Supersingular Diagonal Curves and their Genera

Ryan Catullo, Miguel Machado, Aaryan Sukhadia

SURIM 2023

Abstract. In this paper we study the supersingularity of a class of varieties called diagonal hypersurfaces using Stickleberger's Criterion. We show that a curve is supersingular over $\mathbb{F}_p$ if and only if there is a Fermat curve supersingular over the same field and a surjective morphism to the diagonal curve. Since a Fermat variety of degree m is supersingular over $\mathbb{F}_p$ if and only if $p^v \equiv -1 \mod m$ for some v, this classifies supersingular diagonal curves. Lastly, we give a formula for the genus of a primitive diagonal curves and use the classification to give explicit results on the density of supersingular diagonal curves of low genera. This gives bounds on the prime-genus question of supersingular curves.

Contents

0. Introduction

Building on the work of [SK79] and [Chu+], we prove the following:

> THEOREM 0.0.1. Every supersingular diagonal curve of positive genus is covered by a supersingular Fermat curve

Along with this, we also prove some results on the possible genus-prime combinations of supersingular curves.
The title and above description yield a deceptively complicated picture of the underlying math. Essentially most of the work here deals with gcds, lcms and exploiting the structure of $(\mathbb{Z}/n\mathbb{Z})^\times$. Nevertheless, the aggregate results are hopefully valuable to the interested algebraic geometer.

Structure of the Paper: In Section 1, we review some of the background material to remind the reader of the content of our results. In Section 2, we provide several results that build on one another towards a full classification of supersingular diagonal curves, allowing us to prove 0.0.1. In 3, we deduce some interesting results about the genera of supersingular diagonal curves using our classification.

Acknowledgements. We would like to thank Ben Church and Spencer Dembner for setting up this project, and their continued guidance and helpful discussions throughout. We are especially grateful to Ben for providing us results from an unpublished manuscript, which we cite in this paper as "[Chu+]".

1. Preliminary Theory

Notation. Throughout this paper we let p denote a prime and q a prime power.
X denotes a smooth projective variety and C a curve, both over a field of characteristic p.
By a *diagonal* variety we mean one defined by an equation of the form $x_0^{n_0} + \cdots x_r^{n_r}$.
By F_r^n we denote the Fermat variety of degree n in $\mathbb{P}^r$, that is the variety defined by $x_0^n + \cdots x_r^n$.
We use $\{x\}$ to denote the fractional part of a real number x.

1.1 The Weil Conjectures and Supersingularity

In what perhaps led to the birth of modern algebraic geometry as we know it today, Weil set forth conjectures (now theorems) about point-counting zeta functions of smooth projective varieties in his paper [Wei49].

THEOREM 1.1.1 (Weil Conjectures). Let X be n-dimensional, smooth, projective and defined over a finite field $\mathbb{F}_q$. Let $\#X(\mathbb{F}_{q^k})$ denote the number of $\mathbb{F}_{q^k}$-rational points of X. We define:

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

This zeta function then has the following properties:

(a) Rationality:

$$\zeta_X(t) = \frac{P_1(t)P_3(t)\cdots P_{2n-1}(t)}{P_0(t)P_2(t)\cdots P_{2n}(t)}$$

where each $P_i(t) = \prod_j (1 - \alpha_{i,j}t)$ is an integral polynomial.

(b) Functional Equation:

$$\zeta_X(q^{-n}t^{-1}) = \pm q^{ne/2}t^e\zeta_X(t)$$

where e is the Euler Characteristic of X.

(c) Riemann Hypothesis: $|\alpha_{i,j}| = q^{i/2}$ for each $\alpha_{i,j}$ of $P_i(t)$

(d) Betti Numbers: If X arises as a "good reduction mod p" of a complex variety, then $\deg P_i = \dim H_i(X)$.

We are purposefully omitting some details from the full statement of the conjectures for clarity and brevity. What we are focused on are the reciprocal roots $\alpha_{i,j}$, which the proof of the Weil conjectures showed were exactly the eigenvalues of the Frobenius map on the l-adic cohomologies, which can be seen from the Lefschetz trace formula.

DEFINITION 1.1.2. X is **supersingular** if each reciprocal root $\alpha_{i,j}$ of every polynomial $P_i(t)$ in the zeta function is of the form $q^{i/2}\zeta$ for ζ a root of unity.

Remark. Note that, despite what the name may suggest, "supersingular" does not mean the variety is especially singular or not smooth. Rather, the terminology seems to have arisen from the fact that, in antiquity, elliptic curves over $\mathbb{C}$ with rank > 1 were referred to as "singular".

EXAMPLE 1.1.3. Consider the variety $X = \mathbb{P}^n$. We then have $\#X(\mathbb{F}_q) = \frac{q^{n+1}-1}{q-1}$. Calculating the zeta function, we get:

$$\begin{aligned}
\zeta_X(t) &= \exp\left(\sum_{k\geq 1} \frac{\#X(\mathbb{F}_{q^k})}{k} t^k\right) \\
&= \exp\left(\sum_{k\geq 1} \frac{\sum_{i=0}^{n} q^{ki}}{k} t^k\right) \\
&= \exp\left(\sum_{i=0}^{n} \sum_{k\geq 1} \frac{(q^i t)^k}{k}\right) \\
&= \prod_{i=0}^{n} \frac{1}{1-q^i t}
\end{aligned}$$

which shows that X is supersingular.

There are quite a few alternative equivalent definitions, all with their own geometric or algebraic flavor.

PROPOSITION 1.1.4. X being supersingular over $\mathbb{F}_q$ implies any of the following equivalent conditions:

(a) If X is an elliptic curve, then its endomorphism algebra over the algebraic closure has rank 4.

(b) If X is an abelian variety, then it is $\overline{\mathbb{F}_q}$-isogenous to a power of a supersingular elliptic curve.

(c) If q is a square, the supersingular curves of genus g are exactly the maximizers/minimizers of $\#X(\mathbb{F}_q)$ over all genus-g curves. [G22]

(d) Assuming the Tate conjecture, the even dimensional l-adic cohomologies of X are spanned by algebraic cycles. [SK79]

We are using our definition as it allows for an easy verification of supersingularity in the case of diagonal varieties, as we shall see.

We recall some basic properties of supersingularity.

- X is supersingular over $\mathbb{F}_q$ iff it is supersingular over $\mathbb{F}_{q^k}$ for all k, i.e supersingularity is invariant under base change. Specifically, the roots of ζ_{X^k} are exactly the roots of ζ_X raised to the k-th power, and so being a root of unity (or not) is preserved under any base change. We leave it to the reader to verify this computationally.

- If $\phi : Y \to X$ is a dominant rational map of varieties, then Y being supersingular implies X is supersingular. Intuitively, this is because an injection of cohomologies $H^i(X) \hookrightarrow H^i(Y)$ is induced, and the inclusions commute with Frobenius maps. We refer the reader to Theorem 10.2 and 10.3 of [Chu+] for more details.

- Recall that X is called **unirational** if its function field has a separable extension which is purely transcendental. By definition, this means there is a dominant rational map $\phi : \mathbb{P}^n \to X$. Therefore, by what we saw in 1.1.3 X must also be supersingular.

1.2 Zeta Function of a Diagonal Variety

In his original paper motivating the celebrated conjectures, Weil specifically studies the zeta function of diagonal hypersurfaces of the form

$$X : a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0$$

These varieties have the convenient property of having a "nice" zeta function that makes it easy to verify supersingularity.

Observation. The point counts are independent of the coefficients a_i. This follows from the fact that supersingularity is invariant to base change, so (if need be) we can simply take our variety to a larger field where all the a_i have n_i-th roots and perform the linear transformation $x_i \mapsto (a_i^{-1/n_i})x_i$. Given this, we can WLOG make the following assumptions:

(a) All the coefficients a_i are 1

(b) The field X is defined over is $\mathbb{F}_p$ for p a prime.

To preserve the ease of point-counting these diagonal hypersurfaces, we don't want to projectivize them in the standard way. Rather, we want to embed them into weighted projective space (see Subsection 1.4 for more details). What this means from a point counting persepctive is we take the polynomial that defines X and view it as an affine variety $Y \subseteq \mathbb{A}^{n+1}$. Then we have:

$$\#X(\mathbb{F}_{q^k}) = \frac{\#Y(\mathbb{F}_{q^k}) - 1}{q^k - 1} \tag{1}$$

Counting the points and calculate the zeta function for an arbitrary diagonal variety remains non-trivial. To describe it, we introduce a bunch of new notation.

- Since the zeta function diagonal variety is determined entirely by its exponents, we let $\vec{n}$ the exponent tuple $(n_0, ..., n_r)$. We often use this notation to denote a diagonal variety with exponents $\vec{n}$ and coefficients all 1.

- By α_i we denote an element of $[0, 1] \cap \mathbb{Q}$ and by α we denote a tuple $(\alpha_0, ...\alpha_r)$ of such α_i.

