

Arithmetic Dynamics,
Arithmetic Geometry,
and Number Theory

Joseph H. Silverman

Brown University

MAGNTS (Midwest Arithmetic Geometry and
Number Theory Series)

October 12–13, 2019

What is Arithmetic Dynamics?

Arithmetic Geometry: Study solutions to polynomial equations (points on algebraic varieties) over non-algebraically closed fields.

(Discrete) Dynamical Systems: Study orbits of points under iteration of a function.

Arithmetic Dynamics: Study number theoretic properties of orbits of points on algebraic varieties.

A lot of arithmetic dynamics comes by analogy from arithmetic geometry. Sometimes the analogy is quite direct, sometimes less so, and there are parts of arithmetic geometry that still lack dynamical analogues. Today's talk will be a survey of what arithmetic dynamics is all about, with details on its connections to the arithmetic geometry that we all know and love. Then in tomorrow's talk I'll delve more deeply into some specific topics.

In Arithmetic Geometry We Study ...

Elliptic curves / higher dim'l abelian varieties

Torsion points

Torsion points defined over a fixed K .

Fields generated by torsion points.

Image of Galois $G(\bar{K}/K) \rightarrow \text{Aut}(A_{\text{tors}})$.

Torsion points on subvarieties ($\dim A \geq 2$).

Mordell–Weil groups

Rank of K -rational points ...

for fixed A and varying K ;

for fixed K and varying A .

Intersection with subvarieties ($\dim A \geq 2$).

Moduli spaces of elliptic curve and abelian varieties

Geometry of moduli spaces, e.g., $X_0(N)$ and \mathcal{A}_g .

Distribution of “special” points (CM moduli).

Modular forms, L -series, Hecke operators, ...

In Discrete Dynamics We Study ...

A Space X , a Self-Map $f : X \rightarrow X$, and Iteration

$$f^{\circ n} = \underbrace{f \circ f \circ \cdots \circ f}_{n\text{th iterate of } f}.$$

Orbit of $x \in X$

$$\mathcal{O}_f(x) := \{x, f(x), f^{\circ 2}(x), f^{\circ 3}(x), \dots\}.$$

Preperiodic Point

$x \in X$ with finite orbit $\mathcal{O}_f(x)$.

Periodic Point

$x \in X$ with $f^{\circ n}(x) = x$ for some $n \geq 1$.

Moduli spaces of dynamical systems

Classify (X, f) up to “dynamical equivalence.”

Post-critically finite (**PCF**) maps

In Discrete Dynamics We Study ...

A Space X , a Self-Map $f : X \rightarrow X$, and Iteration

$$f^{\circ n} = \underbrace{f \circ f \circ \cdots \circ f}_{n\text{th iterate of } f}.$$

Orbit of $x \in X$ \iff “Mordell–Weil group”

$$\mathcal{O}_f(x) := \{x, f(x), f^{\circ 2}(x), f^{\circ 3}(x), \dots\}.$$

Preperiodic Point \iff “torsion point”

$$x \in X \text{ with finite orbit } \mathcal{O}_f(x).$$

Periodic Point \iff “torsion point”

$$x \in X \text{ with } f^{\circ n}(x) = x \text{ for some } n \geq 1.$$

Moduli spaces of dynamical systems

Classify (X, f) up to “dynamical equivalence.”

Post-critically finite (**PCF**) maps \iff “**CM points**”

Two Examples

Let A be an abelian variety and $P \in A$. Then

P is a torsion point $\iff P$ is preperiodic for doubling.

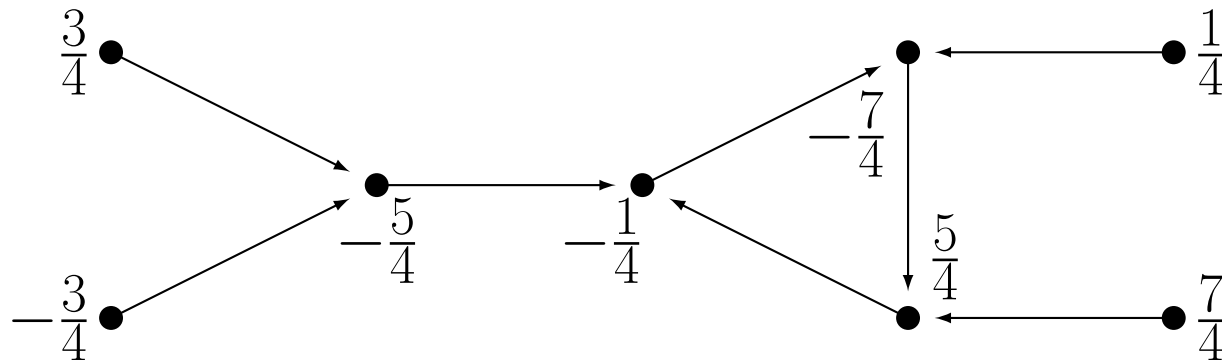
In other words, $A_{\text{tors}} = \text{PrePer}(A, [2])$.

Let $T_P(Q) = Q + P$. Then $\mathbb{Z}P = \mathcal{O}_{T_P}(0) \cup \mathcal{O}_{T_{-P}}(0)$.

Let $f(x) \in \mathbb{Q}(x)$ be the polynomial

$$f(x) = x^2 + \frac{29}{16}.$$

Then f has 8 preperiodic points in \mathbb{Q} :



That's a lot of rational preperiodic points!!

Uniform Boundedness in Arithmetic Geometry

Let E/\mathbb{Q} be an elliptic curve.

Theorem. (Mazur) $E(\mathbb{Q})$ contains at most 16 torsion points.

