Counting isomorphism classes of superspecial curves (Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties)

AUTHOR(S):

KUDO, Momonari

CITATION:

KUDO, Momonari. Counting isomorphism classes of superspecial curves (Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties). 数理解析研究所講究録別冊 2022, B90: 77-95

ISSUE DATE:

2022-06

URL:

http://hdl.handle.net/2433/276274

RIMS Kôkyûroku Bessatsu
B90 (2022), 77–95

Counting isomorphism classes of superspecial curves

By

Momonari KUDO*

Abstract

A superspecial curve is a (non-singular) curve over a field of positive characteristic whose Jacobian variety is isomorphic to a product of supersingular elliptic curves over the algebraic closure. It is known that for given genus and characteristic, there exist only finitely many superspecial curves, up to isomorphism over an algebraically closed field. In this article, we give a brief survey on results of counting isomorphism classes of superspecial curves. In particular, this article summarizes some recent results in the case of genera four and five, obtained by the author and S. Harashita. We also survey results obtained in a joint work with Harashita and E. W. Howe, on the enumeration of superspecial curves in a certain class of non-hyperelliptic curves of genus four.

§ 1. Introduction

Throughout this article, by a curve we mean a non-singular projective variety of dimension one. A curve of genus g over a field K of characteristic $p > 0$ is said to be *superspecial* if $\mathrm{Jac}(C) \cong E^g$ (over the algebraic closure $\overline{K}$) for a supersingular elliptic curve E, where $\mathrm{Jac}(C)$ denotes the Jacobian variety of C. Note that this definition is well-defined by the following fact of Deligne, Ogus and Shioda (cf. [29, Theorem 3.5] or [25, Section 1.6, p. 13]): If $g \geq 2$, for any supersingular elliptic curves E_i for $1 \leq i \leq 2g$, we have $E_1 \times \cdots \times E_g \cong E_{g+1} \times \cdots \times E_{2g}$.

For a pair (g, p), we denote by $\Lambda_{g,p}$ the set of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus g over finite fields of characteristic $p > 0$. The cardinality $\#\Lambda_{g,p}$ is at most finite (zero is possible) by, e.g., a general fact that given an abelian variety A, there exist only finitely many (irreducible) curves D such that $\mathrm{Jac}(D) \cong A$, see [27,

Received December 31, 2020. Revised June 30, 2021.
2020 Mathematics Subject Classification(s): 14G15, 14G17, 14H45, 14Q05
Key Words: *Curves of low genera, Curves over finite fields, Superspecial curves*
Supported by JSPS Grant-in-Aid for Young Scientists 20K14301.
*Graduate School of Information Science and Technology, The University of Tokyo, Tokyo 113-8656, Japan.
e-mail: kudo@mist.i.u-tokyo.ac.jp

Corollary 1.2]. Ekedahl proved in [6, Theorem 1.1], which we will recall in Theorem 2.1 in this article, that if there exists a superspeical curve C of genus g over $\overline{\mathbb{F}_p}$, then we have $2g \leq p^2 - p$, and $2g \leq p - 1$ if C is hyperelliptic and $(g, p) \neq (1, 2)$.

The main problem which we consider in this article is:

Problem 1.1. Determine the number $\#\Lambda_{g,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus g over finite fields of characteristic $p > 0$. Moreover, find complete representatives of the isomorphism classes.

This article is a survey on results of counting the number of isomorphism classes of superspecial curves. For $g = 1$, Deuring [4] proved that $\#\Lambda_{1,p}$ is equal to the class number of a quaternion algebra. Also in the case of $g = 2, 3$, it follows from a general result by Ibukiyama-Katsura-Oort [14, Theorem 2.10] on superspecial principally polarized abelian varieties that $\#\Lambda_{g,p}$ is determined by computing the class numbers of quaternion hermitian lattices. These class numbers were explicitly computed by Eichler [5] for $g = 1$, Hashimoto-Ibukiyama [11] for $g = 2$, and Hashimoto [10] for $g = 3$ (cf. Igusa also computed the class number for $g = 1$ by directly counting the $\overline{\mathbb{F}_p}$-isomorphism classes of supersingular elliptic curves). We review these results for $g \leq 3$ in Section 2.

On the other hand, the problem for $g \geq 4$ has not been solved in all primes, but in recent years, the author and Harashita developed several algorithms to count genus-4 or genus-5 superspecial curves [19], [20], [21], [22]. Sections 3 and 4 describe our results (for small primes) obtained by these algorithms in the case of genus $g = 4, 5$. In Section 5, we also describe our most recent results obtained by a joint work with Harashita and Howe [23], where we presented algorithms to count (or find) superspecial curves among certain 2-dimensional families of genus-4 non-hyperelliptic curves.

Remark. As stated above, this article mainly focuses on the enumeration of superspecial curves of given genus, up to isomorphism over *an algebraically closed field*, i.e., counting $\overline{\mathbb{F}_p}$-isomorphism classes of such curves over $\overline{\mathbb{F}_p}$. On the other hand, we can also consider the enumeration up to isomorphism over *finite fields*, i.e., counting the number of K-isomorphism classes of superspecial curves over a finite field K. Note that it suffices for this to consider the case of $K = \mathbb{F}_p$ or $\mathbb{F}_{p^2}$ since the number of $\mathbb{F}_{p^a}$-isomorphism classes of superspecial curves over $\mathbb{F}_{p^a}$ depends on the parity of a (cf. [21, Proposition 2.3.1]). Main results in [19], [20], [21], [22] that will be stated in Sections 3 and 4 include those on the enumeration not only over $\overline{\mathbb{F}_p}$, but also over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

§ 2. The number of superspecial curves of genus one, two and three

Let p be a rational prime. At first, we recall Ekedahl's results in [6] including the field of definition of superspecial curves. The main theorem of [6] (Theorem 2.1 below) gives bounds on the existence of superspecial curves:

Theorem 2.1 ([6], Theorem 1.1)**.** *If there exists a superspecial curve C of genus g in characteristic p, then we have the following:*

1. $2g \leq p^2 - p$, *and*
2. $2g \leq p - 1$ *if C is hyperelliptic and $(g, p) \neq (1, 2)$.*

Ekedahl also showed in the proof of [6, Theorem 1.1] that any superspecial curve over an algebraically closed field descends to a maximal or minimal curve over $\mathbb{F}_{p^2}$, where a curve C of genus g over $\mathbb{F}_q$ is called *maximal* (resp. *minimal*) if the number of $\mathbb{F}_q$-rational points on C attains the Hasse-Weil upper bound $q + 1 + 2g\sqrt{q}$ (resp. the Hasse-Weil lower bound $q + 1 - 2g\sqrt{q}$). Conversely, it is known that any maximal or minimal curve over $\mathbb{F}_{p^2}$ is superspecial. Thus, for determining $\#\Lambda_{g,p}$, it suffices to count $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus g over $\mathbb{F}_{p^2}$. One more important fact showed in the proof of [6, Theorem 1.1] is that the existence of a superspecial curve over the prime field $\mathbb{F}_p$ implies that of maximal and minimal curves over $\mathbb{F}_{p^2}$.

