Abstract

We study when Hurwitz curves are supersingular. Specifically, we show that the curve $H_{n,\ell}: X^n Y^\ell + Y^n Z^\ell + Z^n X^\ell = 0$, with $n$ and $\ell$ relatively prime, is supersingular over the finite field $\mathbb{F}_p$ if and only if there exists an integer $i$ such that $p^i \equiv -1 \mod (n^2 - n\ell + \ell^2)$. If this holds, we prove that it is also true that the curve is maximal over $\mathbb{F}_{p^2}$. 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

The first supersingular curves found were supersingular elliptic curves. Hasse noticed that some elliptic curves in positive characteristic had endomorphism rings of rank four. 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 $\ell$ 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 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. 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

Let $n$ and $\ell$ be positive integers. The Hurwitz curve is given by the projective equation

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

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

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

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

2.2 The Fermat Curve

The Fermat curve of degree $d$ is given by the projective equation

$$F_d : U^d + V^d + W^d = 0.$$ 

It has genus $\frac{(d-1)(d-2)}{2}$ and is smooth when the characteristic $p$ of the field 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 4.2 for more details.

2.3 Zeta Function

For a curve $C$ defined over a field $\mathbb{F}_q$, denote the number of points on $C$ by $\#C(\mathbb{F}_q)$. For extensions of $\mathbb{F}_q$ define $N_s = \#C(\mathbb{F}_q^s)$. The zeta function of a curve $C/\mathbb{F}_q$ is the series

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

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

(2)

The \( L \)-polynomial, \( L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T] \), is of degree \( 2g \) [IR90, p152],

\[ L(C/\mathbb{F}_q, T) = 1 + C_1 T + \ldots + C_{2g} T^{2g}. \]  

(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, pg. 155]. The coefficients of \( L(C/\mathbb{F}_q, T) \) follow a pattern.

**Lemma 2.1.** In Equation (3) for \( 0 \leq k \leq 2g \), the coefficient \( C_k \) has the form

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

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

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

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

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

(4)

The key step is to recognize the subscripts on the \( N_j \) are the partitions of \( k \). Therefore, the coefficient on \( T^k \) can be written as

\[ \sum_{\gamma \in \text{par}(k)} \frac{\prod_{j \in \gamma} N_j}{\prod_{j \in \gamma} \text{len}(\gamma)!} \]

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) results in the following expansion:

\[ Z(C/\mathbb{F}_q, T) = (1 + C_1 T + \ldots + C_{2g} T^{2g})(1 + T + T^2 + \ldots)(1 + qT + q^2 T^2 + \ldots). \]  

(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 $N_s$.

### 2.4 The Newton Polygon and Supersingularity

Fix a curve $C/\mathbb{F}_q$ with associated $L$-polynomial $L(C/\mathbb{F}_q, T)$. We can verify whether $C/\mathbb{F}_q$ is supersingular by computing its Newton polygon. A couple definitions are required.

**Definition 2.2 (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 $\text{val}_{p^r}(n) = \frac{l}{r}$. If $n = 0$ we say $\text{val}_{p^r}(0) = \infty$.

**Definition 2.3 (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, $\text{val}_{p^r}(C_i)) \mid 0 \leq i \leq 2g\}.

**Remark 2.4.** 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 2.4 we can see that the Newton polygon of a curve $C$ over $\mathbb{F}_{p^r}$ will always be a union of line segments on or below the line $y = \frac{1}{2}x$ with increasing slopes. A curve is supersingular when its Newton polygon is the line segment from $(0, 0)$ to $(2g, g)$.

**Definition 2.5 (Supersingularity).** A curve $C/\mathbb{F}_q$ is supersingular if its Newton polygon is a line segment with slope $\frac{1}{2}$.

### 2.5 Normalized Weil Numbers

The normalized Weil numbers (NWNs) are normalized reciprocal roots of the $L$-polynomial.

**Definition 2.6 (Normalized Weil Numbers).** The Weil numbers of $C/\mathbb{F}_q$ are the reciprocal roots $\alpha_i$ 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 2.7.** The curve $C$ is supersingular if and only if all NWNs are roots of unity.

