RESEARCH

The existence of supersingular curves of genus 4 in arbitrary characteristic

Momonari Kudo¹, Shushi Harashita^{2*} and Hayato Senda³

*Correspondence:

harasita@ynu.ac.jp

²Graduate School of
Environment and Information
Sciences, Yokohama National
University, Yokohama, Japan
Full list of author information is
available at the end of the article

Abstract

We prove that there exists a supersingular nonsingular curve of genus 4 in arbitrary characteristic $p > 0$. For $p > 3$ we shall prove that the desingularization of a certain fiber product over $\mathbf{P}^1$ of two supersingular elliptic curves is supersingular.

1 Introduction

Let K be an algebraically closed field of positive characteristic. For a nonsingular algebraic curve C over K we call C *supersingular* (resp. *superspecial*) if its Jacobian $J(C)$ is isogenous (resp. isomorphic) to a product of supersingular elliptic curves.

As to supersingular curves, the following is a basic problem (cf. [19, Question 2.2]).

For given g , does there exist a supersingular curve of genus g in any characteristic p ?

For $g \leq 3$, this problem was solved affirmatively. The case of $g = 1$, i.e., elliptic curves is due to Deuring [4]. Ibukiyama, Katsura and Oort in [11, Proposition 3.1] proved the existence of superspecial curves of genus 2 for $p > 3$. For the existence of supersingular curves of genus 3 in any characteristic $p > 0$, see Oort [17, Theorem 5.12]. Also, as a proof for $g = 2$ with $p > 3$ and for $g = 3$ with $p > 2$, we refer to the stronger fact that there exists a maximal curve of genus g over $\mathbb{F}_{p^{2e}}$ if $g = 2$ and $p^{2e} \neq 4, 9$ (cf. Serre [20, Théorème 3]) and if $g = 3$, $p \geq 3$ and e is odd (cf. Ibukiyama [10, Theorem 1]), where we recall the general fact that any maximal curve over $\mathbb{F}_{p^2}$ is superspecial (and therefore supersingular). Even for $(g, p) = (2, 3)$, there exists a supersingular curve: for example $y^2 = x^5 + 1$ is supersingular (but is not superspecial), since its Cartier–Manin matrix is nilpotent, see (9) and (10) in Sect. 2 for the Cartier–Manin matrix and a criterion for the supersingularity. For the case of $p = 2$, we refer to the celebrated paper [22] by van der Geer and van der Vlugt, where they proved that there exists a supersingular curve of an arbitrary genus in characteristic 2.

This paper focuses on the first open case, i.e., the case of $g = 4$ (cf. [19, Question 3.4]). Let us recall some recent works, restricting ourselves to the case of $g = 4$. According to [16, Remark 7.2] and [15, Theorem 7.1] by Li, Mantovan, Pries and Tang, there exists a supersingular curve of genus 4 if $p \equiv 5 \pmod{6}$ or if $p \equiv 2, 3, 4 \pmod{5}$. Among them, we review the existence for $(g, p) = (4, 3)$ for the reader's convenience. Indeed $y^{10} = x(1-x)$

is supersingular, as this is a quotient of the Hermitian curve $X^{q+1} + Y^{q+1} = 1$ with $q = 3^2$, where the quotient map is given by $x = X^{q+1}$ and $y = XY$. For odd $p \equiv 2 \pmod{3}$, in [14] the first author showed that there exists a superspecial (and thus supersingular) nonsingular curve of genus 4.

This paper aims to remove any condition on p for the existence of supersingular curves of genus 4. For this, we use curves introduced by Howe in [9], where he studied a curve of genus 4 defined as the desingularization of a fiber product over $\mathbf{P}^1$ of two elliptic curves. In this paper, we call such a curve a *Howe curve*, see Definition 2.1 for the precise definition of Howe curves. Our main theorem is:

Theorem 1.1 *For any $p > 3$, there exists a supersingular Howe curve in characteristic p . The number of isomorphism classes of supersingular Howe curves over an algebraically closed field is finite.*

The next corollary is deduced from Theorem 1.1 together with the existence results for $p = 2$ and for $(g, p) = (4, 3)$ explained above.

Corollary 1.2 *There exists a supersingular nonsingular curve of genus 4 in arbitrary characteristic $p > 0$.*

As any supersingular Howe curve has a -number ≥ 3 for odd p (cf. Sect. 2), Theorem 1.1 is a stronger assertion than the affirmative answer for $p > 3$ to the question by Pries [19, Question 3.6], which predicts that there exists a nonsingular curve of genus 4 with p -rank 0 and a -number at least 2.

Let us describe an outline of the proof of Theorem 1.1, with an overview of this paper. In Sect. 2, we review the definition of Howe curves and their properties, and show that the existence of a supersingular Howe curve of genus 4 is equivalent to that of two supersingular elliptic curves $E_1 : y^2 = f_1$ and $E_2 : y^2 = f_2$ with coprime pair (f_1, f_2) of separable polynomials of degree 3 such that the hyperelliptic curve $C : y^2 = f := f_1 f_2$ of genus 2 is also supersingular. Here E_1 and E_2 can be isomorphic. For the supersingularity of C , we use the fact that any curve of genus 2 is supersingular if and only if $MM^\sigma = 0$ holds for its Cartier-Manin matrix M , where σ denotes the Frobenius map. The moduli space $\mathcal{M}_2$ (resp. $\overline{\mathcal{M}}_2$) of nonsingular (resp. stable) curves of genus two is of dimension 3 and it is known that the supersingular locus on $\overline{\mathcal{M}}_2$ (naturally extending that of $\mathcal{M}_2$) is one. On the other hand, C 's constructed as above from supersingular E_1 and E_2 make a two-dimensional family, say $\mathcal{P}$, in $\mathcal{M}_2$. Then, the Zariski closure $\overline{\mathcal{P}}$ of $\mathcal{P}$ in $\overline{\mathcal{M}}_2$ must intersect the supersingular locus in $\overline{\mathcal{M}}_2$. The difficulty lies in showing that not all of these intersection points lie outside $\mathcal{M}_2$. Almost all of the remaining sections are devoted to overcoming the difficulty. In the proof, instead of $\overline{\mathcal{P}}$, we use a more concrete space, see Sect. 3 for our moduli-theoretic framework. In Sect. 4, we prove two assertions of cubic polynomials (Corollaries 4.4 and 4.7) by reducing the problems to two propositions (Propositions 4.3 and 4.6) for the Legendre form $y^2 = g := x(x-1)(x-t)$. In Sect. 5, based on the two assertions, we investigate properties of entries of MM^σ as polynomials, where we regard coefficients in f_1 and f_2 as variables. The properties show that we get a desired (f_1, f_2) from a solution of a multivariate system obtained by removing trivial factors from $MM^\sigma = 0$, where “desired” means that f_1 and f_2 are separable and are coprime (in other words, the corresponding point belongs to the interior $\mathcal{M}_2$). Finally, we show the existence of such a

solution by proving an analogous result of the quasi-affineness of Ekedahl-Oort strata in the case of abelian varieties.

2 Howe curves

In this section, we recall the definition of Howe curves and properties of these curves, and study the supersingularity of them.

Definition 2.1 A *Howe curve* is a curve which is isomorphic to the desingularization of the fiber product $E_1 \times_{\mathbf{P}^1} E_2$ of two double covers $E_i \rightarrow \mathbf{P}^1$ ramified over S_i , where S_i consists of 4 points and $|S_1 \cap S_2| = 1$ holds.

