

# involve

a journal of mathematics

## The supersingularity of Hurwitz curves

Erin Dawson, Henry Frauenhoff, Michael Lynch, Amethyst Price,  
Seamus Somerstep, Eric Work, Dean Bisogno and Rachel Pries





# The supersingularity of Hurwitz curves

Erin Dawson, Henry Frauenhoeff, Michael Lynch, Amethyst Price,  
Seamus Somerstep, Eric Work, Dean Bisogno and Rachel Pries

(Communicated by Ken Ono)

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  $p^i \equiv -1 \pmod{(n^2 - n\ell + \ell^2)}$ . 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.

## 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  $\ell$  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 find some restrictions on the genera of Hurwitz curves.

## 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.

**2A. The Hurwitz curve and the Fermat curve.** Let  $n$ ,  $\ell$ , and  $d$  be positive integers. Let  $F$  be a field.

---

*MSC2010:* primary 11G20, 11M38, 14H37, 14H45, 11E81; secondary 11G10, 14H40, 14K15.

*Keywords:* Hurwitz curve, Hasse–Weil bound, maximal curve, minimal curve, Fermat curve, supersingular curve.

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

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

Throughout this paper, set  $m = n^2 - n\ell + \ell^2$ . The Hurwitz curve  $H_{n,\ell}$  has 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  $\frac{1}{2}(d-1)(d-2)$  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 3B for more details.

**2B. 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

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

Rationality of the zeta function for curves was proven by Weil [1948a; 1949]. In particular, Weil showed that the zeta function can be written as

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

The  $L$ -polynomial,  $L(C/\mathbb{F}_q, T) \in \mathbb{Z}[T]$ , has degree  $2g$  [Ireland and Rosen 1990, p. 152]:

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

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  $1 \leq i \leq 2g$  [Ireland and Rosen 1990, p. 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  $\alpha_i$  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 2.5.** If  $\{\alpha_1, \dots, \alpha_{2g}\}$  are the normalized Weil numbers over  $\mathbb{F}_q$ , then  $\{\alpha_1^i, \dots, \alpha_{2g}^i\}$  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  $\gamma$  by  $\text{len}(\gamma)$ .

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

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

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

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

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

$$\begin{aligned} Z(C/\mathbb{F}_q, T) \\ = 1 + (N_1)T + \left( \frac{N_2}{2} + \frac{N_1^2}{2} \right) T^2 + \left( \frac{N_3}{3} + \frac{N_1 N_2}{2} + \frac{N_1^3}{6} \right) T^3 + \dots \end{aligned} \quad (4)$$

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

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

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 (3) yields the expansion

$$\begin{aligned} Z(C/\mathbb{F}_q, T) \\ = (1 + C_1 T + \dots + C_{2g} T^{2g})(1 + T + T^2 + \dots)(1 + qT + q^2 T^2 + \dots). \end{aligned} \quad (5)$$

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

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

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

**2C. 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  $\text{val}_{p^r}(n) = l/r$  and the prime-to- $p$  part of  $n$  by  $n_p = k$ . If  $n = 0$ , we say  $\text{val}_{p^r}(0) = \infty$ .

**Definition 2.9** (Newton polygon). Fix a curve  $C/\mathbb{F}_{p^r}$  with  $L$ -polynomial in the form of (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 2.10.** 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  $\frac{1}{2}$ .

**2D. 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 [1948a].

**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** [Weil 1948a, p. 22; 1948b, p. 69]. The curve  $C$  is maximal over  $\mathbb{F}_q$  if and only if all its normalized Weil numbers are  $-1$  over  $\mathbb{F}_q$ , and it is minimal over  $\mathbb{F}_q$  if and only if all its normalized Weil numbers are  $1$  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.

**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  $\zeta_{k_1}^{t_1}, \dots, \zeta_{k_{2g}}^{t_{2g}}$ . 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  $2^{s-1} \operatorname{lcm}(b_1, \dots, b_n)$ .*

*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  $2^{s-1} \operatorname{lcm}(b_1, \dots, b_n)$ .