More generally:

Uniform Boundedness Theorem. (Mazur, Kamienny, Merel) Let K/\mathbb{Q} be a number field and E/K an elliptic curve. Then

$$\#E(K)_{\text{tors}} \leq C([K : \mathbb{Q}]).$$

And even more generally:

Uniform Boundedness Conjecture. Let K/\mathbb{Q} be a number field and A/K an abelian variety. Then

$$\#A(K)_{\text{tors}} \leq C([K : \mathbb{Q}], \dim(A)).$$

Uniform Boundedness in Arithmetic Dynamics

Recall our dictionary:

Mordell–Weil group \leftrightarrow orbit of a point

torsion point \leftrightarrow preperiodic point

Dynamical Uniform Boundedness Conjecture. (Morton–Silverman) Let K/\mathbb{Q} be a number field, and $f : \mathbb{P}^N \rightarrow \mathbb{P}^N$ a morphism of degree ≥ 2 . Then

$$\# \text{PrePer}(f, \mathbb{P}^N(K)) \leq C([K : \mathbb{Q}], \deg f, N).$$

- Northcott: $\text{PrePer}(f, \mathbb{P}^N(\overline{\mathbb{Q}}))$ is a set of bounded ht. Here's a **very** special case that is still far from resolved:

Conjecture. (Poonen) Let $c \in \mathbb{Q}$. Then

$$\# \text{PrePer}(x^2 + c, \mathbb{Q}) \leq 8.$$

- Fakhruddin: Dynamical UBC for $\mathbb{P}^N \implies$ UBC for A

Arithmetic Geometry: Elliptic Modular Curves

To study points of order N on elliptic curves, one looks at the set of pairs

$$Y_1(N) := \left\{ (E, P) : \begin{array}{l} E \text{ is an elliptic curve, and} \\ P \in E_{\text{tors}} \text{ is a point of order } N \end{array} \right\}$$

As is well known, $Y_1(N)$ has a natural structure as an affine curve, and

$$(E, P) \in Y_1(N)(K) \iff E/K \text{ and } P \in E(K).$$

As usual, we let

$$X_1(N) = \text{smooth completion of } Y_1(N) = Y_1(N) \cup \{\text{cusps}\}.$$

Then Mazur's theorem (and proof) say that

$$N > 16 \iff X_1(N)(\mathbb{Q}) = \{\text{cusps}\}.$$

(True more generally if genus $X_1(N) \geq 1$.)

Dynamical Modular Curves (for $x^2 + c$)

Let $f_c(x) = x^2 + c$

We want to classify pairs

$$Y_1^{\text{dyn}}(N) := \{(\alpha, c) : \alpha \text{ has (formal) period } N \text{ for } f_c\}$$

$Y_1^{\text{dyn}}(N)$ has a natural structure as an affine curve. Let

$$X_1^{\text{dyn}}(N) = \text{smooth completion} = Y_1^{\text{dyn}}(N) \cup \{\text{cusps}\}.$$

Conjecture. $N \geq 4 \implies X_1^{\text{dyn}}(N)(\mathbb{Q}) = \{\text{cusps}\}.$

In other words, for all $c \in \mathbb{Q}$, the map $x^2 + c$ has no \mathbb{Q} -rational points of period 4 or larger. This is true for:

$N = 4$ (Morton), $N = 5$ (Flynn–Poonen–Schaefer),
 $N = 6^*$ (Stoll) *assuming B-SwD for a certain abelian 4-fold.

Remark: $\text{Jac}(X_1^{\text{dyn}}(N))$ tends to be irreducible and have positive MW rank over \mathbb{Q} , so no Eisenstein quotient!

Dynamical Modular Curves (for $x^2 + c$)

The curve $Y_1^{\text{dyn}}(N)$ is given explicitly by the equation

$$\Phi_N^{\text{dyn}}(x, y) := \prod_{d|N} (f_y^{\circ d}(x) - x)^{\mu(N/d)} = 0.$$

The inclusion/exclusion is needed to get rid of points of period smaller than N , just as in the formula for the cyclotomic polynomials. Two complications:

- (1) One needs to prove that $\Phi_N^{\text{dyn}}(x, y)$ is a polynomial.
- (2) Even if $\Phi_N^{\text{dyn}}(\alpha, c) = 0$, it may not be true that α has exact period N for f_c . For example, $c = -\frac{3}{4}$ gives

$$\Phi_1^{\text{dyn}}(x, -\frac{3}{4}) = (2x + 1)(2x - 3), \quad \Phi_2^{\text{dyn}}(x, -\frac{3}{4}) = (2x + 1)^2.$$

Following Milnor, one says that α has *formal period* N .

Theorem. (Bousch) $X_1^{\text{dyn}}(N)$ is geometrically irreducible, and there is an explicit formula for its genus.

Unlikely Intersections in Arithmetic Geometry

Many theorems and conjectures in arithmetic geometry fall into the “unlikely intersection” paradigm:

If an algebraic subvariety has a Zariski dense set of special points, then the subvariety is itself special, i.e., there is a geometric reason that it contains so many special points.

Let A be an abelian variety and $Y \subseteq A$ a subvariety.

Theorem. (Faltings, née Mordell–Lang Conjecture)
Let $\Gamma \subset A$ be a finitely generated subgroup.
If $\overline{\Gamma \cap Y} = Y$, then Y is a finite union of translates of abelian subvarieties of A .

Theorem. (Raynaud, née Manin–Mumford Conj.)
If $\overline{A_{\text{tors}} \cap Y} = Y$, then Y is a finite union of translates of abelian subvarieties of A .

Unlikely Intersections in Arithmetic Dynamics 1

Our dictionary says that:

finitely generated subgroup $\Gamma \rightsquigarrow$ orbit $\mathcal{O}_f(x)$.

Dynamical Mordell–Lang Conjecture.

(Bell, Denis, Ghioca, Tucker) Let X/\mathbb{C} be a smooth projective variety, let $Y \subseteq X$, let $f : X \rightarrow X$ be a morphism, and let $P \in X$. Then

$$\overline{\mathcal{O}_f(P)} \cap Y = Y \implies Y \text{ is periodic for } f.$$

The extensive literature proving special cases includes:

Theorem. Dynamical Mordell–Lang is true if:

- (a) (Xie): $f : \mathbb{A}^2 \rightarrow \mathbb{A}^2$ is a morphism defined over $\overline{\mathbb{Q}}$.
- (b) (Bell-Ghioca-Tucker) $f : X \rightarrow X$ is étale and defined over $\overline{\mathbb{Q}}$, e.g., $f : \mathbb{A}^N \rightarrow \mathbb{A}^N$ is a polynomial automorphism. [Proof uses Skolem–Mahler–Lech method.]

Unlikely Intersections in Arithmetic Dynamics 2

Our dictionary also says that:

torsion subgp $A_{\text{tors}} \iff$ preperiodic pts $\text{PrePer}(f, X)$.

Dynamical Manin–Mumford Conjecture. Let X/\mathbb{C} be a smooth projective variety, let $Y \subseteq X$, and let $f : X \rightarrow X$ be a polarized morphism (\exists ample \mathcal{L} with $f^*\mathcal{L} \cong \mathcal{L}^{\otimes d}$ with $d > 1$). Then

$\overline{\text{PrePer}(f)} \cap Y = Y \implies Y$ is periodic for f .

