A Number Theorist's Perspective on Dynamical Systems

Joseph H. Silverman

Brown University

<jhs@math.brown.edu>

Frontier Lectures

Texas A&M, Monday, April 4–7, 2005

1. Rational Functions and Dynamical Systems

A *rational function* is a ratio of polynomials

$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0}{b_e z^e + b_{e-1} z^{e-1} + \cdots + b_1 z + b_0}.$$

- The *degree* of ϕ is the larger of d and e, where $a_d \neq 0$ and $b_e \neq 0$.
- The subject of *Dynamical Systems* is the study of iteration of functions
$$\phi^n(z) = \underbrace{\phi \circ \phi \circ \phi \cdots \phi}_{n \text{ iterations}}(z).$$
- More precisely, start with a number α and look at its *orbit*
$$\mathcal{O}_\phi(\alpha) = \bigl\{\alpha, \phi(\alpha), \phi^2(\alpha), \phi^3(\alpha), \ldots\bigr\}.$$
- One studies the iterates of ϕ by classifying and describing the different sorts of orbits
- We generally assume that $\boxed{\deg(\phi) \geq 2}$.

A Simple Example

Consider the function

$$\phi(z) = z^2.$$

- Some points have orbits that head out to infinity,

$$\mathcal{O}_\phi(2) = \{2, 4, 16, 256, \ldots\},$$

- while others head in towards zero,

$$\mathcal{O}_\phi\left(\tfrac{1}{2}\right) = \left\{\tfrac{1}{2}, \tfrac{1}{4}, \tfrac{1}{16}, \ldots\right\}.$$

- Some points are fixed,

$$\mathcal{O}_\phi(0) = \{0, 0, 0, \ldots\} \qquad \text{and} \qquad \mathcal{O}_\phi(1) = \{1, 1, 1, \ldots\},$$

- while other points are eventually fixed

$$\mathcal{O}_\phi(-1) = \{-1, 1, 1, 1, 1, \ldots\}.$$

- And if we use complex numbers, there are points that cycle,

$$\mathcal{O}_\phi\left(\tfrac{-1+\sqrt{-3}}{2}\right) = \left\{\tfrac{-1+\sqrt{-3}}{2}, \tfrac{-1-\sqrt{-3}}{2}, \tfrac{-1+\sqrt{-3}}{2}, \tfrac{-1-\sqrt{-3}}{2}, \ldots\right\}.$$

Fixed, Periodic, and Preperiodic Points

- A point α is called *periodic* if

  $$\phi^n(\alpha) = \alpha \quad \text{for some } n \geq 1.$$

  The smallest such n is called the *period of* α.
- If $\phi(\alpha) = \alpha$, then α is a *fixed point.*
- A point α is *preperiodic* if some iterate $\phi^i(\alpha)$ is perioidic. Equivalently, α is preperiodic if its orbit $\mathcal{O}_\phi(\alpha)$ is finite.
- A point α that has infinite orbit is called a *wandering point.*

The Example $\phi(z) = z^2$

- 2 and $\frac{1}{2}$ are *wandering points.*
- 0 and 1 are *fixed points.*
- -1 is a *preperiodic* point that is not periodic.
- $\frac{-1+\sqrt{-3}}{2}$ is a periodic point of period 2.

That Pesky Point "At Infinity"

- For rational functions, the orbit of a point may include "infinity."
- For example,

$$\phi(z) = \frac{z^2+1}{z^2-1} \quad \text{has} \quad \phi(1) = \infty. \tag{$*$}$$

- But then what is $\phi^2(1) = \phi(\infty)$? It is natural to set

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

- So for the example $(*)$, we have $\phi(\infty) = 1$ and

$$\mathcal{O}_\phi(1) = \{1, \infty\}.$$

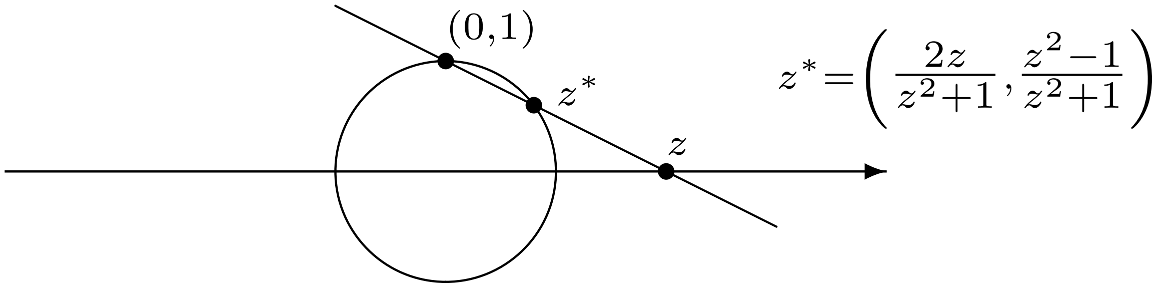
  Thus 1 and ∞ are periodic points of period 2. Similarly

$$\mathcal{O}_\phi(-1) = \{-1, \infty, 1, \infty, 1, \ldots\},$$

  so -1 is preperiodic.
- We want to treat this extra point "at infinity" exactly the same as every other point. In particular, points that are "close to infinity" should be close to one another.

One-Point Compactification of $\mathbb{R}$ and $\mathbb{C}$

- There are many ways to describe the (*one point*) *compactification* of the real line (or of the complex plane).
- A nice pictorial method is to identify $\mathbb{R}$ with the points of the unit circle excluding the point $(0,1)$. The point $(0,1)$ then plays the role of the point at infinity.



