Lecture Notes on Arithmetic Dynamics
Arizona Winter School
March 13–17, 2010

JOSEPH H. SILVERMAN
jhs@math.brown.edu

Contents

About These Notes/Note to Students

These notes are for the Arizona Winter School on *Number Theory and Dynamical Systems*, March 13–17, 2010. They include background material on complex dynamics and Diophantine equations (§§2–4) and expanded versions of lectures on preperiodic points and height functions (§5), arithmetic dynamics of maps with good reduction (§6), and integer points in orbits (§7). Two final sections give a brief description

Date: February 8, 2010.
1991 *Mathematics Subject Classification.* Primary: 37Pxx; Secondary: 11G99, 14G99, 37P15, 37P30, 37F10.
Key words and phrases. arithmetic dynamical systems.
This project supported by NSF DMS-0650017 and DMS-0854755.

of dynamical analogues of classical results from the theory of Diophantine equations (§8) and some pointers toward other topics in arithmetic dynamics (§9).

The study of arithmetic dynamics draws on ideas and techniques from both classical (discrete) dynamical systems and the theory of Diophantine equations. If you have not seen these subjects or want to do further reading, the books [1, 5, 15] are good introductions to complex dynamics and [2, 9, 12] are standard texts on Diophantine equations and arithmetic geometry. Finally, the textbook [22] is an introduction to arithmetic dynamics and includes expanded versions of the material in these notes, as well as additional topics.

I have included a number of exercises that are designed to help the reader gain some feel for the subject matter. Exercises (A)–(J) are in the background material sections. If you are not already familiar with this material, I urge you to work on these exercises as preparation for the later sections. Exercises (K)–(Q) are on arithmetic dynamics and will help you to understand the notes and act as a warm-up for some of the projects.

There are also some brief paragraphs in small type marked "Supplementary Material" that describe advanced concepts and generalizations. This material is not used in these notes and may be skipped on first reading.

Following the notes are three suggested projects for our winter school working group. The specific questions described in these projects are meant only to serve as guidelines, and we may well find ourselves pursuing other problems during the workshop.

1. Introduction

A (*discrete*) *dynamical system* is a pair (S, φ) consisting of a set S and a self-map

$$\varphi : S \longrightarrow S.$$

The goal of dynamics is to study the behavior of points in S as φ is applied repeatedly. We write

$$\varphi^n(x) = \underbrace{\varphi \circ \varphi \circ \cdots \circ \varphi}_{n \text{ iterates}}(x).$$

The *orbit of* x is the set of points obtained by applying the iterates of φ to x. It is denoted

$$\mathcal{O}_\varphi(x) = \bigl\{x, \varphi(x), \varphi^2(x), \varphi^3(x), \ldots\bigr\}.$$

(For convenience, we let $\varphi^0(x) = x$ be the identity map.)

There are two possibilities for the orbits:

- If the orbit $\mathcal{O}_\varphi(x)$ is finite, we say that x is a *preperiodic point*.
- If the orbit $\mathcal{O}_\varphi(x)$ is infinite, we say that x is a *wandering point*.

A important subset of the preperiodic points consists of those points whose orbit eventually return to its starting point. These are called *periodic points*.

Example 1. We study iteration of the polynomial map

$$\varphi(z) = z^2 - 1$$

on the elements of the field $\mathbb{F}_{11}$. Figure 1 describes this dynamical system, where each arrow connects a point to its image by φ.

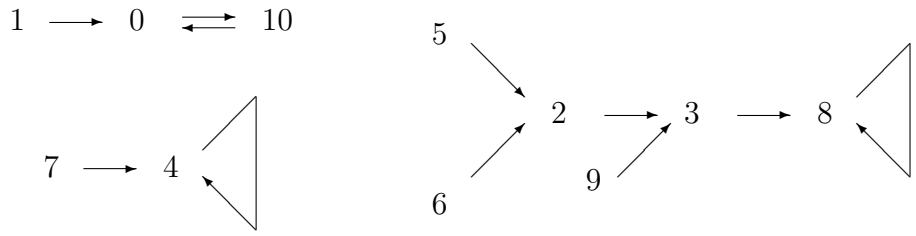

FIGURE 1. Action of $\varphi(z) = z^2 - 1$ on the field $\mathbb{F}_{11}$.

The points 4 and 8 are *fixed points*, i.e., periodic points of period one, while 0 and 10 are periodic points of period two. All other points are preperiodic, but not periodic. And since $\mathbb{F}_{11}$ is a finite set, there obviously are no wandering points.

Example 2. Suppose that we use the same polynomial $\varphi(z) = z^2 - 1$, but we now look at its action on $\mathbb{Z}$. Then

$$1 \longrightarrow 0 \rightleftarrows -1,$$

so 1 is preperiodic, while 0 and -1 are periodic. Every other element of $\mathbb{Z}$ is wandering, since if $|z| \geq 2$, then clearly $\lim_{n\to\infty} \varphi^n(z) = \infty$. More generally, the only φ-preperiodic points in $\mathbb{Q}$ are $\{-1, 0, 1\}$. (Do you see why? Hint: if $z \notin \mathbb{Q}$, let p be a prime in the denominator and prove that $\left|\varphi^n(z)\right|_p \to \infty$.) On the other hand, if we look at $\varphi : \mathbb{C} \to \mathbb{C}$ as a map on $\mathbb{C}$, then φ has (countably) infinitely many complex preperiodic points.

Notation. The sets of preperiodic and periodic points of the map $\varphi : S \to S$ are denoted respectively by

$$\mathrm{PrePer}(\varphi, S) \qquad \text{and} \qquad \mathrm{Per}(\varphi, S).$$

Exercise A. Let G be a group, let $d \ge 2$ be an integer, and define a map $\varphi : G \to G$ by $\varphi(g) = g^d$. Prove that $\mathrm{PrePer}(\varphi, G) = G_{\mathrm{tors}}$, i.e., prove that the preperiodic points are exactly the points of finite order in G.

Exercise B. If S is a finite set, prove that there exists an integer N such that

$$\mathrm{Per}(\varphi, S) = \varphi^n(S) \qquad \text{for all } n \ge N.$$

Arithmetic Dynamics, which is the subject of these notes, is the study of arithmetic properties of dynamical systems. To give a flavor of arithmetic dynamics, here are two motivating questions that we will investigate. Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree at least two.

(I) Can φ have infinitely many $\mathbb{Q}$-rational preperiodic points? More generally, what can we say about the size of $\mathrm{Per}\big(\varphi, \mathbb{P}^1(\mathbb{Q})\big)$ and $\mathrm{PrePer}\big(\varphi, \mathbb{P}^1(\mathbb{Q})\big)$?

(II) Under what circumstances can an orbit $\mathcal{O}_\varphi(\alpha)$ contain infinitely many integers?

Although it may not be immediately apparent, these two questions are dynamical analogues of the following classical questions from the theory of Diophantine equations.

(I′) How many $\mathbb{Q}$-rational points on an elliptic curve can be torsion points? (Answer: Mazur proved that $\#E(\mathbb{Q})_{\mathrm{tors}} \le 16$.)

(II′) Under what circumstances can an affine curve contain infinitely many points with integer coordinates? (Answer: Siegel proved that $C(\mathbb{Z})$ is finite if $\mathrm{genus}(C) \ge 1$.)

2. Background Material: Geometry

A *rational map* $\varphi(z)$ is a ratio of polynomials

$$\varphi(z) = \frac{F(z)}{G(z)} = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

having no common factors. The *degree of* φ is

$$\deg \varphi = \max\{\deg F, \deg G\}.$$

This section contains a brief introduction to the complex projective line $\mathbb{P}^1(\mathbb{C})$ and the geometry of rational maps $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$.

2.1. The Complex Projective Line.

A rational map $\varphi(z) \in \mathbb{C}(z)$ with a nonconstant denominator does not define a map from $\mathbb{C}$ to itself since $\varphi(z)$ will have poles. Instead $\varphi(z)$ defines a self-map of the *complex projective line*

$$\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\},$$

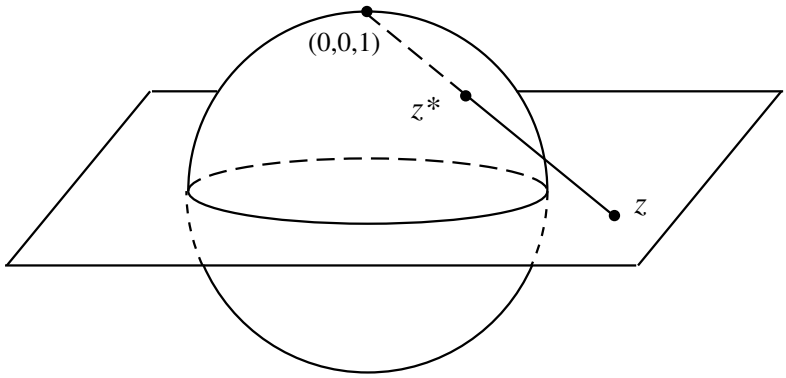

FIGURE 2. Identifying $\mathbb{C} \cup \infty$ with the Riemann sphere.

where we set $\varphi(\alpha) = \infty$ if $\varphi(z)$ has a pole at α, and we define

$$\varphi(\infty) = \lim_{z \to \infty} \varphi(z).$$

A convenient way to visual $\mathbb{P}^1(\mathbb{C})$ is to identify it with the unit sphere in $\mathbb{R}^3$ by drawing lines from the north pole of the sphere to points in the xy-plane. This identification is illustrated in Figure 2.

We put a topology on $\mathbb{P}^1(\mathbb{C})$ using the *chordal metric*,

$$\rho_{\mathrm{ch}}(z_1, z_2) \stackrel{\mathrm{def}}{=} \frac{|z_1 - z_2|}{\sqrt{|z_1|^2 + 1}\sqrt{|z_2|^2 + 1}} = \frac{1}{2}|z_1^* - z_2^*|. \tag{1}$$

Exercise C. Prove the second equality in (1).

If one of z_1 or z_2 is ∞, we take the limit, thus

$$\rho_{\mathrm{ch}}(z, \infty) = \frac{1}{\sqrt{|z|^2 + 1}}.$$

We also note that the chordal metric satisfies $0 \le \rho_{\mathrm{ch}} \le 1$.

2.2. **Linear fractional transformations.** A *linear fractional transformation* (or *Möbius transformation*) is a map of the form

$$z \longmapsto \frac{az + b}{cz + d} \qquad \text{with } ad - bc \neq 0.$$

It defines an automorphism of $\mathbb{P}^1$, and composition corresponds to multiplication of the corresponding matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. These are the only automorphisms of $\mathbb{P}^1(\mathbb{C})$, and two matrices give the same linear fractional transformation if and only if they are scalar multiples of one another, so

$$\mathrm{Aut}(\mathbb{P}^1(\mathbb{C})) = \mathrm{PGL}_2(\mathbb{C}) = \mathrm{GL}_2(\mathbb{C})/\mathbb{C}^*.$$

For $\varphi(z) \in \mathbb{C}(z)$ and $f \in \mathrm{PGL}_2(\mathbb{C})$, we define φ^f to be the conjugation of φ by f,

$$\varphi^f(z) = (f^{-1} \circ \varphi \circ f)(z).$$

Conjugation is illustrated by the commutativity of the diagram

$$\begin{array}{ccc} \mathbb{P}^1 & \xrightarrow{\varphi^f} & \mathbb{P}^1 \\ {\scriptstyle f}\big\downarrow & & {\scriptstyle f}\big\downarrow \\ \mathbb{P}^1 & \xrightarrow{\varphi} & \mathbb{P}^1 \end{array}$$

The reason that conjugation is important for dynamics is because it commutes with iteration,

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

Exercise D. Let $\varphi(z) \in \mathbb{C}(z)$ be a rational function and $f(z) \in \mathrm{PGL}_2(\mathbb{C})$ a linear fractional transformation. Prove that $\alpha \in \mathbb{P}^1(\mathbb{C})$ is periodic for φ of period n if and only if $f^{-1}(\alpha)$ is periodic for φ^f of period n. In particular, there is a natural identification of $\mathrm{Per}\big(\varphi, \mathbb{P}^1(\mathbb{C})\big)$ with $\mathrm{Per}\big(\varphi^f, \mathbb{P}^1(\mathbb{C})\big)$. Formulate and prove an analogous statement for preperiodic points.

