RESEARCH STATEMENT

Andrew W. Herring

1 Introduction

My research belongs to the fast growing field of arithmetic dynamics in which we ask number-theoretic questions of dynamical systems. Specifically, my work considers periodic points of a dynamical system defined by iterating a quadratic polynomial $f_c(x) := x^2 + c \in \mathbb{Q}[x]$.

A point $\alpha \in \bar{\mathbb{Q}}$ is **periodic** for f_c if it is sent to itself by some finite iterate f_c^n of f_c, and then the **period** of α is the smallest positive n satisfying $f_c^n(\alpha) = \alpha$. Many experts have asked about the possible periods of points $\alpha \in \mathbb{Q}$ under f_c; the most important conjecture along these lines is due to Flynn, Poonen, and Schaefer:

Conjecture 1.1 ([5], 1995)**.** *Fix a rational number c and an integer $n \geq 4$. Then there is no $\alpha \in \mathbb{Q}$ of period n for f_c.*

My primary research goal is to prove a slightly weaker version of this hard problem:

Problem 1.2. *Prove that for every $n \geq 5$ there are at most finitely many $c \in \mathbb{Q}$ for which f_c has a point $\alpha \in \mathbb{Q}$ of period n.*

1.1 Bigger picture: uniform boundedness The importance of Problem 1.2 owes to its relation to the Dynamical Uniform Boundedness Conjecture of Morton and Silverman [12]. This powerful conjecture's influence extends beyond arithmetic dynamics—e.g. in number theory it implies not only Mazur's theorem [10] on the size of torsion subgroups for elliptic curves over $\mathbb{Q}$, but also an unproven analogue for arbitrary abelian varieties over number fields [4]. Here is a very special case:

Conjecture 1.3 ([12], 1994)**.** *There is a bound, independent of $c \in \mathbb{Q}$, on the number of $\alpha \in \mathbb{Q}$ for which some iterate $f_c^k(\alpha)$ is periodic*

Even this "simplest possible" case remains unsolved, although Poonen showed in [14] that it suffices to prove Conjecture 1.1. The works [11, 5] solved Conjecture 1.1 in the cases $n = 4, 5$ respectively, and [15] gave a conditional proof for the $n = 6$ case. In [9], Krumm solved problem 1.2 in the special cases $n = 5, 6, 7, 9$, but no other progress has been made.

My thesis considers Problem 1.2 in the (as yet) smallest unsolved case of $n = 8$. The essence of my approach involves calculating the genus of several curves using the Riemann-Hurwitz formula. This in turn relies upon knowledge of various "ramification data" as well as maximal subgroups of a certain semi-direct product.

2 Research methods

2.1 Dynatomic polynomials Let t be transcendental over $\mathbb{Q}$, and let $K := \mathbb{Q}(t)$, the rational function field over $\mathbb{Q}$. In this section we consider the general quadratic $f(x) = x^2 + t \in K[x]$ and the associated **n-th dynatomic polynomial**

$$\Phi_n(x) := \prod_{d|n} (f^d(x) - x)^{\mu(n/d)} \in K[x]$$

where $\mu : \mathbb{Z}_{>0} \to \{0, \pm 1\}$ is the Möbius function. We also consider the splitting field Σ_n of Φ_n over K, its Galois group G_n, and the subset $Z_n \subset \Sigma_n$ of zeros of Φ_n. A standard argument shows that Z_n consists precisely of the points of period n for f, and that $\deg(\Phi_n) = |Z_n| = nr$ for some positive integer r.

It is know that $\Phi_n(x)$ is irreducible over $\bar{\mathbb{Q}}(t)$, hence G_n is a transitive subgroup of $\mathrm{Sym}(Z_n)$. In fact, G_n is the subgroup of $\mathrm{Sym}(Z_n)$ of all automorphisms τ which commute with f, and hence G_n is isomorphic to the semi-direct product $(\mathbb{Z}/n\mathbb{Z})^r \rtimes S_r$ [1].

2.2 Specializations and exceptional values Recall that the zeros of $\Phi_n(x)$ are the n-periodic points for $f(x) = x^2 + t$, and Σ_n is the splitting field of Φ_n over $K = \mathbb{Q}(t)$. Similarly, for any $c \in \mathbb{Q}$ and $f_c(x) = x^2 + c \in \mathbb{Q}[x]$, the zeros of the specialized polynomial

$$\Phi_{n,c}(x) := \prod_{d|n} (f_c^d(x) - x)^{\mu(n/d)} \in \mathbb{Q}[x]$$

are the n-periodic points for f_c. Thus the splitting field $\Sigma_{n,c}$ of $\Phi_{n,c}$ is finite and Galois over $\mathbb{Q}$.