- It is not important to worry about the precise transformation formula. Just remember that a rational map $\phi : \mathbb{R} \to \mathbb{R}$ gives a map

$$\phi : \mathbb{R} \cup \{\infty\} \longrightarrow \mathbb{R} \cup \{\infty\},$$

and that a small interval around a point in $\mathbb{R}$ is no different from a small interval around the point ∞.

2. Dynamics and Chaos

- Consider again the function $\phi(z) = z^2$.
- If we start with a point $0 < \alpha < 1$, then the orbit

  $$\mathcal{O}_\phi(\alpha) = \{\alpha, \alpha^2, \alpha^4, \alpha^8, \ldots\}$$

  has the property that

  $$\lim_{n\to\infty} \phi^n(\alpha) = 0.$$
- Further, if we start with a point β that is close to α, then $\phi^n(\beta)$ remains close to $\phi^n(\alpha)$ as $n \to \infty$.
- Similarly, if we start with a point $\alpha > 1$, then

  $$\lim_{n\to\infty} \phi^n(\alpha) = \infty;$$

  and if we take a point β that is close to α, then $\phi^n(\beta)$ remains close to $\phi^n(\alpha)$ as $n \to \infty$. [N.B. In our one-point compactification, points that are close to ∞ are also close to each other.]

Chaos and the Julia and Fatou Sets

- But look what happens if we take $\alpha = 1$ for $\phi(z) = z^2$.
- The point $\alpha = 1$ has a very simple orbit, since it is a fixed point.
- However, no matter how close we choose β to α, eventually $\phi^n(\beta)$ moves far away from $\phi^n(\alpha)$.
- This is an example of *chaotic behavior*.
- *Informal Definition*: A point α is a *chaotic point* for ϕ if points that are close to α do not remain close to one another when we apply the iterates of ϕ.
- The *Julia set* of ϕ is the set of chaotic points. Its complement is the *Fatou set* of ϕ. They are denoted

$$\begin{aligned} \mathcal{J}(\phi) &= \{\alpha \text{ where } \phi \text{ is chaotic}\}, \\ \mathcal{F}(\phi) &= \{\alpha \text{ where } \phi \text{ is not chaotic}\}. \end{aligned}$$

- *Formal Definition*: The Fatou set is the largest open set on which the set of iterates $\{\phi, \phi^2, \phi^3, \ldots\}$ is equicontinuous.

The Julia Set and the Mandelbrot Set

Theorem.

(a) The Julia set is a closed set

(b) The Julia set $\mathcal{J}(\phi)$ is never empty (if we use complex numbers). In other words, every rational map has chaotic points.

(c) All but finitely many of the periodic points of ϕ are in the Julia set.

Example. Even very simple functions such

$$\phi_c(z) = z^2 + c$$

have very complicated Julia sets. For example, there are some c values for which $\mathcal{J}(\phi_c)$ is connected (but usually fractal looking), while for other c values it is totally disconnected.

The famous *Mandelbrot set* is the set

$$\mathcal{M} = \{c \in \mathbb{C} : \mathcal{J}(\phi_c) \text{ is connected}\}.$$

Another way to describe the Mandelbrot set is as the set of c such that the orbit $\mathcal{O}_{\phi_c}(0) = \{0, \phi_c(0), \phi_c^2(0), \ldots\}$ is bounded.

3. A Number Theorist's View of Periodic Points

For a dynamicist, the periodic points of ϕ are the (complex) numbers satisfying an equation

$$\phi^n(z) = z \quad \text{for some } n = 1, 2, 3, \ldots.$$

A number theorist asks:

What sorts of numbers may appear as periodic points?

For example:

Question: Can periodic points be rational numbers?

The answer is obviously **Yes**. We've seen several examples.

Question: How many periodic points can be rational numbers?

That's a more interesting question. There are always infinitely many complex periodic points, and in many cases there are infinitely many real periodic points. But among the infinitely many periodic points, how many of them can be rational numbers?

Northcott's Theorem

Theorem. (Northcott 1949) A rational function $\phi(z) \in \mathbb{Q}(z)$ has only finitely many periodic points that are rational numbers.

Proof. Since every math talk should have one proof, I'll sketch for you the (relatively elementary) proof of Northcott's result.

An important tool is the *height* of a rational number p/q written in lowest terms:

$$H\left(\frac{p}{q}\right) = \max\bigl\{|p|, |q|\bigr\}.$$

Notice that for any constant B, there are only finitely many rational numbers $\alpha \in \mathbb{Q}$ with height $H(\alpha) \le B$. This makes the height a useful tool for proving finiteness results.

Lemma. If $\phi(z)$ has degree d, then there is a constant $C = C_\phi > 0$ so that

$$H\bigl(\phi(\beta)\bigr) \ge C \cdot H(\beta)^d \qquad \text{for all rational numbers } \beta \in \mathbb{Q}.$$

This is intuitively reasonable if you write out $\phi(z)$ as a ratio of polynomials. The tricky part is making sure there's not too much cancellation.

