Abelian Varieties with Few Isogenies and Cryptography

Travis Scholl
University of Washington

Abstract

We call an elliptic curve $E/\mathbb{F}_q$ *super-isolated* if it is not $\mathbb{F}_q$-isogeneous to another curve. The motivation for super-isolated curves comes from cryptography. If E is isogeneous to E', then the discrete log problem on E can be moved to E', where more attacks may be available. In this work, we generalize the definition of *super-isolated* to arbitrary dimension and estimate the number of such varieties.

Definition of Super-Isolated Abelian Varieties

Definition. An abelian variety A over a finite field $\mathbb{F}_q$ is *super-isolated* if there are no $\mathbb{F}_q$-isogenies to other varieties.

Example. The elliptic curve $E/\mathbb{F}_5$ given by $y^2 = x^2+2x$ is super-isolated. We found E by enumerating all elliptic curves over $\mathbb{F}_5$.

Application to Cryptography

The security of elliptic curve cryptography relies on the difficulty of the elliptic curve discrete log problem (ECDLP). The ECDLP can be transfered between curves via isogenies. If some curves are "weak" in the sense that the ECDLP can be solved quickly on them, then an attack could attempt to transfer the ECDLP from a given curve E to one of these weak curves by computing a chain of isogenies. A more detailed discussion of this scenario is given in [KKM11].

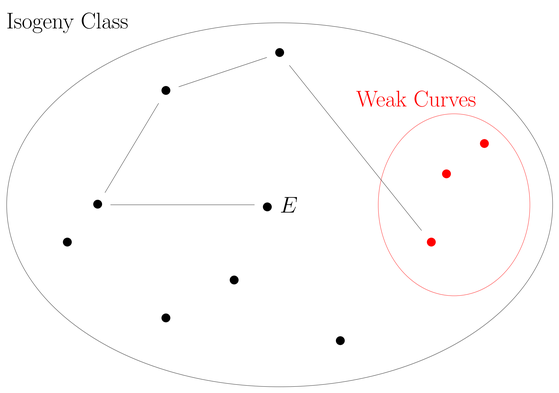

Fig. 1: Visualization of transfering the ECDLP inside of an isogeny class.

Identifying Super-Isolated Varieties

The isogeny class of an abelian variety can be split into *endomorphism classes*, which are subsets of varieties that share the same endomorphism ring. For simple ordinary abelian varieties A, the endomorphism ring $\operatorname{End} A$ is an order $\mathcal{O}$ in a number field. Moreover, $\mathcal{O} \supseteq \mathbb{Z}[\pi, \overline{\pi}]$, where π denotes the Frobenius endomorphism, and the size of the endomorphism class is the class number of $\mathcal{O}$ [Wat69].

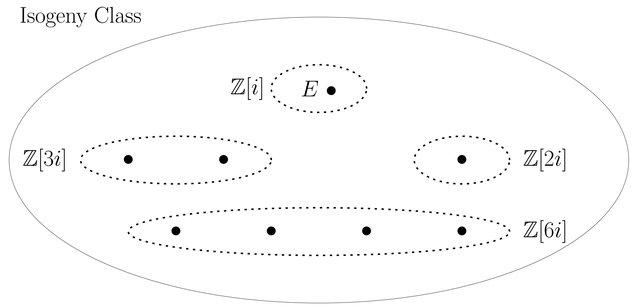

Fig. 2: The isogeny class of $E/\mathbb{F}_{37} : y^2 = x^3 + x$ partitioned into endomorphism classes.

Theorem. Let $A/\mathbb{F}_q$ be a simple ordinary abelian variety, π a root of the characteristic polynomial of the Frobenius endomorphism, and $K = \mathbb{Q}(\pi)$. Then A is super-isolated if and only if $\mathcal{O}_K = \mathbb{Z}[\pi, \overline{\pi}]$ and K has class number 1.

Constructing Super-Isolated Curves

Algorithm.

1. Find $A \in \mathbb{Z}$ such that $p = A^2 + 1$ is prime.
2. Find $\lambda \in \mathbb{F}_p$ such that $y^2 = x^3 + \lambda x$ has $A^2 - 2A + 2$ points.

Remark. The resulting curve has endomorphism ring $\mathbb{Z}[i]$. The Frobenius endomorphism corresponds to $A + i$. This method can be generalized to any quadratic imaginary field with class number 1.

Main Results on Counting Weil Numbers

Our main result is a formula for the number of Weil numbers that look like the Frobenius endomorphism of a super-isolated variety.

Definition. An algebraic integer π is a *Weil generator* for a complex multiplication (CM) field K if $\pi\overline{\pi} \in \mathbb{Z}$ and $\mathcal{O}_K = \mathbb{Z}[\pi, \overline{\pi}]$.

Theorem. Let W be the set of Weil generators in a CM field K of degree $2g$, and for $\beta \in K$, let $h(\beta)$ denote the height of β. Then

$$\#\{\alpha \in W : h(\alpha) \leq N\} = \begin{cases} 4N + O(1) & g = 1 \\ \rho \log N + O(1) & g = 2 \text{ and } W \neq \emptyset \\ O(1) & g \geq 3, \end{cases}$$

where ρ is a constant depending on K. Moreover, for $g \leq 3$, the constants can be made effective.

Estimating the Number of Super-Isolated Varieties

Conjecture. The number of super-isolated ordinary elliptic curves over $\mathbb{F}_p$ with $p \leq M$ is $\Theta(\sqrt{M}/\log M)$.

Heuristic. The number of super-isolated simple ordinary abelian surfaces over $\mathbb{F}_p$ with $p \leq M$ is $\Theta(\log \log M)$.

Theorem. Let $g \geq 3$. The number of super-isolated simple ordinary abelian varieties of dimension g over $\mathbb{F}_p$ with $p \leq M$ is $\Theta(1)$.

References

[KKM11] Ann Hibner Koblitz, Neal Koblitz, and Alfred Menezes. "Elliptic curve cryptography: the serpentine course of a paradigm shift". In: *J. Number Theory* 131.5 (2011), pp. 781–814. ISSN: 0022-314X.

[Sch18] Travis Scholl. "Abelian Varieties with Small Isogeny Class and Applications to Cryptography". PhD thesis. University of Washington, June 2018.

[Wat69] William C. Waterhouse. "Abelian varieties over finite fields". In: *Ann. Sci. École Norm. Sup. (4)* 2 (1969), pp. 521–560. ISSN: 0012-9593.