It is known that the Galois group $G_{n,c}$ of $\Sigma_{n,c}$ over $\mathbb{Q}$ is a subquotient of G_n (in fact, it is usually a subgroup). We say that $G_{n,c}$ is **big** if it equals G_n, and otherwise we say that c is an **exceptional value**. I am interested in the Galois groups $G_{n,c}$ and G_n because of their relation to Problem 1.2.

Claim 2.1. *If $G_{n,c}$ is big, then f_c has no n-periodic points in $\mathbb{Q}$. Equivalently, if f_c has a point $\alpha \in \mathbb{Q}$ of period n, then c is an exceptional value.*

Claim 2.1 allows us to restate Problem 1.2 as: *Show that for every $n \geq 5$, there are only finitely many $c \in \mathbb{Q}$ which are exceptional values.*

2.3 Exceptional values and rational points on curves The extension Σ_n/K is an extension of function fields over $\mathbb{Q}$. Therefore we have curves[1] X_n and $\mathbb{P}^1$ corresponding to Σ_n and $K = \mathbb{Q}(t)$ respectively, and the inclusion $K \subseteq \Sigma_n$ induces a surjective curve morphism $\phi : X_n \to \mathbb{P}^1$. An **intermediate curve** consists of a curve Y together with surjective morphisms $\psi : X_n \to Y$ and $\pi : Y \to \mathbb{P}^1$ such that $\phi = \pi \circ \psi$, and the degree of π is at least two. These intermediate curves grant us access to exceptional values.

Claim 2.2. *The rational number c is an exceptional value if and only if it lies in the image of some $\pi : Y \to \mathbb{P}^1$, where Y is an intermediate curve.*

For any curve C, let $C(\mathbb{Q})$ denote the set of all $\mathbb{Q}$-rational points of C. If c is an exceptional value, then Claim 2.2 tells us that $c = \pi(d)$ where Y is an intermediate curve with morphism $\pi : Y \to \mathbb{P}^1$ and $d \in Y(\mathbb{Q})$. For a fixed n there are only finitely many intermediate curves Y, so for Problem 1.2 it suffices to prove that for every $n \geq 5$ and every intermediate curve Y of $X_n \to \mathbb{P}^1$, the set $Y(\mathbb{Q})$ of all $\mathbb{Q}$-rational points of Y is finite.

2.4 Genus The **genus** of a curve Y is a measure of geometric complexity, and we denote it by $g(Y)$. For a Riemann surface Y (a curve over $\mathbb{C}$) the genus $g(Y)$ is the number of its "handles."

In number theory, the celebrated theorem of Faltings exhibits the genus as a measure of arithmetic complexity as well: *if Y is a curve and $g(Y) \geq 2$, then $Y(\mathbb{Q})$ is finite.* We have thus reduced Problem 1.2 even further: according to Faltings' Theorem, it suffices to show that for every $n \geq 5$ and every intermediate curve Y, the genus $g(Y) \geq 2$. Two natural sub-problems are suggested.

The first sub-problem asks that for each $n \geq 5$, we determine all the intermediate curves Y of $X_n \to \mathbb{P}^1$. According to the Galois theory of curves, this is equivalent to the problem of determining all maximal subgroups of the Galois group G_n.

The second subproblem asks us to prove that $g(Y) \geq 2$ for every intermediate curve Y. The main tool toward this objective is the Riemann-Hurwitz genus formula. Calculating $g(Y)$ explicitly tends to be hard. Fortunately however, it suffices to bound $g(Y)$ from below for which techniques exist.

3 In the Past

While my primary focus is on arithmetic dynamics, I also have experience in algebraic graph theory, and I am continually looking for ways to apply this experience in arithmetic dynamics.

[1] By a curve we will mean a smooth projective geometrically irreducible curve which is defined over $\mathbb{Q}$.

In my MS thesis, I translated some classical results from algebraic topology into graph theory. First I described a category of graphs amenable to discussing covering spaces and fundamental groups, and then I showed that the equivalence between covering spaces and subgroups of "the" fundamental group remains valid in that category [7]. This exercise provided vital background for the paper [8] mentioned below.

Expander graphs are widely studied because they are at once highly connected, yet sparse (hence interesting to network scientists, for example). They can have surprising applications in arithmetic geometry as in the work [3] where expansion properties of Cayley graphs were used to prove a "genus grows" statement (see problem 4.1).

Ramanujan graphs are "optimal" expanders. In [13], degree 2 (graph) covers were used to show that there are infinitely many d-regular Ramanujan graphs for every $d \geq 2$. The r-matching polynomial was introduced in [8] in order to extend the argument of [13] to degree r covers for every r. In [2], we proved a functional equation for the r-matching polynomial of cycle graphs, and along the way gave (we believe) the first graph-theoretic proof that certain Chebyshev polynomials[2] commute under composition.