To achieve our goal, for $p > 3$ we realize a Howe curve in the following way. Let K be an algebraically closed field of characteristic p . Let

$$y^2 = x^3 + A_1x + B_1, \quad (1)$$

$$y^2 = x^3 + A_2x + B_2 \quad (2)$$

be two (nonsingular) elliptic curves, where $A_1, B_1, A_2, B_2 \in K$. Here two elliptic curves (1) and (2) can be isomorphic. Let λ, μ, ν be elements of K and set

$$f_1(x) = x^3 + A_1\mu^2x + B_1\mu^3, \quad (3)$$

$$f_2(x) = (x - \lambda)^3 + A_2\nu^2(x - \lambda) + B_2\nu^3. \quad (4)$$

Consider two elliptic curves

$$E_1 : z^2y = y^3f_1(x/y) = x^3 + A_1\mu^2xy^2 + B_1\mu^3y^3, \quad (5)$$

$$E_2 : w^2y = y^3f_2(x/y) = (x - \lambda y)^3 + A_2\nu^2(x - \lambda y)y^2 + B_2\nu^3y^3 \quad (6)$$

with the double covers

$$\pi_i : E_i \rightarrow \mathbf{P}^1 = \text{Proj}(K[x, y]).$$

Note that the isomorphism classes of E_1 and E_2 are independent of the choice of (λ, μ, ν) provided $\mu \neq 0$ and $\nu \neq 0$. We say that (λ, μ, ν) is of *Howe type* if

- (i) $\mu \neq 0$ and $\nu \neq 0$;
- (ii) f_1 and f_2 are coprime.

If (λ, μ, ν) is of Howe type, then the desingularization of the fiber product $E_1 \times_{\mathbf{P}^1} E_2$ is a Howe curve, since $E_i \rightarrow \mathbf{P}^1$ is ramified over the set consisting of 4 points, say S_i , and $S_1 \cap S_2 = \{(1 : 0)\}$. Conversely, any Howe curve is realized in this way. Indeed, let E_i for $i = 1, 2$ be two elliptic curves with double covers $E_i \rightarrow \mathbf{P}^1$, defining a Howe curve. An automorphism of $\mathbf{P}^1$ moves the ramified point of both of $E_i \rightarrow \mathbf{P}^1$ ($i = 1, 2$) to $(1 : 0)$. By a usual coordinate-change, we make E_1 to be of the form (5) if $p > 3$. Note that any elliptic curve ramified at $(1 : 0)$ is written as in (6).

Suppose that (λ, μ, ν) is of Howe type. Put

$$f(x) = f_1(x)f_2(x)$$

and consider the hyperelliptic curve C of genus 2 defined by

$$C : u^2 = f(x). \quad (7)$$

It was proven by Howe [9, Theorem 2.1] that H is of genus 4 and there exist two isogenies

$$\varphi : J(H) \longrightarrow E_1 \times E_2 \times J(C),$$

$$\psi : E_1 \times E_2 \times J(C) \longrightarrow J(H)$$

such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the multiplication by 2, see [13, Theorem C] for a more general result. Hence H is supersingular if and only if E_1, E_2 and C are supersingular. For an abelian variety Z , let $Z[p]$ denote the kernel of the multiplication-by- p map on Z . If p is odd, then $\psi \circ \varphi$ (resp. $\varphi \circ \psi$) is an automorphism of $J(H)[p]$ (resp. $(E_1 \times E_2 \times J(C))[p]$), whence $J(H)[p]$ and $E_1[p] \times E_2[p] \times J(C)[p]$ are isomorphic, see [5, Corollary 2] for a more general result. Hence the a -number of H is equal to the sum of the a -numbers of E_1, E_2 and $J(C)$, whence any supersingular Howe curve is of a -number ≥ 3 .

Now we recall a criterion for the supersingularity of C . Let γ_i be the x^i -coefficient of $f(x)^{(p-1)/2}$, i.e.,

$$f(x)^{(p-1)/2} = \sum_{i=0}^{3(p-1)} \gamma_i x^i. \quad (8)$$

Put

$$a = \gamma_{p-1}, \quad b = \gamma_{2p-1}, \quad c = \gamma_{p-2} \quad \text{and} \quad d = \gamma_{2p-2}.$$

In Sect. 4, we shall use the fact that γ_i and therefore a, b, c and d are homogeneous when we regard them as polynomials in λ, μ and ν . Let M be the Cartier–Manin matrix of C , that is a matrix representing the Cartier operator on $H^0(C, \Omega_C^1)$ (referred to as the modified Cartier operator in [23]). It is known (cf. [6, 4.1] and [23, §2]) that the Cartier–Manin matrix of C is given by

$$M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \quad (9)$$

Recall the fact (cf. [11, Lemma 1.1, (i)]) that a curve D of genus 2 is supersingular if and only if the Cartier operator V on $H^0(D, \Omega_D^1)$ satisfies $V^2 = 0$. Hence C is supersingular if and only if

$$MM^\sigma = \begin{pmatrix} a^{p+1} + bc^p & ab^p + bd^p \\ a^p c + c^p d & b^p c + d^{p+1} \end{pmatrix} = 0, \quad (10)$$

where $M^\sigma = \begin{pmatrix} a^p & b^p \\ c^p & d^p \end{pmatrix}$. See [2, Step 2 of the proof of Theorem 4.8] and also [7, 4.0.3] for a sufficient condition for supersingularity, generalized in the higher genus case.

Remark 2.2 As Achter and Howe suggested in [1], we need to be careful when we use Cartier–Manin matrices. A notation different from (9) for Cartier–Manin matrices exists: the transpose A of M , see [23]. In the notation, the supersingularity for genus-2 curves is equivalent to $A^\sigma A = 0$, as in [11, Lemma 1.1, (i)].

Proposition 2.3 *Assume that E_1 and E_2 are supersingular. Then H is supersingular if and only if $ad - bc = 0$, $ab^{p-1} + d^p = 0$ and $a^p + c^{p-1}d = 0$.*

Proof Since E_1 and E_2 are supersingular, H is supersingular if and only if C is supersingular. As explained above, C is supersingular if and only if (10) holds. First remark that $ad - bc = 0$ implies

$$a^{p+1} + bc^p = a(a^p + c^{p-1}d), \quad (11)$$

$$ab^p + bd^p = b(ab^{p-1} + d^p), \quad (12)$$

$$a^p c + c^p d = c(a^p + c^{p-1} d), \quad (13)$$

$$b^p c + d^{p+1} = d(ab^{p-1} + d^p). \quad (14)$$

To prove the “if”-part, suppose that $ad - bc = 0$, $ab^{p-1} + d^p = 0$ and $a^p + c^{p-1}d = 0$. It follows from $ad - bc = 0$ that (11)–(14) hold. This means that every entry of the matrix in (10) is a multiple of $ab^{p-1} + d^p$ or $a^p + c^{p-1}d$. Thus the “if”-part is true.

Conversely, suppose that (10) holds. Since $\det(MM^\sigma) = \det(M)^{p+1}$, we have $\det(M) = ad - bc = 0$, which implies

$$a^{p-1}(ab^{p-1} + d^p) = b^{p-1}(a^p + c^{p-1}d), \quad (15)$$

$$c^{p-1}(ab^{p-1} + d^p) = d^{p-1}(a^p + c^{p-1}d). \quad (16)$$

Also by (11)–(14) we have $a^p + c^{p-1}d = 0$ unless $a = c = 0$ and $ab^{p-1} + d^p = 0$ unless $b = d = 0$. If $a = c = 0$, by (15) and (16) we have $a^p + c^{p-1}d = 0$ unless $b = d = 0$. Similarly, if $b = d = 0$, by (15) and (16) we have $ab^{p-1} + d^p = 0$ unless $a = c = 0$. Obviously $(a, b, c, d) = (0, 0, 0, 0)$ satisfies $ad - bc = 0$, $ab^{p-1} + d^p = 0$ and $a^p + c^{p-1}d = 0$. Thus the “only if”-part is true. $\square$

For later use, we review how the Cartier–Manin matrix is converted by a linear change of variables.

Lemma 2.4 *Let X be a new variable and consider substituting $uX + v$ for x , where $u, v \in K$ with $u \neq 0$. Let γ'_i be the X^i -coefficient of $f(uX + v)^{(p-1)/2}$ and set*

$$M' = \begin{pmatrix} \gamma'_{p-1} & \gamma'_{2p-1} \\ \gamma'_{p-2} & \gamma'_{2p-2} \end{pmatrix}.$$

Then we have

$$M' = P^{-1}MP^\sigma$$

with

$$P = \begin{pmatrix} u & 0 \\ uv & u^2 \end{pmatrix}.$$

In particular, we have $\det(M') = \det(M)$ if $u = 1$.