In the following, we review results on the computation of $\#\Lambda_{g,p}$ for $g \leq 3$. Let h_p (resp. t_p) denote the class (resp. type) number of the quaternion algebra $B_{p,\infty}$ over $\mathbb{Q}$ ramified exactly at $\{p, \infty\}$. Deuring [4] showed that the computation of $\#\Lambda_{1,p}$ is reduced into that of the class number h_p.

Theorem 2.2 ([4])**.** *We have the following:*

1. *Every supersingular elliptic curve over $\overline{\mathbb{F}_p}$ has a model over $\mathbb{F}_{p^2}$, and $\#\Lambda_{1,p} = h_p$.*
2. *The number of elements in $\Lambda_{1,p}$ which have models defined over $\mathbb{F}_p$ is $2t_p - h_p$.*

Using results on computing h_p and t_p by Eichler [5], we have the following:

Theorem 2.3 ([4], [5])**.** *The number $\#\Lambda_{1,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of supersingular elliptic curves is equal to*

$$\frac{p-1}{12} + \frac{1 - \left(\frac{-1}{p}\right)}{4} + \frac{1 - \left(\frac{-3}{p}\right)}{3}$$

if $p > 3$, and one if $p = 2$ or 3.

Igusa [16] also proved the same result as in Theorem 2.3 by directly computing the number of supersingular j-invariants from the Legendre form $y^2 = x(x-1)(x-\lambda)$ of an elliptic curve. We also refer to [31, Proposition 4.4] for results on the number of $\mathbb{F}_q$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_q$.

For $g = 2$ and 3, determining $\#\Lambda_{g,p}$ is reduced into counting superspecial principally polarized abelian varieties (PPAV's for short) by the fact that any PPAV is the

Jacobian variety of a (possibly reducible) curve, see the main theorem of [28]. Here we recall a general result by Ibukiyama-Katsura-Oort [14, Theorem 2.10] on the number of superspecial principally polarized abelian varieties:

Theorem 2.4 ([14], Theorem 2.10)**.** *Let E be a supersingular elliptic curve over $\overline{\mathbb{F}_p}$. For $g \geq 2$, the number of principal polarizations on E^g up to automorphisms of E^g is equal to the class number $H_g = H_g(p,1)$ of the principal genus of the quaternion hermitian space $(B_{p,\infty})^g$.*

Counting superspecial curves of genus $g = 2, 3$ is done by removing the contribution of reducible curves. As is noted in [14, p. 145], the number of supersingular abelian surfaces with reducible principal polarization is equal to the number of pairs (E_i, E_j) of supersingular elliptic curves E_i and E_j with $i \leq j$, and thus we have the following result for $g = 2$:

Theorem 2.5 ([14], [11])**.** *The number $\#\Lambda_{2,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus two is equal to $H_2 - H_1(H_1+1)/2$. Using the computational result of H_2 by Hashimoto-Ibukiyama [11] together with Theorem 2.3, we have that*

$$\#\Lambda_{2,p} = \begin{cases} 0 & (p = 2, 3) \\ 1 & (p = 5) \\ \frac{p^3+24p^2+141p-166}{2880} - \frac{1-\left(\frac{-1}{p}\right)}{32} + \frac{1-\left(\frac{-2}{p}\right)}{8} + \frac{1-\left(\frac{-3}{p}\right)}{18} + \epsilon & (p \geq 7), \end{cases}$$

where $\epsilon = 4/5$ if $p \equiv 4 \pmod 5$, and zero otherwise.

The number of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves C of genus 2 such that C has a model over $\mathbb{F}_p$ is also computable, see [15, Section 1].

Similarly to the case of $g = 2$, we can compute the value of $\#\Lambda_{3,p}$, see [3, Theorem 3.10 (d)] for an explicit formula.

§ 3. Case of genus four

Different from the case of $g \leq 3$, for $g \geq 4$ the dimension of the moduli space of curves of genus g is strictly less than that of the moduli space of PPAV's of dimension g. This means that the theory of abelian varieties is not so effective for our purpose for $g \geq 4$. For this reason, the enumeration of superspecial curves of genus 4 has not been completed yet for every p, whereas some results for small and concrete p are known. In this section (resp. the next section), we survey results on the enumeration of superspecial curves of genus 4 (resp. 5). In particular, this section summarizes results in [19], [20] and [21], where the authors proposed computational approaches to enumerate superspecial curves of genus 4.

Let C be a curve of genus 4. We recall that C is either of the following two types (cf. [9, Chap. IV, Example 5.2.2]):

1. *Hyperelliptic.* The normalization of the plane curve $y^2 = f(x)$, where $f(x)$ is a separable polynomial of degree 9 or 10.

2. *Canonical.* A complete intersection of quadratic and cubic hypersurfaces in $\mathbb{P}^3$.

Recall from the paragraph just after Theorem 2.1 that, for counting superspecial curves in characteristic $p > 0$, it suffices to count $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves over $\mathbb{F}_{p^2}$.

First, we consider the case where C is a non-hyperelliptic curve over a finite field $K = \mathbb{F}_q$ with $q = p$ or p^2 for $p \geq 5$, and give a summary of results in [19] and [21]. As a canonical curve, C is defined in the 3-projective space $\mathbb{P}^3 = \mathrm{Proj}(\overline{K}[x, y, z, w])$ by an irreducible quadratic form Q and an irreducible cubic form P in $\overline{K}[x, y, z, w]$, see [9, Chapter IV, Example 5.2.2]. As showed in [19, Section 2.1], we may assume that any coefficient of Q and P belongs to K. By the classification theory of quadratic forms over finite fields, we can transform Q into either of **(N1)** $2xw + 2yz$, **(N2)** $2xw + y^2 - \epsilon z^2$ for $\epsilon \in K^\times \setminus (K^\times)^2$ and **(Dege)** $2yw + z^2$ (cf. [19, Remark 2.1.1]).

Here we recall a criterion on the superspecialty of $C = V(Q, P)$ in Proposition 3.1 below. The proof is done by computing the Hasse-Witt matrix of C, which represents the Frobenius on the first cohomology group $H^1(C, \mathcal{O}_C)$. Each entry of the Hasse-Witt matrix of C is one of the 16 coefficients in $(QP)^{p-1}$ given in Proposition 3.1.

Proposition 3.1 ([19], Corollary 3.1.6)**.** *With notation as above, C is superspecial if and only if the coefficients of $x^{pi-i'}y^{pj-j'}z^{pk-k'}w^{p\ell-\ell'}$ in $(QP)^{p-1}$ are equal to 0 for all positive integers $i, j, k, \ell, i', j', k', \ell'$ with $i + j + k + \ell = i' + j' + k' + \ell' = 5$.*

Based on Proposition 3.1, we have a computational strategy to enumerate superspecial non-hyperelliptic curves of genus 4 over K:

Strategy 3.2.

