Christopher Keyes
Research Statement
christopher.keyes@kcl.ac.uk
https://c-keyes.github.io/

1. Overview

My research interests lie in **number theory**, specifically in arithmetic geometry and arithmetic statistics. **Arithmetic geometry** involves exploiting geometry to study equations defined over the rational numbers $\mathbb{Q}$ and, more generally, over other fields of arithmetic interest such as number fields, p-adic fields, or finite fields. **Arithmetic statistics**, broadly interpreted, encompasses fundamentally quantitative questions about prime numbers, number fields, solutions to equations, and other central objects of number theory.

Rational points lie at the heart of the intersection of these areas. Given a system of polynomial equations with coefficients in $\mathbb{Q}$, a **rational point** is a solution in rational numbers to the defining equations. More generally, a ***K*-point** is a solution in a field K containing $\mathbb{Q}$. The study of rational points dates back to antiquity, and despite centuries of progress, remains a source of profound mystery, even underpinning some modern cryptographic protocols. This brings us to the first of two motivating questions around which my research centers.

Question 1. *Given a system of equations defined over $\mathbb{Q}$, what quantitative statements hold for the set of rational points?*

Denoting our system of equations by X and its set of rational points by $X(\mathbb{Q})$, one can ask about the size of $X(\mathbb{Q})$, or merely attempt to determine whether it is infinite, finite, or empty. This deceptively simple question is deep and often challenging to answer, while intimately related to the underlying geometry of X. For example, when X defines a curve, Faltings' theorem states $X(\mathbb{Q})$ is finite whenever the *genus* of X — a geometric invariant measuring the complexity of a curve — is at least two. In this case it is often still difficult to determine whether any rational points exist at all on a given X.

Oftentimes, we can gain valuable insight about typical and extremal behavior by instead allowing X to vary within a family of interest. This leads to our second central motivating question.

Question 2. *Given a family of systems of equations defined over $\mathbb{Q}$, how many have a rational point?*

A common theme in answering Question 2 is to first understand local behavior, that is, to understand how often X has solutions in the real numbers $\mathbb{R}$ and the p-adic numbers $\mathbb{Q}_p$. The latter boils down to studying the defining equations of X up to powers of a prime p. If X has $\mathbb{R}$-points and $\mathbb{Q}_p$-points for all primes p, we call X **everywhere locally soluble**. In special cases, such as for X given by the vanishing of a quadratic form, everywhere local solubility is sufficient to guarantee X has a rational point; this is known as a **local-to-global principle**, or Hasse principle. In general, however, everywhere local solubility is *not enough* to guarantee X has a rational point. This motivates modifying Question 1 to consider $X(\mathbb{Q}_p)$, or Question 2 to consider how often X in some collection satisfies the local-to-global principle.

Questions 1 and 2 guide my research in multiple directions, three of which I highlight here:

Points on hypersurfaces (§2). In the family of cubic hypersurfaces in projective space, we give a *precise numerical answer* to Question 2 through careful study of p-adic solubility in this family (see Theorem 3, [BK25b]). We also consider a conjecture due to Artin, and prove that hypersurfaces of degrees 5 and 7 in enough variables over $\mathbb{Q}_p$ *always* have $\mathbb{Q}_p$-points when p is sufficiently large (see Theorems 6 and 7, [BK25a]).

Generalized Fermat equations (§3). We characterize a local-to-global principle for *integral* solutions to equations of the form $x^2 + By^2 = Cz^n$, both geometrically in terms of descent, and algebraically in terms of class groups of orders of quadratic fields (see Theorem 8, [DRKK$^+$]). We also study *how often* they satisfy a local-to-global principle (see Theorem 9, [DRKK$^+$]).

Superelliptic curves (§4). We show that for 96.94% of degree 6 forms $f(x, z)$, the curve given by $C_f \colon y^3 = f(x, z)$ is everywhere locally soluble (see Theorem 12, [BK23]). For these and similar curves, we count number fields K coming from K-points of certain degrees (see Theorem 13, [Key22, BK26]).

Throughout, I highlight potential future directions and opportunities for **student involvement** within my research program. Some additional topics and potential projects are discussed in §5.

2. Points on hypersurfaces

A degree d hypersurface in n-dimensional projective space $\mathbb{P}^n$ is given by the vanishing of an integral homogeneous degree d polynomial $f(x_0,\dots,x_n)$ and denoted $X_f \subset \mathbb{P}^n$. Such f are also known as degree d *forms*. Thus, the study of points on degree d hypersurfaces X_f and nontrivial zeros of degree d forms f go hand-in-hand. Motivated by Question 2, for fixed degree d and dimension n, we seek to understand how often X_f has a rational point. To make sense of "how often," we use a height function $\mathrm{ht}(f)$ which associates a positive real value to f, allowing us to define natural densities

$$\rho_{d,n} = \lim_{B\to\infty} \frac{\#\{f : \mathrm{ht}(f) \le B,\ X_f(\mathbb{Q}) \neq \emptyset\}}{\#\{f : \mathrm{ht}(f) \le B\}}, \quad \rho_{d,n}^{\mathrm{ELS}} = \lim_{B\to\infty} \frac{\#\{f : \mathrm{ht}(f) \le B,\ X_f \text{ is everywhere loc. sol.}\}}{\#\{f : \mathrm{ht}(f) \le B\}}.$$