**Remark 2.8.** If $\{\alpha_1, \ldots, \alpha_{2g}\}$ are the NWNs over $\mathbb{F}_q$, then $\{\alpha_1^q, \ldots, \alpha_{2g}^q\}$ are the NWNs over $\mathbb{F}_{q'}$. 

4
2.6 Minimality and Maximality

Minimality or maximality of a curve $C / \mathbb{F}_q$ is determined by the Hasse-Weil bound

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

The curve is called minimal over $\mathbb{F}_q$ if its point count is equal to the lower bound and maximal if the point count is equal to the upper bound. If a curve is minimal or maximal over a field, it is also supersingular.

**Remark 2.9.** The curve $C$ is maximal over $\mathbb{F}_q$ (resp. minimal over $\mathbb{F}_q$) if and only if all its NWNs are $-1$ (resp. $1$) over $\mathbb{F}_q$.

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

**Remark 2.10.** Let $C$ be a supersingular curve over $\mathbb{F}_q$. Suppose the NWNs of $C / \mathbb{F}_q$ are of the form $\zeta_k^{t_1}, \ldots, \zeta_k^{t_2}$. 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 $2^{s-1}\text{lcm}(b_1, \ldots, b_n)$.

**Proof.** Assume $C$ is maximal over $\mathbb{F}_{q^r}$. The curve $C$ is maximal over $\mathbb{F}_{q^r}$ if and only if $\zeta_k^{t_i} = -1$ 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 $\zeta_k^{t_i} = -1$ for all $i$ implies that there exists an $s$ such that $s = s_i$ for all $i$ and $r$ is an odd multiple of $2^{s-1}\text{lcm}(b_1, \ldots, b_n)$.

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

3 Which Genera Occur

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 $\gcd(x, y)$. One might ask which genera can appear? Or, if we are given a genus of a supersingular Hurwitz curve, can we determine possibilities for $x$ and $y$? In this section we will provide information about which genera can appear as a result of these equations.

**Lemma 3.1.** Suppose we have two integers, $m$ and $n$, representable by $q(x, y)$ over $\mathbb{Z}$, then $mn$ is also representable by $q(x, y)$ over $\mathbb{Z}$.
Proof. We can factor \( x^2 - xy + y^2 \) over \( \mathbb{Q}(\sqrt{-3}) \) in the following way
\[
x^2 - xy + y^2 = (x - y\zeta_6)(x - y\overline{\zeta_6}).
\]

Note that \( \zeta_6 = \frac{1 + \sqrt{-3}}{2} \) and \( \zeta_6 + \overline{\zeta_6} = 1 \). Now, by the assumption that \( m \) and \( n \) are representable by \( q(x, y) \), there exist \( a, b, c, d \in \mathbb{Z} \) such that \( q(a, b) = m \) and \( q(c, d) = n \). This means that \( m = (a - b\zeta_6)(a - b\overline{\zeta_6}) \) and \( n = (c - d\zeta_6)(c - d\overline{\zeta_6}) \).

Taking their product yields
\[
mn = (a - b\zeta_6)(a - b\overline{\zeta_6})(c - d\zeta_6)(c - d\overline{\zeta_6}).
\]

Multiplying the terms with \( \zeta_6 \) together, and the terms with \( \overline{\zeta_6} \) together, we get
\[
mn = (ac - (ad + bc)\zeta_6 + bd\zeta_6^2)(ac - (ad + bc)\overline{\zeta_6} + bd\overline{\zeta_6}^2).
\]

Using the identity \( \zeta_6^2 = \zeta_6 - 1 \), and that \( \zeta_6^5 = \overline{\zeta_6} \), we can simplify the previous expression to
\[
mn = ((ac - bd) - (ad + bc - bd)\zeta_6)((ac - bd) - (ad + bc - bd)\overline{\zeta_6}).
\]

This equation has the same form as the ones we started with, and so we can see that \( (ac - bd, ad - bc + bd) \) is a solution to \( q(x, y) = mn \), and since \( a, b, c, d \in \mathbb{Z} \), we have \( (ac - bd, ad - bc - bd) \in \mathbb{Z}^2 \).

