A note on certain superspecial and maximal curves of genus 5

Momonari Kudo*†

June 25, 2019

Abstract

In this note, we characterize certain maximal superspecial curves of genus 5 over finite fields. Specifically, we prove that the desingularization T_p of $xyz^3+x^5+y^5=0$ is a maximal superspecial trigonal curve of genus 5 *if and only if* $p \equiv -1 \pmod{15}$ or $p \equiv 11 \pmod{15}$. Moreover, we give families of maximal curves of more general type, which include T_p.

Key words— Maximal curves, Superspecial curves, Curves of genus 5

1 Introduction

By a curve, we mean a projective, geometrically irreducible, non-singular algebraic curve. Let K be a field of positive characteristic $p > 0$. A curve C of genus g over K is said to be *superspecial* if its Jacobian variety is isomorphic to the product of supersingular elliptic curves over the algebraic closure $\overline{K}$ of K. Any superspecial curve is a *supersingular* curve, which is a curve such that its Jacobian variety is isogenous to the product of supersingular elliptic curves. Furthermore, superspecial curves are closely related to *maximal* curves and *minimal* curves, where a curve over $\mathbb{F}_q$ is called a maximal (resp. minimal) curve if the number of its $\mathbb{F}_q$-rational points attains the Hasse-Weil upper (resp. lower) bound $q + 1 + 2g\sqrt{q}$ (resp. $q + 1 - 2g\sqrt{q}$). It is known that a superspecial curve over an algebraically closed field in characteristic p descends to a maximal or minimal curve over $\mathbb{F}_{p^2}$. In contrast, any maximal or minimal curve over $\mathbb{F}_{p^2}$ is superspecial. Note that superspecial curves over $\mathbb{F}_{p^2}$ are not necessarily $\mathbb{F}_{p^2}$-maximal. This note studies superspecial curves in order to find $\mathbb{F}_{p^2}$-maximal curves.

Finding maximal curves is an active research problem in the study of curves over finite fields, see e.g., [10], [12], [22], [23], [24], [25], and [26]. In particular, Tafazolian and Torres (cf. [22], [23], [24], [25], [26]) characterize maximal curves of various types, e.g., hyperelliptic curves $y^2 = x^m + x$ and $y^2 = x^m + 1$, Fermat type $x^m + y^n = 1$, Hurwitz type $x^m y^a + y^n + x^b = 0$, other types such as $y^n = x^\ell(x^m + 1)$. They use Serre's covering result (cf. [11, Prop. 2.3], [19]): Any curve over $\mathbb{F}_{q^2}$ non-trivially $\mathbb{F}_{q^2}$-covered by a maximal curve over $\mathbb{F}_{q^2}$ is also a maximal curve over $\mathbb{F}_{q^2}$. They prove the maximality of curves by finding subcovers of a maximal curve such as the Hermitian curve.

Another problem is the *enumeration* of superspecial (or maximal) curves. Enumeration means here that we count the number of K-isomorphism classes of superspecial (or maximal) curves of genus g over $\mathbb{F}_q$ for $K = \mathbb{F}_q$ or $\overline{\mathbb{F}_q}$. If $g \leq 3$, some theoretical approaches to enumerate superspecial (or maximal) curves are available, and they are based on Torelli's theorem (cf. [3], [27, Prop. 4.4]

*Kobe City College of Technology.
†Institute of Mathematics for Industry, Kyushu University. E-mail: `m-kudo@math.kyushu-u.ac.jp`

for $g = 1$, [7], [9], [21] for $g = 2$, and [6], [8] for $g = 3$). If $g \geq 4$, however, it is thought that these approaches are not so effective; different from the case of $g \leq 3$, the dimension of the moduli space of curves of genus g is strictly less than that of the moduli space of principally polarized abelian varieties of dimension g.

To deal with the case of $g \geq 4$, alternative approaches based on both theory of algebraic geometry and computer algebraic methods are proposed in [14], [15], [16], [17] and [18]. In [18], superspecial trigonal curves of genus 5 over $\mathbb{F}_q$ are completely enumerated for $q = 5$, 5^2, 7, 7^2, 11 and 13. In particular, there are precisely four $\mathbb{F}_{11}$-isomorphism classes of superspecial trigonal curves. Enumerated isomorphism classes are represented by the non-singular models of the singular plane curves $xyz^3 + sx^5 + ty^5 = 0$ with a singularity $[0 : 0 : 1]$ in $\mathbf{P}^2 = \mathrm{Proj}(\overline{\mathbb{F}_{11}}[x, y, z])$ for some $s \in \mathbb{F}_{11}^\times$ and $t \in \mathbb{F}_{11}^\times$. The non-singular model with $s = t = 1$ is also an $\mathbb{F}_{11^2}$-maximal curve, see [18, Remark 5.1.2].

In this note, we investigate the superspeciality of the non-singular model of $xyz^3 + sx^5 + ty^5 = 0$ with $s \in \mathbb{F}_q^\times$ and $t \in \mathbb{F}_q^\times$ for *arbitrary* q. We also investigate the $\mathbb{F}_{p^2}$-maximality of the curve with $(s, t) = (1, 1)$ for arbitrary $p > 11$. Moreover, we consider curves of more general type: the non-singular model of the homogeneous equation $x^a + y^a + z^b x^c y^c = 0$ for natural numbers a, b and c with $b + 2c = a$. Main results of this note are as follows:

Theorem 1.1. *Let (s, t) be a pair of elements in $\mathbb{F}_q^\times$. Put $F := xyz^3 + sx^5 + ty^5$. Let $V(F)$ denote the projective zero-locus in $\mathbf{P}^2 = \mathrm{Proj}(\overline{\mathbb{F}_q}[x, y, z])$ defined by $F = 0$. Then the desingularization T_p of $V(F)$ is a superspecial trigonal curve of genus 5 if and only if $p \equiv 2 \pmod 3$ and $p \equiv 1, 4 \pmod 5$.*

We directly prove Theorem 1.1 by computing the Hasse-Witt matrix of T_p. Since $\mathbb{F}_{p^2}$-maximal curves are superspecial, the condition $p \equiv 2 \pmod 3$ and $p \equiv 1, 4 \pmod 5$ is necessary for T_p to be $\mathbb{F}_{p^2}$-maximal. In fact, the converse is true for $(s, t) = (1, 1)$.

Theorem 1.2. *Let $V(F)$ denote the projective zero-locus in $\mathbf{P}^2$ defined by $F = xyz^3 + x^5 + y^5 = 0$. Then the desingularization T_p of $V(F)$ is an $\mathbb{F}_{p^2}$-maximal trigonal curve of genus 5 if and only if $p \equiv -1 \pmod{15}$ or $p \equiv 11 \pmod{15}$.*

We prove Theorem 1.3 below by constructing explicit equations for subcovers of the Hermitian curve, similarly to methods in [22], [23], [24], [25] and [26].