We should think of the density $\rho_{d,n}$ (resp. $\rho_{d,n}^{\mathrm{ELS}}$) as a proxy for the *probability* that a randomly chosen degree d hypersurface in $\mathbb{P}^n$ has a rational point (resp. is everywhere locally soluble). Let $\rho_{d,n}(p)$ and $\rho_{d,n}(\infty)$ be the probability that a random X_f has a $\mathbb{Q}_p$-point and $\mathbb{R}$-point, respectively. Poonen and Voloch [PV04] showed that these probabilities are *independent* in a strong sense, establishing a product formula

$$\rho_{d,n}^{\mathrm{ELS}} = \rho_{d,n}(\infty) \textstyle\prod_p \rho_{d,n}(p). \tag{1}$$

Exciting recent work of Browning, Le Boudec, and Sawin [BLBS23] shows that when $n \ge d$, $(n,d) \neq (3,3)$, we have $\rho_{d,n} = \rho_{d,n}^{\mathrm{ELS}}$, settling a conjecture of Poonen and Voloch [PV04] (except for cubic surfaces in $\mathbb{P}^3$). In other words, in these cases *100% of X_f satisfy the local-to-global principle*. Moreover, if we can access the local probabilities $\rho_{d,n}(p)$, we can give an explicit answer to Question 2 for degree d hypersurfaces in $\mathbb{P}^n$.

2.1. Cubic hypersurfaces.

In joint work with Beneish [BK25b], we answer Question 2 for cubic hypersurfaces in $\mathbb{P}^n$ for $n \ge 4$. Following [BLBS23] and (1), we have $\rho_{3,n} = \prod_p \rho_{3,n}(p)$, and we give a formula for the local probabilities $\rho_{3,n}(p)$, as rational functions *uniform in p*.

Theorem 3 (Beneish–K. [BK25b, Theorem 2.3])**.** *For all $n \ge 1$, there exist explicit rational functions $R_n(t) \in \mathbb{Q}[t]$ such that $\rho_{3,n}(p) = R_n(p)$.*

When $n \ge 9$, $\rho_{3,n}(p) = 1$ was known due to Lewis [Lew52], and $\rho_{3,n} = 1$ was shown in celebrated work of Heath-Brown using the circle method [HB83]. The proof of Theorem 3 also recovers a result of Bhargava, Cremona, and Fisher computing $\rho_{3,2}^{\mathrm{ELS}}$, i.e. the likelihood that a plane cubic curve is everywhere locally soluble [BCF16]. A striking feature of Theorem 3 is the *uniform* nature of the local probabilities $\rho_{3,n}(p)$ (see e.g. Theorem 12, where in a family of superelliptic curves, similar local probabilities are not given uniformly by a rational function). This uniformity is explored further for hypersurfaces of higher degree in §2.2.

Theorem 3 is established by studying when points on the reduction of X_f modulo p lift to $\mathbb{Q}_p$-points on X_f. To further illustrate the explicit nature of this approach and the results, consider the case of cubic surfaces in $\mathbb{P}^3$. Our methods, together with the remaining open case of Poonen and Voloch's conjecture, yield the following.

Conjecture 4 (Beneish–K. [BK25b])**.** *The density of cubic surfaces in $\mathbb{P}^3$ with a rational point is given by*

$$\rho_{3,3} = \prod_p \left(1 - \frac{(3p^{26}+p^{24}+p^{23}+4p^{22}-3p^{21}+3p^{20}+2p^{19}+2p^{18}-p^{17}+p^{14}+p^{13}-2p^{12}+3p^{11}+3p^7)(p^2+1)(p+1)^2(p-1)^4}{9(p^{13}-1)(p^7+1)(p^7-1)(p^6+1)(p^5-1)(p^3+1)(p^3-1)}\right) \approx 0.999927.$$

2.2. Artin's Conjecture.

An analogue of the uniformity in p present in Theorem 3 was conjectured by Artin for higher degrees. He conjectured that for all degrees d and $n \ge d^2$, every degree d homogeneous polynomial $f \in \mathbb{Q}_p[x_0,\dots,x_n]$ has a nontrivial zero in $\mathbb{Q}_p$. In geometric language, *every* degree d hypersurface $X_f/\mathbb{Q}_p$ *in sufficiently many variables* has a $\mathbb{Q}_p$-point. This conjecture was shown to be false by Terjanian, who constructed a counterexample with $d = 4$, $n = 17$, and $p = 2$ [Ter66]. However, in all known counterexamples to the conjecture, d is composite and divisible by $p-1$, leaving us with a tantalizing question:

Question 5. *If d is prime, does every degree d form $f \in \mathbb{Q}_p[x_0,\dots,x_{d^2}]$ have a nontrivial zero in $\mathbb{Q}_p$?*

Question 5 has been answered in the affirmative for $d = 2, 3$ due to Hasse and Lewis [Lew52], respectively. Ax and Kochen showed that for fixed d, if p is taken sufficiently large, the answer to Question 5 is "yes" [AK65]. Actually pinning down how large p has to be for their results to be effective is challenging.

