The Supersingularity of Hurwitz Curves

Erin Dawson, Henry Frauenhoff, Michael Lynch, Amethyst Price,
Seamus Somerstep, Eric Work
Graduate Student Advisor: Dean Bisogno
Faculty Advisor: Rachel Pries

July 11, 2021

Abstract

We study when Hurwitz curves are supersingular. Specifically, we show that the curve $H_{n,\ell} : X^nY^\ell + Y^nZ^\ell + Z^nX^\ell = 0$, with n and ℓ relatively prime, is supersingular over the finite field $\mathbb{F}_p$ if and only if there exists an integer i such that $p^i \equiv -1 \bmod (n^2-n\ell+\ell^2)$. If this holds, we prove that it is also true that the curve is maximal over $\mathbb{F}_{p^{2i}}$. Further, we provide a complete table of supersingular Hurwitz curves of genus less than 5 for characteristic less than 37.

Keywords:
Hurwitz Curve, Hasse-Weil Bound, Maximal Curve,
Minimal Curve, Fermat Curve, Supersingular Curve
Subject Classification:
Primary: 11G20, 11M38, 14H37, 14H45, 11E81;
Secondary: 11G10, 14H40, 14K15

1 Introduction

In 1941, Deuring defined the basic theory of supersingular elliptic curves. Supersingular curves are useful in error-correcting codes called Goppa codes. They also have potential applications to quantum resistant cryptosystems.

In this paper we determine a condition for supersingularity of Hurwitz curves $H_{n,\ell}$ when n and ℓ are relatively prime. In particular we show that every supersingular Hurwitz curve $H_{n,\ell}$ is maximal over some finite field. We also provide a classification of supersingular Hurwitz curves with genus less than 5 over fields with characteristic less than 37 and find some restrictions on the genera of Hurwitz curves.

1.1 Acknowledgements

We would like to thank Dr. Rachel Pries for proposing this question and guiding us through our research process. We would also like to thank Dr. Özlem Ejder for all of her help and the referee for helpful comments. Finally, we would like to thank the College of Natural Sciences, the CSU Department of Mathematics, and the National Science Foundation for the REU supplement to DMS-15-02227. Pries was partially supported by NSF grant DMS-15-02227. This project would not be possible without all of you.

2 Background information

We first define the Hurwitz curve and the Fermat curve. Next we define the zeta function of a curve. From the zeta function we compute the normalized Weil numbers which we use to study supersingularity. We must also state the Hasse-Weil bound in order to define maximality and minimality.

2.1 The Hurwitz curve and the Fermat curve

Let n, ℓ, and d be positive integers. Let F be a field.

Definition 2.1 (Hurwitz curve $H_{n,\ell}$). The *Hurwitz curve* $H_{n,\ell}$ over F is given by the projective equation

$$H_{n,\ell} : X^nY^\ell + Y^nZ^\ell + Z^nX^\ell = 0.$$

Throughout this paper, set $m = n^2 - n\ell + \ell^2$. The Hurwitz curve $H_{n,\ell}$ has the following genus

$$g = \frac{m + 2 - 3\gcd(n, \ell)}{2}$$

and is smooth when the characteristic p of F is relatively prime to m.

Definition 2.2 (Fermat curve $\mathcal{F}_d$). The *Fermat curve* of degree d over F is given by the projective equation

$$\mathcal{F}_d : U^d + V^d + W^d = 0.$$

The Fermat curve $\mathcal{F}_d$ has genus $\frac{(d-1)(d-2)}{2}$ and is smooth when the characteristic p of F does not divide d. Note that the Hurwitz curve $H_{n,\ell}$ is covered by the Fermat curve of degree $m = n^2 - n\ell + \ell^2$; see Section 3.2 for more details.

2.2 Zeta Function

Let $\mathbb{F}_q$ be a finite field of cardinality q where q is a power of a prime p. For a curve C defined over $\mathbb{F}_q$, denote the number of points on C by $\#C(\mathbb{F}_q)$. For extensions of $\mathbb{F}_q$, define $N_s = \#C(\mathbb{F}_{q^s})$.

Definition 2.3 (Zeta function). The *zeta function* of a curve $C/\mathbb{F}_q$ is the series

$$Z(C/\mathbb{F}_q, T) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s T^s}{s}\right). \tag{1}$$

Rationality of the zeta function for curves was proven by Weil [Wei48a, Wei49]. In particular, Weil showed that the zeta function can be written as

$$Z(C/\mathbb{F}_q, T) = \frac{L(C/\mathbb{F}_q, T)}{(1-T)(1-qT)}. \tag{2}$$

The L-polynomial, $L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$, has degree $2g$ [IR90, page 152],

$$L(C/\mathbb{F}_q, T) = 1 + C_1 T + ... + C_{2g} T^{2g}. \tag{3}$$

The L-polynomial of a curve C over $\mathbb{F}_q$ with genus g factors in $\mathbb{C}[T]$ as

$$L(C/\mathbb{F}_q, T) = \prod_{i=1}^{2g} (1 - \alpha_i T).$$

Furthermore, $|\alpha_i| = \sqrt{q}$ for each $1 \leq i \leq 2g$ [IR90, page 155]. The normalized Weil numbers (NWNs) are the normalized reciprocal roots of the L-polynomial.