From this we can make an important statement about which numbers can be a result of this quadratic form. This ultimately relates back to our question about which genera can appear for a Hurwitz curve.

**Theorem 3.2** ([Fer99, Vol. II, pp. 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 \( p \equiv 0, 1 \mod 3 \) or \( p \) is raised to an even power.*

*Proof.* This is the key idea of the proof. Let \( p \neq 3 \) be a prime. Then \( p \equiv 1 \mod 3 \) if and only if \( \sqrt{-3} \) is a square in \( \mathbb{F}_p \). This occurs if and only if \( p \) factors in \( \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_6) \) which is true if and only if \( p = x^2 - xy + y^2 \) has a solution for \( (x, y) \in \mathbb{Z}^2 \).

There is no restriction in Theorem 3.2 on what the values \( x \) and \( y \) are. However, for Hurwitz curves we require \( n \) and \( \ell \) 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 \( q(x, y) = m \).

\[
\begin{align*}
f : \mathbb{Z}^2 &\to \mathbb{Z}^2 \mid f(x, y) \mapsto (y, x) \\
g : \mathbb{Z}^2 &\to \mathbb{Z}^2 \mid g(x, y) \mapsto (-x, -y) \\
\phi : \mathbb{Z}^2 &\to \mathbb{Z}^2 \mid \phi(x, y) \mapsto (x, x - y) \\
I : \mathbb{Z}^2 &\to \mathbb{Z}^2 \mid I(x, y) \mapsto (x, y)
\end{align*}
\]
To see that $\varphi(x, y)$ is an automorphism, compute the following
\[ q \circ \varphi(x, y) = x^2 - x(x - y) + (x - y)^2 \]
\[ = x^2 - xy + x^2 - 2xy + y^2 \]
\[ = x^2 - xy + y^2 \]
\[ = q(x, y). \]

**Corollary 3.3.** If the equation $m = q(x, y)$ has 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 $\varphi(y, 0) = (y, y)$.

\[ \square \]

## 4 Curve maps and covers

### 4.1 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 $\alpha$ by permuting the coordinates. For $\sigma \in S_3$ we denote the action by $\alpha^\sigma$. 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
\[(a_1, a_2, a_3) \equiv (tb_{\sigma(1)}, tb_{\sigma(2)}, tb_{\sigma(3)}) \mod m.\]

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 $D_\alpha$ is supersingular.

**Theorem 4.1** ([Aok08b, Theorem 1.1]). The curve $D_\alpha$ is supersingular over $\mathbb{F}_{p^r}$ if and only if at least one of the following conditions holds:

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

7
4.2 Covers of $H_{n,\ell}$ by $F_m$

In Section 2.2, we noted that the Hurwitz curve $H_{n,\ell}$ is covered by the Fermat curve $F_m$ where $m = n^2 - n\ell + \ell^2$. On an affine patch the Fermat and Hurwitz curves are given by the following equations

$$F_m : u^m + v^m + 1 = 0$$
$$H_{n,\ell} : x^n y^\ell + y^n + x^\ell = 0.$$

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

$$\phi : F_m \rightarrow H_{n,\ell}$$
$$(u, v) \rightarrow (u^n v^{-\ell}, u^\ell v^{n-\ell}).$$

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

**Remark 4.2.** If $X \rightarrow Y$ is a covering of curves defined over $\mathbb{F}_{p^r}$, then the NWNs of $Y/\mathbb{F}_{p^r}$ are a subset of the NWNs of $X/\mathbb{F}_{p^r}$, see [Ser85].

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

4.3 A Birational Transformations

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

$$y^m = x^\lambda (x'^\ell - 1)$$

via the following variable change. Suppose $1 \leq \ell < n$ and $\gcd(n, \ell) = 1$. Then there exist integers $\theta$ and $\delta$ such that $1 \leq \theta \leq \ell$, $1 \leq \delta \leq n-1$, 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

$$\begin{cases} x' = -x't^\delta y^{-n} \\ y' = (-1)^\lambda x^\theta y^{-\delta}. \end{cases}$$

Equation (6) is very similar to the equation for $D_\alpha$ 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 \(a = \lambda\).