In low degrees, a p-adic minimization procedure dating back to Birch–Lewis [BL59] and Laxton–Lewis [LL65] has proven fruitful. Their strategy was to reduce to the case of finding nonsingular solutions to f modulo p, which may be lifted to zeros of f in $\mathbb{Q}_p$ via Hensel's lemma. This strategy breaks down for primes $d > 11$, since such d can be written as the sum of composite numbers, permitting the reduction of X_f modulo p to have totally nonreduced nonlinear components. In joint work with Beneish, we improve the state-of-the-art in degrees 5 and 7.

Theorem 6 (Beneish–K.)**.** *If $p > 5$, every quintic form $f \in \mathbb{Q}_p[x_0, \ldots, x_{25}]$ has a nontrivial zero in $\mathbb{Q}_p$.*

In the quintic case, our onging work builds upon further refinements and extensive computations [LY96, HB10, Dum17]. Making further progress has involved carrying out a search for nonsingular zeros in a family of quaternary quintic forms defined over the finite field $\mathbb{F}_p$. One key innovation needed to successfully carry out this search for $p \geq 7$ and prove Theorem 6 is an implementation in C++/CUDA, run on modern GPUs, taking maximal advantage of *parallelization* opportunities in the search algorithm.

Theorem 7 (Beneish–K. [BK25a])**.** *If $p > 679$, every deg. 7 form $f \in \mathbb{Q}_p[x_0, ..., x_{49}]$ has nontrivial zero in $\mathbb{Q}_p$.*

In degree 7, our work builds upon the base strategy by employing an effective Bertini theorem. The classical Bertini theorem states that if X_f is a smooth irreducible hypersurface, then *generically* the intersection with a hyperplane remains smooth and irreducible. However, when working over the finite field $\mathbb{F}_p$, it is possible that no single such hyperplane exists; an *effective* Bertini theorem reveals how large p must be before the existence of such a hyperplane is guaranteed. Wooley used an effective Bertini theorem to reduce to a plane curve, where point counting techniques are especially effective, to answer Question 5 in degrees 7 and 11 when p is sufficiently large. To improve on this, we give a novel effective Bertini theorem [BK25a] enabling us to ensure the presence of *singular* $\mathbb{F}_p$-points on our plane curves, thereby improving the point counts.

2.3. Future directions. We are actively working on extending Theorem 6 to $p \leq 5$. A next step is to search over a family of quintic forms over $\mathbb{F}_5$ in 5 variables, in hopes of showing all members have a nonsingular zero. Further theoretical and computational innovation has the potential to yield an exciting breakthrough for $p < 5$, with the potential to definitively settle Question 5 in the quintic case.

Theorems 3, 6, and 7 also suggest a number of other promising directions.

- Does the local probability $\rho_{d,n}(p)$ have a nice description for $d > 3$? Do these probabilities enjoy the same uniformity as their cubic counterparts, at least when p is large? How large?
- Wooley also gave an answer to Question 5 in degree 11 when p is large [Woo08]. Can this be improved, possibly using the refined effective Bertini theorems used to prove Theorem 7?
- Artin's conjecture and Question 5 have analogues for simultaneous zeros of forms. Can we leverage Bertini theorems or computational techniques to answer them or improve existing results (e.g. [Zah11])?

Variations on this theme of local solubility in families of equations would make an ideal student project. Armed with little more than a working knowledge of p-adic numbers, such a project would suit a wide range of backgrounds and interests, from algebraic geometry to computational number theory.

3. Generalized Fermat equations

Given natural numbers p, q, r, a **generalized Fermat equation** is given by

$$Ax^p + By^q + Cz^r = 0. \tag{2}$$

Much study has been made of integer solutions (x, y, z) to (2); most famously, Fermat's last theorem states that for $p = q = r \geq 3$ and $A, B, C = 1$, the only solutions satisfy $xyz = 0$. More generally, Darmon and Granville [DG95] showed that when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$, a generalized Fermat equation has at most *finitely* many primitive integer solutions. If $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$, then (2) has either *no solutions* or *infinitely* many [Beu98].

In the latter case, to determine the existence of integral solutions (hence infinitely many) to a generalized Fermat equation, we associate to $\mathcal{Y}$ a geometric object whose integral points $\mathcal{Y}(\mathbb{Z})$ are in bijection with solutions to (2). This $\mathcal{Y}$ naturally has the structure of a *stacky curve*, owing to the fact that (2) is not

necessarily homogeneous; in this case, the stacky structure is essentially carrying out extra bookkeeping to keep track of a relevant *weighted* group action.

Nevertheless, $\mathcal{Y}$ enjoys many familiar features of ordinary algebraic curves, and Questions 1 and 2 are easily translated to *integral* points in this setting. In particular, there is a notion of a local-to-global principle for integral points: if (2) has solutions in the p-adic integers $\mathbb{Z}_p$ for all p, as well as real solutions, we say $\mathcal{Y}$ is everywhere locally soluble; if everywhere local solubility implies $\mathcal{Y}(\mathbb{Z})$ is nonempty, then $\mathcal{Y}$ satisfies the local-to-global principle for integral points. Bhargava and Poonen [BP22] gave novel examples of stacky curves which fail this local-to-global principle, which were further explored by Santens [San23].

