COMPOSITIO MATHEMATICA

TOMOYOSHI IBUKIYAMA
TOSHIYUKI KATSURA
FRANS OORT

Supersingular curves of genus two and class numbers

Compositio Mathematica, tome 57, n° 2 (1986), p. 127-152
<http://www.numdam.org/item?id=CM_1986__57_2_127_0>

Compositio Mathematica 57 (1986) 127–152.

SUPERSINGULAR CURVES OF GENUS TWO AND CLASS NUMBERS

Tomoyoshi Ibukiyama *, Toshiyuki Katsura ** and Frans Oort

§0. Introduction

An abelian variety A over an algebraically closed field k of characteristic $p > 0$ is called supersingular if there exists an isogeny $A \sim E^n$, where E is a supersingular elliptic curve (cf. Oort [17], Section 4); we say a curve C is supersingular if its Jacobian $A = J(C)$ is supersingular. A supersingular abelian variety has no points of order p, and the converse holds if $\dim A$ is at most 2. Let $A_{2,1}$ be the coarse moduli scheme of principally polarized abelian surfaces over k. We like to study the set of principally polarized supersingular abelian surfaces

$$V \subset A_{2,1}$$

for every characteristic. It is known that every component of V has dimension one (cf. Koblitz [11], Theorem 7 on page 163), and that every component of V is a rational curve (cf. Oort [17], p. 117). Our final results (cf. Katsura and Oort [10]) will be

$$V \text{ is irreducible} \Leftrightarrow p \leqslant 11.$$

Moreover, we can explicitly calculate the number of irreducible components of V (cf. Remark 2.16). To this end, we first study all curves of genus two; these appear as the polar part of a principal polarization on an abelian surface. In the fundamental paper by Igusa (cf. [9]), we find a complete list of all possible automorphism groups for a curve of genus two. Of course, the prime numbers p with $p \leqslant 5$ need special attention.

In Section 1 we recall these results, we use properties of the Hasse-Witt matrix, and we describe which curves with "many automorphisms" (i.e. $|\mathrm{Aut}(C)| > 2$) are supersingular.

In Section 2 we give the link between the geometry (polarizations) and the number theory (class numbers) involved. We show that the class

* Partially supported by Max-Planck-Institut für Mathematik.
** Partially supported by Z.W.O. (Netherlands Organization for the Advancement of Pure Research), "Moduli", 10-80-004.

number of the principal genus in B^n with B, the definite quaternion algebra over the rational number with discriminant p, is equal to the number of isomorphism classes of principally polarized abelian varieties (A, Θ) with principal polarization Θ, such that A is isomorphic to a product of n supersingular elliptic curves. This enables us to compute explicitly the total number of supersingular curves of genus two whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves (cf. Corollary 2.10). We also examine the class number of the non-principal genus in B^2 (cf. Theorem 2.15). It gives us the tool to relate the number of irreducible components of V with the explicit formula by Hashimoto and Ibukiyama (cf. [6] (II) and (III)); this connection will be given in a subsequent paper (cf. Katsura and Oort [10]).

In Section 3 we finish the study of the supersingularity of various types. We will determine explicitly the number of supersingular curves of genus two with fixed reduced group of automorphisms whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves (cf. Theorem 3.2).

We might remark that it seems interesting to study the stratification by p-rank of moduli spaces of abelian varieties of dimension g in characteristic p. This stratification is completely known in case $g = 1$. The next case p-rank $= 0$ for $g = 2$ is the one studied in this and subsequent paper. Our results seem rather complete, and the description in this case already turns out to be more involved than in the case of elliptic curves.

The second and the third author would like to thank Professor K. Ueno for his stimulating conversation. The first and the second author would like to thank Professor K. Hashimoto for valuable conversation. They would also like to thank University of Utrecht for warm hospitality during their stay in Utrecht.

§1. Jacobian varieties of curves of genus two

1.1. The Hasse-Witt matrix

Let k be an algebraically closed field of characteristic $p \geqslant 3$, and let C be a non-singular complete algebraic curve of genus two defined over k. By a suitable choice of the coordinate system (x, y), the curve C is a non-singular complete model of the curve defined by the equation

$$y^2 = f(x), \tag{1.1}$$

where $f(x)$ is a polynomial of degree 5 or 6 which has only simple zeros. We mean a curve C defined by an equation a non-singular complete model of the affine curve defined by this equation. We denote by $\mathscr{C}$ the Cartier operator on the k-vector space $H^0(C, \Omega^1_C)$ of regular 1-forms on

C. We fix the following basis of $H^0(C, \Omega^1_C)$:

$$\mathrm{d}x/y,\ x\mathrm{d}x/y. \tag{1.2}$$

We consider the following expansion

$$f(x)^{(p-1)/2} = \sum_{j=0}^{N} c_j x^j \tag{1.3}$$

with $N = 5(p-1)/2$ if $\deg f(x) = 5$, $N = 3(p-1)$ if $\deg f(x) = 6$, and $c_j \in k$, $j = 0, 1, \ldots, N$, where $\deg f(x)$ denotes the degree of the polynomial $f(x)$. Using (1.2) and (1.3), we have the following representation by a matrix of the Cartier operator $\mathscr{C}$:

$$\mathscr{C}(\mathrm{d}x/y,\ x\mathrm{d}x/y) = (\mathrm{d}x/y,\ x\mathrm{d}x/y)M^{(1/p)}, \tag{1.4}$$

where M is the 2×2 matrix with elements in k given by

$$M = \begin{pmatrix} c_{p-1} & c_{p-2} \\ c_{2p-1} & c_{2p-2} \end{pmatrix} \quad \text{and} \quad M^{(1/p)} = \begin{pmatrix} \sqrt[p]{c_{p-1}} & \sqrt[p]{c_{p-2}} \\ \sqrt[p]{c_{2p-1}} & \sqrt[p]{c_{2p-2}} \end{pmatrix} \tag{1.5}$$

(cf. Manin [13], p. 78, Shioda [20], p. 159, and Yui [23], p. 381). The matrix $M^{(1/p)}$ is called the Hasse-Witt matrix of the curve C defined by (1.1). The following lemma is well-known.

LEMMA 1.1:

(*i*) *The Jacobian variety $J(C)$ of the curve C defined by* (1.1) *is supersingular if and only if $M^{(p)}M = 0$, where*

$$M^{(p)} = \begin{pmatrix} c_{p-1}^p & c_{p-2}^p \\ c_{2p-1}^p & c_{2p-2}^p \end{pmatrix}.$$

(*ii*) *The Jacobian variety $J(C)$ is isomorphic to a product of two supersingular elliptic curves if and only if $M = 0$.*

(*iii*) *The Jacobian variety $J(C)$ is ordinary if and only if M has rank two.*

For the proofs, see Manin [13], p. 78, Nygaard [16], Theorem 4.1, Yui [23], Theorem 3.1, Theorem 4.1.