Definition 2.4 (Normalized Weil Numbers). The *Weil numbers* of $C/\mathbb{F}_q$ are the reciprocal roots α_i of $L(C/\mathbb{F}_q, T)$ for $1 \leq i \leq 2g$. The *normalized Weil numbers* are the values $\alpha_i/\sqrt{q}$ for $1 \leq i \leq 2g$.

Remark 2.5. If $\{\alpha_1, \ldots, \alpha_{2g}\}$ are the normalized Weil numbers over $\mathbb{F}_q$, then $\{\alpha_1^i, \ldots, \alpha_{2g}^i\}$ are the normalized Weil numbers over $\mathbb{F}_{q^i}$.

The coefficients of $L(C/\mathbb{F}_q, T)$ follow a pattern. For $k \in \mathbb{N}$, we denote the set of partitions of k by $\text{par}(k)$ and the length of a partition γ by $\text{len}(\gamma)$.

Lemma 2.6. *In Equation (3) for $0 \leq k \leq 2g$, the coefficient C_k has the form*

$$C_k = \sum_{\gamma \in \text{par}(k)} \frac{\prod_{j \in \gamma} \frac{N_j}{j}}{\text{len}(\gamma)!} - \sum_{i=0}^{k-1} (C_i \sum_{\mu=0}^{k-i} q^{\mu}).$$

Proof. Equation (1) can be expanded using the Taylor series of the exponential function

$$Z(C/\mathbb{F}_q, T) = \sum_{i=0}^{\infty} \frac{(N_1 T + \frac{N_2}{2} T^2 + \ldots + \frac{N_{2g}}{2g} T^{2g})^i}{i!}.$$

Collecting terms up through T^3 gives a pattern to follow:

$$Z(C/\mathbb{F}_q, T) = 1 + (N_1)T + \left(\frac{N_2}{2} + \frac{N_1^2}{2}\right)T^2 + \left(\frac{N_3}{3} + \frac{N_1 N_2}{2} + \frac{N_1^3}{6}\right)T^3 + \ldots. \tag{4}$$

The key step is to recognize that the subscripts on the N_j are the partitions of k. The coefficient on T^k can be written as

$$\sum_{\gamma\in \mathrm{par}(k)} \frac{\prod_{j\in\gamma} \frac{N_j}{j}}{\mathrm{len}(\gamma)!}.$$

Equation (2) gives a simplified version of $Z(C/\mathbb{F}_q,T)$. Using the Taylor series for each of the denominator terms as well as equation (3) yields the following expansion:

$$Z(C/\mathbb{F}_q,T) = (1+C_1T+...+C_{2g}T^{2g})(1+T+T^2+\dots)(1+qT+q^2T^2+\dots). \quad (5)$$

Expanding and collecting terms, the coefficients on T^k are given by

$$\sum_{i=0}^{k-1}(C_i\sum_{j=0}^{k-i} q^j) + C_k.$$

Setting equation (4) and equation (5) equal and comparing coefficients gives a linear system allowing one to solve for C_k in terms of the values of N_s. □

2.3 The Newton Polygon and Supersingularity

Fix a curve $C/\mathbb{F}_q$ with associated L-polynomial $L(C/\mathbb{F}_q,T)$.

Definition 2.7 (Supersingularity). The curve C is *supersingular* if all its normalized Weil numbers are roots of unity.

Another way to check if C is supersingular is with its Newton polygon.

Definition 2.8 (Normalized Valuation on $\mathbb{F}_{p^r}$). Let $n = p^l k$ be an integer with $p \nmid k$. We denote the normalized $\mathbb{F}_{p^r}$-valuation of n by $\mathrm{val}_{p^r}(n) = \frac{l}{r}$ and the prime-to-p part of n by $n_p = k$. If $n = 0$, we say $\mathrm{val}_{p^r}(0) = \infty$.

Definition 2.9 (Newton Polygon). Fix a curve $C/\mathbb{F}_{p^r}$ with L-polynomial in the form of equation (3). The *Newton polygon* of $C/\mathbb{F}_{p^r}$ is the lower convex hull of the points $\{(i, \mathrm{val}_{p^r}(C_i)) \mid 0 \le i \le 2g\}$.

Remark 2.10. Because $C_0 = 1$ for every curve $C/\mathbb{F}_{p^r}$, the Newton polygon will always have initial point $(0,0)$. Likewise the final coefficient of $L(C/\mathbb{F}_{p^r},T)$ is always $C_{2g} = p^{rg}$. For this reason the Newton polygon always has terminal point $(2g,g)$.

From Remark 2.10, we can see that the Newton polygon of a curve C over $\mathbb{F}_{p^r}$ is always a union of line segments on or below the line $y = \frac{1}{2}x$ with increasing slopes.

Remark 2.11. A curve $C/\mathbb{F}_q$ is supersingular if and only if its Newton polygon is a line segment with slope $\frac{1}{2}$.

