My research for the past few years has been focused on studying dynamical systems through the lenses of number theory and algebraic geometry. Concretely, this involves discovering and explaining new phenomena about the arithmetic of orbits. My interests have also wandered into arithmetic geometry [Fab08, Fab09], tropical geometry [BF], the finite field Kakeya problem [Fab07], analysis on metric graphs [Fab06, BF06], and knot theory [CFM04].

Algebraic dynamics is the study of orbits (of points, subvarieties, etc.) under the iteration of a self-map of a variety. While complex dynamics has quite a long history, the arithmetic aspect has only recently come into its own as a stand-alone field. One might attribute this to a huge influx of external ideas from areas like Arakelov theory, Galois representations, model theory, and rigid analytic geometry. Since 2007, there have been nearly a dozen conferences and AMS special sessions organized around arithmetic dynamics and related topics. These include the 2010 Arizona Winter School and a workshop on Moduli Spaces in Arithmetic Dynamics that I organized at the Bellairs Research Institute in Barbados. Enough papers have been written on arithmetic dynamics to merit its own MSC2010 secondary classification (37Pxx). The recent Springer GTM by Joseph Silverman [Sil07] gives a comprehensive introduction to the subject.

Below I describe my completed research on dynamics and explain where it’s headed in the near future (1-3 years). This includes a few suggestions for how I might involve students in my research program at the undergraduate and graduate level.

---

**Generating Prime Numbers: The Methods of Euclid and Newton**

Algorithmic methods for producing prime numbers are of fundamental import, both theoretically and for modern cryptographic applications. Around 300 BC, Euclid of Alexandria constructed a sequence of integers \((a_n)\) that contains infinitely many prime factors. In fact, he showed that each \(a_n\) admits a prime factor that is not present in \(a_m\) for \(m < n\) (a **primitive prime factor**). In the last century, the existence of primitive prime factors in certain linear recurrences (Lucas and Lehmer sequences) and in sequences related to elliptic curve addition (elliptic divisibility sequences) has been extensively studied. See [BHV01, Sil88], for example. Recently Andrew Granville and I looked at primitive prime factors in certain dynamically defined sequences.

**Theorem 1** ([FG]). Fix a rational function \(\phi(z) \in \mathbb{Q}(z)\) of degree at least two and a rational number \(x_0\). The orbit of \(x_0\) is defined recursively by \(x_n = \phi(x_{n-1})\) for \(n \geq 1\). If the sequence \((x_n)_{n \geq 0}\) is not eventually periodic, then for any fixed \(\Delta \geq 1\) and for \(n\) sufficiently large, there exists a primitive prime factor \(p_n\) of the numerator of \(x_{n+\Delta} - x_n\), except when \(\Delta = 1\) and \(\phi\) is affine conjugate to one of the two rational functions

\[
\frac{z^2}{z+1} \quad \text{or} \quad \frac{z^2}{2z+1}.
\]

In these two exceptional cases, there exists a primitive prime factor in the denominator of \(x_{n+1} - x_n\) when \(n\) is sufficiently large.\(^1\)

The proof uses the Thue/Mahler theorem in Diophantine approximation to find primitive prime factors in a certain auxiliary sequence. Dynamical considerations allow us to show that these prime factors also appear in the sequence \((x_{n+\Delta} - x_n)\). It will appear in *Crelle’s Journal* next year.

The dynamical system that arises from Newton’s method of approximating real roots of a polynomial is a natural setting in which to apply these techniques. José Felipe Voloch and I looked at the success and failure of Newton’s method for the \(p\)-adic topologies that arise in number theory.

**Theorem 2** ([FV10]). Let \(f(z)\) be an irreducible polynomial of degree \(d \geq 3\) with rational coefficients. Fix \(x_0 \in \mathbb{Q}\) and define the Newton approximation sequence by \(x_n = x_{n-1} - f(x_{n-1})/f'(x_{n-1})\) for \(n \geq 1\). Write \(\mathcal{P}_c\) for the set of primes \(p\) such that \((x_n)_{n \geq 0}\) converges to a root of \(f\) in \(\mathbb{Q}_p\), and write \(\mathcal{P}_c'\) for its complement in the set of all primes. If the sequence \((x_n)_{n \geq 0}\) is not eventually periodic, then both \(\mathcal{P}_c\) and its complement are infinite sets.\(^2\)

---

\(^1\)In principle this result is effective — i.e., one can explicitly say what “\(n\) sufficiently large” means. However, the only known method for doing so uses Baker’s linear forms in logarithms and yields bounds that are likely to be far from the truth.

