# Supersingular Diagonal Curves and their Genera

Ryan Catullo Miguel Machado Aaryan Sukhadia
Mentors: Benjamin Church and Spencer Dembner
Stanford University Department of Mathematics

## Introduction

Consider a diagonal variety in weighted projective space of the form:

$$X : x_0^{n_0} + \cdots + x_0^{n_r} = 0$$

Our main result is as follows:

### Theorem

*Every supersingular diagonal curve of positive genus is covered by a supersingular Fermat curve.*

We also give a formula for the genera of these curves and use the above to deduce results on distributions of these genera.

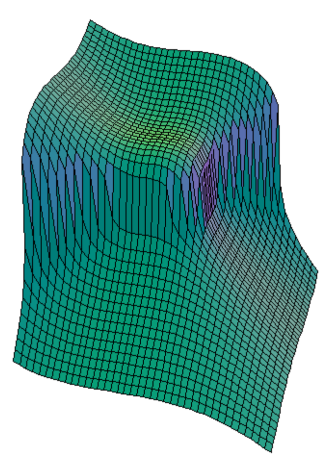

Figure 1. The Fermat Surface $x^3 + y^3 - z^3 = 0$ over $\mathbb{C}$ [Ano]

## Background: Zeta Functions and Supersingularity

### Hasse-Weil Zeta Function

The local zeta function of a variety $X$ over a field $\mathbb{F}_q$ is defined as

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

where $\#X(\mathbb{F}_{q^k})$ denotes the rational point-count of $X$ over $\mathbb{F}_{q^k}$. By the Weil conjectures this function is rational for smooth projective curves, with polynomial factors in the numerator and denominator all having the form

$$P_i(t) = \prod_j (1 - \alpha_{i,j} t)$$

### Supersingularity

If every reciprocal root $\alpha_{i,j}$ of $\zeta_X(t)$ is $q^{i/2}\zeta$ for a root of unity $\zeta$ then $X$ is called **supersingular**.
Motivation for deducing supersingularity include:

- A supersingular abelian variety is isogenous to product of supersingular elliptic curve, by Honda-Tate Theory.
- Assuming the Tate conjecture, supersingularity implies the cycle class map is surjective.
- If $q$ is a square, then supersingular curves of genus $g$ are exactly the maximizers/minimizers of $\#X(\mathbb{F}_q)$ over all genus-$g$ curves.

## Background: Stickelberger's Theorem and Fermat Varieties

We work with diagonal varieties because they have "nice" zeta functions for which supersingularity is easily computable.

### Stickelberger Criterion for Diagonal Varieties

It was shown in [Chu+] using Stickelberger's theorem that for a diagonal variety $X : x_0^{n_0} + \ldots + x_r^{n_r} = 0$ with $n = \text{lcm}(n_i)$, $f = ord_n(p)$, then $X$ is supersingular over $\mathbb{F}_p$ if and only if, for each $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$ and for each

$$l \in \left\{ (l_0, \ldots, l_r) : l_i \in (0, n) \cap \mathbb{Z} \text{ and } n \mid \sum_{i=0}^{r} l_i \text{ and } n \mid l_i n_i \right\}$$

the following equality holds:

$$\sum_{i=0}^{r} \sum_{j=0}^{f-1} \left\{ \frac{\mu p^j l_i}{n} \right\} = \frac{(r+1)f}{2}$$

This allowed us to write code to verify supersingularity.

### Fermat Varieties

The Fermat variety $F_r^n : x_0^n + \ldots + x_r^n = 0$ is supersingular if and only if there exists $v$ such that $p^v \equiv -1 \mod n$ by [SK79].
For any diagonal variety $X$ there exists a surjective morphism $F_r^n \twoheadrightarrow X$ where $n = \text{lcm}(n_i)$. Since dominant rational maps preserve supersingularity, this gives us a sufficient condition for the supersingularity of diagonal varieties.
Extensive computation suggested that for diagonal curves this was also a necessary condition. Our classification showed this is indeed the case.

## Classification of Supersingular Diagonal Curves

A **primitive exponent set** $(n_0, \ldots, n_r)$ is such that $n_i \mid \text{lcm}_{j\neq i}(n_j)$ for each $n_i$. Since every diagonal variety is birational to a variety with primitive exponents [Chu+], it is sufficient to deal with only primitive exponent sets.

### Theorem

*A primitive curve $C : x_0^{n_0} + x_1^{n_1} + x_2^{n_2} = 0$ is supersingular over $\mathbb{F}_p$ if and only if either of the following hold:*

*(1) one of the $n_i$ is 1*

*(2) $F_2^n$ is supersingular for $n = lcm(n_0, n_1, n_2)$*

Using our genus formula, we showed every positive genus curve lands in case (2), implying every such curve is covered by a supersingular Fermat.
The proof relied on deducing functional equations from the Stickelberger criterion and using them along the supersingularity of "simple" curves $C$ to deduce conditions for the supersingularity of other curves. This allowed us to create an inductive pattern with the prime factorization of the exponents, leading to the proof for all curves.

## Calculating the Genus

A direct application of [Hos20] shows that the diagonal curve $C : x_0^{n_0} + x_1^{n_1} + x_2^{n_2} = 0$ with primitive exponents has genus

$$g_C = 1 + \frac{(n_0-1)(n_1-1)(n_2-1) - (n_0+n_1+n_2) + 1}{2N}$$

where $N = \text{lcm}(n_0, n_1, n_2)$. We then showed that if $n_0 \leq n_1 \leq n_2$ then if $g_C > 0$ we have that

$$g_C \geq \frac{(n_0-1)}{2n_0} n_1$$

This reduces enumerating all possible diagonal curves of a given genus to a finite computational check.

## The Prime-Genus Question

**Question:** Does there exist a supersingular curve of every genus in every positive characteristic?

This question is answered positively for $g \leq 4$, but it is generally unknown otherwise. By our exponent bounds on a given genus, we can calculate $\delta_g$, the density of primes with a supersingular diagonal curve of a genus $g$. We showed that:

### Theorem

*$\delta_g$ always has denominator a power of 2 and $\limsup_{g\to\infty} \delta_g = 1$*

## Future Work

**Conjecture**: Our data strongly suggests that

$$\liminf_{g\to\infty} \delta_g \geq 1/2$$

We could also ask the reverse question fixing a prime $p$, can we compute bounds on the density of genera that arise as a diagonal supersingular curve over characteristic $p$?

## Acknowledgements

We want to thank our mentors Ben Church and Spencer Dembner for their guidance, help, and insights. We also thank Dr. Lernik Asserian and the SURIM program for their support of our research.

## References

[Ano] Anonymous. Wikimedia Commons.
[Chu+] Benjamin Church et al. Private communications.
[Hos20] Timothy Hosgood. *An introduction to varieties in weighted projective space*. 2020. arXiv: `1604.02441 [math.AG]`.
[SK79] Tetsuji Shioda and Toshiyuki Katsura. "On Fermat varieties". In: *Tohoku Mathematical Journal* 31 (Jan. 1979). DOI: `10.2748/tmj/1178229881`.