5 Supersingular Hurwitz Curves

We arrive at explicit conditions on supersingularity for \(H_{n, \ell}\) when \(n\) and \(\ell\) 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 5.1. If \(n\) and \(\ell\) 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 \(p^i \equiv -1 \mod m\).
   (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 \(p^i \equiv -1 \mod \left(\frac{m}{d}\right)\) 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 5.2. If \(n\) and \(\ell\) are relatively prime, then \(n\) and \(\ell\) are relatively prime to \(n^2 - n \ell + \ell^2\).

Theorem 5.3. Suppose \(n\) and \(\ell\) 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 \(p^i \equiv -1 \mod m\) for some positive integer \(i\).

Proof. If \(p^i \equiv -1 \mod m\) for some positive integer \(i\), then \(F_m\) is supersingular over \(\mathbb{F}_p\) by [SK79, Prop. 3.10]. Recall from section 4.2 that \(F_m\) covers \(H_{n, \ell}\), thus \(H_{n, \ell}\) is supersingular over \(\mathbb{F}_p\).
Suppose \( H_{n, \ell} \) is supersingular over \( \mathbb{F}_p \). By Lemma 5.1 it is enough to show condition 2 in Lemma 5.1 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 \( \left( \frac{\ell}{n} - 1, 1, -\frac{\ell}{n} \right) \approx (1, -p^i, p^i - 1) \) for some \( i \) such that \( d = (p^i - 1, m) > 1 \) and \( p^i \equiv -1 \mod \left( \frac{m}{d} \right) \) 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 \( (\ell n - 1, 1, -\frac{\ell}{n}) \) 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 5.2 we know that \( n^{-1} \) exists modulo \( m \) and modulo \( d \). Finally, note that \( \frac{\ell}{n} \) is relatively prime to \( d \).

- \((a, b, c) \equiv t(A, B, C) \mod m\): Comparing \( c \) and \( tC \) yields
  \[-\frac{\ell}{n} \equiv t(p^i - 1) \mod m.\]
  Consequently, \( \frac{\ell}{n} \equiv 0 \mod d \). Therefore, \( d = 1 \).

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

- \((a, b, c) \equiv t(A, C, B) \mod m\): Comparing \( b \) and \( tC \) yields
  \[-\frac{\ell}{n} \equiv t(p^i - 1) \mod m.\]
  This is identical to the first case.

- \((a, b, c) \equiv t(C, B, A) \mod m\): Comparing \( a \) and \( tC \) yields
  \[-\frac{\ell}{n} \equiv t(p^i - 1) \mod m.\]
  Thus \( \frac{\ell}{n} - 1 \equiv 0 \mod d \). Recall by the definition of \( m \) and selection of \( d \), we have \( d \mid n^2 - n\ell + \ell^2 \). Hence, \( d \) divides \( 1 - \frac{\ell}{n} + \left( \frac{\ell}{n} \right)^2 \). We conclude \( d \mid \frac{\ell}{n} \), thus \( d = 1 \).

- \((a, b, c) \equiv t(C, A, B) \mod m\): Comparing \( b \) with \( tA \) and \( c \) with \( tB \) yields
  \[1 \equiv t \mod m\]
  \[-\frac{\ell}{n} \equiv tp^i \mod m.\]
  This case is completed as in the previous case.
• \((a, b, c) \equiv t(B, C, A) \mod m\): Comparing \(b\) with \(tC\) yields

\[ 1 \equiv t(p^i - 1) \mod m. \]

Modulo \(d\) this reduces to \(1 \equiv 0 \mod d\). Therefore, \(d = 1\).

\[ \square \]

**Corollary 5.4.** If \(n\) and \(\ell\) are relatively prime and \(H_{n,\ell}\) is supersingular over \(\mathbb{F}_p\), then it will be maximal over \(\mathbb{F}_{p^{2^i}}\) where \(i\) is the same as in Theorem 5.3.