2.4 Minimality and Maximality

As a consequence of the Weil conjectures, the number of points on a curve $C/\mathbb{F}_q$ is controlled by the Hasse-Weil bound:

$$1 + q - 2g\sqrt{q} \leq \#C(\mathbb{F}_q) \leq 1 + q + 2g\sqrt{q}.$$

The Hasse-Weil bound for curves was proven by Weil [Wei48a].

Definition 2.12 (Minimal). A curve $C/\mathbb{F}_q$ is *minimal* if

$$\#C(\mathbb{F}_q) = 1 + q - 2g\sqrt{q}.$$

Definition 2.13 (Maximal). A curve $C/\mathbb{F}_q$ is *maximal* if

$$\#C(\mathbb{F}_q) = 1 + q + 2g\sqrt{q}.$$

Remark 2.14 ([Wei48a, page 22], [Wei48b, page 69]). The curve C is maximal over $\mathbb{F}_q$ (resp. minimal over $\mathbb{F}_q$) if and only if all its normalized Weil numbers are -1 (resp. 1) over $\mathbb{F}_q$.

In the following remark, we use the notation that ζ_k is the primitive k^{th} root of unity $e^{\frac{2\pi i}{k}}$. Notice that there is a power s such that $\zeta_k^s = -1$ if and only if k is even.

Lemma 2.15. *Let C be a supersingular curve over $\mathbb{F}_q$. Suppose the normalized Weil numbers of $C/\mathbb{F}_q$ are of the form $\zeta_{k_1}^{t_1}, \ldots, \zeta_{k_{2g}}^{t_{2g}}$. Assume $\gcd(k_i, t_i) = 1$. The curve C is maximal over $\mathbb{F}_{q^r}$ if and only if*

- *there exists $s \geq 1$ and b_i odd, such that $k_i = 2^s(b_i)$*
- *and r is an odd multiple of $2^{s-1}\mathrm{lcm}(b_1, \ldots, b_n)$.*

Proof. Assume C is maximal over $\mathbb{F}_{q^r}$. By Remark 2.14, the curve C is maximal over $\mathbb{F}_{q^r}$ if and only if $\zeta_{k_i}^{rt_i} = -1$ for all i. Consequently, k_i is even for all i. Thus $k_i = 2^{s_i}b_i$ for some positive integer s_i and odd integer b_i. The condition $\zeta_{k_i}^{rt_i} = -1$ for all i implies that there exists an s such that $s = s_i$ for all i and r is an odd multiple of $2^{s-1}\mathrm{lcm}(b_1, \ldots, b_n)$.

For the converse, the conditions imply that the normalized Weil numbers of C over $\mathbb{F}_{q^r}$ are all -1. □

3 Curve maps and covers

3.1 Aoki's Curve

Let $\alpha = (a, b, c) \in \mathbb{N}^3$ with $a + b + c = m$. Note that S_3, the symmetric group on three letters, acts on α by permuting the coordinates. For $\sigma \in S_3$ we denote the action by α^σ. We say two triples $\alpha = (a_1, a_2, a_3)$ and $\beta = (b_1, b_2, b_3)$ are equivalent, denoted $\alpha \approx \beta$, if there exist elements $t \in (\mathbb{Z}/m)^*$ and $\sigma \in S_3$ such that

$$(a_1, a_2, a_3) \equiv (tb_{\sigma(1)}, tb_{\sigma(2)}, tb_{\sigma(3)}) \bmod m.$$

In [Aok08a] and [Aok08b], Aoki studies curves of the form

$$D_\alpha : v^m = (-1)^c u^a (1-u)^b.$$

He provides the following conditions for when D_α is supersingular.

Theorem 3.1 ([Aok08b, Theorem 1.1]). *The curve D_α is supersingular over $\mathbb{F}_{p^r}$ if and only if at least one of the following conditions holds:*

- $p^i \equiv -1 \bmod m$ *for some i.*
- $\alpha = (a, b, c) \approx (1, -p^i, p^i - 1)$ *for some integer i such that $d = \gcd(p^i - 1, m) > 1$ and $p^j \equiv -1 \bmod \frac{m}{d}$ for some integer j.*

3.2 Covers of $H_{n,\ell}$ by $\mathcal{F}_m$

In Section 2.1, we noted that the Hurwitz curve $H_{n,\ell}$ is covered by the Fermat curve $\mathcal{F}_m$ where $m = n^2 - n\ell + \ell^2$. On an affine patch the Fermat and Hurwitz curves are given by the following equations

$$\begin{aligned} \mathcal{F}_m &: u^m + v^m + 1 = 0 \\ H_{n,l} &: x^n y^\ell + y^n + x^\ell = 0. \end{aligned}$$

Then the following covering map is provided by [AKT01, Lemma 4.1]

$$\begin{aligned} \phi : \mathcal{F}_m &\to H_{n,\ell} \\ (u, v) &\mapsto (u^n v^{-l}, u^l v^{n-l}). \end{aligned}$$

Furthermore, it is known that $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$ if and only if $p^i \equiv -1 \bmod m$ for some integer i [SK79, Prop. 3.10]. See also [Yui80, Theorem 3.5]. In [Taf10, Theorem 5] it is shown that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{p^{2i}}$ if and only if $p^i \equiv -1 \bmod m$.