2.3. **Critical points and the Riemann–Hurwitz formula.** Let $\varphi(z) \in \mathbb{C}(z)$ be a rational function and $\alpha \in \mathbb{C}$ a point with $\varphi(\alpha) \neq \infty$. Then φ has a Taylor series expansion around α of the form

$$\varphi(z) = \varphi(\alpha) + \varphi'(\alpha)(z-\alpha) + \frac{1}{2}\varphi''(\alpha)(z-\alpha)^2 + \cdots .$$

We say that α is a *critical point* if $\varphi'(\alpha) = 0$, in which case $\varphi(\alpha)$ is a *critical value*. The *ramification index of φ at α*, denoted $e_\alpha(\varphi)$, is the smallest integer $e \geq 1$ such that

$$\varphi(z) = \varphi(\alpha) + c(z-\alpha)^e + \ldots \qquad \text{with } c \neq 0.$$

Thus α is a critical point if and only if $e_\alpha(\varphi) \geq 2$. If $e_\alpha(\varphi) = \deg(\varphi)$, we say that φ is *totally ramified at α*, in which case $\varphi^{-1}\big(\varphi(\alpha)\big) = \{\alpha\}$ consists of a single point.

Exercise E. Prove that

$$(\varphi^n)'(\alpha) = \prod_{i=0}^{n-1} \varphi'\big(\varphi^i(\alpha)\big).$$

In particular, α is a critical point of φ^n if and only if one of the points $\alpha, \varphi(\alpha), \ldots, \varphi^{n-1}(\alpha)$ is a critical point of φ.

Remark 3. To deal with the case that $\alpha = \infty$ and/or $\varphi(\alpha) = \infty$, we choose some $f \in \mathrm{PGL}_2(\mathbb{C})$ such that $f(\infty)$ does not equal either α or $\varphi(\alpha)$ and then set

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

Exercise F. Prove that $e_\alpha(\varphi)$ is independent of the choice of the map f in Remark 3.

Example 4. The function $\varphi(z) = z^d$ is totally ramified at 0 and ∞, and has no other critical points.

The ramification indices are defined locally at the critical points. The following important result says that they satisfy a global relation.

Theorem 5 (Riemann–Hurwitz formula)**.** *Let $\varphi(z) \in \mathbb{C}(z)$ be a rational function of degree $d \ge 1$. Then*

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

Proof. See, e.g., [22, Theorem 1.1]. □

3. Background Material: Classical Dynamics

Let α be a periodic point of φ of exact period n. The *multiplier of φ at α* is the quantity

$$\lambda_\alpha(\varphi) = (\varphi^n)'(\alpha).$$

(If $\infty \in \mathcal{O}_\varphi(\alpha)$, then we first change variables using an appropriate $f \in \mathrm{PGL}_2(\mathbb{C})$ and set $\lambda_\alpha(\varphi) = \lambda_{f^{-1}(\alpha)}(\varphi^f)$.) Since α is fixed by φ^n, the behavior of φ^n locally around α is determined by the Taylor series

$$\varphi^n(z) = \alpha + \lambda_\alpha(\varphi)(z - a) + O\big((z - \alpha)^2\big).$$

In particular, the size of $\lambda_\alpha(\varphi)$ controls what happens when we iterate φ^n. The periodic point α is called:

superattracting	if $\lambda_\alpha(\varphi) = 0$
attracting	if $\big\lvert\lambda_\alpha(\varphi)\big\rvert < 1$

neutral	if $\big\lvert\lambda_\alpha(\varphi)\big\rvert = 1$
repelling	if $\big\lvert\lambda_\alpha(\varphi)\big\rvert > 1$

Neutral periodic points, which are also sometimes called *indifferent*, are further categorized as being *rationally neutral* if $\lambda_\alpha(\varphi)$ is a root of unity and *irrationally neutral* otherwise.

We now come to the central definition of complex (or more generally, metric) dynamics. Let $\varphi(z) \in \mathbb{C}(z)$ be a rational map and let $\alpha \in \mathbb{P}^1(\mathbb{C})$ be a point. We say that φ is *equicontinuous at α* if for every $\epsilon > 0$ there exists a $\delta > 0$ such that

$$\rho_{\mathrm{ch}}(\alpha, \beta) < \delta \quad \Longrightarrow \quad \rho_{\mathrm{ch}}\big(\varphi^n(\alpha), \varphi^n(\beta)\big) < \epsilon \qquad \text{for all } n \ge 0.$$

The intuition of equicontinuity is that if β starts close to α, then all of the points in the φ-orbit of β stay close to the corresponding points in the φ-orbit of α. Thus we can approximate the value of $\varphi^n(\alpha)$ by computing $\varphi^n(\beta)$, even when n becomes very large. Conversely,

if φ is not equicontinuous at α, then no matter how close β is to α, eventually $\varphi^n(\beta)$ moves away from $\varphi^n(\alpha)$.

Definition. The *Fatou set of* φ, denoted $\mathcal{F}(\varphi)$, is the largest open subset of $\mathbb{P}^1(\mathbb{C})$ such that φ is equicontinuous at every point of $\mathcal{F}(\varphi)$. The *Julia set of* φ, denoted $\mathcal{J}(\varphi)$, is the complement of the Fatou set. One says that points in the Julia set behave *chaotically*.

Example 6. If α is an attracting periodic point of φ, then $\alpha \in \mathcal{F}(\varphi)$, and similarly, if α is a repelling periodic point of φ, then $\alpha \in \mathcal{J}(\varphi)$.

Example 7. Let $\varphi(z) = z^d$ with $d \ge 2$. Then

$$\mathcal{J}(\varphi) = S^1 = \bigl\{z \in \mathbb{C} : |z| = 1\bigr\},$$

i.e., the Julia set is the unit circle in $\mathbb{C}$. It is easy to see that $\mathcal{J}(\varphi) \subset S^1$, since if $\alpha \notin S^1$, then there is a neighborhood U of α such that $\lim_{n\to\infty} \varphi^n(U)$ converges to either 0 or ∞, so $\alpha \in \mathcal{F}(\varphi)$. Conversely if $\alpha \in S^1$, then any neighborhood of α contains points whose orbit goes to 0 and points whose orbit goes to ∞, so φ is not equicontinuous at α. Hence $\mathcal{J}(\varphi) = S^1$.

Exercise G. The d^{th} *Chebyshev polynomial* $T_d(z) \in \mathbb{C}[z]$ is the unique polynomial satisfying the identity

$$T_d(z + z^{-1}) = z^d + z^{-d}.$$

(a) Prove that the Chebyshev polynomials satisfy the recursion

$$T_0(x) = 2, \quad T_1(x) = x, \quad T_{d+2}(x) = xT_{d+1}(x) - T_d(x) \quad \text{for } d \ge 0.$$

(b) Compute $T_2(z)$, $T_3(z)$, and $T_4(z)$. Prove that $\deg T_d(z) = d$.
(c) Prove that the Chebyshev polynomials satisfy $(T_d \circ T_e)(z) = T_{de}(z)$, and hence they commute under composition.
(d) Prove that $T_d(-w) = (-1)^d T_d(w)$.
(e) For $d \ge 2$, prove that $T_d(z)$ maps the closed interval $[-2, 2]$ to itself, and that if $\alpha \in \mathbb{C}$ is not in $[-2, 2]$, then $\lim_{n\to\infty} T_d^n(\alpha) = \infty$. Deduce that $\mathcal{J}(T_d) = [-2, 2]$. (*Hint.* Note that $T_d(2\cos\theta) = 2\cos(d\theta)$.)
(f) For $d \ge 2$, prove that aside from ∞, the periodic points of $T_d(z)$ are all in $[-2, 2]$ and are dense in that interval.

Definition. A subset $V \subset \mathbb{P}^1(\mathbb{C})$ is said to be *completely invariant for* φ if $\varphi(V) = V = \varphi^{-1}(V)$.

Theorem 8. *Let $\varphi(z) \in \mathbb{C}(z)$ be a rational map of degree $d \ge 2$.*

(a) *The Fatou set $\mathcal{F}(\varphi)$, the Julia set $\mathcal{J}(\varphi)$, and the boundary $\partial\mathcal{J}(\varphi)$ of the Julia set are all completely invariant for φ.*
(b) *For every $n \ge 1$ we have $\mathcal{F}(\varphi^n) = \mathcal{F}(\varphi)$ and $\mathcal{J}(\varphi^n) = \mathcal{J}(\varphi)$.*
(c) *The Julia set $\mathcal{J}(\varphi)$ is nonempty.*

(d) *The Julia set $\mathcal{J}(\varphi)$ is a perfect set, i.e., it contains no isoloated points.*

Remark 9. For polynomials, the Julia set $\mathcal{J}(\varphi)$ is a bounded subset of $\mathbb{C}$, so the Fatou set $\mathcal{F}(\varphi)$ is also nonempty, but rational maps may have empty Fatou set.

The next result illustrates the importance of the critical orbits to the overall dynamical behavior of φ.

Theorem 10. *Let $\varphi(z) \in \mathbb{C}[z]$ be a polynomial of degree $d \ge 2$.*

(a) *The Julia set $\mathcal{J}(\varphi)$ is connected if and only if every critical point $\alpha \ne \infty$ has orbit $\mathcal{O}_\varphi(\alpha)$ that is bounded in $\mathbb{C}$.*
(b) *If every critical point α of φ satisfies $\lim_{n\to\infty} \varphi^n(\alpha) = \infty$, then the Julia set $\mathcal{J}(\varphi)$ is totally disconnected.*

Finally, we describe some of the ways in which the algebraically defined periodic points of φ interact with the metrically defined Fatou and Julia sets. In particular, all but finitely many of the periodic points are in $\mathcal{J}(\varphi)$, and they form a dense subset of $\mathcal{J}(\varphi)$.

Theorem 11. *Let $\varphi(z) \in \mathbb{C}(z)$ be a rational map of degree $d \ge 2$.*

(a) *The map φ has at most $2d-2$ non-repelling periodic cycles in $\mathbb{P}^1(\mathbb{C})$. If φ is a polynomial map, then it has at most $d-1$ non-repelling periodic cycles in $\mathbb{C}$.*
(b) *The Julia set $\mathcal{J}(\varphi)$ is equal to the closure of the repelling periodic points of φ.*

4. Background Material: Diophantine Equations

This section contains an overview, without proofs, of the material from the theory of Diophantine equations that is used later in these notes.

4.1. **Height functions.**

The height of an algebraic number measures its arithmetic complexity.

Definition. Let $\beta \in \bar{\mathbb{Q}}$ with $\beta \ne 0$ and choose a minimal polynomial

$$F_\beta(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X] \quad \text{with } \gcd(a_0,\dots,a_d) = 1.$$

Factor F_β over $\mathbb{C}$ as

$$F_\beta(X) = (X-\beta_1)(X-\beta_2)\dots(X-\beta_d).$$

Then the (*absolute multiplicative*) *height* of β is

$$H(\beta) = \left(|a_0| \prod_{i=1}^{d} \max\bigl\{|\beta_i|, 1\bigr\}\right)^{1/d},$$

and the (*absolute logarithmic*) *height* of β is[1]

$$h(\beta) = \log H(\beta).$$

(We also set $H(0) = H(\infty) = 1$, and thus $h(0) = h(\infty) = 0$.)