1. For each of the three types (**(N1)**, **(N2)** and **(Dege)**) of Q, collect superspecial curves $V(Q, P)$ as follows:

   (a) Collect cubic forms $P \in K[x, y, z, w]$ such that HW-matrix = 0, i.e., the 16 coefficients in $(QP)^{p-1}$ given in Proposition 3.1 are all zero.

   (b) For each P collected in (a), test whether $V(Q, P)$ is non-singular or not.

2. For the superspecial curves $V(Q, P)$ collected in Step 1, compute their isomorphism classes.

Both of Step 1 (a), (b) and Step 2 are done with Gröbner basis computation. We here focus on Step 1 (a) and Step 2, and give their brief descriptions. Note that Step 1 (b) is done by a general method for the non-singularity test, see e.g., [19, Section 3.2].

Step 1 computes the solutions of multivariate systems HW-matrix $= 0$ with respect to unknown coefficients in P. Naively, P has 20 unknowns, but in fact, the dimension of the moduli space of non-hyperelliptic curves of genus 4 is 9. Thus it requires to reduce the number of unknowns as much as possible, since the number deeply affects the computational cost of solving multivariate systems. The author and Harashita [19, Section 4], [21, Section 3] reduced the number by considering the action of elements in the orthogonal similitude group $\tilde{\mathrm{O}}_\varphi(K)$ to the cubic form P, where φ is the symmetric matrix associated to Q. Note that they realized elements in $\tilde{\mathrm{O}}_\varphi(K)$ by computing the Bruhat decomposition of $\tilde{\mathrm{O}}_\varphi(K)$, see [19, Section 3] for more details.

In Lemmas 3.3 – 3.5 below, we collect the reduced form of P for each of the three types of Q.

Lemma 3.3 ([21], Lemma 3.4.1)**.** *Let $Q = 2xw + 2yz$, and φ the symmetric matrix associated to Q. An element of $\tilde{\mathrm{O}}_\varphi(K)$ transforms P into the following form:*

$$\begin{aligned}(y + b_1z)x^2 + b_2xz^2 + a_1y^3 + a_2y^2z + a_3yz^2 + a_4z^3\\ + (a_5y^2 + a_6yz + a_7z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3\end{aligned} \tag{3.1}$$

for $a_i \in K$ and for $b_1 \in \{0\} \cup K^\times/(K^\times)^2$ and $b_2 \in \{0, 1\}$.

Lemma 3.4 ([21], Lemma 3.5.1)**.** *Let $Q = 2xw + y^2 - \epsilon z^2$ for $\epsilon \in K^\times$ with $\epsilon \notin (K^\times)^2$. An element of $\tilde{\mathrm{O}}_\varphi(K)$ transforms P into the following form:*

$$\begin{aligned}(a_1y + a_2z)x^2 + a_3(y^2 - \epsilon z^2)x + b_1y(y^2 - \epsilon z^2) + a_4y(y^2 + 3\epsilon z^2)\\ + a_5z(3y^2 + \epsilon z^2) + (a_6y^2 + a_7yz + b_2z^2)w + (a_8y + a_9z)w^2 + a_{10}w^3\end{aligned} \tag{3.2}$$

for some $a_i \in K$ with $(a_1, a_2) \neq (0, 0)$ and for $b_1, b_2 \in \{0, 1\}$.

Lemma 3.5 ([21], Lemma 3.6.1)**.** *Let $Q = 2yw + z^2$, and φ the symmetric matrix associated to Q. An element of $\tilde{\mathrm{O}}_\varphi(K)$ transforms P into the following form* (3.3) *if $\#K > 5$, and into either of the following forms* (3.3) *and* (3.4) *if $\#K = 5$:*

$$\begin{aligned}a_0x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw)x\\ + a_6y^3 + a_7z^3 + a_8w^3 + a_9yz^2 + b_1z^2w + b_2zw^2,\end{aligned} \tag{3.3}$$

for some $a_i \in K$ with $a_0, a_6 \in K^\times$ and for $b_1, b_2 \in \{0, 1\}$, where the leading coefficient of $R := a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + a_5zw$ is 1 or $R = 0$;

$$x^3 + (a_1y^2 + a_2z^2 + a_3w^2 + a_4yz + b_1zw)x + y^2z + zw^2 \tag{3.4}$$

for $a_i \in K = \mathbb{F}_5$ and $b_1 \in \{0, 1\}$.

Thus Step 1 (a) of Strategy 3.2 is done by: For each of the three types of Q, collect P in the corresponding reduced form given in Lemma 3.3 for **(N1)**, Lemma 3.4 for **(N2)** and Lemma 3.5 for **(Dege)** such that HW-matrix $= 0$.

We next consider Step 2 of Strategy 3.2, i.e., how to decide whether two non-hyperelliptic curves of genus 4 are isomorphic or not over k, where $k = K$ or $\overline{K}$. Let $C_1 = V(Q_1, P_1)$ and $C_2 = V(Q_2, P_2)$ be non-hyperelliptic curves of genus 4 over k. If there exists an isomorphism over k from C_1 to C_2, the quadratic forms Q_1 and Q_2 are equivalent over k. Hence it suffices to consider the case of $Q_1 = Q_2$, say Q. Let φ be the symmetric matrix associated to Q. As is described in [19, Section 6.1], the two curves C_1 and C_2 are k-isomorphic if and only if there exist $g \in \tilde{\mathrm{O}}_\varphi(k)$ and $\lambda \in k^\times$ such that $g \cdot P_1 \equiv \lambda P_2 \bmod Q$. Using the Bruhat decomposition of $\tilde{\mathrm{O}}_\varphi(k)$ given in [19, Section 3], we reduce the (non-)existence of such g and λ into that of solutions over k of multivariate systems, see [21, Section 4.2] for more details including concrete algorithms to test the (non)-existence of such solutions.

In [19, Section 5] and [21, Section 4], the authors wrote down explicit algorithms for Strategy 3.2, and implemented them over Magma [1]. To implement Step 1 (a), they adopted the hybrid method [2], which combines the Gröbner basis computation with the brute force on some unknown coefficients in P. In Theorem 3.6 below, we collect main results in [19] and [21] obtained by executing proposed algorithms over Magma.

Theorem 3.6.