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

### 3. Curve maps and covers

**3A. 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 by  $\alpha \approx \beta$ , if there exist elements  $t \in (\mathbb{Z}/m)^*$  and  $\sigma \in S_3$  such that

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

Aoki [2008a; 2008b] studied 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 3.1** [Aoki 2008b, 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:*

- $p^i \equiv -1 \pmod{m}$  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  $p^j \equiv -1 \pmod{(m/d)}$  for some integer  $j$ .

**3B. Covers of  $H_{n,\ell}$  by  $\mathcal{F}_m$ .** In Section 2A, 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 equations

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

Then the following covering map is provided by [Aguglia et al. 2001, Lemma 4.1]:

$$\phi : \mathcal{F}_m \rightarrow H_{n,\ell}, \quad (u, v) \mapsto (u^n v^{-l}, u^l v^{n-l}).$$

Furthermore, it is known that  $\mathcal{F}_m$  is supersingular over  $\mathbb{F}_p$  if and only if  $p^i \equiv -1 \pmod{m}$  for some integer  $i$  [Shioda and Katsura 1979, Proposition 3.10]. See also [Yui 1980, Theorem 3.5]. In [Tafazolian 2010, Theorem 5] it is shown that  $\mathcal{F}_m$  is maximal over  $\mathbb{F}_{p^{2i}}$  if and only if  $p^i \equiv -1 \pmod{m}$ .

**Remark 3.2.** If  $X \rightarrow Y$  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 [Serre 1985].

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

**3C. A birational transformations.** Bennama and Carbonne [1997] 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  $1 \leq \ell < n$  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

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

Equation (6) is very similar to the equation for  $D_\alpha$  that Aoki studied 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 (6) is divisible by  $(x' - 1)$  while Aoki studied 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 (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  $\ell$  are relatively prime. We use results from [Bennama and Carbonne 1997; Aoki 2008a] to accomplish this. We will be using affine equations for the Hurwitz curve in this section.



**Lemma 4.1.** *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  $p^i \equiv -1 \pmod{m}$ . (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  $p^j \equiv -1 \pmod{(m/d)}$  for some integer  $j$ .*

*Proof.* We use the variable substitution from [Bennama and Carbonne 1997] to apply Aoki's results to Hurwitz curves. We use the substitutions

$$m = n^2 - n\ell + \ell^2, \quad a = \lambda = \delta(n - \ell) + \ell\theta - 1, \quad b = 1, \quad c = m - (\delta(n - \ell) + \ell\theta). \quad (7)$$

Combining these with Aoki's results completes the proof.  $\square$

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

**Theorem 4.3.** *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  $p^i \equiv -1 \pmod{m}$  for some positive integer  $i$ .*

*Proof.* If  $p^i \equiv -1 \pmod{m}$  for some positive integer  $i$ , then  $\mathcal{F}_m$  is supersingular over  $\mathbb{F}_p$  by [Shioda and Katsura 1979, Proposition 3.10]. Recall from Section 3B 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 cannot happen. We begin by simplifying it using the substitution  $\theta = (1 + \ell\delta)/n$  and reducing modulo  $m$  to show that condition (2) is equivalent to  $(\ell/n - 1, 1, -\ell/n) \approx (1, -p^i, p^i - 1)$  for some  $i$  such that  $d = (p^i - 1, m) > 1$  and  $p^j \equiv -1 \pmod{(m/d)}$  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  $(\ell/n - 1, 1, -\ell/n)$  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  $\ell/n$  is relatively prime to  $d$ .

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

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

Consequently,  $\ell/n \equiv 0 \pmod{d}$ . Therefore,  $d = 1$ .

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

$$\frac{\ell}{n} - 1 \equiv -tp^i \pmod{m}, \quad 1 \equiv t \pmod{m}.$$

Substituting we have  $\ell/n \equiv p^i - 1 \pmod{m}$ . Reducing modulo  $d$  produces  $\ell/n \equiv 0 \pmod{d}$ , thus  $d = 1$ .

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

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

This is identical to the first case.

