Counting Points on Varieties and Applications to Ranks of Elliptic Curves over Function Fields

Ben Church and Spencer Dembner

May 5, 2023

1 Introduction

1.1 Supersingularity

Suppose we have a polynomial, $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with coefficients in the finite field $\mathbb{F}_q$. Let X be the *variety* defined by f. An interesting sequence of numbers associated to X are the counts of the number of solutions to f in each of the larger fields $\mathbb{F}_q$,

$$\#X(\mathbb{F}_{q^n}) = \#\{(x_1, \ldots, x_n) \in \mathbb{F}_{q^n} \mid f(x_1, \ldots, x_n) = 0\}$$

To analyze the behavior of this sequence, we put it into an exponential generating function called the *zeta function* of X,

$$\zeta_X(t) = \exp\left(\sum_{n \geq 1} \frac{\#X(\mathbb{F}_{q^n})}{n} t^n\right)$$

One of the crowning achievements of modern algebraic geometry is understanding the properties of this generating function in terms of the geometry of X. What I mean by the geometry of X is considering a lift the defining polynomial $f \in \mathbb{Z}[x_0, \ldots, x_n]$ to one with integer coefficients and considering the complex vanishing locus,

$$Z(f) = \{(x_1, \ldots, x_n) \in \mathbb{C}^n \mid f(x_0, \ldots, x_n) = 0 \subset \mathbb{C}^n$$

This is an actual geometric space. One result says that,

$$\zeta_X(t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_p(t) \cdots P_{2n}(t)}$$

where $P_i(t)$ is a polynomial of degree b_i where,

$$b_i = \dim_{\mathbb{Q}} H^i(Z(f), \mathbb{Q})$$

is the dimension of the i^{th}-homology group of the complex variety $Z(f)$.

We say that X is *supersingular* if each of the polynomials $P_i(t)$ has roots of the form $\zeta q^{\frac{i}{2}}$ where ζ is a root of unity. Part of the point of the project will be to find new examples of supersingular varieties.

One reason to care about supersingular varieties is the following conjecture. We say that X is *rational* if f can be "solved by rational functions". Explicitly this means there exist rational functions $r_1, \dots, r_n \in \overline{\mathbb{F}}_q(t_1, \dots, t_n)$ in n indeterminants such that,

$$f(r_1(t_1, \dots, t_n), \dots, r_n(t_1, \dots, t_n)) = 0$$

such that every indeterminants t_i appears in some r_j. Shioda [Shi77] conjectured that if $n = 2$ then X is rational if and only if X is supersingular. An overarching goal of this project is to test this conjecture.

1.2 Ranks of Elliptic Curves

An *elliptic curve* is an algebraic curve E defined by a polynomial of the form,

$$y^2 = x^3 + ax + b$$

A fundamental property of E is that its points form an abelian group with a group composition defined by some polynomial functions. A foundational theorem due to Mordell shows that the rational solutions of this equation $E(\mathbb{Q})$ forms a finitely generated abelian group. Therefore, abstractly,

$$E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$$

where $r \in \mathbb{N}$ is an integer called the *rank* of E and $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group.

A major area of research in contemporary number theory concerns the distribution of ranks of these elliptic curves. It is not even know whether there is an upper bound on the ranks of elliptic curves over $\mathbb{Q}$. Currently, the largest known rank is 28 [KSW16]. Some conjecture that the ranks of elliptic curves are indeed bounded (and even that we may have found close to the largest ranks over $\mathbb{Q}$) based on heuristics coming from random matrix models [Par+18]. However, over $\mathbb{Q}$ this problem remains extremely difficult, the boundedness question is wide open with weak evidence for unboundedness coming from the work of Elkies [EK20]. There is a fruitful analogy between number fields, such as $\mathbb{Q}$, and "function fields" such as $\mathbb{F}_q(t)$. The later is often more accessible using the tools of algebraic geometry. With this in mind, it is natural to study the ranks of elliptic curves with equations defined over the function field $\mathbb{F}_q(t)$. However, in this case, Ulmer demonstrated the existence of elliptic curves over $\mathbb{F}_q(t)$ with arbitrary large ranks [Ulm04]. These constructions rely heavily on our knowledge of supersingular surfaces to get around a particular stumbling block in our knowledge: that the rank can only conjecturally be computed in terms of a more accessible quantity called the analytic rank. In general, this equality is known as Birch and Swinnerton-Dyer conjecture, one of the famed Millennium problems. However, for elliptic curves constructed in terms of supersingular surfaces, this equality can be proven.