\(^2\)The fact that \(\mathcal{P}_c'\) is infinite was first observed in [SV09].
Future Prospect — Density Questions: The prime factors that show up in the sequences above appear to be rather sparse in the set of all primes. We ask the very general

**Question 1.** Let \( \phi(z) \in \mathbb{Q}(z) \) be a rational function, and let \( x_0, y_0 \in \mathbb{P}^1(\mathbb{Q}) \) be two points. Define \( x_n = \phi(x_{n\cdot1}) \) for all \( n \geq 1 \), and similarly for \( y_n \). Suppose that the orbits \( (x_m)_{m\geq0} \) and \( (y_n)_{n\geq0} \) have no intersection. Write \( \mathcal{P} \) for the set of primes \( p \) such that the orbits \( (x_m)_{m\geq0} \) and \( (y_n)_{n\geq0} \) have a nonempty intersection modulo \( p \). Is it true that the density of \( \mathcal{P} \) is zero?

It seems unlikely that a complete answer is within the scope of our current technology. Galois theoretic techniques and the Chebotarev density theorem have made progress possible when \( \phi \) is a generic polynomial of fixed degree \( d \geq 2 \) [Odo85a].

If \( f(z) \) is a polynomial of degree \( d \geq 3 \), if \( y_0 \) is a root of \( f \), and if \( \phi(z) = z - f(z)/f'(z) \) is the Newton approximation map, then we are in the setting of Theorem 2. In this case, Question 1 can be rephrased as, “Does Newton’s method fail for 100% of primes?” In order to gain further understanding of the situation, I would like to have an undergraduate compute some data for cubic polynomials with small integer coefficients. I also plan to use trying sieve methods from analytic number theory to prove something for generic polynomials \( f \).

**Rational Points and Dynamical \( p \)-Torsion**

A special case of a folklore conjecture from the mid 20th century asserts that there is a uniform bound for the size of the rational torsion subgroup of an elliptic curve \( E/\mathbb{Q} \). It was proved by Mazur in the late 70’s, but a decade earlier Manin made the following important contribution:

**Manin’s \( p \)-Torsion Theorem** ([Man69]). For each prime number \( p \), there exists a positive integer \( A \) such that for any elliptic curve \( E/\mathbb{Q} \), the \( p \)-power torsion subgroup of \( E \) has size at most \( A \).

We can reinterpret this result in a dynamical context. An elliptic curve \( E/\mathbb{Q} \) is an algebraic group, and so we have the multiplication-by-\( p \) map \( [p] : E \rightarrow E \). Write \( \mathcal{O} \) for the origin of the group law. Then the \( p \)-power torsion subgroup \( E[p^\infty] \) can be viewed as the iterated pre-images of \( \mathcal{O} \) via this map:

\[
E[p^\infty] = \{ x \in E(\overline{\mathbb{Q}}) : [p]^N(x) = \mathcal{O} \text{ for some } N \geq 0 \}.
\]

Viewed in this light, Manin’s result gives a bound on the number of rational iterated pre-images of the origin for any elliptic curve.

For a rational number \( c \), define a dynamical system \( f_c(z) = z^2 + c \) on the affine line \( \mathbb{A}^1 \). For each \( n \geq 0 \), write \( f^n_c = f_c \circ \cdots \circ f_c \) for the \( n \)-fold composition of \( f_c \) with itself. In collaboration with six other authors (the product of a discussion at an AIM workshop), I showed that the number of rational iterated pre-images of \( a \) under the map \( f_c \) is bounded as one varies the parameter \( c \in \mathbb{Q} \). More precisely:

**Theorem 3** ([FHI+09]). For \( a \in \mathbb{Q} \), define

\[
\kappa(a) := \sup_{c \in \mathbb{Q}} \# \{ x \in \mathbb{A}^1(\mathbb{Q}) | f_c^N(x) = a \text{ for some } N \geq 1 \}.
\]