1.2. Curves of genus two with many automorphisms (general theory)

In this section, we again assume char. $k = p \geqslant 3$. We recall results by Igusa [9]. Every curve C defined by (1.1) is in a unique way a two-sheeted

covering of the projective line $\mathbb{P}^1$. We denote by ι the automorphism of C which is the generator of the Galois group of this two-sheeted covering. We denote by $\langle\iota\rangle$ the group generated by ι. The group $\langle\iota\rangle$ is of order two, and it is contained in the center of the group $\mathrm{Aut}(C)$ of automorphisms of C. We call the factor group $\mathrm{Aut}(C)/\langle\iota\rangle$ the reduced group of automorphisms of C, and denote it by $\mathrm{RA}(C)$. We can consider $\mathrm{RA}(C)$ as a group of automorphisms of the projective line $\mathbb{P}^1$. We call an element of $\mathrm{RA}(C)$ a reduced automorphism. If $\mathrm{RA}(C)$ has at least two elements, then we say that the curve C has many automorphisms. According to Igusa [9], a curve C with many automorphisms is isomorphic to one of the following curves:

(1) C: $y^2 = x(x-1)(x-\lambda)(x-\mu)\{x-\lambda(1-\lambda)^{-1}(1-\mu)\}$ with $\mathrm{RA}(C) \cong \mathbb{Z}/2$, unless by specialization this case reduces to one of the cases below,

(2) C: $y^2 = x(x-1)(x-\lambda)\{x-(\lambda-1)\lambda^{-1}\}\{x-(1-\lambda)^{-1}\}$ with $\mathrm{RA}(C) \cong S_3$, unless by specialization this case reduces to one of the cases below,

(3) C: $y^2 = x(x-1)(x+1)(x-\lambda)\{x-(1/\lambda)\}$ with $\mathrm{RA}(C) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, unless by specialization this case reduces to one of the cases below,

(4) ($p \neq 3, 5$) C: $y^2 = x(x-1)(x+1)(x-2)\{x-(1/2)\}$ with $\mathrm{RA}(C) \cong D_{12}$ (the dihedral group of order 12),

(5) C: $y^2 = x(x^2-1)(x^2+1)$ with $\mathrm{RA}(C) \cong S_4$ if $p \neq 5$, and $\mathrm{RA}(C) \cong \mathrm{PGL}(2, 5)$ if $p = 5$,

(6) ($p \neq 5$) C: $y^2 = x(x-1)(x-1-\zeta)(x-1-\zeta-\zeta^2)(x-1-\zeta-\zeta^2-\zeta^3)$ with $\mathrm{RA}(C) \cong \mathbb{Z}/5$, where ζ is a primitive fifth root of unity.

It should be noticed that each curve in Class (2) or (3) is a specialization of a curve in Class (1), and that each curve in Class (4) or (5) is a specialization of a curve in Class (2) and also of a curve in Class (3) (cf. Igusa [9]).

Now, we consider the following automorphism σ of order two of the curve in Class (1), (2), (3), (4) or (5):

$$\sigma: \begin{cases} x \mapsto \lambda(x-\mu)/(x-\lambda), \\ y \mapsto \lambda^{3/2}(\lambda-\mu)^{3/2} y/(x-\lambda)^3, \end{cases} \tag{1.6}$$

where $\lambda^{3/2}(\lambda-\mu)^{3/2}$ is a root of the equation $z^2 = \lambda^3(\lambda-\mu)^3$. We set

$$\tau = \sigma \cdot \iota. \tag{1.7}$$

Then we see that τ is also an automorphism of order two of C. We set

$$E_\sigma = C/\langle\sigma\rangle \quad \text{and} \quad E_\tau = C/\langle\tau\rangle. \tag{1.8}$$

By the Hurwitz formula, these are elliptic curves (cf. Igusa [9], Lemma 9). The fixed points of σ (resp. τ) are given by the equation

$$x = \lambda + (\lambda^2 - \lambda\mu)^{1/2} \quad \left(\text{resp. } x = \lambda - (\lambda^2 - \lambda\mu)^{1/2}\right). \tag{1.9}$$

We set

$$t = x + \lambda(x - \mu)/(x - \lambda). \tag{1.10}$$

Then, we see that t is invariant under the actions of σ and τ. Considering t as a coordinate of $\mathbb{P}^1$, we can express E_σ and E_τ as two-sheeted coverings of this $\mathbb{P}^1$. Then, considering the ramification points of E_σ and E_τ on $\mathbb{P}^1$, we have the following defining equations for E_σ and E_τ:

$$s^2 = (t - \mu)\{t - (1 - \lambda\mu)/(1 - \lambda)\}\left\{t - 2\left(\lambda \mp (\lambda^2 - \lambda\mu)^{1/2}\right)\right\} \tag{1.11}$$

with a suitable variable s. For the coordinate (t, s), we set

$$\begin{cases} t = (\mu - 1)X/(\lambda - 1) + \mu, \\ s = (\mu - 1)^{3/2}Y/(\lambda - 1)^{3/2}. \end{cases} \tag{1.12}$$

Then, we conclude E_σ and E_τ are respectively defined by the equations

$$Y^2 = X(X - 1)\left\{X - (1 - \lambda)\left(\mu - 2\lambda \pm 2(\lambda^2 - \lambda\mu)^{1/2}\right)/(\mu - 1)\right\}. \tag{1.13}$$

We consider a polynomial in u:

$$\psi(u) = u^2 - \{2(1 - \lambda)(\mu - 2\lambda)/(\mu - 1)\}u + \{(1 - \lambda)\mu/(\mu - 1)\}^2. \tag{1.14}$$

Then, $(1 - \lambda)(\mu - 2\lambda \pm 2(\lambda^2 - \lambda\mu)^{1/2})/(\mu - 1)$ are different zeros of $\psi(u)$.

DEFINITION 1.2 (Legendre polynomial).

$$\Phi(u) = \sum_{\nu=0}^{(p-1)/2} \binom{(p-1)/2}{\nu}^2 u^\nu.$$

PROPOSITION 1.3: *For the curve C of genus two in Class* (1), (2), (3), (4) *or* (5), *the following conditions are equivalent.*

(*i*) *The Jacobian variety $J(C)$ of C is a supersingular abelian surface.*

(*ii*) *The Jacobian variety $J(C)$ of C is isomorphic to a product of two supersingular elliptic curves.*

(*iii*) *E_σ and E_τ are supersingular.*

(*iv*) *$\psi(u)$ divides $\Phi(u)$.*

PROOF: The equivalence of (iii) and (iv) is trivial (cf. Deuring [1], §8). By Igusa [9], p. 648, we have the following mappings:

$$C \overset{j}{\hookrightarrow} J(C) \overset{\pi}{\to} E_\sigma \times E_\tau, \tag{1.15}$$

where $\pi \cdot j$ is the natural morphism defined by the natural projections, and π is an isogeny. Therefore, the equivalence of (i) and (iii) follows from (1.15). Let $H^0(C, \Omega^1_C)$ be the vector space of regular 1-forms on C. By a direct calculation, we see that $\mathrm{d}x/y + \sigma^*(\mathrm{d}x/y)$ (resp. $\mathrm{d}x/y + \tau^*(\mathrm{d}x/y)$) generates the one-dimensional subspace consisting of invariant elements of $H^0(C, \Omega^1_C)$ under σ^* (resp. τ^*). Moreover, it is clear that $\{\mathrm{d}x/y + \sigma^*(\mathrm{d}x/y), \mathrm{d}x/y + \tau^*(\mathrm{d}x/y)\}$ is a basis of $H^0(C, \Omega^1_C)$. Since the natural projections $C \to E_\sigma$ and $C \to E_\tau$ are separable morphisms of degree two we have isomorphisms

$$H^0\big(C, \Omega^1_C\big) \underset{\sim}{\overset{j^*}{\leftarrow}} H^0\big(J(C), \Omega^1_{J(C)}\big) \underset{\sim}{\overset{\pi^*}{\leftarrow}} H^0\big(E_\sigma, \Omega^1_{E_\sigma}\big) \oplus H^0\big(E_\tau, \Omega^1_{E_\tau}\big).$$

This means that π is a separable isogeny. Hence, using the theory of Oort [18], p. 36, we conclude that $J(C)$ is isomorphic to a product of two supersingular elliptic curves if both E_σ and E_τ are supersingular elliptic curves. This shows the equivalence of (ii) and (iii). Q.E.D.