Remark 3.2. If $X \to Y$ is a covering of curves defined over $\mathbb{F}_{p^r}$, then the normalized Weil numbers of $Y/\mathbb{F}_{p^r}$ are a subset of the normalized Weil numbers of $X/\mathbb{F}_{p^r}$, see [Ser85].

Thus when a covering curve is supersingular (or maximal or minimal) the curve it covers is as well.

3.3 A Birational Transformations

In [BC97], Bennama and Carbonne show that $H_{n,\ell}$ is isomorphic to a curve with affine equation

$$y'^m = x'^\lambda (x'-1) \tag{6}$$

via the following variable change. Suppose $1 \le \ell < n$ and $\gcd(n, \ell) = 1$. Then there exist integers θ and δ such that $1 \le \theta \le \ell$, $1 \le \delta \le n-1$, and $n\theta - \delta\ell = 1$. Let $\lambda = \delta n - \theta(n-\ell)$ and $m = n^2 - n\ell + \ell^2$. The birational transformation is as follows

$$\begin{cases} x = (-x')^{-\delta}((-1)^\lambda y')^n \\ y = (-x')^{-\theta}((-1)^\lambda y')^\ell \end{cases}$$

and

$$\begin{cases} x' = -x^\ell y^{-n} \\ y' = (-1)^\lambda x^\theta y^{-\delta}. \end{cases}$$

Equation (6) is very similar to the equation for D_α that Aoki studies but there are small differences. The following argument shows that these can be reconciled. Consequently, this variable change can be used to apply Aoki's results to Hurwitz curves.

Notice that equation (6) is divisible by $(x'-1)$ while Aoki studies curves whose equation contains a $(1-x')$ factor. Aoki requires that $a+b+c=m$ so the exponent on the negative sign is important. Inspecting equation (6) we see that m will always be odd since $(n, \ell) = 1$. Consequently, this negative sign is not an issue. Since m is always odd we can replace v with $-v$. This choice allows us to pick $c = m - a - b$. Then $b = 1$ and $a = \lambda$.

4 Supersingular Hurwitz Curves

We arrive at explicit conditions on supersingularity for $H_{n,\ell}$ when n and ℓ are relatively prime. We use results from [BC97] and [Aok08a] to accomplish this. We will be using affine equations for the Hurwitz curve in this section.

Lemma 4.1. *If n and ℓ are relatively prime then $x^n y^\ell + y^n + x^\ell = 0$ is supersingular over $\mathbb{F}_p$ if and only if at least one of the following conditions holds.*

1. *There exists $i \in \mathbb{Z}_{>0}$ such that $p^i \equiv -1 \bmod m$.*

   (In this case the Fermat curve covering the Hurwitz curve is maximal over $\mathbb{F}_{p^{2i}}$.)

2. *There exists $i \in \mathbb{Z}_{>0}$ with $d = (p^i - 1, m) > 1$ such that*

   $$(\delta(n-\ell) + \ell\theta - 1, 1, -(\delta(n-\ell) + \ell\theta)) \approx (1, -p^i, p^i - 1)$$

   and $p^j \equiv -1 \bmod (\frac{m}{d})$ for some integer j.

Proof. We use the variable substitution from [BC97] to apply Aoki's results to Hurwitz curves. We use the substitutions:

- $m = n^2 - n\ell + \ell^2$,
- $a = \lambda = \delta(n - \ell) + \ell\theta - 1$,
- $b = 1$,
- $c = m - (\delta(n - \ell) + \ell\theta)$.

Combining these with Aoki's results completes the proof. □

Remark 4.2. If n and ℓ are relatively prime, then n and ℓ are relatively prime to $n^2 - n\ell + \ell^2$.

Theorem 4.3. *Suppose n and ℓ are relatively prime and $m = n^2 - n\ell + \ell^2$. Then $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$ if and only if $p^i \equiv -1 \bmod m$ for some positive integer i.*

Proof. If $p^i \equiv -1 \bmod m$ for some positive integer i, then $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$ by [SK79, Prop. 3.10]. Recall from section 3.2 that $\mathcal{F}_m$ covers $H_{n,\ell}$. Thus $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$ by Remark 3.2.

Suppose $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$. By Lemma 4.1 it is enough to show condition 2 in Lemma 4.1 can not happen. We begin by simplifying it using the substitution $\theta = \frac{1+\ell\delta}{n}$ and reducing modulo m to show that condition 2 is equivalent to $(\frac{\ell}{n} - 1, 1, -\frac{\ell}{n}) \approx (1, -p^i, p^i - 1)$ for some i such that $d = (p^i - 1, m) > 1$ and $p^j \equiv -1 \mod (\frac{m}{d})$ for some integer j. Recall that $\alpha \approx \alpha'$ if $\alpha = t\alpha'^{\sigma}$ for some $t \in (\mathbb{Z}/m)^*$ and $\sigma \in S_3$. We will show that $p^i - 1$ and m are relatively prime. We label the three coordinates of $(\frac{\ell}{n} - 1, 1, -\frac{\ell}{n})$ as (a, b, c) and the three coordinates of $(1, -p^i, p^i - 1)$ as (A, B, C).