Proof of Northcott's Theorem

We apply the lemma repeatedly:

$$\begin{aligned}
H\bigl(\phi(\alpha)\bigr) & & &\ge C \cdot H(\alpha)^d \\
H\bigl(\phi^2(\alpha)\bigr) &\ge C \cdot H\bigl(\phi(\alpha)\bigr)^d & &\ge C^{1+d} \cdot H(\alpha)^{d^2} \\
H\bigl(\phi^3(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^2(\alpha)\bigr)^d & &\ge C^{1+d+d^2} \cdot H(\alpha)^{d^3} \\
&\vdots & &\vdots \\
H\bigl(\phi^n(\alpha)\bigr) &\ge C \cdot H\bigl(\phi^{n-1}(\alpha)\bigr)^d & &\ge C^{1+d+d^2+\cdots+d^{n-1}} \cdot H(\alpha)^{d^n}
\end{aligned}$$

Now suppose that α is periodic with period n, so $\phi^n(\alpha) = \alpha$. Then we get

$$H(\alpha) = H\bigl(\phi^n(\alpha)\bigr) \ge C^{(d^n-1)/(d-1)} H(\alpha)^{d^n}.$$

A little bit of algebra yields

$$H(\alpha) \le C^{-1/(d-1)}.$$

This proves that the rational periodic points have bounded height, hence there are only finitely many of them. QED

Rational Periodic Points

All right, we now know that $\phi(z)$ has only finitely many rational periodic points. This raises the question:

Question: How many rational periodic points can $\phi(z)$ have?

If we don't restrict the degree of ϕ, then we can get as many as we want. Simply take $\phi(z)$ to have large degree, set

$$\phi(0)=1, \quad \phi(1)=2, \quad \phi(2)=3, \quad \ldots, \quad \phi(n-1)=0,$$

and treat these as n linear equations for the coefficients of ϕ.

Hence to be an interesting question, we must restrict attention to rational functions of a fixed degree.

Conjecture—Uniform Boundedness of Rational Periodic Points (Morton-Silverman) Fix an integer $d \geq 2$. Then there is a constant $P(d)$ so that every rational function $\phi(z) \in \mathbb{Q}(z)$ of degree d has at most $P(d)$ rational periodic points.

Rational Periodic Points of $\phi(z) = z^2 + c$

Even for very simple families of functions, for example

$$\phi_c(z) = z^2 + c,$$

very little is known about the allowable periods for rational periodic points. Here is what's known in this case:

Theorem.

(a) There are (many) values of c such that the polynomial $\phi_c(z)$ has a rational periodic point of period 1, and similarly for period 2 and period 3.

(b) (Morton) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 4.

(c) (Flynn, Poonen, Schaefer) The polynomial $\phi_c(z)$ cannot have a rational periodic point of period 5.

(d) It is not known if $\phi_c(z)$ can have rational periodic points of period 6 or greater, although Poonen has conjectured that it cannot.

4. Integers and Wandering Points

Number theorists like rational numbers, but their first love is the set of integers

$$\dots,-4,-3,-2,-1,0,1,2,3,4,\dots.$$

The orbit of a rational number α consists of rational numbers, so it is natural to ask how often those rational numbers can be integers.

Question: Can an orbit $\mathcal{O}_\phi(\alpha)$ contain infinitely many integers?

The obvious answer is **Yes**, of course it can. For example, take $\phi(z) = z^2+1$ and $\alpha = 1$. More generally, if $\phi(z)$ is any polynomial

$$\phi(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \qquad \text{with } a_d,\dots,a_0 \in \mathbb{Z}$$

and if $\alpha \in \mathbb{Z}$, then clearly

$$\mathcal{O}_\phi(\alpha) \subset \mathbb{Z}.$$

Are there any other possibilities?

Rational Functions with Polynomial Iterate

Here is an example of a nonpolynomial with an orbit containing infinitely many integer points. Let

$$\phi(z) = \frac{1}{z^d} \quad \text{and let} \quad \alpha \in \mathbb{Z}.$$

Then

$$\mathcal{O}_\phi(\alpha) = \left\{ \alpha^{-d}, \alpha^{d^2}, \alpha^{-d^3}, \alpha^{d^4}, \ldots \right\}.$$

In some sense, this is not a new example, since $\phi^2(z) = z^{d^2}$ is a polynomial. In principle, the same thing happens if some higher iterate of ϕ is a polynomial, but it turns out this cannot occur.

Theorem. If $\phi^n(z)$ is a polynomial, then already $\phi^2(z)$ is a polynomial.

The proof of this theorem is not hard if you know the formula

$$2d - 2 = \sum \bigl(e_\alpha(\phi) - 1 \bigr)$$

for maps of degree d from the 2-sphere to itself, where $e_\alpha(\phi)$ is the ramification index of ϕ at α. I leave the proof as an exercise.

Integer Points in Wandering Orbits

If we rule out the trivial counterexamples, then orbits cannot contain many integer points.

Theorem. (Silverman) Assume that $\phi^2(z)$ is not a polynomial. Then an orbit $\mathcal{O}_\phi(\alpha)$ can contain only finitely many integers.

- The proof is an adaptation of Siegel's proof that curves of genus $g \geq 2$ have only finitely many integer points.
- However, the proof is somewhat more complicated due to the fact that the map ϕ is always ramified, while Siegel was able to use unramified covering maps of curves.
- Ultimately the proof reduces to a Diophantine approximation problem.
- For particular functions and orbits it is sometimes possible to give an elementary proof of finiteness, but I don't know a general proof that does not ultimately rely on Roth's theorem or one of its variants.