In [DRKK+], we consider the family of generalized Fermat equations given by

$$\mathcal{Y}_{B,C}\colon x^2 + By^2 = Cz^n.$$

In the vein of Question 1, or aim is to determine when $\mathcal{Y}_{B,C}(\mathbb{Z})$ and $\mathcal{Y}_{B,C}(\mathbb{Z}_p)$ are nonempty.

To understand the local situation, we give a complete characterization of (B, C) for which $\mathcal{Y}_{B,C}(\mathbb{Z}_p) \neq \emptyset$, in terms of p-adic valuations and quadratic residues. To find integral points, we offer an approach inspired by classical methods from algebraic curves, adapted to the more general setting of stacks. In particular, we perform an explicit *descent*, in which we characterize integral points in $\mathcal{Y}_{B,C}(\mathbb{Z})$ as lying in the image of finitely many maps from algebraic curves $\mathcal{C}_d$; here the parameter d is a class in $K^\times/(K^\times)^n$ for the quadratic field $K = \mathbb{Q}(\sqrt{-B})$, satisfying some additional conditions. An upshot of our analysis is an equivalent interpretation in terms of the class group of K, $\mathrm{Cl}(K)$, described below in Theorem 8.

Theorem 8 (Duque-Rosero–K.–Kobin–Roy–Sankar–Wang [DRKK+, Theorem A])**.** *Let $B \equiv 1, 2 \pmod 4$ be squarefree and suppose C is squarefree and coprime to B. Set $K = \mathbb{Q}(\sqrt{-B})$. There exists an explicit finite set $A_{B,C} \subset K^\times/(K^\times)^n$, depending on B, C, n, such that the following are equivalent:*

(i) $\mathcal{Y}_{B,C}(\mathbb{Z}) \neq \emptyset$*;*

(ii) $A_{B,C} \neq \emptyset$ *and C is not divisible by any inert primes of K;*

(iii) C factors over $\mathcal{O}_K$ as $C\mathcal{O}_K = J_+J_-$, where J_+, J_- are conjugate and coprime, such that $[J_\pm] \in n\mathrm{Cl}(K)$.

The equivalence of (i) and (iii) above was known previously in limited cases due to Darmon and Granville [DG95, Prop. 8.1]. The geometric origin of (ii) recovers this equivalence while adding the geometric context. We are also able to remove the squarefree hypotheses on B and C and produce an algorithm for determining whether or not $\mathcal{Y}_{B,C}$ satisfies the local-to-global principle for integral points in much greater generality.

Motivated by Question 2, we also consider *how often* $\mathcal{Y}_{B,C}$ satisfies the local-to-global principle. To answer this question, we count the number of (B, C) for which $\mathcal{Y}_{B,C}$ has an integral point,

$$N_n(T) = \#\left\{(B, C) \in \mathbb{Z}^2 : |B|, |C| \leq T,\ \mathcal{Y}_{B,C}(\mathbb{Z}) \neq \emptyset\right\},$$

and similarly $N_n^{\mathrm{loc}}(T)$ counts those which have points everywhere locally. In contrast to the situation of hypersurfaces explored in §2, it turns out that $\mathcal{Y}_{B,C}$ has points locally *0% of the time*; more precisely, $N_n^{\mathrm{loc}}(T)$ grows like $T^2/\sqrt{\log T}$ [DRKK+, Theorem C]. Of these, however, it turns out a positive proportion have integral points when $n = 3$.

Theorem 9 ([DRKK+, Theorem D])**.** *For $n = 3$, at least 0.988% of everywhere locally soluble $\mathcal{Y}_{B,C}$ satisfy the local-to-global principle for integral points.*

A similar result holds for odd primes $n > 3$, conditional on an estimate for the average n-rank of class groups of quadratic fields, which follows from the Cohen–Lenstra heuristics.

3.1. Future directions. In ongoing work, we are considering how similar methods shed light on a local-to-global principle for primitive integral solutions to (2) with $(p, q, r) = (3, 3, 2)$. There, the relevant cover has group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (as opposed to $\mathbb{Z}/n\mathbb{Z}$), and the 2-part of the class group of a *cubic* extension appears to be related to obstructions to the local-to-global principle for integral points.

The statistical result [DRKK+, Theorem C] for $N_n^{\mathrm{loc}}(T)$ fits into a larger program of studying local solubility in families, where existing literature (e.g. [BBL16, LS16]) focuses on families of varieties, rather than stacks. Our results, together with preliminary results on generalized Fermat equations with $(p, q, r) = (m, m, n)$ more generally, suggest these statistics may behave differently in the setting of stacks.

Question 10. *Given a family of stacky curves (or more generally stacks) parametrized by a fibration $\mathcal{Y} \to \mathbb{A}^n$, how many have integral points everywhere locally?*

4. Superelliptic curves

Let $m \geq 2$ be a positive integer and $m \mid d$. A **superelliptic curve** $C_f/\mathbb{Q}$ is given by an equation

$$C_f \colon y^m = f(x, z), \tag{3}$$

where f is an integral binary form of degree d. When $m = 2$, C_f is known as a **hyperelliptic curve**. Much like quadratic (and cyclic) extensions are the first nontrivial examples of field extensions, hyperelliptic (and superelliptic) curves are in some sense the simplest family of curves beyond the projective line $\mathbb{P}^1$.