Ghioca–Tucker: This statement is FALSE!

- There is a partial fix due to Ghioca–Tucker–Zhang.

Arithmetic Geometry: The Image of Galois

Classical Case: Let $f_m(x) = x^m$. We consider cyclotomic fields and their Galois groups,

$$\mathbb{Q}_m := \mathbb{Q}(f_m^{-1}(1)) = \mathbb{Q}(\boldsymbol{\mu}_m), \quad G_m := \text{Gal}(\mathbb{Q}_m/\mathbb{Q}).$$

A fundamental theorem on cyclotomic fields says that

$$\rho_m : G_m \longrightarrow \text{Aut}(\boldsymbol{\mu}_m) = (\mathbb{Z}/m\mathbb{Z})^* \quad \text{is surjective.}$$

Iwasawa theory gives information about the ideal class groups in the tower of fields $\mathbb{Q} \subset \mathbb{Q}_p \subset \mathbb{Q}_{p^2} \subset \mathbb{Q}_{p^3} \dots$

Elliptic Curves: Let E/K and $[m] : E \rightarrow E$. Let

$$K_m := K([m]^{-1}(0)) = K(E[m]), \quad G_m := \text{Gal}(K_m/K).$$

Theorem. (Serre) If E does not have CM, then

$$\text{Image of } \rho_{E,m} : G_m \longrightarrow \text{Aut}(E[m]) = \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

has index that is bounded independent of m .

Arithmetic Dynamics: Arboreal Representations

Let K/\mathbb{Q} be a number field, let

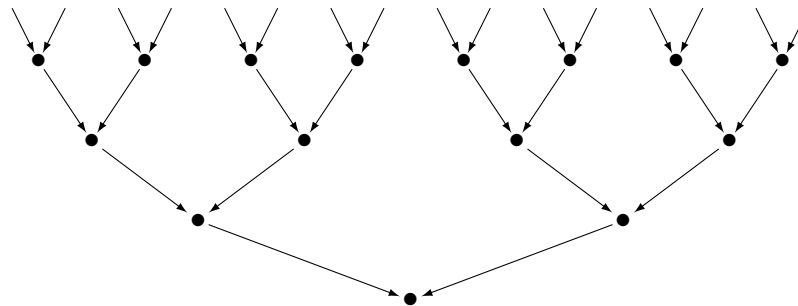
$$f : \mathbb{P}_K^N \rightarrow \mathbb{P}_K^N$$

be a map of degree $d \geq 2$, and let $P \in \mathbb{P}^N(K)$. We look at the **backward orbit**

$$\mathcal{O}_f^-(P) := \{Q \in \mathbb{P}^N(\bar{K}) : Q \in f^{-n}(P) \text{ for some } n \geq 0\}.$$

Assumption: $\#f^{-n}(P) = d^n$ for all $n \geq 0$.

$\mathcal{O}_f^-(P)$ looks like a complete rooted d -ary tree \mathcal{T}_d .



The complete binary inverse image tree \mathcal{T}_2

Key Observation: $\text{Gal}(\bar{K}/K)$ acts on $\mathcal{O}_f^-(P)$, and the action respects the tree structure.

Arboreal Representations — Fundamental Problems

Let

$$K_{f,P} := K(Q : Q \in \mathcal{O}_f^-(P))$$

be the field generated by the inverse orbit of P .

Analogue: Iwasawa tower $K([p]^{-n}(0) : n \geq 1)$.

Natural Question: How big is $\text{Gal}(K_{f,P}/K)$? Note:

$$\text{Gal}(K_{f,P}/K) \hookrightarrow \text{Aut}(\mathcal{T}_d) \cong \varprojlim_{n \rightarrow \infty} \underbrace{\mathcal{S}_d \wr \mathcal{S}_d \wr \cdots \wr \mathcal{S}_d}_{n\text{-fold wreath product}}.$$

Definition: The **Odoni index** is

$$\iota_K(f, P) := [\text{Aut}(\mathcal{T}_d) : \text{Gal}(K_{f,P}/K)].$$

Fundamental Problems.

- (1) Characterize (f, P) such that $\iota_K(f, P) = 1$.
- (2) Characterize (f, P) such that $\iota_K(f, P)$ is finite.

Arboreal Representations — Recent Progress

We restrict attention to $N = 1$, i.e., $f(x) \in K(x)$.

Theorem. (Looper, Specter, Benedetto, Juul, Kadets; née Odoni Conjecture) Let K/\mathbb{Q} . For all $d \geq 2$ there is a monic $f(x) \in K[x]$ with $\iota_K(f, P) = 1$.

Conjecture. $\iota_K(f, P) < \infty$ unless (f, P) is “special.”

A complete definition of “special” is still lacking, but we do know that $\iota_K(f, P) = \infty$ in the following situations:

- P is a periodic point for f .
- $f \circ \phi = \phi \circ f$ and $\phi(P) = P$ for some $\phi \in \text{PGL}_2(K)$.
- f is **postcritically finite (PCF)**, i.e., its critical points (points satisfying $f'(\alpha) = 0$) are preperiodic.

Question. For a given $d \geq 2$ and number field K , is it true that “most” polynomials $f(x) \in K[x]$ satisfy $\iota_K(f, P) = 1$ for all (most) $P \in K$?

Algebraic-Geometric Moduli Spaces

Fix $g \geq 1$. The set of (principally polarized) abelian varieties of dimension g has the natural structure of an algebraic variety:

$$\mathcal{A}_g := \{\text{principally polarized } A\} / \text{isomorphism.}$$

And if desired, one may add level structure, for example:

$$\mathcal{A}_g[N] := \left\{ \begin{array}{l} A \text{ is a principally polarized} \\ (A, P) : \text{abelian variety and } P \in A \\ \text{is a point of order } N \end{array} \right\} / \sim .$$

Classical Theorem.

$$\dim \mathcal{A}_1[N] = 1 \quad \text{and} \quad \text{genus } \mathcal{A}_1[N] \approx N/12.$$

Theorem. For all sufficiently large g , the moduli space \mathcal{A}_g is a variety of general type.