Exercise H. Let $\beta = a/b \in \mathbb{Q}$ be a rational number written in lowest terms. Prove that $H(\beta) = \max\bigl\{|a|, |b|\bigr\}$.

Height functions are used extensively throughout arithmetic geometry because they transform geometry into arithmetic and they have important finiteness properties, as in the following result.

Theorem 12.

(a) *Let $\varphi(z) \in \bar{\mathbb{Q}}(z)$ be a rational function of degree $d \ge 1$. Then*

$$h\bigl(\varphi(\beta)\bigr) = dh(\beta) + O(1) \quad \textit{for all } \beta \in \mathbb{P}^1(\bar{\mathbb{Q}}).$$

(N.B. The $O(1)$ depends on φ, but is independent of β.)

(b) *Fix a number field K. Then for all $B > 0$, the set*

$$\bigl\{\beta \in \mathbb{P}^1(K) : h(\beta) \le B\bigr\} \quad \textit{is finite.}$$

More generally, for all $B > 0$ and $D \ge 1$, the set

$$\bigl\{\beta \in \mathbb{P}^1(\bar{\mathbb{Q}}) : h(\beta) \le B \textit{ and } [\mathbb{Q}(\beta) : \mathbb{Q}] \le D\bigr\} \quad \textit{is finite.}$$

Proof Sketch. (a) For simplicity, we restrict attention to $\beta \in \mathbb{Q}$. Write $\varphi(z) = F(z)/G(z)$ with $F(z) = \sum A_i z^i$ and $G(z) = B_i z^i$, and let $\beta = a/b$. Then

$$\varphi\left(\frac{a}{b}\right) = \frac{\sum A_i a^i b^{d-i}}{\sum B_i a^i b^{d-i}} = \frac{U}{V}.$$

(The fraction U/V need not be in lowest terms.) The triangle inequality can be used to show that

$$\max\bigl\{|U|, |V|\bigr\} \le C \max\bigl\{|a|, |b|\bigr\}^d,$$

where $C = C(\varphi)$ is independent of $\beta = a/b$. This gives one inequality. For the other, one uses the relative primality of $F(z)$ and $G(z)$ to limit the amount of cancelation $\gcd(U, V)$ and then to obtain the opposite inequality. (For details, see [22, Theorem 3.7]. The case $\beta \in \mathbb{Q}$ is in [23, III §3, Lemma 3′].)

(b) It is reasonable to suppose that the height of the roots of a polynomial are related to the size of its coefficients, since the coefficients are the elementary symmetric polynomials of the roots. This is indeed the case. For $F_\beta(X)$ be as above, one proves that

$$\log \max\bigl\{1, |a_1|, |a_2|, \dots, |a_d|\bigr\} \le dh(\beta) + d \log 2.$$

[1] From a information theory perspective, it takes $O\bigl(h(\beta)\bigr)$ bits to store an exact description of β.

Hence if $h(\beta)$ and d are bounded by $h(\beta) \le B$ and $d \le D$, then $F_\beta(X)$ is a polynomial of degree at most D whose coefficients are integers of bounded absolute value. There are only finitely many such polynomials, hence only finitely many β. (For details, see [22, Theorem 3.11].) □

Supplementary Material (**Weil's Height Machine**). Let $V/\bar{\mathbb{Q}}$ be a nonsingular algebraic variety. The general theory of heights, which is due to Weil, assigns a height function $h_D : V(\bar{\mathbb{Q}}) \to \mathbb{R}$ to each divisor $D \in \mathrm{Div}(V)$, where h_D is determined by D up to a bounded function. Heights have many useful properties, including the following:

(i) (Functoriality) Let $\varphi : W \to V$ be a morphism defined over $\bar{\mathbb{Q}}$. Then $h_{V,D}(\varphi(P)) = h_{W,\varphi^* D}(P) + O(1)$ for all $P \in V(\bar{\mathbb{Q}})$.
(ii) (Additivity) Let $D, E \in \mathrm{Div}(V)$. Then $h_{D+E}(P) = h_D(P) + h_E(P) + O(1)$ for all $P \in V(\bar{\mathbb{Q}})$.
(iii) (Linear Equivalence) Let $D, E \in \mathrm{Div}(V)$ be linearly equivalent divisors. Then $h_D(P) = h_E(P) + O(1)$ for all $P \in V(\bar{\mathbb{Q}})$.
(iv) (Finiteness) If $D \in \mathrm{Div}(V)$ is ample, then $\{P \in V(\bar{\mathbb{Q}}) : h_D(P) \le B \text{ and } [\mathbb{Q}(V,P) : \mathbb{Q}] \le D\}$ is finite. (Here $\mathbb{Q}(V,P)$ is the smallest field over which V and P are defined.)

For the construction of Weil's height machine, see for example [9, Theorem B.3.2] or [12, Chapter 4].

4.2. **Diophantine approximation.** The subject of Diophantine approximation asks how closely an irrational number $\beta \in \mathbb{R}$ can be approximated by rational numbers $a/b \in \mathbb{Q}$. The obvious answer is that we can make a/b arbitrarily close to β, since $\mathbb{Q}$ is dense in $\mathbb{R}$. The subtlety is to get a/b close to β without taking a and b too large, as in the following classical result.

Proposition 13. (Dirichlet) *Let $\beta \in \mathbb{R}$ with $\beta \notin \mathbb{Q}$. Then there are infinitely many rational numbers $a/b \in \mathbb{Q}$ satisfying*

$$\left|\frac{a}{b} - \beta\right| \le \frac{1}{b^2}.$$

Proof. See [9, Theorem D.1.1]. □

Exercise I. Let $\beta = (1+\sqrt{5})/2$.

(a) Prove that for all $0 < k \le \sqrt{5}$ there are infinitely many $a/b \in \mathbb{Q}$ satisfying $|a/b - \beta| \le 1/kb^2$.
(b) Prove that for all $k > \sqrt{5}$ there are only finitely many $a/b \in \mathbb{Q}$ satisfying $|a/b - \beta| \le 1/kb^2$.

If β is an algebraic number, then a famous result of Roth says that we cannot do much better.

Theorem 14. (Roth) *Let $\beta \in \bar{\mathbb{Q}}$ with $\beta \notin \mathbb{Q}$, and let $\epsilon > 0$. Then there is a constant $c = c(\beta, \epsilon) > 0$ such that*

$$\left|\frac{a}{b} - \beta\right| \ge \frac{c}{b^{2+\epsilon}} \quad \textit{for all} \quad \frac{a}{b} \in \mathbb{Q}.$$

Proof. See [9, Theorem D.2.1]. □

Exercise J. Let $f(X,Y) = X^d + a_1X^{d-1}Y + \cdots + a_dY^d \in \mathbb{Z}[X,Y]$ be a homogeneous polynomial of degree $d \ge 3$ with the property that $f(X,1)$ has distinct complex roots. Use Roth's theorem to prove that for all nonzero integers m, the Diophantine equation $f(X,Y) = m$ has only finitely many solutions $(x,y) \in \mathbb{Z}^2$.

5. Preperiodic Points and Height Functions

Periodic and preperiodic points play a crucial role in classical complex dynamics, as illustrated for example by Theorem 11, which says that $\varphi(z)$ has only finitely many non-repelling cycles and that the Julia set is the closure of the repelling periodic points. If $\varphi(z) \in \bar{\mathbb{Q}}(z)$ has algebraic coefficients, then the preperiodic points of φ are clearly in $\mathbb{P}^1(\bar{\mathbb{Q}})$. In this section we prove a theorem of Northcott which says that there are only finitely many φ-preperiodic points in $\mathbb{P}^1(K)$ for any number field K. The proof uses height functions, and a more detailed analysis leads us to the construction of a canonical height associated to φ.

5.1. **Finiteness of preperiodic points.** A natural arithmetic problem is to describe the fields generated by preperiodic points. The first result in this direction was proven by Northcott in 1950.

Theorem 15. (Northcott [18]) *Let $\varphi(z) \in \bar{\mathbb{Q}}(z)$ be a rational function of degree $d \ge 2$. Then*

$$\mathrm{PrePer}(\varphi, \bar{\mathbb{Q}}) \stackrel{\mathrm{def}}{=} \big\{\beta \in \mathbb{P}^1(\bar{\mathbb{Q}}) : \beta \text{ is } \varphi\text{-preperiodic}\big\}$$

is a set of bounded height. In particular, if K is a number field and $\varphi(z) \in K(z)$, then $\mathrm{PrePer}(\varphi, K)$ is a finite set.

Proof. Theorem 12(a) says that there is a constant $C = C(\varphi)$ so that

$$h\big(\varphi(\alpha)\big) \ge dh(\alpha) - C \quad \text{for all } \alpha \in \bar{\mathbb{Q}}.$$

Applying this inequality to $\alpha, \varphi(\alpha), \ldots, \varphi^{n-1}(\alpha)$ yields

$$\begin{aligned}
h\big(\varphi(\alpha)\big) &\ge dh(\alpha) - C \\
h\big(\varphi^2(\alpha)\big) &\ge dh\big(\varphi(\alpha)\big) - C && \ge d^2h(\alpha) - (d+1)C \\
h\big(\varphi^3(\alpha)\big) &\ge dh\big(\varphi^2(\alpha)\big) - C && \ge d^3h(\alpha) - (d^2+d+1)C \\
&\vdots && \vdots \\
h\big(\varphi^n(\alpha)\big) &\ge dh\big(\varphi^{n-1}(\alpha)\big) - C && \ge d^nh(\alpha) - (d^{n-1} + \cdots + d + 1)C.
\end{aligned}$$

Using the estimate

$$d^{n-1} + \cdots + d + 1 = \frac{d^n - 1}{d-1} \le \frac{d^n}{d-1},$$

this last inequality implies that

$$\frac{C}{d-1} \ge h(\alpha) - \frac{1}{d^n} h\big(\varphi^n(\alpha)\big), \tag{2}$$

where the constant C is independent of both α and n.

Now suppose that $\beta \in \mathrm{PrePer}(\varphi, \bar{\mathbb{Q}})$, so

$$\varphi^{i+n}(\beta) = \varphi^i(\beta) \quad \text{for some } i \ge 0 \text{ and } n \ge 1.$$

We apply (2) with $\alpha = \varphi^i(\beta)$ and use the assumption $\varphi^{i+n}(\beta) = \varphi^i(\beta)$ to deduce that

$$\frac{C}{d-1} \ge h\big(\varphi^i(\beta)\big) - \frac{1}{d^n} h\big(\varphi^{i+n}(\beta)\big) = \left(1 - \frac{1}{d^n}\right) h\big(\varphi^i(\beta)\big).$$

Since $n \ge 1$, this proves that $h\big(\varphi^i(\beta)\big)$ is bounded. More precisely, $h\big(\varphi^i(\beta)\big) \le Cd/(d-1)^2$.

Finally, applying (2) with $\alpha = \beta$ and $n = i$ yields

$$\frac{C}{d-1} \ge h(\beta) - \frac{1}{d^i} h\big(\varphi^i(\beta)\big).$$

Hence

$$h(\beta) \le \frac{C}{d-1} + h\big(\varphi^i(\beta)\big) \le \frac{C}{d-1} + \frac{dC}{(d-1)^2} = \frac{(2d-1)C}{(d-1)^2}.$$

This completes the proof that the preperiodic points of φ have height that is bounded by a constant depending only on the map φ.

The second statement is then an immediate consequence of Theorem 12(b), which says that there are only finitely elements of K of bounded height. □

As an immediate consequence of Northcott's theorem and the fact (Theorem 12(b)) that there are only finitely many algebraic numbers of bounded degree and bounded height, we have the following result.

