi(d)}} = \zeta.$$

Hence $\omega = \zeta + \zeta^{-1}$ is fixed by $T_q^{\varphi(d)}$. □

We see that counting the periodic points for $T_q(z)$ in $\mathbb{F}_{p^n}$ reduces to counting $\zeta \in \mathbb{F}_{p^n}$ such that $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ and $\zeta^d = 1$ for some d prime to q.

Lemma 3.5.4. *Let $\zeta \in \overline{\mathbb{F}_p}$. Then $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ if and only if $0 \neq \zeta \in \mathbb{F}_{p^n}$ or $\zeta^{p^n + 1} = 1$.*

Proof. We have $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$ if and only if it satisfies

$$\left(\zeta + \zeta^{-1}\right)^{p^n} = \zeta + \zeta^{-1}$$
$$\zeta^{p^n} + \zeta^{-p^n} = \zeta + \zeta^{-1}.$$

So by Lemma 3.5.2 either $\zeta = \zeta^{p^n}$ (i.e. $\zeta \in \mathbb{F}_{p^n}$) or $1/\zeta = \zeta^{p^n}$. □

Once again, the classification of periodic points explains our choice of limit in Definition 3.5.1.

Proposition 3.5.5. *If $\delta \nmid 2n$, then all points of $\mathbb{F}_{p^n}$ are periodic under T_q.*

Proof. Given that

$$q \nmid p^{2n} - 1, \quad \text{we conclude that} \quad q \nmid p^n + 1 \text{ and } q \nmid p^n - 1.$$

By Lemma 3.5.4, every $\omega \in \mathbb{F}_{p^n}$ can be written as $\zeta + \zeta^{-1}$ for some ζ with either $\zeta^{p^n-1} = 1$ or $\zeta^{p^n+1} = 1$. Since $p^n - 1$ and $p^n + 1$ are both prime to q, the result follows from Lemma 3.5.3. □

We now prove our main results for Chebyshev polynomials. As in the case of pure power maps, the statements are slightly different in the case $q = 2$ versus q odd.

Theorem 3.5.6. *Let $\mu = \max\{v_2(p-1), v_2(p+1)\}$. Then*

$$R_\nu(T_2) = \frac{2^{\mu+\nu-1}+1}{2^{\mu+\nu+1}}.$$

Proof. Assume $\omega \in \mathbb{F}_{p^n}$ is periodic for T_2. Then by Lemma 3.5.3, $\omega = \zeta + \zeta^{-1}$, where $\zeta^d = 1$ for some odd d. Since $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$, we apply Lemma 3.5.4 to conclude that $\zeta^{p^n+1} = 1$ or $\zeta^{p^n-1} = 1$.

First suppose $v_2(n) = 0$, so by Lemma 3.3.2 $v_2(p-1) = v_2(p^n-1)$. Then

$$\begin{array}{ll} p^n - 1 = 2^\mu d_1 & \\ p^n + 1 = 2d_2; & \end{array} \quad \text{or} \quad \begin{array}{ll} p^n - 1 = 2d_2 & \\ p^n + 1 = 2^\mu d_1, & \end{array} \tag{3.5.1}$$

where d_1 and d_2 are odd. Note that d_1 and d_2 are relatively prime since $d_1 \mid (p^n+1)$ and $d_2 \mid (p^n-1)$ or vice-versa, with both odd.

Similarly, if $v_2(n) = \nu \geq 1$, Lemma 3.3.3 shows that $v_2(p^n-1) = \mu + \nu$, so we have

$$p^n - 1 = 2^{\mu+\nu} d_1 \quad \text{and} \quad p^n + 1 = 2d_2;$$

where d_1 and d_2 are odd and relatively prime.

In either case, $\zeta + \zeta^{-1}$ is periodic if and only if $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. Each such pair (ζ, ζ^{-1}) — including the pair $(1, 1)$ — corresponds to a periodic point for T_2. Therefore, we have $(d_1 + d_2)/2$

periodic points for T_2 in $\mathbb{F}_{p^n}$.

Asymptotically, $p^n + 1 \sim p^n - 1$. That is,

$$2^{\mu+\nu} d_1 \sim 2d_2, \quad \text{so} \quad 2^{\mu+\nu-1} d_1 \sim d_2.$$

Hence

$$R_\nu(T_2) = \lim_{\substack{n\to\infty \\ v_2(n)=\nu}} \frac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{d\to\infty \\ d \text{ odd}}} \frac{(d + 2^{\mu+\nu-1}d)/2}{2^\mu d + 1} = \frac{2^{\mu+\nu-1}+1}{2^{\mu+\nu+1}}.$$

□

In Tables 3.7–3.8, we illustrate Theorem 3.5.6 using data from Sage [25].

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_p)}{p}$	0.333333333	0.285714286	0.294117647
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^3})}{p^3}$	0.370370370	0.311953353	0.281294525
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^5})}{p^5}$	0.374485597	0.312488844	0.281250154
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^7})}{p^7}$	0.374942844	0.312499772	0.281250001
$\dfrac{2^{\mu-1}+1}{2^{\mu+1}}$	0.375	0.3125	0.28125

Table 3.7: $\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})}{p^n}$ with n odd.

Theorem 3.5.7. *Let q be an odd prime. Let $v_q(p^\delta - 1) = \mu \geq 1$. Then*

$$R_\nu(T_q) = \frac{q^{\mu+\nu}+1}{2q^{\mu+\nu}}.$$

Proof. Assume $\omega \in \mathbb{F}_{p^n}$ is periodic for T_q. Then by Lemma 3.5.3, $\omega = \zeta + \zeta^{-1}$, where $\zeta^d = 1$ for some d prime to q. Since $\zeta + \zeta^{-1} \in \mathbb{F}_{p^n}$, we apply Lemma 3.5.4 to conclude that $\zeta^{p^n+1} = 1$ or $\zeta^{p^n-1} = 1$.

p	3	7	17
$\mu = \max\{v_2(p-1), v_2(p+1)\}$	2	3	4
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^2})}{p^2}$	0.333333333	0.285714286	0.266435986
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^6})}{p^6}$	0.312757202	0.281251859	0.265625010
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^{10}})}{p^{10}}$	0.312503175	0.281250001	0.265625000
$\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^{14}})}{p^{14}}$	0.312500039	0.281250000	0.265625000
$\dfrac{2^\mu + 1}{2^{\mu+2}}$	0.3125	0.28125	0.265625

Table 3.8: $\dfrac{\#\operatorname{Per}(T_2, \mathbb{F}_{p^n})}{p^n}$ with $v_2(n) = 1$.