4.1. Local solubility. In the spirit of Question 2, we ask how often C_f given by (3) has a rational point. In the hyperelliptic case, cornerstone work of Bhargava, Gross, and Wang [BGW17] shows that when suitably counted, a positive proportion of C_f fail the local-to-global principle for rational points. In fact, they go further to show that a positive proportion of C_f have no K-points for *any odd degree field extension* $K/\mathbb{Q}$.

For $m > 2$, however, even the very first step of their approach — determining how often C_f is everywhere locally soluble – remained open. In joint work with Beneish [BK23], we study the proportion of superelliptic curves over $\mathbb{Q}$ which are everywhere locally soluble.

This proportion, denoted $\rho^{\mathrm{ELS}}_{m,d}$, represents the probability that for a randomly chosen degree d form f, the superelliptic curve C_f is everywhere locally soluble. This is defined in a similar manner as in the case of hypersurfaces discussed in §2. Also like the case of hypersurfaces, $\rho_{m,d}$ is nonzero and can be expressed by a product of local probabilities $\rho_{m,d}(p)$ and $\rho_{m,d}(\infty)$ which capture the likelihood of C_f having p-adic and real points, analogous to (1).

Theorem 11 (Beneish–K., [BK23, Theorem A])**.** *For all $m \geq 2$ and d such that $m \mid d$ and $(m, d) \neq (2, 2)$,*

$$\rho^{\mathrm{ELS}}_{m,d} = \rho_{m,d}(\infty) \textstyle\prod_p \rho_{m,d}(p) > 0.$$

By studying $\mathbb{F}_p$-points on the reduction of C_f modulo a prime p, we can determine when they give rise to a $\mathbb{Q}_p$-point of C_f, leading to effective bounds for $\rho_{m,d}(p)$. In the case of $(m, d) = (3, 6)$, we determine $\rho_{m,d}(p)$ exactly for all p, yielding a numerical result for $\rho^{\mathrm{ELS}}_{3,6}$.

Theorem 12 (Beneish–K., [BK23, Theorem C])**.** *For 96.94% of sextic forms $f(x, z)$, we have $C_f \colon y^3 = f(x, z)$ is everywhere locally soluble.*

More precisely, we give explicit rational functions $R_1(t), R_2(t)$ for which $\rho_{3,6}(p) = R_i(p)$ whenever $p \equiv i \pmod 3$ is sufficiently large. Considerable care and additional computations are needed to determine $\rho_{3,6}(p)$ for small primes p, as they do not conform to the same formulae.

Contrast this to the situation of cubic hypersurfaces in Theorem 3: while there is some uniformity in $\rho_{3,6}(p)$, the dichotomy between residue classes modulo 3 is a considerable departure from Theorem 3. Moreover, the limited uniformity does *not* extend to the smallest primes; this is a consequence of the existence of curves C_f with $C_f(\mathbb{F}_p) = \emptyset$ for small primes p, something which does not occur for cubic hypersurfaces!

4.2. Fields generated by points. Suppose C is a curve defined over $\mathbb{Q}$. We say a number field $K/\mathbb{Q}$ is generated by a point of C if it is the minimal field of definition for a K-point of C. We can count these number fields of degree n by their discriminant,

$$N_{n,C}(X) = \#\left\{K/\mathbb{Q} : K = \mathbb{Q}(P),\ [K : \mathbb{Q}] = n,\ |\mathrm{Disc}(K)| \leq X\right\}.$$

We can also impose conditions on the Galois group, with $N_{n,C}(X, G)$ denoting the number of those extensions also satisfying $\mathrm{Gal}(\widetilde{K}/\mathbb{Q}) \simeq G$, with $\widetilde{K}$ denoting a Galois closure of K.

In their paper on *Diophantine stability*, Mazur and Rubin [MR18] ask to what extent the set of fields generated by algebraic points of C determines the curve C. When C is an elliptic curve, studying how the rank changes upon field extension has recently led to an answer to *Hilbert's tenth problem* over rings of integers of number fields: there does not exist a general algorithm to decide whether a Diophantine equation has a solution in $\mathcal{O}_K$ [KP25]. Motivated by this, we ask how this set of fields grows, i.e. how does $N_{n,C}(X)$ grow as $X \to \infty$? This can be viewed as a modification of our guiding Question 1.

In [Key22], I proved an asymptotic lower bound for $N_{n,C}(X, S_n)$ when C is a hyperelliptic curve. Joint with Beneish in [BK26], we consider the case of $C = C_f$ a superelliptic curve and give asymptotic lower bonds for $N_{n,C}(X)$ in this larger family. The main results of both papers are summarized in the following theorem.

Theorem 13 (K., Beneish–K.). *Let C be a superelliptic curve and n sufficiently large. Then we have*

$$N_{n,C}(X) \gg X^{\delta_n}, \tag{4}$$

where δ_n is an explicit constant depending on m, d, and n, with $\delta_n \to \frac{1}{m^2}$ as $n \to \infty$.

In particular, when n is a multiple of $\gcd(m,d)$ and sufficiently large, the constant δ_n is positive. Thus, Theorem 13 quantifies that there are *many* degree n fields $K/\mathbb{Q}$ arising from points on superelliptic curves.