Then \( \kappa(a) \) is finite for any \( a \in \mathbb{Q} \).³

To prove it, we construct a tower of “pre-image curves”

\[
\cdots \rightarrow X^\text{pre}(N, a) \rightarrow X^\text{pre}(N - 1, a) \rightarrow \cdots \rightarrow X^\text{pre}(1, a),
\]

where \( X^\text{pre}(N, a) \) is a smooth projective curve that parameterizes pairs \( (x, c) \) such that \( x \) is an \( N \)-th pre-image of \( a \) via the map \( z \mapsto z^2 + c \). The arrows correspond to the natural map \( (x, c) \mapsto (f_c(x), c) \). We give exact formulas for the genera of these curves, and then the result follows essentially from Faltings’ theorem for rational points on high genus curves (a.k.a. the Mordell conjecture).⁴

The proof of Theorem 3 gives no information on the exact value of \( \kappa(a) \). As a first attempt to remedy this problem, I formulated an effective refinement of the Mordell conjecture (which I did not prove) and

³This is a simplified version of our main theorem. We were also able to prove that the supremum remains finite if one is allowed to vary \( c \) in a number field \( K \) of uniformly bounded degree, and if one is allowed to take \( x \in \mathbb{Q} \) of uniformly bounded degree over \( K \) (at the cost of introducing a set of potential exceptions \( a \in \mathbb{Q} \)).

⁴In the more general setting, we compute the gonality of these curves and apply Vojta’s refinement of Faltings’ theorem.
used it to show that \( \kappa(a) \) depends at most on the absolute logarithmic height of \( a \in \mathbb{Q} \) [Fab10a]. Then in collaboration with Benjamin Hutz and Michael Stoll, I performed a more careful study of the rational points on the curves \( X^{pre}(N,0) \) for \( N = 1, 2, 3, 4 \) [FHS10]. We were able to prove that \( \kappa(0) = 6 \) assuming certain standard conjectures in number theory. (More precisely, we assumed the existence of the L-series functional equation and the Birch and Swinnerton-Dyer conjecture for the Jacobian of the curve \( X^{pre}(4,0) \), which has genus 5.) We also use a number of modern tools including 2-descent for hyperelliptic curves, the Weil conjectures, and the method of Chabauty and Coleman.

It is possible to proceed without assuming any unproved conjectures if we are allowed to discard finitely many members of the family. Define

\[
\bar{\kappa}(a) = \lim_{c \to 0} \sup_{c \in \mathbb{Q}} \# \{ x \in \mathbb{A}^1(\mathbb{Q}) : f_c^N(x) = a \text{ for some } N \geq 1 \}.
\]

Then we showed \( \bar{\kappa}(0) = 6 \) unconditionally [FHS10]. The proof requires one to show that the algebraic curves that parameterize the configurations of more than 6 pre-images all have genus at least 2, and hence only finitely many rational points.

**Future Prospect — Other Families:** A finiteness result like Theorem 3 cannot hold for an arbitrary 1-parameter family of dynamical systems. For example, the family \( g_b(z) = (z - b)^2 + b \) can have arbitrarily large numbers of pre-images of the origin as one varies the parameter \( b \). The reason is that \( g_b \) is conjugate to the constant morphism \( z \mapsto z^2 \), and so it doesn’t actually vary in the moduli space of quadratic dynamical systems \( \mathcal{M}_2 \). (Here conjugate means changing coordinates in the same way on both the source and target.)

With this observation in hand, we make the following conjecture:

**Conjecture.** Let \( \phi_t : \mathbb{P}^1 \to \mathbb{P}^1 \) be a 1-parameter family of morphisms of degree \( d \geq 2 \) defined over \( \mathbb{Q} \), and suppose its image in the moduli space of dynamical systems \( \mathcal{M}_d \) is not reduced to a point. Then for any \( a \in \mathbb{Q} \), one has

\[
\sup_{t \in \mathbb{Q}} \# \{ x \in \mathbb{P}^1(\mathbb{Q}) : \phi_t^N(x) = a \text{ for some } N \geq 1 \} < \infty.
\]

It would suffice to show that the genera of the associated pre-image curves \( X^{pre}(\phi,N,a) \) grow with \( N \). Although it is not difficult to check this assertion for any explicitly described family \( \phi_t \), it is not clear how to proceed for an arbitrary one. A detailed understanding of the ramification in the corresponding “pre-image tower” will be necessary to proceed further.