Corollary 16. *With notation as in Theorem 15, let $\varphi(z) \in K(z)$ and let $\beta_1, \beta_2, \ldots \in \mathbb{P}^1(\bar{\mathbb{Q}})$ be a sequence of distinct preperiodic points of φ. Then*

$$\lim_{i\to\infty} \big[K(\beta_i) : K\big] = \infty.$$

5.2. **Canonical heights.** Let $\varphi(z) \in \bar{\mathbb{Q}}(z)$ be a rational function of degree $d \ge 2$. Theorem 12(a) says that

$$h\big(\varphi(\beta)\big) - dh(\beta)$$

is bounded as β varies over $\mathbb{P}^1(\bar{\mathbb{Q}})$. It would be nice if we could modify the height so that $h\big(\varphi(\beta)\big)$ exactly equals $dh(\beta)$. A construction of Tate shows how this can be done.

Theorem 17. *Let $\varphi(z) \in \bar{\mathbb{Q}}(z)$ be a rational function of degree $d \ge 2$. Then for all $\beta \in \mathbb{P}^1(\bar{\mathbb{Q}})$ the limit*

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

exists and has the following properties:

(a)
$$\hat{h}_\varphi(\beta) = h(\beta) + O(1) \quad \textit{for all } \beta \in \mathbb{P}^1(\bar{\mathbb{Q}}),$$
where the $O(1)$ depends only on φ and is independent of β.

(b)
$$\hat{h}_\varphi\big(\varphi(\beta)\big) = d\hat{h}_\varphi(\beta) \quad \textit{for all } \beta \in \mathbb{P}^1(\bar{\mathbb{Q}}).$$

(c) *$\hat{h}_\varphi(\beta) \ge 0$, and $\hat{h}_\varphi(\beta) = 0$ if and only if β is a preperiodic point for φ.*

Exercise K. Prove that (a) and (b) in Theorem 17 uniquely characterize the function $\hat{h}_\varphi$.

Proof. Theorem 12(a) says that there is a constant $C = C(\varphi)$ such that

$$\big|h\big(\varphi(\alpha)\big) - dh(\alpha)\big| \le C \quad \text{for all } \alpha \in \mathbb{P}^1(\bar{\mathbb{Q}}). \tag{3}$$

We are going to show that the sequence $d^{-n}h\big(\varphi^n(\beta)\big)$ for $n = 0, 1, 2, \ldots$ is Cauchy. To do this, we let $n > m \ge 0$ and compute

$$\begin{aligned}
&\left|\frac{1}{d^n}\, h\big(\varphi^n(\beta)\big) - \frac{1}{d^m} h\big(\varphi^m(\beta)\big)\right| \\
&\qquad = \left|\sum_{i=m}^{n-1} \left(\frac{1}{d^{i+1}} h\big(\varphi^{i+1}(\beta)\big) - \frac{1}{d^i} h\big(\varphi^i(\beta)\big)\right)\right| \quad \text{telescoping sum,} \\
&\qquad \le \sum_{i=m}^{n-1} \frac{1}{d^{i+1}} \Big|h\big(\varphi^{i+1}(\beta)\big) - dh\big(\varphi^i(\beta)\big)\Big| \qquad \text{triangle inequality,} \\
&\qquad \le \sum_{i=m}^{n-1} \frac{1}{d^{i+1}} C \qquad \text{using (3) with } \alpha = \varphi^i(\beta), \\
&\qquad \le \frac{C}{d^m(d-1)}.
\end{aligned} \tag{4}$$

This last quantity goes to 0 as $n \ge m \to \infty$, which completes the proof that the sequence $d^{-n}h\big(\varphi^n(\beta)\big)$ is Cauchy, hence converges.
(a) Taking $m = 0$ in the inequality (4) yields

$$\left|\frac{1}{d^n} h\big(\varphi^n(\beta)\big) - h(\beta)\right| \le \frac{C}{d-1}.$$

Now let $n \to \infty$ to obtain

$$\bigl|\hat{h}_\varphi(\beta) - h(\beta)\bigr| \le \frac{C}{d-1}.$$

(b) This is immediate from the limit definition of $\hat{h}_\varphi$. Thus

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

(c) It is clear that $\hat{h}_\varphi(\beta) \ge 0$, since it is a limit of non-negative quantities. Further, if β is preperiodic, then $h\bigl(\varphi^n(\beta)\bigr)$ takes on only finitely many values as $n \to \infty$, so the limit definition of $\hat{h}_\varphi$ shows that $\hat{h}_\varphi(\beta) = 0$.

Suppose now that $\beta \in \mathbb{P}^1(\bar{\mathbb{Q}})$ satisfies $\hat{h}_\varphi(\beta) = 0$. Then

$$h\bigl(\varphi^n(\beta)\bigr) = \hat{h}_\varphi\bigl(\varphi^n(\beta)\bigr) + O(1) = d^n \hat{h}_\varphi(\beta) + O(1) = O(1).$$

Hence the points in the orbit

$$\mathcal{O}_\varphi(\beta) = \bigl\{\beta, \varphi(\beta), \varphi^2(\beta), \ldots\bigr\}$$

have bounded height. Further, if we let K be a number field such that $\varphi(z) \in K(z)$ and $\beta \in \mathbb{P}^1(K)$, then $\mathcal{O}_\varphi(\beta)$ is contained in $\mathbb{P}^1(K)$. Theorem 12(b) says that sets of bounded height in $\mathbb{P}^1(K)$ are finite, so $\mathcal{O}_\varphi(\beta)$ is a finite set, and hence β is preperiodic. □

Néron and Tate originally constructed canonical heights on abelian varieties. Tate used the telescoping sum trick as in Theorem 17, while Néron constructed the canonical height as a sum of local heights. See [3] for the general construction of canonical heights associated to polarized dynamical systems.

Supplementary Material (**Polarized dynamical systems**). A *polarized dynamical system* is a triple (V, φ, D) consisting of a (smooth projective) variety $V/\bar{\mathbb{Q}}$, a morphism $\varphi : V \to V$, and a divisor $D \in \mathrm{Div}(V) \otimes \mathbb{R}$ satisfying $\varphi^* D \sim \kappa D$ for some real number $\kappa > 1$, where $\sim$ denotes linear equivalence. (The terminology polarized dynamical system is due to Shouwu Zhang.) The limit construction described in Theorem 17 works in the setting of polarized dynamical systems, and the associated canonical height is defined by

$$\hat{h}_{\varphi,D}(P) = \lim_{n\to\infty} \frac{1}{\kappa^n} h_D\bigl(\varphi^n(P)\bigr).$$

If D is ample, then $\hat{h}_{\varphi,D}(P) = 0$ if and only if P is preperiodic for φ.

Supplementary Material (**Local heights, Green functions, and invariant measures**). The canonical height $\hat{h}_\varphi$ associated to φ may be decomposed as a sum of local height functions $\hat{\lambda}_{\varphi,v}$, one for each absolute value v on the number field K,

$$\hat{h}_\varphi(P) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} n_v \hat{\lambda}_{\varphi,v}(P).$$

(See [3] or [22, §§3.5, 5.9] for details.) If $\varphi(z) \in K[z]$ is a polynomial, then the local height is given by the natural limit

$$\hat{\lambda}_{\varphi,v}(\beta) = \lim_{n\to\infty} \frac{1}{d^n} \log \max\bigl\{\bigl|\varphi^n(\beta)\bigr|_v, 1\bigr\},$$

but for rational maps the construction is somewhat more complicated. For archimedean v, the associated local height function is a Green function for the filled Julia set and is closely related to the invariant measure attached to the rational map φ.

5.3. **Conjectures and generalizations.** We proved (Theorem 15) that a rational map has only finitely many rational preperiodic points. It is natural to ask how large this set can be as we vary the map φ.

Exercise L. Prove that for all $d \ge 2$ there exists a rational function $\varphi(z) \in \mathbb{Q}(z)$ of degree d with a $\mathbb{Q}$-rational periodic point of period $2d+1$.

Thus if we allow the degree to be large, then we can get rational periodic points of large period. What happens if we look at maps of a fixed degree?

Conjecture 18 (Uniform Boundedness Conjecture I)**.** *Let $d \ge 2$. There is a constant $C = C(d)$ such that for all rational maps $\varphi(z) \in \mathbb{Q}(z)$ of degree d,*

$$\#\operatorname{Per}\bigl(\varphi, \mathbb{P}^1(\mathbb{Q})\bigr) \le C.$$

The conjecture is not known even if we restrict to polynomials of degree two. Here is the current status in that case.

Theorem 19. *For $c \in \mathbb{Q}$, let $\varphi_c(z) = z^2 + c$.*

(a) *There are infinitely many $c \in \mathbb{Q}$ such that φ_c has a $\mathbb{Q}$-rational point of period 1, period 2, or period 3.*
(b) (Morton [16]) *There is no $c \in \mathbb{Q}$ such that φ_c has a $\mathbb{Q}$-rational point of period 4.*
(c) (Flynn–Poonen–Schaefer [8]) *There is no $c \in \mathbb{Q}$ such that φ_c has a $\mathbb{Q}$-rational point of period 5.*
(d) (Stoll [24]) *If the conjecture of Birch and Swinnerton-Dyer is true, then there is no $c \in \mathbb{Q}$ such that φ_c has a $\mathbb{Q}$-rational point of period 6.*

Poonen has conjectured that $\varphi_c(z) = z^2 + c$ can never have a $\mathbb{Q}$-rational point of period greater than 3.

Exercise M. Prove part (a) of Theorem 19.

The general form of uniform boundedness for preperiodic points on projective space reads as follows.

Conjecture 20 (Uniform Boundedness Conjecture II)**.**
(Morton–Silverman [17]) *Let $d \ge 2$, $D \ge 1$, and $n \ge 1$. There is a constant $C = C(d, D, n)$ such that for all fields $K/\mathbb{Q}$ of degree at most D and all morphisms $\varphi : \mathbb{P}^n \to \mathbb{P}^n$ of degree d defined over K,*

$$\#\operatorname{PrePer}\bigl(\varphi, \mathbb{P}^n(K)\bigr) \le C.$$

Supplementary Material (**Applications of Uniform Boundedness**). To illustrate the depth of Conjecture 20, we note that the case $(d, D, n) = (4, 1, 1)$ implies Mazur's theorem [13] that the size of the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ of an elliptic curve $E/\mathbb{Q}$ is bounded by a constant that does not depend on E. The proof uses the existence of a rational map $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ making the following diagram commute:

$$\begin{array}{ccc} E & \xrightarrow{P\mapsto 2P} & E \\ {\scriptstyle x}\downarrow & & {\scriptstyle x}\downarrow \\ \mathbb{P}^1 & \xrightarrow{\varphi} & \mathbb{P}^1 \end{array}$$

(In dynamics, maps of this sort are called Làttes maps.) Fakhruddin [6] has shown that the full Conjecture 20 implies uniform boundedness of torsion on abelian varieties of fixed dimension over fields of bounded degree. This last statement is known unconditionally only in dimension one, i.e., for elliptic curves, where it was proven by Merel [14].

Wandering points are characterized by the fact that their heights are strictly positive (Theorem 17(c)), so we might ask how small these positive heights can be. There are two natural ways make this precise. We can fix the map φ and vary the field of defintion of the wandering point β, or we can fix a field K and vary the map $\varphi \in K(z)$ and the point $\beta \in \mathbb{P}^1(K)$. Questions of of the first sort were studied by Lehmer for the multiplicative group, and those of the second type by Dem'janenko and Lang for elliptic curves. Here are the dynamical analogues.