Proof We have

$$\gamma'_i = \sum_{j=i}^{3(p-1)} \binom{j}{i} u^i v^{j-i} \gamma_j$$

as

$$f(uX + v)^{(p-1)/2} = \sum_{j=0}^{3(p-1)} \gamma_j (uX + v)^j = \sum_{i=0}^{3(p-1)} \left(\sum_{j=i}^{3(p-1)} \binom{j}{i} u^i v^{j-i} \gamma_j \right) X^i.$$

Then we have

$$\begin{aligned} \gamma'_{p-1} &= u^{p-1}(\gamma_{p-1} + v^p \gamma_{2p-1}), \\ \gamma'_{2p-1} &= u^{2p-1} \gamma_{2p-1}, \\ \gamma'_{p-2} &= u^{p-2}(\gamma_{p-2} - v \gamma_{p-1} + v^p \gamma_{2p-2} - v^{p+1} \gamma_{2p-1}), \\ \gamma'_{2p-2} &= u^{2p-2}(\gamma_{2p-2} - v \gamma_{2p-1}) \end{aligned}$$

by calculating, in characteristic p , the binomials

$$\begin{aligned} \binom{j}{p-1} &= \begin{cases} 1 & \text{if } j = p-1, 2p-1, \\ 0 & \text{otherwise,} \end{cases} & \binom{j}{2p-1} &= \begin{cases} 1 & \text{if } j = 2p-1, \\ 0 & \text{otherwise,} \end{cases} \\ \binom{j}{p-2} &= \begin{cases} 1 & \text{if } j = p-2, 2p-2 \\ -1 & \text{if } j = p-1, 2p-1, \\ 0 & \text{otherwise,} \end{cases} & \binom{j}{2p-2} &= \begin{cases} 1 & \text{if } j = 2p-2, \\ -1 & \text{if } j = 2p-1, \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

for $j \leq 3p-3$. These are obtained by applying a general formula

$$\binom{kp+\ell}{k'p+\ell'} = \binom{k}{k'} \binom{\ell}{\ell'} \quad (17)$$

for $0 \leq \ell, \ell' \leq p-1$ to the case of $k' = 0, 1$ and $\ell' = p-1, p-2$ with $\binom{\ell}{\ell'} = 0$ for $\ell' > \ell$. The formula (17) follows from

$$(x+1)^{kp+\ell} = (x^p+1)^k (x+1)^\ell = \sum_{k'} \sum_{\ell'} \binom{k}{k'} \binom{\ell}{\ell'} x^{pk'+\ell'}$$

in characteristic p . $\square$

3 A moduli-theoretic observation and ingredients of the proof

From the next section onward, we go into the details of the proof of the main theorem. Before that, let us give an outline of the proof with a moduli-theoretic observation. We use the same notation as in Sect. 2. We choose A_1, B_1, A_2 and B_2 so that the elliptic curves (1) and (2) are supersingular. Let $\tilde{C}$ be the desingularization only at the infinity of C defined in (7). Note that $\tilde{C}$ is nonsingular if and only if the corresponding point $(\lambda : \mu : \nu)$ is of Howe type. Considering λ, μ and ν as indeterminates, we have a family of curves $\tilde{C}$ over $\mathbf{P}^2 = \text{Proj } K[\lambda, \mu, \nu]$. To prove the existence of a supersingular Howe curve, it suffices to find a nonsingular supersingular fiber from this family. The possible Newton polygons of nonsingular $\tilde{C}$'s are supersingular, p -rank-one and ordinary. Note that a nonsingular $\tilde{C}$ has p -rank ≤ 1 if and only if its Cartier–Manin matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant zero. Since the determinant $ad - bc$ turns out to be a multiple of a power of $\mu\nu$ and every fiber $\tilde{C}$ over the locus $\mu\nu = 0$ is singular, it would be better to divide $ad - bc$ by $\mu\nu$ as much as possible. We shall prove in Lemma 5.3 that the order of $ad - bc$ with respect to $\mu\nu$ is exactly $(p+1)/2$. The exactness is important and its proof requires an assertion (Corollary 4.4) on cubic polynomials from the next section.

Put

$$\begin{aligned} h_0 &:= (ad - bc)/(\mu\nu)^{(p+1)/2}, \\ h_1 &:= ab^{p-1} + d^p, \\ h_2 &:= a^p + c^{p-1}d. \end{aligned}$$

We consider

$$V(h_0, h_1, h_2) \subset V(h_0) \subset \mathbf{P}^2$$

as the Newton polygon stratification for this family over $\mathbf{P}^2$, where $V(h_0, h_1, h_2)$, $V(h_0) \setminus V(h_0, h_1, h_2)$ and $\mathbf{P}^2 \setminus V(h_0)$ are called the supersingular locus, the p -rank-one locus and the ordinary locus respectively. The expected dimensions of the loci would be 0, 1 and 2

respectively. Indeed, this is proved in Proposition 5.7. (A priori, on the open subscheme where $\tilde{C}$ is nonsingular, the dimension of each locus is greater than or equal to the expected one by the purity theorem [3, 4.1] due to de Jong and Oort.) If the p -rank-one locus is proved not to be projective, then $V(h_0, h_1, h_2) \neq \emptyset$ follows from it (cf. Proposition 5.7). Our proof is along this line. However, an obstruction is that $V(h_0, h_1, h_2)$ may be contained in the locus consisting of points which are not of Howe type (equivalently, over which $\tilde{C}$ is singular). The main part of our proof is to show that there is no obstruction, i.e., the condition $h_i = 0$ for $i = 0, 1, 2$ implies that $\tilde{C}$ is nonsingular. This is proven in Proposition 5.6, where the proof needs another assertion (Corollary 4.7) on cubic polynomials from the next section.

4 Two assertions on cubic polynomials

In this section, we prove two assertions on cubic polynomials (Corollaries 4.4 and 4.7), which play important roles in the proof of the main theorem. The proof is done by reducing the problems to those of the Legendre form (Propositions 4.3 and 4.6).

Assume $p \geq 3$. Let $g(x) = x(x-1)(x-t)$ and $e = (p-1)/2$, where we regard t as an indeterminate. We define a polynomial $H_p(t)$ by

$$H_p(t) := \sum_{i=0}^e \binom{e}{i}^2 t^i. \quad (18)$$

Let $\delta_{p-1}(t)$ be the x^{p-1} -coefficient of $g(x)^e$. It follows from

$$\delta_{p-1}(t) = (-1)^e H_p(t) \quad (19)$$

that $y^2 = x(x-1)(x-t_0)$ is a supersingular elliptic curve for $t_0 \in \overline{\mathbb{F}_p}$ if and only if $H_p(t_0) = 0$, see e.g., [21, Chap. V, Theorem 4.1].

For our purpose, we need to study the x^{p-2} -coefficient $\delta_{p-2}(t)$ of $g(x)^e$. Specifically, we shall show Proposition 4.3 below, which asserts that $\delta_{p-1}(t)$ and $\delta_{p-2}(t)$ are coprime. We start with giving an explicit formula of $\delta_{p-2}(t)$.

Lemma 4.1 *We have*

$$\delta_{p-2}(t) = (-1)^{e-1} \sum_{i=0}^{e-1} \binom{e}{i} \binom{e}{i+1} t^{i+1}. \quad (20)$$

Proof By the binomial theorem, $g(x)^e = x^e(x-1)^e(x-t)^e$ is equal to

$$x^e \sum_{i=0}^e \binom{e}{i} x^i (-1)^{e-i} \sum_{j=0}^e \binom{e}{j} x^{e-j} (-t)^j = \sum_{i=0}^e \sum_{j=0}^e (-1)^{e-i+j} \binom{e}{i} \binom{e}{j} x^{2e+i-j} t^j. \quad (21)$$

The x^{p-2} -coefficient of this is the sum over (i, j) with $j = i+1$, since $j = i+1$ if $2e+i-j = p-2$. Thus, we have the desired equation. $\square$

The next lemma is the essential part of the proof of the coprimeness of $\delta_{p-1}(t)$ and $\delta_{p-2}(t)$.