The proof will address six cases accounting for the orbit of (A, B, C) under the action of S_3. In each case we will show that $\gcd(p^i - 1, m) = 1$. Specifically, we show $d = 1$ by taking these congruences modulo d. By Remark 4.2 we know that n^{-1} exists modulo m and modulo d. Finally, note that $\frac{\ell}{n}$ is relatively prime to d.

- $(a, b, c) \equiv t(A, B, C) \bmod m$: Comparing c and tC yields
$$-\frac{\ell}{n} \equiv t(p^i - 1) \bmod m.$$
Consequently, $\frac{\ell}{n} \equiv 0 \bmod d$. Therefore, $d = 1$.
- $(a, b, c) \equiv t(B, A, C) \bmod m$: Comparing a with tB and b with tA yields
$$\frac{\ell}{n} - 1 \equiv -tp^i \bmod m$$
$$1 \equiv t \bmod m.$$
Substituting we have $\frac{\ell}{n} \equiv p^i - 1 \bmod m$. Reducing modulo d produces $\frac{\ell}{n} \equiv 0 \bmod d$, thus $d = 1$.

- $(a,b,c) \equiv t(A,C,B) \bmod m$: Comparing b and tC yields

$$-\frac{\ell}{n} \equiv t(p^i - 1) \bmod m.$$

This is identical to the first case.

- $(a,b,c) \equiv t(C,B,A) \bmod m$: Comparing a and tC yields

$$\frac{\ell}{n} - 1 \equiv t(p^i - 1) \bmod m.$$

Thus $\frac{\ell}{n} - 1 \equiv 0 \bmod d$. Recall by the definition of m and selection of d, we have $d \mid n^2 - n\ell + \ell^2$. Hence, d divides $1 - \frac{\ell}{n} + (\frac{\ell}{n})^2$. We conclude $d|(\frac{\ell}{n})$, thus $d = 1$.

- $(a,b,c) \equiv t(C,A,B) \bmod m$: Comparing b with tA and c with tB yields

$$1 \equiv t \bmod m$$
$$\frac{\ell}{n} \equiv tp^i \bmod m.$$

This case is completed as in the previous case.

- $(a,b,c) \equiv t(B,C,A) \bmod m$: Comparing b with tC yields

$$1 \equiv t(p^i - 1) \bmod m.$$

Modulo d this reduces to $1 \equiv 0 \bmod d$. Therefore, $d = 1$.

□

Remark 4.4. There is a family of Hurwitz type curves with affine equations $\mathcal{C}_{a_1,a_2,n_1,n_2} : x^{n_1}y^{a_1} + y^{n_2} + x^{a_2} = 0$. Set $\delta = a_1a_2 - a_2n_2 + n_1n_2$. When $q = p^r$ is coprime to δ then the curve C_{a_1,a_2,n_1,n_2} is $\mathbb{F}_q$-covered by the Fermat curve $\mathcal{F}_\delta$ of degree δ. In [TT17, Theorem 2.9] Tafazolian and Torres show that under certain numerical conditions the statements

- the Fermat curve $\mathcal{F}_\delta$ is maximal over $\mathbb{F}_{q^2}$;
- the Hurwitz type curve $\mathcal{C}_{1,a_2,n_1,n_2}$ is maximal over $\mathbb{F}_{q^2}$;
- and $q + 1 \equiv 0 \mod \delta$

are all equivalent.

The Hurwitz type curve $\mathcal{C}_{\ell,\ell,n,n}$ is the Hurwitz curve $H_{n,\ell}$. Thus in the case that $\ell = a_1 = a_2$ and $n = n_1 = n_2$, Theorem 4.3 generalizes [TT17, Theorem 2.9].

Remark 4.5. Consider the family of curves with affine equations

$$N_{a_1,a_2,n_1,n_2} : x^{n_1}y^{a_1} + k_1y^{n_2} + k_2x^{a_2} = 0$$

over $\mathbb{F}_{p^r}$ with $k_1, k_2 \in (\mathbb{F}_q)^*$, $n_1 \geq a_1$, $n_1 + a_1 > a_2$, $n_1 + a_1 > n_2$, if $n_1 = a_1$ then $n_2 \geq a_2$, and $p \nmid \gcd(a_1, a_2, n_1, n_2)$. Set $d = \gcd(a_1, a_2, n_1, n_2)$ and δ as in Remark 4.4. Recall the definition of n_p in Definition 2.8. With these assumptions [Nie16, Theorem 4.12] shows that if $(\delta/d)_p$ divides $q + 1$ then N_{a_1,a_2,n_1,n_2} is maximal over $\mathbb{F}_q$ and if N_{a_1,a_2,n_1,n_2} is maximal over $\mathbb{F}_{q^2}$ then $(\delta/d)_p$ divides $q^2 + 1$.

Note $N_{\ell,\ell,n,n} = H_{n,\ell}$. Thus Theorem 4.3 generalizes [Nie16, Theorem 4.12] when $a_1 = a_2 = \ell$ and $n_1 = n_2 = n$.