Conjecture 21. (Dynamical Lehmer conjecture) *Let $K/\mathbb{Q}$ be a number field and let $\varphi(z) \in K(z)$ be a rational function of degree $d \ge 2$. There is a constant $C = C(\varphi)$ such that for all φ-wandering points $\beta \in \mathbb{P}^1(\bar{K})$,*

$$\hat{h}_\varphi(\beta) \ge \frac{C}{\big[K(\beta) : K\big]}.$$

In order to state the second conjecture, we need a way of measuring the intrinsic size of a rational map. For simplicity, we restrict attention to functions with $\mathbb{Q}$-coefficients

Definition. Let $\varphi(z) \in \mathbb{Q}(z)$. The *height of* φ is the quantity

$$h(\varphi) = \log \max\big\{|a_0|, \dots, |a_d|, |b_0|, \dots, |b_d|\big\},$$

where we write $\varphi(z)$ as

$$\varphi(z) = \frac{F(z)}{G(z)} = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

with integer coefficients satisfying

$$\gcd(a_0, a_1, \dots, a_d, b_0, b_1, \dots, b_d) = 1.$$

We say that $\varphi(z) \in \mathbb{Q}(z)$ is *minimal* if

$$h(\varphi) = \min_{f \in \mathrm{PGL}_2(\mathbb{Q})} h(\varphi^f).$$

Conjecture 22. (Dynamical Lang height conjecture) *Let $K/\mathbb{Q}$ be a number field and let $d \ge 2$ be an integer. There is a constant $C = C(K,d) > 0$ so that for all minimal rational maps $\varphi(z) \in K(z)$ of degree d and all φ-wandering points $\beta \in \mathbb{P}^1(K)$,*

$$\hat{h}_\varphi(\beta) \ge C h(\varphi).$$

6. Arithmetic Dynamics of Maps with Good Reduction

In the last section we gave a global proof that a rational map has only finitely many preperiodic points defined over any given number field. In this section we take a local point of view and study the reduction of maps and points modulo p. For ease of exposition, we restriction attention to $\mathbb{Q}$, but everything in this section can be generalized to arbitrary fields K that come equipped with a (discrete) valuation v. We begin by describing which rational maps behave well when reduced modulo p, after which we prove our main theorem on reduction of periodic points for maps that have good reduction.

6.1. **Resultants and Good Reduction.** We say that a rational map $\varphi(z) \in \mathbb{Q}(z)$ is in *normalized form* if it is written as a ratio of polynomials

$$\varphi(z) = \frac{F(z)}{G(z)} = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

with integer coefficients satisfying

$$\gcd(a_0, a_1, \ldots, a_d, b_0, b_1, \ldots, b_d) = 1.$$

For a given prime p, we can then reduce φ modulo p to get a rational function

$$\tilde{\varphi}(z) = \frac{\tilde{F}(z)}{\tilde{G}(z)} = \frac{\tilde{a}_0 + \tilde{a}_1 z + \cdots + \tilde{a}_d z^d}{\tilde{b}_0 + \tilde{b}_1 z + \cdots + \tilde{b}_d z^d} \in \mathbb{F}_p(z)$$

with coefficients in the finite field $\mathbb{F}_p$. We say that $\varphi(z)$ has *good reduction at p* if

$$\deg(\tilde{\varphi}) = \deg(\varphi),$$

or equivalently, if $\tilde{F}(z)$ and $\tilde{G}(z)$ have no common factors in $\mathbb{F}_p[z]$.

For any two polynomials $F(z)$ and $G(z)$, the *resultant of F and G*, denoted $\operatorname{Res}(F,G)$, is polynomial in the coefficients of F and G that vanishes if and only if F and G have a common factor (or if their leading coefficients both vanish). This gives the alternative definition

$$\varphi \text{ has good reduction at } p \quad \Longleftrightarrow \quad p \nmid \operatorname{Res}(F,G).$$

In particular, we see that φ has only finitely many primes of bad reduction.

Supplementary Material (**Scheme-Theoretic Definition of Good Reduction**). A rational map $\varphi \in \mathbb{Q}_p(z)$ is a morphism $\varphi : \mathbb{P}^1_{\mathbb{Q}_p} \to \mathbb{P}^1_{\mathbb{Q}_p}$, so it induces a rational map $\varphi : \mathbb{P}^1_{\mathbb{Z}_p} \dashrightarrow \mathbb{P}^1_{\mathbb{Z}_p}$ over $\mathrm{Spec}(\mathbb{Z}_p)$. Then φ has good reduction at p if and only if this rational map extends to a morphism over $\mathrm{Spec}(\mathbb{Z}_p)$. If this happens, then the reduced map $\tilde{\varphi}$ is the restriction of φ to the special fiber $\mathbb{P}^1_{\mathbb{F}_p}$.

Example 23. The resultant of two quadratic polynomials $F(z) = a_0 + a_1 z + a_2 z^2$ and $G(z) = b_0 + b_1 z + b_2 z^2$ is given by the formula

$$\mathrm{Res}(F,G) = a_2^2 b_0^2 - a_2 a_1 b_1 b_0 + a_1^2 b_2 b_0 - 2a_2 a_0 b_2 b_0 + a_2 a_0 b_1^2 - a_1 a_0 b_2 b_1 + a_0^2 b_2^2.$$

The following elementary proposition shows why good reduction is a useful property for φ to have when studying its dynamical properties.

Proposition 24. *Let $\varphi(z) \in \mathbb{Q}(z)$ have good reduction at p.*

(a) $\widetilde{\varphi^n} = \tilde{\varphi}^n$, *i.e., reduction commutes with iteration.*
(b) $\widetilde{\varphi(\alpha)} = \tilde{\varphi}(\tilde{\alpha})$, *i.e., reduction commutes with evaluation.*
(c) *Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a periodic point of exact period n for φ. Then $\tilde{\alpha} \in \mathbb{P}^1(\mathbb{F}_p)$ is periodic for $\tilde{\varphi}$ and its period m divides n.*

Proof. Parts (a) and (b) follow easily from standard properties of resultants, or directly from the scheme-theoretic description of good reduction. See [22, Theorem 2.18] for details.

To prove (c), we use (a) and (b) to compute

$$\tilde{\alpha} = \widetilde{\varphi^n(\alpha)} = \tilde{\varphi}^n(\tilde{\alpha}),$$

so $\tilde{\alpha}$ is periodic with period at most n. Let m be its exact period, so $\tilde{\varphi}^m(\tilde{\alpha}) = \tilde{\alpha}$, and write $n = mq + r$ with $0 \le r < m$. Then

$$\tilde{\alpha} = \tilde{\varphi}^n(\tilde{\alpha}) = \tilde{\varphi}^r \circ \underbrace{\tilde{\varphi}^m \circ \cdots \circ \tilde{\varphi}^m}_{q \text{ iterations}}(\tilde{\alpha}) = \tilde{\varphi}^r(\tilde{\alpha}).$$

The minimality of m implies that $r = 0$, and hence m divides n. □

Exercise N. Give examples of maps with bad reduction for which parts (a) and (b) of Proposition 24 are false.

We now come to the main theorem on reduction of periodic points for rational maps having good reduction. It is the dynamical analogue of classical theorems on reduction of torsion points on elliptic curves and abelian varieties (cf. [20, Proposition VII.3.1] and [9, Theorem C.1.4]).

Theorem 25. *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \ge 2$ and let p be a prime of good reduction for φ. Let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a*

periodic point of φ, and set:

$n =$ *the exact period of* α *for the map* φ.

$m =$ *the exact period of* $\tilde{\alpha}$ *for the map* $\tilde{\varphi}$.

$r =$ *the smallst integer such that* $\lambda_{\tilde{\varphi}}(\tilde{\alpha})^r = 1$, *or* ∞ *if no power of* $\lambda_{\tilde{\varphi}}(\tilde{\alpha})$ *equals* 1. (*Note that the multiplier is* $\lambda_{\tilde{\varphi}}(\tilde{\alpha}) = (\tilde{\varphi}^m)'(\tilde{\alpha})$.)

Then n *has one of the following forms*:

$$n = m \quad \text{or} \quad n = mr \quad \text{or} \quad n = mrp.$$

(*If* $p \ge 5$, *then only the first two are possible.*)

Proof. Proposition 24(c) tells us that $m \mid n$, so replacing φ by φ^m and m by 1, we are reduced to the case that $\tilde{\alpha}$ is a fixed point of $\tilde{\varphi}$. If $\varphi(\alpha) = \alpha$, then $n = 1 = m$ and we are done. Otherwise we can find a change of variables that moves α to 0 and preserves the good reduction property of φ. (See [22, Proposition 2.11].) The assumption that 0 is fixed modulo p means that φ has the form

$$\varphi(z) = \frac{a_0 + a_1 z + \cdots + a_d z^d}{b_0 + b_1 z + \cdots + b_d z^d}$$

with

$$\varphi(0) = a_0/b_0 \equiv 0 \pmod{p}.$$

The fact that $\varphi(z)$ has good reduction implies that a_0 and b_0 are not both divisible by p, so we see that $p \mid a_0$ and $p \nmid b_0$. Let

$$R_p = \left\{ \frac{a}{b} \in \mathbb{Q} : p \nmid b \right\}$$

be the localization of $\mathbb{Z}$ at p. Then long division shows that the Taylor expansion of $\varphi(z)$ around $z = 0$ looks like

$$\varphi(z) = \mu + \lambda z + \frac{A(z)}{1 + zB(z)} z^2, \tag{5}$$

where

$$A(z), B(z) \in R_p[z], \qquad \lambda = \varphi'(0), \qquad \text{and} \qquad \mu = a_0/b_0 \in pR_p.$$

Applying (5) repeatedly to $\alpha = 0$, an easy induction shows that

$$\varphi^j(0) \equiv \mu(1 + \lambda + \lambda^2 + \cdots + \lambda^{j-1}) \pmod{\mu^2 R_p}.$$

In particular, since $\varphi^n(0) = 0$ and $\mu \in pR_p$, we see that

$$0 = \varphi^n(0) \equiv 1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \pmod{pR_p}. \tag{6}$$

Suppose now that $r \ge 2$, i.e., $\lambda \not\equiv 1 \pmod{p}$. Then (6) implies that $\lambda^n \equiv 1 \pmod{p}$, so $r \mid n$. (Recall that r is the multiplicative order of λ in $\mathbb{F}_p^*$.) If $n = r$, we are done. Otherwise we replace φ with φ^r

and n with n/r, which has the effect of replacing λ with λ^r, so our new multiplier satisfies

$$\lambda \equiv 1 \pmod{pR_p}.$$

Retaining the notation in (5) (of course, μ, λ, $A(z)$, and $B(z)$ will change), we have reduced to the case that

$$\begin{aligned} \varphi(0) &\neq 0, & \mu &= \varphi(0) \equiv 0 \pmod{pR_p}, \\ \varphi^n(0) &= 0, & \lambda &= \varphi'(0) \equiv 1 \pmod{pR_p}. \end{aligned}$$

Then (6) yields

$$0 \equiv 1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv n \pmod{pR_p},$$

so $p \mid n$. This allows us to replace φ by φ^p and n by n/p. If now $\varphi(0) = 0$, we're done, otherwise repeating the same argument again shows that $p \mid n$. This process must stop eventually, which concludes the proof that either $n = m$ or $n = mr$ or $n = mrp^k$ for some $k \geq 1$.

A refined analysis using a third-order expansion

$$\varphi(z) = \mu + \lambda z + \nu z^2 + \frac{A(z)}{1 + zB(z)} z^3$$

can be used to prove that $k = 0$ when $p \geq 5$; see [22, Theorem 2.31] for details. The remaining cases $p = 2$ and $p = 3$ are more complicated and are left for the reader. □

Corollary 26. *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \geq 2$ and let p be the smallest primes for which $\varphi(z)$ has good reduction. Suppose that $\alpha \in \mathbb{P}^1(\mathbb{Q})$ is a periodic point for φ of exact period n. Then*

$$n \leq p^3 - p.$$

(If $p \geq 5$, then $n \leq p^2 - 1$.)