Lemma 4.2 *We have the equality*

$$\delta_{p-2}(t) = t\delta_{p-1}(t) + 2t(t-1) \frac{d}{dt} \delta_{p-1}(t).$$

Proof The lemma follows from the equality

$$\binom{e}{i} \binom{e}{i+1} = -\binom{e}{i}^2 - 2\binom{e}{i}^2 i + 2\binom{e}{i+1}^2 (i+1) \quad (22)$$

in characteristic p for $i = 0, 1, \dots, e$ with $\binom{e}{e+1} = 0$. Indeed, multiplying both sides of (22) by $(-1)^{e-1} t^{i+1}$ and taking the sum over $i = 0, 1, \dots, e$, we have

$$\delta_{p-2}(t) = t\delta_{p-1}(t) + 2t^2 \frac{d}{dt} \delta_{p-1}(t) - 2t \frac{d}{dt} \delta_{p-1}(t).$$

Since $2(e-i) \equiv -1-2i \pmod{p}$, we have

$$1 = 2(i+1) - 1 - 2i = \frac{(-1-2i)(i+1)}{e-i} + 2(e-i) = -\frac{i+1}{e-i} - 2i \frac{i+1}{e-i} + 2(e-i).$$

The equation (22) is obtained by multiplying both sides by $\binom{e}{i} \binom{e}{i+1}$. $\square$

Now we prove

Proposition 4.3 *The polynomials $\delta_{p-1}(t)$ and $\delta_{p-2}(t)$ are coprime, i.e., have no common root in $\overline{\mathbb{F}_p}$.*

Proof Note that $\delta_{p-1}(0)$ and $\delta_{p-1}(1)$ are not zero, since $\delta_{p-1}(t) = (-1)^e H_p(t)$ by (19) and $H_p(0) = 1$ and $H_p(1) = (-1)^e$, see the proof of [21, Chap. V, Theorem 4.1 (c)]. If $\delta_{p-1}(\alpha) = \delta_{p-2}(\alpha) = 0$ for some $\alpha \in \overline{\mathbb{F}_p} \setminus \{0, 1\}$, then one has $\left(\frac{d}{dt} \delta_{p-1}\right)(\alpha) = 0$ by Lemma 4.2. We have $H_p(\alpha) = \left(\frac{d}{dt} H_p\right)(\alpha) = 0$, which means that α is a double root of $H_p(t)$. This contradicts the fact shown by Igusa [12] that all roots of $H_p(t)$ are simple (cf. [21, Chap. V, Theorem 4.1 (c)]). $\square$

The following corollary derived from Proposition 4.3 will be used in the next section.

Corollary 4.4 *Let K be an algebraically closed field of characteristic p . Let E_0 be an elliptic curve $y^2 = g_0(x)$ over K , where $g_0(x)$ is a cubic separable polynomial in $K[x]$. Assume that E_0 is supersingular, i.e., the x^{p-1} -coefficient of $g_0(x)^e$ is zero. Then x^{p-2} -coefficient of $g_0(x)^e$ is not zero.*

Proof There exist $u \neq 0$ and v in K such that $g_0(x) = g(X)$ with $X := ux + v$, where $g(X) = X(X-1)(X-t)$ for some $t \in K \setminus \{0, 1\}$. Let ϵ_i (resp. ϵ'_i) be the X^i -coefficients (resp. x^i -coefficients) of $g(X)^{(p-1)/2}$ and $g_0(x)^{(p-1)/2}$ respectively for $0 \leq i \leq 3(p-1)/2$. Similarly to the proof of Lemma 2.4, we have

$$\epsilon'_i = \sum_{j=i}^{3(p-1)/2} \binom{j}{i} u^i v^{j-i} \epsilon_j$$

for $0 \leq i \leq 3(p-1)/2$, and in particular ϵ'_{p-1} and ϵ'_{p-2} are

$$\epsilon'_{p-1} = u^{p-1} \epsilon_{p-1}, \quad (23)$$

$$\epsilon'_{p-2} = u^{p-2} (\epsilon_{p-2} - v \epsilon_{p-1}). \quad (24)$$

It follows from $\epsilon'_{p-1} = 0$ and (23) that $\epsilon_{p-1} = 0$. By Proposition 4.3, $\epsilon_{p-1} = 0$ implies $\epsilon_{p-2} \neq 0$. By (24) we obtain $\epsilon'_{p-2} \neq 0$. $\square$

The second aim of this section is to show that the e -th derivative $(g_0(x)^e)^{(e)}$ of $g_0(x)^e$ is separable for any cubic separable polynomial $g_0(x)$. We start with reviewing an elementary congruence relation for the reader's convenience.

Lemma 4.5 *We have*

$$(p-1-n)! \equiv \frac{(-1)^{n+1}}{n!} \pmod{p}$$

for $n = 0, 1, \dots, p-1$.

Proof We have

$$(p-1-n)! = \frac{(p-1)!}{(p-1)(p-2)\cdots(p-n)} \equiv \frac{-1}{(-1)(-2)\cdots(-n)} = \frac{(-1)^{n+1}}{n!} \pmod{p},$$

where we used Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$. $\square$

The next proposition gives a factorization of $(g(x)^e)^{(e)}$ for $g(x) = x(x-1)(x-t)$. Let $H_p(t)$ be the polynomial defined by (18). Let $a_i \in \overline{\mathbb{F}_p}$ ($i = 1, \dots, e$) be the roots of $H_p(t) = 0$, i.e.,

$$H_p(t) = \prod_{i=1}^e (t - a_i). \quad (25)$$

Proposition 4.6 *We have*

$$\frac{1}{e!} \cdot (g(x)^e)^{(e)} = \prod_{i=1}^e ((t - a_i)x - (1 - a_i)t), \quad (26)$$

where $(g(x)^e)^{(e)}$ denotes the e -th derivative of $g(x)^e$ with respect to x .

Proof Replacing j by $e-j$ in (21) and taking its e -th derivative, we have

$$(g(x)^e)^{(e)} = \sum_{i=0}^e \sum_{j=0}^e (-1)^{i+j} \frac{(e+i+j)!}{(i+j)!} \binom{e}{i} \binom{e}{j} x^{i+j} t^{e-j}. \quad (27)$$

Hence $x^{i+j} t^{e-j}$ -coefficient of the left side of (26) is $(-1)^{i+j} \binom{e}{i} \binom{e}{j}$ times

$$\frac{(e+i+j)!}{e!(i+j)!}. \quad (28)$$

Put $P := \prod_{i=1}^e ((t - a_i)x - (1 - a_i)t)$. We have

$$\begin{aligned} P &= (x-t)^e \prod_{i=1}^e \left(\frac{t(x-1)}{x-t} - a_i \right) = (x-t)^e H_p \left(\frac{t(x-1)}{x-t} \right) \\ &= (x-t)^e \sum_{k=0}^e \binom{e}{k}^2 \left(\frac{t(x-1)}{x-t} \right)^k \end{aligned}$$

by (25) and (18). Using the binomial theorem, one obtains

$$\begin{aligned} P &= \sum_{k=0}^e \binom{e}{k}^2 (x-t)^{e-k} t^k (x-1)^k \\ &= \sum_{k=0}^e \binom{e}{k}^2 t^k \sum_{j=0}^e \binom{e-k}{j} x^j (-t)^{e-k-j} \sum_{i=0}^e \binom{k}{i} x^i (-1)^{k-i} \\ &= \sum_{k=0}^e \sum_{j=0}^e \sum_{i=0}^e (-1)^{e-i-j} \binom{e}{k}^2 \binom{e-k}{j} \binom{k}{i} x^{i+j} t^{e-j}, \end{aligned} \quad (29)$$

where we used $\binom{k}{i} = 0$ for $i > k$ and $\binom{e-k}{j} = 0$ for $j > e-k$ in the second equality. Since

$$\binom{e}{k} \binom{e-k}{j} = \binom{e}{j} \binom{e-j}{k} \quad \text{and} \quad \binom{e}{k} \binom{k}{i} = \binom{e}{i} \binom{e-i}{e-k},$$

the $x^{i+j}t^{e-j}$ -coefficient of P is

$$(-1)^{e-i-j} \binom{e}{i} \binom{e}{j} \sum_{k=0}^e \binom{e-j}{k} \binom{e-i}{e-k}. \quad (30)$$