Although Ulmer's construction shows that ranks over $\mathbb{F}_q(t)$ are unbounded, there remains a conjecture that those elliptic curves having a particular numerical property – that their j-invariant satisfies a bound on its degree (in $\mathbb{F}_q(t)$) – should have bounded ranks.

2 Project Outline

This project aims to find new examples of supersingular varieties and use them to find new examples of elliptic curves over $\mathbb{F}_q(t)$ with large ranks. We will search for these examples with a view towards testing both the Shioda conjecture and the boundedness of ranks of special elliptic curves over $\mathbb{F}_q(t)$.

Participants will study the requisite background material and then write or adapt a code-base to search for numerical examples with the desired properties. We will then aim to make conjectures about the structure of the examples discovered and attempt to prove these conjectures. A major technical tool will be the algorithm for point counting on diagonal hypersurfaces developed by Weil in [Wei49]. Analysis of this method will make heavy use of Gaussian sums which participants will work with to improve the efficiency of computer searches.

Approximate timeline of the project:

Weeks:

1 Background reading and exercises.

2-3 Understand and improve existing code-base in SAGE to search for supersingular varieties.

4-5 Analyze data to determine numerical conditions for a variety to be supersingular.

6-7 Try to use new examples to create elliptic curves of large ranks.

8-10 Attempt to test the Shioda and boundedness conjectures with our new examples.

3 Project Requirements

It it required that participants have a solid foundation in algebra at the level of Dummit and Foote. Furthermore, it is expected that participants have basic familiarity with Python or at least some programming experience. Prior experience with SAGE is not expected. While it is not required, students with some exposure to algebraic geometry – for example Fulton's *Algebraic Curves* – will be in the best position to make progress on the theoretical aspects of this project. That said, there is significant technical work in optimization and data analysis involved in the project which will not involve background knowledge of algebraic geometry. The majority of problems encountered will be reducible to statements about the direct analysis of polynomial equations and Galois theory. Therefore, it is most important that the participants foster teamwork and communication between more and less experienced participants to make sure that problems are reduced to, or stated in, the shared tongue of algebra.

Our intention is that this project combines concrete computational goals with ambitious open-ended research aims. Participants will be given concrete programming tasks and exercises at the advanced undergraduate level to build familiarity with concrete examples. However, as the program continues, participants will be encouraged to pursue ambitious mathematical aims such as proving any conjectures they develop over the course of the program.

References

[EK20] Noam D Elkies and Zev Klagsbrun. "New rank records for elliptic curves having rational torsion". In: *Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley.* 2020, pp. 233–250.

[KSW16] Zev Klagsbrun, Travis Sherman, and James Weigandt. *The Elkies Curve has Rank 28 Subject only to GRH*. 2016. arXiv: `1606.07178 [math.NT]`.

[Par+18] Jennifer Park et al. *A heuristic for boundedness of ranks of elliptic curves*. 2018. arXiv: `1602.01431 [math.NT]`.

[Shi77] Tetsuji Shioda. "Some Results on Unirationality of Algebraic Surfaces." In: *Mathematische Annalen* 230 (1977), pp. 153–168. URL: `http://eudml.org/doc/163036`.

[Ulm04] Douglas Ulmer. *Elliptic curves with large rank over function fields*. 2004. arXiv: `math/0109163 [math.NT]`.

[Wei49] André Weil. "Numbers of solutions of equations in finite fields". In: *Bulletin of the American Mathematical Society* 55.5 (1949), pp. 497 –508.