Since $v_q(p^\delta - 1) = \mu \geq 1$ and $v_q(n) = \nu$, by Lemma 3.3.4 $v_q(p^{2n} - 1) = \mu + \nu \geq 1$. So

$$q \mid p^{2n} - 1, \quad \text{which means that} \quad q \mid p^n - 1 \text{ or } q \mid p^n + 1 \text{ but not both.}$$

Therefore

$$\begin{array}{ll} p^n - 1 = q^{\mu+\nu} d_1 & \\ p^n + 1 = d_2; & \end{array} \quad \text{or} \quad \begin{array}{ll} p^n - 1 = d_2 & \\ p^n + 1 = q^{\mu+\nu} d_1, & \end{array} \tag{3.5.2}$$

where $q \nmid d_1 d_2$.

Now, $\zeta + \zeta^{-1}$ is periodic if and only if $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. Each such pair (ζ, ζ^{-1}) — including the pairs $(1, 1)$ and $(-1, -1)$ if p odd — corresponds to a periodic point for T_q. So we have $(d_1 + d_2)/2$ periodic points for T_q in $\mathbb{F}_{p^n}$.

Again, $p^n + 1 \sim p^n - 1$ meaning

$$q^{\mu+\nu} d_1 \sim d_2.$$

Hence

$$R_\nu(T_q) = \lim_{\substack{n \to \infty \\ \delta \mid 2n \\ v_q(n) = \nu}} \frac{\#\operatorname{Per}(T_q, \mathbb{F}_{p^n})}{p^n} = \lim_{\substack{d \to \infty \\ q \nmid d}} \frac{(d + q^{\mu+\nu} d)/2}{q^{\mu+\nu} d + 1} = \frac{q^{\mu+\nu} + 1}{2q^{\mu+\nu}}.$$

□

Remark. Theorem 3.5.6 says that the proportion of periodic points in the appropriate towers for

T_2 is something slightly more than $1/4$, where the difference depends on the tower. Similarly, Theorem 3.5.7 says that for q an odd prime, the proportion is slightly greater than $1/2$. We can understand these results a bit more intuitively in the following way.

Consider roots of the polynomials $z^{p^n+1}-1$ and $z^{p^n-1}-1$ over the field $\overline{\mathbb{F}_p}$. Equation (3.5.2) shows that for one of the two equations, all roots ζ yield a periodic point $\zeta+\zeta^{-1}$ for T_q. So we are guaranteed something close to $p^n/2$ periodic points from roots of one of the polynomials, and we pick up a few more from roots of the other polynomial. A similar explanation for T_2 can be derived from equation (3.5.1).

In Table 3.9, we illustrate Theorem 3.5.7 for $T_3(z)$ over various finite fields. Note that for the choices of primes in the table, $\delta \mid 2n$ for all integers n.

p	5	19	53
δ	2	1	2
$\mu = v_3(p^\delta - 1)$	1	2	3
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_p)}{p}$	0.600000000	0.578947368	0.509433962
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_{p^2})}{p^2}$	0.680000000	0.556786704	0.518689925
$\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_{p^4})}{p^4}$	0.667200000	0.555558966	0.518518579
$\dfrac{3^\mu+1}{2\cdot 3^\mu}$	0.666666667	0.555555556	0.518518519

Table 3.9: $\dfrac{\#\operatorname{Per}(T_3, \mathbb{F}_{p^n})}{p^n}$ with $v_3(n) = 0$.

Once again, we wish to extend our results to polynomials with composite degree. Lemma 3.3.5 takes care of prime power degree, so we are left to consider the case of the t^{th} Chebyshev polynomial, $T_t(z)$, for $t = q_1^{f_1} q_2^{f_2} \cdots q_r^{f_r}$ and $r \geq 2$. We continue with the notation introduced at the end of Section 3.4: for each $1 \leq i \leq r$, let

$$\delta_i \text{ is the multiplicative order of } p_i \text{ modulo } q_i \qquad \text{and} \quad \mu_i = v_{q_i}(p^{\delta_i} - 1).$$

We also define

$$\Delta = \operatorname{lcm}\{\delta_i\}_{1 \leq i \leq r}.$$

The argument in Proposition 3.5.5 can be modified to show that if $\gcd(\Delta, 2n) = 1$, then all points of $\mathbb{F}_{p^n}$ will be periodic. But as in Section 3.4, we need not require $\Delta \mid 2n$ to have a nontrivial ratio of periodic points.

As before, for each $n \in \mathbb{Z}$ we define an r-tuple of valuations

$$v(n) = \langle v_{q_i}(n) \rangle_{1 \le i \le r}.$$

We then define the ratios of interest:

$$R_{\delta,\nu}(T_t) = \lim_{\substack{n \to \infty \\ \gcd(\Delta,n)=\delta \\ v(n)=\langle \nu_i \rangle}} \frac{\#\operatorname{Per}(T_t, \mathbb{F}_{p^n})}{p^n}.$$

Theorem 3.5.8. *Let $t = q_1^{f_1} q_2^{f_2} \dots q_r^{f_r}$, with q_i distinct odd primes for $1 \le i \le r$. Then there are disjoint subsets $I, J \subseteq \{1, 2, \dots, r\}$ such that*

$$R_{\delta,\nu}(T_t) = \frac{Q_I + Q_J}{2 Q_I Q_J},$$

where

$$Q_I = \prod_{i \in I} q_i^{\mu_i + \nu_i} \quad \text{and} \quad Q_J = \prod_{j \in J} q_j^{\mu_j + \nu_j}.$$

Proof. Take J maximal with $\delta_J \mid \delta$; then we know that $q_j \mid p^\delta - 1$ if and only if $j \in J$. Now define

$$I = \left\{ 1 \le i \le r \colon q_i \mid p^\delta + 1 \right\}.$$

Since the primes dividing t are distinct odd primes, no q_i divides both $p^\delta - 1$ and $p^\delta + 1$. Hence $I \cap J = \emptyset$.