Dynamical Moduli Spaces

A degree d rational map of \mathbb{P}^N is given by an $(N + 1)$ -tuple of homogeneous polynomials

$$f : \mathbb{P}^N \longrightarrow \mathbb{P}^N, \quad f = [f_0, \dots, f_N].$$

We identify f with its list of coefficients,

$$f \longleftrightarrow (\text{coeffs. of } f) \in \mathbb{P}^\nu, \quad \nu = \binom{N+d}{d} (N+1) - 1.$$

Not every $f \in \mathbb{P}^\nu$ is a morphism, or even a rational map of degree d . We let

$$\text{End}_d^N = \{f \in \mathbb{P}^\nu : f \text{ is a morphism}\},$$

The dynamics of f is unchanged if we change coordinates. So for $\phi \in \text{PGL}_{N+1} = \text{Aut}(\mathbb{P}^N)$, we define

$$f^\phi := \phi^{-1} \circ f \circ \phi. \quad \text{Note that } (f^\phi)^n = (f^n)^\phi.$$

Dynamical Moduli Spaces

Isomorphism classes of algebraic dynamical systems on \mathbb{P}^N are classified by the points of the quotient space

$$\mathcal{M}_d^N := \text{End}_d^N / \text{PGL}_{N+1}.$$

Analogue: The moduli space \mathcal{A}_g of abelian varieties of dimension g .

Theorem. (Levy, Milnor, Petsche, Silverman, Szpiro, Tepper) Let $N \geq 1$ and $d \geq 2$.

(a) $\mathcal{M}_d^N := \text{End}_d^N // \text{SL}_{N+1}$ exists as a GIT-stable quotient scheme over \mathbb{Z} .

(b) $\mathcal{M}_2^1 \cong \mathbb{A}^2$.

(c) $\mathcal{M}_d^1 \otimes \mathbb{Q}$ is a rational variety for all $d \geq 2$.

Remark/Question: \mathcal{M}_d^N is unirational for all (N, d) , since it is a quotient of an open subset of \mathbb{P}^N . Is it always rational?

Dynamical Moduli Spaces with Level Structure

The natural structure to add to a dynamical system is a periodic point,

$$\mathcal{M}_d^N[n] := \{(f, P) : f \in \mathcal{M}_d^N, P \in \mathbb{P}^N \text{ period } n\}.$$

Analogue: $X_1(n) := \{(E, P) : P \in E[n]^*\} / \sim$.

Conjecture.

$$n \geq n_0(N, d) \implies \mathcal{M}_d^N[n] \text{ is of general type.}$$

More generally, we might specify a list of points and their f -orbits, possibly with associated multiplicities. In dynamics, these are called **portraits**, for example:

$$\mathcal{P} : \quad \bullet \curvearrowright \quad \bullet \xrightarrow{2} \bullet \quad \bullet \xrightarrow{2} \begin{array}{c} \curvearrowright 3 \\ \bullet \quad \bullet \\ \curvearrowleft \end{array}$$

Theorem. (Doyle–Silverman) The dynamical portrait moduli space $\mathcal{M}_d^N[\mathcal{P}]$ exists as a GIT-quotient scheme over \mathbb{Z} .

Arithmetic Geometry: Integer Points on Varieties

We start with a classical, but deep and beautiful, result.

Theorem. (Thue) Let $f(X, Y) \in \mathbb{Z}[X, Y]$ be a homogeneous form of degree $d \geq 3$ with $\text{Disc}(f) \neq 0$. Then for all non-zero $m \in \mathbb{Z}$, the equation

$$f(X, Y) = m \text{ has finitely many solutions in } \mathbb{Z}^2.$$

This was vastly generalized by Siegel and Faltings. Let K/\mathbb{Q} be a number field and R_S a ring of S -integers in K .

Theorem. (Siegel) Let C/K be a curve of genus $g \geq 1$, and let $f \in K(C)$ be non-constant function. Then

$$\{P \in C(K) : f(P) \in R_S\} \text{ is a finite set.}$$

Theorem. (Faltings) Let A/K be an abelian variety, and let $H \subset A$ be an ample effective divisor. Then $(A \setminus H)(R_S)$ is finite.

Arithmetic Dynamics: Integer Points in Orbits

Let $f(x) \in \mathbb{Q}(x)$ with $\deg(f) \geq 2$, and let $\alpha \in \mathbb{Q}$.

~~**Dynamical Siegel Theorem**: $\mathcal{O}_f(\alpha) \cap \mathbb{Z}$ is finite.~~

This is clearly false, for example $f(x) = x^2$ and $\alpha = 2$.

More generally, it is false for all $f(x) \in \mathbb{Z}[x]$ and $\alpha \in \mathbb{Z}$.

But there are other counterexamples, for example:

$$f(x) = \frac{1}{x^2}, \quad \alpha = 2, \quad \mathcal{O}_f(\alpha) = \left\{ 2, \frac{1}{4}, 16, \frac{1}{256}, 65536, \dots \right\}.$$

Half the points are in \mathbb{Z} , because $f^{\circ 2}(x) = x^4 \in \mathbb{Z}[x]$.

And there is a similar problem if $f^{\circ n}(x) \in \mathbb{Z}[x]$ for some larger n .

Amusing Proposition/Exercise. If $f(x) \in \mathbb{C}(x)$ satisfies $f^{\circ n}(x) \in \mathbb{C}[x]$ for some $n \geq 1$, then already $f^{\circ 2}(x) \in \mathbb{C}[x]$.

Arithmetic Dynamics: Integer Points in Orbits

This leads to the correct statement.

Theorem. (Silverman) Let $f(x) \in \mathbb{Q}(x)$ satisfy $f^{\circ 2}(x) \notin \mathbb{Q}[x]$, and let $\alpha \in \mathbb{Q}$. Then

$$\mathcal{O}_f(\alpha) \cap \mathbb{Z} \text{ is finite.}$$

A stronger version of Siegel's theorem says that if $P \in C(\mathbb{Q})$ and one writes $f(P) = A_P/B_P \in \mathbb{Q}$, then A_P and B_P have roughly the same number of digits. Here is the dynamical analogue:

Theorem. Assume further that $\mathcal{O}_f(\alpha)$ is infinite, and that $1/f^{\circ 2}(1/x) \notin \mathbb{Q}[x]$. Write $f^{\circ n}(\alpha) = A_n/B_n \in \mathbb{Q}$. Then

$$\lim_{n \rightarrow \infty} \frac{\log |A_n|}{\log |B_n|} = 1.$$

Problem: Generalize these results to \mathbb{P}^N .