1. *([19, Theorem A]) Any superspecial curve of genus* 4 *over* $\mathbb{F}_{5^2}$ *is* $\mathbb{F}_{5^2}$*-isomorphic to* $2yw + z^2 = x^3 + a_1y^3 + a_2w^3 + a_3zw^2 = 0$ *in* $\mathbb{P}^3$*, where* $a_1, a_2 \in \mathbb{F}_{5^2}^\times$ *and* $a_3 \in \mathbb{F}_{5^2}$*.*
2. *([19, Corollary 5.1.1]) All superspecial curves of genus* 4 *in characteristic* 5 *are isomorphic to each other over an algebraically closed field.*
3. *([21, Theorem A] and [19, Example 6.2.4]) There exist exactly seven (resp.* 21*) superspecial curves of genus* 4 *over* $\mathbb{F}_5$ *(resp.* $\mathbb{F}_{25}$*) up to isomorphism over* $\mathbb{F}_5$ *(resp.* $\mathbb{F}_{25}$*).*
4. *([19, Theorem B]) There is no superspecial curve of genus* 4 *in characteristic* 7*.*
5. *([21, Theorem B]) There exist exactly* 30 *(resp. nine) non-hyperelliptic superspecial curves of genus* 4 *over* $\mathbb{F}_{11}$ *up to isomorphism over* $\mathbb{F}_{11}$ *(resp.* $\overline{\mathbb{F}_{11}}$*).*

Second, we consider the case where C is hyperelliptic, and give a summary of results in [20]. In general, a hyperelliptic curve H over K is realized as the desingularization of the homogenization of $y^2 = f(x)$, where $f(x)$ is a polynomial over K with non-zero discriminant. In [20, Section 3.2], the authors gave a reduction of a defining equation of H so that the set of all the ramification points of the reduced model is defined over K:

Lemma 3.7 ([20], Lemma 2)**.** *Assume that p and $2g+2$ are coprime. Let $\epsilon \in K^\times \smallsetminus (K^\times)^2$. Any hyperelliptic curve H of genus g over K is the desingularization of the homogenization of*

$$cy^2 = x^{2g+2} + bx^{2g} + a_{2g-1}x^{2g-1} + \cdots + a_1 x + a_0$$

for $a_i \in K$ for $i = 0, 1, \ldots, 2g-1$ where $b = 0, 1, \epsilon$ and $c = 1, \epsilon$.

We also recall a criterion on the superspecialty of the hyperelliptic curve H of genus g in Corollary 3.8 below. This criterion comes from a well-known explicit formula for the Cartier-Manin matrix of H (cf. [32]), which represents the Cartier operator on the space $H^0(H, \Omega^1_H)$ of regular differential forms on H.

Corollary 3.8 ([20], Corollary 1)**.** *Let H be a hyperelliptic curve $y^2 = f(x)$ of genus g over K, where $\deg(f) = 2g+1$ or $2g+2$. Then H is superspecial if and only if the coefficients of x^{pi-j} in $f^{(p-1)/2}$ are equal to 0 for all pairs of integers with $1 \leq i, j \leq g$.*

Here we also describe a method given in [20, Section 3.3] to test whether two hyperelliptic curves $C_1 : c_1 y^2 = f_1(x)$ and $C_2 : c_2 y^2 = f_2(x)$ with $c_1, c_2 \in K^\times$ of genus g are isomorphic or not over $k = K$ or $\overline{K}$, where f_i is a separable polynomial in $K[x]$ of degree $2g+2$ for each $1 \leq i \leq 2$. Let F_i be the homogenization of f_i with respect to an extra variable z for each $1 \leq i \leq 2$. Recall from [20, Lemma 1] that $C_1 \cong C_2$ over k if and only if there exist $h \in \mathrm{GL}_2(k)$ and $\lambda \in k^\times$ such that $h \cdot F_1 = \lambda^2 F_2$. Regarding entries of h and λ as variables, we reduce the (non-)existence of such h and λ into that of a solution over k of a multivariate system, see [20, Section 3.3] for more details including concrete algorithms to test the (non)-existence of such a solution.

Combining Lemma 3.7 and Corollary 3.8 with the isomorphism test described as above, we can construct a strategy similar to Strategy 3.2 for enumerating superspecial hyperelliptic curves of genus g over K, see [20, Section 3] for concrete algorithms. The authors of [20] implemented the algorithms over Magma, and executed them for $g = 4$ with $q = 11, 11^2, 13, 13^2, 17, 17^2, 19$. Theorem 3.9 below collects main results in [20].

Theorem 3.9.

1. *([20, Theorem 1]) There is no superspecial hyperelliptic curve of genus 4 in characteristic 11 and 13.*
2. *([20, Theorem 2]) There exist precisely 5 (resp. 25) superspecial hyperelliptic curves of genus 4 over $\mathbb{F}_{17}$ (resp. $\mathbb{F}_{17^2}$) up to isomorphism over $\mathbb{F}_{17}$ (resp. $\mathbb{F}_{17^2}$). Moreover, there exist precisely 2 superspecial hyperelliptic curves of genus 4 over the algebraic closure in characteristic 17 up to isomorphism.*

3. *([20, Theorem 3]) There exist precisely* 12 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$ *up to isomorphism over* $\mathbb{F}_{19}$*. Moreover, there exist precisely* 2 *superspecial hyperelliptic curves of genus* 4 *over* $\mathbb{F}_{19}$ *up to isomorphism over the algebraic closure.*

Table 1 summarizes known values of the number $\#\Lambda_{4,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus 4 in characteristic p. The non-existence of non-hyperelliptic (resp. hyperelliptic) superspecial curves of genus 4 for $p \leq 3$ (resp. $p \leq 7$) is deduced from Ekedahl's bounds given in Theorem 2.1. The number written in bold type is determined by our theorems (Theorems 3.6 and 3.9) described in this section. The notation '**H**' and '**C**' denote the hyperelliptic and canonical cases respectively. The number written in each bracket is the number of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves C such that C has a model over $\mathbb{F}_p$.

Table 1. Known values of the number $\#\Lambda_{4,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus 4 in characteristic p.

p	2	3	5	7	11	13	17	19	≥ 23
H	0	0	0	0	**0**	**0**	**2** (**2**)	? (**2**)	?
C	0	0	**1** (**1**)	**0**	? (**9**)	?	?	?	?
$\#\Lambda_{4,p}$	0	0	**1** (**1**)	**0**	? (**9**)	?	?	?	?

We close this section with open problems in the enumeration of superspecial curves of genus four:

Problem 3.10 (Genus four)**.** Determine the number of K or $\overline{K}$-isomorphism classes of superspecial curves of genus four over K in the following cases:

1. Canonical case over $K = \mathbb{F}_p$ for $p \geq 13$ or over $K = \mathbb{F}_{p^2}$ for $p \geq 11$.
2. Hyperelliptic case over $K = \mathbb{F}_p$ for $p \geq 23$ or over $K = \mathbb{F}_{p^2}$ for $p \geq 19$.

§ 4. Case of genus five

First, we recall that a curve of genus 5 is either of the following three types:

1. *Hyperelliptic.* The normalization of the plane curve $y^2 = f(x)$, where $f(x)$ is a separable polynomial of degree 11 or 12.
2. *Trigonal.* A curve C such that there exists a morphism $C \to \mathbb{P}^1$ of degree 3.

3. *Generic (canonical and non-trigonal).* A complete intersection of three quadric in $\mathbb{P}^4$.

In this paper, we say that a curve of genus 5 is "generic" if it is canonical and non-trigonal.