**Proof.** By Theorem 5.3, if \(H_{n,\ell}\) is supersingular over \(\mathbb{F}_p\), then \(p^i \equiv -1 \mod m\) for some \(i\). By the results of [Taf10] we know that this implies \(\mathcal{F}_m\) will be maximal over \(\mathbb{F}_{p^{2^i}}\). Since \(\mathcal{F}_m\) covers \(H_{n,\ell}\), this implies \(H_{n,\ell}\) will also be maximal over \(\mathbb{F}_{p^{2^i}}\). \[ \square \]

Apriori, 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 NWNs.

**Corollary 5.5.** If \(n\) and \(\ell\) 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 5.3 shows the existence of positive integer \(i\) such that \(p^i \equiv -1 \mod m\). Then by [SK79, Prop. 3.10] \(\mathcal{F}_m\) is supersingular over \(\mathbb{F}_p\). \[ \square \]

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

**Theorem 5.6 ([AKT01, Theorem 3.1]).** Let \(\ell = 1\). The curve \(H_{n,1}\) is maximal over \(\mathbb{F}_{q^{2^j}}\) if and only if \(p^i \equiv -1 \mod m\) for some positive integer \(j\).

**Theorem 5.7 ([AKT01, Theorem 4.5]).** Assume that \(\gcd(n, \ell) = 1\) and \(m\) is prime. Then \(H_{n,\ell}\) is maximal over \(\mathbb{F}_{p^{2^j}}\) if and only if \(p^i \equiv -1 \mod m\) for some positive integer \(j\).

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

\[ p^j \equiv -1 \mod m. \tag{7} \]

**Remark 5.8.** 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 \(\mathbb{F}_{q^{2^j}}\) if and only if \(H_{n,\ell}\) is maximal over \(\mathbb{F}_{q^{2^j}}\).

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

**Corollary 5.9.** If \(\ell = 1\), or \(n\) and \(\ell\) are relatively prime and \(m\) is prime, \(H_{n,\ell}\) is minimal over \(\mathbb{F}_{p^{4^i}}\) if and only if \(\mathcal{F}_m\) is minimal over \(\mathbb{F}_{p^{4^i}}\).
Proof. First suppose $F_m$ is minimal over $F_{p^{4i}}$ with set $N$ of NWNs. Then the NWNs of $H_{n,\ell}$ are a subset of $N$. Thus $H_{n,\ell}$ will also be minimal over $F_{p^{4i}}$.

Now assume $H_{n,\ell}$ is minimal over $F_{p^{4i}}$. Minimality implies supersingularity, thus $H_{n,\ell}$ must also be supersingular. By Theorem 5.3 supersingularity of $H_{n,\ell}$ over $F_p$ implies $p^j \equiv -1 \mod m$ for some positive integer $j$. Choose a minimal such $j$. Then Corollary 5.4 shows $H_{n,\ell}$ is maximal over $F_{p^{2j}}$, thus minimal over $F_{p^{4j}}$. Minimality of $j$ implies that $F_{p^{4j}}$ is a subfield of $F_{p^{4i}}$. Consequently, $j | i$.

Now, by [AKT01] $p^j \equiv -1 \mod m$ implies that $F_m$ is maximal over $F_{p^{2j}}$. Hence, $F_m$ is minimal over $F_{p^{4j}}$. Because $j | i$, $F_m$ is minimal over $F_{p^{4i}}$.

Remark 5.10. The curve $H_{3,3}$ is maximal over $F_5$ but $F_0$ is not. The above theorems show a supersingular Hurwitz curve and its covering Fermat curve will both be maximal over $F_{p^{2i}}$. 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 $F_{p^{2j}}$ where $j | i$ 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 $\ell$ being relatively prime. It is difficult to find an example with $n$ and $\ell$ relatively prime, as the genera of Hurwitz curves grow quickly causing the point counts to become computationally expensive.