Theorem 1.3. *Let a, b and c be natural numbers with $b + 2c = a$. Put $n := ab/\gcd(a, b, c)$. Let $C_{p,a,b,c}$ be the non-singular model of $x^a + y^a + z^b x^c y^c = 0$. Then we have the following:*

1. *The curve $C_{p,a,b,c}$ is maximal over $\mathbb{F}_{p^2}$ if $p \equiv -1 \pmod n$.*
2. *Suppose that a and b are coprime. Since there exists an integer d such that $d \equiv 2 \pmod a$ and $d \equiv 0 \pmod b$, and since any two such d are congruent modulo ab, we fix such a d in the interval $[0, ab)$. Then the curve $C_{p,a,b,c}$ is maximal over $\mathbb{F}_{p^2}$ if $p \equiv d - 1 \pmod n$.*

Acknowledgments

I thank Shushi Harashita for his comments on the preliminary version of this note. I also thank Bradley Brock for sending me his thesis [2]. From his thesis, I learned much about superspecial curves.

2 Superspeciality of the trigonal curve T_p

As in the previous section, let K be a perfect field of characteristic $p > 2$. Let $K[x, y, z]$ denote the polynomial ring of the three variables x, y and z. As an example of a superspecial curve of genus $g = 5$ in characteristic 11, we have the desingularization of the projective variety $xyz^3 + sx^5 + ty^5 = 0$ with $(s, t) \in (K^\times)^2$ in the projective plane $\mathbf{P}^2 = \mathrm{Proj}(\overline{K}[x, y, z])$, see [18, Theorem B].

In this section, we shall prove that the desingularization of the variety $xyz^3 + sx^5 + ty^5 = 0$ over K is (resp. not) a superspecial curve of genus 5 if $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 5$ or if $p \equiv 2 \pmod 3$ and $p \equiv 4 \pmod 5$ (resp. otherwise). Throughout this section, we set $F := xyz^3 + sx^5 + ty^5$. Let T_p denote the non-singular model of the projective variety $V(F)$ in $\mathbf{P}^2$ defined by $F = 0$.

2.1 Singularity of $V(F)$

First, we prove that the variety $V(F)$ has a unique singular point if $p > 5$.

Lemma 2.1.1. *If $p > 5$ (resp. $p = 5$), then the variety $V(F)$ has a unique singular point $[0 : 0 : 1]$ (resp. at least two singular points).*

Proof. Let $J(F)$ denote the set of all the elements of the Jacobian matrix

$$\begin{pmatrix} \frac{\partial F}{\partial x} & \frac{\partial F}{\partial y} & \frac{\partial F}{\partial z} \end{pmatrix} = \begin{pmatrix} yz^3 + 5sx^4 & xz^3 + 5ty^4 & 3xyz^2 \end{pmatrix}.$$

Namely, the set $J(F)$ consists of the following 3 elements: $f_1 = yz^3 + 5sx^4$, $f_2 = xz^3 + 5ty^4$ and $f_3 := 3xyz^2$. Assume $p > 5$. It suffices to show that x and y belong to the radical of the ideal generated by F and $J(F)$. By straightforward computations, we have

$$\begin{aligned} F - xf_1 - 5^{-1}yf_2 + 5^{-1}xf_1 &= -3sx^5 \\ F - yf_2 - 5^{-1}xf_1 + 5^{-1}yf_2 &= -3ty^5 \end{aligned}$$

which belong to the ideal $\langle F, J(F)\rangle$ in $K[x, y, z]$. Thus, x and y belong to its radical.

If $p = 5$, then the point $[s^{-1/5} : -t^{-1/5} : 0]$ on $V(F)$ is a singular point over the algebraic closure $\overline{\mathbb{F}_5}$ for each $(s, t) \in K^{\oplus 2} \smallsetminus \{(0, 0)\}$. ☐

2.2 Irreducibility of F

In this subsection, we show that the variety $V(F)$ with $F = xyz^3 + sx^5 + ty^5$ is irreducible for s and $t \in K^\times$, equivalently the quintic form F is irreducible over the algebraic closure $\overline{K}$.

Lemma 2.2.1. *The quintic form $F = xyz^3 + sx^5 + ty^5$ is irreducible for s and $t \in K^\times$ over the algebraic closure.*

Proof. It suffices to prove that $s^{-1}F = x^5 + s^{-1}ty^5 + s^{-1}xyz^3$, which is monic with respect to x, is irreducible over $\overline{K}$. If $s^{-1}F$ is reducible, we have either of the following two cases: (1) $s^{-1}F = g_1g_4$ for some linear form g_1 and some quartic form g_4 in $\overline{K}[x, y, z]$, or (2) $s^{-1}F = g_2g_3$ for some quadratic form g_2 and some cubic form g_3 in $\overline{K}[x, y, z]$.

(1) We may assume that the coefficient of x (resp. x^4) in g_1 (resp. g_4) is 1. Writing

$$\begin{aligned} g_1 &= x + a_1y + a_2z, \quad \text{and} \\ g_4 &= x^4 + a_3x^3y + a_4x^3z + a_5x^2y^2 + a_6x^2yz + a_7x^2z^2 + a_8xy^3 + a_9xy^2z \\ &\quad + a_{10}xyz^2 + a_{11}xz^3 + a_{12}y^4 + a_{13}y^3z + a_{14}y^2z^2 + a_{15}yz^3 + a_{16}z^4 \end{aligned}$$

for $a_i \in \overline{K}$ with $1 \leq i \leq 16$, we have

$$\begin{aligned} g_1g_4 &= x^5 + (a_1 + a_3)x^4y + (a_2 + a_4)x^4z + (a_1a_3 + a_5)x^3y^3 + (a_2a_3 + a_1a_4a_6)x^3yz + (a_2a_4 + a_7)x^3z^2 \\ &\quad +(a_1a_5 + a_8)x^2y^3 + (a_2a_5 + a_1a_6 + a_9)x^2y^2z + (a_2a_6 + a_1a_7 + a_10)x^2yz^2 + (a_2a_7 + a_{11})x^2z^3 \\ &\quad +(a_1a_8 + a_{12})xy^4 + (a_2a_8 + a_1a_9 + a_{13})xy^3z + (a_2a_9 + a_1a_{10} + a_{14})xy^2z^2 \\ &\quad +(a_2a_{10} + a_1a_{11} + a_{15})xyz^3 + (a_2a_{11} + a_{16})xz^4 + a_1a_{12}y^5 + (a_2a_{12} + a_1a_{13})y^4z \\ &\quad +(a_2a_{13} + a_1a_{14})y^3z^2 + (a_2a_{14} + a_1a_{15})y^2z^3 + (a_2a_{15} + a_1a_{16})yz^4 + a_2a_{16}z^5. \end{aligned}$$

Note that $a_1 \neq 0$ and $a_{12} \neq 0$ since the coefficient a_1a_{12} of y^5 is $s^{-1}t$. Since the coefficient of z^5 in F is zero, we have $a_2a_{16} = 0$ and thus $a_2 = 0$ or $a_{16} = 0$. Assume $a_2 = 0$. In this case, we have $a_1a_i = 0$ and hence $a_i = 0$ for $13 \leq i \leq 16$ since the coefficients of yz^4, y^2z^3, y^3z^2 and y^4z are zero. The coefficients of y^5 and xyz^3 are $a_1a_{12} = s^{-1}t$ and $a_2a_{10}+a_1a_{11}+a_{15} = a_1a_{11} = s^{-1}$ respectively, and thus $ta_{11} = a_{12}$ by $a_1 \neq 0$. The coefficient of x^2z^3 is $a_2a_7 + a_{11} = a_{11}$ is zero, which contradicts $ta_{11} = a_{12} \neq 0$. Assume $a_2 \neq 0$ and $a_{16} = 0$. Since the coefficients of yz^4, y^2z^3, y^3z^2 and y^4z are zero, one has $a_i = 0$ for $12 \leq i \leq 15$. The condition $a_{12} = 0$ is a contradiction.