Integer-Like Points in Wandering Orbits

- It is possible to give a stronger, and more striking, description of the extent to which wandering points fail to be integral.
- Fix an initial number $\alpha \in \mathbb{Q}$ and write its orbit as

$$\phi^n(\alpha) = \frac{a_n}{b_n} \in \mathbb{Q} \qquad \text{for } n = 0, 1, 2, 3 \ldots.$$

- Notice that $\phi^n(\alpha)$ is an integer if and only if $|b_n| = 1$. So the previous theorem says that $|b_n| \to \infty$ as $n \to \infty$.

Theorem. (Silverman) Assume that neither $\phi^2(z)$ nor $1/\phi^2(z^{-1})$ are polynomials and that $\alpha \in \mathbb{Q}$ is a wandering point for ϕ. Then

$$\lim_{n\to\infty} \frac{\text{Number of digits in } a_n}{\text{Number of digits in } b_n} = \lim_{n\to\infty} \frac{\log|a_n|}{\log|b_n|} = 1.$$

In other words, as n increases, the numerator a_n and the denominator b_n of $\phi^n(\alpha)$ have approximately the same number of digits!

Integer-Like Points — An Example

We give an example. Let

$$\phi(z) = \frac{z^2-1}{z} = z - \frac{1}{z} \qquad \text{and take } \alpha = 2.$$

$$\begin{array}{rlrr}
\phi(2) = & \frac{3}{2} & \phi^5(2) = & \frac{497941}{257070} \\
\phi^2(2) = & \frac{5}{6} & \phi^6(2) = & \frac{181860254581}{128005692870} \\
\phi^3(2) = & -\frac{11}{30} & \phi^7(2) = & \frac{16687694789137362648661}{23279147893155496537470} \\
\phi^4(2) = & \frac{779}{330} & \phi^8(2) = & -\frac{26343956\cdots77222799937788907979}{38847531\cdots9081347493631827670}
\end{array}$$

A table of values shows the convergence of $\log|a_n|/\log|b_n|$:

$$\begin{array}{l|l|l}
\frac{\log|a_1|}{\log|b_1|} = \frac{0.47}{0.30} = 1.585 & \frac{\log|a_4|}{\log|b_4|} = \frac{2.892}{2.519} = 1.148 & \frac{\log|a_7|}{\log|b_7|} = \frac{22.22}{22.36} = 0.994 \\
\frac{\log|a_2|}{\log|b_2|} = \frac{0.69}{0.77} = 0.898 & \frac{\log|a_5|}{\log|b_5|} = \frac{5.697}{5.410} = 1.053 & \frac{\log|a_8|}{\log|b_8|} = \frac{44.42}{44.58} = 0.996 \\
\frac{\log|a_3|}{\log|b_3|} = \frac{1.04}{1.47} = 0.705 & \frac{\log|a_6|}{\log|b_6|} = \frac{11.26}{11.10} = 1.014 & \frac{\log|a_9|}{\log|b_9|} = \frac{88.91}{89.01} = 0.999
\end{array}$$

5. Final Remarks

- For simplicity of exposition, I have restricted attention to the rational numbers $\mathbb{Q}$ and ordinary integers $\mathbb{Z}$, but all of the results are valid for number fields $K/\mathbb{Q}$ and rings of S-integers R_S in K.
- Also for simplicity I have restricted attention to rational functions of one variable. The reason for this restriction is the fact that the dynamics of multivariable functions are not well understood even over $\mathbb{C}$, much less over $\mathbb{Q}$.
- However, Northcott's theorem is true: A morphism $\phi : \mathbb{P}^N \to \mathbb{P}^N$ has only finitely many rational periodic points.
- And conjecturally, if K is a number field and if $\phi : \mathbb{P}^N \to \mathbb{P}^N$ is a morphism of degree d, then the number of K-rational periodic points of ϕ is bounded solely in terms d, N, and $[K : \mathbb{Q}]$.

Preview of Lectures II and III

We have only touched the surface of the arithmetic study of dynamical systems. During the next two lectures I will delve more deeply into the subject, included a description of several important theorems and a discussion of a number of fascinating conjectures.

Lecture II. Wednesday, April 6, 2005

Arithmetic Dynamics: Periodic Rationals and Wandering Integers

- Reduction of maps and orbits modulo p and an alternative proof of Northcott's theorem.
- A sketch of the proof that wandering orbits contain only finitely many integer points.

Lecture III. Thursday, April 7, 2005

Further Topics in Arithmetic Dynamics

- Canonical Heights in Dynamics
- p-adic Dynamics
- Moduli Spaces for Dynamical Systems

Arithmetic Dynamics: Periodic Rationals and Wandering Integers Lecture II

Joseph H. Silverman

Brown University

<jhs@math.brown.edu>

Frontier Lectures

Texas A&M, Monday, April 4–7, 2005

6. Periodic Points and Multipliers

Attracting and Repelling Fixed Points

- Suppose that α is a fixed point of $\phi(z)$.
- Then the Taylor expansion of $\phi(z)$ around α looks like

$$\phi(z) = \alpha + \lambda_\alpha(z-\alpha) + \nu_\alpha(z-\alpha)^2 + \cdots.$$

- The number $\lambda_\alpha = \phi'(\alpha)$ is called the *multiplier of ϕ at α.*
- If $|\lambda_\alpha| > 1$, then ϕ tends to push points near α away from one another, so we say that α is a *repelling point of ϕ.*
- Similarly, if $|\lambda_\alpha| < 1$, then ϕ tends to pull together points that are near to α, so we say that α is an *attracting point of ϕ.*