- For a given $\vec{n}, q$ let $\mathcal{A}_{\vec{n},q}$ denote the set of all α such that $\sum \alpha_i \in \mathbb{Z}$ and $d_i\alpha_i \in \mathbb{Z}$ for every i, where $d_i := \gcd(n_i, q-1)$.
- Let $\chi_{\alpha_i} : \mathbb{F}_q^\times \to \mathbb{C}^\times$ denote the multiplicative character that sends a primitive root γ to $e^{2\pi i\alpha_i}$. To make eventual calculations work we extend all such characters to $\mathbb{F}_q$ by setting:

$$\chi_{\alpha_i}(0) = \begin{cases} 0 & \alpha_i \neq 0 \\ 1 & \alpha_i = 0 \end{cases}$$

- Fixing an additive character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$, for a nontrivial multiplicative character χ we recall the **Gauss sum** to be:

$$g(\chi) := \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x)$$

- For a given α, we recall the **Jacobi sum** to be:

$$j(\alpha) := \frac{1}{q}\prod_i g(\chi_{\alpha_i})$$

- Finally, for fixed $\vec{n}, q$ let $n := \operatorname{lcm}(n_i)$ and $f = \operatorname{ord}_n(q)$. Then for every $\alpha \in \mathcal{A}_{\vec{n},q^f}$ we define $\mu(\alpha)$ to be the smallest integer such that $(q^{\mu(\alpha)} - 1)\alpha_i \in \mathbb{Z}$ for each i.

THEOREM 1.2.1. Given the notation as above, for $X : x_0^{n_0} + \cdots + x_r^{n_r} = 0$,

$$\zeta_X(t) = \left[\prod_{i=0}^{r-1} \frac{1}{1-q^i t}\right] \cdot \left[\prod_{\alpha \in A_{\vec{n},q^f}/\sim} \left(1 + (-1)^r j(\alpha)\, t^{\mu(\alpha)}\right)\right]^{(-1)^r}$$

where the $\alpha, \alpha' \in \mathcal{A}_{\vec{n},q^f}$ are equivalent iff $\alpha = q^e\alpha'$ for some $e \in \mathbb{Z}$.

Proof. The details of this result are messy and laborious enough for a paper of their own. We refer the reader to Weil's original paper [Wei49] and Sections 1-5 of [Chu+] for proofs. □

COROLLARY 1.2.1.1. A diagonal variety X is supersingular over $\mathbb{F}_q$ if and only if $j(\alpha) = \zeta q^{i/2}$ for ζ a root of unity for every $\alpha \in \mathcal{A}_{\vec{n},q^f}$.

1.3 The Stickleberger Criterion

Corollary 1.2.1.1 gives us a (somewhat) simpler criterion to check for supersingularity. As a quick sanity check, we note that for any non-trivial character χ that $|g(\chi)| = \sqrt{q}$, and so our condition satisfies the Riemann Hypothesis.

From this, we deduce that $|j(\alpha)| = q^{(r-1)/2}$, and basic algebraic number theory tells us this divided by $q^{r-1}/2$ is a root of unity iff $\text{ord}_{\mathfrak{p}}(j(\alpha)) \geq \frac{r-1}{2}$ for all $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ lying above p, where $K = \mathbb{Q}(\zeta_p, \zeta_{q^f-1})$. Verifying this condition is in general a hard problem, which we tackle via a theorem of Stickleberger.

THEOREM 1.3.1 (Stickleberger). Let $\mathfrak{p}$ be a prime lying over p in $\mathbb{Q}(\zeta_{q^f-1})$ and let $\mathfrak{P}$ be a prime lying over $\mathfrak{p}$ in $\mathbb{Q}(\zeta_{q^f-1}, \zeta_p)$. Let χ be a character of $\mathbb{F}_q$ such that

$$\chi(a) \equiv a^{-(q-1)/m} \mod \mathfrak{p}$$

Then for any integer $r \geq 1$ we have:

$$\tau(\chi^r) \sim \mathfrak{P}^{\eta(r)}$$

where

$$\eta(r) = \frac{1}{f} \sum_{\mu} s\left(\frac{(q-1)\mu r}{q^f - 1}\right) \sigma_{\mu}^{-1}$$

where the summation runs over all $\mu \in (\mathbb{Z}/(q^f-1)\mathbb{Z})^{\times}$ and where $s(v)$ is the sum of the digits of the p-adic expansion of v modulo $q-1$, i.e

$$s(v) = (p-1) \sum_{i=0}^{f-1} \left\{\frac{p^i v}{q-1}\right\}$$

Proof. See Theorem 10, page 97 of [Lan94]. □

Remark. Readers may be familiar with this theorem phrased in an alternative manner, that the Stickleberger ideal of an abelian number field K annihilates $Cl(K)$. The above is simply a raw, calculatory phrasing of this result in the case of $K = \mathbb{Q}(\zeta_{q^f-1}, \zeta_p)$.

This theorem, combined with what we deduced before about the Jacobi sum, leads us to our main tool for calculating supersingularity:

THEOREM 1.3.2. Let X be diagonal, defined by $(n_0, ..., n_r)$. Let $n = \text{lcm}(n_i)$, $f = ord_n(p)$ and $q = p^f$. Then X is supersingular over $\mathbb{F}_p$ if and only if, for each $\mu \in (\mathbb{Z}/n\mathbb{Z})^{\times}$,

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

for each

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

Proof. This essentially comes down to determining when the normalized product $\omega = q^{-(r+1)/2} \prod_i g(\chi_{\alpha_i})$ is a root of unity, and the result follows from an application of Stickleberger's theorem. For details

we refer the reader to Theorems 6.14 and 6.15 of [Chu+] □

Remark. The l_i here are the numerators of the $\alpha_i \in \mathcal{A}_{\vec{n},q}$. Using this rephrasing makes casework and computation simpler. As such, we henceforth refer to these l_i as the **Stickleberg numerators**.

This result allows us to write code that can verify supersingularity for any diagonal variety. See A for more details.

1.4 Weighted Projective Space Interlude

As mentioned before, we don't want to projectivize diagonal varieties in the standard way, as we lose the "nice" zeta function. Instead, we make use of the fact that the diagonal variety $(n_0, ..., n_r)$ naturally embeds into $\mathbb{P}(w_0, ...w_r)$, where each weight $w_i = \text{lcm}(n_i)/n_i$. One issue that arises here, however, is that this weighted projective space may not always be well-formed (i.e any subset of r weights must have gcd).

> DEFINITION 1.4.1. We say an exponent tuple $(n_0, ..., n_r)$ is **primitive** if $n_i \mid \text{lcm}(\{n_j\}_{j\neq i})$ for all i. Consequently we may talk about primitive diagonal varieties.

The ambient weighted projective space of a diagonal curve with primitive exponents is naturally well-formed because $w_i = N/n_i = \text{lcm}(n_i, n_j)/n_i = n_j/\gcd(n_i, n_j)$ which is coprime to $w_j = n_i/\text{lcm}(n_i, n_j)$. In fact, something stronger is true.

Observation. Every well-formed projective space arises from a set of primitive exponents. Suppose $n_0, ...n_r$ was not primitive, then WLOG $n_0 \nmid L_0 := \text{lcm}(n_1, ...n_r)$. In particular, some prime power $p^e \nmid L_0$. However this means that $p^e \mid w_i = n/n_i$ for all $i > 0$, and so the weights are not coprime, thus the space is not well-formed.

Generally when working with weighted projective space we only want to look at well-formed cases. To deal with diagonal varieties that have non-primitive exponents, however, we use the following result.

> PROPOSITION 1.4.2. Suppose X is the variety in weighted projective space over $\mathbb{F}_p$ defined by
>
> $$x_0^{n_0} + \ldots + x_r^{n_r} = 0$$
>
> For each i between 0 and r, let $l_i = \text{lcm}(\{n_j\}_{j\neq i})$ and $n_i' = \gcd(l_i, n_i)$. Then the variety X' in weighted projective space over $\mathbb{F}_p$ defined by
>
> $$x_0^{n_0'} + \ldots + x_r^{n_r'} = 0$$
>
> satisfies $\#X(\mathbb{F}_q) = \#X'(\mathbb{F}_q)$.

Proof. See Theorem 1.1 of [Chu+] □

Since every weighted projective space is isomorphic to a well-formed space (see [Hos20]), the variety X and X' in the above proposition are birationally isomorphic. As such, when continuing it suffices to only consider primitive exponent tuples. This result also allows us to have a very simple criterion for supersingularity of diagonal curves.

PROPOSITION 1.4.3. If $X : x_0^{n_0} + \cdots + x_r^{n_r}$ is such that $\gcd(n_0, n_i) = 1$ for all i, then X is supersingular.

Proof. By 1.4.2, once we reduce the exponents, the exponent of x_0 will be 1. However this means that, whatever the value of $(x_1, ..., x_r)$, there will be exactly one value of x_0 that sets the polynomial equal to 0. Thus, $\#X(\mathbb{F}_q) = q^r$ is the affine point-count of the variety. From what we saw in 1.1.3, the zeta function for this variety is $\frac{1}{1-q^r t}$, hence it is supersingular. □

1.5 Fermat Varieties

One of the major strides in understanding supersingular varieties was made by Shioda in his classification of Fermat varieties. We give an alternative proof of one the directions of his main result using our Stickleberger criterion, to give a flavor of the types of arguments that will be seen in Section 2.

THEOREM 1.5.1. The Fermat variety F_r^n is supersingular if and only if there exists v such that $p^v \equiv -1 \mod n$

Proof. If $p^v \equiv -1 \mod n$ then the order of p modulo n (i.e f) must be even.
Since we have:

$$s\left(\frac{(q-1)\mu l_i}{n}\right) = (p-1)\sum_{j=0}^{f-1}\left\{\frac{p^j \mu l_i}{n}\right\}$$

we can substitute it in and factor out the $(p-1)$ of the double summation, meaning it remains for us to show that:

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

for every $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$.
Breaking up the inner sum, we get

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

Note that $\{\{a\}+\{b\}\} = \{a+b\}$, which gives us:

$$\left\{\left\{\frac{p^j \mu l_i}{n}\right\} + \left\{\frac{p^{j+f/2}\mu l_i}{n}\right\}\right\} = \left\{\frac{p^j \mu l_i (p^{f/2}+1)}{n}\right\}$$

Since f is even, $p^{f/2} \equiv -1 \mod n$ and so $n \mid (p^{f/2}+1)$, and so the fraction in the brackets above is an integer, so the fractional part is zero. This means the sum of the two fractional parts can only be zero or one.