As for the non-existence of superspecial curves of genus 5, it follows from Ekedahl's bound given in Theorem 2.1 that there is no superspecial curve of genus 5 in characteristic $p = 2$, 3. The non-existence holds also for $p = 5$. Indeed, by [19, Lemma 2.2.1], if there were a superspecial curve of genus 5 in characteristic 5, then there would exist a maximal curve of genus 5 over $\mathbb{F}_{5^2}$, which contradicts the fact due to Fuhrmann and Torres [7] that if there exists a maximal curve of genus g over $\mathbb{F}_{p^2}$, then $4g \leq (p-1)^2$ or $2g = p^2 - p$. For $p \geq 7$, there is no result that shows the non-existence in the canonical case. The problem of counting superspecial curves of genus 5 is left for $p \geq 11$ in the hyperelliptic case, and for $p \geq 7$ in the canonical case.

This section briefly describes results in [22], where the authors enumerated superspecial trigonal curves of genus $g = 5$ over finite fields $\mathbb{F}_{p^a}$ for any a if $p \leq 7$ and for odd a if $p \leq 13$. Recall from [19, Proposition 2.3.1] that it suffices to study the case of $a = 1$, 2 if $p \leq 7$ and the case of $a = 1$ if $p \leq 13$.

Let C be a trigonal curve of genus 5 over a finite field $K = \mathbb{F}_q$, where $q = p$ or p^2 with $p \geq 5$. It is shown in [22, Section 2] that C is the normalization of a plane quintic $C' = V(F) \subset \mathbb{P}^2$ with a unique singular point for some quintic form $F \in K[x, y, z]$. The quintic forms defining our curves are divided into the following three types: **(Split node case)** $F = xyz^3 + f$, **(Non-split node case)** $F = (x^2 - \epsilon y^2)z^3 + f$ with $\epsilon \in K \smallsetminus (K^\times)^2$, **(Cusp case)** $F = x^2z^3 + f$, where f is the sum of monomial terms which can not be divided by z^3. Specifically, we have the reduced forms of F in Propositions 4.1 – 4.3 below. In the following, let ζ be a primitive element of $K^\times$, and ϵ an element of $K^\times \smallsetminus (K^\times)^2$.

Proposition 4.1 ([22], Proposition 3.1.1)**.** *Any trigonal curve of genus* 5 *over* K *in* **(Split node case)** *has a quintic model in* $\mathbb{P}^2$ *of the form* (4.1) *or* (4.2)*:*

$$\begin{aligned} F = {} & xyz^3 + (x^3 + b_1y^3)z^2 + (a_1x^4 + a_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ & + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5, \end{aligned} \tag{4.1}$$

for $a_i \in K$*, where* $b_1 \in \{0, 1\}$ *if* $q \equiv 2 \bmod 3$ *and* $b_1 \in \{0, 1, \zeta\}$ *if* $q \equiv 1 \bmod 3$.

$$\begin{aligned} F = {} & xyz^3 + (c_1x^4 + c_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ & + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5. \end{aligned} \tag{4.2}$$

for $(c_1, c_2) = (0, 0), (1, 0), (0, 1), (1, 1), (1, \zeta)$ *and for* $a_i \in K$.

Proposition 4.2 ([22], Proposition 3.2.1)**.** *Any trigonal curve of genus* 5 *over* K *in* **(Non-split node case)** *has a quintic model in* $\mathbb{P}^2$ *of the form* (4.3), (4.4) *or* (4.5)*:*

$$\begin{aligned} F = {} & (x^2 - \epsilon y^2)z^3 + \{x(x^2 + 3\epsilon y^2) + by(3x^2 + \epsilon y^2)\}z^2 \\ & + (a_1x^4 + a_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ & + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5, \end{aligned} \tag{4.3}$$

for $a_i \in K$*, where* $b = 0$ *if* $q \not\equiv -1 \bmod 3$ *and otherwise* b *has three possibilities determined by the condition that* $(1, b)$ *is parallel to* $(1, 0)A$ *for a representative* A *of* $\tilde{\mathrm{C}}/\tilde{\mathrm{C}}^3$ *(for example* $b = 0, 6, 10$ *if* $q = 11$*), where*

$$\tilde{\mathrm{C}} = \left\{ \begin{pmatrix} r & \epsilon s \\ s & r \end{pmatrix} \middle| \, (r, s) \in K^2, \ (r, s) \neq (0, 0) \right\}.$$

$$\begin{aligned} F = {} & (x^2 - \epsilon y^2)z^3 + (cx^4 + a_2x^3y + a_3x^2y^2 + a_4xy^3 + a_5y^4)z \\ & + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5. \end{aligned} \tag{4.4}$$

for $c = 1, \zeta$ *and for* $a_i \in K$*.*

$$F = (x^2 - \epsilon y^2)z^3 + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + a_{10}xy^4 + a_{11}y^5. \tag{4.5}$$

for $a_i \in K$*.*

Proposition 4.3 ([22], Proposition 3.3.1)**.** *Any trigonal curve of genus* 5 *over* K *in* **(Cusp case)** *has a quintic model in* $\mathbb{P}^2$ *of the form* (4.6)*:*

$$\begin{aligned} F = {} & x^2z^3 + a_1y^3z^2 + (a_2x^4 + a_3x^3y + a_4x^2y^2 + b_1xy^3 + a_5y^4)z \\ & + a_6x^5 + a_7x^4y + a_8x^3y^2 + a_9x^2y^3 + b_2xy^4 + a_{10}y^5 \end{aligned} \tag{4.6}$$

for $a_i \in K$ $(i = 1, \ldots, 10)$ *with* $a_1 \neq 0$*, where* $b_1 \in \{0, 1\}$ *and* $b_2 \in \{0, 1\}$*.*

Here we recall a criterion on the superspecialty of the trigonal curve C of genus 5 in Proposition 4.4 below. For the proof, see [22, Section 2.2], where the authors computed the Hasse-Witt matrix of C.

Proposition 4.4 ([22], Corollary 2.2.2)**.** *With notation as above,* C *is superspecial if and only if the coefficients of the monomials* $x^{pi-i'}y^{pj-j'}z^{pk-k'}$ *in* F^{p-1} *are equal to zero, where* (i, j, k) *and* (i', j', k') *run through* $(3, 1, 1), (1, 3, 1), (2, 2, 1), (2, 1, 2), (1, 2, 2)$*.*

Here we also describe a method given in [22, Section 5.1] to test whether two trigonal curves of genus 5 are k-isomorphic or not, where $k = K$ or $\overline{K}$. Let C_1 and C_2 be trigonal curves of genus 5 over K, and let $V(F_1)$ and $V(F_2)$ be the associate quintics

in $\mathbb{P}^2$. Recall from [22, Lemma 2.1.2] that $C_1 \cong C_2$ over k is equivalent to $V(F_1) \cong V(F_2)$ over k, i.e., there exist $M \in \mathrm{GL}_3(k)$ and $\lambda \in k^\times$ such that $M \cdot F_1 = \lambda F_2$. Regarding entries of M and λ as variables, we reduce the (non-)existence of such M and λ into that of a solution over k of a multivariate system, see [22, Section 5.1] for more details including concrete algorithms to test the (non)-existence of such a solution.