Topics for Tomorrow's Lecture

- Geometric and arithmetic complexity of orbits
- Canonical heights
- Dynamical degrees and arithmetic degrees
- ...

Additional Creatures in the Arithmetic Dynamics Barnyard

- **Stability of Iterates:** Let $f(x) \in K(x)$. To what extent does $f^n(x)$ factor as $n \rightarrow \infty$?
- **Primes in Orbits:** Let $f(x) \in \mathbb{Z}[x]$ and $\alpha \in \mathbb{Z}$.
 1. Is $\mathcal{O}_f(\alpha) \cap \text{PRIMES}$ always finite? E.g., $2^{2^n} + 1$.
 2. What is the density of

$$\text{Support } \mathcal{O}_f(\alpha) := \bigcup_{n \geq 0} \{p : f^n(\alpha) \equiv 0 \pmod{p}\}.$$

- **Dynamical Shafarevich Conjecture:** What is the dimension in $\mathcal{M}_d^N(K)$ of the Zariski closure of the set of maps having good reduction outside S ? For $N = 1$ and $d \geq 3$, it is known that this **Shafarevich dimension** is between $d + 1$ and $2d - 2$.

Additional Topics (continued)

- **Local–Global Questions in Dynamics:** For $f : X \rightarrow X$ and $Y \subset X$, is the **Dynamical Brauer–Manin Obstruction** the only obstruction to the existence of points in $\mathcal{O}_f(P) \cap Y$?
- **André–Oort Unlikely Intersections:** Unlikely intersection problems that take place in moduli space. Sample (deep) result:

Theorem. (Baker–DeMarco) Fix $a, b \in \mathbb{C}$ with $a^2 \neq b^2$. Then

$$\{c \in \mathbb{C} : a \text{ and } b \text{ are both in } \text{PrePer}(x^2 + c)\}$$

is finite.

Additional Topics (continued)

- **Non-archimedean (p -adic) Dynamics:** This is a huge field in its own right, with theorems/conjectures on invariant measures, Lyapunov exponents, wandering domains, etc. Most work these days takes place on Berkovich spaces.
- **Finite Field Dynamics:** Again, a field in its own right, with many ties to p -adic dynamics. Sample (deep) result:

Theorem. (Jones)

$$\lim_{n \rightarrow \infty} \frac{\#\{c \in \mathbb{F}_{p^n} : 0 \text{ is periodic for } x^2 + c\}}{p^n} = 0.$$

Arithmetic Dynamics,
Arithmetic Geometry,
and Number Theory

Joseph H. Silverman

Brown University

MAGNTS (Midwest Arithmetic Geometry and
Number Theory Series)

October 12–13, 2019

Arithmetic Dynamics,
Arithmetic Geometry,
and Number Theory:
Lecture #2

MAGNTS
October 12–13, 2019

Complexity

A Rough Working Definition. The **complexity** of an object α is:

Complexity(α) = number of bits needed to describe α .

Examples.

$$\text{Complexity}(\alpha \in \mathbb{Z}) = \log_2 |\alpha| + 1 \approx \log |\alpha|.$$

$$\text{Complexity}(p(x) \in \mathbb{C}[x]) = \# \text{ of monomials} = \deg(p).$$

Fancier Examples.

Number theory: height of points on varieties

Algebraic geometry: dimension of cohomology spaces

Dynamics: entropy of maps

Fundamental Problem. Given a set S , a way to measure complexity, and a function $f : S \rightarrow S$:

How fast does Complexity($f^{\circ n}(\alpha)$) grow as $n \rightarrow \infty$?

Dynamical Complexity of Maps on \mathbb{P}^N

Let

$$f : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$$

be a dominant rational map. A coarse measure of its complexity is its degree. What happens when we iterate?

Example: Let $f(X, Y, Z) = [YZ, XY, Z^2]$. Then

$$\begin{aligned} f &= [YZ, XY, Z^2] & \deg f &= 2 \\ f^{\circ 2} &= [XYZ, XY^2, Z^3] & \deg f^{\circ 2} &= 3 \\ f^{\circ 3} &= [XY^2Z^2, X^2Y^3, Z^5] & \deg f^{\circ 3} &= 5 \\ f^{\circ 4} &= [X^2Y^3Z^3, X^3Y^5, Z^8] & \deg f^{\circ 4} &= 8 \end{aligned}$$

Exercise: $\deg f^{\circ n} = \text{Fibonacci}_{n+2} \approx \left(\frac{1+\sqrt{5}}{2}\right)^n$.

In general, how fast does $\deg f^{\circ n}$ grow?

The **dynamical degree** of $f : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ is

$$\delta_f := \lim_{n \rightarrow \infty} (\deg f^{\circ n})^{1/n}.$$

Dynamical Degree on \mathbb{P}^N

Exercise: The limit

$$\delta_f := \lim_{n \rightarrow \infty} (\deg f^{\circ n})^{1/n} \quad \text{exists.}$$

Hint. Use convexity $\deg(f \circ g) \leq (\deg f)(\deg g)$.

Intuition: $\deg(f^n) \approx \delta_f^n$.

Here is a surprising arithmetic conjecture about the values of dynamical degrees.

~~**Conjecture.** (Bellon–Viallet 1999) The dynamical degree δ_f is always an algebraic integer.~~

Oops! Twenty years later ...

Theorem. (Bell–Diller–Jonsson, 2019) There exists a dominant rational map $f : \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$ whose dynamical degree is transcendental.

A Transcendental Dynamical Degree

The Bell–Diller–Jonsson construction is very explicit. For example, let

$$\begin{aligned}\phi &= [X(X - Y - Z), Y(-X + Y - Z), \\ &\quad Z(-X - Y + Z)], \\ \psi &= [X^3Y, Y^2Z^2, Z^4], \\ f &= \psi \circ \phi.\end{aligned}$$

Then δ_f^{-1} is the unique real positive solution T to the equation

$$\sum_{n=1}^{\infty} \deg(\psi^n) T^n = 1,$$

and this value is transcendental.

Dynamical Degree on Varieties

More generally, we consider a dominant rational map

$$f : X \dashrightarrow X$$

of a smooth projective variety of dimension N . Let H be an ample divisor on X .