Proof. In the notation of Theorem 25, the period m of $\tilde{\alpha}$ is certainly no larger than $p+1$, since $\mathbb{P}^1(\mathbb{F}_p)$ has $p+1$ points. Similarly, $r \leq p-1$, since r is the order of λ in $\mathbb{F}_p^*$ and $\#\mathbb{F}_p^* = p - 1$. Hence

$$n \leq mrp \leq (p+1)(p-1)p = p^3 - p.$$

Further, if $p \geq 5$, then $n \leq mr \leq p^2 - 1$. □

Exercise O. Let $\varphi(z) = (az^2 + bz + c)/z^2$ with $a, b, c \in \mathbb{Z}$ and $\gcd(c, 6) = 1$. Suppose that $\alpha \in \mathbb{P}^1(\mathbb{Q})$ is periodic for $\varphi(z)$ of exact period n. Prove that $n \in \{1, 2, 3\}$, and that all three values are possible. (Challenge: Prove the same result under the weaker assumption that $\gcd(c, 2) = 1$.)

A modified version of Theorem 25 is true when φ is defined over an extension field, but the proof is much harder when p is highly ramified. Here is the full generalization.

Theorem 27. (Zieve [28]) *Let $K/\mathbb{Q}_p$ be a finite extension, let $e = e(K/\mathbb{Q}_p)$ be the ramification degree, let $\varphi(z) \in K(z)$ be a rational map with good reduction, and let $\alpha \in \mathbb{P}^1(K)$ be a periodic point of exact period n. Further let m and r be defined as in Theorem 25. Then either $n = m$ or $n = mrp^k$ for some $k \ge 0$ satisfying*

$$p^{k-1} \le \frac{2e}{p-1}.$$

(If $p = 2$, the upper bound may be replaced with $e/(p-1)$.)

7. Integer Points in Orbits

Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational function of degree $d \ge 2$ and let $\alpha \in \mathbb{Q}$. A natural number theoretic question to ask is whether the orbit $\mathcal{O}_\varphi(\alpha)$ may contain infinitely many integers. The answer is obviously yes, since for example, if $\varphi(z) \in \mathbb{Z}[z]$ and $\alpha \in \mathbb{Z}$, then every point $\varphi^n(\alpha)$ in the orbit is an integer. But even if we rule out polynomials, there are rational functions with orbits containing infinitely integers. For example,

$$\varphi(z) = \frac{2z^2 - 2z + 1}{4z^2 - 4z + 1}$$

has the orbit

$$2 \xrightarrow{\varphi} \frac{5}{9} \xrightarrow{\varphi} 41 \xrightarrow{\varphi} \frac{3281}{6561} \xrightarrow{\varphi} 21523361 \xrightarrow{\varphi} \frac{926510094425921}{1853020188851841} \xrightarrow{\varphi} 1716841910146256242328924544641 \xrightarrow{\varphi} \dots$$

in which every other entry is an integer. The explanation is that the second iterate of φ is itself a polynomial,

$$\varphi^2(z) = 8z^4 - 16z^3 + 12z^2 - 4z + 1.$$

Clearly a similar phenomenon will occur if some higher iterate of $\varphi(z)$ is polynoimal, but surprisingly, if this happens, then already $\varphi^2(z)$ is a polynomial.

Proposition 28. *Let $\varphi(z) \in \mathbb{C}(z)$ be a rational function of degree d, and suppose that some iterate $\varphi^n(z)$ is a polyomial, i.e., $\varphi^n(z) \in \mathbb{C}[z]$. Then one of the following is true.*

(a) *$\varphi(z)$ is a polynomial.*
(b) *$\varphi^2(z)$ is a polynomial, and there is a linear function $f(z) = az + b$ such that $\varphi^f(z) = z^{-d}$.*

Proof. The fact that $\varphi^n(z)$ is a polynomial implies that $(\varphi^n)^{-1}(\infty)$ consists of the single point ∞. For notational convenience, we let

$$\alpha_i = \varphi^i(\infty) \quad \text{for } i = 0, 1, 2, \dots, n.$$

Note that $\alpha_0 = \infty$ and $\alpha_n = \varphi^n(\infty) = \infty$. Further, the fact that $(\varphi^n)^{-1}(\infty) = \{\infty\}$ implies the $\varphi^{-1}(\alpha_i)$ consists of the single point α_{i-1} for each $1 \le i \le n$. Thus φ is totally ramified at every α_i, so the ramification index at α_i satisfies $e_{\alpha_i}(\varphi) = d$.

Let m be the smallest integer such that $\varphi^m(\infty) = \infty$, so $\alpha_0, \ldots, \alpha_{m-1}$ are distinct points. We apply the Riemann–Hurwitz formula (Theorem 5) to compute

$$\begin{aligned} 2d-2 &= \sum_{\beta\in\mathbb{P}^1(\mathbb{C})} \bigl(e_\beta(\varphi)-1\bigr) \qquad \text{(Riemann–Hurwitz formula)} \\ &\ge \sum_{i=0}^{m-1} \bigl(e_{\alpha_i}(\varphi)-1\bigr) \\ &= m(d-1). \end{aligned}$$

Hence $m \le 2$. (Note how we use here the assumption that $d \ge 2$.)

There are two cases. First, if $m = 1$, then $\alpha_0 = \alpha_1 = \infty$, so

$$\varphi^{-1}(\infty) = \varphi^{-1}(\alpha_1) = \{\alpha_0\} = \{\infty\}.$$

Hence φ is a polynomial.

Second, if $m = 2$, then $\alpha_0 = \alpha_2 = \infty$ and $\alpha_1 \ne \infty$. Conjugating $\varphi(z)$ by $f(z) = z + \alpha_1$, we may assume that $\alpha_1 = 0$. Then $\varphi^{-1}(0) = \{\infty\}$ and $\varphi^{-1}(\infty) = \{0\}$. The only rational functions of degree d with this property have the form $\varphi(z) = az^{-d}$, and conjugating by $f(z) = a^{1/(d+1)}z$ puts φ into the form z^{-d}. □

In view of Proposition 28, the following result is perhaps not surprising. The proof, however, is not trivial.

Theorem 29. ([21]) *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational map such that $\varphi^2(z)$ is not a polynomial and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$. Then*

$$\mathcal{O}_\varphi(\alpha) \cap \mathbb{Z}$$

is a finite set.

In the next section we sketch the proof of a stronger result.

7.1. **A non-integrality theorem for wandering points.**

Theorem 30. ([21]) *Let $\varphi(z) \in \mathbb{Q}(z)$ be a rational map such that $\varphi^2(z)$ is not a polynomial and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$ be a wandering point for φ. For each $n \ge 0$, write*

$$\varphi^n(\alpha) = \frac{a_n}{b_n} \in \mathbb{Q}$$

as a fraction in lowest terms. Then

$$\liminf_{n\to\infty} \frac{\log|b_n|}{\log|a_n|} \ge 1.$$

In other words, as n increases, the number of digits in the denominator b_n is (up to a small factor) at least as large as the number of digits in the numerator a_n. Further, we know from Theorem 17 that

$$\begin{aligned}\max\bigl\{\log|a_n|, \log|b_n|\bigr\} = h\bigl(\varphi^n(\alpha)\bigr) &= \hat{h}_\varphi\bigl(\varphi^n(\alpha)\bigr) + O(1)\\ &= d^n\hat{h}_\varphi(\alpha) + O(1),\end{aligned}$$

so Theorem 30 implies that there are constants $C > 0$ and $B > 1$ such that

$$|b_n| \ge CB^{d^n} \qquad \text{for all } n \ge 0.$$

This statement is clearly much stronger than Theorem 29, which merely says that $|b_n| \ge 2$ for sufficiently large values of n.

Proof Sketch of Theorem 30. Let $\epsilon > 0$. We need to show that there are only finitely many points in the orbit satisfying

$$|b_n| \le |a_n|^{1-\epsilon}. \tag{7}$$

In particular, such points satisfy $|a_n| \ge |b_n|$, so

$$H\bigl(\varphi^n(\alpha)\bigr) \stackrel{\text{def}}{=} \max\bigl\{|a_n|, |b_n|\bigr\} = |a_n|.$$

(Here H is the multiplicative height defined in Section 4.1.) This allows us to rewrite (7) as

$$\bigl|\varphi^n(\alpha)\bigr| \ge H\bigl(\varphi^n(\alpha)\bigr)^\epsilon. \tag{8}$$

Since $\log H\bigl(\varphi^n(\alpha)\bigr) \approx d^n\hat{h}_\varphi(\alpha)$ from Theorem 17, this shows that $\bigl|\varphi^n(\alpha)\bigr|$ gets extremely large as $n \to \infty$ for points satisfying (7). In terms of $\mathbb{P}^1(\mathbb{C})$, the point $\bigl|\varphi^n(\alpha)\bigr|$ gets close to ∞, and an easy calculation gives the quantitative estimate

$$\rho_{\text{ch}}\bigl(\varphi^n(\alpha), \infty\bigr) \approx \frac{1}{\bigl|\varphi^n(\alpha)\bigr|} \le H\bigl(\varphi^n(\alpha)\bigr)^{-\epsilon} \approx e^{-\epsilon d^n\hat{h}_\varphi(\alpha)}.$$

Here is a rough idea of the proof. Since $\varphi^n(\alpha)$ is very close to ∞, the rational number $\varphi^{n-k}(\alpha)$ should be quite close to one of the algebraic numbers β in the inverse image $\varphi^{-k}(\infty)$. With some care and a little

luck, we can apply Roth's theorem (Theorem 14) to show that this cannot happen if n is sufficiently large.

We fix an integer k satisfhing $d^k > 6/\epsilon$ and we let $\beta \in \bar{\mathbb{Q}}$ be the point in $\varphi^{-k}(\infty)$ that is closest to $\varphi^{n-k}(\alpha)$. Assume for the moment that the map φ is unramified, i.e., it has no critical points.[2] Unramified maps more-or-less preserve distances, so

$$\rho_{\mathrm{ch}}\bigl(\varphi^{n-k}(\alpha),\beta\bigr) \approx \rho_{\mathrm{ch}}\bigl(\varphi^{n}(\alpha),\varphi^{k}(\beta)\bigr) = \rho_{\mathrm{ch}}\bigl(\varphi^{n}(\alpha),\infty\bigr).$$

We now do a computation, where the constants $C_1, C_2, \ldots$ may depend on φ, α, β, and k, but do not depend on n.

$$\begin{aligned}
\frac{1}{|a_n|^\epsilon} &\ge \left|\frac{b_n}{a_n}\right| && \text{from the assumption (7),}\\
&= \frac{1}{\bigl|\varphi^n(\alpha)\bigr|} && \text{since } \varphi^n(\alpha) = a_n/b_n,\\
&\ge C_1\rho_{\mathrm{ch}}\bigl(\varphi^n(\alpha),\infty\bigr) && \text{from definition of } \rho_{\mathrm{ch}},\\
&= C_1\rho_{\mathrm{ch}}\bigl(\varphi^n(\alpha),\varphi^k(\beta)\bigr) && \text{since } \varphi^k(\beta) = \infty,\\
&\ge C_2\rho_{\mathrm{ch}}\bigl(\varphi^{n-k}(\alpha),\beta\bigr) && \text{from our choice of } \beta, \text{ and}\\
&&& \text{assuming } \varphi \text{ is unramified,}\\
&\ge C_3\bigl|\varphi^{n-k}(\alpha)-\beta\bigr| && \text{definition of } \rho_{\mathrm{ch}},\\
&\ge \frac{C_4}{H\bigl(\varphi^{n-k}(\alpha)\bigr)^3} && \text{Roth's theorem (with exponent 3),}\\
&\ge \frac{C_5}{H\bigl(\varphi^{n}(\alpha)\bigr)^{3/d^k}} && \text{using the canonical height,}\\
&= \frac{C_5}{|a_n|^{3/d^k}} && \text{since } |a_n| \ge |b_n|,\\
&\ge \frac{C_6}{|a_n|^{\epsilon/2}} && \text{since } k \text{ satisfies } d^k \ge 6/\epsilon.
\end{aligned}$$

Hence $|a_n| \le C_6^{2/\epsilon}$, so there are only finitely many choices for a_n, and since $|a_n| \ge |b_n|$, there are also only finitely many choices for b_n.