To prove Theorem 13, the approach is to produce a family of polynomials of degree n whose roots give rise to algebraic points on C. The major challenge is to prove that this family is irreducible, hence it consists almost entirely of irreducible polynomials. These polynomials can then be counted, adjusting for the multiplicity of the fields generated, producing the lower bound (4).

Included in [BK26, §7] is a discussion of whether and how often C_f can have points of degree n which do not arise as the pullback of a degree n/m point on $\mathbb{P}^1$. We highlight here a new result in this direction.

Proposition 14 (Beneish–K., [BK26, Proposition 7.2]). *Suppose k is an odd prime and m, d satisfy $4 \mid m$, $m \mid d$, $m \le k$, and $n = 2k < \frac{d}{2} - 1$. Then for a positive proportion of squarefree degree d polynomials $f(x)$ ordered by height, the superelliptic curve given by $C\colon y^m = f(x)$ has at most finitely points of degree n.*

4.3. Future directions. Theorems 11 and 12 suggest a number of follow up questions. Among them is Question 2 for superelliptic curves with $(m,d) = (3,6)$.

Question 15. *What proportion of superelliptic curves C_f with $(m,d) = (3,6)$ have a $\mathbb{Q}$-point?*

Since we now know how often such curves are everywhere locally soluble, this is equivalent to determining how often they fail the local-to-global principle for rational points. Equally interesting would be to relax this question and study how often C_f has a K-point over a field $K/\mathbb{Q}$ of degree *coprime to* m, generalizing the work of Bhargava, Gross, and Wang in the hyperelliptic case [BGW17].

Question 16. *How often does a superelliptic curve C_f with $(m,d) = (3,6)$ have a K-point for a field $K/\mathbb{Q}$ with degree coprime to 3?*

One approach to Question 16 is to explore explicit descent methods for $\mathrm{Pic}^1(C_f)$ developed by Creutz [Cre13, Cre20]. When $m = 3$, C_f has *no* K-points for $K/\mathbb{Q}$ of degree coprime to 3 if and only if $\mathrm{Pic}^1(C_f)(\mathbb{Q}) = \emptyset$, as is the case for e.g.

$$C_f\colon y^3 = 3(x^6 + x^4 + 4x^3 + 2x^2 + 4x + 3) \qquad \text{(see [Cre13, Example 7.3])}.$$

Performing larger-scale computations in these families could help us to make precise conjectures.

In another direction, we want to understand the Galois groups of fields generated by points.

Question 17. *What can we say about $N_{n,C}(X, G)$ for various subgroups $G \subseteq S_n$?*

In the hyperelliptic case, the lower bound (4) holds for $N_{n,C}(X, S_n)$ [Key22, Theorems 1.1, 1.2]. We expect the same holds for superelliptic curves more generally. It would also be of interest to understand when proper subgroups $G \subsetneq S_n$ occur often as the Galois group of a field K generated by a point on C, and to count $N_{n,C}(X, G)$. A problem of this flavor is well suited to an advanced undergraduate student with some background in Galois theory.

5. Further topics

5.1. Mertens' product theorem for Chebotarev sets. In his classical product theorem, Mertens studied the rate at which the Euler product of the inverse of the Riemann zeta function approaches zero,

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x}, \qquad \text{as } x \to \infty. \tag{5}$$

Here γ is the Euler constant. In some sense, (5) captures the fact that for integers in the interval $(\sqrt{x}, x)$, the probabilities of being divisible by distinct primes *fail to be independent*; if they were independent, then we would expect this to agree with $\frac{1}{\log x}$ the density of primes given by the prime number theorem!

Mertens' theorem has been generalized appropriately to number fields, varieties over finite fields, and primes in congruence classes [Ros99, Leb07, Wil74]. In a joint publication with Santiago Arango-Piñeros and Daniel Keliher [APKK22], we extend it further to *Chebotarev sets* of primes in a number field and give a power saving error term.

More precisely, fix a Galois extension of number fields E/F with group G. If $C \subset G$ is a conjugacy class, let $\mathcal{C}(x)$ denote the set of unramified primes P in $\mathcal{O}_F$ with Frobenius $\mathrm{Frob}_P = \left(\frac{E/F}{P}\right) = C$ and bounded norm $NP \leq x$.

Theorem 18 (Arango-Piñeros–Keliher–K., [APKK22, Theorem A]). *As $x \to \infty$, we have*

$$\prod_{P \in \mathcal{C}(x)} \left(1 - \frac{1}{NP}\right) = \left(\frac{e^{-\gamma(E/F,C)}}{\log x}\right)^{|C|/|G|} + O\left(\frac{1}{(\log x)^{|C|/|G|+1}}\right).$$

The implied constant depends on the extension E/F and C. Furthermore, the constant $e^{-\gamma(E/F,C)}$ is given by

$$e^{-\gamma(E/F,C)} = e^{-\gamma_F} \prod_{P \in \Sigma_F} \left(1 - \frac{1}{NP}\right)^{\alpha(E/F,C;P)}$$

where $\gamma_F = \gamma + \log \varkappa_F$, with $\varkappa_F$ denoting the residue of the Dedekind zeta function $\zeta_F(s)$ at $s = 1$, and

$$\alpha(E/F, C; P) = \begin{cases} -1, & P \mid \Delta, \\ \frac{|G|}{|C|} - 1, & \mathrm{Frob}_P = C, \\ -1, & \mathrm{Frob}_P \neq C. \end{cases}$$

The proof of Theorem 18 involves studying several Euler products and using the orthogonality of characters. Extra care must be taken when the group G has representations of dimension greater than one. Theorem 18 may be applied to produce a version of Mertens' product theorem over primes represented by quadratic forms; see [APKK22, Corollary 4.2].