The **dynamical degree of f** is

$$\delta_f := \lim_{n \rightarrow \infty} \left((f^{\circ n})^* H \cdot H^{N-1} \right)^{1/n}.$$

A few remarks are in order:

- The limit defining δ_f exists and is independent of H .
- The action of rational maps on $\text{Pic}(X)$ is not functorial, so generally

$$(f^{\circ n})^* H \not\sim (f^*)^{\circ n} H.$$

- **Intuition:** As with \mathbb{P}^N , the idea is that

$$\text{Geometric Complexity of } f^{\circ n} \approx \delta_f^n.$$

Heights and Arithmetic Complexity of Points

Let point $P \in \mathbb{P}^N(\mathbb{Q})$. We write its coordinates as

$$P = [a_0, \dots, a_N] \text{ with } a_i \in \mathbb{Z} \text{ and } \gcd(a_0, \dots, a_N) = 1.$$

Then the **(logarithmic) height of P** is

$$h(P) := \log \max\{|a_0|, |a_1|, \dots, |a_N|\}.$$

It measures the “arithmetic complexity of P .”

More generally, for

$$P = [a_0, \dots, a_N] \in \mathbb{P}^N(K) \subset \mathbb{P}^N(\overline{\mathbb{Q}}),$$

the **height of P** is

$$h(P) := \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \log \max_{0 \leq i \leq N} \|a_i\|_v.$$

What does it all mean? Just keep in mind the intuition:

$$h(P) \asymp \# \text{ of bits needed to describe the point } P.$$

A Height Finiteness Theorem

We would expect there to be finitely many objects of bounded complexity. This is certainly true for points in $\mathbb{P}^N(\mathbb{Q})$, since

$$h(P) \leq B \implies P = \overbrace{[a_0, \dots, a_N]}^{\text{integers}} \text{ with } |a_i| \leq e^B.$$

Theorem. (Northcott) For all K/\mathbb{Q} and all $B \geq 0$,

$$\{P \in \mathbb{P}^N(K) : h(P) \leq B\} \text{ is finite.}$$

More generally, for all $D \geq 1$,

$$\{P \in \mathbb{P}^N(\overline{\mathbb{Q}}) : h(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\} \text{ is finite.}$$

In words, there are only finitely many points in $\mathbb{P}^N(\overline{\mathbb{Q}})$ of bounded height and bounded degree.

A Height Transformation Formula

Let $f : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ be a rational map of degree d .

f is given by degree d polynomials, and roughly speaking,

$$(\# \text{ of bits in } a^d) \approx d \times (\# \text{ of bits in } a).$$

So we'd expect $h(f(P))$ to be roughly $dh(P)$. This turns out to be correct — sort of!

Theorem.

$$h(f(P)) \leq dh(P) + C(f) \quad \text{for all } P \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

If f is a morphism, then also

$$h(f(P)) \geq dh(P) - C(f) \quad \text{for all } P \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

The proof (of the lower bound) uses the Nullstellensatz.

Intuition: $\underbrace{f \text{ complicated}}_{\text{high degree}} \implies \underbrace{h(f(P)) \text{ complicated}}_{\text{lots of bits}}$.

Arithmetic Degree of Points in $\mathbb{P}^N(\overline{\mathbb{Q}})$

For $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$,

$h(P) =$ “arithmetic complexity of P ” \asymp # of bits in P .

Let $f : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$, and assume that the orbit $\mathcal{O}_f(P)$ is well-defined. Then

$h(f^{\circ n}(P)) =$ “arithmetic complexity of $f^{\circ n}(P)$ ”.

Each time we iterate, the number of bits in $f^{\circ n}(P)$ is multiplied by (at most) d , just as the degree of $f^{\circ n}$ is multiplied by at most d . This suggests looking at the following arithmetic analogue of the dynamical degree:

$$\alpha_f(P) := \lim_{n \rightarrow \infty} h(f^{\circ n}(P))^{1/n}.$$

The quantity $\alpha_f(P)$ is called the **arithmetic degree** of the f -orbit of P . It measures the average growth of arithmetic complexity in the orbit $\mathcal{O}_f(P)$.

Heights on (Abelian) Varieties

The next step is to generalize the height construction to arbitrary algebraic varieties $X/\overline{\mathbb{Q}}$. For each such variety, we fix a projective embedding

$$\iota : X \hookrightarrow \mathbb{P}^N,$$

and we use ι to define a height function on X ,

$$h_X : X(\overline{\mathbb{Q}}) \longrightarrow [0, \infty), \quad h_X(P) := h(\iota(P)).$$

Clearly h_X depends on the embedding. There is a beautiful general theory, called the *Weil Height Machine*, that associates a height function to each divisor on X . But for our purposes, it suffices to use one embedding.

For abelian varieties $A/\overline{\mathbb{Q}}$, it will be convenient later if we take a symmetric embedding, i.e., an embedding

$$\iota : A \hookrightarrow \mathbb{P}^N \quad \text{satisfying} \quad (\iota \circ [-1])^* H \sim \iota^* H.$$

This allows us to assume that $h_A(-P) = h_A(P) + O(1)$.

Arithmetic Degree of Points on Varieties

Definition/Conjecture. Let $X/\overline{\mathbb{Q}}$ be a smooth projective variety, let

$$h_X : X(\overline{\mathbb{Q}}) \longrightarrow [0, \infty)$$

be the height associated to an embedding $\iota : X \hookrightarrow \mathbb{P}^M$, let

$$f : X \dashrightarrow X$$

be a dominant rational map defined over $\overline{\mathbb{Q}}$, and let

$$P \in X_f(\overline{\mathbb{Q}}) := \{P \in X(\overline{\mathbb{Q}}) : \mathcal{O}_f(P) \text{ is well-defined}\}.$$

The

arithmetic degree of the f -orbit of P ,

which is defined by the limit

$$\alpha_f(P) := \lim_{n \rightarrow \infty} h_X(f^{\circ n}(P))^{1/n},$$

converges for all such P .

Dynamical Degree versus Arithmetic Degree

We have:

$$\begin{aligned}\delta_f^n &\approx \text{geometric complexity of } f^{\circ n}, \\ \alpha_f(P)^n &\approx \text{arithmetic complexity of } f^{\circ n}(P).\end{aligned}$$

It makes sense that if $f^{\circ n}(P)$ is complicated, it should force $f^{\circ n}$ to be complicated.