Corollary 4.6. *If n and ℓ are relatively prime and $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then it will be maximal over $\mathbb{F}_{p^{2i}}$ where i is the same as in Theorem 4.3.*

Proof. By Theorem 4.3, if $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then $p^i \equiv -1 \bmod m$ for some i. By the results of [Taf10], this implies $\mathcal{F}_m$ will be maximal over $\mathbb{F}_{p^{2i}}$. Since $\mathcal{F}_m$ covers $H_{n,\ell}$, this implies $H_{n,\ell}$ will also be maximal over $\mathbb{F}_{p^{2i}}$. □

A priori, if $H_{n,\ell}$ is supersingular (or maximal or minimal) over $\mathbb{F}_p$ then $\mathcal{F}_m$ may not be because it has more normalized Weil numbers.

Corollary 4.7. *If n and ℓ are relatively prime and $H_{n,\ell}$ is supersingular over $\mathbb{F}_p$, then $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$.*

Proof. If $H_{n,\ell}$ supersingular over $\mathbb{F}_p$ and $\gcd(n, \ell) = 1$, Theorem 4.3 shows the existence of positive integer i such that $p^i \equiv -1 \bmod m$. Then by [SK79, Proposition 3.10], $\mathcal{F}_m$ is supersingular over $\mathbb{F}_p$. □

Partial results are known for when a Hurwitz curve is maximal.

Theorem 4.8 ([AKT01, Theorem 3.1])**.** *Let $\ell = 1$. The curve $H_{n,1}$ is maximal over $\mathbb{F}_{q^{2j}}$ if and only if $p^j \equiv -1 \bmod m$ for some positive integer j.*

Theorem 4.9 ([AKT01, Theorem 4.5])**.** *Assume that $\gcd(n, \ell) = 1$ and m is prime. Then $H_{n,\ell}$ is maximal over $\mathbb{F}_{p^{2j}}$ if and only if $p^j \equiv -1 \bmod m$ for some positive integer j.*

Note that the key property used in [AKT01] is the existence of some positive integer j such that

$$p^j \equiv -1 \bmod m. \tag{7}$$

Remark 4.10. Under the requirements $\ell = 1$, or $\gcd(n, \ell) = 1$ and m prime, the results in [AKT01] and [Taf10, Theorem 5] show that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{q^2}$ if and only if $H_{n,\ell}$ is maximal over $\mathbb{F}_{q^2}$.

We consider the case when $H_{n,\ell}$ and $\mathcal{F}_m$ are minimal.

Corollary 4.11. *If $\ell = 1$, or n and ℓ are relatively prime and m is prime, $H_{n,\ell}$ is minimal over $\mathbb{F}_{p^{4i}}$ if and only if $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4i}}$.*

Proof. First suppose $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4i}}$ with set N of normalized Weil numbers. Then the normalized Weil numbers of $H_{n,\ell}$ are a subset of N. Thus $H_{n,\ell}$ will also be minimal over $\mathbb{F}_{p^{4i}}$.

Now assume $H_{n,\ell}$ is minimal over $\mathbb{F}_{p^{4i}}$. Minimality implies supersingularity, thus $H_{n,\ell}$ must also be supersingular. By Theorem 4.3 supersingularity of $H_{n,\ell}$ over $\mathbb{F}_p$ implies $p^j \equiv -1 \bmod m$ for some positive integer j. Choose a minimal such j. Then Corollary 4.6 shows $H_{n,\ell}$ is maximal over $\mathbb{F}_{p^{2j}}$ thus minimal over $\mathbb{F}_{p^{4j}}$. Minimality of j implies that $\mathbb{F}_{p^{4j}}$ is a subfield of $\mathbb{F}_{p^{4i}}$. Consequently, $j \mid i$.

Now, by [AKT01] $p^j \equiv -1 \bmod m$ implies that $\mathcal{F}_m$ is maximal over $\mathbb{F}_{p^{2j}}$. Hence, $\mathcal{F}_m$ is minimal over $\mathbb{F}_{p^{4j}}$. Because $j \mid i$, $\mathcal{F}_m$ is minimal over $\mathcal{F}_{p^{4i}}$. □

Remark 4.12. The curve $H_{3,3}$ is maximal over $\mathbb{F}_{5^2}$ but $\mathcal{F}_9$ is not. The above theorems show a supersingular Hurwitz curve and its covering Fermat curve will both be maximal over $\mathbb{F}_{p^{2i}}$. This does not imply that the Fermat curve will always be maximal over the same field extension that the Hurwitz curve is. The Hurwitz curve could also be maximal over $\mathbb{F}_{p^{2j}}$ where $j \mid i$ with i/j odd. In this case the Fermat curve may not be maximal over this field because it has a higher genus. Unfortunately our example of this does not have n and ℓ being relatively prime. It is difficult to find an example with n and ℓ relatively prime, as the genera of Hurwitz curves grow quickly causing the point counts to become computationally expensive.