(2) Writing

$$\begin{aligned} g_2 &= x^2 + b_1xy + b_2xz + b_3y^2 + b_4yz + b_5z^2, \quad \text{and} \\ g_3 &= x^3 + b_6x^2y + b_7x^2z + b_8xy^2 + b_9xyz + b_{10}xz^2 + b_{11}y^3 + b_{12}y^2z + b_{13}yz^2 + b_{14}z^3 \end{aligned}$$

for $b_i \in \overline{K}$ with $1 \leq i \leq 14$, we have

$$\begin{aligned} g_2g_3 &= x^5 + (b_1 + b_6)x^4y + (b_2 + b_7)x^4z + (b_1b_6 + b_3 + b_8)x^3y^2 \\ &\quad +(b_2b_6 + b_1b_7 + b_4 + b_9)x^3yz + (b_2b_7 + b_5 + b_{10})x^3z^2 \\ &\quad +(b_3b_6 + b_1b_8 + b_{11})x^2y^3 + (b_4b_6 + b_3b_7 + b_2b_8 + b_1b_9 + b_{12})x^2y^2z \\ &\quad +(b_5b_6 + b_4b_7 + b_2b_9 + b_1b_{10} + b_{13})x^2yz^2 + (b_5b_7 + b_2b_{10} + b_{14})x^2z^3 \\ &\quad +(b_3b_8 + b_1b_{11})xy^4 + (b_4b_8 + b_3b_9 + b_2b_{11} + b_1b_{12})xy^3z \\ &\quad +(b_5b_8 + b_4b_9 + b_3b_{10} + b_2b_{12} + b_1b_{13})xy^2z^2 \\ &\quad +(b_5b_9 + b_4b_{10} + b_2b_{13} + b_1b_{14})xyz^3 + (b_5b_{10} + b_2b_{14})xz^4 \\ &\quad +b_3b_{11}y^5 + (b_4b_{11} + b_3b_{12})y^4z + (b_5b_{11} + b_4b_{12} + b_3b_{13})y^3z^2 \\ &\quad +(b_5b_{12} + b_4b_{13} + b_3b_{14})y^2z^3 + (b_5b_{13} + b_4b_{14})yz^4 + b_5b_{14}z^5. \end{aligned}$$

Note that $b_3 \neq 0$ and $b_{11} \neq 0$ since the coefficient b_3b_{11} of y^5 is $s^{-1}t$. Since the coefficient of z^5 in F is zero, we have $b_5b_{14} = 0$ and thus $b_5 = 0$ or $b_{14} = 0$. Assume $b_5 \neq 0$ and $b_{14} = 0$. Since the coefficients of yz^4, y^2z^3 and y^3z^2 are zero, we have $b_{13} = b_{12} = b_{11} = 0$, which contradicts $b_{11} \neq 0$. Assume $b_5 = 0$ and $b_{14} \neq 0$. Since the coefficients of yz^4, y^2z^3 and y^3z^2 are zero, we have $b_4 = b_3 = 0$, which contradicts $b_3 \neq 0$. Assume $b_5 = b_{14} = 0$. Since the coefficient of y^2z^3 is zero, we have $b_4b_{13} = 0$. If $b_4 = 0$, then we have $b_{13} = 0$ since the coefficient of y^3z^2 is $b_5b_{11} + b_4b_{12} + b_3b_{13} = b_3b_{13}$ and since $b_3 \neq 0$. Now we have $b_4 = b_5 = b_{13} = b_{14} = 0$, which contradicts that the coefficient of xyz^3 is not zero. If $b_{13} = 0$ and $b_4 \neq 0$, then we have $b_{12} = 0$ since the coefficient of y^3z^2 is $b_5b_{11} + b_4b_{12} + b_3b_{13} = b_4b_{12}$ and since $b_4 \neq 0$. Since the coefficient $b_4b_{11} + b_3b_{12} = b_4b_{11}$ of y^4z is zero, we have $b_{11} = 0$, which is a contradiction for $b_{11} \neq 0$.

□

2.3 Superspeciality of T_p

In the following, we suppose $p > 5$. It is shown in [18] that we can decide whether the desingularization T_p of $V(F)$ is superspecial or not by computing the coefficients of certain monomials in $(F)^{p-1}$, where $F = xyz^3 + sx^5 + ty^5$.

Proposition 2.3.1 ([18], Corollary 3.1.6)**.** *With notation as above, the desingularization T_p of $V(F)$ is superspecial if and only if the coefficients of all the following 25 monomials of degree $5(p-1)$ in $(F)^{p-1}$ are zero:*

$$\begin{array}{ccccc}
(x^3yz)^{p-1}, & x^{3p-1}y^{p-3}z^{p-1}, & x^{3p-2}y^{p-2}z^{p-1}, & x^{3p-2}y^{p-1}z^{p-2}, & x^{3p-1}y^{p-2}z^{p-2}, \\
x^{p-3}y^{3p-1}z^{p-1}, & (xy^3z)^{p-1}, & x^{p-2}y^{3p-2}z^{p-1}, & x^{p-2}y^{3p-1}z^{p-2}, & x^{p-1}y^{3p-2}z^{p-2}, \\
x^{2p-3}y^{2p-1}z^{p-1}, & x^{2p-1}y^{2p-3}z^{p-1}, & (x^2y^2z)^{p-1}, & x^{2p-2}y^{2p-1}z^{p-2}, & x^{2p-1}y^{2p-2}z^{p-2}, \\
x^{2p-3}y^{p-1}z^{2p-1}, & x^{2p-1}y^{p-3}z^{2p-1}, & x^{2p-2}y^{p-2}z^{2p-1}, & (x^2yz^2)^{p-1}, & x^{2p-1}y^{p-2}z^{2p-2}, \\
x^{p-3}y^{2p-1}z^{2p-1}, & x^{p-1}y^{2p-3}z^{2p-1}, & x^{p-2}y^{2p-2}z^{2p-1}, & x^{p-2}y^{2p-1}z^{2p-2}, & (xy^2z^2)^{p-1}.
\end{array}$$