Theorem. (Kawaguchi–Silverman, Matsuzawa) Let $f : X \dashrightarrow X$ and $P \in X_f(\mathbb{Q})$. Then

$$\bar{\alpha}_f(P) \leq \delta_f.$$

This gives a precise quantitative formulation to:

$$\left(\begin{array}{l} \text{Arithmetic Complexity} \\ \text{of the Points in the} \\ \text{Orbit } \{f^{\circ n}(P)\}_{n \geq 1} \end{array} \right) \leq \left(\begin{array}{l} \text{Geometric Complexity} \\ \text{of the Dynamical} \\ \text{System } \{f^{\circ n}\}_{n \geq 1} \end{array} \right)$$

Dynamical Degree Equals Arithmetic Degree

An inequality such as $\alpha_f(P) \leq \delta_f$ immediately suggests a question. When is there equality, i.e., for which points does the orbit have maximal complexity?

Density Conjecture. (Kawaguchi–Silverman) Let $f : X \dashrightarrow X$ and $P \in X_f(\mathbb{Q})$. Then

$$\mathcal{O}_f(P) \text{ Zariski dense in } X \implies \alpha_f(P) = \delta_f.$$

$$\left(\begin{array}{c} \text{Maximal geometric} \\ \text{complexity of an orbit} \end{array} \right) \implies \left(\begin{array}{c} \text{Maximal arithmetic} \\ \text{complexity of the orbit} \end{array} \right)$$

The density conjecture is known in various cases, including:

- (1) Monomial maps of \mathbb{P}^N .
- (2) Many classes of rational maps of \mathbb{P}^2 .
- (3) Maps of abelian varieties. More generally, translated isogenies of semi-abelian varieties.
- (4) Morphisms of surfaces.
- (5) Morphisms of certain higher dimensional varieties having additional structure.
- (6) Dominant rational maps of large topological degree.

A variety of tools are used in the proofs, including: linear-forms-in-logarithms, the canonical height pairing, resolution of singularities, the minimal model program,

The Canonical Height on Abelian Varieties

The height on an abelian variety A transforms quite nicely relative to the group law. For example:

Theorem. Let $m \geq 1$. Then for all $P \in A(\overline{\mathbb{Q}})$,

$$h_A([m]P) = m^2 h_A(P) + O(1).$$

This plays a vital role in the proof of the Mordell–Weil theorem. But that $O(1)$ is kind of annoying, right?

Theorem. (Néron–Tate) For all $P \in A(\overline{\mathbb{Q}})$, the limit

$$\hat{h}_A(P) := \lim_{n \rightarrow \infty} 4^{-n} h_A([2^n]P)$$

exists and satisfies:

$$\hat{h}_A([m]P) = m^2 \hat{h}_A(P). \quad (\text{No more } O(1).)$$

$$\hat{h}_A(P) = h_A(P) + O(1). \quad (\hat{h}_A \text{ measures complexity.})$$

- The function \hat{h}_A is called the **canonical height**.

Dynamical Height Functions

Let

$$f : \mathbb{P}^N \longrightarrow \mathbb{P}^N$$

be a morphism of degree $d \geq 2$ defined over $\overline{\mathbb{Q}}$. Tate's construction of \hat{h}_A carries over to iteration of f .

Theorem. For all $P \in \mathbb{P}^N(\overline{\mathbb{Q}})$, the limit

$$\hat{h}_f(P) := \lim_{n \rightarrow \infty} d^{-n} h(f^{\circ n}(P))$$

exists and satisfies:

$$\hat{h}_f(f(P)) = d\hat{h}_f(P).$$

$$\hat{h}_f(P) = h(P) + O(1).$$

$$\hat{h}_f(P) = 0 \iff P \in \text{PrePer}(f).$$

The function \hat{h}_f is called the

dynamical canonical height associated to f .

$\hat{h}_f(P)$ measures the arithmetic complexity of $\mathcal{O}_f(P)$.

Lang's Height Lower Bound Conjecture

Let's start with an elliptic curve E/K . It is reasonable to expect that:

E arithmetically complicated

$\implies P \in E(K)$ is arithmetically complicated.

We measure the arithmetic complexity of E via the height of its j -invariant, while arithmetic complexity of $P \in E(K)$ is measured by its canonical height.

Conjecture. (Lang Height Conjecture) There are constants $c_1 > 0$ and c_2 , depending only on K , such that for all E/K and all non-torsion $P \in E(K)$,

$$\hat{h}_E(P) \geq c_1 h(j(E)) - c_2.$$

- Theorem: $ABC \implies$ Lang's height conjecture.
- The conjecture generalizes to abelian varieties.

A Dynamical Height Lower Bound Conjecture

We use our usual dictionary:

abelian variety $A \iff$ morphism $f : \mathbb{P}^N \rightarrow \mathbb{P}^N$.

moduli space $\mathcal{A}_g \iff$ moduli space \mathcal{M}_d^N .

canonical height $\hat{h}_A \iff$ canonical height \hat{h}_f .

height $h_{\mathcal{A}}$ on $\mathcal{A}_g(\overline{\mathbb{Q}}) \iff$ height $h_{\mathcal{M}}$ on $\mathcal{M}_d^N(\overline{\mathbb{Q}})$.

Dynamical Lang Height Lower Bound Con-

jecture. Fix $N \geq 1$ and $d \geq 2$ and K/\mathbb{Q} . There are constants $c_1 > 0$ and c_2 , depending only on (N, d, K) and the choice of height function $h_{\mathcal{M}}$, so that

for all $f \in \text{End}_d^N(K)$ and

for all $P \in \mathbb{P}^N(K)$ with Zariski dense $\mathcal{O}_f(P)$,

we have

$$\hat{h}_f(P) \geq c_1 h_{\mathcal{M}}(f) - c_2.$$

What is the Dynamical Analog of Complex Multiplication

There are dynamical systems $f : \mathbb{P}^N \rightarrow \mathbb{P}^N$ that have automorphisms, in the sense that

$$\text{Aut}(f) := \{ \phi \in \text{PGL}_{N+1} : \phi^{-1} \circ f \circ \phi = f \} \neq \{1\}.$$

But a theorem of Levy says that the set of such maps in \mathcal{M}_d^N is a Zariski closed subset. So $\text{Aut}(f) \neq 1$ is not a good analogue for CM.

If we interpret CM more loosely as “abelian varieties with special geometric properties,” then we should look at “dynamical systems with special geometric properties.”