Combining Propositions 4.1 – 4.4 with the isomorphism test described as above, we can construct a strategy similar to Strategy 3.2 for enumerating superspecial trigonal curves of genus 5 over K, see [22, Section 4] for concrete algorithms. In Theorem 4.5 below, we collect main results in [22] obtained by executing the algorithms over Magma.

Theorem 4.5.

1. *([22, Theorem A]) There is no superspecial trigonal curve of genus* 5 *in characteristic* 7*.*

2. *([22, Theorem B]) Any superspecial trigonal curve of genus* 5 *over* $\mathbb{F}_{11}$ *is* $\mathbb{F}_{11}$*-isomorphic to the normalization of*

$$xyz^3 + a_1x^5 + a_2y^5 = 0 \tag{4.7}$$

in $\mathbb{P}^2$*, where* $a_1, a_2 \in \mathbb{F}_{11}^\times$*, or the normalization of*

$$(x^2 - 2y^2)z^3 + ax^5 + bx^4y + (9a)x^3y^2 + 4bx^2y^3 + (9a)xy^4 + 3by^5 = 0 \tag{4.8}$$

in $\mathbb{P}^2$*, where* $(a, b) \in (\mathbb{F}_{11})^{\oplus 2} \smallsetminus \{(0, 0)\}$*.*

3. *([22, Proposition 5.1.1 (I)]) There exist precisely four* $\mathbb{F}_{11}$*-isomorphism classes of superspecial trigonal curves of genus* 5 *over* $\mathbb{F}_{11}$*. Representatives of the four isomorphism classes are given by the normalization* C_i *of* $C_i' = V(F_i) \subset \mathbb{P}^2$*, where*

$$\begin{aligned} F_1 &= xyz^3 + x^5 + y^5, \\ F_2 &= xyz^3 + 2x^5 + y^5, \\ F_3 &= xyz^3 + 3x^5 + y^5, \\ F_4 &= (x^2 - 2y^2)z^3 + x^5 + 9x^3y^2 + 9xy^4. \end{aligned}$$

4. *([22, Proposition 5.1.1 (II)]) There exists a unique* $\overline{\mathbb{F}_{11}}$*-isomorphism class of superspecial trigonal curves of genus* 5 *over* $\mathbb{F}_{11}$*. A representative of the unique isomorphism class is given by the normalization* $C^{(\mathrm{alc})}$ *of the singular curve* $C^{(\mathrm{alc})'} = V(F) \subset \mathbb{P}^2$ *with* $F = xyz^3 + x^5 + y^5$*.*

5. *([22, Theorem C]) There is no superspecial trigonal curve of genus* 5 *over* $\mathbb{F}_{13}$*.*

In Table 2, we summarize known values of the number $\#\Lambda_{5,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus 5 in characteristic p. As described at the beginning of this section, there is no superspecial non-hyperelliptic (resp. hyperelliptic) curve of genus 5 for $p \leq 5$ (resp. $p \leq 7$). The number written in bold type is determined by our theorem (Theorems 4.5) described in this section. The notation '**H**', '**T**' and '**G**' denote the hyperelliptic, trigonal, generic (canonical and non-trigonal) cases respectively. The number written in each bracket is the number of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves C such that C has a model over $\mathbb{F}_p$.

Table 2. Known values of the number $\#\Lambda_{5,p}$ of $\overline{\mathbb{F}_p}$-isomorphism classes of superspecial curves of genus 5 in characteristic p.

p	2	3	5	7	11	13	17	19	≥ 23
H	0	0	0	0	?	?	?	?	?
T	0	0	0	**0**	? (**1**)	? (**0**)	?	?	?
G	0	0	0	?	?	?	?	?	?
$\#\Lambda_{5,p}$	0	0	0	?	?	?	?	?	?

We close this section with open problems in the enumeration of superspecial curves of genus five:

Problem 4.6 (Genus five)**.** Determine the number of K or $\overline{K}$-isomorphism classes of superspecial curves of genus five over K in the following cases:

1. Hyperelliptic case over $K = \mathbb{F}_p$ or over $K = \mathbb{F}_{p^2}$ for $p \geq 11$.
2. Trigonal case over $K = \mathbb{F}_p$ for $p \geq 17$ or over $K = \mathbb{F}_{p^2}$ for $p \geq 11$.
3. Generic (canonical and non-trigonal) case over $K = \mathbb{F}_p$ or over $K = \mathbb{F}_{p^2}$ for $p \geq 7$.

§ 5. Enumeration of certain genus-four superspecial curves

While our papers [19] and [21] (resp. [20]) enumerate superspecial curves among the *whole* space of non-hyperelliptic (resp. hyperelliptic) curves of genus 4, the paper [23] enumerates those among a certain family of non-hyperelliptic curves of genus 4, that is, *Howe curves*. In [12], these curves were first studied in order to quickly construct

genus-4 curves with many rational points, and also they heuristically tend to be superspecial. It was also proved in [24] that there exists a supersingular Howe curve in every characteristic $p > 3$.

In this section, we briefly describe results of [23], where the authors present computational methods ((A), (B) and (C) below) for enumerating superspecial Howe curves. We start with recalling the definition of a Howe curve. Throughout this section, let K be an algebraically closed field of characteristic $p \neq 2$.

Definition 5.1. A *Howe curve* over K is a curve which is isomorphic to the normalization of the fiber product $E_1 \times_{\mathbb{P}^1} E_2$ of two genus-1 double covers $E_i \to \mathbb{P}^1$ ramified over S_i, where each S_i consists of 4 points and where $\#(S_1 \cap S_2) = 1$.

The superspeciality of a Howe curve is reduced into that of curves of low genera as follows: For a Howe curve H with two genus-1 double covers $E_i : y^2 = f_i(x)$, where f_i is a separable polynomial of degree 3 or 4 with $i = 1, 2$, we have a genus 2-curve $C : y^2 = f_1 f_2$. It follows from [12, Theorem 2.1] (see also [18, Theorem C] for a more general result) that H is supersingular if and only if E_1, E_2 and C are all supersingular.

In order to enumerate superspecial Howe curves, two strategies (A) and (B) below are provided in [23]. The authors of [23] also gave a method ((C) below) to decide whether two Howe curves are K-isomorphic, or not.