$$\begin{tikzcd}
\mathcal{F}_m \text{ s.s.}/\mathbb{F}_p \arrow[r, shift left, "{[\text{Taf10}]}"] \arrow[d, shift right, "{[\text{Ser85}]}"'] \arrow[rr, bend left, dotted, <->] & \mathcal{F}_m \text{ max}/\mathbb{F}_{q^2} \arrow[l, shift left] \arrow[r] \arrow[d, shift right, "{[\text{Ser85}]}"'] & \mathcal{F}_m \text{ min}/\mathbb{F}_{q^4} \arrow[d, shift right, "{[\text{Ser85}]}"'] \\
H_{n,\ell} \text{ s.s.}/\mathbb{F}_p \arrow[u, shift right, "\text{Corollary 4.7}"'] \arrow[r, shift right, "\text{Corollary 4.6}"'] \arrow[rr, bend right, dotted, <->] & H_{n,\ell} \text{ max}/\mathbb{F}_{q^2} \arrow[l, shift right] \arrow[r] \arrow[u, shift right, dotted, "{[\text{AKT01}]}"'] & H_{n,\ell} \text{ min}/\mathbb{F}_{q^4} \arrow[u, shift right, dotted, "\text{Corollary 4.11}"']
\end{tikzcd}$$

Figure 1: Current results regarding supersingularity, minimality, and maximality of Hurwitz and Fermat curves.

Figure 1 illustrates how the current theory fits together. The straight, dotted arrows are under the conditions $\ell = 1$, or $\gcd(n, \ell) = 1$ and m prime. The notation max/$\mathbb{F}_{q^2}$ means, for some power q of p, the curve is maximal over $\mathbb{F}_{q^2}$. If a curve is maximal over $\mathbb{F}_{q^2}$ then it is minimal over $\mathbb{F}_{q^4}$. The curved arrows show that under appropriate conditions a Hurwitz or Fermat curve is supersingular if and only if it is minimal over some field extension. Corollaries 4.6 and 4.7 are under the condition that $\gcd(n, \ell) = 1$, while [AKT01] and Corollary 4.11 are under the condition that $\ell = 1$, or $\gcd(n, \ell) = 1$ and m is prime.

5 Which Genera Occur and Data

Here we provide information about which genera occur for Hurwitz curves and provide a classification of supersingular Hurwitz curves having genus less than 5 defined over $\mathbb{F}_p$ when $p < 37$.

Recall that the genus of the Hurwitz curve $H_{n,\ell}$ has the following equation

$$g = \frac{n^2 - n\ell + \ell^2 - 3\gcd(n, \ell) + 2}{2}.$$

From this, it can be seen that the genus is determined by the quadratic form $q(x, y) = x^2 - xy + y^2$ and $\gcd(x, y)$. In this section, we provide information about which genera can appear as a result of these equations.

Theorem 5.1 ([Fer99, Vol. II, pages 310-314])**.** *The equation $m = x^2 - xy + y^2$ has solutions $x, y \in \mathbb{Z}$ if and only if for every prime p in the prime decomposition of m, either $p \equiv 0, 1 \bmod 3$ or p is raised to an even power.*

There is no restriction in Theorem 5.1 on what the values x and y are. However, for Hurwitz curves we require n and ℓ to be positive. The question remains as to when the equation $m = q(x, y)$ has solutions in the positive integers. To solve this we study the following automorphisms of $q(x, y) = m$.

$$\begin{cases} f: \ \mathbb{Z}^2 \to \mathbb{Z}^2 \mid f(x, y) \mapsto (y, x) \\ g: \ \mathbb{Z}^2 \to \mathbb{Z}^2 \mid g(x, y) \mapsto (-x, -y) \\ \varphi: \ \mathbb{Z}^2 \to \mathbb{Z}^2 \mid \varphi(x, y) \mapsto (x, x - y) \\ I: \ \mathbb{Z}^2 \to \mathbb{Z}^2 \mid I(x, y) \mapsto (x, y) \end{cases}$$

To see that $\varphi(x, y)$ is an automorphism, compute the following

$$\begin{aligned} q \circ \varphi(x, y) &= x^2 - x(x - y) + (x - y)^2 \\ &= x^2 - x^2 + xy + x^2 - 2xy + y^2 \\ &= x^2 - xy + y^2 \\ &= q(x, y). \end{aligned}$$

Corollary 5.2. *If the equation $m = q(x, y)$ has a solution $(x, y) \in \mathbb{Z}^2$ then there is a solution with $(x', y') \in \mathbb{N}^2$.*

Proof. We separate into cases, depending on the values of x and y.

1. If both x and y are negative, then $g(x, y) = (-x, -y) \in \mathbb{N}^2$.

2. If y negative and x positive, then $\varphi(x, y) = (x, x - y) \in \mathbb{N}^2$.

3. If x negative and y positive, then $\varphi(f(x,y)) = (y, y-x) \in \mathbb{N}^2$.
4. If x is 0, then $\varphi \circ f(0,y) = (y,y)$ and if y is 0, then $\varphi(y,0) = (y,y)$.