I plan to start a sequence of studies on the arithmetic of pre-images for other families of dynamical systems. For example, it is known that any quadratic rational map \( \phi : \mathbb{P}^1_\mathbb{Q} \to \mathbb{P}^1_\mathbb{Q} \) is conjugate to one of the following forms by a change of coordinates defined over a cubic extension of \( \mathbb{Q} \):

\[
\phi_{\alpha,\beta}(z) = \frac{z^2 + \alpha z}{\beta z + 1}, \quad \psi_c(z) = \frac{1}{z} + c.
\]

The varieties parameterizing the \( N^{th} \) pre-images of a basepoint \( a \) for the family \( \psi_c \) are curves, and the analysis of their pre-images should be similar to that for the family \( f_c \). A graduate student could learn a great deal of arithmetic geometry by computing the analogous quantities \( \kappa \) and \( \bar{\kappa} \) for this family. On the other hand, the family \( \phi_{\alpha,\beta} \) will admit a surface parameterizing \( N^{th} \) pre-images of the basepoint \( a \); call it \( S(N,a) \).\(^5\) Is the surface \( S(N,a) \) of general type for \( N \) sufficiently large?

**Future Prospect — Explicit Methods for Rational Points:** The explicit methods for finding rational points on curves in [FHS10] have also piqued my interest in a more general direction. Given a polynomial equation \( F(x,y) = 0 \) with rational coefficients, we may associate a projective algebraic curve \( C/\mathbb{Q} \). If this curve is irreducible of genus at least 2, we know by the work of Faltings that the equation \( F(x,y) = 0 \) has finitely many solutions \( (x,y) \in \mathbb{Q} \times \mathbb{Q} \). Or said another way, the set of rational points \( C(\mathbb{Q}) \) is finite. For various applications in number theory, one often needs to explicitly write down the set \( C(\mathbb{Q}) \), or at least compute its size. For example, much of our energy in [FHS10] was spent on trying to do exactly this for a curve of genus 3 (successful) and a curve of genus 5 (successful subject to certain standard conjectures). One of the central problems in Diophantine geometry is to answer

---

\(^5\)Some preliminary work has been done by A. Levin on the integral points of curves lying on \( S(N,a) \) [Lev10].
Question 2. Can one effectively determine the set \( C(\mathbb{Q}) \)?

A strategy for affirmatively answering this question via Arakelov theory has been proposed by Paršin and then refined by Moret-Bailly [Par88, MB90]. The idea is to give an upper bound of a certain shape for the square of the admissible relative dualizing sheaf \( \omega_\phi^2 \) associated to \( C/\mathbb{Q} \); it is analogous to the Bogomolov-Miyaoka-Yau inequality on algebraic surfaces. But this approach has the disadvantage of implying the abc-conjecture, which has always struck me as being too strong to be true.

Explicit calculations testing the plausibility of this strategy for certain genus 2 curves were performed by Bost, Mestre, and Moret-Bailly [BM89, BMM90]. Modern computing power and the recent work of S.-W. Zhang should make it possible to extend these calculations to a much larger class of hyperelliptic curves. If we suppose that \( C/\mathbb{Q} \) is hyperelliptic, then Zhang gives a formula for the square of the admissible dualizing sheaf \( \omega_\phi^2 \) in terms of differential invariants of the Riemann surface \( C(\mathbb{C}) \) and the reduction graphs \( \Gamma_p \) for \( p < \infty \) [Zha10]. I wrote Mathematica code to compute some of these invariants for a different purpose in my PhD thesis [Fab09], and I intend to revisit it (now using Sage) to survey the behavior of \( \omega_\phi^2 \) for a large number of curves.

Non-Archimedean Geometry

Given a compact Riemann surface \( X \) and a collection of points \( S = \{p_1, \ldots, p_n\} \) (not necessarily distinct), does there exist a meromorphic function \( f : X \to \mathbb{C} \cup \{\infty\} \) whose derivative vanishes exactly on \( S \)? Equivalently, does there exist a holomorphic map \( f : X \to \mathbb{P}^1 \) such that \( f \) is ramified exactly on \( S \)?

