Course Outline and Project Descriptions for a Course on Arithmetic Dynamics Arizona Winter School March 13–17, 2010

JOSEPH H. SILVERMAN
jhs@math.brown.edu

What is Arithmetic Dynamics?

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

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

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. Consider the polynomial $\varphi(z) = z^2 - 1$ as a map $\mathbb{Z} \to \mathbb{Z}$. Then

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

so 1 is preperiodic, while 0 and -1 are periodic. It is easy to see that every other element of $\mathbb{Z}$ is wandering, since $\lim_{n\to\infty}\bigl|\varphi^n(z)\bigr| = \infty$, and more generally, the only φ-preperiodic points in $\mathbb{Q}$ are $\{-1, 0, 1\}$.

Date: November 25, 2009.
1991 *Mathematics Subject Classification.* 37Pxx.
Key words and phrases. arithmetic dynamical systems.
This project supported by NSF DMS-0650017 and DMS-0854755.

(Do you see why?) On the other hand, $\varphi : \mathbb{C} \to \mathbb{C}$ has infinitely many complex preperiodic points.

Arithmetic Dynamics is the study of arithmetic properties of dynamical systems. To give a flavor of arithmetic dynamics, here are two motivating questions. 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 set of $\mathbb{Q}$-rational periodic or preperiodic points of φ?

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

These are dynamical analogues of important results in the theory of Diophantine equations, where preperiodic points correspond to torsion points on elliptic curves and integer points in orbits correspond to points on elliptic curves having integer coordinates.

Course Summary

Lecture I: *Background Material: Geometry, Classical Dynamics, and Diophantine Equations*

As the title indicates, this introductory lecture will summarize, without proof, those topics from (algebraic) geometry, complex dynamics, and the theory of Diophantine equations that will be needed for subsequent lectures. Among the topics covered will be the complex projective line, the Riemann–Hurwitz formula, the Fatou and Julia sets, height functions, and Diophantine approximation.

Lecture II: *Preperiodic Points and Height Functions*

This lecture is devoted to arithmetic properties of preperiodic points. It will include a proof of Northcott's theorem that there are only finitely many preperiodic points defined over a given number field, the construction of canonical heights, and a discussion of the uniform boundedness conjecture.

Lecture III: *Arithmetic Dynamics of Maps with Good Reduction*

An algebraic object has "good reduction modulo p" if the reduction retains the principal properties of the original object. I will define good reduction for rational maps and prove an important theorem describing what happens to a periodic point when it is reduced modulo a prime of good reduction. A corollary is an alternative proof of Northcott's theorem.

Lecture IV: *Integer Points in Orbits*

In the final lecture we take up the problem alluded to earlier of integer points in orbits. I will sketch a proof that the orbit of a rational wandering point contains only finitely many integers, except in those trivial cases where there are infinitely many. Of course, it's important here to have a good description of the trivial cases!

Projects

The following is a *tentative* list of projects for the AWS lecture series on arithmetic dynamics. It is followed by a detailed description of each project.

- Dynamics over finite fields
- Orbits with many integer points
- Primes, prime support, and primitive divisors in orbits

Project I: Dynamics over finite fields.
We consider a rational map $\varphi(z) \in \mathbb{F}_p(z)$ with coefficients in 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 $\mathrm{Per}\big(\tilde{\varphi}_p, \mathbb{P}^1(\mathbb{F}_p)\big)$ is "large," does that imply that $\mathrm{Per}\big(\varphi, \mathbb{P}^1(\mathbb{Q})\big)$ 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.
It is not hard to show that an orbit may contain arbitrarily many integers, but if we restrict to rational maps φ given by an "affine minimal equation," then it is conjectured that the number of integer points should be bounded in terms of the degree of φ.

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

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

(Warm-up: Prove that that $M(d) \ge 2d+2$, and 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 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. *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.)*

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 Rafe Jones 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. (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. 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. Patrick Ingram and I 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. However, the proof relies on Roth's theorem, so it 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