Now consider any n with $\gcd(\Delta, n) = \delta$. Clearly $q_j \mid p^n - 1$ if and only if $j \in J$. For any $i \in I$, we have

$$q_i \mid p^\delta + 1 \quad \Longrightarrow \quad q_i \mid p^{2\delta} - 1 \quad \Longrightarrow \quad q_i \mid p^{2n} - 1.$$

Since $i \notin J$, $q_i \nmid p^n - 1$. Therefore $q_i \mid p^n + 1$. Furthermore, since $\gcd(\Delta, 2n) \mid 2\delta$, we have

$$q_i \mid p^{2n} - 1 \quad \Longleftrightarrow \quad q_i \mid p^{2\delta} - 1 \quad \Longleftrightarrow \quad i \in I \cup J.$$

That is, $q_i \mid p^n + 1$ if and only if $i \in I$.

Therefore

$$p^n - 1 = d_1 \prod_{j \in J} q_j^{e_j} \qquad\qquad p^n + 1 = d_2 \prod_{i \in I} q_i^{e_i},$$

with $\gcd(t, d_1) = \gcd(t, d_2) = 1$. Lemma 3.3.4, applied to n and $2n$ respectively, shows that $e_j = \mu_j + \nu_j$ for $j \in J$ and $e_i = \mu_i + \nu_i$ for $i \in I$.

Lemma 3.5.3 extends easily to the case of composite degree, and we conclude that $\omega \in \mathbb{F}_{p^n}$ is periodic for T_t if and only if $\omega = \zeta + \zeta^{-1}$ with $\zeta^{d_1} = 1$ or $\zeta^{d_2} = 1$. As before, we have $(d_1 + d_2)/2$ periodic points for T_t in $\mathbb{F}_{p^n}$.

Since $p^n + 1 \sim p^n - 1$, we have

$$d_1 \prod_{j \in J} q_j^{\mu_j + \nu_j} \sim d_2 \prod_{i \in I} q_i^{\mu_i + \nu_i}, \quad \text{meaning} \quad d_2 \sim d_1 \frac{Q_J}{Q_I}.$$

We can now calculate the limit:

$$\begin{aligned} R_{\delta,\nu}(T_t) &= \lim_{\substack{n \to \infty \\ \gcd(\Delta, n) = \delta \\ v(n) = \langle \nu_i \rangle}} \frac{\#\operatorname{Per}(T_t, \mathbb{F}_{p^n})}{p^n} \\ &= \lim_{\substack{d \to \infty \\ \gcd(t,d) = 1}} \frac{\left(d + d\frac{Q_J}{Q_I}\right)/2}{Q_J d + 1} = \frac{Q_I + Q_J}{2 Q_I Q_J}. \end{aligned}$$

□

In Table 3.10 we use data from Sage [25] to illustrate Theorem 3.5.8 for the 15^{th} Chebyshev polynomial over fields $\mathbb{F}_{2^n}$. In the notation of the theorem, we have:

$$\begin{array}{lll} q_1 = 3 & q_2 = 5 & p = 2 \\ \delta_1 = 2 & \delta_2 = 4 & \Delta = 4 \\ \mu_1 = v_3(2^2 - 1) = 1 & \mu_2 = v_5(2^4 - 1) = 1. & \end{array}$$

Note that in the table, we restrict to values of n with $\gcd(4, n) = \delta$.

δ	1	2	4
$2^\delta - 1$	1	3	$3 \cdot 5$
$2^\delta + 1$	3	5	17
$\frac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^\delta})}{2^\delta}$	0.500000000	0.266662598	0.562500000
$\frac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^{7\delta}})}{2^{7\delta}}$	0.656250000	0.266666651	0.506667137
$\frac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^{11\delta}})}{2^{11\delta}}$	0.664062500	0.266666667	0.533333335
$\{q_i : i \in I\}$	$\{3\}$	$\{5\}$	$\emptyset$
$\{q_j : j \in J\}$	$\emptyset$	$\{3\}$	$\{3, 5\}$
$\frac{Q_I + Q_J}{2Q_I Q_J}$	0.666666667	0.266666667	0.533333333

Table 3.10: $\frac{\#\operatorname{Per}(T_{15}, \mathbb{F}_{2^n})}{2^n}$ with $\nu = (v_3(n), v_5(n)) = (0, 0)$.

CHAPTER 4
RATIONAL MAPS WITH K-RATIONAL CRITICAL POINTS

4.1 Background

Let K be a field and L/K an extension. By an L-rational function we mean $\phi \in L(z)$ with $\deg(\phi) = d \geq 2$. We define an equivalence relation:

Definition 4.1.1. Two rational functions ϕ_1 and ϕ_2 will be called *equivalent* if $\phi_1 = f \circ \phi_2$ where $f \in \mathrm{PGL}_2$.

(Note, this is not the standard conjugacy based equivalence $\phi^f = f^{-1} \circ \phi \circ f$ used in Chapter 2.)

Definition 4.1.2. A rational map $\phi \in L(z)$ is called *K-critical* if $\mathrm{Crit}(\phi) \subset \mathbb{P}^1(K)$.

Definition 4.1.3. We say that the field K is *critically reducible at d* if all K-critical degree d maps $\phi \in L(z)$ are equivalent to a K-rational function.

In [1], Gabrielov and Eremenko prove

Theorem 4.1.4. *The real numbers are critically reducible at d for every degree $d \geq 2$.*

A natural question is:

Question. Which fields K are critically reducible at d for every degree d?

We establish that all fields of characteristic 0 are critically reducible at2 and there exist fields that will not be critically reducible at 3. Our results are summarized here:

Theorem 4.1.5. (Theorem 4.3.3, Theorem 4.6.2, and Theorem 4.7.7)

(i) If the characteristic of K is 0, then K is critically reducible at 2.

(ii) If K is a number field, then K is not critically reducible at 3.

(iii) If $p \neq 3$, then $\mathbb{Q}_p$ is not critically reducible at 3.

We conclude with an outline of the chapter and a survey of the techniques used.

Section 4.2 We prove useful lemmas regarding to critical points and critical values.

Section 4.3 We prove the first of our main results: All fields K of characteristic 0 are critically reducible at 2. This follows from a more general result that all K-critical maps with a totally ramified critical point are equivalent to a K-rational map.

Section 4.4 We provide a useful normal form for degree 3 maps with 4 distinct critical points.

Section 4.5 We give a testable algebraic condition that is equivalent to afield K being critically reducible at 3.

Sections 4.6 and 4.7 We use the algebraic condition to prove our main results for number fields K and $\mathbb{Q}_p$ respectively.

4.2 Preliminaries

The following lemmas show that equivalent rational functions have the same critical sets.