This classical question was investigated in the 19th century by a number of authors, including Riemann and Hurwitz. If \( X = \mathbb{P}^1 \) as well, and if \( S \subset \mathbb{P}^1 \) is a general subset satisfying certain necessary combinatorial conditions, then an affirmative answer is given in the work of Eisenbud and Harris on limit linear series [EH83]. The goal of my work in this area is to transport these questions over to a non-Archimedean setting, in which some new (non-algebraic!) phenomena arise. My motivation comes from certain applications to the ergodic theory of non-Archimedean dynamical systems [FRL10].

Let \( k \) be an algebraically closed field that is complete with respect to a nontrivial non-Archimedean absolute value. For example, \( k \) could be the completion of an algebraic closure of \( \mathbb{Q}_p \) or \( \mathbb{F}_p((t)) \). The projective line \( \mathbb{P}^1(k) = k \cup \{\infty\} \) endowed with the metric topology from \( k \), is neither connected nor locally compact. The Berkovich analytification of the projective line \( \mathbb{P}^1 \) over \( k \) was introduced to remedy these defects. It is a compact topological tree that contains a homeomorphic copy of \( \mathbb{P}^1(k) \). One may view it as a compactified parameter space of disks in \( \mathbb{P}^1(k) \). A rational function \( \phi : k(z) \to k(z) \) extends functorially to a morphism of \( \mathbb{P}^1 \) (which we also call \( \phi \)); intuitively, it describes the action of \( \phi \) on disks in \( \mathbb{P}^1(k) \).

Question 3. What is the correct analogue of the ramification divisor inside \( \mathbb{P}^1 \)? Said another way, what is the shape of the set of points in \( \mathbb{P}^1 \) at which \( \phi \) is not locally injective?

There is a local degree function \( m_\phi : \mathbb{P}^1 \to \{1, \ldots, \deg(\phi)\} \) that extends the usual algebraic multiplicity at points of \( \mathbb{P}^1(k) \), and we define the Berkovich ramification locus \( R_\phi = \{x \in \mathbb{P}^1 : m_\phi(x) > 1\} \). For example, any \( k \)-rational point that is ramified for the algebraic map \( \phi : \mathbb{P}^1_k \to \mathbb{P}^1_k \) lies inside \( R_\phi \).

In a manuscript currently in preparation, I have begun to answer the above question:

Theorem 4 ([Fab10b]). Suppose \( \phi \in k(z) \) is a rational function of degree \( d \geq 1 \). Then \( R_\phi \) is a disjoint union of at most \( d - 1 \) closed subtrees of \( \mathbb{P}^1_k \), none of which is reduced to a point. Write \( p = \text{res.char}(k) \). If \( p = 0 \) or \( p > d \), then \( R_\phi \) is the topological realization of a finite graph.

The pair \((R_\phi, m_\phi)\) consisting of the ramification locus equipped with the local degree function must satisfy certain strict combinatorial conditions. While I omit them in the interest of space, let us call them hypothesis (H). (They are closely related to the Hurwitz formula.) This allows us to generalize the question we asked in the introduction:

Question 4. Fix a general subset \( T \subset \mathbb{P}^1 \) equipped with a function \( \rho : T \to \{1, \ldots, d\} \) satisfying hypothesis (H). Does there exist a rational function \( \phi \in k(z) \) of degree \( d \) such that \((T, \rho) = (R_\phi, m_\phi)\)?

Footnotes:
6More precisely, if some \( p_i \) is repeated \( r \) times in \( S \), we required that \( \frac{d\phi}{dz} \) vanish to order exactly \( r \) at \( p_i \).
7The Hurwitz formula dictates that \( \# S = 2d - 2 \) and no point is repeated more than \( d - 1 \) times.
Let $\text{Rat}_d(k)$ be the parameter space of rational maps $\phi \in k(z)$ of degree $d \geq 1$. It is an affine variety of dimension $2d + 1$. Rather than asking about existence of maps, we may ask the more general

**Question 5.** Fix a subset $T \subset \mathbb{P}^1$ equipped with a function $\rho : T \to \{1, \ldots, d\}$ satisfying hypothesis (H). What is the structure of the set $Y(T, \rho) \subset \text{Rat}_d(k)$ of rational maps $\phi$ such that $(T, \rho) \cong (R_\phi, m_\phi)$ in some appropriate sense? Is it affinoid? Do the sets $Y(T, \rho)$ stratify $\text{Rat}_d(k)$ as we vary the pair $(T, \rho)$?