REMARK 1.4: We write here the explicit equations of elliptic curves E_σ and E_τ for the classes (2), (3), (4) and (5).

(2) $y^2 = x(x-1)\{x - (1-\lambda)(\lambda \mp (\lambda^2 - \lambda + 1)^{1/2})^2\}$,

(3) $y^2 = x(x-1)\{x + (\lambda \mp (\lambda^2 - 1)^{1/2})^2\}$,

(4) $y^2 = x(x-1)\{x + (2 \mp \sqrt{3})^2\}$,

(5) $y^2 = x(x-1)\{x - (1 \mp \sqrt{2})^2\}$.

1.3. Curves of genus two with many automorphisms (special cases)

In this section, we assume char. $k = p \geqslant 3$. We consider the following two classes of curves of genus two defined by the equations

$$C_\alpha : y^2 = (x^3 - 1)(x^3 - \alpha),\ \alpha \neq 0, 1, \tag{a}$$

$$C_\beta : y^2 = x(x^2 - 1)(x^2 - \beta),\ \beta \neq 0, 1, \tag{b}$$

where in the case of (a), we assume $p \geqslant 5$. Since the curves defined by (a) have automorphisms of order three, any curve of genus two in Class (a) is isomorphic to a curve in Class (2), (4) or (5). Conversely, it is easy to show that any curve of genus two with automorphisms of order three is isomorphic to a curve in Class (a) with a suitable element $\alpha \in k$. Since the reduced groups of automorphisms of the curves in Class (b) contain the Klein four group $\mathbb{Z}/2 \times \mathbb{Z}/2$, any curve in Class (b) is isomorphic to a curve in Class (3), (4) or (5). To prove the converse, we consider an automorphism of $\mathbb{P}^1$ defined by

$$x \mapsto (x+1)/(x-1), \tag{1.16}$$

where x is a global coordinate of an affine line in $\mathbb{P}^1$ which is used in the equations in Classes (3), (4) and (5). Setting

$$\beta = (\lambda+1)^2/(\lambda-1)^2 \quad (\text{resp. } \beta = 9, \text{ resp. } \beta = -1), \tag{1.17}$$

and using the automorphism of $\mathbb{P}^1$ given by (1.16), we see that any curve C in Class (3) (resp. Class (4), resp. Class (5)) is isomorphic to a curve in Class (b) with β as given in (1.17). For these curves, we have the following:

LEMMA 1.5: *Let C_α and $C_{\alpha'}$ (resp. C_β and $C_{\beta'}$) be curves in Class (a) (resp. Class (b)). Then, the curve C_α (resp. C_β) is isomorphic to $C_{\alpha'}$ (resp. $C_{\beta'}$) if and only if $\alpha = \alpha'$ or $\alpha = 1/\alpha'$ (resp. $\beta = \beta'$ or $\beta = 1/\beta'$).*

PROOF: Let C_α and $C_{\alpha'}$ be curves in Class (a). Assume that C_α is isomorphic to $C_{\alpha'}$, say, $\tilde{\varphi}\colon C_\alpha \to C_{\alpha'}$ is an isomorphism. Since C_α (resp. $C_{\alpha'}$) is a two sheeted covering of $C_\alpha/\langle\iota\rangle \cong \mathbb{P}^1$ (resp. $C_{\alpha'}/\langle\iota\rangle \cong \mathbb{P}^1$), the isomorphism $\tilde{\varphi}$ induces an isomorphism φ from $\mathbb{P}^1 \cong C_\alpha/\langle\iota\rangle$ to $\mathbb{P}^1 \cong C_{\alpha'}/\langle\iota\rangle$. We have the following three cases:

(i) $\mathrm{RA}(C_\alpha) \cong \mathrm{RA}(C_{\alpha'}) \cong S_3$,
(ii) $\mathrm{RA}(C_\alpha) \cong \mathrm{RA}(C_{\alpha'}) \cong D_{12}$,
(iii) $\mathrm{RA}(C_\alpha) \cong \mathrm{RA}(C_{\alpha'}) \cong S_4$.

Let σ_α (resp. $\sigma_{\alpha'}$) be the element of $\mathrm{RA}(C_\alpha)$ (resp. $\mathrm{RA}(C_{\alpha'})$) defined by

$$\sigma_\alpha(\text{resp. } \sigma_{\alpha'})\colon x \mapsto \omega x, \tag{1.18}$$

where ω is a primitive cube root of unity. By the structure of the group $\mathrm{RA}(C_{\alpha'})$, the elements of order three in $\mathrm{RA}(C_{\alpha'})$ are conjugate to each other. Since $\varphi \cdot \sigma_\alpha \cdot \varphi^{-1}$ is an element of order three in $\mathrm{RA}(C_{\alpha'})$, we see that there exists an element θ in $\mathrm{RA}(C_{\alpha'})$ such that

$$\sigma_{\alpha'} = \theta \cdot \varphi \cdot \sigma_\alpha \cdot \varphi^{-1} \cdot \theta^{-1}. \tag{1.19}$$

Set $\psi = \theta \cdot \varphi$. Then, the isomorphism ψ from $\mathbb{P}^1 \cong C_\alpha/\langle \iota \rangle$ to $\mathbb{P}^1 \cong C_{\alpha'}/\langle \iota \rangle$ induces a bijection from the set of six branch points

$$S_\alpha = \{1, \omega, \omega^2, \sqrt[3]{\alpha}, \sqrt[3]{\alpha}\,\omega, \sqrt[3]{\alpha}\,\omega^2\}$$

to the six branch points

$$S_{\alpha'} = \{1, \omega, \omega^2, \sqrt[3]{\alpha'}, \sqrt[3]{\alpha'}\,\omega, \sqrt[3]{\alpha'}\,\omega^2\}.$$