By applying Vandermonde's identity to the sum, (30) is equal to $(-1)^{i+j} \binom{e}{i} \binom{e}{j}$ times

$$(-1)^e \binom{2e-i-j}{e}. \quad (31)$$

If $i+j > e$, then both of (28) and (31) are zero. Otherwise, applying Lemma 4.5 to $n = i+j$ and $n = e-i-j$, we have that (28) is equal to (31). Thus the equation (26) holds. $\square$

As a corollary of Proposition 4.6, we have

Corollary 4.7 *Let $g_0(x)$ be a separable cubic polynomial. Then $(g_0(x)^e)^{(e)}$ is a separable polynomial.*

Proof A linear coordinate change makes g_0 a Legendre form $g(x) = x(x-1)(x-t)$ with $t \neq 0, 1$. It is clear that $(g_0(x)^e)^{(e)}$ is separable if and only if $(g(x)^e)^{(e)}$ is separable. Let $a_1, \dots, a_e$ be the roots of $H_p(t)$ as above. Note that $a_i \neq 0, 1$ for $i = 1, 2, \dots, e$ as $H_p(0) = 1$ and $H_p(1) = (-1)^e$ (cf. the proof of [21, Chap. V, Theorem 4.1 (c)]). If $t \notin \{a_1, \dots, a_e\}$, the roots of $(g(x)^e)^{(e)}$ are $(1-a_i)t/(t-a_i)$ for $i = 1, \dots, e$. Otherwise, we may assume $t = a_1$ without loss of generality, and then the roots of $(g(x)^e)^{(e)}$ are $(1-a_i)a_1/(a_1-a_i)$ for $i = 2, \dots, e$. In both cases, it is straightforward to see that the roots are mutually distinct, using the fact that $H_p(t)$ is separable, i.e., $a_1, \dots, a_e$ are mutually distinct (cf. [12] and [21, Chap. V, Theorem 4.1 (c)]). $\square$

5 Proof of the main theorem

Assume $p > 3$. Let K be an algebraically closed field of characteristic p . We use the same notation as in Sect. 2, i.e., $A_1, B_1, A_2, B_2, \lambda, \mu, \nu, f_1, f_2, f, a, b, c, d$ are as in Sect. 2. We choose A_1, B_1, A_2, B_2 in K so that (1) and (2) are supersingular. By Proposition 2.3, it suffices to show that there exists $(\lambda, \mu, \nu) \in K^3$ of Howe type such that $ad - bc = 0$, $ab^{p-1} + d^p = 0$ and $a^p + c^{p-1}d = 0$.

From now on, we regard λ, μ and ν as indeterminates, and consider a, b, c, d as polynomials in λ, μ, ν . Note that a, b, c and d are homogeneous polynomials in λ, μ, ν of degrees $2p-2, p-2, 2p-1$ and $p-1$ respectively.

We start with studying the factors of μ and ν in $ad - bc$. More precisely, we prove that $ad - bc$ is a multiple of $(\mu\nu)^{(p+1)/2}$ in Lemma 5.3 below. Set $e := (p-1)/2$ as in Section 3. Let α_k and β_k be the x^k -coefficients of $f_1(x)$ and $f_2(x)$ respectively, i.e.,

$$f_1(x)^e = \sum_{k=0}^{3e} \alpha_k x^k \quad \text{and} \quad f_2(x)^e = \sum_{k=0}^{3e} \beta_k x^k.$$

Let γ_i be the x^i -coefficient of $f(x)^{(p-1)/2}$ with $f(x) = f_1(x)f_2(x)$ as in (8). We have

$$\gamma_i = \sum_{k=0}^{3e} \alpha_k \beta_{i-k}$$

and recall that $a = \gamma_{p-1}$, $b = \gamma_{2p-1}$, $c = \gamma_{p-2}$ and $d = \gamma_{2p-2}$. Put

$$F_2(x) := x^3 + A_2 v^2 x + B_2 v^3. \quad (32)$$

Note $f_2(x) = F_2(x - \lambda)$. We denote by β'_n the x^n -coefficient of $F_2(x)^e$, i.e.,

$$F_2(x)^e = \sum_{n=0}^{3e} \beta'_n x^n \quad (33)$$

with $\beta'_{3e} = 1$. Looking at the x^k -coefficients of both sides of $f_2(x)^e = F_2(x - \lambda)^e$, we have

$$\beta_k = \sum_{n=k}^{3e} \binom{n}{k} \beta'_n \cdot (-\lambda)^{n-k}. \quad (34)$$

From this, we find the highest terms in λ of β_k for some k , making use of $\binom{n}{k} = 0$ in $\mathbb{F}_p$ if $0 \leq k \leq p-1$ and $p \leq n \leq p+k-1$:

Lemma 5.1 *The coefficient β_k is a homogeneous polynomial in $K[\lambda, v]$ of degree $3e - k$. Moreover*

- (1) *the highest term in λ of β_0 is $(-\lambda)^{3e}$,*
- (2) *the highest term in λ of β_1 is $3e(-\lambda)^{3e-1}$,*
- (3) *the highest term in λ of β_e is $\binom{p-2}{e} \beta'_{p-2} \cdot (-\lambda)^{\frac{p-3}{2}}$ and*
- (4) *the highest term in λ of β_{e+1} is $\binom{p-2}{e+1} \beta'_{p-2} \cdot (-\lambda)^{\frac{p-5}{2}}$.*

Proof Note that β'_n is a monomial in $K[v]$ of degree $3e - n$, since $F_2(x)^e$ is homogeneous of degree $3e$ as a polynomial in $K[x, v]$. Hence, by (34) the coefficient β_k is a homogeneous polynomial in $K[\lambda, v]$ of degree $3e - k$.

(1) and (2): For $k = 0, 1$, the highest term in λ of β_k is the term of $n = 3e$ of (34), which is

$$\binom{3e}{k} (-\lambda)^{3e-k}.$$

(3) and (4): Let k be e or $e + 1$. Since $\binom{n}{k} = 0$ for $p \leq n \leq p+k-1$ with $p+k-1 \geq 3e$, it follows from (34) that

$$\beta_k = \sum_{n=k}^{p-1} \binom{n}{k} \beta'_n \cdot (-\lambda)^{n-k}. \quad (35)$$

Since E_2 is supersingular, we have $\beta'_{p-1} = 0$ and $\beta'_{p-2} \neq 0$ by Corollary 4.4. Hence, the highest term in λ of (35) is

$$\binom{p-2}{k} \beta'_{p-2} \cdot (-\lambda)^{p-2-k}.$$

Note that $p-2 \geq k$ for $k = e$ and $e+1$ if $p \geq 5$. □

Remark 5.2 The assumption $p > 3$ is used in Lemma 5.1 (2) and (4). This is the reason why the proof of the main theorem does not work for $p = 3$. In fact, there is no superspecial Howe curve in characteristic 3, see Remark 5.8.

In the next lemma, we study the order $\text{ord}_\mu(a)$ of a with respect to μ and so on, where $\text{ord}_\mu(a)$ is the largest number k such that a is a multiple of μ^k in $K[\lambda, \mu, v]$.

Lemma 5.3 *We have the following:*

- (1) $\text{ord}_\mu(a) = \frac{p+1}{2}$.
- (2) $\text{ord}_\mu(c) = \frac{p+1}{2}$.

- (3) $\text{ord}_\mu(ad - bc) = \text{ord}_v(ad - bc) = \frac{p+1}{2}$.
 (4) $\frac{ad-bc}{(\mu v)^{\frac{p+1}{2}}} \equiv B\lambda^{2p-4} \pmod{(\mu, v)}$ for some constant $B \in K^\times$.