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

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

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

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

$$1 \equiv t \pmod{m}, \quad \frac{\ell}{n} \equiv tp^i \pmod{m}.$$

This case is completed as in the previous case.

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

$$1 \equiv t(p^i - 1) \pmod{m}.$$

Modulo  $d$  this reduces to  $1 \equiv 0 \pmod{d}$ . 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  $\delta = a_1 a_2 - a_2 n_2 + n_1 n_2$ . When  $q = p^r$  is coprime to  $\delta$ , the curve  $\mathcal{C}_{a_1, a_2, n_1, n_2}$  is  $\mathbb{F}_q$ -covered by the Fermat curve  $\mathcal{F}_\delta$  of degree  $\delta$ . Tafazolian and Torres [2017, Theorem 2.9] showed 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  $q + 1 \equiv 0 \pmod{\delta}$

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 [Tafazolian and Torres 2017, Theorem 2.9].

**Remark 4.5.** Consider the family of curves with affine equations

$$N_{a_1, a_2, n_1, n_2} : x^{n_1} y^{a_1} + k_1 y^{n_2} + k_2 x^{a_2} = 0$$

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  $\delta$  as in Remark 4.4. Recall the definition of  $n_p$  in Definition 2.8. With these assumptions [Nie 2016, 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 [Nie 2016, Theorem 4.12] when  $a_1 = a_2 = \ell$  and  $n_1 = n_2 = n$ .

**Corollary 4.6.** *If  $n$  and  $\ell$  are relatively prime and  $H_{n, \ell}$  is supersingular over  $\mathbb{F}_p$ , then it will be maximal over  $\mathbb{F}_{p^{2i}}$ , 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  $p^i \equiv -1 \pmod{m}$  for some  $i$ . By [Tafazolian 2010], 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  $\mathbb{F}_{p^{2i}}$ .  $\square$

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  $\ell$  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 4.3 shows the existence of positive integer  $i$  such that  $p^i \equiv -1 \pmod{m}$ . Then by [Shioda and Katsura 1979, Proposition 3.10],  $\mathcal{F}_m$  is supersingular over  $\mathbb{F}_p$ .  $\square$

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

**Theorem 4.8** [Aguglia et al. 2001, Theorem 3.1]. *Let  $\ell = 1$ . The curve  $H_{n, 1}$  is maximal over  $\mathbb{F}_{q^{2j}}$  if and only if  $p^j \equiv -1 \pmod{m}$  for some positive integer  $j$ .*

**Theorem 4.9** [Aguglia et al. 2001, 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  $p^j \equiv -1 \pmod{m}$  for some positive integer  $j$ .*

Note that the key property used in [Aguglia et al. 2001] is the existence of some positive integer  $j$  such that

$$p^j \equiv -1 \pmod{m}. \quad (8)$$

**Remark 4.10.** Under the requirements  $\ell = 1$ , or  $\gcd(n, \ell) = 1$  and  $m$  prime, the results in [Aguglia et al. 2001] and [Tafazolian 2010, 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  $\ell$  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  $\mathbb{F}_{p^{4i}}$ .*

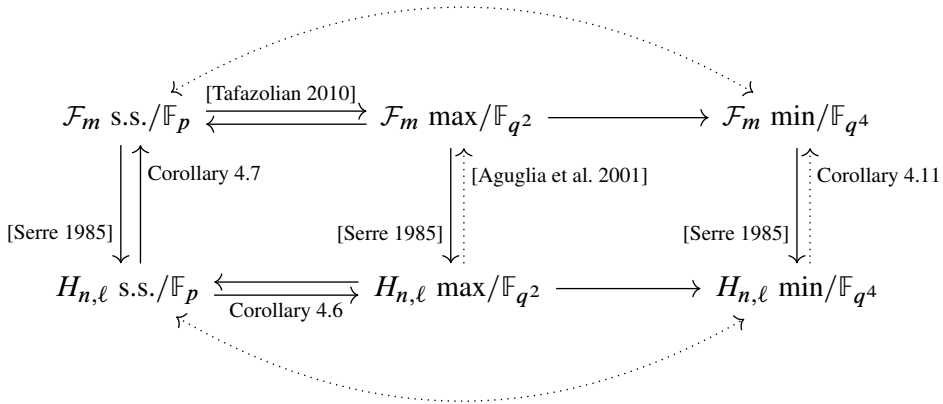
*Proof.* First suppose  $\mathcal{F}_m$  is minimal over  $\mathbb{F}_{p^{4i}}$  with set  $N$  of normalized Weil numbers. Then the normalized Weil numbers of  $H_{n,\ell}$  are a subset of  $N$ . Thus  $H_{n,\ell}$  will also be minimal over  $\mathbb{F}_{p^{4i}}$ .