To prove Theorem 1.1 stated in Section 1 (and in Section 2.3.3), we compute the 25 coefficients given in Proposition 2.3.1. We have

$$\begin{aligned}
(F)^{p-1} &= \sum_{a+b+c=p-1} \binom{p-1}{a,b,c} (xyz^3)^a (sx^5)^b (ty^5)^c \\
&= \sum_{a+b+c=p-1} \binom{p-1}{a,b,c} (x^a y^a z^{3a})(s^b x^{5b})(t^c y^{5c}) \\
&= \sum_{a+b+c=p-1} s^b t^c \cdot \binom{p-1}{a,b,c} x^{a+5b} y^{a+5c} z^{3a} \qquad (2.1)
\end{aligned}$$

by the multinomial theorem. To express $(F)^{p-1}$ as a sum of the form

$$(F)^{p-1} = \sum_{(i,j,k)\in(\mathbb{Z}_{\geq 0})^{\oplus 3}} c_{i,j,k} x^i y^j z^k,$$

we consider the linear system

$$\begin{cases} a+b+c = p-1, \\ a+5b = i, \\ a+5c = j, \\ 3a = k, \end{cases} \qquad (2.2)$$

and put

$$S(i,j,k) := \{(a,b,c) \in [0,p-1]^{\oplus 3} : (a,b,c) \text{ satisfies (2.2)}\} \qquad (2.3)$$

for each $(i,j,k) \in (\mathbb{Z}_{\geq 0})^{\oplus 3}$. Using the notation $S(i,j,k)$, we have

$$(F)^{p-1} = \sum_{(i,j,k)\in(\mathbb{Z}_{\geq 0})^{\oplus 3}} \left(\sum_{(a,b,c)\in S(i,j,k)} s^b t^c \cdot \binom{p-1}{a,b,c} \right) x^i y^j z^k. \qquad (2.4)$$

2.3.1 Case of $p \equiv 2 \pmod 3$

We first consider the case of $p \equiv 2 \pmod 3$.

Lemma 2.3.2. *With notation as above, if $p \equiv 2 \pmod 3$, the coefficients of the monomials $x^i y^j z^{p-1}$ and $x^i y^j z^{2p-2}$ in $(F)^{p-1}$ are zero for all $(i,j) \in (\mathbb{Z}_{\geq 0})^{\oplus 2}$.*

Proof. Recall from (2.1) that the z-exponent of each monomial in $(F)^{p-1}$ is $3a$, which is divided by 3. On the other hand, the z-exponents of the monomials $x^i y^j z^{p-1}$ and $x^i y^j z^{2p-2}$ are $p-1$ and $2p-2$, which are congruent to 1 and 2 modulo 3 respectively. Thus their coefficients in $(F)^{p-1}$ are all zero. □

Let $\mathcal{M}$ be the set of the 25 monomials given in Proposition 2.3.1, and set

$$E(\mathcal{M}) := \{(i,j,k) \in (\mathbb{Z}_{\geq 0})^{\oplus 3} : x^i y^j z^k = m \text{ for some } m \in \mathcal{M}\},$$

which is the set of the exponent vectors of the monomials in $\mathcal{M}$.

Lemma 2.3.3. *Assume $p \equiv 2 \pmod 3$. If $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, then we have $S(i,j,k) = \emptyset$ for any $(i,j,k) \in E(\mathcal{M})$.*

Proof. Note that for each $(i,j,k) \in E(\mathcal{M})$, we have $i+j+k = 5(p-1)$, see Proposition 2.3.1. Using matrices, we write the system (2.2) as

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 5 & 0 \\ 1 & 0 & 5 \\ 3 & 0 & 0 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix} = \begin{pmatrix} p-1 \\ i \\ j \\ k \end{pmatrix}, \tag{2.5}$$

whose extended coefficient matrix is transformed as follows:

$$\begin{pmatrix} 1 & 1 & 1 & p-1 \\ 1 & 5 & 0 & i \\ 1 & 0 & 5 & j \\ 3 & 0 & 0 & k \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 & p-1 \\ 0 & 1 & -4 & -j+(p-1) \\ 0 & 0 & 15 & i+4j-5(p-1) \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Considering modulo 5, we have the following linear system over $\mathbb{F}_5$:

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \end{pmatrix} = \begin{pmatrix} p-1 \\ -j+(p-1) \\ i-j \\ 0 \end{pmatrix}. \tag{2.6}$$

Note that the system (2.6) over $\mathbb{F}_5$ has a solution if and only if $i - j \equiv 0 \pmod 5$. Assume $p \equiv 2 \pmod 3$. We claim that if $p \equiv 1 \pmod 5$ or if $p \equiv 4 \pmod 5$, the original system (2.5) over $\mathbb{Z}$ has no solution in $[0, p-1]^{\oplus 3}$ for any $(i,j,k) \in E(\mathcal{M})$. Indeed, if $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, and if the system (2.5) has a solution in $[0, p-1]^{\oplus 3}$ for some $(i,j,k) \in E(\mathcal{M})$, the system (2.6) has a solution. Since $p \equiv 2 \pmod 3$, it follows from Lemma 2.3.2 that $k \neq p-1$ and $k \neq 2p-2$, i.e., $k = 2p-1$ or $k = p-2$. Thus we may assume that (i,j,k) is either of the following:

$$(3p-2, p-1, p-2), \quad (3p-1, p-2, p-2), \quad (p-2, 3p-1, p-2), \quad (p-1, 3p-2, p-2),$$

$$(2p-2,2p-1,p-2),\quad (2p-1,2p-2,p-2),\quad (2p-3,p-1,2p-1),\quad (2p-1,p-3,2p-1),$$
$$(2p-2,p-2,2p-1),\quad (p-3,2p-1,2p-1),\quad (p-1,2p-3,2p-1),\quad (p-2,2p-2,2p-1).$$

The value $i-j$ takes $2p-1$, $2p+1$, $-2p-1$, $-2p+1$, -1, 1, $p-2$, $p+2$, p, $-p-2$ or $-p+2$, $-p$, each of which is not congruent to 0 modulo 5 if $p \equiv 1 \pmod 5$ or if $p \equiv 4 \pmod 5$. This is a contradiction. □

Proposition 2.3.4. *Assume $p \equiv 2 \pmod 3$. If $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, then the desingularization T_p of $V(F)$ is superspecial.*

Proof. It follows from Lemma 2.3.3 that the coefficient of $x^i y^j z^k$ in (2.4) is zero for each $(i,j,k) \in E(\mathcal{M})$. By Proposition 2.3.1, the desingularization of $V(F)$ is superspecial. □

It follows from the proof of Lemma 2.3.3 that (2.2) is equivalent to the following system:

$$\begin{cases} a+b+c = p-1, \\ b-4c = -j+(p-1), \\ 15c = i+4j-5(p-1). \end{cases} \tag{2.7}$$

Different from the case where $p \equiv 1 \pmod 5$ or $p \equiv 4 \pmod 5$, the desingularization of $V(F)$ is not superspecial if $p \equiv 3 \pmod 5$.