Lemma 4.2.1. *Let $f, g \in \mathrm{PGL}_2$. If the diagram below commutes then $\gamma \in \mathrm{Crit}(\phi_1)$ if and only if $f(\gamma) \in \mathrm{Crit}(\phi_2)$.*

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\phi_1} & \mathbb{P}^1 \\ f\downarrow & & \downarrow g \\ \mathbb{P}^1 & \xrightarrow{\phi_2} & \mathbb{P}^1 \end{array}$$

Proof. By Proposition 1.2.7 if $\phi_1 : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ and $g : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ are nonconstant rational maps, then for all $\gamma \in \mathbb{P}^1(K)$,

$$e_{g\circ\phi_1}(\gamma) = e_{\phi_1}(\gamma) e_g(\phi_1(\gamma)).$$

A map $g \in \mathrm{PGL}_2$ has ramification index 1 for all $\alpha \in \mathbb{P}^1(K)$. So by commutativity of the diagram,

$$\begin{aligned} e_{\phi_2}(f(\gamma)) &= e_{\phi_2}(f(\gamma))e_f(\gamma) = e_{\phi_2 \circ f}(\gamma) \\ &= e_{g\circ\phi_1}(\gamma) = e_{\phi_1}(\gamma)e_g(\phi_1(\gamma)) \\ &= e_{\phi_1}(\gamma). \end{aligned}$$

□

Lemma 4.2.2. *If ϕ_1 and ϕ_2 are equivalent then* $\mathrm{Crit}(\phi_1) = \mathrm{Crit}(\phi_2)$.

Proof. In Lemma 4.2.1, let f be the identity map id. The statement follows. □

Throughout, we will be considering fields L over K, where K has characteristic 0, and K-critical functions $\phi \in L(z)$. We ask whether there is a function equivalent to ϕ with coefficients in K. The next Lemma shows that rather than working with ϕ directly, we may work with a function $\phi \circ f$ with $f \in \mathrm{PGL}_2(K)$. We will make frequent use of this fact.

Lemma 4.2.3. *Let L/K be an extension of fields with $\phi \in L(z)$. If there exists an $f \in \mathrm{PGL}_2(K)$ such that $\phi \circ f$ is equivalent to a function with K coefficients, then ϕ is also equivalent to a function with K coefficients.*

Proof. If $g \circ \phi \circ f = \psi \in K(z)$ and $f \in \mathrm{PGL}_2(K)$ then $g \circ \phi = \psi \circ f^{-1} \in K(z)$. □

Around a point, ϕ is d-to-1 counting multiplicity. Critical points map forward with multiplicity greater than 1. In Section 4.4, we focus on cubic maps with four distinct critical points. The following lemma shows that such maps have at least 3 distinct critical values.

Lemma 4.2.4. *Let ϕ be a rational function of degree $d > 2$ with $2d-2$ distinct critical points. Then ϕ has at least three distinct critical values.*

Proof. For any $\alpha \in \mathbb{P}^1$, $\displaystyle\sum_{\beta \in \phi^{-1}(\alpha)} e_\phi(\beta) = d$ by Corollary 1.2.6. If ϕ has only one critical value α_1, then the $2d-2$ critical points all get sent to α_1 with multiplicity 2. So $\displaystyle\sum_{\beta \in \phi^{-1}(\alpha_1)} e_\phi(\beta) = 4d-4 > d$. Hence, the rational map ϕ must have more than one critical value.

Suppose now ϕ has exactly 2 distinct critical values α_1 and α_2. First, suppose each α_i has $d-1$ critical points in its preimage. The ramification index of each critical point is 2, so $\displaystyle\sum_{\beta \in \phi^{-1}(\alpha_i)} e_\phi(\beta) = 2d-2 > d$ when $d > 2$. So we have at least three distinct critical values.

If critical value α_1 has fewer than $d-1$ critical points in its preimage, then the critical value α_2 must have more than $d-1$ critical points in its preimage. Hence $\sum_{\beta \in \phi^{-1}(\alpha_2)} e_\phi(\beta) > 2d-2 > d$ for $d > 2$. Again, we must have at least three critical values. □

Lemma 4.2.5. *For degree 2 rational maps or degree $d > 2$ rational maps with exactly two distinct critical points, there are at least two distinct critical values.*

Proof. A counting argument similar to the proof of Lemma 4.2.4 leads to this conclusion. □

4.3 Rational Map with a Totally Ramified Critical Point

Let K be a field of characteristic 0 and let L be an extension of K. Recall that a critical point $\alpha \in \mathbb{P}^1$ is *totally ramified* if $e_\phi(\alpha) = \deg(\phi)$.

Theorem 4.3.1. *Let $\phi \in L(z)$ be a K-critical degree d rational map with a totally ramified critical point. Then ϕ is equivalent to a K-rational map.*

Proof. Suppose ϕ has a totally ramified point at a finite point γ_1. We can move γ_1 to infinity via a linear transformation f on the source and consider $\phi \circ f$. By Lemma 4.2.3 if $\phi \circ f$ is equivalent to a K-rational function we conclude that ϕ is also equivalent to a K-rational function.

We can find $g \in \mathrm{PGL}_2$ such that ∞ is a fixed point for $g \circ \phi \circ f$. By Propostion 1.2.7, ∞ is still totally ramified. If $g \circ \phi \circ f$ is equivalent to a K-rational function we conclude that ϕ is also.

Suppose ∞ is a totally ramified fixed point of ϕ. Then ϕ is a polynomial and

$$\phi'(z) = b(z-c_1)(z-c_2)...(z-c_{d-1})$$

with $b \in L$ and $c_i \in K$ (not necessarily distinct), since the critical points are all in K. Expanding the function ϕ' we get

$$\phi'(z) = b(z^{d-1} + a_{d-2}z^{d-2} + ... + a_1 z + a_0)$$

where $a_i \in K$.

We can integrate this function with respect to z to get

$$b\left(\frac{z^d}{d} + a_{d-2}\frac{z^{d-1}}{d-1} + ... + a_1\frac{z}{2} + a_0 z\right) + c,$$

where $c \in L$.

Define $s \in \mathrm{PGL}_2$ by $s(z) = \frac{z-c}{b}$, then we see that

$$\begin{aligned} s \circ \phi &= \frac{(b\left(\frac{z^d}{d} + a_{d-2}\frac{z^{d-1}}{d-1} + ... + a_1\frac{z}{2} + a_0 z\right) + c) - c}{b} \\ &= \frac{(b\left(\frac{z^d}{d} + a_{d-2}\frac{z^{d-1}}{d-1} + ... + a_1\frac{z}{2} + a_0 z\right)}{b} \\ &= \left(\frac{z^d}{d} + a_{d-2}\frac{z^{d-1}}{d-1} + ... + a_1\frac{z}{2} + a_0 z\right) \in K(z). \end{aligned}$$

So ϕ is equivalent to a K-rational map. □

Remark. In fact, Theorem 4.3.1 holds for all K with characteristic $p \neq 2$.