Note that for any combination, of μ, j and l_i, the value $\left\{\frac{p^j \mu l_i}{n}\right\}$ is never zero, since p and μ are both coprime to n and $l_i < n$. Thus the sum of the two fractional parts in the expression cannot be zero, so it must be one. There are $f/2$ terms in the inner summation and $r+1$ terms in the outer summation, giving us our desired equality.
For the reverse direction, refer to Section 3 of [SK79] □

Observation. Suppose $X : (n_0, ..., n_r)$, $Y : (m_0, ..., m_r)$ are two diagonal varieties of dimension $r-1$ such that each $n_i \mid m_i$. Then we have a surjective morphism $Y \to X$ given by $(x_i) \mapsto (x_i^{m_i/n_i})$, and so supersingularity of Y implies supersingularity of X.

This gives us an easy way to rule out supersingularity of an arbitrary diagonal variety X. If p is not a root of -1 modulo n, the lcm of the exponents, then F_r^n is not supersingular and thus X cannot be supersingular.

Question. Is every supersingular diagonal variety X covered by a supersingular Fermat?

The answer to this question in general is no.

> EXAMPLE 1.5.2. Pick primes r, s and an integer d such that $r, s, d \equiv 1 \mod p$ and p is a primitive root modulo r and s. Then by a theorem of [Chu+],
>
> $$X : x_0^r + x_1^s + x_2^{rd} + x_3^{sd}$$
>
> is supersingular over $\mathbb{F}_p$. However, clearly the Fermat surface F_3^{rsd} is not supersingular, by 1.5.1.

However, we shall see that this converse implication is actually true most of the time in the case of curves, i.e when $r = 2$. This will be our main result.

2. Classifying Supersingular Diagonal Curves

Our goal in this section will be to prove the following:

THEOREM 2.0.1 (Classification). Let (n_0, n_1, n_2) be a primitive tuple. Then, over $\mathbb{F}_p$, the curve $C\colon x_0^{n_0} + x_1^{n_1} + x_2^{n_2} = 0$ is supersingular if and only if either of the folllowing hold:

(1) one of the n_i is 1

(2) F_2^n is supersingular for $n = \text{lcm}(n_0, n_1, n_2)$

Using 3.2.2, we will see later that all the curves of genus $g > 0$ fall into case (2), and thus Theorem 0.0.1 follows from this classification.

Outline of the Proof Subsection 2.1 will build up some notation and results on prime powers modulo n to help simplify the later calculations. This subsection also classifies all possible primitive exponent tuples. Subsection 2.2 then proves some lemmas that will allow us to conduct the final casework to prove the theorem in 2.3.

2.1 S, N functions and Prime Powers

We use "primitive curve" to mean a curve with a primitive exponent tuple.

PROPOSITION 2.1.1. Every primitive exponent tuple of a curve is of the form (drs, dst, drt) for some pairwise coprime r, s, t.

Proof. Clearly picking any 4 integers d, r, s, t satisfying the above property produces a primitive exponent set.
Conversely, suppose that n_0, n_1, n_2 is a primitive exponent set. Let $d = \gcd(n_0, n_1, n_2)$, $r = \gcd(n_0, n_2)/d$, $s = \gcd(n_0, n_1)/d$, and $t = \gcd(n_1, n_2)/d$. Simple calculation verifies that they satisfy the desired equalities. □

To simplify a lot of the proofs and results of the next section, we introduce the following helpful notations, which we denote the S-function and N-function, respectively.

DEFINITION 2.1.2. Given a prime (power) p, a denominator n coprime to p, $f := \text{ord}_n(p)$, an element $\mu \in (\mathbb{Z}/n\mathbb{Z})^\times$ and integers $l_0, l_1 \in (0, n)$, we write:

$$S(l_k) := \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i l_k}{n} \right\}$$
$$N(l_0, l_1) := \#\left\{ i : \mu p^i (l_0 + l_1) \geq n \right\}$$

In most cases the values of μ, p and n will either be obvious from context or won't be relevant to calculations involing these functions, and so they are omitted from notation.

PROPOSITION 2.1.3. (Basic properties of the S and N functions)

(a) $S(l_0) + S(l_1) = S(l_0 + l_1) + N(l_0, l_1)$

(b) For n a fixed denominator, $S(a) = S(a + n)$ (i.e what really matters is the value of our input modulo n)

(c) For $n \nmid a$, we have $f - S(a) = S(-a)$

(d) If p is a root of -1 modulo n and $n \nmid a$ we have $S(a) = f/2$

(e) Suppose $d \mid a, n$, and $n' := n/d$ is such that p is a root of -1 modulo n'. Then $S(a) = f/2$.

Proof. a) and b) follow by simple inspection of definitions.

For c), we make the observation that $1 - \{\alpha\} = \{-\alpha\}$ for any $\alpha \neq 0$. Thus:

$$f - S(a) = f - \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i a}{n} \right\} = \sum_{i=0}^{f-1} 1 - \left\{ \frac{\mu p^i a}{n} \right\} = \sum_{i=0}^{f-1} \left\{ \frac{-\mu p^i a}{n} \right\} = S(-a)$$

where in the 3rd equality we can apply the identity because we know none of the terms are zero as we imposed that $n \nmid a$.

For d), since $p^v \equiv -1 \mod n$ for some v minimal, note that $p^{2v} \equiv 1$ and so it must be that $v = f/2$. Thus $p^i \equiv -p^{i+f/2} \mod q^e$. This gives us:

$$\begin{aligned} S(a) &= \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i a}{q^e} \right\} \\ &= \sum_{i=0}^{(f-2)/2} \left\{ \frac{\mu p^i a}{q^e} \right\} + \left\{ \frac{\mu p^{i+f/2} a}{q^e} \right\} \\ &= \sum_{i=0}^{(f-2)/2} 1 = f/2 \end{aligned}$$

For e), we can define $a' := a/d$ and write:

$$\begin{aligned} S(a) &= \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i a}{n} \right\} \\ &= \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i a'}{n'} \right\} \\ &= \frac{f}{f'} \left(\sum_{i=0}^{f'-1} \left\{ \frac{\mu p^i a'}{n'} \right\} \right) \\ &= \frac{f}{f'} \left(\frac{f'}{2} \right) = f/2 \end{aligned}$$

where the third line follows from the fact that each p^i repeats itself modulo n' with multiplicity f/f' and the last line follows from the observation that a', n' satisfy the conditions of property d). □

In the proof of the classification we will inductively build on results of supersingularity of Fermat curves, F_2^n. Recalling Shioda's condition of a prime p being a root of -1 modulo n, the following results will prove useful in our argument.

> LEMMA 2.1.4. If $n = a_1 \dots a_m$ for a_m coprime integers and for all $i \neq j$ there exists $v_{i,j}$ such that $p^{v_{i,j}} \equiv -1 \mod a_i a_j$ then $p^v \equiv -1 \mod n$ for $v = \operatorname{lcm}\{\operatorname{ord}_{a_i}(p)/2\}$.

Proof. We first make the observation that we can assume none of the a_i are 2, since even if there was, excluding it does not affect any part of the theorem statement.
Let $f_i := \operatorname{ord}_{a_i}(p)$, $h_i := \nu_2(f_i)$ (i.e the 2-adic valuation) and j be such that h_j is maximal. For any $i \neq j$ let $v_{i,j}$ be as in the statement of the theorem. Note $p^{v_{i,j}} \equiv -1 \mod a_i a_j \implies p^{v_{i,j}} \equiv -1 \mod a_i$, and thus $f_i \mid 2v_{i,j}$. Likewise $f_j \mid 2v_{i,j}$.
Consequently we can let $v_{i,j} = \operatorname{lcm}(f_i/2, f_j/2)$, and we deduce that $\nu_2(v_{i,j}) = h_j - 1$. If $h_j > h_i$ then f_i divides $2^{h_j - h_i - 1} f_i$ which in turn divides $v_{i,j}$. This would imply $p^{v_{i,j}} \equiv 1 \mod a_i$ which is a contradiction. Therefore $h_i = h_j = \nu_2(v_{i,j}) + 1$ for all i, j.
Setting $v := \operatorname{lcm}\{f_i/2\}$ then, we observe that for every i we have $v/(f_i/2)$ being an odd integer. Thus:

$$p^v \equiv (p^{f_i/2})^{v/(f_i/2)} \equiv (-1)^{v/(f_i/2)} \equiv -1 \mod a_i$$

and by the Chinese remainder theorem $p^v \equiv -1 \mod n$. □

> COROLLARY 2.1.4.1. If $n = q_1^{e_1} \dots q_m^{e_m}$ for $m \geq 3$ primes q_i and $p^{v_i} \equiv -1 \mod n/q_i^{v_i}$ for all i then $p^v \equiv -1 \mod n$ where $v = \operatorname{lcm}\{v_i\}$.

2.2 Intermediary Results

All of the following results will be used in the full casework of the classification theorem.