Proof (1) We claim that there exists $\tilde{\alpha}_k \in K$ such that $\alpha_k = \mu^{3e-k}\tilde{\alpha}_k$ for each $0 \leq k \leq 3e$ with $e = (p-1)/2$. Indeed, we have

$$\begin{aligned} \alpha_k &= \sum_{3n_0+n_1=k} \frac{e!}{n_0!n_1!(e-n_0-n_1)!} (A_1\mu^2)^{n_1} (B_1\mu^3)^{e-n_0-n_1} \\ &= \left(\sum_{3n_0+n_1=k} \frac{e!}{n_0!n_1!(e-n_0-n_1)!} A_1^{n_1} B_1^{e-n_0-n_1} \right) \mu^{3e-k}, \end{aligned}$$

and thus α_k is a multiple of μ^{3e-k} . Putting $\tilde{\alpha}_k := \alpha_k/(\mu^{3e-k})$, we also have $\tilde{\alpha}_k \in K$ for $0 \leq k \leq 3e$. Since both the elliptic curves $E_1 : z^2 = f_1(x)$ and $E_2 : w^2 = f_2(x)$ are supersingular, we have $\alpha_{p-1} = 0$ and $\beta_{p-1} = 0$, whereas $\alpha_{p-2} \neq 0$ (and thus $\tilde{\alpha}_{p-2} \neq 0$) and $\beta_{p-2} \neq 0$ by Corollary 4.4. It follows that

$$a = \gamma_{p-1} = \sum_{k=1}^{p-2} \alpha_k \beta_{p-1-k} = \sum_{k=1}^{p-2} \mu^{3e-k} \tilde{\alpha}_k \beta_{p-1-k} = \sum_{j=\frac{p+1}{2}}^{\frac{3p-5}{2}} \mu^j \tilde{\alpha}_{3e-j} \beta_{j-e}, \quad (36)$$

where β_k is a polynomial in $K[\lambda, v]$ for each $0 \leq k \leq 3e$. Since $\beta_1 \neq 0$ by Lemma 5.1 (2), we have $\tilde{\alpha}_{3e-j} \beta_{j-e} = \tilde{\alpha}_{p-2} \beta_1 \neq 0$ for $j = (p+1)/2$, and thus $\text{ord}_\mu(a) = (p+1)/2$.

(2) Similarly to the proof of (1), one has

$$c = \gamma_{p-2} = \sum_{k=0}^{p-2} \alpha_k \beta_{p-2-k} = \sum_{k=0}^{p-2} \mu^{3e-k} \tilde{\alpha}_k \beta_{p-2-k} = \sum_{j=\frac{p+1}{2}}^{\frac{3p-3}{2}} \mu^j \tilde{\alpha}_{3e-j} \beta_{j-e-1}. \quad (37)$$

Since we have $\tilde{\alpha}_{p-2} \neq 0$, and $\beta_0 \neq 0$ by Lemma 5.1 (1), we also have $\tilde{\alpha}_{3e-j} \beta_{j-e-1} = \tilde{\alpha}_{p-2} \beta_0 \neq 0$ for $j = (p+1)/2$, and thus $\text{ord}_\mu(c) = (p+1)/2$.

(3) Similarly to the proof of (1), remaining two entries of the Cartier-Manin matrix M are written as

$$b = \gamma_{2p-1} = \sum_{k=\frac{p+1}{2}}^{\frac{3}{2}(p-1)} \alpha_k \beta_{2p-1-k} = \sum_{k=\frac{p+1}{2}}^{\frac{3}{2}(p-1)} \mu^{3e-k} \tilde{\alpha}_k \beta_{2p-1-k} = \sum_{j=0}^{p-2} \mu^j \tilde{\alpha}_{3e-j} \beta_{j+e+1}, \quad (38)$$

$$d = \gamma_{2p-2} = \sum_{k=\frac{p-1}{2}}^{\frac{3}{2}(p-1)} \alpha_k \beta_{2p-2-k} = \sum_{k=\frac{p-1}{2}}^{\frac{3}{2}(p-1)} \mu^{3e-k} \tilde{\alpha}_k \beta_{2p-2-k} = \sum_{j=0}^{p-1} \mu^j \tilde{\alpha}_{3e-j} \beta_{j+e}, \quad (39)$$

both of which are not a multiple of μ since $\alpha_{3e} = 1$ and since $\beta_e, \beta_{e+1} \neq 0$ by Lemma 5.1 (3) and (4). Thus, if the coefficient of $\mu^{(p+1)/2}$ in $ad - bc$ is not zero, then we have $\text{ord}_\mu(ad - bc) = (p+1)/2$. By straightforward computation, the coefficients of $\mu^{(p+1)/2}$ in ad and bc are $\tilde{\alpha}_{p-2} \beta_1 \tilde{\alpha}_{3e} \beta_e$ and $\tilde{\alpha}_{p-2} \beta_0 \tilde{\alpha}_{3e} \beta_{e+1}$, respectively. Here we have

$$\tilde{\alpha}_{p-2} \beta_1 \tilde{\alpha}_{3e} \beta_e - \tilde{\alpha}_{p-2} \beta_0 \tilde{\alpha}_{3e} \beta_{e+1} = \tilde{\alpha}_{p-2} \tilde{\alpha}_{3e} (\beta_1 \beta_e - \beta_0 \beta_{e+1}),$$

where $\tilde{\alpha}_{p-2} \neq 0$ and $\tilde{\alpha}_{3e} = \alpha_{3e} = 1$. If $\beta_1 \beta_e - \beta_0 \beta_{e+1} \neq 0$, we have $\text{ord}_\mu(ad - bc) = (p+1)/2$. By Lemma 5.1, the highest term of $\beta_1 \beta_e$ in λ is

$$3e(-\lambda)^{3e-1} \cdot \binom{p-2}{e} \beta'_{p-2} \cdot (-\lambda)^{e-1} = 3e \binom{p-2}{e} \beta'_{p-2} \cdot (-\lambda)^{2p-4}$$

and that of $\beta_0\beta_{e+1}$ is

$$(-\lambda)^{3e} \cdot \binom{p-2}{e+1} \beta'_{p-2} \cdot (-\lambda)^{e-2} = \binom{p-2}{e+1} \beta'_{p-2} \cdot (-\lambda)^{2p-4}.$$

Since $\beta'_{p-2} \neq 0$ by Corollary 4.4, it suffices to show

$$3e \binom{p-2}{e} \neq \binom{p-2}{e+1}$$

in $\mathbb{F}_p$. If the equality held, we would have $3e/(p-2-e) = 1/(e+1)$ in $\mathbb{F}_p$. Multiplying the denominators and the numerators of both sides by 2, we get $3(p-1)/(p-3) = 2/(p+1)$ in $\mathbb{F}_p$. But the left hand side is equal to 1 and the right hand side is equal to 2. This is a contradiction.

Next, we show $\text{ord}_v(ad-bc) = (p+1)/2$. To show this, we consider the transformation $X = x - \lambda$. The polynomials $f_1(x)$ and $f_2(x)$ are rewritten as

$$F_1(X) = (X + \lambda)^3 + A_1\mu^2(X + \lambda) + B_1\mu^3, \quad (40)$$

$$F_2(X) = X^3 + A_2v^2X + B_2v^3 \quad (41)$$

respectively. Let γ'_l denote the coefficient of X^l in $(F_1(X)F_2(X))^{(p-1)/2}$. Putting $a' = \gamma'_{p-1}$, $c' = \gamma'_{p-2}$, $b' = \gamma'_{2p-1}$ and $d' = \gamma'_{2p-2}$, we have $ad-bc = a'd' - b'c'$ by the second assertion of Lemma 2.4. By the same argument as in the proof of $\text{ord}_\mu(ad-bc) = (p+1)/2$ for $f_1(x)$ and $f_2(x)$, we have $\text{ord}_v(a'd' - b'c') = (p+1)/2$ for $F_2(X)$ and $F_1(X)$, and thus $\text{ord}_v(ad-bc) = (p+1)/2$.