□

By counting points and using Lemma 2.6 we computed, using [Sag16], the L-polynomials and normalized Weil numbers of many supersingular Hurwitz curves over $\mathbb{F}_p$. When n and ℓ are not relatively prime, it is possible that certain points of the equation for $H_{n,\ell}$ are singular. Resolving these singularities requires taking a field extension of $\mathbb{F}_p$. To adjust for this we check if $q \equiv 1 \bmod \gcd(n,\ell)$ and count the multiplicities of singular points. This gives the correct point counts to compute the L-polynomial of the normalization of the equation. The table has all supersingular Hurwitz curves $H_{n,\ell}$ of genus less than 5 for primes less than 37. The table also includes some curves of genus 6.

n	**l**	**p**	**g**	**L-Polynomial**	**NWNs (multiplicity)**
2	1	5	1	$5T^2+1$	i, -i
2	1	11	1	$11T^2+1$	i, -i
2	1	17	1	$17T^2+1$	i, -i
2	1	23	1	$23T^2+1$	i, -i
2	1	29	1	$29T^2+1$	i, -i
3	3	5	1	$5T^2+1$	i, -i
3	3	11	1	$11T^2+1$	i, -i
3	3	17	1	$17T^2+1$	i, -i
3	3	23	1	$23T^2+1$	i, -i
3	3	29	1	$29T^2+1$	i, -i
3	1	3	3	$27T^6+1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	5	3	$125T^6+1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	13	3	$2197T^6+507T^4+39T^2+1$	i(3), -i(3)
3	1	17	3	$4913T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	19	3	$6859T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	1	31	3	$29791T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	3	3	$27T^6+1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	5	3	$125T^6+1$	i,-i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	13	3	$2197T^6+507T^4+39T^2+1$	i(3), -i(3)
3	2	17	3	$4913T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	19	3	$6859T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
3	2	31	3	$29791T^6+1$	i, -i, $\zeta_{12}, \zeta_{12}^5, \zeta_{12}^7, \zeta_{12}^{11}$
4	2	5	4	$625T^8+500T^6+150T^4+20T^2+1$	i(4), -i(4)
4	2	17	4	$83521T^8+19652T^6+1734T^4+68T^2+1$	i(4), -i(4)
4	2	29	4	$707281T^8+97556T^6+5046T^4+116T^2+1$	i(4), -i(4)
4	1	5	6	$15625T^{12}+1875T^8+75T^4+1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
4	3	5	6	$15625T^{12}+1875T^8+75T^4+1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	3	6	$729T^{12}+243T^8+27T^4+1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	7	6	$117649T^{12}+7203T^8+147T^4+1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$
5	5	13	6	$4826809T^{12}+85683T^8+507T^4+1$	$\zeta_8(3), \zeta_8^3(3), \zeta_8^5(3), \zeta_8^7(3)$

Table 1: Supersingular Hurwitz curves in characteristic $p < 37$ with genus < 5.

References

[AKT01] Angela Aguglia, Gábor Korchmáros, and Fernando Torres. Plane maximal curves. *Acta Arith.*, 98(2):165–179, 2001.

[Aok08a] Noboru Aoki. On supersingular cyclic quotients of Fermat curves. *Comment. Math. Univ. St. Pauli*, 57(1):65–90, 2008.

[Aok08b] Noboru Aoki. On the zeta function of some cyclic quotients of Fermat curves. *Comment. Math. Univ. St. Pauli*, 57(2):163–185, 2008.

[BC97] H. Bennama and P. Carbonne. Courbes $X^mY^n+Y^mZ^n+Z^mX^n=0$ et décomposition de la jacobienne. *J. Algebra*, 188(2):409–417, 1997.

[Fer99] Pierre Fermat. *Œuvres de Pierre Fermat. I.* Collection Sciences dans l'Histoire. [Science in History Collection]. Librairie Scientifique et Technique Albert Blanchard, Paris, 1999. La théorie des nombres. [Number theory], Translated by Paul Tannery, With an introduction and commentary by R. Rashed, Ch. Houzel and G. Christol.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1990.

[Nie16] Menglong Nie. Zeta functions of trinomial curves and maximal curves. *Finite Fields Appl.*, 39:52–82, 2016.

[Sag16] Inc. SageMath. *CoCalc Collaborative Computation Online*, 2016.

[Ser85] Jean Pierre Serre. Rational points on curves over finite fields. unpublished notes by F.Q. Gouvêa of lectures at Harvard Univ., 1985.

[SK79] Tetsuji Shioda and Toshiyuki Katsura. On Fermat varieties. *Tôhoku Math. J. (2)*, 31(1):97–115, 1979.

[Taf10] Saeed Tafazolian. A characterization of maximal and minimal Fermat curves. *Finite Fields Appl.*, 16(1):1–3, 2010.

[TT17] Saeed Tafazolian and Fernando Torres. A note on certain maximal curves. *Comm. Algebra*, 45(2):764–773, 2017.

[Wei48a] André Weil. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945). Hermann et Cie., Paris, 1948.

[Wei48b] André Weil. *Variétés abéliennes et courbes algébriques.* Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949.

[Yui80] Noriko Yui. On the Jacobian variety of the Fermat curve. *J. Algebra*, 65(1):1–35, 1980.