> PROPOSITION 2.2.1. The curve $x_0^{2a} + x_1^{2b} + x_2^{2c} = 0$ is trivially supersingular over all primes p if a, b, c are pairwise coprime.

Proof. First, $n = \operatorname{lcm}(2a, 2b, 2c) = 2abc$ as a, b, c are coprime. Then $l_0 = bck_0$, $l_1 = ack_1$, and

$l_2 = abk_2$ with $0 < k_0 < 2a$, $0 < k_1 < 2b$, and $0 < k_2 < 2c$. Further, $2abc \mid (bck_0 + ack_1 + abk_2)$ so

$$\begin{aligned} bck_0 + ack_1 + abk_2 &= 2abct \\ bck_0 &= 2abct - ack_1 - abk_2 \\ bck_0 &= a(2bct - ck_1 - bk_2) \end{aligned}$$

so $a \mid k_0$, and by symmetry $b \mid k_1$, $c \mid k_2$ so $k_0 = a$, $k_1 = b$, and $k_2 = c$. That is, $l_i = abc$ for all i, but then $2abc \mid 3abc$ which is a contradiction so there are no such l. Thus, this curve is vacuously supersingular. □

LEMMA 2.2.2. If $x_0^r + x_1^s + x_2^{rs} = 0$ for $\gcd(r, s) = 1$ is supersingular the Fermat curve F_2^{rs} is supersingular if and only F_2^r and F_2^s are supersingular.

Proof. We first show that supersingularity of $x_0^r + x_1^s + x_2^{rs}$ implies that the Fermat curve F_2^{rs} is supersingular iff a specially constructed variety X is supersingular. We will then prove that F_2^r, F_2^s being supersingular imply the supersingularity of X, thereby showing the desired equivalence.

Suppose that $x_0^r + x_1^s + x_2^{rs} = 0$ is supersingular. Then the Stickleberger condition is true for all $l_0, l_1, l_2 \in (0, rs)$ such that $rs | l_0 + l_1 + l_2$, $s | l_0$, $r | l_1$, and $\mu \in (\mathbb{Z}/rs\mathbb{Z})^\times$.
Since $l_0 + l_1 \equiv -l_2 \mod rs$, we have, for all μ and i, that $\left\{\frac{\mu p^i (l_0+l_1)}{rs}\right\} + \left\{\frac{\mu p^i l_2}{rs}\right\} = 1$, since the sum of the numerators in each fractional part must be an integer (note since $rs \nmid l_2$, it cannot divide $l_0 + l_1$ either). Thus we get:

$$\begin{aligned} 3f/2 &= S(l_0) + S(l_1) + S(l_2) \\ &= N(l_0, l_1) + S(l_0 + l_1) + S(l_2) \\ &= N(l_0, l_1) + f \end{aligned}$$

Thus, for any $l_0, l_1 \in (0, rs)$ such that $s \mid l_0$ and $r \mid l_1$, it must hold that $N(l_0, l_1) = f/2$.

Consider the variety X defined by $x_0^r + x_1^r + x_2^r + x_3^s + x_4^s + x_5^s$. Our set of possible numerators for the Stickleberger sum is given by $l_0, \ldots, l_5 \in (0, rs)$ such that $rs | \sum l_i$, $s | l_0, l_1, l_2$, $r | l_3, l_4, l_5$. The sum can be then written as:

$$\sum_{i=0}^{5} S(l_i) = \sum_{i=0}^{2} S(l_i + l_{i+3}) - S(l_i, l_{i+3})$$

Since $l_i, l_{i+3} \in (0, rs)$ satisfy $s \mid l_i, r \mid l_{i+3}$, we get that $S(l_i, l_{i+3}) = f/2$. Our sum then becomes:

$$3f/2 + \sum_{i=0}^{2} S(l_i + l_{i+3})$$

and X is supersingular iff the summation over S is $3f/2$. Note that the tuple $(l_0+l_3, l_1+l_4, l_2+l_5)$ satisfy all the conditions for a tuple of the Fermat curve F_2^{rs}. Thus the supersingularity of X and F_2^{rs} is equivalent.

Now assume that F_2^r, F_2^s are supersingular. We will show that each term in the summation $\sum_{i=0}^{5} S(l_i)$ for our variety X is equal to $f/2$, thereby proving supersingularity of X.
Since $s \mid l_j$ for $j \leq 2$ and $rs/s = r$, supersingularity of F_2^r implies the Shioda condition, i.e $p^v \equiv -1 \mod r$ for some v. We can thus apply property e) from 2.1.3 to deduce $S(l_j) = f/2$ for $j \leq 2$. By symmetry this equality also holds for $j > 2$, as desired. □

> COROLLARY 2.2.2.1. If $x_0^r + x_1^s + x_2^{rs}$ is supersingular over $\mathbb{F}_q$ for coprime r, s then $\text{ord}_{rs}(q)$ is even.

Proof. In the proof of the above lemma we showed that $N(l_0, l_1) = f/2$. Since this is an integer, f must be even. □

> LEMMA 2.2.3. For s odd, the curve $C : x_0^2 + x_1^s + x_2^{2s}$ is supersingular iff F_2^{2s} is supersingular.

Proof. The Stickleberger numerators for our curve C will be of the form $l_0, l_1, l_2 \in (0, 2s)$ such that $s|l_0, 2|l_1$, and $2s|\sum l_i$. Necessarily, $l_0 = s$, and $l_1 + l_2 \equiv s \mod 2s$, and thus l_2 must be odd. By property e) of 2.1.3 we deduce that $S(l_0) = f/2$. Supersingularity of C then tells us that that $S(l_1) + S(l_2) = f$, which implies $S(l_1) = S(-l_2)$, by property c) of 2.1.3. Observe this equality holds for any l_1, l_2 that sum to s, since this condition along with $l_0 = s$ is both necessary and sufficient for being a valid numerator tuple in the Stickleberger sum for C.
To prove supersingularity of the Fermat curve F_2^{2s} covering C, we will show that for any $l_j \in (0, 2s)$ that $S(l_j) = f/2$. We already know this is true for $l_j = s$. Otherwise from what we showed, we can use properties of the S-function to deduce that:

$$S(l_j) = S(l_j - s) = S(l_j + s) \tag{2}$$

since we only care about inputs of the S-function modulo $2s$. Expanding this identity, we get:

$$\begin{aligned} S(l_j) &= S(l_j + s) \\ &= \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i (l_j + s)}{2s} \right\} \\ &= \sum_{i=0}^{f-1} \left\{ \frac{\mu p^i l_j}{2s} + \frac{1}{2} \right\} \\ &= S(l_j) + f/2 - \# \left\{ i : \frac{\mu p^i l_j}{2s} \geq \frac{1}{2} \right\} \\ \implies f/2 &= \#\{i : 2\mu p^i l_j \geq 2s\} = N(l_j, l_j) \end{aligned}$$

This implies that for any $l_j \neq s$, we have that $2S(l_j) = S(2l_j) - f/2$. Using this as a base case, we proceed show for all k that

$$2^k S(l_j) = S(2^k l_j) + (2^k - 1)\frac{f}{2} \tag{3}$$

Inductively, we have:

$$\begin{aligned} 2^{k+1} S(l_j) &= 2S(2^k l_j) + 2(2^k - 1)f/2 \\ &= S(2^{k+1} l_j) + f/2 + (2^{k+1} - 2)f/2 \\ &= S(2^{k+1} l_j) + (2^{k+1} - 1)f/2 \end{aligned}$$

Now take e such that $= 2^e \equiv 1 \mod s$. We note that either $2^e l_j$ is either equivalent to l_j or $l_j + s$ modulo $2s$. In either case, applying the identity in (2) we have $S(2^e l_j) = S(l_j)$. Applying (3), we get:

$$\begin{aligned} 2^e S(l_j) &= S(2^e l_j) + (2^e - 1)f/2 \\ &= S(l_j) + (2^e - 1)f/2 \\ \implies S(l_j) &= f/2 \end{aligned}$$

Therefore F_2^{2s} is supersingular. □

2.3 Classification Theorem

To fully classify all curves we have to take into account all possible primitive exponent tuples. That is, all possible (drt, dst, drs) for r, s, t coprime. We first tackle the case where $d = 1$, and $t = 1$ as well.

> PROPOSITION 2.3.1. For $\gcd(r, s) = 1$ and p a prime power the curve $C : x_0^r + x_1^s + x_2^{rs} = 0$ over $\mathbb{F}_p$ is supersingular if and only if F_2^{rs} is supersingular over $\mathbb{F}_p$.

Proof. We split this up into 3 cases: 1) both r, s are prime powers, 2) one of them has multiple prime

factors and 3) both have multiple prime factors. Each case will build inductively on the previous one.