Multiplier	*Name of Point*	*Location*
$\lvert\lambda_\alpha\rvert > 1$	α is repelling	$\alpha \in \mathcal{J}(\phi)$
$\lvert\lambda_\alpha\rvert = 1$	α is neutral	
$\lvert\lambda_\alpha\rvert < 1$	α is attracting	$\alpha \in \mathcal{F}(\phi)$

Attracting and Repelling Periodic Points

- More generally, if α is a periodic point of period n, then α is a fixed point of ϕ^n and we define the *multiplier* λ_α *of* ϕ *at* α using the Taylor expansion of $\phi^n(z)$:

$$\phi^n(z) = \alpha + \lambda_\alpha(z-\alpha) + \nu_\alpha(z-\alpha)^2 + \cdots .$$

- Thus α is a *repelling*, *neutral*, or *attracting* periodic point of ϕ depending on whether

$$|\lambda_\alpha| > 1, \qquad |\lambda_\alpha| = 1, \qquad \text{or} \qquad |\lambda_\alpha| < 1, \quad \text{respectively.}$$

- The repelling periodic points are in the Julia set $\mathcal{J}(\phi)$ and the attracting periodic points are in the Fatou set $\mathcal{F}(\phi)$.

Theorem. (Fatou, Julia) Let $\phi(z) \in \mathbb{C}(z)$ have degree $d \ge 2$.
(a) $\phi(z)$ has only finitely many nonrepelling periodic points.
(b) The repelling periodic points are dense in the Julia set $\mathcal{J}(\phi)$.

7. Reduction Modulo p

Reduction of Maps and of Points Modulo p

- Let p be a prime. We recall that the integers modulo p form a field $\mathbb{F}_p$ of p elements and that there is a natural *reduction modulo p* homomorphism $\mathbb{Z} \to \mathbb{F}_p$ whose kernel is the ideal generated by p. We denote this homomorphism by $a \mapsto \tilde{a}$.
- Let $\alpha = a/b \in \mathbb{Q}$ be a rational number. The *reduction of α modulo p* is defined by

$$\tilde{\alpha} = \widetilde{a/b} = \begin{cases} \tilde{a}\tilde{b}^{-1} & \text{if } p \nmid b, \\ \infty & \text{if } p \mid b. \end{cases}$$

  The reciprocal $\tilde{b}^{-1}$ of $\tilde{b}$ exists in the field $\mathbb{F}_p$ provided that $p \nmid b$.
- The *reduction of ϕ modulo p* is defined in the obvious way:

$$\tilde{\phi}(z) = \frac{\tilde{a}_d z^d + \tilde{a}_{d-1} z^{d-1} + \cdots + \tilde{a}_1 z + \tilde{a}_0}{\tilde{b}_e z^e + \tilde{b}_{e-1} z^{e-1} + \cdots + \tilde{b}_1 z + \tilde{b}_0} \in \mathbb{F}_p(z).$$

Good and Bad Reduction of Maps

- Reduction modulo p is one of the most powerful tools in the number theorist's arsenal.
- However, although some maps behave well when reduced modulo p, others behave badly.
- Here are some examples of bad behavior modulo 5:

$$\phi(z) = 5z^2 + 10z + 1 \qquad \tilde{\phi}(z) = \tilde{1} \text{ is constant!}$$

$$\phi(z) = \frac{2z^2+3z}{z+10} \qquad \tilde{\phi}(z) = \frac{\tilde{2}z^2+\tilde{3}z}{z} = \tilde{2}z+\tilde{3} \text{ has degree 1!}$$

$$\phi(z) = \frac{z^2-2z-3}{z^2+4z-16} \qquad \tilde{\phi}(z) = \frac{(z+\tilde{1})(z-\tilde{3})}{(z+\tilde{2})(z-\tilde{3})} = \frac{z+\tilde{1}}{z+\tilde{2}} \text{ has degree 1.}$$

Definition. The map $\phi(z)$ has *good reduction modulo p* if

$$\bigl(\text{degree of } \phi(z)\bigr) = \bigl(\text{degree of } \tilde{\phi}(z)\bigr).$$

The examples given above have bad reduction modulo 5.

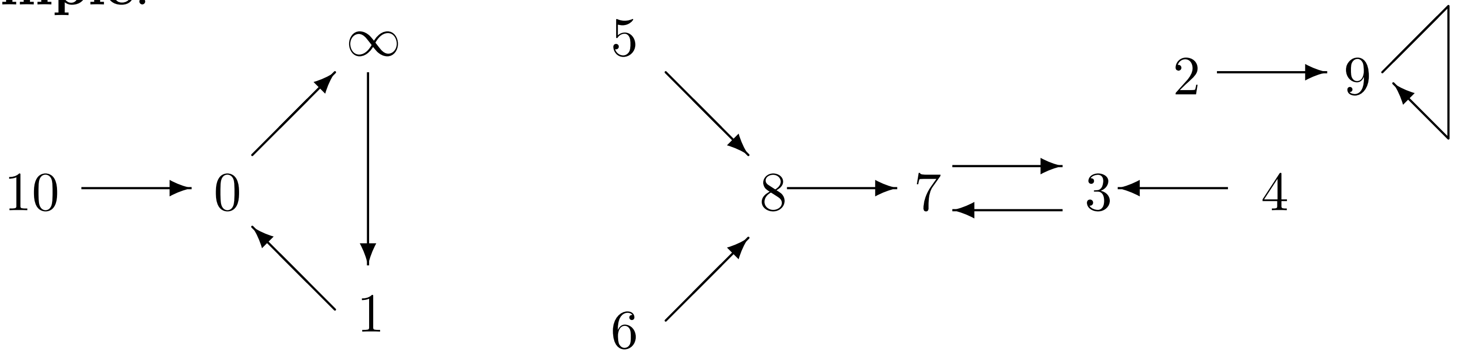
Dynamics of $\tilde{\phi}$ on $\mathbb{F}_p$