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/$F_{q^2}$ means, for some power $q$ of $p$, the curve is maximal over $F_{q^2}$. If a curve is maximal over $F_{q^2}$ then it is minimal over $F_{q^4}$. 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. Corollary 5.4 and Corollary 5.5 are under the condition that gcd$(n,\ell) = 1$, while [AKT01]
and Corollary 5.9 are under the condition that $\ell = 1$, or $\gcd(n, \ell) = 1$ and $m$ is prime.

## 6 Data

Here we provide a classification of supersingular Hurwitz curves over fields with characteristic $p < 37$ and with genus less than 5.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$l$</th>
<th>$p$</th>
<th>$g$</th>
<th>$L$-Polynomial</th>
<th>NWNs (multiplicity)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
<td>1</td>
<td>$5T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>1</td>
<td>$11T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>17</td>
<td>1</td>
<td>$17T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>23</td>
<td>1</td>
<td>$23T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>29</td>
<td>1</td>
<td>$29T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>$5T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>11</td>
<td>1</td>
<td>$11T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>17</td>
<td>1</td>
<td>$17T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>23</td>
<td>1</td>
<td>$23T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>29</td>
<td>1</td>
<td>$29T^2 + 1$</td>
<td>i, -i</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>$27T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>$125T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>13</td>
<td>3</td>
<td>$2197T^{36} + 507T^4 + 39T^2 + 1$</td>
<td>i(3), -i(3)</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>17</td>
<td>3</td>
<td>$4913T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>19</td>
<td>3</td>
<td>$6859T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>31</td>
<td>3</td>
<td>$29791T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>$27T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>$125T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>13</td>
<td>3</td>
<td>$2197T^{36} + 507T^4 + 39T^2 + 1$</td>
<td>i(3), -i(3)</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>17</td>
<td>3</td>
<td>$4913T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>19</td>
<td>3</td>
<td>$6859T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>31</td>
<td>3</td>
<td>$29791T^8 + 1$</td>
<td>i, -i, $\zeta_{12}, \zeta_{12}^3, \zeta_{12}^7, \zeta_{12}^{11}$</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>$625T^8 + 500T^6 + 150T^4 + 20T^2 + 1$</td>
<td>i(4), -i(4)</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>17</td>
<td>4</td>
<td>$83521T^8 + 19652T^6 + 1734T^4 + 68T^2 + 1$</td>
<td>i(4), -i(4)</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>29</td>
<td>4</td>
<td>$707281T^8 + 97556T^6 + 5046T^4 + 116T^2 + 1$</td>
<td>i(4), -i(4)</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>5</td>
<td>6</td>
<td>$15625T^{32} + 1875T^8 + 75T^4 + 1$</td>
<td>$\zeta_3(3)^2, \zeta_3(3)^3, \zeta_3(3)^7, \zeta_3(3)^{11}$</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>$15625T^{32} + 1875T^8 + 75T^4 + 1$</td>
<td>$\zeta_3(3)^2, \zeta_3(3)^3, \zeta_3(3)^7, \zeta_3(3)^{11}$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>6</td>
<td>$729T^{12} + 243T^6 + 27T^4 + 1$</td>
<td>$\zeta_3(3)^2, \zeta_3(3)^3, \zeta_3(3)^7, \zeta_3(3)^{11}$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>7</td>
<td>6</td>
<td>$117649T^{12} + 7203T^8 + 147T^4 + 1$</td>
<td>$\zeta_3(3)^2, \zeta_3(3)^3, \zeta_3(3)^7, \zeta_3(3)^{11}$</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>13</td>
<td>6</td>
<td>$48268097^{12} + 85683T^8 + 50T^4 + 1$</td>
<td>$\zeta_3(3)^2, \zeta_3(3)^3, \zeta_3(3)^7, \zeta_3(3)^{11}$</td>
</tr>
</tbody>
</table>

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

By counting points and using Lemma 2.1 we computed, using [Sag16], the $L$-polynomials and NWNs of many supersingular Hurwitz curves over $\mathbb{F}_p$. When $n$ and $\ell$ 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 see if $q \equiv 1 \mod \gcd(n, \ell)$ 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.

References