Case 1: r, s prime powers

We claim in this case that p must be a negative root of -1 modulo both r and s.
By 2.2.2.1, f is even and thus either $f_r = \text{ord}_r(p)$ is even or $f_s = \text{ord}_s(p)$ is even. If r, s are both odd then WLOG f_r is even and since r is a prime power, p must be a root of -1 modulo r. Otherwise, WLOG $s = 2^e$, and supersingularity of C implies that $C' : x_0^r + x_1^2 + x_2^{2r}$ is also supersingular. By 2.2.3, F_2^{2r} must be supersingular which then implies F_2^r is supersingular, and by the Shioda condition p must be a root of -1 modulo r.
We proceed treating r as an odd prime and s as a prime power not equal to 2. Stickleberger for C tells us that for all $l_0, l_1, l_2 \in (0, rs)$ such that $rs | \sum l_i$, $s | l_0$, $r | l_1$, $f = \text{ord}_{rs}(p)$ and $\mu \in (\mathbb{Z}/rs\mathbb{Z})^\times$:

$$3f/2 = \sum_{j=0}^{2} S(l_j)$$

Note our condition implies $l_2 \equiv -l_0 - l_1 \mod rs$, so we have:

$$S(l_1) = 3f/2 - S(l_0) - S(-l_0 - l_1)$$

Since $s \mid l_0$ and $r \mid l_1$, we get the functional equation:

$$S(ra_1) = 3f/2 - S(sa_0) - S(-ra_1 - sa_0)$$

for all $0 < a_0 < r$, and $0 < a_1 < s$. By property e) of 2.1.3, $S(sa_0) = f/2$.
Applying the above equality and result c) of 2.1.3, our functional equation thus becomes:

$$S(ra_1) = S(ra_1 + sa_0) \tag{4}$$

for all $0 < a_1 < s$ and $0 < a_0 < r$.

Consider the variety $X : x_0^r + x_1^r + x_2^{rs} + x_3^{rs} = 0$, which we claim is supersingular if C is supersingular. The numerators in the Stickleberger sum are $l_0, \ldots, l_3 \in (0, rs)$ such that $rs | \sum l_i$ and $s | l_0, l_1$. Note this implies $s | l_2 + l_3$. Writing $l_2 = ra_2 + sb_2$ and $l_2 = ra_3 + sb_3$, we deduce that $a_2 \equiv -a_3 \mod s$, implying $ra_2 \equiv -ra_3 \mod rs$.
By supersingularity of C we apply equation 4 to get:

$$S(l_2) = S(ra_2 + sb_2) = S(ra_2)$$

Similarly $S(l_3) = S(ra_3)$, and so by property b) and c) of 2.1.3 we get $S(l_2) + S(l_3) = S(l_2) + S(-l_2) = f$.
Moreover since $s \mid l_0, l_1$ we can apply property e) of 2.1.3 to deduce that $S(l_0) = S(l_1) = f/2$.

Therefore our Stickleberger sum is:

$$S(l_0) + S(l_1) + S(l_2) + S(l_3) = f + S(l_2) + S(-l_2) = 2f$$

and thus X is supersingular.

We claim this implies F_2^{rs} (which covers our original curve C) is supersingular. Suppose that there does not exist v such that $p^v \equiv -1 \mod s$. Let a be a primitive root modulo r and consider the subgroupgroup $H := \langle a \mod r \rangle \times \langle p \mod s \rangle \subseteq (\mathbb{Z}/r\mathbb{Z})^\times \times (\mathbb{Z}/s\mathbb{Z})^\times \cong (\mathbb{Z}/rs\mathbb{Z})^\times$. Clearly $p \in H$. Note $(-1 \mod r, 1 \mod s) \in H$, so if $-1 \in H$ then $(1 \mod r, -1 \mod q) \in H$, which would imply p is a root of $\equiv -1 \mod s$, which is a contradiction. Therefore $-1 \notin H$. Finally clearly the map $H \hookrightarrow (\mathbb{Z}/rs\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/r\mathbb{Z})$ is a surjection since $(a \mod r, 1 \mod s) \mapsto a \mod r$. Note all of these conditions sastisfy Theorem 15.3 of [Chu+], implying X is not supersingular, and we arrive at a contradiction. Therefore p must be a root of -1 modulo s.

We claim that all three terms in the Stickleberger sum of the Fermat curve covering C are equal to $f/2$, implying supersingularity. If r or s divide l_i, using the fact that we just showed p is a root of -1 modulo both of them, we can apply property e) of 2.1.3 to get that $S(l_i) = f/2$. Otherwise, let $l_i = ra_i + sb_i$. Define $l_j := -ra_i$ and $l_k := -sb_i$. Then l_i, l_j, l_k are numerators for the Stickleberger sum of our original curve C, and by supersingularity we have:

$$\begin{aligned} 3f/2 =& S(l_i) + S(l_j) + S(l_k) \\ &= S(ra_i + s^e b_i) + S(-ra_i) + S(-s^e b_i) \\ &= S(l_i) + f/2 + f/2 \\ \implies f/2 =& S(l_i) \end{aligned}$$

where the third line follows from property e) of 2.1.3. Thus F_2^{rs} is supersingular, as desired.

Case 2: r a prime power, s has multiple prime factors

First suppose s has only 2 distinct prime factors, i.e $s = q_1^{e_1} q_2^{e_2}$ for primes q_1, q_2. If C is supersingular then so is $x_0^r + x_1^{q_1^{e_1}} + x_2^{rq_1^{e_1}} = 0$. By our base case this implies $F_2^{rq_1^{e_1}}$ is supersingular and thus so is F_2^r. Given a_0, a_1 such that $0 < a_0 < r$ and $0 < a_1 < s$, we note that the numerators $l_0 = sa_0, l_1 = ra_1$, and $l_2 = -sa_0 - ra_1$ satisfy the conditions of Stickleberger for our curve C. This gives us:

$$3f/2 = S(sa_0) + S(ra_1) + S(-sa_0 - ra_1)$$

Since p is a root of $-1 \mod r$ we apply property e) to see that $S(sa_0) = f/2$ which gives us the functional equation:

$$S(ra_1) = S(ra_1 + sa_0)$$

By the exact same argument as in the case where s is a prime power, we deduce that the variety

$X : x_0^r + x_1^r + x_2^{rs} + x_3^{rs}$ is supersingular. This then implies that p is a root of -1 modulo s, again by the same reasoning as before. Writing $r = q_0^{e_0}$ then $rs = q_0^{e_0} q_1^{e_1} q_2^{e_2}$, then by supersingularity of $F^{rq_i^{e_i}}$ for $i = 1, 2$ we have that there exist v_i such that $p^{v_i} \equiv -1 \mod rs/q_i^{e_i}$ for all i, and thus there exists v such that $p^v \equiv -1 \mod rs$ by 2.1.4.1. Therefore F_2^{rs} is supersingular.

Now suppose s has more that three prime divisors. Let $r = q_0$ and $s = q_1^{e_1} \dots q_m^{e_m}$. We wish to show for each i that the curve $F_2^{rs/q_i^{e_i}}$ is supersingular, which will imply F_2^{rs} is supersingular by 2.1.4.1.
For $i \geq 1$ the curve $x_0^{q_0} + x_1^{s/q_i^{e_i}} + x_2^{rs/q_i^{e_i}} = 0$ is supersingular, and by the inductive hypothesis this implies $F_2^{rs/q_i^{e_i}}$ is supersingular. Thus there exists v_i such that $p^{v_i} \equiv -1 \mod rs/q_i^{e_i}$ for each $i \geq 1$. For $i = 0$, we note that $F_2^{rs/q_i^{e_i}}$ being supersingular implies $F_2^{s/q_i^{e_i}}$ is supersingular. This means there exist u_i such that $p^{u_i} \equiv -1 \mod s/q_i^{e_i}$ and hence there exists v_0 such that $p^{v_0} \equiv -1 \mod s$, as desired. Thus F_2^{rs} is supersingular.

Case 3: r, s both have multiple prime factors

Now let $r = q_1^{e_1} \cdots q_n^{e_n}$ and $s = q_{n+1}^{e_{n+1}} \cdots q_{n+m}^{e_{n+m}}$, and assume C is supersingular. For every $i \leq n$ we have that the curve $C_i : x_0^{q_i^{e_i}} + x_1^s + x_2^{q_i^{e_i} s} = 0$ is supersingular. By what we previously showed this means $F_2^{q_i^{e_i} s}$ is supersingular, which implies that F_2^s is supersingular. Symmetrically, F_2^r is supersingular. By 2.2.2 we deduce F_2^{rs} is supersingular. □

This result allows us to easily generalize to the case where we fix $d = 1$ and let t vary.

> COROLLARY 2.3.1.1. For coprime r, s, t, the curve (rt, st, rs) is supersingular over $\mathbb{F}_p$ if and only if F_2^{rst} is supersingular.

Proof. This curve being supersingular implies that (r, s, rs), (r, t, rt) and (s, t, st) are also all supersingular. By our result above, these imply F_2^{rs}, F_2^{rt} and F_2^{st} are all supersingular as well, which means p is a root of -1 modulo all possible pairwise products of r, s, t. By 2.1.4 it is also a root of minus -1 modulo rst, and so F_2^{rst} is supersingular over $\mathbb{F}_p$, as desired. □

We now proceed to the full proof of the classification.

proof of 2.0.1. Case (2) of the theorem follows trivially from 1.4.3. Thus we assume $C : x_0^{drt} + x_1^{dst} + x_2^{drs}$ is supersingular, where none of the exponents are 1. The case of $d = 1$ is dealth with in 2.3.1.1. As such we may assume $d > 1$.

Case 1: $drst$ is a prime power

By primitivity, we deduce the exponent tuple is of the form (w^e, w^{e+h}, w^{e+h}) for a prime w, and we wish to deduce $F_2^{w^{e+h}}$ is supersingular. Supersingularity of this curve implies supersingularity of $F_2^{w^e}$, which means p is a root of -1 modulo w^e, and so the order of p modulo w^e is even. If w is odd

then that means p must also be a root of -1 modulo w^{e+h}, giving us our desired result. As such, we assume $w = 2$.