Corollary 4.3.2. *Let $\phi \in L(z)$ be a degree $d \geq 2$ rational map with exactly two distinct critical points. If ϕ is K-critical, then ϕ is equivalent to a K-rational function.*

Proof. By Riemann-Hurwitz Theorem 1.2.5, both critical points are ramified. Hence, Theorem 4.3.1 applies to this case. □

Corollary 4.3.3. *A K-critical quadratic map is always equivalent to a K-rational map. Hence K is critically reducible at 2.*

Proof. By Riemann-Hurwitz Theorem 1.2.5, both critical points are ramified. Hence, Theorem 4.3.1 applies to this case. □

4.4 Degree 3 Rational Maps

In Section 4.3, we showed that every characteristic 0 field is critically reducible at 2. We now turn to the question of which fields are critically reducible at 3. By Riemann-Hurwitz Theorem 1.2.5, a cubic function has either $2 \cdot 3 - 2 = 4$ critical points, counting multiplicity.

Since K has characteristic 0, we know a cubic function can not have one critical point by [2]. If the map ϕ has exactly 2 or 3 critical points, then at least one critical point is totally ramified by 1.2.5. So by Theorem 4.3.1, if ϕ is K-critical then ϕ is equivalent to a K-rational map. We consider the next logical case: degree 3 maps with exactly 4 critical points, each of which necessarily has ramification index 2.

In this section, we develop a normal form for cubic functions with four distinct critical points. In the sequel, we will use this normal form to show that number fields and $\mathbb{Q}_p$ fail to be critically reducible at 3, for $p \neq 3$.

Suppose ϕ is a degree $d \geq 3$ rational map with at least 3 distinct critical points. The following lemma shows that we can use a K-rational change of coordinates on the source to move these points to $0, 1$, and ∞. Lemma 4.2.3 then allows us to study only this case.

Lemma 4.4.1. *Let K be a field and L/K be a (not necessarily finite) extension. If $\phi \in L(z)$ has at least three distinct critical points and ϕ is K-critical, then there exists $f \in \mathrm{PGL}_2(K)$ and $g \in \mathrm{PGL}_2(L)$ such that $\psi := g \circ \phi \circ f$ satisifies*

(i) $\{0, 1, \infty\} \subset \mathrm{Crit}(\psi)$, *and*

(ii) ψ *fixes* 0, 1, *and* ∞.

Proof. By Lemma 4.2.4 we may choose critical points γ_1, γ_2, and γ_3 that map to distinct critical values.

Suppose no γ_i is ∞ for $i = 1, 2, 3$. Let $f(z) = \frac{(z-\gamma_1)(\gamma_3-\gamma_2)}{(z-\gamma_2)(\gamma_3-\gamma_1)}$. This map will move γ_1 to 0, γ_2 to ∞, and γ_3 to 1.

If $\gamma_2 = \infty$ we may take $f(z) = \frac{z-\gamma_1}{\gamma_3-\gamma_1}$.

Choosing f in this way, we have $\{0, 1, \infty\} \subset \mathrm{Crit}(\phi \circ f)$ still with distinct critical values. Suppose $\phi(0) = \alpha_1$, $\phi(\infty) = \alpha_2$, and $\phi(1) = \alpha_3$. If α_i is finite for all $i = 1, 2, 3$, then take $g(z) = \frac{(z-\alpha_1)(\alpha_3-\alpha_2)}{(z-\alpha_2)(\alpha_3-\alpha_1)}$.

Now assume that only two of the critical values are finite. Renumber if necessary so that $\alpha_1 = \infty$. Then set $g(z) = \frac{(\alpha_3-\alpha_2)}{(z-\alpha_2)}$.

A computation and an application of Lemma 4.2.1 shows that $\psi(z) = g \circ \phi \circ f$ will have critical fixed points 0, 1, and ∞. □

Proposition 4.4.2. *Let K be a field and $\phi \in L(z)$ have degree* 3. *Suppose* $\mathrm{Crit}(\phi) = \{0, 1, \infty, c\}$ *(so ϕ has four distinct critical points), and that ϕ fixes* 0, 1, *and* ∞. *Then ϕ has the form*

$$\phi_a = \frac{z^2(z+a)}{(2a+3)z - (a+2)}.$$

with $a \notin \{-1, -2, -3/2\}$.

Proof. Because ϕ is a cubic function with 4 distinct critical points, each critical point has ramification index 2. Since 0 and ∞ are fixed with ramification 2

$$\phi(z) = \frac{z^2(a_0 z + a_2)}{b_0 z + b_1}.$$

Furthermore, 1 is fixed we have that $a_0 + a_1 = b_0 + b_1$. Take the derivative and simplify to get

$$\phi'(z) = \frac{z((b_0 z + b_1)(3a_0 z + 2a_1) - b_0 z(a_0 z + a_1 z))}{(b_0 z + b_1)^2}.$$

Also, 1 is a critical point we know $b_0 + b_1 \neq 0$, so we can use the fact that $a_0 + a_1 = b_0 + b_1$ and divide $b_0 + b_1$ out of the function. So we have

$$\phi'(1) = \frac{3a_0 + 2a_1 - b_0}{b_0 + b_1}.$$

Hence

$$3a_0 + 2a_1 = b_0$$
$$-(2a_0 + a_1) = b_1.$$

Now

$$\phi(z) = \frac{z^2(a_0 z + a_1)}{(3a_0 + 2a_1)z - (2a_0 + a_1)}.$$

If a_0 were 0, then the function would no longer be cubic, so we can divide by a_0 and set $a = \frac{a_1}{a_0}$. Now we have a one parameter family

$$\phi_a(z) = \frac{z^2(z + a)}{(2a + 3)z - (a + 2)}.$$

The map ϕ_a has critical fixed points 0, 1, and ∞ with remaining critical point

$$c = -a\frac{a + 2}{2a + 3}.$$

If $a \in \{-1, -2, -3/2\}$, then ϕ would not have four distinct critical points. □

Lemma 4.4.3. *Two maps in this family ϕ_a and ϕ_b are equivalent if and only if $a = b$.*

Proof. Suppose that there is $f \in \mathrm{PGL}_2$ such that $f \circ \phi_a = \phi_b$. We know ϕ_b fixes $0, 1$, and ∞, so $f \circ \phi_a$ fixes $0, 1$, and ∞. Since ϕ_a already fixes $0, 1$, and ∞, f must as well. This means that f must be the identity and $a = b$. □

Proposition 4.4.4. *Let L/K be a field extension, and suppose that $\phi_a \in L(z)$. Then ϕ_a is equivalent to a rational function in $K(z)$ if and only if $a \in K$.*

Proof. One implication is obvious.