(A) (E_1, E_2)-first, using Cartier-Manin matrices

In this strategy, we use the same realization of Howe curves as in [24], that is, the fiber product of $E_1 \colon z^2 = f_1(x) := x^3 + A_1\mu^2 x + B_1\mu^3$ and $E_2 \colon w^2 = f_2(x) := (x-\lambda)^3 + A_2\mu^2(x-\lambda) + B_2\mu^3$ over $\mathbb{P}^1 = \mathrm{Proj}(K[x, y])$, where A_1, B_1, A_2 and B_2 are elements in K such that $E_{A_i,B_i} : y^2 = x^3 + A_i x + B_i$ $(i = 1, 2)$ are supersingular elliptic curves over K, and where λ, μ and ν are elements in K such that (i) $\mu \neq 0$ and $\nu \neq 0$, and (ii) f_1 and f_2 are coprime. Note that a point $(\lambda : \mu : \nu) \in \mathbb{P}^2(K)$ satisfying (i) and (ii) is said to be *of Howe type* in [24]. It was shown in [23, Proposition 4.1] that any superspecial Howe curve is K-isomorphic to the normalization of $E_1 \times_{\mathbb{P}^1} E_2$ obtained as above for A_1, B_1, A_2, B_2, λ, μ and ν belonging to $\mathbb{F}_{p^2}$.

This strategy enumerates pairs of supersingular elliptic curves $E_i : y^2 = f_i(x)$ $(i = 1, 2)$ so that $C : y^2 = f_1(x)f_2(x)$ is superspecial. To do this, for each unordered pair of (A_1, B_1) and (A_2, B_2), it suffices to compute the solutions $(\lambda : \mu : \nu) \in \mathbb{P}^2(\mathbb{F}_{p^2})$ (of Howe type) to the homogeneous system $M \equiv 0$, where M is the Cartier-Manin matrix of C. Once all pairs (E_1, E_2) are enumerated, we classify isomorphism classes of Howe curves defined by the pairs, by the isomorphism test described in (C) below. For a concrete algorithm of the enumeration based on this strategy, see [23, Section 4.2]. It is also shown in [23, Section 4.3] that the complexity of this algorithm is $\tilde{O}(p^6)$ arithmetic operations in $\mathbb{F}_{p^2}$.

(B) C-first, using Richelot isogenies

The second strategy first enumerates superspecial curves $C\colon y^2 = f(x)$ of genus 2, where $f(x) \in K[x]$ is a separable polynomial of degree 6. Once all superspecial curves of genus 2 are enumerated, we then enumerate decompositions $f(x) = f_1(x)f_2(x)$ with $f_i(x)$ of degree 3 so that there is an element $b \in K \cup \{\infty\}$ that makes both genus-1 curves $E_i\colon y^2 = (x-b)f_i(x)$ $(i = 1, 2)$ supersingular.

For this, we first apply a method given in [13, Section 3] to construct some (at least one) superspecial curves of genus 2 by gluing supersingular elliptic curves together along their 2-torsion. We then produce more such curves by applying *Richelot isogenies* to the curves already produced, where the definition of a Richelot isogeny of two curves of genus 2 is as follows:

Definition 5.2. Two genus-2 curves are *Richelot isogenous* if there exits an isogeny $\Psi : J(C_1) \to J(C_2)$ such that $\mathrm{Ker}(\Psi)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ that is maximal isotropic with respect to 2-Weil pairing. In this case, the isogeny Ψ is called a *Richelot isogeny*.

Note that given a curve C_1, we can compute (at most 15) genus-2 curves C_2, which are Richelot isogenous to C_1, with an isogeny map Ψ, see e.g., [30, Chapter 8] for more details. The above procedure to enumerate superspecial genus-2 curves terminates because there are only finitely many superspecial curves of genus 2, and a recent result of Jordan and Zaytman [17, Theorem 43] shows that we obtain all isomorphism classes of superspecial curves of genus 2 in this way. Once all pairs (E_1, E_2) are enumerated, we classify isomorphism classes of Howe curves defined by the pairs, by the isomorphism test described in (C) below. A concrete algorithm of the enumeration of superspecial Howe curves based on this strategy is given in [23, Section 5.3], and its complexity is $\tilde{O}(p^4)$ arithmetic operations in $\mathbb{F}_{p^2}$.

(C) A new isomorphism test for Howe curves.

Since every Howe curve is canonical (cf. [23, Lemma 2.1]), we can test whether two Howe curves are isomorphic or not, by applying the isomorphism test for canonical curves of genus 4 given in Section 3 (cf. [19, Section 6.1] and [20, Section 4.3]). However, this turns out to be very costly since it uses many Gröbner basis computations. In [23, Section 3], the authors present an efficient isomorphism test specific to Howe curves. We here briefly describe the isomorphism test given in [23, Section 3].

We first recall from the beginning of [23, Section 3] that a Howe curve is specified by the following three pieces of information: (1) A genus-2 curve C. (2) An unordered pair of disjoint sets $\{W_1, W_2\}$, each consisting of three Weierstrass points of C. (3) An unordered pair of distinct points $\{P_1, P_2\}$ on C that are mapped to one another by the

hyperelliptic involution. We here call $(C, \{W_1, W_2\}, \{P_1, P_2\})$ *a Howe triple* of a Howe curve. A criterion given in [23, Section 3] for determining whether two Howe curves are isomorphic or not is the following:

Proposition 5.3 ([23], Corollary 3.3)**.** *Two Howe triples* $(C, \{W_1, W_2\}, \{P_1, P_2\})$ *and* $(C', \{W_1', W_2'\}, \{P_1', P_2'\})$ *give isomorphic Howe curves if and only if there is an isomorphism* $C \to C'$ *that takes* $\{W_1, W_2\}$ *to* $\{W_1', W_2'\}$ *and* $\{P_1, P_2\}$ *to* $\{P_1', P_2'\}$*.*

This isomorphism test is conducted by simply deciding whether there exist any automorphisms of $\mathbb{P}^1$ that respect the sets of Weierstrass points and their divisions, and that take the x-coordinate of P_1 and P_2 to that of P_1' and P_2'. Clearly this procedure does not require any Gröbner basis computation, and also it is shown to be more efficient than the isomorphism test for canonical curves of genus 4 given in Section 3.

Main theorems in [23] and open questions

The authors of [23] implemented algorithms based on (A) – (C) over Magma, and executed them to enumerate superspecial Howe curves for concrete p. Recall that the complexities of (A) and (B) are $\tilde{O}(p^6)$ and $\tilde{O}(p^4)$ respectively. Practical time behaver of (A) and (B) for $5 \leq p \leq 53$ is shown in [23, Table 2]. As the estimated complexities show, we expect from [23, Table 2] that (B) is extremely faster than (A) in practice; e.g., for $p = 53$, (A) takes 5678.32 seconds, while (B) takes only 1.46 seconds, under the authors' experimental environment (details are written in [23, Section 6]). From this, the authors of [23] decided to adopt (B) in order to obtain results for p larger than 53.

Main results obtained by the execution of (B) together with (C) are the following:

Theorem 5.4.

1. *([23, Theorem 1.1]) For every prime* p *with* $7 < p < 20000$*, there exists a superspecial Howe curve in characteristic* p*.*
2. *([23, Theorem 1.2]) For every prime* p *with* $7 < p \leq 199$*, the number of* $\overline{\mathbb{F}_p}$*-isomorphism classes of superspecial Howe curves in characteristic* p *is given in Table* 3*.*

We can easily increase the upper bounds on p in these two theorems. For example, on a 2.8 GHz Quad-Core Intel Core i7 with 16GB RAM, computing the 8351 superspecial Howe curves in characteristic 199 using an algorithm based on (B) took 124 seconds in Magma. Finding examples of superspecial Howe curves for every p between 7 and 20000 took 680 minutes on the same PC.