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  $p^j \equiv -1 \pmod{m}$  for some positive integer  $j$ . Choose a minimal such  $j$ . Then Corollary 4.6 shows  $H_{n,\ell}$  is maximal over  $\mathbb{F}_{p^{2j}}$  and 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 [Aguglia et al. 2001]  $p^j \equiv -1 \pmod{m}$  implies that  $\mathcal{F}_m$  is maximal over  $\mathbb{F}_{p^{2j}}$ . Hence,  $\mathcal{F}_m$  is minimal over  $\mathbb{F}_{p^{4j}}$ . Because  $j \mid i$ , we have  $\mathcal{F}_m$  is minimal over  $\mathbb{F}_{p^{4i}}$ .  $\square$

**Remark 4.12.** The curve  $H_{3,3}$  is maximal over  $\mathbb{F}_{5^2}$  but  $\mathcal{F}_9$  is not. The theorems above 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  $\ell$  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 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



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

$\max/\mathbb{F}_{q^2}$  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 [Aguglia et al. 2001] and Corollary 4.11 are under the condition that  $\ell = 1$ , or  $\gcd(n, \ell) = 1$  and  $m$  is prime.

## 5. Genera of Hurwitz curves and additional 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  $H_{n,\ell}$  is

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

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** [Fermat 1999, Volume 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  $p \equiv 0, 1 \pmod{3}$  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  $\ell$  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  $q(x, y) = m$ :

$$\begin{aligned} f : \mathbb{Z}^2 &\rightarrow \mathbb{Z}^2, & f(x, y) &\mapsto (y, x), \\ g : \mathbb{Z}^2 &\rightarrow \mathbb{Z}^2, & g(x, y) &\mapsto (-x, -y), \\ \varphi : \mathbb{Z}^2 &\rightarrow \mathbb{Z}^2, & \varphi(x, y) &\mapsto (x, x - y), \\ I : \mathbb{Z}^2 &\rightarrow \mathbb{Z}^2, & I(x, y) &\mapsto (x, y). \end{aligned}$$

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

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

**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  $(x', y') \in \mathbb{N}^2$ .*

$n$	$l$	$p$	$g$	$L$ -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  $< 5$ .

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

- (3) If  $x$  is negative and  $y$  is 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  $\varphi(y, 0) = (y, y)$ .  $\square$

By counting points and using Lemma 2.6 we computed, using CoCalc, the  $L$ -polynomials and normalized Weil numbers 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 check if  $q \equiv 1 \pmod{\gcd(n, \ell)}$  and count the multiplicities of singular points. This gives the correct point counts to compute the  $L$ -polynomial of the normalization of the equation. Table 1 has all supersingular Hurwitz curves  $H_{n,\ell}$  of genus less than 5 for primes less than 37. Table 1 also includes some curves of genus 6.