Suppose first that $e = 1$, we proceed by induction on h. For $h = 0$ the result is immediate. Otherwise, Stickleberger dictates that $l_0 = 2^h$, and since $2^{h+1} \mid \sum l_i$ we must have that $l_1 + l_2 \equiv 2^h \mod 2^{h+1}$. By property e) of 2.1.3 we have that $S(l_0) = f/2$, and consequently $S(l_1) = S(-l_2)$. Thus we are only concerned with the value of the Stickleberger numerators modulo 2^h.

Let us write $l_1 = (2^h + 1)a$. If a is even then we write it as $2b$. Noting that supersingularity of $(2, 2^{h+1}, 2^{h+1})$ implies supersingularity of $(2, 2^h, 2^h)$, we apply the inductive hypothesis to deduce $F_2^{2^h}$ is supersingular. From there, we apply property e) again to see that $S(a) = S(2b) = f/2$. Now suppose that a is odd, then we note that

$$\left\{\frac{\mu p^i a(2^h+1)}{2^{h+1}}\right\} = \left\{\frac{\mu p^i a}{2} + \frac{\mu p^i a}{2^{h+1}}\right\}$$

Here we can apply the exact same trick we did in the proof of 2.2.3 to deduce that $N(a, a) = f/2$. Continuing along the same proof method, we also deduce for all k that $2^k S(a) = S(2^k a) + (2^k - 1)\frac{f}{2}$, which then implies $S(a) = \frac{f}{2}$ for all a. Therefore $F_2^{2^{h+1}}$ is supersingular.

Now suppose that $e > 1$, then $x_0^2 + x_1^{2^{e+h}} + x_2^{2^{e+h}} = 0$ is supsersingular and $F_2^{2^{e+h}}$ is supersingular by changing variables $e + h \to h$.

For our next cases we assume that $drst = \prod q_i^{e_i}$ has multiple prime factors. Note by Lemma 2.1.4 that if we can show that p is a root of minus one modulo $q_i^{e_i} q_j^{e_j}$ for every pair (i, j) then it follows that F_2^{drst} is supersingular. This will be our strategy.

Case 2A: $drst$ has multiple prime factors, $r, s = 1$

Here our curve is of the form $C : x_0^d + x_1^{dt} + x_2^{dt} = 0$. We first only consider odd primes $q^e, q'^f || dt$. If either of them divide d, let it be q without loss of generality, supersingularity of C implies the curve with exponents (q, q', qq') is supersingular, which implies $F_2^{qq'}$ is supersingular by 2.3.1. Otherwise, suppose $q, q' \mid t$ but neither of them divide d. Letting z be a prime factor of d, we deduce that the curve with exponents $(qq', z, qq'z)$ is supersingular which implies supersingularity of $F_2^{qq'z}$ and hence of $F_2^{qq'}$. In either case, since q, q' are both odd, if p is a root of -1 modulo their product it is also a root of -1 modulo $q^e q'^f$ for any powers, which is what we want.

Now let q be an odd prime factor of dt and 2 be the other one. Suppose $2^e, q^h || dt$. If $q \mid d$ then the curve with exponents $(q, 2^e, 2^e q)$ is supersingular and so $F_2^{2^e q}$ is supersingular. Note if $p^v \equiv -1 \mod 2^e q$ then $p^{vq^{h-1}} \equiv -1 \mod 2^e q^h$, which implies $2^e q^h$ is also supersingular. Otherwise if $q \nmid d$, it must divide t. If e' is such that $2^{e'} || d$, then supersingularity of C implies $(2^{e'}, 2^e q^h, 2^e q^h)$ is supersingular. If $e' = e$ we are fine, so suppose $e' < e$. The case where $e' = 0$ reduces to a trivial previous case so we can assume e' is positive. In this case, this implies the curve C' with exponents $(2, 2^e q^h, 2^e q^h)$ is supersingular. Using the same trick as with the prime power 2 case, we deduce

that for any Stickleberger numerator of C' that $S(l_i) = f/2$. As such, the same holds for any Stickleberger numerator of $F_2^{2^e q^h}$, implying supersingularity, which is what we wanted.
Thus, for every possible pair of prime factors $q_i^{e_i}, q_j^{e_j}$ of dt, we showed that p is a root of -1 modulo their product, and so F_2^{dt} is supersingular, as desired.

Case 2B: $drst$ has multiple prime factors, $r, s \neq 1$

Here our curve C has exponents (drs, dst, drt). Let q, q' be primes that divide $drst$ and $q^e, q'^f || drst$. If both these powers divide d, then supersingularity of C implies supersingularity of the curve with exponents $(q^e, q'^f, q^e q'^f)$, and consequently of $F_2^{q^e q'^f}$.
Otherwise, since r and s are coprime, we can assume without loss of generality that either they both divide dr or one divides dr and the other divides ds. The former case implies supersingularity of $(q^e q'^f, s, q^e q'^f s)$, and the latter implies supersingularity of $(q^e, q'^f, q^e q'^f)$. In either case, $F_2^{q^e q'^f}$ is supersingular for every posssible pair of primes, and so F_2^{drst} is supersingular, as desired. □

3. Genera of Diagonal Curves

Recall that every curve has a non-negative genus that is birational-invariant.

Question. Does there exist a supersingular curve of every genus over every possible characteristic?

This question has been answered positively for $g \leq 4$ (see [KHS20]), but to our knowledge there is little to no literature on $g > 5$.
We will see that by limiting ourselves to diagonal curves, we can get nice lower bounds on the density of primes over which a supersingular curve of genus g can be found. In particular, we compute $\delta'(g)$, the density of primes over which a supersingular diagonal curve of genus g arises.

3.1 Smoothness

> PROPOSITION 3.1.1. A diagonal curve is smooth over a field of characteristic p if and only if p does not divide any of its exponents.

Proof. Consider the general form of the curve

$$C\colon a_0 x_0^{n_0} + a_1 x_1^{n_1} + a_2 x_2^{n_2} = 0$$

over $\mathbb{F}_p$. Without loss of generality we can assume $a_0 = a_1 = a_2 = 1$ and the exponents are primitive as every diagonal curve is isomorphic to such a curve over the algebraic closure, which preserves smoothness when we base change back to the ground field. We have the canonical action on the space $\mathbb{A}^3 \setminus \{0\}$ by μ_N where $N = \operatorname{lcm}(n_0, n_1, n_2)$ given by $\zeta \cdot (x_0, x_1, x_2) = (\zeta^{w_0} x_0, \zeta^{w_1} x_1, \zeta^{w_2} x_2)$, and the quotient $\mathbb{P}(w_0, w_1, w_2) = (\mathbb{A}^3 \setminus \{0\})/\mu_N$ (where the weights $w_i = N/n_i$). The fixed points of this

action are those for which $\zeta^{w_i} x_i = x_i$. Without loss of generality, assume $x_0 \neq 0$ so that $\zeta^{w_0} = 1$ or $\zeta \in \mu_{w_0}$. Then assume $x_1 \neq 0$ such that $\zeta^{w_1} = 1$, which implies $\zeta \in \mu_{w_1}$. Since the exponents are primitive, the weights are well-formed or are pairwise coprime, so $\zeta = 1$. Hence the only fixed points are those for which exactly one coordinate is nonzero, but that is not a point on C so it misses all fixed points of the group action.
Hence we can apply the Jacobian criterion on an affine open set $D(x_0)$. Then $C \cap D(x_0)$ is given by $1+y_1^{m_1}+y_2^{m_2} = 0$ where $y_i = x_i^{a_0}/x_0^{a_i}$ and $m_i = \gcd(n_0, n_i)$. Then the Jacobian is $[m_1 y_1^{m_1-1}, m_2 y_2^{m_2-1}]$. Since $p \nmid n_0$, we have $m_i \neq 0$ and if $m_i = 1$ then $m_i y_i^{m_i-1} \neq 0$, hence $y_1 = y_2 = 0$ but this is not a point on $C \cap D(x_0)$, so it is smooth. The other patches are smooth by a symmetric argument. □

3.2 Genus Formula

By smoothness the geometric and arithmetic genus are the same, so we apply the ideas of [Hos20] which gives a generalization of the degree-genus formula to weighted projective space via Riemann-Hurwitz.

THEOREM 3.2.1 (Hosgood). Let $C = C_f \subset \mathbb{P}(a_0, a_1, a_2)$ be a nonsingular plane curve where f is weighted-homogeneous of degree d and sufficiently general. Assume further that the straight cover $\overline{C}$ is non-singular. Then,

$$g_C = \frac{1}{a_0 a_1 a_2}\left(\frac{(d-1)(d-2)}{2} - \left[\frac{b(\pi)}{2} + 1 - a_0 a_1 a_2\right]\right) \tag{5}$$

where the branching index $b(\pi)$ is given by

$$b(\pi) = (d-1)\sum_{i=1}^{3}(a_i - 1) + \sum_{i=1}^{3}\begin{cases} a_i - 1 & a_i \mid d \\ a_0 a_1 a_2 - 1 & a_i \nmid d \end{cases}$$

Proof. See Theorem 5.3.7 of [Hos20]. □

The curve is sufficiently general in the sense of [Hos20] as for all i, $a_i = N/n_i \mid N$. Thus, we have the following.

COROLLARY 3.2.1.1. The diagonal curve $C\colon x_0^{n_0} + x_1^{n_1} + x_2^{n_2} = 0$ with primitive exponents has

$$g_C = 1 + \frac{(n_0-1)(n_1-1)(n_2-1) - (n_0+n_1+n_2) + 1}{2N} \tag{6}$$

Proof. Direct application of (5) with $a_i = N/n_i$, $d = N$, and $b(\pi) = d(a_0 + a_1 + a_2 - 3)$ □

PROPOSITION 3.2.2. If C is a genus 0 diagonal curve with primitive exponents then C is given by $(1, n, n)$ for some $n \geq 1$ or $(2, 2, 2)$.