4 In the Future

Most of my time is occupied by thinking about my thesis problems of proving Problem 1.2 in the case $n = 8$ and also trying to understand all maximal subgroups of the Galois group G_n. Whenever time permits though, I cannot resist thinking about some natural longer term research goals. One of these involves proving that "**genus grows with** n:"

Problem 4.1. *Let g_0 be a non-negative integer. Prove that there is a constant $n(g_0)$ such if $n \geq n(g_0)$, then $g(Y) \geq g_0$ for every intermediate curve Y of $X_n \to \mathbb{P}^1$.*

Other "genus grows" like statements appear in arithmetic geometry. The paper [3] deduces arithmetic consequences (for "families of division fields") by proving that genus grows. I am especialy intrigued by [3] because the authors prove that "genus grows" by showing that a family of Cayley graphs has nice expansion properties. Given that their approach unifies number theory and graph theory, I would be very excited to emulate this method in arithmetic dynamics.

Another area which profitably combines number theory and graph theory is **isogeny-based cryptography**. Given that the advent of a full scale and efficient quantum computer seems increasingly inevitable, our society must create new "post-quantum cryptosystems" which we believe will resist attacks by such machines. One proposal along these lines is built upon "supersingular isogeny graphs." The set of all supersingular elliptic curves together with isogenies form a Ramanujan graph; a fact which combines my primary areas of interest. The champions of isogeny-based cryptography are betting that this Ramanujan graph structure yields problems which are too hard even for a quantum computer, and I would love to lend my experience in arithmetic geometry and graph theory to their cause.

[2] Chebyshev polynomials appear in graph theory as the (classical) matching polynomials of the cycle graphs. See [6].

References

[1] Thierry Bousch. "Sur quelques problemes de dynamique holomorphe". PhD thesis. Paris 11, 1992.

[2] Garner Cochran, Corbin Groothuis, Andrew Herring, Ranjan Rohatgi, and Eric Stucky. *A New [Combinatorial] Proof of the Commutativity of Matching Polynomials for Cycles*. 2018. arXiv: 1810.05889 [math.CO].

[3] Jordan S. Ellenberg, Chris Hall, and Emmanuel Kowalski. "Expander graphs, gonality, and variation of Galois representations". In: *Duke Math. J.* 161.7 (2012), pp. 1233–1275. ISSN: 0012-7094.

[4] Najmuddin Fakhruddin. "Boundedness results for periodic points on algebraic varieties". In: *Proc. Indian Acad. Sci. Math. Sci.* 111.2 (2001), pp. 173–178. ISSN: 0253-4142.

[5] EV Flynn, Bjorn Poonen, and Edward F Schaefer. "Cycles of quadratic polynomials and rational points on a genus-two curve". In: *arXiv preprint math/9508211* (1995).

[6] C. D. Godsil. *Algebraic combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993, pp. xvi+362. ISBN: 0-412-04131-6.

[7] Andrew Herring. "Groups and Covers of Graphs". MA thesis. Laramie, WY: University of Wyoming, 2016. URL: http://publish.uwo.ca/~aherrin6/research/AWH_MS_THESIS.pdf.

[8] Chris Hall, Doron Puder, and William F. Sawin. "Ramanujan coverings of graphs". In: *Advances in Mathematics* 323 (2018), pp. 367–410. ISSN: 0001-8708.

[9] David Krumm. "A finiteness theorem for specializations of dynatomic polynomials". In: *Algebra & Number Theory* 13.4 (2019), pp. 963–993.

[10] B. Mazur. "Modular curves and the Eisenstein ideal". In: *Inst. Hautes Études Sci. Publ. Math.* 47 (1977). With an appendix by Mazur and M. Rapoport, 33–186 (1978). ISSN: 0073-8301.

[11] Patrick Morton. "Arithmetic properties of periodic points of quadratic maps, II". In: *Acta Arithmetica* 87.2 (1998), pp. 89–102.

[12] Patrick Morton and Joseph H Silverman. "Rational periodic points of rational functions". In: *International Mathematics Research Notices* 1994.2 (1994), pp. 97–110.

[13] Adam Marcus, Daniel A Spielman, and Nikhil Srivastava. "Interlacing families I: Bipartite Ramanujan graphs of all degrees". In: *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*. IEEE. 2013, pp. 529–537.

[14] Bjorn Poonen. "The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture". In: *Mathematische Zeitschrift* 228.1 (1998), pp. 11–29.

[15] Michael Stoll. "Rational 6-cycles under iteration of quadratic polynomials". In: *LMS Journal of Computation and Mathematics* 11 (2008), pp. 367–380.