(4) From the first part of the proof of (3), the coefficient of $(\mu v)^{\frac{p+1}{2}}$ in $ad-bc$ is $B\lambda^{2p-4}$ with

$$B := \tilde{\alpha}_{p-2}\tilde{\alpha}_{3e}(\beta'_{p-2}/v^{\frac{p+1}{2}}) \left(3e \binom{p-2}{e} - \binom{p-2}{e+1} \right) (-1)^{2p-4},$$

which is not zero. Recall from the proof of (1) that $\tilde{\alpha}_{p-2}$ and $\tilde{\alpha}_{3e}$ are non-zero constants in k . Recall also from the beginning of this section that β'_{p-2} is a monomial in $K[v]$ of degree $3e - (p-2) = (p+1)/2$, and thus $(\beta'_{p-2}/v^{\frac{p+1}{2}}) \in K^\times$. Thus, the assertion of (4) holds. $\square$

Let $R := K[\lambda, \mu, v]$ and put

$$h_0 := (ad-bc)/(\mu v)^{(p+1)/2},$$

$$h_1 := ab^{p-1} + d^p,$$

$$h_2 := a^p + c^{p-1}d,$$

which belong to R . Since a, b, c and d are homogeneous polynomials in λ, μ, v of degrees $2p-2, p-2, 2p-1$ and $p-1$ respectively, we have that h_0, h_1 and h_2 are homogeneous of degrees $2p-4, p(p-1)$ and $2p(p-1)$ respectively. We have the stratification

$$V(h_0, h_1, h_2) \subset V(h_0) \subset \mathbf{P}^2$$

as mentioned in Sect. 3. Our aim is to prove that any point $(\lambda : \mu : v)$ of $V(h_0, h_1, h_2)$ is of Howe type. In particular, we need to prove that μ and v are not zero. First we show:

Lemma 5.4 Assume $p > 3$. For any point $(\lambda_0 : \mu_0 : v_0)$ on $V(h_0)$ in $\mathbf{P}^2$, we have $\mu_0 \neq 0$ or $v_0 \neq 0$.

Proof It suffices to show that $\mu_0 = v_0 = 0$ implies $\lambda_0 = 0$ for $(\lambda_0 : \mu_0 : v_0) \in V(h_0)$. This immediately follows from Lemma 5.3 (4). $\square$

Thanks to Lemma 5.4, it suffices to consider the set of points with $\mu \neq 0$ or $\nu \neq 0$. We study only the case of $\nu \neq 0$, since a similar argument works also for $\mu \neq 0$ (exchange the roles of μ and ν by the coordinate change $X = x - \lambda$ as in (40) and (41)). From now on, we substitute 1 for ν and consider a, b, c, d as polynomials in λ, μ , i.e., we work over the ring

$$S := K[\lambda, \mu].$$

Set $a' = a/\mu^{(p+1)/2}$ and $c' = c/\mu^{(p+1)/2}$, which belong to S by Lemma 5.3 (1) and (2). Let a'_0, c'_0, b_0, d_0 be the constant terms of a', c', b, d as polynomials in μ , which are polynomials in λ .

Lemma 5.5 *As polynomials in λ , we have*

- (1) c'_0 and d_0 are coprime.
- (2) b_0 and d_0 are coprime.

Proof Since β_k is the x^k -coefficient of “the Maclaurin series expansion” of $f_2(x)^e = F_2(x - \lambda)^e$, we have

$$\beta_k = \frac{1}{k!} (F_2^e)^{(k)}(-\lambda) \quad (42)$$

if $k < p$. We use the fact that $\tilde{\alpha}_k := \alpha_k/\mu^{3e-k}$ belongs to K for $0 \leq k \leq 3e$ with $\tilde{\alpha}_{p-2} \neq 0$ and $\tilde{\alpha}_{3e} \neq 0$, as seen in the proof of Lemma 5.3 (1).

- (1) By (37) and (39), we have

$$c'_0 = \tilde{\alpha}_{p-2}\beta_0 \quad \text{and} \quad d_0 = \tilde{\alpha}_{3e}\beta_e.$$

As $\tilde{\alpha}_{p-2}$ and $\tilde{\alpha}_{3e}$ are non-zero constants, it suffices to see that β_0 and β_e are coprime as polynomials in λ . Since

$$\beta_0 = F_2^e(-\lambda), \quad \beta_e = \frac{1}{e!} (F_2^e)^{(e)}(-\lambda)$$

and F_2 is a separable polynomial, β_0 and β_e are coprime by the next claim. For any separable $Q(\lambda) \in K[\lambda]$ and for any integer n with $0 \leq n < p$, we claim that $Q(\lambda)^n$ and $(Q(\lambda)^n)^{(n)}$ are coprime. Indeed, let r be any root of $Q(\lambda)$ and write $Q(\lambda) = (\lambda - r)Q_0(\lambda)$ with $Q_0(r) \neq 0$. By the generalized Leibniz rule, we have

$$(Q(\lambda)^n)^{(n)} = \sum_{i=0}^n \binom{n}{i} \frac{n!}{i!} (\lambda - r)^i (Q_0(\lambda)^n)^{(i)}.$$

Hence $(Q(\lambda)^n)^{(n)}|_{\lambda=r} = n!Q_0(r)^n \neq 0$.

- (2) By (38) and (39), we have

$$b_0 = \tilde{\alpha}_{3e}\beta_{e+1} \quad \text{and} \quad d_0 = \tilde{\alpha}_{3e}\beta_e.$$

As $\tilde{\alpha}_{3e}$ is a non-zero constant, it suffices to see that β_e and β_{e+1} are coprime. This follows from

$$\beta_e = \frac{1}{e!} (F_2^e)^{(e)}(-\lambda), \quad \beta_{e+1} = \frac{1}{(e+1)!} (F_2^e)^{(e+1)}(-\lambda),$$

since $(F_2^e)^{(e)}(-\lambda)$ is separable by Corollary 4.7. $\square$

Now let us show that if $(\lambda_0, \mu_0, \nu_0)$ satisfies $h_i = 0$ for $i = 0, 1, 2$, then $(\lambda_0, \mu_0, \nu_0)$ is of Howe type. This is a key ingredient of this paper, as we explained in Sect. 3.

Proposition 5.6 *Suppose that $p > 3$. Then any point $(\lambda_0 : \mu_0 : \nu_0)$ on $V(h_0, h_1, h_2)$ is of Howe type.*

Proof Let $(\lambda_0 : \mu_0 : \nu_0)$ be a point of $V(h_0, h_1, h_2)$. By Lemma 5.4, we have $\mu_0 \neq 0$ or $\nu_0 \neq 0$. Consider the case of $\nu_0 \neq 0$. We study the open affine subscheme of $V(h_0, h_1, h_2)$ defined by $\nu \neq 0$. Substituting 1 for ν , it is isomorphic to $\text{Spec } S/J$, where $S = K[\lambda, \mu]$ and J is the ideal $\langle h_0(\lambda, \mu, 1), h_1(\lambda, \mu, 1), h_2(\lambda, \mu, 1) \rangle_S$ of S . On S/J , we have

$$\begin{aligned} a'_0 d_0 - b_0 c'_0 &\equiv h_0(\lambda, \mu, 1) = 0 \pmod{\mu}, \\ d_0^p &\equiv h_1(\lambda, \mu, 1) = 0 \pmod{\mu}. \end{aligned}$$

By Lemma 5.5, $a'_0 d_0 - b_0 c'_0$ and d_0^p are coprime as polynomials in λ , and therefore there exist polynomials u, v in λ such that $u(a'_0 d_0 - b_0 c'_0) + v d_0^p = 1$. Hence we have $1 \equiv 0 \pmod{\mu}$. This means that μ is unit in S/J . Thus we have shown that $\nu_0 \neq 0$ implies $\mu_0 \neq 0$ for any point $(\lambda_0 : \mu_0 : \nu_0)$ on $V(h_0, h_1, h_2)$. A similar argument shows that $\mu_0 \neq 0$ implies that $\nu_0 \neq 0$ (exchange the roles of μ and ν by the coordinate change $X = x - \lambda$ as in (40) and (41)). Hence we conclude that both of μ_0 and ν_0 are not zero.

It remains to show that $f_1(x)$ and $f_2(x)$ defined in (3) and (4) for $(\lambda_0, \mu_0, \nu_0)$ are coprime. As μ_0 and ν_0 are not zero, $f_1(x)$ and $f_2(x)$ are separable polynomials. Suppose that $f_1(x)$ and $f_2(x)$ were not coprime. After taking a linear coordinate change, they are written as $f_1(x) = x(x-1)(x-t_1)$ and $f_2(x) = x(x-t_2)(x-t_3)$. Then

$$(f_1(x)f_2(x))^e = x^{p-1}((x-1)(x-t_1)(x-t_2)(x-t_3))^e.$$

Then the Cartier-Manin matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ of the curve $y^2 = f_1(x)f_2(x)$ becomes a upper triangular matrix (i.e., $c = 0$) with $a = (t_1 t_2 t_3)^e$. Since $f_1(x)$ and $f_2(x)$ are separable, we have $t_i \neq 0$ for $i = 1, 2, 3$ and therefore $h_2 = a^p + c^{p-1}d \neq 0$. This is a contradiction. $\square$

Finally we show that $V(h_0, h_1, h_2)$ is not empty. The fact is reminiscent of the quasi-affineness (cf. [18, (6.5). Theorem]) of Ekedahl-Oort strata in the case of the moduli space of principally polarized abelian varieties.