Proof. Let (n_0, n_1, n_2) be the exponents of C ordered smallest to largest. If the exponents are $(2,2,2)$ then the curve has genus zero by the degree-genus formula. If $n_2 \leq 2$ then the possible curves are $(1,1,1), (1,2,2), (1,1,2), (2,2,2)$ but note that $(1,1,1)$ and $(1,2,2)$ are of the supposed form and $(1,1,2)$ is not primitive, so we may assume $n_2 > 2$. We want to show $n_0 = 1$, so suppose $n_0 > 1$. Note that $n_1 n_2 - n_1 - n_2 = (n_1 - 1)(n_2 - 1) - 1 > 0$ as $n_2 > 2$ and $n_1 \geq n_0 > 1$. Then

$$\begin{aligned}
\frac{n_0 n_1 n_2 - n_0 n_1 - n_0 n_2 - n_1 n_2}{2\mathrm{lcm}(n_0, n_1, n_2)} &= -1 \\
n_0 n_1 n_2 - n_0 n_1 - n_0 n_2 - n_1 n_2 &= -2\mathrm{lcm}(n_0, n_1, n_2) \\
n_0(n_1 n_2 - n_1 - n_2) - n_1 n_2 &= -2\mathrm{lcm}(n_1, n_2) \\
n_1 n_2 - n_1 - n_2 - n_1 n_2 &< -2\mathrm{lcm}(n_1, n_2) \\
n_1 + n_2 &> 2\mathrm{lcm}(n_1, n_2) \geq 2n_2 \\
n_1 &> n_2
\end{aligned}$$

This is a contradiction since we assumed $n_1 \leq n_2$, and so $n_0 = 1$. Then $n_1 \mid \mathrm{lcm}(1, n_2) = n_2$ and $n_2 \mid \mathrm{lcm}(1, n_1) = n_1$ so $n_1 = n_2 = n$ and we are done.

□

PROPOSITION 3.2.3. Let C be a diagonal curve with primitive exponents (n_0, n_1, n_2) in ascending order. Then if $g_C \neq 0$ we have that

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

Proof. By 3.2.2 if $g_C \geq 1$ then $n_0 > 1$. We use the genus formula as defined before:

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

and without loss of generality we assume $n_0 \leq n_1 \leq n_2$. By assumption of the exponent tuple being primitive, we note that since $n_2 \mid \mathrm{lcm}(n_0, n_1)$ we have that $\mathrm{lcm}(n_0, n_1, n_2) = \mathrm{lcm}(n_0, n_1)$. Since $g_C \geq 1$, we have

$$\frac{n_2(n_0 n_1 - n_0 - n_1) - n_0 n_1}{2\mathrm{lcm}(n_0, n_1)} \geq 0$$

and hence $(n_0 n_1 - n_0 - n_1) \geq 0$. Since $n_2 \geq n_1$, we have $n_2(n_0 n_1 - n_0 - n_1) \geq n_1(n_0 n_1 - n_0 - n_1)$ so

$$g_C \geq 1 + \frac{n_1(n_0 n_1 - n_0 - n_1) - n_0 n_1}{2\mathrm{lcm}(n_0, n_1)} = 1 + \frac{(n_0 - 1)n_1^2 - 2n_0 n_1}{2\mathrm{lcm}(n_0, n_1)}$$

Now $(n_0 - 1)n_1^2 - 2n_0 n_1 \geq 0$ if and only if $(n_0 - 1)n_1 \geq 2n_0$ or $(n_0 - 1)/(2n_0) \cdot n_1 \geq 1$. Noting that $(n_0 - 1)/(2n_0)$ is increasing and $n_0 > 1$, we have that this is true if and only if $n_1 \geq 4$.

Then since $\operatorname{lcm}(n_0, n_1) \leq n_0 n_1$, this implies

$$\begin{aligned} g_C &\geq 1 + \frac{(n_0 - 1)n_1^2 - 2n_0 n_1}{2n_0 n_1} \\ &\geq \frac{(n_0 - 1)n_1^2}{2n_0 n_1} \\ &\geq \frac{(n_0 - 1)}{2n_0} n_1 \end{aligned}$$

Now we treat the exceptional cases $n_1 = 2, 3$. If $n_0 = 2$ the only primitive curves are $(2, 2, 2), (2, 3, 6)$. The first has genus 0, and so is excluded, and the second has genus 1 which is greater than $(n_0 - 1)/(2n_0) \cdot n_1 = 3/4$. If $n_0 = 3$ the only primitive curve is $(3, 3, 3)$ which is genus 1, which is equal to $(n_0 - 1)/(2n_0) \cdot n_1 = 1$. Thus we are done. □

This is significant because if $n_0 \geq 2$ this implies $n_0, n_1 \leq 4g_C$ and thus $n_2 \leq 16g_C^2$, which implies there exists a supersingular diagonal genus $g_C \geq 1$ curve over $\mathbb{F}_p$ if and only if there is such a curve with primitive exponents satisfying $(n_0, n_1, n_2) \leq (4g_C, 4g_C, 16g_C^2)$, which is a finite computation.

Example 3.2.4. If C is a diagonal elliptic curve then it is given by one of

$$C\colon \begin{cases} a_0 x_0^2 + a_1 x_1^3 + a_2 x_2^6 = 0 \\ a_0 x_0^2 + a_1 x_1^4 + a_2 x_2^4 = 0 \\ a_0 x_0^3 + a_1 x_1^3 + a_2 x_2^3 = 0 \end{cases}$$

Proof. Finite computational check. □

3.3 Density of Primes for a Given Genus

Proposition 3.3.1. For every genus g, there are infinitely primes over which a curve of genus g is supersingular, and infinitely many primes over which no curve of genus g is supersingular.

Proof. Take any genus-g curve $C : (n_0, n_1, n_2)$ with lcm n and consider the arithemtric progression $n - 1, 2n - 1, \ldots$. By Dirichlet's theorem, it contains infinitely primes, and C is supersingular over all of them by our classification.
Now consider all curves of genus g, and suppose they are each covered by a minimal Fermat of degree N_i. Let N be the lcm of all these N_i. Then the arithmetic progression $N + 1, 2N + 1, \ldots$ also contains infinitely many primes, and none of the curves can be supersingular over any of them because none of the Fermat's covering them are supersingular over any of them. □

The above proposition essentially shows that we could never hope to fully answer the prime-genus question by solely restricting to diagonal curves. However, we nonetheless can get nice lower bounds on densities.

PROPOSITION 3.3.2. The denominator of $\delta'(g)$ is always a power of 2.

Proof. Taking the group $(\mathbb{Z}/n\mathbb{Z})^\times$, we write it as $A \times B$, where A is the 2-group. Let $R \subseteq A_i$ be the roots of -1 modulo n that have order a power of 2. Then note $R \times B$ is exactly the set of all possible roots of -1.
Let π_i denote the surjection $(\mathbb{Z}/n\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/n_i\mathbb{Z})^\times$ for each i, and let A_i, B_i, R_i be the images of A, B, R respectively. Then the density $\delta'(g)$ is:

$$\begin{aligned}\delta'(g) &= \frac{|\bigcup_i(\pi^{-1}(R_i \times B_i)|}{|(\mathbb{Z}/m\mathbb{Z})^\times|} \\ &= \frac{|(\bigcup_i \pi^{-1}R_i) \times B|}{|A \times B|} \\ &= \frac{|(\bigcup_i \pi^{-1}R_i)| \cdot |B|}{|A| \cdot |B|} = \frac{|(\bigcup_i \pi^{-1}R_i)|}{|A|}\end{aligned}$$

and since A is a 2-group it has order a power of 2, which is what we wanted to show. □

[Wat84] computes the density of primes $\delta(m)$ over which a Fermat variety of degree m is supersingular via the following result.

PROPOSITION 3.3.3 (Waterhouse). If m is divisible by 4, then $\delta(m) = 2^{-d}$ where 2^d is the highest power of 2 dividing $\varphi(m)$. If m is not divisible by 4 and is divisible by s different odd primes p_i, then

$$\delta(m) = (2^{sc} - 1)/2^d(2^s - 1) \tag{7}$$

where 2^c is the highest power of 2 dividing all $p_i - 1$.

We wish to extend this to compute $\delta'(g)$. Fix some g, and let (a_i, b_i, c_i) for $i = 0, \ldots, k$ be the primitive exponents whose diagonal curve C_i has genus $g_{C_i} = g$. Let $n_i = \text{lcm}(a_i, b_i, c_i)$ for all i, and note that C_i is supersingular over $\mathbb{F}_p$ if and only if $F_2^{n_i}$ is supersingular, if and only if $p^v \equiv -1 \pmod{n_i}$ for some v. This reduces to counting the proportion of primes p such that $p \equiv a \pmod{n_i}$ where a is a root of -1 mod n_i, for some i.