While I suspect the answer to all of these questions is “yes”, at present I can only show it for quadratic rational maps (easy) and for cubic rational maps (much harder). Questions 4 and 5 will be addressed in a second manuscript on this topic.

**Future Direction — Julia Sets:** Given a rational map $\phi \in \mathbb{C}(z)$ of degree at least 2, one may associate its Julia set; roughly, it is the locus in $\mathbb{P}^1(\mathbb{C})$ on which $\phi$ behaves chaotically under iteration. Many dynamical phenomena for the map $\phi$ can be explained by restricting attention to its Julia set.

Non-Archimedean dynamics began as the study of iteration of rational maps $\phi \in k(z)$ on the space $\mathbb{P}^1(k)$, but many authors soon realized that this space is inadequate for the task. For example, the analogous Julia set $J_\phi(k) \subset \mathbb{P}^1(k)$ can be empty, unlike its counter part in complex dynamics. This annoyance was remedied by passing to the Berkovich projective line $\mathbb{P}^1$, in which case the Berkovich Julia set $J_\phi$ is never empty. But a fundamental question to ask is

**Question 6.** What can be said about these new points $J_\phi \setminus J_\phi(k)$?

The simplest family of 1-dimensional non-polynomial dynamical systems is the quadratic family $\phi_c(z) = c(z + 1/z)$. Each map $\phi_c$ admits the nontrivial automorphism $z \mapsto -z$, which essentially cuts its complexity in half. Michelle Manes and I recently gave a complete description of the Julia sets for this family of maps [FM10].

Provided the residue characteristic of $k$ is different from 2, we found that $J_\phi \setminus J_\phi(k)$ is either empty, or else it consists of a single grand orbit of a repelling periodic cycle. A similar phenomenon occurs for polynomials [Tru10], but not for an arbitrary rational map [FRL10]. Further exploration is merited.

A rational function $\phi \in k(z)$ is called **tame** if its ramification locus is the topological realization of a finite graph (as in the second conclusion of Theorem 4). The presence of ramified points in the Julia set has important implications for the dynamics of the map. For tame polynomials, it is not too difficult to show that $R_\phi \cap J_\phi$ is a finite set, but the situation is more complicated for a general rational map. I believe it could be a suitable project for a PhD student to try to answer the following

**Question 7.** For which tame rational functions $\phi \in k(z)$ of degree at least 2 is it true that the intersection of the Julia set and the ramification locus in $\mathbb{P}^1$ is finite?

In another direction, dynamics on the Berkovich projective line can be used to study degenerations of complex dynamical systems. Let $f_t : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ be a holomorphic family of holomorphic dynamical systems that degenerates at $t = 0$. By this I mean that $f_t$ generically has degree $d \geq 2$, but $f_0$ has smaller degree. To this family, one can associated a dynamical system $f$ on the Berkovich projective line $\mathbb{P}^1_L$, where $L$ denotes the completion of the field of Puiseux series $\mathbb{C}\{t\}$. A number of experts have suggested that this type of degeneration can be studied by looking at the dynamics of $f$. Write $J_f \subset \mathbb{P}^1(\mathbb{C})$ for the Julia set of the complex dynamical system $f_t$. As a starting point, we might ask

**Question 8.** Is there a precise sense in which the Julia set $J_f$ converges to the Julia set of the associated Berkovich dynamical system $J_f$? (Note that they are supported on different spaces.)

Laura DeMarco and I can give an affirmative answer if the degeneration is not too singular [DF10], and we are working to extend our ideas to arbitrary degenerations. It appears to have some interesting connections with the theory of algebraically stable resolutions of surface endomorphisms.

---

8We started this work to enlarge the arena for testing arithmetic conjectures on families of dynamical systems. At present, most of the relevant literature focuses on the family $f_c(z) = z^2 + c$.

9Compare with the results of E. Trucco for tame polynomials [Tru10].

10For example, Jan Kiwi has made a precise connection for quadratic rational maps and cubic polynomials [Kiw10, Kiw06].