Lemma 2.3.5. *Assume $p \equiv 2 \pmod 3$. If $p \equiv 3 \pmod 5$, then we have $\#S(3p-2,p-1,p-2)=1$. In other words, the system (2.7) with $(i,j,k)=(3p-2,p-1,p-2)$ has a unique solution in $[0,p-1]^{\oplus 3}$. The solution is given by*

$$\begin{pmatrix} a, & b, & c \end{pmatrix} = \begin{pmatrix} (p-2)/3, & 4(2p-1)/15, & (2p-1)/15 \end{pmatrix}. \tag{2.8}$$

Note that $(p-2)/3$, $4(2p-1)/15$ and $(2p-1)/15$ are less than $p-1$.

Proof. The system to be solved with $(i,j,k)=(3p-2,p-1,p-2)$ is given by

$$\begin{cases} a+b+c = p-1, & (2.9) \\ b-4c = 0, & (2.10) \\ 15c = 2p-1 & (2.11) \end{cases}$$

with $(a,b,c) \in [0,p-1]^{\oplus 3}$. Note that $2p-1 \equiv 2\cdot 2-1 \equiv 0 \pmod 3$ and $2p-1 \equiv 2\cdot 3-1 \equiv 0 \pmod 5$, and thus $2p-1$ is divided by 15. We have $c=(2p-1)/15$ by (2.11) and $b=4c=4(2p-1)/15$ by (2.10). Since $b+c=(2p-1)/3$, it follows from (2.9) that $a=(p-2)/3$. □

Lemma 2.3.6. *Assume $p \equiv 2 \pmod 3$. If $p \equiv 3 \pmod 3$, then the coefficient of the monomial $x^{3p-2}y^{p-1}z^{p-2}$ in $(F)^{p-1}$ is not zero.*

Proof. Let $c_{3p-2,p-1,p-2}$ be the coefficient of $x^{3p-2}y^{p-1}z^{p-2}$ in $(F)^{p-1}$. Recall from (2.4) that $c_{3p-2,p-1,p-2}$ is given by

$$\sum_{(a,b,c)\in S(3p-2,p-1,p-2)} s^b t^c \cdot \binom{p-1}{a,b,c},$$

where $S(3p-2, p-1, p-2)$ is defined in (2.3). By Lemma 2.3.5, the set $S(3p-2, p-1, p-2)$ consists of only the element given by (2.8), and hence

$$c_{3p-2,p-1,p-2} = \frac{(p-1)!}{\left(\frac{p-2}{3}\right)!\left(\frac{4(2p-1)}{15}\right)!\left(\frac{2p-1}{15}\right)!},$$

which is not divisible by p. □

Proposition 2.3.7. *Assume $p \equiv 2 \pmod 3$. If $p \equiv 3 \pmod 5$, then the desingularization T_p of $V(F)$ is not superspecial.*

Proof. It follows from Lemma 2.3.6 that the coefficient of $x^{3p-2}y^{p-1}z^{p-2}$ in $(F)^{p-1}$ is not zero. By Proposition 2.3.1, the desingularization of $V(F)$ is not superspecial. □

2.3.2 Case of $p \equiv 1 \pmod 3$

Next, we consider the case of $p \equiv 1 \pmod 3$.

Lemma 2.3.8. *Assume $p \equiv 1 \pmod 3$. Then we have $\#S(2p-2, 2p-2, p-1) = 1$. In other words, the system (2.7) with $(i, j, k) = (2p-2, 2p-2, p-1)$ has a unique solution in $[0, p-1]^{\oplus 3}$. The solution is given by*

$$\begin{pmatrix} a, & b, & c \end{pmatrix} = \begin{pmatrix} (p-1)/3, & (p-1)/3, & (p-1)/3 \end{pmatrix}. \tag{2.12}$$

Proof. The system to be solved with $(i, j, k) = (2p-2, 2p-2, p-1)$ is given by

$$\begin{cases} a + b + c = p - 1, & (2.13) \\ b - 4c = -(p-1), & (2.14) \\ 15c = 5(p-1) & (2.15) \end{cases}$$

with $(a, b, c) \in [0, p-1]^{\oplus 3}$. Since $p - 1$ is divided by 3 from our assumption, it follows from (2.15) that $c = (p-1)/3$. By (2.14) and (2.13), we have $a = b = (p-1)/3$. □

Lemma 2.3.9. *Assume $p \equiv 1 \pmod 3$. Then the coefficient of the monomial $x^{2p-2}y^{2p-2}z^{p-1}$ in $(F)^{p-1}$ is not zero.*

Proof. Let $c_{2p-2,2p-2,p-1}$ be the coefficient of $x^{2p-2}y^{2p-2}z^{p-1}$ in $(F)^{p-1}$. Recall from (2.4) that $c_{2p-2,2p-2,p-1}$ is given by

$$\sum_{(a,b,c)\in S(2p-2,2p-2,p-1)} s^b t^c \cdot \binom{p-1}{a, b, c},$$

where $S(2p-2, 2p-2, p-1)$ is defined in (2.3). By Lemma 2.3.8, the set $S(2p-2, 2p-2, p-1)$ consists of only the element given by (2.12), and hence

$$c_{2p-2,2p-2,p-1} = \frac{(p-1)!}{\left(\frac{p-1}{3}\right)!\left(\frac{p-1}{3}\right)!\left(\frac{p-1}{3}\right)!},$$

which is not divisible by p. □

Proposition 2.3.10. *Assume* $p \equiv 1 \pmod 3$*. Then the desingularization* T_p *of* $V(F)$ *is not superspecial.*

Proof. It follows from Lemma 2.3.9 that the coefficient of $x^{2p-2}y^{2p-2}z^{p-1}$ in $(F)^{p-1}$ is not zero. By Proposition 2.3.1, the desingularization T_p of $V(F)$ is not superspecial. □

2.3.3 Proofs of the superspeciality of T_p

Theorem 1.1. *Let* (s,t) *be a pair of elements in* $\mathbb{F}_q^\times$*. Put* $F := xyz^3 + sx^5 + ty^5$*. Let* $V(F)$ *denote the projective zero-locus in* $\mathbf{P}^2 = \mathrm{Proj}(\overline{K}[x,y,z])$ *defined by* $F = 0$*. Then the desingularization* T_p *of* $V(F)$ *is a superspecial trigonal curve of genus* 5 *if and only if* $p \equiv 2 \pmod 3$ *and* $p \equiv 1, 4 \pmod 5$*.*

Proof. Since F is an irreducible quintic form over K, the desingularization T_p of $V(F)$ is a trigonal curve of genus 5 over K, see [18, Section 2]. The assertion follows from Propositions 2.3.4, 2.3.7 and 2.3.10. □

Corollary 2.3.11. *There exist superspecial trigonal curves of genus* 5 *in characteristic* p *for infinitely many primes* p*. The set of primes* p *for which* T_p *is superspecial has natural density* 1/4*.*

Proof. Note that $p \equiv 2 \pmod 3$ and $p \equiv 1 \pmod 5$ (resp. $p \equiv 2 \pmod 3$ and $p \equiv 4 \pmod 5$) is equivalent to $p \equiv 11 \pmod{15}$ (resp. $p \equiv 14 \pmod{15}$). Since both 11 and 14 are coprime to 15, it follows from Dirichlet's Theorem that there are infinitely many primes congruent to 11 or 14 modulo 15. Thus, the first claim follows from Theorem 1.1. The second claim is deduced from the fact that the natural density of primes equal to 11 or 14 modulo 15 is

$$\frac{1}{\varphi(15)} + \frac{1}{\varphi(15)} = \frac{1}{8} + \frac{1}{8} = \frac{1}{4},$$

where φ is Euler's totient function. □

Problem 2.3.12. *Does there exist a superspecial trigonal curve of genus* 5 *in characteristic* p *for each of the following case?*

(1) $p \equiv 1 \pmod 3$*. Cf. the non-existence for* $p = 7$ *(and* 13 *over* $\mathbb{F}_{13}$*) is already shown in* [18].