### 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.

### References

- [Aguglia et al. 2001] A. Aguglia, G. Korchmáros, and F. Torres, “Plane maximal curves”, *Acta Arith.* **98**:2 (2001), 165–179. MR Zbl
- [Aoki 2008a] N. Aoki, “On supersingular cyclic quotients of Fermat curves”, *Comment. Math. Univ. St. Pauli* **57**:1 (2008), 65–90. MR Zbl
- [Aoki 2008b] N. Aoki, “On the zeta function of some cyclic quotients of Fermat curves”, *Comment. Math. Univ. St. Pauli* **57**:2 (2008), 163–185. MR Zbl
- [Bennama and Carbonne 1997] H. Bennama and P. Carbonne, “Courbes  $X^m Y^n + Y^m Z^n + Z^m X^n = 0$  et décomposition de la jacobienne”, *J. Algebra* **188**:2 (1997), 409–417. MR Zbl
- [Fermat 1999] P. Fermat, *Œuvres de Pierre Fermat, I: La théorie des nombres*, Librairie Scientifique et Technique Albert Blanchard, Paris, 1999. MR Zbl
- [Ireland and Rosen 1990] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics **84**, Springer, 1990. MR Zbl
- [Nie 2016] M. Nie, “Zeta functions of trinomial curves and maximal curves”, *Finite Fields Appl.* **39** (2016), 52–82. MR Zbl
- [Serre 1985] J. P. Serre, “Rational points on curves over finite fields”, handwritten notes by F. Q. Gouvêa of lectures given at Harvard University, 1985.
- [Shioda and Katsura 1979] T. Shioda and T. Katsura, “On Fermat varieties”, *Tohoku Math. J. (2)* **31**:1 (1979), 97–115. MR Zbl

- [Tafazolian 2010] S. Tafazolian, “A characterization of maximal and minimal Fermat curves”, *Finite Fields Appl.* **16**:1 (2010), 1–3. MR Zbl
- [Tafazolian and Torres 2017] S. Tafazolian and F. Torres, “A note on certain maximal curves”, *Comm. Algebra* **45**:2 (2017), 764–773. MR Zbl
- [Weil 1948a] A. Weil, *Sur les courbes algébriques et les variétés qui s’en déduisent*, Actualités Sci. Ind. **1041**, Hermann et Cie., Paris, 1948. MR Zbl
- [Weil 1948b] A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind. **1064**, Hermann et Cie., Paris, 1948. MR Zbl
- [Weil 1949] A. Weil, “Numbers of solutions of equations in finite fields”, *Bull. Amer. Math. Soc.* **55** (1949), 497–508. MR Zbl
- [Yui 1980] N. Yui, “On the Jacobian variety of the Fermat curve”, *J. Algebra* **65**:1 (1980), 1–35. MR Zbl

Received: 2018-11-15      Revised: 2019-06-24      Accepted: 2019-07-06

erinrdawson@gmail.com	Colorado State University, Fort Collins, CO, United States
hwy027@gmail.com	Colorado State University, Fort Collins, CO, United States
keylynch@rams.colostate.edu	Colorado State University, Fort Collins, CO, United States
ameprice@rams.colostate.edu	Colorado State University, Fort Collins, CO, United States
smstep@rams.colostate.edu	Colorado State University, Fort Collins, CO, United States
ewewok75@gmail.com	Colorado State University, Fort Collins, CO, United States
dean.bisogno@gmail.com	Colorado State University, Fort Collins, CO, United States
pries@math.colostate.edu	Colorado State University, Fort Collins, CO, United States