- A rational function $\tilde{\phi}(z) \in \mathbb{F}_p(z)$ gives a map

$$\tilde{\phi} : \mathbb{F}_p \cup \{\infty\} \longrightarrow \mathbb{F}_p \cup \{\infty\}.$$

- We can iterate $\tilde{\phi}$ and study the dynamics of $\tilde{\phi}$ on $\mathbb{F}_p \cup \{\infty\}$.

Example:



Iteration of $\phi(z) = \dfrac{z^2 - 1}{z^2}$ on $\mathbb{F}_{11}$

8. Maps with Good Reduction

- Every point in $\mathbb{F}_p$ is preperiodic for $\tilde{\phi}$, since there are only finitely many points.
- For any particular p, it is only a finite amount of work to describe the dynamics of $\tilde{\phi}$ on $\mathbb{F}_p$.
- One might hope that the dynamics of $\tilde{\phi}$ on $\mathbb{F}_p$ provides information about the dynamics of ϕ on $\mathbb{Q}$.
- This is not always the case, but the following proposition shows that it is true if the rational map has good reduction.

Proposition. Suppose that ϕ has good reduction modulo p.

(a) For all $\alpha \in \mathbb{Q}$ and all $n \geq 0$,

$$\widetilde{\phi^n(\alpha)} = \tilde{\phi}^n(\tilde{\alpha}).$$

(b) If $\alpha \in \mathbb{Q}$ is periodic for ϕ and has period n, then $\tilde{\alpha}$ is periodic for $\tilde{\phi}$ and has period m satisfying $m|n$.

The Periodic Point Reduction Theorem

If a map has good reduction, then the dynamical properties of $\tilde{\phi}$ closely reflect those of ϕ. The following is an amalgamation of results due to (at least) Li, Morton-Silverman, Narkiewicz, Pezda, and Zieve.

Theorem. Let $\phi(z) \in \mathbb{Q}(z)$ be a rational map of degree $d \geq 2$ with good reduction at p and let $\alpha \in \mathbb{Q}$ be a periodic point of ϕ. Set

n	the period of the point α for ϕ
m	the perioid of the point $\tilde{\alpha}$ for $\tilde{\phi}$
r	the order of the multiplier $\lambda_{\tilde{\alpha}}$ in $\mathbb{F}_p^*$

In other words, r is the smallest positive integer so that $\lambda_{\tilde{\alpha}}^r = 1$ in $\mathbb{F}_p$.

Then one of the following is true:

$$n = m$$

$$n = mr$$

$$n = mrp \quad \text{with } p = 2 \text{ or } p = 3.$$

Remark. This result is very powerful because m and r are bounded.

Applying the Periodic Point Reduction Theorem — Examples

Example 1: Let $\phi(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_0 \in \mathbb{Z}[z]$.

- Suppose that the leading coefficient $\underline{a_d \text{ is odd}}$.
- Let $\alpha \in \mathbb{Q}$ be a periodic point of ϕ.
- Notice that $\phi(z)$ has good reduction at 2.
- Further, there are only two points in $\mathbb{F}_2$, so either $\tilde{\alpha}$ is fixed by $\tilde{\phi}$ ($m = 1$) or $\tilde{\alpha}$ has period 2 ($m = 2$).
- Similarly, the multiplier $\lambda_{\tilde{\alpha}}$ is either 1 (so $r = 1$) or 0 (in which case r is undefined).
- The reduction theorem tells us that the period n of α is either 1, 2, or 4. (In fact, only 1 and 2 are possible.)

Example 2: Let $\phi(z) = \dfrac{az^2 + bz + c}{z^2}$ with $a, b, c \in \mathbb{Z}$ and c odd.

- Now m may equal 1, 2, or 3, so n might be 1, 2, 3, or 6.
- A more detailed analysis (exercise!) shows that 6 is not possible.

A General Periodic Point Bound

Corollary. Let $\phi(z) \in \mathbb{Q}(z)$ be a rational map of degree $d \geq 2$, let $\alpha \in \mathbb{Q}$ be a periodic point of ϕ of period n, and let p be the smallest prime for which ϕ has good reduction. Then

$$n \leq p^3 - p. \qquad (\text{If } p \geq 5, \text{ then } n \leq p^2 - 1.)$$

Proof.

- The map $\tilde{\phi}$ is a permuation of $\mathbb{F}_p \cup \{\infty\}$, so the period m of $\tilde{\alpha}$ is at most $p + 1$.
- Similarly, the order r of $\lambda_{\tilde{\alpha}}$ divides the order of the group $\mathbb{F}_p^*$, so $r \leq p - 1$.
- Now apply the theorem to conclude that

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

If $p \geq 5$, the theorem gives the upper bound is $mr \leq p^2 - 1$. QED

N.B. The bound in the corollary depends on ϕ, so it is not uniform.