(2) $p \equiv 2 \pmod 3$ *and* $p \equiv 3 \pmod 5$*.*

2.4 Application: Finding maximal curves over $K = \mathbb{F}_{p^2}$ for large p

In the following, we set $K := \mathbb{F}_{p^2}$. It is known that any maximal or minimal curve over $\mathbb{F}_{p^2}$ is supersepcial. Conversely, any superspecial curve over an algebraically closed field descends to a maximal or minimal curve over $\mathbb{F}_{p^2}$, see the proof of [16, Proposition 2.2.1]. Under the condition given in Theorem 1.1, we computed the number of $\mathbb{F}_{p^2}$-rational points on T_p with $s = t = 1$ for $7 \leq p \leq 1000$ using a computer algebra system Magma [1]. Table 1 shows our computational results for $7 \leq p \leq 179$. We see from Table 1 that any superspecial T_p is maximal over $\mathbb{F}_{p^2}$ for $7 \leq p \leq 179$ (also for $180 \leq p \leq 1000$, but omit to write them in the table). From our computational results, let us give a conjecture on the existence of $\mathbb{F}_{p^2}$-maximal (trigonal) curves of genus 5.

- For any p with $p \equiv 2 \pmod 3$ and $p \equiv 1, 4 \pmod 5$, the desingularization T_p of $V(F)$ over $\mathbb{F}_{p^2}$ is maximal.

In the next subsection we prove this conjecture (in fact, the condition $p \equiv 2 \pmod 3$ and $p \equiv 1, 4 \pmod 5$) is a necessary and sufficient condition for the maximality of T_p).

Table 1: The number of $\mathbb{F}_{p^2}$-rational points on the desingularization T_p of $V(F)$ for $7 \leq p \leq 100$ with $p \equiv 2 \pmod 3$, where $F = xyz^3 + x^5 + y^5$. We denote by $\#T_p(\mathbb{F}_{p^2})$ the number of $\mathbb{F}_{p^2}$-rational points on T_p for each p.

p	p mod 5	S.sp. or not	$\#T_p(\mathbb{F}_{p^2})$	p	p mod 5	S.sp. or not	$\#T_p(\mathbb{F}_{p^2})$
11	1	S.sp.	232 (Max.)	89	4	S.sp.	8812 (Max.)
29	4	S.sp.	1132 (Max.)	101	1	S.sp.	11212 (Max.)
41	1	S.sp.	2092 (Max.)	131	1	S.sp.	18472 (Max.)
59	4	S.sp.	4072 (Max.)	149	4	S.sp.	23692 (Max.)
71	1	S.sp.	5752 (Max.)	179	4	S.sp.	33832 (Max.)

3 Main results

Let T_p denote the non-singular model of $x^5 + y^5 + xyz^3 = 0$. In this section, we prove that T_p is $\mathbb{F}_{p^2}$-maximal if and only if $p \equiv 2 \pmod 3$ and $p \equiv 1, 4 \pmod 5$. Furthermore, we give a family of $\mathbb{F}_{p^2}$-maximal curves defined by equations of a more general form.

3.1 Maximality of $T_p : x^5 + y^5 + xyz^3 = 0$

Theorem 1.2. *Let $V(F)$ denote the projective zero-locus in $\mathbf{P}^2$ defined by $F = xyz^3 + x^5 + y^5 = 0$. Then the desingularization T_p of $V(F)$ is an $\mathbb{F}_{p^2}$-maximal trigonal curve of genus 5 if and only if $p \equiv -1 \pmod{15}$ or $p \equiv 11 \pmod{15}$.*

Proof. First, we suppose that T_p is $\mathbb{F}_{p^2}$-maximal. Since an $\mathbb{F}_{p^2}$-maximal curve is superspecial, the curve T_p is superspecial. By Theorem 1.1, we have $p \equiv -1 \pmod{15}$ or $p \equiv 11 \pmod{15}$.

Conversely, assume $p \equiv -1 \pmod{15}$ or $p \equiv 11 \pmod{15}$. It suffices to show that T_p is covered by an $\mathbb{F}_{p^2}$-maximal curve. Note that we have $1 + y^5 + yz^3 = 0$ for $x = 1$.

Case of $p \equiv -1 \pmod{15}$. There exists an integer m such that $p + 1 = 15m$. It follows from the following morphism

$$\begin{cases} \mathcal{H}_{p+1} : 1 + Y^{p+1} + Z^{p+1} = 0 & \rightarrow \quad 1 + y^5 + yz^3 = 0 \\ \qquad (Y, Z) & \mapsto \quad \left(Y^{3m}, Y^{-m} Z^{5m}\right) \end{cases}$$

that T_p is covered by the maximal Hermitian curve $\mathcal{H}_{p+1}$. Thus T_p is also maximal over $\mathbb{F}_{p^2}$.

Case of $p \equiv 11 \pmod{15}$. In this case, there exists an integer m such that $p + 1 = 12 + 15m$. It follows from the following morphism

$$\begin{cases} \mathcal{H}_{p+1} : Y^p + Y = -Z^{p+1} & \rightarrow \quad 1 + y^5 = -yz^3 \\ \qquad (Y, Z) & \mapsto \quad \left(Y^{3m+2}, Y^{-(m+1)} Z^{5m+4}\right) \end{cases}$$

that T_p is covered by $\mathcal{H}_{p+1}$. Thus T_p is also maximal over $\mathbb{F}_{p^2}$.

□

3.2 A generalization of the maximal curve of the form $x^5 + y^5 + xyz^3 = 0$

More generally, we consider the homogeneous equation $x^a + y^a + z^b x^c y^c = 0$ for natural numbers a, b and c with $b + 2c = a$. Let $C_{p,a,b,c}$ be the non-singular model of $x^a + y^a + z^b x^c y^c = 0$. Note that $C_{p,a,b,c}$ has genus

$$\frac{1}{2}\left(ab - a + 2 - \gcd(b, a-c) - \gcd(b, c)\right).$$

Here, we give sufficient conditions under which $C_{p,a,b,c}$ is $\mathbb{F}_{p^2}$-maximal.