How do we fix the proof? First we need to know how ramification affects the distance between points. Near a point γ of ramification index e for a map ψ we have $\psi(z) = \psi(\gamma) + c(z-\gamma)^e + \cdots$, so distances are dilated by an exponent of e. In other words, if z is close to γ, then

$$\rho_{\mathrm{ch}}\bigl(\psi(z),\psi(\gamma)\bigr) \approx \rho_{\mathrm{ch}}(z,\gamma)^{e_\gamma(\psi)}.$$

[2]Yes, I know this is a ridiculous assumption, since φ always has at least two critical points! But this incorrect argument will help clarify the correct proof and will show exactly where we use the assumption that $\varphi^2(z)$ is not a polynoimal.

If we use this corrected formula in our earlier calculation, we get (after some work)

$$\begin{aligned}
\frac{1}{|a_n|^\epsilon} &\ge C_1 \rho_{\mathrm{ch}}\bigl(\varphi^n(\alpha), \varphi^k(\beta)\bigr) && \text{from earlier,}\\
&\ge C_2 \rho_{\mathrm{ch}}\bigl(\varphi^{n-k}(\alpha), \beta\bigr)^{e_\beta(\varphi^k)} && \text{corrected for ramification,}\\
&\ge \frac{C_5}{|a_n|^{3e_\beta(\varphi^k)/d^k}} && \text{completing the calculation as above.}
\end{aligned}$$

We want to choose a value of k that makes the exponent

$$\frac{3e_\beta(\varphi^k)}{d^k} \tag{9}$$

smaller than $\epsilon/2$.

Suppose, for example, that $\varphi(z)$ were a polynomial and $\beta = \infty$. Then $\varphi(z)$ is totally ramified at β, so

$$e_\beta(\varphi^k) = e_\infty(\varphi)^k = d^k$$

and we're stuck. Similarly, $e_\beta(\varphi^k) = d^k$ if $\varphi^2(z)$ is a polynomial. But if we assume that $\varphi^2(z)$ is not a polynomial, then iteration tends to spread out ramification, and the Riemann-Hurwitz formula (Theorem 5) can be used to prove that

$$\lim_{k\to\infty} \frac{\max\limits_{\beta\in\varphi^{-k}(\infty)} e_\beta(\varphi^k)}{d^k} = 0. \tag{10}$$

The proof of (10) is an elaboration of the proof of Proposition 28; see [22, Lemma 3.52] for details. This allows us to make (9) smaller than $\epsilon/2$ and completes our sketch of the proof of Theorem 30. For full details, see [22, §3.8], or see [21] for the proof of a more general statement. □

Exercise P. Let $\varphi(z) \in \mathbb{C}(z)$ be a rational map of degree $d \ge 2$, let $k \ge 1$, and let $\beta \in \mathbb{P}^1(\mathbb{C})$ be a point such that $\beta, \varphi(\beta), \dots, \varphi^{k-1}(\beta)$ are distinct. Prove that $e_\beta(\varphi^k) \le e^{2d-2}$. (Note that e_β is the ramification index, while $e = 2.71828\dots$.)

7.2. **Orbits with lots of integer points.** Theorem 29 says that orbits generally contain only finitely many integer points. It is natural to ask how large $\#\bigl(\mathcal{O}_\varphi(\alpha)\cap\mathbb{Z}\bigr)$ may be. If we take φ to have degree d, then it is easy to find lots of examples with $2d+2$ integer points. (Do you see why?) But even for fixed degree we can make $\#\bigl(\mathcal{O}_\varphi(\alpha)\cap\mathbb{Z}\bigr)$ as large as desired by using a "clearing the denominators" trick that was originally used by Chowla [4] to find elliptic curves with many integer points.

Proposition 31. *Let $\psi(z) \in \mathbb{Q}(z)$ be a nonconstant rational function and let $\beta \in \mathbb{Q}$ be a wandering point for ψ. Then for all $N \ge 1$ there exists an integer $B \ge 1$ such that the rational map $\varphi_B(z) = B\psi(z/B)$ satisfies*

$$\#\big(\mathcal{O}_{\varphi_B}(B\beta) \cap \mathbb{Z}\big) \ge N.$$

Proof. For each $n \ge 1$ write

$$\psi^n(\beta) = \frac{a_n}{b_n}$$

as a fraction in lowest terms. Let

$$B = \mathrm{LCM}(b_1, b_2, \ldots, b_n).$$

Note that $\varphi_B^n(z) = B\psi^n(z/B)$, so for all $n \le N$ we have

$$\varphi_B^n(B\beta) = B\psi^n(\beta) = B\frac{a_n}{b_n} \in \mathbb{Z}. \qquad \square$$

Exercise Q. In Proposition 31, prove that there is a constant $c > 0$ and an increasing sequence of values for B so that

$$\#\big(\mathcal{O}_{\varphi_B}(B\beta) \cap \mathbb{Z}\big) \ge c \log\log B.$$

If we prohibit the trick used in the proof of Proposition 31, then it is not known if $\mathcal{O}_\varphi(\beta) \cap \mathbb{Z}$ can be large.

Definition. A map $\varphi(z) \in \mathbb{Q}(z)$ is said to be *affine minimal* if

$$h(\varphi) = \min_{\substack{f = az+b \\ a \in \mathbb{Q}^*, b \in \mathbb{Q}}} h(\varphi^f).$$

(See Section 5.3, page 17, for the definition of the height of φ and for the analogous definition of minimal rational maps.)

The following is a dynamical analogue of a conjecture originally due to Lang in the case of elliptic curves.

Conjecture 32. *Let $d \ge 2$ be an integer. There is a constant $C = C(d)$ such that for all* affine minimal *rational functions $\varphi(z) \in \mathbb{Q}(z)$ of degree d with $\varphi^2(z) \notin \mathbb{Q}[z]$ and all φ-wandering points $\beta \in \mathbb{P}^1(\mathbb{Q})$,*

$$\#\big(\mathcal{O}_\varphi(\beta) \cap \mathbb{Z}\big) \le C.$$

8. Dynamical Analogues of Classical Results

In this section we briefly recall some classical results and conjectures from arithmetic geometry and describe their dynamical analogues. A rough dictionary between the two subjects equates:

Arithmetic Geometry		**Dynamical Systems**
torsion points	$\longleftrightarrow$	preperiodic points
finitely generated groups	$\longleftrightarrow$	orbits of wandering points

We start with Raynaud's theorem (originally conjectured by Manin and Mumford).

Theorem 33. (Raynaud [19]) *Let $A/\mathbb{C}$ be an abelian variety and let $X \subset A$ be an algebraic subvariety. Then the Zariski closure of*

$$A_{\mathrm{tors}} \cap X$$

in A is a union of a finite number of translates of abelian subvarieties of A by torsion points of A.

Replacing the abelian variety A and its torsion subgroup A_{tors} with a dynamical system $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ and its set of preperiodic points leads to a dynamical analogue of the Manin–Mumford conjecture.

Definition. A subvariety $Y \subset \mathbb{P}^N$ is *φ-periodic* if there exists an integer $n \ge 1$ such that $\varphi^n(Y) = Y$. Similarly, Y is *φ-preperiodic* if there exist integers $n > m \ge 0$ such that $\varphi^n(Y) = \varphi^m(Y)$.

Conjecture 34. (Dynamical Manin–Mumford Conjecture) *Let $\varphi : \mathbb{P}^N_{\mathbb{C}} \to \mathbb{P}^N_{\mathbb{C}}$ be a morphism of degree at least 2 and let $X \subset \mathbb{P}^N$ be an algebraic subvariety. Then the Zariski closure of*

$$\mathrm{PrePer}\big(\varphi, \mathbb{P}^N(\mathbb{C})\big) \cap X$$

in $\mathbb{P}^N$ is a union of a finite number of φ-preperiodic subvarieties of $\mathbb{P}^N$.

A strengthened version of the Manin–Mumford conjecture using canonical heights was posed by Bogomolov and proven by Ullmo [25] and Zhang [26]. Here is the dynamical analogue.

Conjecture 35. (Dynamical Bogomolov Conjecture) *Let $\varphi : \mathbb{P}^N_{\bar{\mathbb{Q}}} \to \mathbb{P}^N_{\bar{\mathbb{Q}}}$ be a morphism of degree at least 2 and let $X \subset \mathbb{P}^N$ be an irreducible algebraic subvariety that is not preperiodic for φ. Then there exists an $\epsilon > 0$ such that the set*

$$\big\{P \in X(\bar{\mathbb{Q}}) : \hat{h}_\varphi(P) < \epsilon\big\}$$

is not Zariski dense in X.

Since preperiodic points are characterized by having canonical height zero (Theorem 17), Conjecture 35 says in particular that the preperiodic points of φ are not Zariski dense in X.

We next recall Mordell's conjecture, as strengthened by Lang and proven by Faltings.

Theorem 36. (Faltings [7]) *Let $A/\mathbb{C}$ be an abelian variety, let $\Gamma \subset A(\mathbb{C})$ be a finitely generated subgroup, and let $X \subset A$ be an algebraic subvariety that contains no nontrivial abelian subvarieties of A. Then*

$$X \cap \Gamma$$

is a finite set.

Replacing A and Γ with a dynamical system and a wandering orbit gives a dynamical analogue.

Conjecture 37. (Dynamical Mordell–Lang Conjecture) *Let $\varphi : \mathbb{P}^N_{\mathbb{C}} \to \mathbb{P}^N_{\mathbb{C}}$ be a morphism of degree at least 2, let $P \in \mathbb{P}^N(\mathbb{C})$ be a wandering point for φ, and let $X \subset \mathbb{P}^N$ be an irreducible algebraic subvariety that contains no φ-periodic subvarieties of dimension at least one. Then*

$$X \cap \mathcal{O}_\varphi(P)$$

is a finite set.

For further material on these and other related dynamical conjectures, see the survey article by Zhang [27].

9. Additional Topics

The preceding notes have covered only a small portion of the subject that loosely goes by the name arithmetic dynamics. Among the many important topics that have been omitted, we mention:

- p-adic dynamics, especially in the bad reduction case. This includes dynamics over finite extensions of $\mathbb{Q}_p$, over $\mathbb{C}_p$, and in recent years, on the Berkovich projective line.
- Moduli spaces associated to dynamical systems, especially the dynamical modular curves that classify quadratic polynomials $z^2 + c$ with a marked periodic point or periodic orbit.
- Arithmetic dynamics of maps associated to (commutative) algebraic groups.
- Arithmetic dynamics of rational maps $\varphi : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ that are not morphisms; in particular, (regular) automorphisms $\mathbb{A}^N \to \mathbb{A}^N$ that do not extend to morphisms on $\mathbb{P}^N$.
- Equidistribution for points of small height, for Galois conjugates of periodic points, and for backward orbits.

- Dynamics over finite fields, over function fields, over power series rings, and over Drinfeld modules.
- Dynamics on Lie groups and homogeneous spaces, and associated problems of equidistribution, ergodicity, and entropy. (This area is a huge field in its own right.)

If you want to investigate any of these areas, you will find an introduction to the first four topics in Chapters 4–7 of [22]. And see [22, pages 5–6] for some pointers towards the literature on the other topics in this list.

Acknowledgements. I would like to thank Michelle Manes for her careful reading of these notes.

References

[1] A. F. Beardon. *Iteration of Rational Functions*, volume 132 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[2] E. Bombieri and W. Gubler. *Heights in Diophantine Geometry*. Number 4 in New Mathematical Monographs. Cambridge University Press, Cambridge, 2006.

[3] G. S. Call and J. H. Silverman. Canonical heights on varieties with morphisms. *Compositio Math.*, 89(2):163–205, 1993.

[4] A. Chowla. Contributions to the analytic theory of numbers (II). *J. Indian Math. Soc.*, 20:120–128, 1933.