COROLLARY 3.3.3.1.

$$\limsup_{g\to\infty} \delta'(g) = 1$$

Proof. We make the basic observation that $\delta'(g) \geq \max\{\delta(n_i)\}_{i\in[0,k]}$. By picking g that is of the form $(p-1)(p-2)/2$ for p a prime number that is one more than 2^u for u large, then $\delta(m)$ is of the form $\frac{2^u-1}{2^u}$. Since u can get arbitrarily large, we can get arbitrarily close to 1, as desired. □

This density can be computed explicity by letting $n = \text{lcm}(n_i)_{i=0,\ldots,k}$ and determining how many residue $(\mathbb{Z}/n\mathbb{Z})^\times$ reduce to a root of -1 in $(\mathbb{Z}/n_i\mathbb{Z})^\times$ for some i, and then using Dirichlet to compute

the density of primes congruent to one of those residue classes. Appendix C contains the data for these densities, and Appendix B contains the code for calculating them.

As of yet we seem to have no good way of lower-bounding these densities, as it requires understanding the size of the pre-images of all the R_i in proportion to the 2-group of $\mathbb{Z}/n\mathbb{Z}$. However, based on our data so far we make the following conjecture:

> CONJECTURE 3.3.4.
>
> $$\liminf_{g\to\infty} \delta'(g) \geq 1/2$$

Hopefully future work yields fruit on this hypothesis.

A. Supersingularity Computation

```
from sage.all import *
from sage.arith.functions import LCM_list

# Calculate relevant s-function in Stickleberger's thm
def s(v, p, f):
    q = p**f;
    return (p-1) * sum([frac(p**i * v) for i in range(0, f)])


# Check modulo condition for L-tuples
def condition(l, N, n, r):
    for j in range(0, r + 1):
        if (l[j] * N[j]) % n != 0:
            return False;
    return True;

# Check if covered by supersingular fermat
def fermatCover(N, p):
    n = LCM_list(N);
    for v in range(euler_phi(n)):
        if power_mod(p, v, n) == Mod(-1, n):
            return True;
    return False;

# Check if one exponent is coprime to the rest
def gcdCondition(N):
    for i in range(len(N)):
        coprime = True;
        for j in range(len(N)):
            if i != j and gcd(N[i], N[j]) != 1:
                coprime = False;
        if coprime:
            return True;
    return False;

# Check if of the form 2a, 2b, 2c for a,b,c pairwise coprime
def quadricCondition(N):
    if len(N) == 3:
        if N[0] % 2 == 0 and N[1] % 2 == 0 and N[2] % 2 == 0:
            a = N[0]/2; b = N[1]/2; c = N[2]/2;
            if gcd(a,b) == 1 and gcd(a,c) == 1 and gcd(b,c) == 1:
                return True;
    return False;

# Check if the curve is singular
def singular(N, p):
    for i in range(len(N)):
        if N[i] % p == 0:
            return True;
    return False;

# Exclude cases we don't care about
def isTrivial(N, p):
    if gcdCondition(N) or quadricCondition(N):
        return True;
```

```
    return False;

# Reduce the exponent set to an equivalent set
def reduceExp(N):
    newN = [1]*len(N);
    for i in range(len(N)):
        Li = LCM_list(N[:i] + N[i+1:]);
        newN[i] = gcd(Li, N[i]);
    return tuple(newN[i] for i in range(len(N)));

# Check if N is a set of primitive (reduced) exponents
def primitiveExp(N):
    return reduceExp(N) == N;

#Returns if a diagonal hypersurface with exponent list N is superingular over F_p
def supersingular(N, p):
    if isTrivial(N, p):
        return True;
    r = len(N) - 1;
    n = LCM_list(N);
    f = Mod(p, n).multiplicative_order();
    q = p**f;
    # Create list of tuples {L_0,...L_r} to iterate over
    n_set = [i for i in range(1, n)];
    L0 = Tuples(n_set, r + 1);
    L = [l for l in L0 if (sum(l) % n == 0 and condition(l, N, n, r))];
    # Check condition for each tuple
    value = (r+1)/2 * (p-1) * f;
    for l in L:
        for m in [i for i in range(1, n) if gcd(i, n) == 1]:
            if sum([s(m * l[i] / n, p, f) for i in range(0, r + 1)]) != value:
                return False;
    return True;
```

B. Genus Computation

```
from sage.all import *
from sage.arith.misc import is_prime_power

# Compute the genus of a curve with exponents N if possible, or return -1
def genus(N):
    if primitiveExp(N):
        return 1 + ((N[0]-1) * (N[1]-1) * (N[2]-1) - N[0] - N[1] - N[2] + 1)/(2 * LCM_list(N));
    return -1;

# Give a genus g, return a list of all the primitive exponents of curve with the given genus
def genusExponents(g):
    g_exps = [];
    for a in range(1, 4*g + 1):
        for b in range(a, 4*g + 1):
            for c in divisors(lcm(a, b)):
                if c >= b:
                    N = (a, b, c);
                    if genus(N) == g:
                        g_exps.append(N);
    return g_exps;

# Return the multiplicative group of Z/mZ as a set
def mult(M):
    mult = [];
    for a in range(1, M):
        if gcd(a, M) == 1:
            mult.append(a);
    return mult;

# Reduce the list of N to N/2 if exactly one factor of 2 divides N
def reduce2Factor(Nlist):
    result = [];
    for N in Nlist:
        if N % 2 == 0 and (N/2) % 2 == 1:
            result.append(N/2);
        else:
            result.append(N);
    return result;

# If an N in Nlist is an odd prime power, reduce it to the prime
def reducePrimePower(Nlist):
    result = [];
    for N in Nlist:
        N = ZZ(N);
        t = N.is_prime_power(get_data = True); # returns (p, k) where N = p^k
        if t[1] != 0 and t[0] % 2 == 1:
            result.append(t[0]);
        else:
            result.append(N);
    return result;

# Remove anything from Nlist that is a multiple of something else
def removeMultiples(Nlist):
    result = [];
    for i in range(len(Nlist)):
```

```
        mult = False;
        for j in range(len(Nlist)):
            if i != j and Nlist[i] != Nlist[j] and Nlist[i] % Nlist[j] == 0:
                mult = True;
        if not mult:
            result.append(Nlist[i]);
    return result;


# Reduce the list of congruences we have to check
def reduceNList(Nlist):
    Nlist = reduce2Factor(Nlist);
    Nlist = reducePrimePower(Nlist);
    Nlist = removeMultiples(Nlist);
    return Nlist;


# Given a list of exponents for genus g, compute fraction of primes which are root of -1 mod a Fermat coverit
def rootResidues(g):
    Nlist = [LCM_list(N) for N in genusExponents(g)];
    Nlist = reduceNList(Nlist);
    M = 1;
    for N in Nlist:
        M = lcm(M, N);

    residues = [];

    for a in mult(M):
        for N in Nlist:
            if a not in residues:
                f = Mod(a, N).multiplicative_order();
                if f % 2 == 0 and power_mod(a, f/2, N) == N - 1:
                    residues.append(a);

    return len(residues)/euler_phi(M);
```

C. Genus Density Table

g	$\delta'(g)$	g	$\delta'(g)$	g	$\delta'(g)$
1	3/4	11	39/64	21	97/128
2	7/8	12	61/64	22	39/64
3	3/4	13	21/32	23	17/32
4	7/8	14	101/128	24	225/256
5	5/8	15	217/256	25	9/16
6	31/32	16	127/128	26	57/64
7	9/16	17	11/32	27	61/128
8	31/32	18	57/64	28	7/8
9	47/64	19	41/64	29	37/64
10	3/4	20	235/256	30	3793/4096
31	1153/2048	41	147/256	51	367/512
32	1223/2048	42	?	52	7/8
33	701/1024	43	27/64	53	5/8
34	15/32	44	115/128	54	?
35	19/32	45	?	55	?
36	255/256	46	473/512	56	?
37	141/256	47	29/128	57	1015/2048
38	53/128	48	2023/2048	58	85/128
39	177/256	49	2217/4096	59	39/256
40	15/16	50	1707/2048	60	?
61	139/256	71	345/1024	81	?
62	53/64	72	?	82	1251/2048
63	?	73	267/512	83	151/256
64	21/32	74	833/1024	84	?
65	173/256	75	?	85	?
66	?	76	?	86	13/16
67	1021/2048	77	81/256	87	?
68	119/128	78	?	88	?
69	?	79	65/128	89	41/64
70	?	80	?	90	?

Table 1: Densities of genera g diagonal curves supersingular over $\mathbb{F}_p$. The squares without a value have LCMs of the Fermats too large for our desktop computers to run through in a reasonable time.

References

[Chu+] Benjamin Church et al. Private communications.

[G22] Asvin G. *Supersingularity of Motives with Complex Multiplication and a Twisted Polarization*. 2022. arXiv: 2208.11719 [math.AG].

[Hos20] Timothy Hosgood. *An introduction to varieties in weighted projective space*. 2020. arXiv: 1604.02441 [math.AG].

[KHS20] Momonari Kudo, Shushi Harashita, and Hayato Senda. "The existence of supersingular curves of genus 4 in arbitrary characteristic". In: *Research in Number Theory* 6.4 (2020). DOI: 10.1007/s40993-020-00217-x. URL: https://doi.org/10.1007%2Fs40993-020-00217-x.

[Lan94] S. Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1994. ISBN: 9780387942254. URL: https://books.google.com/books?id=u5eGtA0YalgC.

[SK79] Tetsuji Shioda and Toshiyuki Katsura. "On Fermat varieties". In: *Tohoku Mathematical Journal* 31 (Jan. 1979). DOI: 10.2748/tmj/1178229881.

[Wat84] Waterhouse. "The density of supersingular Fermat varieties". In: *Archiv der Mathematik* 42 (1984), pp. 238–241. DOI: 10.1007/BF01191181.

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