Theorem 1.3. *Let a, b and c be natural numbers with $b + 2c = a$. Put $n := ab/\gcd(a, b, c)$. Let $C_{p,a,b,c}$ be the non-singular model of $x^a + y^a + z^b x^c y^c = 0$. Then we have the following:*

(1) *The curve $C_{p,a,b,c}$ is maximal over $\mathbb{F}_{p^2}$ if $p \equiv -1 \pmod{n}$.*

(2) *Suppose that a and b are coprime. Since there exists an integer d such that $d \equiv 2 \pmod{a}$ and $d \equiv 0 \pmod{b}$, and since any two such d are congruent modulo ab, we fix such a d in the interval $[0, ab)$. Then the curve $C_{p,a,b,c}$ is maximal over $\mathbb{F}_{p^2}$ if $p \equiv d - 1 \pmod{n}$.*

Proof. It suffices to show that T_p is covered by an $\mathbb{F}_{p^2}$-maximal curve. For $x = 1$, we have $1 + y^a + z^b y^c = 0$.

(1) Assume $p \equiv n - 1 \pmod{n}$. There exists an integer m such that $p + 1 = nm$. It follows from the following morphism

$$\begin{cases} \mathcal{H}_{p+1} : 1 + Y^{p+1} + Z^{p+1} = 0 & \to \qquad 1 + y^a + z^b y^c = 0 \\ \qquad (Y, Z) & \mapsto \left(Y^{\frac{bm}{\gcd(a,b,c)}}, Y^{\frac{-cm}{\gcd(a,b,c)}} Z^{\frac{am}{\gcd(a,b,c)}}\right) \end{cases}$$

that $C_{p,a,b,c}$ is covered by the maximal Hermitian curve $\mathcal{H}_{p+1}$, and so is $\mathbb{F}_{p^2}$-maximal.

(2) Assume that a and b are coprime. Let d be a unique integer with $0 \leq d < ab$ such that $d \equiv 2 \pmod{a}$ and $d \equiv 0 \pmod{b}$. Note that cd and $a - 2c$ (resp. $c(d-2)$ and a) are divisible by b (resp. a). Since $\gcd(a, b) = 1$, the sum $cd + (a - 2c) = c(d-2) + a$ is divisible by ab. We also assume that $p \equiv d - 1 \pmod{n}$, and then there exists an integer m such that $p + 1 = nm + d$. It follows from the following morphism

$$\begin{cases} \mathcal{H}_{p+1} : Y^p + Y = -Z^{p+1} & \to \qquad 1 + y^a + z^b y^c = 0 \\ \qquad (Y, Z) & \mapsto \left(Y^{\frac{bm}{\gcd(a,b,c)} + \frac{d-2}{a}}, Y^{\frac{-cm}{\gcd(a,b,c)} - \frac{c(d-2)+a}{ab}} Z^{\frac{am}{\gcd(a,b,c)} + \frac{d}{b}}\right) \end{cases}$$

that $C_{p,a,b,c}$ is covered by the maximal Hermitian curve $\mathcal{H}_{p+1}$, and so is maximal over $\mathbb{F}_{p^2}$.

□

Now we can see that Theorem 1.2 is a special case of Theorem 1.3 for $(a, b, c) = (5, 3, 1)$ with $d = 15$.

Remark 3.2.1. We replace y and z in $1 + y^a + z^b y^c = 0$ with x and y respectively, say $1 + x^a + y^b x^c = 0$. It follows from $\gcd(a, b) = 1$ with $b + 2c = a$ that $\gcd(b, c) = 1$, and that a and b are odd numbers. There exist ℓ and k such that $kb + \ell c = 1$. Without loss of generality, we may assume

Table 2: Parameters for which $C_{p,a,b,c}$ are maximal and superspecial curves over $\mathbb{F}_{p^2}$. There are two cases listed in Theorem 1.3.

genus	congruence	(a, b, c)	case
4	$p \equiv 15 \pmod{16}$	$(8, 2, 3)$	case (1) with $n = 16$
	$p \equiv 9 \pmod{10}$	$(10, 2, 4)$	case (1) with $n = 10$
5	$p \equiv 14 \pmod{15}$ $p \equiv 11 \pmod{15}$	$(5, 3, 1)$	case (1) with $n = 15$ case (2) with $(n, d) = (15, 12)$
6	$p \equiv 13 \pmod{14}$	$(14, 2, 6)$	case (1) with $n = 14$
	$p \equiv 23 \pmod{24}$	$(12, 2, 5)$	case (1) with $n = 24$
7	$p \equiv 20 \pmod{21}$ $p \equiv 8 \pmod{21}$	$(7, 3, 2)$	case (1) with $n = 21$ case (2) with $(n, d) = (21, 9)$
	$p \equiv 8 \pmod{9}$	$(9, 3, 3)$	case (1) with $n = 9$
8	$p \equiv 31 \pmod{32}$	$(16, 2, 7)$	case (1) with $n = 32$
	$p \equiv 17 \pmod{18}$	$(18, 2, 8)$	case (1) with $n = 18$
9	$p \equiv 23 \pmod{24}$	$(6, 4, 1)$	case (1) with $n = 24$
10	$p \equiv 39 \pmod{40}$	$(20, 2, 9)$	case (1) with $n = 40$
	$p \equiv 21 \pmod{22}$	$(22, 2, 10)$	case (1) with $n = 22$
11	$p \equiv 32 \pmod{33}$ $p \equiv 23 \pmod{33}$	$(11, 3, 4)$	case (1) with $n = 33$ case (2) with $(n, d) = (33, 24)$
	$p \equiv 15 \pmod{16}$	$(8, 4, 2)$	case (1) with $n = 16$

$\ell < 0$ with $0 \leq -\ell < b$. One can check that $-\ell a + 2 \equiv 2 \pmod{a}$ and $-\ell a + 2 \equiv 0 \pmod{b}$ with $0 \leq -\ell a + 2 < ab$, and thus can take d to be $-\ell a + 2$. Considering $(x, y) \mapsto (x^{-\ell}, -y/x^k)$, we transform $1 + x^a + y^b x^c = 0$ into $y^b = x(1 + x^{-\ell a})$. Assume $p \equiv d - 1 \pmod{ab}$, i.e., $p \equiv -\ell a + 1 \pmod{ab}$. If $p \equiv -\ell a + 1 \pmod{-\ell ab}$, it follows from [25, Proposition 4.12] that the curve $\mathcal{C}(b, -\ell a + 1) : y^b = x^{-\ell a+1} + x$ is maximal over $\mathbb{F}_{p^2}$, and hence $1 + x^a + y^b x^c = 0$ is also maximal over $\mathbb{F}_{p^2}$.

3.3 Examples

There exists an $\mathbb{F}_{p^2}$-maximal and superspecial curve for each case in Table 2. Three concrete examples introduced below are constructed from parameters in Table 2. We also refer to [20] for the existence of (smooth) supersingular curves over $\overline{\mathbb{F}_p}$, and [13] for the existence of (non-hyperelliptic) superspecial curves of genus 4.