Now suppose ϕ is a K-rational map and ϕ_a is equivalent to ϕ. By Lemma 4.2.2, ϕ_a and ϕ have the same critical points 0, 1, ∞, and c. Let us choose

$$f(z) = \frac{(z - \alpha_1)(\alpha_2 - \alpha_3)}{(z - \alpha_2)(\alpha_3 - \alpha_1)}$$

where $\phi(0) = \alpha_1$, $\phi(\infty) = \alpha_2$, and $\phi(1) = \alpha_3$, $\alpha_i \in K$, thus $f \in \mathrm{PGL}_2(K)$. By a simple counting argument similar to Lemma 4.2.4, we know that $\alpha_i \neq \alpha_j$ when $i \neq j$. Thus $f \circ \phi \in K(z)$ and it fixes the critical points 0, 1, and ∞. By Lemma 4.4.2, it is of the form ϕ_b for some $b \in K$. By Lemma 4.4.3, $a = b$. So $a \in K$ as desired. □

4.5 Algebraic Condition

Define $c(z) = -z\frac{z+2}{2z+3}$. Then c is a quadratic rational function, and $c(a)$ is the fourth critical point of ϕ_a from Proposition 4.4.2. Our question 4.1 may be rephrased as follows:

Question. Let L/K be a field extension, and let $\phi_a \in L(z)$. If $c(a) \in K$, may we conclude that $a \in K$?

Given a degree 3 K-critical map $\phi \in L(z)$ with distinct critical points, by Lemma 4.4.1 we may consider the map $g \circ \phi \circ f$, which has critical fixed points 0, 1, and ∞. By Lemma 4.4.2, $g \circ \phi \circ f = \phi_a$ for some $a \in L$. If $a \in K$, then the map $\phi_a \circ f^{-1} \in K(z)$ is equivalent to ϕ. If we can do this for every such ϕ then K is critically reducible at 3.

Definition 4.5.1. Write $\mathbb{F}$ for the field $\mathbb{Q}$ or the field $\mathbb{F}_p$ for a prime p. Let $f \in \mathbb{F}(z)$ be a nonconstant rational function. We say that a field extension $K/\mathbb{F}$ is *f-perfect* if the map $f : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is surjective.

Example 4.5.2. Let $c(z) = -z\frac{z+2}{2z+3}$. Then the field of real numbers is c-perfect. Indeed, $c(-2/3) = \infty$, and if $c_0 \in \mathbb{R}$, then the equation $c(z) = c_0$ is equivalent to a quadratic equation with discriminant

$$4(c_0^2 - c_0 + 1) = (2c_0 - 1)^2 + 3 > 0.$$

Hence there exists a real solution to the equation $c(z) = c_0$. This recovers Theorem 4.1.4 for degree 3 rational maps.

Theorem 4.5.3. *The following are equivalent:*

(i) K is c-perfect, where $c(z) = -z\frac{z+2}{2z+3}$; and

(ii) Any K-critical cubic function $\phi \in \overline{K}(z)$ is equivalent to a function in $K(z)$.

Proof. First recall that if $\phi \in \overline{K}(z)$ is K-critical with a totally ramified critical point, then by Theorem 4.3.1 it is equivalent to a rational function with coefficients in K. So statement (2) may be replaced with

(3) Any K-critical cubic rational function $\phi \in \overline{K}(z)$ with four distinct critical points is equivalent to a function in $K(z)$.

(1) $\Rightarrow$ (3) Suppose that $\phi \in \overline{K}(z)$ has four distinct K-rational critical points. By Lemma 4.4.1, we may make a K-rational change of coordinates on the source so that three of the critical points are 0, 1, and ∞ and a $\overline{K}$-rational change of coordinates on the target so that these three points are fixed. That is, we may assume $\phi = \phi_a$ for some $a \in \overline{K}$. That hypothesis that ϕ_a has four K-rational critical points means the remaining critical point $c_0 = c(a) \in K$. Applying the c-perfect hypothesis on K, we find that there exists $a' \in K$ such that $c(a') = c_0$. But c is quadratic, so this means $a \in K$ as well. That is, $\phi_a \in K(z)$ and (3) is proved.

(3) $\Rightarrow$ (1) Take $c_0 \in K$. We must show there is an $a \in K$ such that $c(a) = c_0$. If $c_0 = 0, 1$, or ∞ then we can take $a = 0, 1$, or $-3/2$, respectively. So let us assume that $c_0 \notin \{0, 1, \infty\}$. Choose $a \in \overline{K}$ such that $c(a) = c_0$. Then the rational function ϕ_a has four distinct K-rational critical points $\{0, 1, \infty, c_0\}$, and our hypothesis implies that ϕ_a is equivalent to a rational function in $K(z)$. But now Proposition 4.4.4 shows that $a \in K$. Since c_0 was arbitrary, we conclude that K is c-perfect as desired. □

Remark. The above proof also goes through for fields of characteristic not equal to 2.

4.6 Number Fields

In this section, we show that a number field K is not critically reducible at 3.

Theorem 4.6.1. *Let K be a number field. Then K is not f-perfect for any rational function f of degree $d > 1$.*

Proof. We want to show that there exists an $\alpha \in \mathbb{P}^1(K)$ such that for all $z \in \mathbb{P}^1(K)$ $f(z) \neq \alpha$.