Proposition 5.7 *Assume $p > 3$. Then $V(h_0, h_1, h_2)$ is non-empty and finite.*

Proof We suppose that $V(h_0, h_1, h_2) = \emptyset$ were true. Set $X := V(h_0) = V(h_0) \setminus V(h_0, h_1, h_2)$. Note that (a, d) can not be $(0, 0)$ on X , since $(a, d) = (0, 0)$ implies $h_1 = h_2 = 0$. Consider the morphism

$$\varphi : X \longrightarrow \mathbf{P}^1 \setminus \{(0 : 1)\} \simeq \mathbf{A}^1$$

sending $(\lambda : \mu : \nu)$ to $(a^p + c^{p-1}d : c^{p-1}d)$ for the part of $a \neq 0$ and $(ab^{p-1} + d^p : d^p)$ for the part of $d \neq 0$, which is well-defined, i.e., $(a^p + c^{p-1}d, c^{p-1}d) \neq (0, 0)$ for $a \neq 0$ and $(ab^{p-1} + d^p, d^p) \neq (0, 0)$ for $d \neq 0$ with the equality $(a^p + c^{p-1}d : c^{p-1}d) = (ab^{p-1} + d^p : d^p)$ for $a \neq 0$ and $d \neq 0$ deduced from (16). Let Y be the scheme-theoretic image of φ ([8, Chap. II, Exercise 3.11, (d)]). Note that Y is affine, as it is a closed subscheme of $\mathbf{A}^1$. Since the scheme-theoretic image of a proper scheme is proper (cf. [8, Chap. II, Exercise 4.4]), Y has to be finite. But, this is absurd, since the image of φ is not finite by the following two facts. Firstly X is connected, since it is a hypersurface in $\mathbf{P}^2$ (cf. [8, Chap. III, Cor. 7.9]). Secondly the image of φ contains two distinct points. Indeed, $(1 : 1)$ (resp. $(1 : 0)$) is in

the image of φ , since there exists a point of $\mathbf{P}^2$ where $h_0 = 0$ and $a = 0$ (resp. $h_0 = 0$ and $d = 0$), by [8, Chap. I, Theorem 7.2].

In the proof of Proposition 5.6, we have seen that $V(h_0, h_1, h_2)$ is contained in $\mathbf{P}^2 \setminus V(\mu) \simeq \mathbf{A}^2$, whence $V(h_0, h_1, h_2)$ is affine. Thus, $V(h_0, h_1, h_2)$ is finite, as it is projective. $\square$

Finally, we look at the case of $p = 3$.

Remark 5.8 Assume $p = 3$. There exists a unique supersingular elliptic curve $y^2 = x^3 - x$. We use the notation in Sect. 2. Remark that we assumed $p > 3$ in Sect. 2 only to assure that any elliptic curve can be written as $y^2 = x^3 + Ax + B$ and that all arguments in Sect. 2 work for $A_1 = A_2 = -1$ and $B_1 = B_2 = 0$ with $p = 3$. It is straightforward to see that the $(1, 1)$ -entry of MM^σ is equal to $(\mu\nu)^8$. Hence the supersingularity of C associated to (λ, μ, ν) implies that μ or ν is zero, whence (λ, μ, ν) is not of Howe type. Thus, we conclude that there is no supersingular Howe curve for $p = 3$.

Acknowledgements

The authors thank Everett Howe, Tomoyoshi Ibukiyama and Rachel Pries for their valuable helpful comments to earlier versions of this paper. The authors are also grateful to the anonymous referees for their careful reading of this article and their comments. This work was supported by JSPS Grant-in-Aid for Research Activity Start-up Grant Nos. 18H05836, 19K21026, 20K14301 and JSPS Grant-in-Aid for Scientific Research (C) 17K05196.

Author details

¹Department of Mathematical Informatics, Graduate School of Information Science and Technology, The University of Tokyo, Tokyo, Japan, ²Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan, ³Research conducted while at Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan.

Received: 23 October 2019 Accepted: 19 September 2020 Published online: 27 October 2020

References

1. Achter, J., Howe, E.: Hasse–Witt and Cartier–Manin matrices: a warning and a request. In: Aubry, Y., Howe, E.W., Ritzenthaler, C. (eds.) *Arithmetic Geometry: Computation and Applications Contemporary Mathematics*, vol. 722. American Mathematical Society, Providence, RI (2019)
2. Chai, C.-L., Oort, F.: Monodromy and irreducibility of leaves. *Ann. Math. (2)* **173**(3), 1359–1396 (2011)
3. de Jong, A.J., Oort, F.: Purity of the stratification by Newton polygons. *J. Am. Math. Soc.* **13**(1), 209–241 (2000)
4. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg* **14**(1), 197–272 (1941)
5. Glass, D., Pries, R.: Hyperelliptic curves with prescribed p -torsion. *Manuscripta Math.* **117**, 299–317 (2005)
6. González, J.: Hasse–Witt matrices for the Fermat curves of prime degree. *Tohoku Math. J. (2)* **49**(2), 149–163 (1997)
7. Harashita, S.: Ekedahl–Oort strata and the first Newton slope strata. *J. Algebr. Geom.* **16**(1), 171–199 (2007)
8. Hartshorne, R.: *Algebraic Geometry*, Graduate Texts in Mathematics **52**. Springer, New York (1977)
9. Howe, E.: Quickly constructing curves of genus 4 with many points. In: Kohel, D., Shparlinski, I. (eds.) *Frobenius Distributions: Sato–Tate and Lang–Trotter conjectures Contemporary Mathematics*, vol. 663, pp. 149–173. American Mathematical Society, Providence, RI (2016)
10. Ibukiyama, T.: On rational points of curves of genus 3 over finite fields. *Tohoku Math. J.* **45**, 311–329 (1993)
11. Ibukiyama, T., Katsura, T., Oort, F.: Supersingular curves of genus two and class numbers. *Compos. Math.* **57**(2), 127–152 (1986)
12. Igusa, J.-I.: Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. USA* **44**, 312–314 (1958)
13. Kani, E., Rosen, M.: Idempotent relations and factors of Jacobians. *Math. Ann.* **284**, 307–327 (1989)
14. Kudo, M.: On the existence of superspecial nonhyperelliptic curves of genus 4. *Commun. Algebra* **47**(12), 5020–5038 (2019). <https://doi.org/10.1080/00927872.2019.1609013>
15. Li, W., Mantovan, E., Pries, R., Tang, Y.: Newton polygon stratification of the Torelli locus in PEL-type Shimura varieties, [arXiv:1811.00604](https://arxiv.org/abs/1811.00604) [math.NT]
16. Li, W., Mantovan, E., Pries, R., Tang, Y.: Newton polygons arising for special families of cyclic covers of the projective line. *Res. Number Theory* **5**(1), 12 (2019)
17. Oort, F.: Hyperelliptic supersingular curves, *Progress in Mathematics* **89**, pp. 247–284, Birkhäuser, Boston, (1991)
18. Oort, F.: A stratification of a moduli space of abelian varieties, *Progress in Mathematics* **195**, pp. 345–416, Birkhäuser, Basel, (2001)
19. Pries, R.: Current results on Newton polygons of curves. *Open problems in arithmetic algebraic geometry. Adv. Lect. Math.* **46**, 179–207 (2019)
20. Serre, J.-P.: Nombre des points des courbes algebrique sur $\mathbf{F}_q$. *Sém. Théor. Nombres Bordeaux* **12**, 22 (1982–1983)
21. Silverman, J.H.: *The Arithmetic of Elliptic Curves*, Second edition. Graduate Texts in Mathematics **106**. Springer, Dordrecht (2009)

22. van der Geer, G., van der Vlugt, M.: On the existence of supersingular curves of given genus. *J. Reine Angew. Math.* **458**, 53–61 (1995)
23. Yui, N.: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *J. Algebra* **52**(2), 378–410 (1978)

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.