# involve

msp.org/involve

## INVOLVE YOUR STUDENTS IN RESEARCH

*Involve* showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

## MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

## BOARD OF EDITORS

Colin Adams	Williams College, USA	Robert B. Lund	Clemson University, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Gaven J. Martin	Massey University, New Zealand
Martin Bohner	Missouri U of Science and Technology, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of N Carolina, Chapel Hill, USA	Frank Morgan	Williams College, USA
Pietro Cerone	La Trobe University, Australia	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Scott Chapman	Sam Houston State University, USA	Zuhair Nashed	University of Central Florida, USA
Joshua N. Cooper	University of South Carolina, USA	Ken Ono	Univ. of Virginia, Charlottesville
Jem N. Corcoran	University of Colorado, USA	Yuval Peres	Microsoft Research, USA
Toka Diagana	Howard University, USA	Y.-F. S. Pétermann	Université de Genève, Switzerland
Michael Dorff	Brigham Young University, USA	Jonathon Peterson	Purdue University, USA
Sever S. Dragomir	Victoria University, Australia	Robert J. Plemmons	Wake Forest University, USA
Joel Foisy	SUNY Potsdam, USA	Carl B. Pomerance	Dartmouth College, USA
Errin W. Fulp	Wake Forest University, USA	Vadim Ponomarenko	San Diego State University, USA
Joseph Gallian	University of Minnesota Duluth, USA	Bjorn Poonen	UC Berkeley, USA
Stephan R. Garcia	Pomona College, USA	József H. Przytycki	George Washington University, USA
Anant Godbole	East Tennessee State University, USA	Richard Rebarber	University of Nebraska, USA
Ron Gould	Emory University, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Javier Rojo	Oregon State University, USA
Jim Haglund	University of Pennsylvania, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Johnny Henderson	Baylor University, USA	Hari Mohan Srivastava	University of Victoria, Canada
Glenn H. Hurlbert	Virginia Commonwealth University, USA	Andrew J. Sterge	Honorary Editor
Charles R. Johnson	College of William and Mary, USA	Ann Trenk	Wellesley College, USA
K. B. Kulasekera	Clemson University, USA	Ravi Vakil	Stanford University, USA
Gerry Ladas	University of Rhode Island, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
David Larson	Texas A&M University, USA	John C. Wierman	Johns Hopkins University, USA
Suzanne Lenhart	University of Tennessee, USA	Michael E. Zieve	University of Michigan, USA
Chi-Kwong Li	College of William and Mary, USA		

## PRODUCTION

Silvio Levy, Scientific Editor


Cover: Alex Scorpan

See inside back cover or [msp.org/involve](http://msp.org/involve) for submission instructions. The subscription price for 2019 is US \$195/year for the electronic version, and \$260/year (+\$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1444-4184 electronic, 1444-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2019 Mathematical Sciences Publishers

# involve

2019

vol. 12

no. 8

On the zero-sum group-magicness of cartesian products	1261
ADAM FONG, JOHN GEORGES, DAVID MAURO, DYLAN SPAGNUOLO, JOHN WALLACE, SHUFAN WANG AND KIRSTI WASH	
The variable exponent Bernoulli differential equation	1279
KAREN R. RÍOS-SOTO, CARLOS E. SEDA-DAMIANI AND ALEJANDRO VÉLEZ-SANTIAGO	
The supersingularity of Hurwitz curves	1293
ERIN DAWSON, HENRY FRAUENHOFF, MICHAEL LYNCH, AMETHYST PRICE, SEAMUS SOMERSTEP, ERIC WORK, DEAN BISOGNO AND RACHEL PRIES	
Multicast triangular semilattice network	1307
ANGELINA GROSSO, FELICE MANGANIELLO, SHIWANI VARAL AND EMILY ZHU	
Edge-transitive graphs and combinatorial designs	1329
HEATHER A. NEWMAN, HECTOR MIRANDA, ADAM GREGORY AND DARREN A. NARAYAN	
A logistic two-sex model with mate-finding Allee effect	1343
ELIZABETH ANDERSON, DANIEL MAXIN, JARED OTT AND GWYNETH TERRETT	
Unoriented links and the Jones polynomial	1357
SANDY GANZELL, JANET HUFFMAN, LESLIE MAVRAKIS, KAITLIN TADEMY AND GRIFFIN WALKER	
Nonsplit module extensions over the one-sided inverse of $k[x]$	1369
ZHEPING LU, LINHONG WANG AND XINGTING WANG	
Split Grothendieck rings of rooted trees and skew shapes via monoid representations	1379
DAVID BEERS AND MATT SZCZESNY	
On the classification of Specht modules with one-dimensional summands	1399
AUBREY PIPER COLLINS AND CRAIG J. DODGE	
The monochromatic column problem with a prime number of colors	1415
LORAN CROWELL AND STEVE SZABO	
Total Roman domination edge-critical graphs	1423
CHLOE LAMPMAN, KIEKA (C. M.) MYNHARDT AND SHANNON OGDEN	