The subgroup $\langle \sigma_\alpha \rangle$ (resp. $\langle \sigma_{\alpha'} \rangle$) generated by σ_α (resp. $\sigma_{\alpha'}$) acts on S_α (resp. $S_{\alpha'}$). It has two orbits $\mathcal{O}_1 = \{1, \omega, \omega^2\}$ and $\mathcal{O}_2 = \{\sqrt[3]{\alpha}, \sqrt[3]{\alpha}\,\omega, \sqrt[3]{\alpha}\,\omega^2\}$ (resp. $\mathcal{O}_1' = \{1, \omega, \omega^2\}$ and $\mathcal{O}_2' = \{\sqrt[3]{\alpha'}, \sqrt[3]{\alpha'}\,\omega, \sqrt[3]{\alpha'}\,\omega^2\}$). Therefore, by (1.19), the isomorphism ψ induces a mapping either from $\mathcal{O}_1$ to $\mathcal{O}_1$ and from $\mathcal{O}_2$ to $\mathcal{O}_2'$, or from $\mathcal{O}_1$ to $\mathcal{O}_2'$ and from $\mathcal{O}_2$ to $\mathcal{O}_1'$. In the former case, the isomorphism ψ, $\sigma_{\alpha'} \cdot \psi$ or $\sigma_{\alpha'}^2 \cdot \psi$ is the identity from $\mathcal{O}_1$ to $\mathcal{O}_1'$. Therefore, one of them is the identity from $\mathbb{P}^1 \cong C_\alpha/\langle \iota \rangle$ to $\mathbb{P}^1 \cong C_{\alpha'}/\langle \iota \rangle$. Hence, we have $\alpha = \alpha'$. In the latter case, we consider the automorphism θ' of $\mathbb{P}^1$ defined by

$$\theta' \colon x \mapsto x/\sqrt[3]{\alpha'}. \tag{1.20}$$

Then, the isomorphism $\theta' \cdot \psi$, $\theta' \cdot \sigma_{\alpha'} \cdot \psi$ or $\theta' \cdot \sigma_{\alpha'}^2 \cdot \psi$ is the identity from $\{1, \omega, \omega^2\}$ to $\{1, \omega, \omega^2\}$, hence, the identity from $\mathbb{P}^1$ to $\mathbb{P}^1$. Hence, the isomorphism ψ, $\sigma_{\alpha'} \cdot \psi$ or $\sigma_{\alpha'}^2 \cdot \psi$ is given by

$$x \mapsto \sqrt[3]{\alpha'}\,x. \tag{1.21}$$

Since this isomorphism gives a mapping from $\mathcal{O}_2$ to $\mathcal{O}_1'$, we conclude $\alpha\alpha' = 1$.

Next, let C_β and $C_{\beta'}$ be curves in Class (b). Assume that C_β is isomorphic to $C_{\beta'}$, say, $\tilde{\varphi}\colon C_\beta \to C_{\beta'}$ is an isomorphism. We denote by φ the isomorphism from $\mathbb{P}^1 \cong C_\beta/\langle \iota \rangle$ to $\mathbb{P}^1 \cong C_{\beta'}/\langle \iota \rangle$ which is induced by $\tilde{\varphi}$. We have the following three cases:

(i) $\mathrm{RA}(C_\beta) \cong \mathrm{RA}(C_{\beta'}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$,
(ii) $\mathrm{RA}(C_\beta) \cong \mathrm{RA}(C_{\beta'}) \cong D_{12}$,
(iii) $\mathrm{RA}(C_\beta) \cong \mathrm{RA}(C_{\beta'}) \cong S_4$.

We set

$$S_\beta = \{0, \infty, 1, -1, \sqrt{\beta}, -\sqrt{\beta}\}$$

$$\left(\text{resp. } S_{\beta'} = \{0, \infty, 1, -1, \sqrt{\beta'}, -\sqrt{\beta'}\}\right).$$

Let σ_β (resp. $\sigma_{\beta'}$) be the element of $\mathrm{RA}(C_\beta)$ (resp. $\mathrm{RA}(C_{\beta'})$) defined by

$$\sigma_\beta(\text{resp. } \sigma_{\beta'})\colon x \mapsto -x. \tag{1.22}$$

The subgroup $\langle\sigma_\beta\rangle$ of $\mathrm{RA}(C_\beta)$ (resp. $\langle\sigma_{\beta'}\rangle$ of $\mathrm{RA}(C_{\beta'})$) acts on S_β (resp. $S_{\beta'}$). It has four orbits $\mathcal{O}_1 = \{0\}$, $\mathcal{O}_2 = \{\infty\}$, $\mathcal{O}_3 = \{1, -1\}$ and $\mathcal{O}_4 = \{\sqrt{\beta}, -\sqrt{\beta}\}$ (resp. $\mathcal{O}'_1 = \{0\}$, $\mathcal{O}'_2 = \{\infty\}$, $\mathcal{O}'_3 = \{1, -1\}$ and $\mathcal{O}'_4 = \{\sqrt{\beta'}, -\sqrt{\beta'}\}$). In Case (i), the element $\sigma_{\rho'}$ is the unique element of order two in $\mathrm{RA}(C_{\beta'})$ which has two fixed points in $S_{\beta'}$. Therefore, we have $\varphi \cdot \sigma_\beta \cdot \varphi^{-1} = \sigma_{\beta'}$. In Cases (ii) and (iii), we have three elements of order two in $\mathrm{RA}(C_{\beta'})$ which have respectively two fixed points in $S_{\beta'}$. By the structure of the group $\mathrm{RA}(C_{\beta'})$, they are conjugate to each other. Therefore, by a suitable choice of an isomorphism φ, we can assume $\varphi \cdot \sigma_\beta \cdot \varphi^{-1} = \sigma_{\beta'}$. Hence, in any case, we can assume that the isomorphism φ maps either $\mathcal{O}_1$ to $\mathcal{O}'_1$ and $\mathcal{O}_2$ to $\mathcal{O}'_2$, or $\mathcal{O}_1$ to $\mathcal{O}'_2$ and $\mathcal{O}_2$ to $\mathcal{O}'_1$. Hence, by the similar method as in the first part of this proof, we can conclude $\beta = \beta'$ or $\beta = 1/\beta'$. The converse is trivial. Q.E.D.

For a real number γ, we denote by $[\gamma]$ the integral part of γ.

DEFINITION 1.6:

$$g(x) = \sum_{j=0}^{[p/3]} \binom{(p-1)/2}{[(p+1)/6]+j} \binom{(p-1)/2}{j} x^j.$$

DEFINITION 1.7:

$$h(x) = \sum_{j=0}^{[p/4]} \binom{(p-1)/2}{[(p+1)/4]+j} \binom{(p-1)/2}{j} x^j.$$

PROPOSITION 1.8: *A curve C_α in Class (a) is supersingular (resp. ordinary) if and only if $g(\alpha) = 0$ (resp. $g(\alpha) \neq 0$).*

PROOF: Using the notation in (1.5), we have

$$M = \begin{cases} g(\alpha)\begin{pmatrix} \alpha^{(p-1)/6} & 0 \\ 0 & 1 \end{pmatrix} & \text{if } p \equiv 1 \pmod 6, \\ -g(\alpha)\begin{pmatrix} 0 & \alpha^{(p+1)/6} \\ 1 & 0 \end{pmatrix} & \text{if } p \equiv 5 \pmod 6. \end{cases} \tag{1.23}$$

Therefore, this proposition follows from Lemma 1.1. Q.E.D.

PROPOSITION 1.9: *A curve C_β in Class (b) is supersingular (resp. ordinary) if and only if $h(\beta) = 0$ (resp. $h(\beta) \neq 0$).*

PROOF: Using the notation in (1.5), we have

$$M = \begin{cases} (-1)^{(p-1)/4} h(\beta) \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(p-3)/4} h(\beta) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.24}$$

Therefore, this proposition follows from Lemma 1.1. Q.E.D.