5.2. Arithmetical structures on graphs. Given a graph G, an *arithmetical structure* on G is a solution to a system of linear equations with integer coefficients related to the adjacency matrix of G. A well known special case is the *graph Laplacian*, which is related to the classical *chip-firing game*; for more, see e.g. [GK20].

While interesting as purely combinatorial objects, arithmetic structures were originally introduced in the context of arithmetic geometry, specifically, to study special fibers of models of curves [Lor89]. Lorenzini showed for a graph with finite vertex and edge sets, the set of arithmetical structures, $A(G)$, is finite [Lor89]. Beyond this, little is known outside a few special cases:

- if G is a path or cycle $\#A(G)$ may be computed exactly [BCC+18],
- if G is a bident graph, there are known bounds for $\#A(G)$ [ABDL+20], and
- if G is a path with one doubled edge, there are conjectured asymptotics for $\#A(G)$ [GW19].

In joint work with Tomer Reiter [KR21], we give the first known general upper bound for $\#A(G)$ when G is a graph on n vertices with edge set $E(G)$.

Theorem 19 (K.–Reiter, [KR21]). *Let G be a connected, undirected graph on n vertices, with no loops but possible multiedges. Then the following is an upper bound for the number of arithmetical structures on G.*

$$\#A(G) \leq \frac{n!}{2} \cdot \#E\left(G\right)^{2^{n-2}-1} \cdot \#E\left(G\right)^{2^{n-1} \cdot \frac{1.538 \log(2)}{(n-1)\log(2) + \log(\log(\#E(G)))}}.$$

The proof of Theorem 19 relies on inductively applying a *smoothing* process to reduce the number of vertices, reminiscent of a strategy used in [BCC+18, ABDL+20]. In special cases, it is inverse to a *blowup* construction [Lor89] and extends observations about how the *clique-star transformation* interacts with arithmetical structures [CV18].

Questions related to arithmetical structures on graphs are readily accessible to undergraduates. One potential avenue for undergraduate involvement is to consider them in families, as proposed below.

Question 20. *Fix a family of graphs G_n with n vertices. Determine (or bound) the asymptotic growth rate of $\#A(G_n)$. If a graph G is chosen at random in some appropriate sense, how is $\#A(G)$ distributed?*

References

[ABDL+20] Kassie Archer, Abigail C. Bishop, Alexander Diaz-Lopez, Luis D. García Puente, Darren Glass, and Joel Louwsma. Arithmetical structures on bidents. *Discrete Math.*, 343(7):111850, 23, 2020.

[AK65] James Ax and Simon Kochen. Diophantine problems over local fields. I. *Amer. J. Math.*, 87:605–630, 1965.

[APKK22] Santiago Arango Piñeros, Daniel Keliher, and Christopher Keyes. Mertens' theorem for Chebotarev sets. *Int. J. Number Theory*, 18(8):1823–1842, 2022. Preprint available at https://arxiv.org/pdf/2103.14747.

[BBL16] M. J. Bright, T. D. Browning, and D. Loughran. Failures of weak approximation in families. *Compos. Math.*, 152(7):1435–1475, 2016.

[BCC+18] Benjamin Braun, Hugo Corrales, Scott Corry, Luis David García Puente, Darren Glass, Nathan Kaplan, Jeremy L. Martin, Gregg Musiker, and Carlos E. Valencia. Counting arithmetical structures on paths and cycles. *Discrete Math.*, 341(10):2949–2963, 2018.

[BCF16] Manjul Bhargava, John Cremona, and Tom Fisher. The proportion of plane cubic curves over $\mathbb{Q}$ that everywhere locally have a point. *Int. J. Number Theory*, 12(4):1077–1092, 2016.

[Beu98] Frits Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Mathematical Journal*, 91:61–88, 1998.

[BGW17] Manjul Bhargava, Benedict H. Gross, and Xiaoheng Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *J. Amer. Math. Soc.*, 30(2):451–493, 2017. With an appendix by Tim Dokchitser and Vladimir Dokchitser.

[BK23] Lea Beneish and Christopher Keyes. On the proportion of locally soluble superelliptic curves. *Finite Fields and Their Applications*, 85:102128, 2023. Available at https://doi.org/10.1016/j.ffa.2022.102128.

[BK25a] Lea Beneish and Christopher Keyes. An effective Bertini theorem and an application to p-adic fields. Submitted, 2025. Available at https://arxiv.org/pdf/2508.20192.

[BK25b] Lea Beneish and Christopher Keyes. How often does a cubic hypersurface have a rational point? *Selecta Mathematica*, 31(92), 2025. Available at https://doi.org/10.1007/s00029-025-01079-w.

[BK26] Lea Beneish and Christopher Keyes. Fields generated by points on superelliptic curves. *Journal of Number Theory*, 278:380–421, 2026. Available at https://doi.org/10.1016/j.jnt.2025.04.011.