Primes of Bad Reduction

- In order to apply the corollary, it remains to determine at which primes ϕ has bad reduction.
- Write $\phi(z)$ as a quotient of polynomials
$$\phi(z) = \frac{F(z)}{G(z)} = \frac{a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0}{b_e z^e + b_{e-1} z^{e-1} + \cdots + b_1 z + b_0}$$
with $a_0, \ldots, a_d, b_0, \ldots, b_e \in \mathbb{Z}$ and $\gcd(a_0, \ldots, a_d, b_0, \ldots, b_e) = 1$.
- Then $\phi(z)$ has good reduction at all primes that do not divide the *resultant* $\operatorname{Res}(F,G)$, where $\operatorname{Res}(F,G)$ is a certain universal polynomial expression involving $a_0, \ldots, a_d, b_0, \ldots, b_e$.
- In particular, $\phi(z)$ has good reduction at all but finitely many primes, and the smallest prime of bad reduction may be bounded in terms of the coefficients of ϕ.

Example. $\phi(z) = \dfrac{F(z)}{G(z)} = \dfrac{4z^2 + 3z - 7}{5z^3 - 4z + 2}$ satisfies $\operatorname{Res}(F,G) = -3417$.

$3417 = 3 \cdot 17 \cdot 67$, so ϕ has good reduction except at $p = 3$, 17 and 67.

The Periodic Point Reduction Theorem — Proof Sketch

- Replacing $\phi(z)$ by $\phi(z+\alpha)-\alpha$, we may assume that $\alpha = 0$.
- Replacing ϕ by ϕ^m, we may assume that $\tilde{\alpha}$ is a fixed point of $\tilde{\phi}$ (i.e., $m=1$).
- Then the Taylor expansion of $\phi(z)$ around $\alpha = 0$ has the form

$$\phi(z) = \mu + \lambda z + \cdots \qquad \text{with } \mu \equiv 0 \pmod{p} \text{ and } \lambda \equiv \lambda_{\tilde{\alpha}} \pmod{p}.$$

- If $\mu = 0$, then $n = 1$ and we're done. Assume that $\mu \ne 0$ and $n > 1$.
- The n^{th} iterate of ϕ looks like

$$\phi^n(z) = (1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1})\mu + \lambda^n z + \cdots .$$

- We have $\phi^n(0) = 0$ by assumption and $\mu \ne 0$, so $\lambda \ne 1$ and $\lambda^n = 1$.
- Hence $\lambda_{\tilde{\alpha}}^n \equiv \lambda^n = 1 \pmod{p}$, so r divides n.
- If $n = r$, we are done, so assume $n > r$.
- Replacing ϕ by ϕ^r, we may assume that $\lambda_{\tilde{\alpha}} = 1$ (i.e., $r = 1$).

Periodic Point Reduction Theorem — Proof Sketch (cont.)

- Consider the value of $\phi^n(0)$ modulo $p\mu$. Note that

  $$1 + \lambda + \lambda^2 + \cdots + \lambda^{n-1} \equiv 1 + \lambda_{\tilde{\alpha}} + \lambda_{\tilde{\alpha}}^2 + \cdots + \lambda_{\tilde{\alpha}}^{n-1} \equiv n \pmod{p}.$$

  Hence

  $$0 = \phi^n(0) \equiv n\mu \pmod{p\mu}, \qquad \text{so } p \text{ divides } n.$$

- If $n = p$, we are done. Otherwise replace ϕ by ϕ^p and n by n/p and repeat to conclude again that p divides n.
- We eventually conclude that n is a power of p.
- Tracing back the substitutions, this proves that either

  $$n = m \quad \text{or} \quad n = mr \quad \text{or} \quad n = mrp^k \text{ for some power } k.$$

- In order to prove a bound for the exponent k, one must use the first three terms

  $$\phi(z) = \mu + \lambda z + \nu z^2 + \cdots$$

  and perform a more careful analysis. QED

9. A Soupçon of Diophantine Approximation

- To study integer points in the orbits of wandering points, we ultimately need results from the theory of *Diophantine Approximation.*
- Diophantine approximation seeks to answer the question:

How closely can an irrational number
be approximated by rational numbers?

- The trivial answer is "arbitrary closely," since $\mathbb{Q}$ is dense in $\mathbb{R}$.
- A refined question quantifies a relationship between the "closeness" of the approximation and the "complexity" of the rational number.

Theorem. (Dirichlet) Let $\beta \in \mathbb{R}$ be an irrational number. 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. Use the pigeon-hole principle. (Exercise.)

Roth's Theorem

- Inequalities in the other direction are much more difficult.
- Indeed, some real numbers can be much better approximated than others.
- Recall that a number β is called an *algebraic number* if it is the root of a polynomial having rational coefficients.
- The set of algebraic numbers is a field.
- Roth received a Fields' medal in 1950 for his proof that algebraic numbers cannot be approximated significantly better than specified in Dirichlet's theorem.

Theorem. (Roth) Let α be an irrational algebraic number and let $\epsilon > 0$. Then there is a positive constant $\kappa = \kappa(\alpha, \epsilon) > 0$ so that

$$\left|\frac{a}{b} - \beta\right| \geq \frac{\kappa}{b^2} \qquad \text{for all rational numbers } \frac{a}{b} \in \mathbb{Q}.$$

10. Integer Points in Wandering Orbits

Recall the theorem stating that numerators and denominators in wandering orbits have approximately the same number of digits.