PROPOSITION 1.10: *For a curve C in Class* (2), (3), (4) *or* (5), *the following conditions are equivalent.*

(*i*) *The Jacobian variety $J(C)$ is a supersingular abelian surface.*

(*ii*) *The Jacobian variety $J(C)$ is isomorphic to a product of two supersingular elliptic curves.*

(*iii*) *E_σ or E_τ is a supersingular elliptic curve.*

PROOF: In these cases, the Jacobian variety $J(C)$ is either supersingular or ordinary by Propositions 1.8 and 1.9. Therefore, if E_σ or E_τ is a supersingular elliptic curve, then both E_σ and E_τ are supersingular elliptic curves. Hence, this proposition follows from Proposition 1.3. Q.E.D.

EXAMPLE: There exists a curve C in Class (1) such that E_σ or E_τ is a supersingular elliptic curve, and the Jacobian variety $J(C)$ is not supersingular. For example, we consider the curve C defined by the equation

$$y^2 = x^6 + 3x^2 + 4 \tag{1.25}$$

over an algebraically closed field of characteristic 13. Then, using the notation in (1.5), we have

$$M = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}.$$

Incidentally, we have $\mathrm{RA}(C) = \mathbb{Z}/2$.

For the curves in Class (4), (5) or (6), we have the following propositions.

PROPOSITION 1.11: *The Jacobian variety $J(C)$ of the curve C in Class* (4) *is isomorphic to a product of two supersingular elliptic curves* (*resp. $J(C)$ is ordinary*) *if and only if $p \equiv 5 \pmod 6$* (*resp. $p \equiv 1 \pmod 6$*).

PROOF: Since the reduced group of automorphisms of this curve contains an element of order six, by the uniqueness of such a curve, this

curve C is isomorphic to the one defined by

$$y^2 = x^6 - 1. \tag{1.26}$$

Using the notation in (1.5), we have

$$M = \begin{cases} \begin{pmatrix} \binom{(p-1)/2}{(p-1)/3} & 0 \\ 0 & (-1)^{(p-1)/6}\binom{(p-1)/2}{(p-1)/3} \end{pmatrix} & \text{if } p \equiv 1 \pmod 6 \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } p \equiv 5 \pmod 6. \end{cases} \tag{1.27}$$

Therefore, this proposition follows from Lemma 1.1. Q.E.D.

PROPOSITION 1.12: *The Jacobian variety $J(C)$ of the curve C in Class* (5) *is isomorphic to a product of two supersingular elliptic curves (resp. $J(C)$ is ordinary) if and only if $p \equiv 5$ or $7 \pmod 8$ (resp. $p \equiv 1$ or $3 \pmod 8$).*

PROOF: Using the notation in (1.5), we have

$$M = \begin{cases} (-1)^{(p-1)/8}\binom{(p-1)/2}{(p-1)/8}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \text{if } p \equiv 1 \pmod 8, \\ (-1)^{(p-3)/8}\binom{(p-1)/2}{(p-3)/8}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} & \text{if } p \equiv 3 \pmod 8, \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } p \equiv 5 \text{ or } 7 \pmod 8. \end{cases} \tag{1.28}$$

Therefore, this proposition follows from Lemma 1.1. Q.E.D.

PROPOSITION 1.13: *For the Jacobian variety $J(C)$ of the curve C in Class* (6), *we have the following three cases.*

(*i*) *If $p \equiv 1 \pmod 5$, then the Jacobian variety $J(C)$ is ordinary.*

(*ii*) *If $p \equiv 2$ or $3 \pmod 5$, then the Jacobian variety $J(C)$ is supersingular and $J(C)$ is not isomorphic to a product of two supersingular elliptic curves.*

(*iii*) *If $p \equiv 4 \pmod 5$, then the Jacobian variety $J(C)$ is isomorphic to a product of two supersingular elliptic curves.*

PROOF: Since the curve C has automorphisms of order five, by the uniqueness of such a curve, this curve C is isomorphic to the curve

defined by

$$y^2 = x^5 - 1. \tag{1.29}$$

Using the notation in (1.5), we have

$$M = \begin{cases} (-1)^{(p-1)/10} \begin{pmatrix} \binom{(p-1)/2}{(p-1)/5} & 0 \\ 0 & \binom{(p-1)/2}{(p-1)/10} \end{pmatrix} & \text{if } p \equiv 1 \pmod 5, \\ (-1)^{(p-7)/10} \begin{pmatrix} 0 & \binom{(p-1)/2}{(p-2)/5} \\ 0 & 0 \end{pmatrix} & \text{if } p \equiv 2 \pmod 5, \\ (-1)^{(p-3)/10} \begin{pmatrix} 0 & 0 \\ \binom{(p-1)/2}{(p-3)/10} & 0 \end{pmatrix} & \text{if } p \equiv 3 \pmod 5, \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \text{if } p \equiv 4 \pmod 5. \end{cases} \tag{1.30}$$

Therefore, this proposition follows from Lemma 1.1. Q.E.D.

1.4. Simpleness of zeros of g(x) and h(x)

In this section, we prove the following proposition.

PROPOSITION 1.14: *The zeros of* $g(x)$ *(resp.* $h(x)$*) are simple.*

PROOF: The method to prove this proposition is similar to the method in Igusa [8]. First, we consider the hypergeometric differential equation

$$x(1-x)d^2u/dx^2 + \{c - (a+b+1)x\}\mathrm{d}u/\mathrm{d}x - abu = 0, \tag{1.31}$$

where a, b, c are rational numbers. It is well-known that this equation has a solution

$$F(a, b, c; x) = \sum_{n=0}^{\infty} (\Gamma(a+n)\Gamma(b+n)\Gamma(c)/\Gamma(a)\Gamma(b)\Gamma(c+n))(x^n/n!), \tag{1.32}$$

where $\Gamma(x)$ is the gamma function. We set

$$G(x) = g(x)/\binom{(p-1)/2}{[(p+1)/6]}, \quad H(x) = h(x)/\binom{(p-1)/2}{[(p+1)/4]},$$

$$F_0(a, b, c; x) = \sum_{n=0}^{p-1} (\Gamma(a+n)\Gamma(b+n)\Gamma(c)/\Gamma(a)\Gamma(b)\Gamma(c+n))(x^n/n!). \tag{1.33}$$

Then, by direct calculation, we have

$$G(x) \equiv \begin{cases} F_0(1/2, 1/3, 5/6; x) \pmod{p} & \text{if } p \equiv 1 \pmod 6, \\ F_0(1/2, 2/3, 7/6; x) \pmod{p} & \text{if } p \equiv 5 \pmod 6, \end{cases}$$

$$H(x) \equiv \begin{cases} F_0(1/2, 1/4, 3/4; x) \pmod{p} & \text{if } p \equiv 1 \pmod 4, \\ F_0(1/2, 3/4, 5/4; x) \pmod{p} & \text{if } p \equiv 3 \pmod 4. \end{cases} \tag{1.34}$$

Therefore, choosing suitable a, b, c for $G(x)$ (resp. $H(x)$) as above, we see that $G(x)$ (resp. $H(x)$) is a solution of a differential equation in (1.31) in characteristic p. Since the zeros of $G(x)$ (resp. $H(x)$) are different from 0 and 1, the zeros of $G(x)$ (resp. $H(x)$) are simple. Hence, we conclude that the zeros of $g(x)$ (resp. $h(x)$) are simple. Q.E.D.