[BL59] B. J. Birch and D. J. Lewis. $\mathfrak{p}$-adic forms. *J. Indian Math. Soc. (N.S.)*, 23:11–32, 1959.

[BLBS23] Tim Browning, Pierre Le Boudec, and Will Sawin. The Hasse principle for random Fano hypersurfaces. *Ann. of Math. (2)*, 197(3):1115–1203, 2023.

[BP22] Manjul Bhargava and Bjorn Poonen. The local-global principle for integral points on stacky curves. *Journal of Algebraic Geometry*, 31(4):773–782, 2022.

[Cre13] Brendan Creutz. Explicit descent in the Picard group of a cyclic cover of the projective line. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 295–315. Math. Sci. Publ., Berkeley, CA, 2013.

[Cre20] Brendan Creutz. Generalized Jacobians and explicit descents. *Math. Comp.*, 89(323):1365–1394, 2020.

[CV18] Hugo Corrales and Carlos E. Valencia. Arithmetical structures on graphs. *Linear Algebra Appl.*, 536:120–151, 2018.

[DG95] Henri Darmon and Andrew Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[DRKK$^+$] Juanita Duque-Rosero, Christopher Keyes, Andrew Kobin, Manami Roy, Soumya Sankar, and Yidi Wang. The integral Hasse principle for stacky curves associated to a family of generalized Fermat equations. Submitted. Available at https://arxiv.org/pdf/2509.13248.

[Dum17] Jan H. Dumke. p-adic zeros of quintic forms. *Math. Comp.*, 86(307):2469–2478, 2017.

[GK20] Darren Glass and Nathan Kaplan. *Chip-Firing Games and Critical Groups*, pages 107–152. Springer International Publishing, Cham, 2020.

[GW19] Darren Glass and Joshua Wagner. Arithmetical Structures on Paths With a Doubled Edge. *arXiv e-prints*, page arXiv:1903.01398, Mar 2019.

[HB83] D. R. Heath-Brown. Cubic forms in ten variables. *Proc. London Math. Soc. (3)*, 47(2):225–257, 1983.

[HB10] D. R. Heath-Brown. Zeros of p-adic forms. *Proc. Lond. Math. Soc. (3)*, 100(2):560–584, 2010.

[Key22] Christopher Keyes. Growth of points on hyperelliptic curves over number fields. *J. Théor. Nombres Bordeaux*, 34(1):271–294, 2022. Available at https://doi.org/10.5802/jtnb.1201.

[KP25] Peter Koymans and Carlo Pagano. Hilbert's tenth problem via additive combinatorics, 2025.

[KR21] Christopher Keyes and Tomer Reiter. Bounding the number of arithmetical structures on graphs. *Discrete Mathematics*, 344(9):112494, 2021. Available at https://doi.org/10.1016/j.disc.2021.112494.

[Leb07] Philippe Lebacque. Generalised Mertens and Brauer-Siegel theorems. *Acta Arithmetica*, 130(4):333–350, 2007.

[Lew52] D. J. Lewis. Cubic homogeneous polynomials over p-adic number fields. *Ann. of Math. (2)*, 56:473–478, 1952.

[LL65] R. R. Laxton and D. J. Lewis. Forms of degrees 7 and 11 over $\mathfrak{p}$-adic fields. In *Proc. Sympos. Pure Math., Vol. VIII*, pages 16–21. Amer. Math. Soc., Providence, RI, 1965.

[Lor89] Dino J. Lorenzini. Arithmetical graphs. *Math. Ann.*, 285(3):481–501, 1989.

[LS16] D. Loughran and A. Smeets. Fibrations with few rational points. *Geom. Funct. Anal.*, 26(5):1449–1482, 2016.

[LY96] David B. Leep and Charles C. Yeomans. Quintic forms over p-adic fields. *J. Number Theory*, 57(2):231–241, 1996.

[MR18] Barry Mazur and Karl Rubin. Diophantine stability. *Amer. J. Math.*, 140(3):571–616, 2018. With an appendix by Michael Larsen.

[PV04] Bjorn Poonen and José Felipe Voloch. Random Diophantine equations. In *Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002)*, volume 226 of *Progr. Math.*, pages 175–184. Birkhäuser Boston, Boston, MA, 2004. With appendices by Jean-Louis Colliot-Thélène and Nicholas M. Katz.

[Ros99] Michael Rosen. A generalization of Mertens' theorem. *Journal of the Ramanujan Mathematical Society*, 14:1–20, 1999.

[San23] Tim Santens. The Brauer-Manin obstruction for stacky curves, 2023. Preprint, arXiv:2210.17184.

[Ter66] Guy Terjanian. Un contre-exemple à une conjecture d'Artin. *C. R. Acad. Sci. Paris Sér. A-B*, 262:A612, 1966.

[Wil74] Kenneth S. Williams. Mertens' theorem for arithmetic progressions. *J. Number Theory*, 6:353–359, 1974.

[Woo08] Trevor D. Wooley. Artin's conjecture for septic and unidecic forms. *Acta Arith.*, 133(1):25–35, 2008.

[Zah11] Jahan Zahid. Simultaneous zeros of a cubic and quadratic form. *Journal of the London Mathematical Society*, 84(3):612–630, 2011.