(1) The curve $C_{p,8,2,3}$ with $(a, b, c) = (8, 2, 3)$, given by $x^8 + y^8 + z^2 x^3 y^3 = 0$, is an $\mathbb{F}_{p^2}$-maximal superspecial curve of genus 4 if $p \equiv 15 \pmod{16}$, e.g., $p = 31, 47, 79, 127, 191$. Since $31 \equiv 1$

(mod 3) and $31 \equiv 1 \pmod 5$, the superspecial (and hence supersingular) curve $C_{31,8,2,3}$ is not obtained in [20, Theorems 1.1 and 5.5] nor [13, Theorem 3.1]. The existence of a superspecial curve of genus 4 for $p \equiv 1 \pmod 3$ is a positive answer to [13, Problem 3.3].

(2) For $(a, b, c) = (12, 2, 5)$, the curve $C_{p,12,2,5}$ with $x^{12} + y^{12} + z^2x^5y^5 = 0$ is an $\mathbb{F}_{p^2}$-maximal superspecial curve of genus 6 if $p \equiv 23 \pmod{24}$, e.g., $p = 23$, 47, 71, 167, 191. Since $191 \equiv 9 \pmod{13}$ and $191 \equiv 2 \pmod 7$, the superspecial (and thus supersingular) curve $C_{191,12,2,5}$ is not obtained in [20, Theorems 1.1 and 5.5].

(3) For $(a, b, c) = (7, 3, 2)$, the curve $C_{p,7,3,2}$ of genus 7 is $\mathbb{F}_{p^2}$-maximal and superspecial if $p \equiv 20 \pmod{21}$, e.g., $p = 41$, 83, 167 or if $p \equiv 8 \pmod{21}$, e.g., $p = 29$, 71, 113, 197. Note that except for $p = 29$, each p listed above does not satisfy any of congruences ($p \equiv 14$ mod 15 and $p \equiv 15$ mod 16) for $g = 7$ listed in [20, Theorems 1.1 and 5.5].

References

[1] Bosma, W., Cannon, J. and Playoust, C.: *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24**, 235–265 (1997)

[2] B. W. Brock, *Superspecial Curves of Genera Two and Three*, Princeton University (1993), Ph. D. Thesis.

[3] Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14** (1941), no. 1, 197–272.

[4] Ekedahl, T.: *On supersingular curves and abelian varieties*, Math. Scand. **60** (1987), 151–178.

[5] Fuhrmann R., Garcia, A., Torres, F.: *On maximal curves*, J. of Number Theory **67**, 29–51, 1997

[6] Hashimoto K.: *Class numbers of positive definite ternary quaternion Hermitian forms*, Proc. Japan Acad. Ser. A Math. Sci. **59** (1983), no. 10, 490–493.

[7] Hashimoto, K. and Ibukiyama, T.: *On class numbers of positive definite binary quaternion Hermitian forms. II*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 695–699 (1982).

[8] Ibukiyama, T.: *On rational points of curves of genus* 3 *over finite fields*, Tohoku Math. J. **45** (1993), 311–329.

[9] Ibukiyama, T. and Katsura, T.: *On the field of definition of superspecial polarized abelian varieties and type numbers*, Compositio Math. **91** (1994), no. 1, 37–46.

[10] Kawakita, M.: *Some sextics of genera five and seven attaining the Serre bound*, In: Proceedings of International Workshop on the Arithmetic of Finite Fields, WAIFI 2018, to appear in Lecture Notes in Computer Science, Springer, 2018, post-proceedings version is available at `http://www.waifi.org/documents/AcceptedPapers2018/S3-WAIFI_2018_paper_2.pdf`

[11] Kazemifard, A., Naghipour, A. R. and Tafazolian, S.: *A note on superspecial and maximal curves*, Bull. Iranian Math. Soc. **39** (2013), 405–413.

[12] Kazemifard, A., Tafazolian, S. and Torres, F.: *On maximal curves related to Chebyshev polynomials*, Finite Fields and Their Applications, **52**, 200–213, 2018.

[13] Kudo, M.: *On the existence of superspecial nonhyperelliptic curves of genus 4*, arXiv: 1804.09063 [math.AG], 2018.

[14] Kudo, M. and Harashita, S.: *Enumerating superspecial curves of genus* 4 *over prime fields*, arXiv: 1702.05313 [math.AG], 2017.

[15] Kudo, M. and Harashita, S.: *Enumerating Superspecial Curves of Genus* 4 *over Prime Fields* (abstract version of [14]), In: Proceedings of The Tenth International Workshop on Coding and Cryptography 2017 (WCC2017), September 18-22, 2017, Saint-Petersburg, Russia, available at `http://wcc2017.suai.ru/proceedings.html`

[16] Kudo, M. and Harashita, S.: *Superspecial curves of genus* 4 *in small characteristic*, Finite Fields and Their Applications, **45**, 131–169, 2017.

[17] Kudo, M. and Harashita, S.: *Superspecial Hyperelliptic Curves of Genus* 4 *over Small Finite Fields*, In: Proceedings of International Workshop on the Arithmetic of Finite Fields, WAIFI 2018, to appear in Lecture Notes in Computer Science, Springer, 2018, post-proceedings version is available at
`http://www.waifi.org/documents/AcceptedPapers2018/T2-WAIFI_2018_paper_15.pdf`

[18] Kudo, M. and Harashita, S.: *Superspecial trigonal curves of genus* 5, arXiv: 1804.11277 [math.AG], 2018.

[19] Lachaud, G.: *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 16, pp. 729–732.

[20] Li,W., Mantovan, E., Pries, R. and Tang, T.: *Newton polygons of cyclic covers of the projective line branched at three points*, arXiv: 1805.04598 [math.NT], 2018.

[21] Serre, J.-P.: *Nombre des points des courbes algebrique sur* $\mathbb{F}_q$, Sém. Théor. Nombres Bordeaux (2) 1982/83, 22 (1983).

[22] Tafazolian, S. and Torres, F.: *A note on certain maximal curves*, Communications in Algebra, **45** (2017), Issue 2, 764–773.

[23] Tafazolian, S.: *A note on certain maximal hyperelliptic curves*, Finite Fields and Their Applications, **18**, 1013–1016, 2012.

[24] Tafazolian, S. and Torres, F.: *On maximal curves of Fermat type*, Advances in Geometry, **13** (4), 613–617, 2013.

[25] Tafazolian, S. and Torres, F.: *On the curve* $y^n = x^m + x$ *over finite fields*, Journal of Number Theory, **145**, 51–66, 2014.

[26] Tafazolian, S. and Torres, F.: *On the curve* $y^n = x^\ell(x^m + 1)$ *over finite fields*, Advances in Geometry, 2018, DOI: https://doi.org/10.1515/advgeom-2017-0041.

[27] Xue, J., Yang, T.-C. and Yu, C.-F.: *On superspecial abelian surfaces over finite fields*, Doc. Math. **21** (2016) 1607–1643.