REMARK 1.15: By Igusa [8], the zeros of the Legendre polynomial $\Phi(x)$ are all simple. Using this fact and Proposition 1.10, we can also prove Proposition 1.14. We omit the details.

2. Class numbers of quaternion hermitian forms and polarizations

2.1. Quaternion hermitian forms

First, we recall definitions by Shimura [19]. Let B be a definite quaternion algebra over $\mathbb{Q}$ with discriminant D. We regard B^n as a left vector space over B. The definite quaternion hermitian form on B^n is unique up to base change over B, and it is given explicitly by $\sum_{i=1}^n x_i \bar{y}_i$ for row vectors $x = (x_i)$, $y = (y_i) \in B^n$. Here, $\bar{}$ means the canonical involution of B. For a valuation v of $\mathbb{Q}$, we put $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$. By continuous prolongation, we get a quaternion hermitian form on B_v^n. The groups of similitudes of these forms are given by

$$\begin{aligned} &G = \{ g \in M_n(B) : g\bar{g}^t = \lambda(g)1_n, \ \lambda(g) \in \mathbb{Q}^\times \}, \\ &\text{or} \\ &G_v = \{ g \in M_n(B_v) : g\bar{g}^t = \lambda(g)1_n, \ \lambda(g) \in Q_v^\times \}, \end{aligned} \tag{2.1}$$

where $\mathbb{Q}^\times$ (resp. $\mathbb{Q}_v^\times$) denotes the group of units of $\mathbb{Q}$ (resp. $\mathbb{Q}_v$) and where 1_n is the identity matrix. Let $\mathcal{O}$ be a maximal order of B. A $\mathbb{Z}$-module L in B^n is called a left $\mathcal{O}$-lattice if L is a left $\mathcal{O}$-module and at the same time a $\mathbb{Z}$-lattice in B^n. Two $\mathcal{O}$-lattices L_1 and L_2 are said to be equivalent globally (resp. locally at p) if $L_1 g = L_2$ for some $g \in G$ (resp. $(L_1 \otimes \mathbb{Z}_p)g = L_2 \otimes \mathbb{Z}_p$ for some $g \in G_p$). A genus of $\mathcal{O}$-lattices is a set of (global) $\mathcal{O}$-lattices in B^n which are equivalent to each other locally at every prime p. From here on, we treat only maximal lattices. We set $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. First, if $B_p = M_2(\mathbb{Q}_p)$, then maximal $\mathcal{O}_p$-lattices in B_p^n form the unique local equivalence class, which is represented by

$$M_p = \mathcal{O}_p^n.$$

Secondly, if B_p is a division algebra, there exist exactly two local equivalence classes, which are represented by

$$M_p = \mathcal{O}_p^n \quad \text{or} \quad N_p = \mathcal{O}_p^n \begin{pmatrix} 1_r & 0 \\ 0 & \pi 1_s \end{pmatrix} \xi,$$

where the integer r is given by $r = [n/2]$, the scalar π is a prime element of $\mathcal{O}_p$, and the matrix ξ is an element of $GL_n(B_p)$ such that

$$\xi \xi^t = \begin{pmatrix} 0 & & & 1 \\ & & \iddots & 1 \\ & \iddots & & \\ 1 & & & 0 \end{pmatrix}.$$

For positive integers D_1, D_2 such that $D = D_1 D_2$, we denote by $\mathscr{L}_n(D_1, D_2)$ the set of left $\mathcal{O}$-lattices in B^n which are equivalent to M_p at p if p does not divide D_2, and to N_p at p if p divides D_2. The genus $\mathscr{L}_n(D, 1)$ is called a principal genus. When D is a prime number, we call $\mathscr{L}_n(1, D)$ a non-principal genus. We denote by $H_n(D_1, D_2)$ the number of global equivalence classes in $\mathscr{L}_n(D_1, D_2)$. As is well-known, the class number $H_n(D_1, D_2)$ is finite. Now, we characterize some elements in $\mathscr{L}_n(D_1, D_2)$ more explicitly.

THEOREM 2.1: (*Eichler* [3]). *The class number of $M_n(B)$ is equal to one for $n \geqslant 2$.*

COROLLARY 2.2: *For every left $\mathcal{O}$-lattice L in B^n ($n \geqslant 2$), there exists $x \in GL_n(B)$ such that $L = \mathcal{O}^n x$.*

PROOF: This is rather well-known. Since $\mathrm{Hom}_{\mathcal{O}}(\mathcal{O}^n, L)$ is a left $M_n(\mathcal{O})$-ideal, we can take as x a generator for this ideal. Q.E.D.

We denote by $\mathbb{Q}_+^\times$ the group of positive rational numbers. For

$g \in GL_n(\mathcal{O})$, we mean by $g > 0$ that g is positive definite, that is, $yg\bar{y}^t > 0$ for all $y \in B^n$, $y \neq 0$.

LEMMA 2.3: *Let x be an element of $GL_n(B)$. Then, a lattice $L = \mathcal{O}^n x$ is contained in $\mathcal{L}_n(D, 1)$ if and only if $x\bar{x}^t = mg$ for some $m \in \mathbb{Q}_+^\times$ and $g \in GL_n(\mathcal{O})$ such that $g = \bar{g}^t > 0$.*

PROOF: If $\mathcal{O}^n x$ is contained in $\mathcal{L}_n(D, 1)$, then we have $\mathcal{O}_p^n x = \mathcal{O}_p^n \gamma_p$ for some $\gamma_p \in G_p$. So we have $x = \delta_p \gamma_p$ for some $\delta_p \in GL_n(\mathcal{O}_p)$. Since the mapping

$$\mathcal{O}_p^\times \ni a \mapsto a\bar{a} \in \mathbb{Z}_p^\times$$

is surjective, by changing δ_p if necessary, we can assume $\gamma_p \bar{\gamma}_p^t = p^{e_p} 1_n$ with an integer e_p. Then, we see that $m = \prod_p p^{e_p}$ and $g = m^{-1} x\bar{x}^t$ satisfy our requirement. The converse follows from the following lemma.

