Abelian Varieties with Few Isogenies and Cryptography

Travis Scholl
University of Washington

Abstract

We call an elliptic curve $E/F_p$ super-isolated if it is not $F_p$-isogenous to another curve. The motivation for super-isolated curves comes from cryptography. If $E$ is isogenous 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 $F_p$ is super-isolated if there are no $F_p$-isogenies to other varieties.

Example. The elliptic curve $E/F_p$ given by $y^2 = x^3 + 2x$ is super-isolated. We found $E$ by enumerating all elliptic curves over $F_p$.

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 transferred between curves via isogenies. If some curves are elliptic curve discrete log problem (ECDLP). The ECDLP can be transferred between curves via isogenies. If some curves are weak, their ECDLP can be easily solved. This is a weakness in the security of elliptic curve cryptography.

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 $End A$ is an order $O$ in a number field. Moreover, $O \subseteq \mathbb{Z}[\pi, \overline{\pi}]$, where $\pi$ denotes the Frobenius endomorphism, and the size of the endomorphism class is the class number of $O$ [Wat60].

Construction of Super-Isolated Curves

Algorithm.
1. Find $A \in Z$ such that $p = A^2 + 1$ is prime.
2. Find $\lambda \in F_p$ such that $\lambda y = x^3 + \lambda x$ has $A^2 - 2A + 2$ points.

Remark. The resulting curve has endomorphism ring $\mathbb{Z}[\overline{\pi}]$. The Frobenius endomorphism corresponds to $A + 1$. 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 $\pi$ is a Weil generator for a complex multiplication (CM) field $K$ if $\pi \in Z$ and $O_K = Z[\pi, \overline{\pi}]$.

Theorem. Let $W$ be the set of Weil generators in a CM field $K$ of degree $2g$ and let $h(\beta)$ denote the height of $\beta$. Then
$$\# \{\alpha \in W : h(\alpha) \leq N\} = \begin{cases} 4N + O(1) & g = 1 \\ \rho \log N + O(1) & g = 2 \\ O(1) & g \geq 3 \end{cases}$$
where $\rho$ 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 $F_p$ with $p \leq M$ is $\Theta(\sqrt{M}/\log M)$.

Heuristic. The number of super-isolated simple ordinary abelian surfaces over $F_p$ 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 $F_p$ with $p \leq M$ is $\Theta(1)$.

References