[5] R. Devaney. *An Introduction to Chaotic Dynamical Systems*. Addison-Wesley, Redwood City, CA, 2nd edition, 1989.

[6] N. Fakhruddin. Boundedness results for periodic points on algebraic varieties. *Proc. Indian Acad. Sci. Math. Sci.*, 111(2):173–178, 2001.

[7] G. Faltings. Diophantine approximation on abelian varieties. *Ann. of Math. (2)*, 133:349–366, 1991.

[8] 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.

[9] M. Hindry and J. H. Silverman. *Diophantine Geometry: An Introduction*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[10] P. Ingram and J. H. Silverman. Primitive divisors in arithmetic dynamics. *Proc. Camb. Philos. Soc.*, 2008. `arxiv.org/abs/0707.2505`.

[11] R. Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials, 2006. `ArXiv:math.NT/0612415`.

[12] S. Lang. *Fundamentals of Diophantine Geometry*. Springer-Verlag, New York, 1983.

[13] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

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

[15] J. Milnor. *Dynamics in One Complex Variable*. Friedr. Vieweg & Sohn, Braunschweig, 1999.

[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] M. Raynaud. Sous-variétés d'une variété abélienne et points de torsion. In *Arithmetic and Geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 327–352. Birkhäuser Boston, Boston, MA, 1983.

[20] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.

[21] J. H. Silverman. Integer points, Diophantine approximation, and iteration of rational maps. *Duke Math. J.*, 71(3):793–829, 1993.

[22] J. H. Silverman. *The Arithmetic of Dynamical Systems*, volume 241 of *Graduate Texts in Mathematics*. Springer, New York, 2007.

[23] J. H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.
[24] M. Stoll. Rational 6-cycles under iteration of quadratic polynomials, 2008. `arXiv:0803.2836`.
[25] E. Ullmo. Positivité et discrétion des points algébriques des courbes. *Ann. of Math. (2)*, 147(1):167–179, 1998.
[26] S.-W. Zhang. Equidistribution of small points on abelian varieties. *Ann. of Math. (2)*, 147(1):159–165, 1998.
[27] S.-W. Zhang. Distributions in algebraic dynamics. In *Differential Geometry: A Tribute to Professor S.-S. Chern, Surv. Differ. Geom., Vol. X*, pages 381–430. Int. Press, Boston, MA, 2006.
[28] M. Zieve. *Cycles of Polynomial Mappings*. PhD thesis, University of California at Berkeley, 1996. `www.math.rutgers.edu/~zieve/papers/ucthesis.ps`.

List of Notation

Index

Appendix A. Projects

This section describes three projects that we might work on during the AWS.

Project I: Dynamics over finite fields.
We consider a rational map $\varphi(z) \in \mathbb{F}_p(z)$ defined over a finite field. It is clear that every point in $\mathbb{P}^1(\mathbb{F}_p)$ is preperiodic, since $\mathbb{P}^1(\mathbb{F}_p)$ is a finite set. But there are many natural questions to ask about the structure of the orbits. Here are a few problems on which we might work.

(1) Let $\varphi(z) \in \mathbb{F}_p(z)$. What can we say about the proportion of points that are periodic for φ? For example, for which maps φ is it true that
$$\lim_{n\to\infty} \frac{\#\operatorname{Per}\bigl(\varphi, \mathbb{P}^1(\mathbb{F}_{p^n})\bigr)}{p^n} = 0?$$
(2) Let $\varphi(z) \in \mathbb{Q}(z)$. Then for all but finitely many p, we can reduce φ modulo p to get a map $\tilde{\varphi}_p : \mathbb{P}^1(\mathbb{F}_p) \to \mathbb{P}^1(\mathbb{F}_p)$. For which maps is it true that
$$\lim_{p\to\infty} \frac{\#\operatorname{Per}\bigl(\tilde{\varphi}_p, \mathbb{P}^1(\mathbb{F}_p)\bigr)}{p} = 0?$$
(3) Can we find maps $\varphi(z) \in \mathbb{Q}(z)$ such that $\#\operatorname{Per}\bigl(\tilde{\varphi}_p, \mathbb{P}^1(\mathbb{F}_p)\bigr)$ is large for infinitely many p? (An extreme case is given by *permuation polynomials*, which are polynomials $\varphi(z) \in \mathbb{Z}[z]$ with the property that $\tilde{\varphi}_p : \mathbb{F}_p \to \mathbb{F}_p$ is a bijection for infinitely many p, so in particular every point in $\mathbb{F}_p$ is periodic.)
(4) Given $\varphi(z) \in \mathbb{F}_p(z)$, form a (directed) graph Γ_φ whose vertices are the points in $\mathbb{P}^1(\mathbb{F}_p)$ and such that vertices α and β are connected if $\varphi(\alpha) = \beta$. On average, how many connected components would we expect φ to have? To answer this question, we could average over all (or a subset of) maps of a given degree in $\mathbb{F}_p(z)$, or we could fix one $\varphi(z) \in \mathbb{Q}(z)$ and look at $\Gamma_{\tilde{\varphi}_p}$ as p varies.

A guiding principle in mathematics is to determine to what extent local information can be used to make global deductions. So we would like to use information about the reductions $\tilde{\varphi}_p$ for varying p to deduce information about φ itself. For example, here's a vague question. If $\operatorname{Per}\bigl(\tilde{\varphi}_p, \mathbb{P}^1(\mathbb{F}_p)\bigr)$ is "large," does that imply that $\operatorname{Per}\bigl(\varphi, \mathbb{P}^1(\mathbb{Q})\bigr)$ is non-empty? And here's a more precise question. Suppose that $\tilde{\varphi}_p$ has a point of exact period N in $\mathbb{P}^1(\mathbb{F}_p)$ for all but finitely many p. Does it follow that φ has a point of exact period N in $\mathbb{P}^1(\mathbb{Q})$?

Project II: Orbits with many integer points.
Proposition 31 says that orbits may contain arbitrarily many integers, but if we restrict to affine minimal rational maps φ, then Conjecture 32 says that the number of integer points should be bounded in terms of the degree of φ.

As a warm-up, prove that for every $d \ge 2$ there exist infinitely many affine minimal rational maps $\varphi(z) \in \mathbb{Q}(z)$ with $\varphi^2(z) \notin \mathbb{Q}[z]$ such that

$$\#\big(\mathcal{O}_\varphi(0) \cap \mathbb{Z}\big) \ge 2d+2.$$

In general, for each $d \ge 2$, define

$$M(d) = \sup\left\{ \#\big(\mathcal{O}_\varphi(\beta) \cap \mathbb{Z}\big) : \begin{array}{l} \varphi(z) \in \mathbb{Q}(z),\ \varphi^2(z) \notin \mathbb{Q}[z], \\ \varphi \text{ is affine minimal, and} \\ \beta \in \mathbb{P}^1(\mathbb{Q}) \text{ is } \varphi\text{-wandering} \end{array} \right\}.$$

The warm-up shows that $M(d) \ge 2d+2$. As a further warm-up, find examples of rational maps which show that $M(2) \ge 7$ and $M(3) \ge 9$.

One aim of this project is construct rational maps that give improved lower bounds for $M(d)$, first for small values of d, and ultimately for all d. For example, one goal would be to show that $M(d) \ge 2d+3$ for all d. A subsidiary task will be to develop a good algorithm for determining whether a given rational map is affine minimal.

We might also consider the conjecture on restricted families of maps, for example maps of the form $\varphi(z) = (az^2+bz+c)/z$. There is also the question of integral points in orbits of maps $\varphi : \mathbb{P}^N \to \mathbb{P}^N$ on higher dimensional projective spaces.

Project III: Primes, prime support, and primitive divisors in orbits.
Let $\varphi(z) \in \mathbb{Z}[z]$ be a polynomial and $\beta \in \mathbb{Z}$ a wandering point for $\varphi(z)$. The orbit $\mathcal{O}_\varphi(\beta)$ consists entirely of integers, so it is natural to ask if it contains infinitely many primes. Of course, there are many cases where this never happens, for example if $\varphi(z)$ factors.

Question 38. *Does there exist a polynomial $\varphi(z) \in \mathbb{Z}[z]$ of degree $d \ge 2$ that has an orbit $\mathcal{O}_\varphi(\beta)$ containing infinitely many primes?*

An elementary probabilistic argument suggests that the answer is no.

Exercise R. A nonzero integer is said to be P_k if it is a product of at most k (not necessarily distinct) primes. Let $\varphi(z) \in \mathbb{Z}[z]$ be a polynomial of of degree $d \ge 2$ and let $\beta \in \mathbb{Z}$. Give a probabilistic argument to show that for any fixed $k \ge 1$, the orbit $\mathcal{O}_\varphi(\beta)$ should contain only finitely many P_k-integers. (*Hint.* A variant of the prime number theorem says that the number

of P_k-integers less than X is asymptotic to $X(\log\log X)^{k-1}/(\log X)$ as $X \to \infty$ with k fixed.)

A potentially easier question is to study the set of all primes that divide some point in the orbit.

Definition. The *support* of a sequence of integers $\mathcal{A} = (A_1, A_2, A_3, \ldots)$ is the set

$$\text{Support}(\mathcal{A}) = \big\{\text{primes } p : p \text{ divides some term } A_i \text{ in the sequence}\big\}.$$

There are some maps and orbits whose support is uninteresting. For example, if $\varphi(z) = z^d$, then $\text{Support}\big(\mathcal{O}_\varphi(\beta)\big)$ is simply the set of primes dividing β. But for most polynomials $\varphi(z) \in \mathbb{Q}[z]$, it is a challenging problem to determine if $\text{Support}\big(\mathcal{O}_\varphi(\beta)\big)$ has positive density. There is recent work of Jones [11] showing that the support of certain quadratic polynomials has positive density, while others have zero density. As one part of this project, we will study the support of orbits of polynomials, and more generally the support of the numerator and denominator sequences arising from orbits of rational maps.

It is also interesting to look at the primes that divide the individual terms in a sequence. A *primitive prime divisor of* A_n is a prime p such that

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

The existence (or lack thereof) of primitive divisors in integer sequences is both interesting in its own right and useful as a tool. Here is an example of a famous theorem on primitive divisors.

Theorem 39. (Zsigmondy) *Let $a > b \ge 1$ be integers and define $A_n = a^n - b^n$. Then A_n has a primitive prime divisor for all $n \ge 7$.*

Example 40. Zsigmondy's theorem is best possible, since

$$2^6 - 1 = 63 = 3^2 \cdot 7, \qquad 2^2 - 1 = 3, \qquad \text{and} \qquad 2^3 - 1 = 7,$$

so $2^6 - 1$ has no primitive divisors.

Definition. The *Zsigmondy set* of a sequence $\mathcal{A}$ is

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

Thus Zsigmondy's theorem says that

$$\max \mathcal{Z}\big(\{a^n - b^n\}_{n\ge1}\big) \le 6.$$

There are similar statements for other sequences such as the Fibonacci sequences and the sequence of denominators of multiples of a point on an elliptic curve. In this project we will study primitive divisors in orbits. Ingram and I [10] recently proved a general result which says

(under suitable hypotheses) that $\mathcal{Z}\big(\mathcal{O}_\varphi(\beta)\big)$ is finite, i.e., $\varphi^n(\beta)$ has a primitive prime divisor for all sufficiently large n. The proof uses Theorem 30, which in turn relies on Roth's theorem, so is ineffective.

For special classes of rational maps and orbits, it should be possible to obtain explicit bounds for the largest element in the Zsigmondy set $\mathcal{Z}\big(\mathcal{O}_\varphi(\beta)\big)$, as Zsigmondy did for the sequence $a^n - b^n$. Looking for such bounds is the second part of this project.

Mathematics Department, Box 1917, 151 Thayer Street, Brown University, Providence, RI 02912 USA

E-mail address: jhs@math.brown.edu