LEMMA 2.4: *Any $g = \bar{g}^t \in GL_n(\mathcal{O}_p)$ can be written as $g = \delta\bar{\delta}^t$ with some $\delta \in GL_n(\mathcal{O}_p)$.*

PROOF: We write

$$g = \begin{pmatrix} a_1 & & & \\ & a_2 & & x_{ij} \\ & & \ddots & \\ & & & a_n \end{pmatrix}$$

with $a_i \in \mathbb{Z}_p$, $x_{ij} \in \mathcal{O}_p$ and $x_{ji} = \bar{x}_{ij}$. First, assume that a_1 is not contained in $\mathbb{Z}_p^\times$. If some a_i is contained in $\mathbb{Z}_p^\times$, then changing rows and columns, we get a matrix whose (1, 1)-component is contained in $\mathbb{Z}_p^\times$. So, assume that all a_i's are not contained in $\mathbb{Z}_p^\times$. Since $g \in GL_n(\mathcal{O}_p)$, there exists some j such that $x_{1j} \notin p\mathcal{O}_p$, and besides if B_p is a division algebra, we have $x_{1j} \notin \pi\mathcal{O}_p$ for some j. For the sake of simplicity, we assume $j = 2$. It is easy to see that there exists an element y of $\mathcal{O}_p$ such that $\mathrm{tr}(x_{12}\bar{y}) \in Z_p^\times$. Considering the matrix

$$\begin{pmatrix} 1 & y & & \\ & 1 & & 0 \\ & 0 & \ddots & \\ & & & 1 \end{pmatrix} g \begin{pmatrix} 1 & & & \\ \bar{y} & 1 & & 0 \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix}, \tag{2.2}$$

we see that the (1, 1)-component of this matrix is equal to $a_1 + a_2 y\bar{y} + \mathrm{tr}(x_{12}\bar{y})$, which is contained in $\mathbb{Z}_p^\times$. Therefore, we can assume that a_1 is

contained in $\mathbb{Z}_p^\times$. Now, we set

$$\gamma = \begin{pmatrix} 1 & & & \\ -a_1^{-1}\bar{x}_{12} & 1 & 0 & \\ \vdots & & \ddots & \\ -a_1^{-1}\bar{x}_{1n} & & 0 & 1 \end{pmatrix}. \tag{2.3}$$

Then, we have

$$\gamma g \bar{\gamma}^t = \begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ 0 & & & & \\ \vdots & & & * & \\ 0 & & & & \end{pmatrix}. \tag{2.4}$$

Therefore, by induction, we can assume that g is a diagonal matrix. Hence, this lemma follows from the surjectivity of the norm mapping of $\mathcal{O}_p^\times$ to $\mathbb{Z}_p^\times$. Q.E.D.

Let $L_1 = \mathcal{O}^n x_1$ and $L_2 = \mathcal{O}^n x_2$ ($x_1, x_2 \in GL_n(B)$) be two lattices in $\mathcal{L}_n(D, 1)$. By Lemma 2.3, there exist elements m_1, m_2 of $\mathbb{Q}_+^\times$ and elements g_1, g_2 of $G_n(\mathcal{O})$ which satisfy $g_1 = \bar{g}_1^t$ and $g_2 = \bar{g}_2^t$ such that $x_1\bar{x}_1^t = m_1 g_1$ and $x_2\bar{x}_2^t = m_2 g_2$. Then, we have the following:

LEMMA 2.5: *Under the above notations, two lattices L_1 and L_2 are equivalent globally if and only if there exist $\gamma \in GL_n(\mathcal{O})$ and $m \in \mathbb{Q}_+^\times$ such that $\bar{\gamma}^t g_1 \gamma = m g_2$.*

PROOF: Assume that L_1 and L_2 are equivalent globally. Then, there exists an element g of G in (2.1) such that

$$\mathcal{O}^n x_1 g = \mathcal{O}^n x_2.$$

Since we have the equality

$$GL_n(\mathcal{O}) = \{ g \in GL_n(B) : \mathcal{O}^n g = \mathcal{O}^n \},$$

there exists an element γ of $GL_n(\mathcal{O})$ such that

$$x_1 g = \bar{\gamma}^t x_2.$$

Therefore, we have

$$m_1 \lambda(g) g_1 = \lambda(g) x_1 \bar{x}_1^t = x_1 g \bar{g}^t x_1^t = \bar{\gamma}^t x_2 \bar{x}_2^t \gamma = m_2 \bar{\gamma}^t g_2 \gamma.$$

Conversely, assume that there exist $\gamma \in GL_n(\mathcal{O})$ and $m \in \mathbb{Q}_+^\times$ such that

$mg_1 = \bar{\gamma}^t g_2 \gamma$. Set $g = x_1^{-1}\gamma x_2$. Then, we see that $g \in G$ and $L_1 g = L_2$. Q.E.D.

For each prime p which divides D, we denote by $\mathfrak{P}$ the two sided prime ideal of $\mathcal{O}$ above p. By the same method as in Lemma 2.3, we have the following lemma.

LEMMA 2.6: *Assume that the discriminant of B is equal to a prime number p. Then, a lattice $L = \mathcal{O}^2 x$ with $x \in GL_2(B)$ is contained in $\mathscr{L}_2(1, p)$ if and only if*

$$x\bar{x}^t = m\begin{pmatrix} ps & r \\ \bar{r} & pt \end{pmatrix}$$

for some $m \in \mathbb{Q}_+^\times$, $s, t \in \mathbb{Z}$, $s > 0$, $t > 0$ and $r \in \mathfrak{P}$ such that $p^2 st - r\bar{r} = p$.

Let $L_1 = \mathcal{O}^n x_1$ and $L_2 = \mathcal{O}^n x_2$ ($x_1, x_2 \in GL_n(B)$) be two lattices in $\mathscr{L}_2(1, p)$. By Lemma 2.6, there exist m_1, m_2 of $\mathbb{Q}_+^\times$ and two matrices

$$g_1 = \begin{pmatrix} ps_1 & r_1 \\ \bar{r}_1 & pt_1 \end{pmatrix} \quad \text{and} \quad g_2 = \begin{pmatrix} ps_2 & r_2 \\ \bar{r}_2 & pt_2 \end{pmatrix}$$

($s_i, t_i \in \mathbb{Z}$, $s_i > 0$, $t_i > 0$, $r_i \in \mathfrak{P}$ and $p^2 s_i t_i - r_i \bar{r}_i = p$ ($i = 1, 2$)) such that $x_1 \bar{x}_1^t = m_1 g_1$ and $x_2 \bar{x}_2^t = m_2 g_2$. *Then, by the same method as in Lemma* 2.5, *we have the following*:

LEMMA 2.7: *Under the above notations, two lattices Lattices L_1 and L_2 in $\mathscr{L}_2(1, p)$ are equivalent globally if and only if there exist $\gamma \in GL_2(\mathcal{O})$ and $m \in \mathbb{Q}_+^\times$ such that $\bar{\gamma}^t g_1 \gamma = m g_2$.*

2.2. The number of principally polarized supersingular abelian varieties

Let E be a supersingular elliptic curve defined over an algebraically closed field k of characteristic $p > 0$. Then, it is well-known that $B = \mathrm{End}(E) \otimes_Z \mathbb{Q}$ is the definite quaternion algebra over $\mathbb{Q}$ with discriminant p, and that $\mathcal{O} = \mathrm{End}(E)$ is a maximal order of B. We set $A = E^n$ ($n \geqslant 2$). For a divisor L on A, we denote by φ_L the homomorphism from A to the dual A^t defined by $\varphi_L(x) = T_x^* L - L$ for $x \in A$, where T_x is the translation by x (cf. Mumford [14], p. 60 and Lang [12]). We set

$$X = E^{n-1} \times \{0\} + E^{n-2} \times \{0\} \times E + \ldots + \{0\} \times E^{n-1}.$$

Then, the polarization X is a principal polarization on A. We define an injective homomorphism j from the Néron-Severi group $\mathrm{NS}(A)$ to

End(A) as follows:

$$\begin{array}{ccccc} j: & \mathrm{NS}(A) & \to & \mathrm{End}(A) = M_n(\mathcal{O}). \\ & \cup & & \cup \\ & L & \mapsto & \varphi_X^{-1} \circ \varphi_L \end{array} \tag{2.5}$$

For $g \in M_n(B)$ such that $g = \bar{g}^t$, we denote by $\mathrm{HNm}(g)$ the Hauptnorm of g. In case $n = 2$, we have $\mathrm{HNm}(g) = \det(g)$. The following proposition follows easily from Mumford [14], p. 150, p. 209, and the definition of φ_X.