Theorem. Write $\phi^n(\alpha) = a_n/b_n \in \mathbb{Q}$. Assume that neither $\phi^2(z)$ nor $1/\phi^2(z^{-1})$ are polynomials and that $\alpha \in \mathbb{Q}$ is a wandering point for ϕ. Then

$$\lim_{n\to\infty} \frac{\text{Number of digits in } a_n}{\text{Number of digits in } b_n} = \lim_{n\to\infty} \frac{\log|a_n|}{\log|b_n|} = 1.$$

Rough Idea for a Proof.

- Suppose that $|a_n|$ is much larger than $|b_n|$.
- This means that $\phi^n(\alpha) = a_n/b_n$ is very close to the point at ∞.
- Hence $\alpha = a_1/b_1 \in \mathbb{Q}$ is very close(?) to some point $\beta \in \phi^{-n}(\infty)$, i.e., to some point β satisfying $\phi^n(\beta) = \infty$.
- Maybe(?) the rational number α is so close to the algebraic number β that it contradicts Roth's theorem.
- *Problem*: β depends on n, but Roth's theorem deals with a single β.

Integer Points in Wandering Orbits — Proof of Main Theorem

Better Idea for a Proof (but still not quite right!).

- Suppose that $|a_n|$ is much larger than $|b_n|$ for infinitely many n.
- More precisely, fix $\delta > 0$ and suppose that
$$|a_n|^{1-\delta} \ge |b_n| \quad \text{for infinitely many } n.$$
- Fix an integer $m \ge 6/\delta$. In particular, m is independent of n.
- The idea is to find an algebraic number in $\phi^{-m}(\infty)$ that is too close to the rational number $\phi^{n-m}(\alpha)$.
- We fix a point $\beta \in \phi^{-m}(\infty)$ that is close to $\phi^{n-m}(\alpha)$ for infinitely many n and compute:

Integer Points in Wandering Orbits

$$
\begin{aligned}
\frac{1}{|a_n|^{\delta}} &\geq \left|\frac{b_n}{a_n}\right| = |\phi^n(\alpha)|^{-1} && \text{since } |a_n|^{1-\delta} \geq |b_n|, \\
&\approx \text{dist. from } \phi^n(\alpha) \text{ to } \infty, && \\
&\approx \text{dist. from } \phi^n(\alpha) \text{ to } \phi^m(\beta), && \text{since } \phi^m(\beta) = \infty, \\
&\approx \text{dist. from } \phi^{n-m}(\alpha) \text{ to } \beta, && \text{assuming } \phi \text{ is unramified}, \\
&\approx \left|\frac{a_{n-m}}{b_{n-m}} - \beta\right|, && \text{since } \phi^{n-m}(\alpha) = \frac{a_{n-m}}{b_{n-m}}, \\
&\geq \frac{\kappa}{b_{n-m}^3} && \text{Roth's Theorem (with exponent 3)}, \\
&\geq \frac{\kappa}{H(\phi^{n-m}(\alpha))^3}, && \text{where recall } H(a/b) = \max\{|a|, |b|\}, \\
&\approx \frac{\kappa}{H(\phi^n(\alpha))^{3/d^m}}, && \text{property of heights}, \\
&= \frac{\kappa}{|a_n|^{3/d^m}}, && \text{since } |a_n| \geq |b_n|, \\
&\geq \frac{\kappa}{|a_n|^{\delta/2}}, && \text{since } m \text{ satisfies } d^m > 6/\delta.
\end{aligned}
$$

Completion of the "Proof"

- We conclude that $|a_n| \le (\text{Constant})^{2/\delta}$, so there are only finitely many possibilities for a_n.
- Similarly $|b_n| \le |a_n|^{1-\delta}$ is bounded. Hence there are only finitely many possibilities for $\phi^n(\alpha)$.
- But α is a wandering point, so there are only finitely many values of n with $|a_n|^{1-\delta} \ge |b_n|$. Equivalently,

$$\frac{\log|a_n|}{\log|b_n|} \le \frac{1}{1-\delta} \qquad \text{for all sufficiently large } n.$$

- This is true for all $\delta > 0$, so we have proven (well, not quite) that

$$\limsup_{n\to\infty} \frac{\log|a_n|}{\log|b_n|} \le 1.$$

- Repeating the argument using $\psi(z) = 1/\phi(z^{-1})$ and $1/\alpha$ gives the reciprocal estimate and completes the proof.

What's Wrong with the Proof and How to Fix It

- *Problem.* The map ϕ may be ramified at points in the orbit of α, in which case ϕ^{-1} does not (even approximately) preserve distances.
- Intuition: If locally ϕ looks like $\phi(z) = A + B(z-\alpha)^e + \cdots$, so $\phi(\alpha) = A$ and ϕ is ramified at α, then distances get raised to a power,
$$\bigl|\phi(\beta) - \phi(\alpha)\bigr| \approx |B| \cdot |\beta - \alpha|^e.$$
- However, as long as the ramification exponent e is not too large, then the proof still works.
- The final ingredient is to replace $\phi(z)$ with $\phi^k(z)$ for an appropriately chosen k and break the orbit of α up into suborbits.
- Note that somewhere we must use the assumption that $\phi(z)$ is not a polynomial. One proves that under this assumption, even if $\phi(z)$ itself if highly ramified at some points, taking the iterate $\phi^k(z)$ has the effect of spreading out the ramification sufficiently to allow the proof to work.