We close this section with an open problem in the enumeration of superspecial Howe curves, and an open question on the existence of such curves:

Table 3. For each prime p from 11 to 199, we give the number $n(p)$ of superspecial Howe curves over $\overline{\mathbb{F}_p}$ and the ratio of $n(p)$ to the heuristic prediction $p^3/1152$ (see [23, Section 5]).

p	$n(p)$	Ratio	p	$n(p)$	Ratio	p	$n(p)$	Ratio
11	4	3.462	67	260	0.996	137	2430	1.089
13	3	1.573	71	742	2.388	139	2447	1.050
17	10	2.345	73	316	0.936	149	3082	1.073
19	4	0.672	79	595	1.390	151	3553	1.189
23	33	3.125	83	655	1.320	157	3427	1.020
29	45	2.126	89	863	1.410	163	3518	0.936
31	59	2.281	97	802	1.012	167	6268	1.550
37	41	0.932	101	1207	1.350	173	4780	1.064
41	105	1.755	103	1151	1.213	179	5771	1.159
43	79	1.145	107	1237	1.163	181	5419	1.053
47	235	2.608	109	1193	1.061	191	9610	1.589
53	167	1.292	113	1323	1.056	193	6298	1.009
59	259	1.453	127	2013	1.132	197	6839	1.030
61	243	1.233	131	2606	1.335	199	8351	1.221

Problem 5.5.

1. (Problem) Determine the number of $\mathbb{F}_{p^2}$-isomorphism classes of superspecial Howe curves.
2. (Question) Does there exist a superspecial Howe curve in any characteristic $p > 7$?

References

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

[2] Bettale, L., Faugere, J.-C. and Perret, L., Hybrid approach for solving multivariate systems over finite fields, *J. Math. Cryptol.*, **3** (2009) 177–197.

[3] Brock, B. W., Superspecial curves of genera two and three, Ph.D. thesis, Princeton University, 1993, MR 2689446.

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

[5] Eichler, M., Über die Idealklassenzahl total definiter Quaternionenalgebren, *Math. Z.*, **43** (1938), 102–109.

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

[7] Fuhrmann, R. and Torres, F., The genus of curves over finite fields with many rational points, *Manuscripta Math.*, **89**, 103–106, 1996.
[8] Gonzalez, J., Hasse-Witt matrices for the Fermat curves of prime degree, *Tohoku Math. J.*, (2) **49** (1997), no. 2, 149–163, MR 1447179 (98b:11064).
[9] Hartshorne, R., Algebraic Geometry, GTM **52**, Springer-Verlag (1977).
[10] Hashimoto, H., Class numbers of positive definite ternary quaternion Hermitian forms, *Proc. Japan Acad. Ser. A Math. Sci.*, **59** (1983), no. 10, 490–493.
[11] 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).
[12] Howe, E. W., Quickly constructing curves of genus 4 with many points, pp. 149–173 in: Frobenius Distributions: Sato-Tate and Lang-Trotter conjectures (D. Kohel, I. Shparlinski, eds.), Contemporary Mathematics **663**, American Mathematical Society, Providence, RI (2016).
[13] Howe, E. W., Leprévost, F. and Poonen, B., Large torsion subgroups of split Jacobians of curves of genus two or three, *Forum Math.*, **12** (2000), no. 3, 315–364, MR 1748483.
[14] Ibukiyama, T., Katsura, T. and Oort, F., Supersingular curves of genus two and class numbers, *Compositio Mathematica*, **57** (1986), 127–152.
[15] 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.
[16] Igusa, J., Class number of a definite quaternion with prime discriminant, *Proc. Nat. Acad. Sci. U.S.A.*, **44** (1958) 312–314.
[17] Jordan, B. W. and Zaytman, Y., Isogeny graphs of superspecial abelian varieties and generalized Brandt matrices, 2020, arXiv:2005.09031v4 [math.NT].
[18] Kani, E. and Rosen, M., Idempotent relations and factors of Jacobians, *Math. Ann.*, **284**, 307–327 (1989).
[19] Kudo, M. and Harashita, S., Superspecial curves of genus 4 in small characteristic, *Finite Fields and Their Applications*, **45**, 131–169 (2017).
[20] Kudo, M. and Harashita, S., Superspecial Hyperelliptic Curves of Genus 4 over Small Finite Fields, In: L. Budaghyan, F. Rodriguez-Henriquez (eds), Arithmetic of Finite Fields, WAIFI 2018, Lecture Notes in Computer Science, **11321**, 58–73, Springer, Cham, 2018.
[21] Kudo, M. and Harashita, S., Computational approach to enumerate non-hyperelliptic superspecial curves of genus 4, *Tokyo Journal of Mathematics*, Vol. **43**, Number 1, 259–278, 2020.
[22] Kudo, M. and Harashita, S., Superspecial trigonal curves of genus 5, *Experimental Mathematics*, published online: 16 Apr. 2020, (DOI) 10.1080/10586458.2020.1723745.
[23] Kudo, M., Harashita, S. and Howe, E. W., Algorithms to enumerate superspecial Howe curves of genus four, to appear in Proceedings of Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV), MSP, 2020, 15 pages.
[24] Kudo, M., Harashita, S. and Senda, H., The existence of supersingular curves of genus 4 in arbitrary characteristic, *Research in Number Theory*, Vol. **6**, Issue 4, Article number: 44, 2020.
[25] Li K.-Z. and Oort, F., Moduli of Supersingular Abelian Varieties, Lecture Notes in Math., vol. **1680**, Springer-Verlag, 1998.
[26] Manin, J. I., On the theory of Abelian varieties over a field of finite characteristic, *AMS Translations*, Series 2, **50**, 127–140, 1966, translated by G. Wagner (originally published in *Izv. Akad. Nauk SSSR Ser. Mat.*, **26**, 281–292, 1962).

[27] Narasimhan, M. S. and Nori, M. V., Polarisations on an abelian variety, *Proc. Indian Acad. Sci. (Math. Sci.)* **90**, 125–128 (1981).
[28] Oort, F. and Ueno, K., Principally polarized abelian varieties of dimension two or three are Jacobian varieties, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **20** (1973), 377–381.
[29] Shioda, T., Supersingular K3 surfaces, Lecture Notes in Math., **732**. Berlin-Heidelberg-New York: Springer (1979) pp. 564–591.
[30] Smith, B., Explicit endomorphisms and correspondences, PhD thesis, University of Sydney, 2005.
[31] Xue, J., Yang, T.-C. and Yu, C.-F., On superspecial abelian surfaces over Finite Fields, *Doc. Math.*, **21** (2016), 1607–1643.
[32] Yui, N., On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$, *Journal of algebra*, **52**, 378–410 (1978).