Definition. A map $f : \mathbb{P}^1 \rightarrow \mathbb{P}^1$ of degree $d \geq 2$ is said to be **post-critically finite (PCF)** if all of its critical points are preperiodic, i.e.,

$$\begin{aligned} \text{Crit}(f) &:= \{ \alpha \in \mathbb{P}^1 : f'(\alpha) = 0 \}, \\ \text{PCF}_d &:= \{ f \in \mathcal{M}_d^1 : \text{Crit}(f) \subset \text{PrePer}(f) \}. \end{aligned}$$

Some (Mostly Geometric) Properties of PCF Maps

- The PCF locus PCF_d is Zariski dense in \mathcal{M}_d^1 .
- PCF maps are very important in the study of complex dynamics on $\mathbb{P}^1(\mathbb{C})$.
- PCF points are algebraic, i.e., $\text{PCF}_d \subset \mathcal{M}_d^1(\overline{\mathbb{Q}})$.
- If $f \in \text{PCF}_d$, then the f -orbit of its $2d - 2$ critical points forms a finite graph (portrait).
- Thurston gives a combinatorial method to determine if a given portrait is the portrait of a PCF map.
- Thurston also proved that critical point relations are “transversal” in \mathcal{M}_d^1 .

Some Arithmetic Properties of PCF Maps

Definition. The **critical height of $f \in \mathcal{M}_d^1(\overline{\mathbb{Q}})$** is

$$\hat{h}^{\text{crit}}(f) := \sum_{\alpha \in \text{Crit}(f)} \hat{h}_f(\alpha).$$

We recall that

$$\hat{h}_f(\alpha) \geq 0, \quad \text{and} \quad \hat{h}_f(\alpha) = 0 \iff \alpha \in \text{PrePer}(f).$$

Hence

$$\hat{h}^{\text{crit}}(f) \geq 0, \quad \text{and} \quad \hat{h}^{\text{crit}}(f) = 0 \iff f \in \text{PCF}_d.$$

Does $\hat{h}^{\text{crit}}(f)$ measure arithmetic complexity of the map f ?

Theorem. (Ingram) Fix a height $h_{\mathcal{M}}$ on $\mathcal{M}_d^1(\overline{\mathbb{Q}})$. There are constants $c_1, c_2, c_3, c_4 > 0$ so that for all $f \in \mathcal{M}_d^1(\overline{\mathbb{Q}})$,

$$c_1 h_{\mathcal{M}}(f) - c_2 \leq \hat{h}^{\text{crit}}(f) \leq c_3 h_{\mathcal{M}}(f) + c_4.$$

How Much Can a Rational Map Decrease Complexity?

Let $f : \mathbb{P}^N \dashrightarrow \mathbb{P}^N$ be a dominant rational map of degree $d \geq 2$ defined over $\overline{\mathbb{Q}}$. Then there is an upper bound that comes, more-or-less, from the triangle inequality:

$$h(f(P)) \leq dh(P) + c(f), \quad \text{valid for all } P \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

For morphisms, there is a corresponding lower bound, but in general there cannot be a lower bound for rational maps. For example, a rational map can fix an entire hyperplane.

However, we might hope that for “most” points, the arithmetic complexity of $f(P)$ can’t be “a lot smaller” than the complexity of P .

Theorem. There are a non-empty Zariski open set $U_f \subset \mathbb{P}^N$ and positive constants $c_1(f), c_2(f)$ so that

$$h(f(P)) \geq c_1(f)h(P) - c_2(f) \quad \text{for all } P \in U_f(\overline{\mathbb{Q}}).$$

A Uniform Bound for Height Contraction

In the inequality,

$$h(f(P)) \geq c_1(f)h(P) - c_2(f) \quad \text{for all } P \in U_f(\overline{\mathbb{Q}}),$$

how small can $c_1(f)$ get as we vary f ? We have to be careful, since U_f also depends on f .

Definition. The **height contraction coefficient of f** is the quantity

$$\mu(f) := \sup_{\emptyset \neq U \subset \mathbb{P}^N} \liminf_{\substack{P \in U(\overline{\mathbb{Q}}) \\ h(P) \rightarrow \infty}} \frac{h(f(P))}{h(P)}.$$

The theorem asserts that $\mu(f) > 0$.

Theorem. There is a lower bound for $\mu(f)$ that depends only on N and d .

A Uniform Bound for Height Contraction

In other words, the following **universal height contraction coefficient for degree d maps of \mathbb{P}^N** is positive:

$$\bar{\mu}_d(\mathbb{P}^N) := \inf_{\substack{f: \mathbb{P}^N \dashrightarrow \mathbb{P}^N \\ \deg(f)=d \\ f \text{ is defined over } \overline{\mathbb{Q}} \\ f \text{ is dominant}}} \mu(f) > 0.$$

Question. What is the value of $\bar{\mu}_d(\mathbb{P}^N)$? This seems like a very interesting question. We do have an estimate:

Theorem.

$$\bar{\mu}_d(\mathbb{P}^N) \leq \frac{1}{d^{N-1}} \quad \text{for all } N \geq 2 \text{ and all } d \geq 2.$$

This is proved using the theory of canonical heights associated to regular affine automorphisms $\mathbb{A}^N \rightarrow \mathbb{A}^N$.

I want to thank you for your attention.

I want to thank you for your attention.

And please join me in thanking the organizers,
Wei Ho, Roman Holowinsky,
Jennifer Park, Kevin Tucker,
for this inaugural MAGNTS conference.

Further Reading

- *The Arithmetic of Dynamical Systems*, Silverman, GTM 241, Springer, 2007.
- *Moduli Spaces and Arithmetic Dynamics*, Silverman, CRM Monograph Series 30, AMS, 2012.
- Galois representations from pre-image trees: an arboreal survey, Jones, *Actes de la Conférence “Théorie des Nombres et Applications”*, Publ. Math. Besançon Algèbre Théorie Nr., 107–136, Presses Univ. Franche-Comté, Besançon, 2013.
- *Current Trends and Open Problems in Arithmetic Dynamics*, Benedetto, Ingram, Jones, Manes, Silverman, Tucker, Bull. Amer. Math. Soc. (N.S.), 2019. <https://doi.org/10.1090/bull/1665>
- *Complexity Problems in Algebraic, Complex and Arithmetic Dynamics: An Annotated Bibliography*, DeMarco, Jonsson, Silverman (coordinating authors), in preparation.

Arithmetic Dynamics,
Arithmetic Geometry,
and Number Theory

Joseph H. Silverman

Brown University

MAGNTS (Midwest Arithmetic Geometry and
Number Theory Series)

October 12–13, 2019