Choose $y \in \mathbb{P}^1(K)$, not in an exceptional set, so that $\bigcup_{n\geq 0} f^{-n}(y)$ is infinite [23]. Define $B := \hat{h}(y)$. By properties of the canonical height function for all $x \in \mathbb{P}^1(\overline{K})$ such that $f^n(x) = y$,

$$\hat{h}(x) = \frac{1}{d^n}\hat{h}(y) = \frac{1}{d^n}B.$$

So $\bigcup_{n\geq 0} f^{-n}(y)$ is a set of bounded height (that is all elements have height $\leq B$). Therefore, $\bigcup_{n\geq 0}(f^{-n}(y)) \cap \mathbb{P}^1(K)$ is finite. This implies there exists an $N \in \mathbb{N}$ such that for all $n \geq N$

$$f^{-n}(y) \cap \mathbb{P}^1(K) = \emptyset.$$

Let m be maximal such that $f^{-m}(y) \cap \mathbb{P}^1(K) \neq \emptyset$. Choose $\alpha \in f^{-m}(y) \cap \mathbb{P}^1(K)$ then for all $z \in \mathbb{P}^1(K)$, we have $f(z) \neq \alpha$. □

Corollary 4.6.2. *Let K be a number field. There exist K-critical cubic functions $\phi \in \overline{K}(z)$ such that ϕ is not equivalent to a K-rational function. Hence K is not critically reducible at 3.*

Proof. By Theorem 4.6.1, for K a number field it is not f-perfect for any rational function f with degree $d > 1$. So K is not c-perfect for $c(z) = -z\frac{z+2}{2z+3}$. By Theorem 4.5.3, there exists a K-critical degree 3 rational function that fails to be equivalent to a K-rational function. □

Example 4.6.3. Let $\phi(z) = \frac{z^2(z-3+\sqrt{3})}{(-3+2\sqrt{3})z+1-\sqrt{3}} \in \mathbb{Q}[\sqrt{3}](z)$. This function has $\mathrm{Crit}(\phi) = \{0, 1, \infty, 2\} \subset \mathbb{P}^1(\mathbb{Q})$. But there does not exist a $g \in \mathrm{PGL}_2$ such that $g \circ \phi \in \mathbb{Q}(z)$.

Suppose there did exist such a $g = \frac{\alpha z+\beta}{\gamma z+\delta}$. Then

$$\begin{aligned} g \circ \phi &= \frac{\alpha(z^2(z-3+\sqrt{3})) + \beta((-3+2\sqrt{3})z+1-\sqrt{3})}{\gamma(z^2(z-3+\sqrt{3})) + \delta((-3+2\sqrt{3})z+1-\sqrt{3})} \\ &= \frac{\alpha z^3 + \alpha(-3+\sqrt{3})z^2 + \beta(-3+\sqrt{3})z + \beta(1-\sqrt{3})}{\gamma z^3 + \gamma(-3+\sqrt{3})z^2 + \delta(-3+\sqrt{3})z + \delta(1-\sqrt{3})}. \end{aligned}$$

We can list the coefficients as an 8-tuple in projective 7 space and we get

$$[\alpha : \alpha(-3+\sqrt{3}) : \beta(-3+\sqrt{3}) : \beta(1-\sqrt{3}) : \gamma : \gamma(-3+\sqrt{3}) : \delta(-3+\sqrt{3}) : \delta(1-\sqrt{3})] \in \mathbb{P}^7(\mathbb{Q}[\sqrt{3}, \alpha, \beta, \gamma, \delta]).$$

This can not be an element in $\mathbb{P}^7(\mathbb{Q})$.

4.7 $\mathbb{Q}_p$ case

In this section, we show that for primes $p \neq 3$, $\mathbb{Q}_p$ is not critically reducible at 3. But $\mathbb{Q}_3$ is critically reducible at 3.

Let $c(z) = -z\frac{z+2}{2z+3}$ as before.

Lemma 4.7.1. *The function $c(z)$ has good reduction for $p \neq 3$.*

Proof. By Theorem 1.3.3, a function has good reduction for prime p if and only if $\widetilde{\mathrm{Res}(\phi)} \neq 0$, where $\widetilde{\mathrm{Res}(\phi)}$ is the reduction mod p. Consider

$$\mathrm{Res}(c(z)) = \det \begin{vmatrix} -1 & -2 & 0 \\ 2 & 3 & 0 \\ 0 & 2 & 3 \end{vmatrix} = 3 \det \begin{vmatrix} -1 & -2 \\ 2 & 3 \end{vmatrix} = 3.$$

So $c(z)$ has good reduction everywhere except when $p|3$. So $p \neq 3$. □

Lemma 4.7.2. *Let $p \neq 2$. If $\alpha \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, then $c(\alpha) \in \mathbb{Q}_p \setminus \mathbb{Z}_p$.*

Proof. Consider

$$|c(\alpha)|_p = \left| \frac{-\alpha^2 - 2\alpha}{2\alpha + 3} \right|_p = \frac{\left|-\alpha^2 - 2\alpha\right|_p}{|2\alpha + 3|_p}.$$

Since $|\alpha|_p > 1$ and $p \neq 2$ we know that $|\alpha|_p^2 > |2\alpha|_p > 1$. So by Lemma 1.4.3, $|-\alpha^2 - 2\alpha|_p = |\alpha|_p^2$. Similarly, $|2\alpha + 3|_p = |\alpha|_p$. Thus we have

$$|c(\alpha)|_p = \frac{|\alpha|_p^2}{|\alpha|_p} = |\alpha|_p > 1.$$

Hence $c(\alpha) \in \mathbb{Q}_p \setminus \mathbb{Z}_p$ as desired. □

Theorem 4.7.3. *$\mathbb{Q}_p$ is not c-perfect for any prime $p > 3$.*

Proof. We want to show there exists a $\beta \in \mathbb{P}^1(\mathbb{Q}_p)$ such that for all $z \in \mathbb{P}^1(\mathbb{Q}_p)$, $c(z) \neq \beta$. Let $\beta \in \{0, 1, 2, 3, ..., p-1\} \subseteq \mathbb{Z}_p$. Suppose there exists a root $\alpha \in \mathbb{Q}_p$ such that $c(\alpha) = \beta$. Then,

$$\widetilde{c}(\widetilde{\alpha}) = \widetilde{\beta}$$

for all primes $p \neq 3$ since c has good reduction by Lemma 4.7.1. By our choice of β we can conflate them; hence $\beta = \widetilde{\beta}$.

On $\mathbb{F}_p$, in order to be surjective the map must be injective. But this map can not be injective for $p \neq 2$ since $0 \mapsto 0$ and $p-2 \mapsto 0$. Some $\widetilde{\beta}$ does not have a preimage α in $\mathbb{F}_p$. Therefore that same β does not have a preimage $\alpha \in \mathbb{Z}_p$. So by Lemma 4.7.2, β does not have a preimage in $\mathbb{Q}_p$.

So $\mathbb{Q}_p$ is not c-perfect for primes $p > 3$. □

Corollary 4.7.4. *Let $p > 3$. There exist $\mathbb{Q}_p$-critical cubic functions $\phi \in \bar{\mathbb{Q}}_p(z)$ such that ϕ is not equivalent to a $\mathbb{Q}_p$-rational function.*

Proof. This follows from Theorem 4.5.3. □

Theorem 4.7.5. *Let $p = 2$. There exist $\mathbb{Q}_2$-critical cubic functions $\phi \in \bar{\mathbb{Q}}_2(z)$ such that ϕ is not equivalent to a $\mathbb{Q}_2$-rational function.*

Proof. We show that $\mathbb{Q}_2$ is not c-perfect and apply Theorem 4.5.3. Suppose $c_0 \in \mathbb{Q}_2$. Then we have

$$c(z) = -z\frac{z+2}{2z+3} = c_0 \Leftrightarrow z^2 + 2(1+c_0)z + 3c_0 = 0.$$

The discriminant of this quadratic is

$$\Delta = 4(c_0^2 - c_0 + 1) = (2c_0 - 1)^2 + 3. \tag{4.7.1}$$

Now let's specialize by taking $c_0 = \frac{1}{2} + \nu$ with $\nu \in \mathbb{Z}_2$. The discriminant becomes

$$\Delta = (2\nu)^2 + 3 \equiv 3 \pmod 4,$$

which is not a square, hence the discriminant is not a square in $\mathbb{Z}_2$. It follows that $c(z) = c_0$ has no solution in $\mathbb{Q}_2$ when $c_0 \in \frac{1}{2} + \mathbb{Z}_2$. □

Theorem 4.7.6. *$\mathbb{Q}_3$ is c-perfect. Hence $\mathbb{Q}_3$ is critically reducible at 3.*

Proof. Let $c_0 \in \mathbb{Q}_3$. After solving $c(z) = c_0$ we see that the discriminant Δ in 4.7.1 is a square modulo 3. This is equivalent to being a square in $\mathbb{Z}_3$ by Hensel's Lemma. If $c_0 \notin \mathbb{Z}_3$, set $\mathrm{ord}_3(c_0) = r$. Then

$$\mathrm{ord}_3(\Delta) = 2r.$$

Multiplying through by 3^{2r} gives

$$3^{2r}\Delta = (2c_0 3^r - 3^r)^2 + 3^{2r+1}.$$

This quantity is a nonzero square modulo 3, and hence $3^{2r}\Delta$ is a square in $\mathbb{Z}_3$ by Hensel's lemma. It follows that Δ is a square in $\mathbb{Q}_3$. □

We summarize the results in the following theorem:

Theorem 4.7.7. *Let p be a rational prime. The following hold:*

(i) $\mathbb{Q}_p$ is critically reducible at 3 if and only if $p = 3$.

(ii) If $p \neq 3$, then $\mathbb{Q}_p$ is not critically reducible at d for all d. Namely it fails to be critically reducible at 3.

This leads to the question:

Question. Is $\mathbb{Q}_p$ always critically reducible at p or is there something special about 3?

We will continue working on the problem in hopes of proving or disproving the following conjecture:

Conjecture 3. *$\mathbb{Q}_p$ fails to be critically reducible at d for all d except $d = p$.*

BIBLIOGRAPHY

[1] A. Eremenko and A. Gabrielov. Rational functions with real critical points and the B. and M. Shapiro conjecture in real enumerative geometry. *Ann. of Math. (2)*, 155(1):105–129, 2002.

[2] X. Faber. Rational functions with a unique critical point. *Int. Math. Res. Not. IMRN*, (3):681–699, 2014.

[3] N. Fakhruddin. Questions on self maps of algebraic varieties. *J. Ramanujan Math. Soc.*, 18(2):109–122, 2003.

[4] E. V. Flynn, B. Poonen, and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Math. J.*, 90(3):435–463, 1997.

[5] R. Flynn and D. Garton. Graph components and dynamics over finite fields. *Int. J. Number Theory*, 10(3):779–792, 2014.

[6] F. Q. Gouvêa. *p-adic numbers*. Universitext. Springer-Verlag, Berlin, Germany, 1993. An introduction.

[7] R. P. Kurshan and A. M. Odlyzko. Values of cyclotomic polynomials at roots of unity. *Math. Scand.*, 49(1):15–35, 1981.

[8] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, NY, third edition, 2002.

[9] A. Levy. The space of morphisms on projective space. *Acta Arith.*, 146(1):13–31, 2011.

[10] A. Levy, M. Manes, and B. Thompson. Uniform bounds for preperiodic points in families of twists. *Proc. Amer. Math. Soc.*, 142(9):3075–3088, 2014.

[11] K. Madhu. *Galois Theory and Polynomial Orbits*. PhD thesis, University of Rochester, 2011.

[12] M. Manes. $\mathbb{Q}$-rational cycles for degree-2 rational maps having an automorphism. *Proc. Lond. Math. Soc. (3)*, 96(3):669–696, 2008.

[13] M. Manes and B. Thompson. Periodic points in towers of finite fields for polynomials associated to algebraic groups. arXiv:1201.1605 [math.NT], January 2013.

[14] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

[15] S. J. Miller and R. Takloo-Bighash. *An invitation to modern number theory*. Princeton University Press, Princeton, NJ, 2006.

[16] P. Morton. Arithmetic properties of periodic points of quadratic maps. II. *Acta Arith.*, 87(2):89–102, 1998.

[17] P. Morton and J. H. Silverman. Rational periodic points of rational functions. *Internat. Math. Res. Notices*, (2):97–110, 1994.

[18] D. G. Northcott. Periodic points on an algebraic variety. *Ann. of Math. (2)*, 51:167–177, 1950.

[19] A. Ostrowski. Über einige Lösungen der Funktionalgleichung $\psi(x) \cdot \psi(x) = \psi(xy)$. *Acta Math.*, 41(1):271–284, 1916.

[20] C. Petsche, L. Szpiro, and M. Tepper. Isotriviality is equivalent to potential good reduction for endomorphisms of $\mathbb{P}^N$ over function fields. *J. Algebra*, 322(9):3345–3365, 2009.

[21] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over q: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998.

[22] J. H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.

[23] J. H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, NY, 2007.

[24] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, Netherlands, second edition, 2009.

[25] W. Stein et al. *Sage Mathematics Software (Version 4.7.2)*. The Sage Development Team, 2011. `http://www.sagemath.org`.

[26] M. Stoll. Rational 6-cycles under iteration of quadratic polynomials. *LMS J. Comput. Math.*, 11:367–380, 2008.