PROPOSITION 2.8: *The image of* $\mathrm{NS}(A)$ *by* j *is*

$$\{ g \in M_n(\mathcal{O}) : g = \bar{g}^t \},$$

and $L^n/n! = \mathrm{HNm}(j(L))$ *for* $L \in \mathrm{NS}(A)$. *The divisor* L *is ample if and only if* $j(L)$ *is positive definite. Moreover, the homomorphism* j *induces a bijection from the set of principal polarizations on* A *to*

$$\{ g \in GL_n(\mathcal{O}) : g = g^t > 0 \}.$$

COROLLARY 2.9: *Assume* $n = 2$. *Then, for each positive integer* d *the following map is bijective*:

$$\begin{array}{ccc} \{ C \in \mathrm{NS}(A) : C > 0,\ C^2 = 2d \} & \to & \left\{ \begin{pmatrix} s & r \\ \bar{r} & t \end{pmatrix} \in M_n(\mathcal{O}) : \begin{array}{l} s,\ t \in \mathbb{Z}, \\ s > 0,\ t > 0, \\ st - r\bar{r} = d \end{array} \right\}. \\ \cup & & \cup \\ C & \longmapsto & \varphi_X^{-1} \cdot \varphi_C \end{array} \tag{2.6}$$

THEOREM 2.10 *: *The number of principal polarizations on* $A = E^n (n \geqslant 2)$ *up to automorphisms of* A *is equal to the class number* $H_n(p, 1)$ *of the principal genus of the quaternion hermitian space* B^n.

PROOF: Let g be an automorphism of A. For $L_1,\ L_2 \in \mathrm{NS}(A)$, we have $g^* L_1 = L_2$ in $\mathrm{NS}(A)$ if and only if $(\varphi_X^{-1} g' \varphi_X)(\varphi_X^{-1} \varphi_{L_1}) g = \varphi_X^{-1} \varphi_{L_2}$, where g' is the dual homomorphism of g. Therefore, this theorem follows from Lemmas 2.3, 2.5 and Proposition 2.8. Q.E.D.

* The authors heard that Professor J.-P. Serre had also known this theorem (cf. J.-P. Serre: Nombres de points des courbes algébriques sur $\mathbb{F}_q$, Séminaire de Théorie des Nombres (Bordeaux), Année 1982–1983, Exposé n°22, where the result is mentioned in the case of $n = 2$).

REMARK 2.11: The class number $H_n(p, 1)$ was explicitly computed by Eichler [2], Satz 2 (see also [4]) for $n = 1$, Hashimoto and Ibukiyama [6], (I), for $n = 2$, and Hashimoto [5] for $n = 3$.

We set $h = H_1(p, 1)$ and $H = H_2(p, 1)$. As is shown in Deuring [1], p. 266, the number h is equal to the number of isomorphism classes of supersingular elliptic curves over k. Let $\{E_i\}_{i=1,2,\ldots,h}$ be a set of representatives of isomorphism classes of supersingular elliptic curves. P. Deligne proved that $E_i \times E_j$ is isomorphic to $E \times E$ for any i, j (cf. Shioda [21], Theorem 3.5). It is easy to see that every supersingular abelian surface with reducible principal polarization is isomorphic to some $E_i \times E_j$ with polarization $E_i \times \{0\} + \{0\} \times E_j$ $(i \leqslant j)$, and that $E_i \times E_j$ with polarization $E_i \times \{0\} + \{0\} \times E_j$ $(i \leqslant j)$ are not isomorphic to each other as principally polarized abelian surfaces. Using these results, we have the following corollary to Theorem 2.10.

COROLLARY 2.12: *The number of isomorphism classes of non-singular irreducible curves of genus two whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves is equal to* $H - \{h(h+1)/2\}$.

REMARK 2.13: In case $\mathrm{End}(E)$ is isomorphic to the principal order of an imaginary quadratic field $Q(\sqrt{-m})$, the number of isomorphism classes of curves of genus two whose Jacobian varieties are isomorphic to $E \times E$ is explicitly calculated in Hayashida [7].

2.3. Polarizations and the non-principal genus

Let E be a supersingular elliptic curve defined over the finite field $\mathbb{F}_p$ with p elements. Let A be a supersingular abelian surface which is not isomorphic to a product of two supersingular elliptic curves. Then, by Oort [18], Corollary 7, there exists an exact sequence

$$0 \to \alpha_p \xrightarrow{\varepsilon} E^2 \xrightarrow{\psi} A \to 0. \tag{2.7}$$

Let i, j be elements of k such that (i, j) defines the inclusion ε of α_p into $\alpha_p \times \alpha_p \subset E \times E$ in (2.7). An abelian surface A is not isomorphic to a product of two supersingular elliptic curves if and only if $j \neq 0$ and $i/j \notin \mathbb{F}_{p^2}$ (cf. Oort [18], Introduction). Let $\mathfrak{P}$ be the two sided ideal of $\mathcal{O} = \mathrm{End}(E)$ over p. Then, by our choice of E, the ideal $\mathfrak{P}$ is principal, that is, $\mathfrak{P} = \pi\mathcal{O}$ for some $\pi \in \mathcal{O}$. We consider the composition of injective homomorphisms:

$$\begin{array}{ccccccc} \mathrm{NS}(A) & \to & \mathrm{Hom}(A, A') & \to & \mathrm{End}(E^2) = M_2(\mathcal{O}), \\ \cup & & \cup & & \cup \\ C & \mapsto & \varphi_C & f & \mapsto & \varphi_X^{-1} \cdot \psi' \cdot f \cdot \psi \end{array} \tag{2.8}$$

where $X = E \times \{0\} + \{0\} \times E$ as before and where ψ^t is the dual homomorphism of ψ. Using this homomorphism, we have the following proposition.

PROPOSITION 2.14: *Let A be a supersingular abelian surface with $j \neq 0$, $i/j \notin \mathbb{F}_{p^2}$. Then, the set of principal polarizations on A is naturally bijective to*

$$\Lambda = \left\{ \begin{pmatrix} ps & r \\ \bar{r} & pt \end{pmatrix} : s,\ t \in \mathbb{Z},\ s > 0,\ t > 0,\ r \in \pi\mathcal{O},\ p^2 st - r\bar{r} = p \right\}. \tag{2.9}$$

PROOF: Let C be a principal polarization on A. Then, we have the following commutative diagram:

$$\begin{array}{ccccc} E \times E & \xrightarrow{\varphi_{\psi^* C}} & (E \times E)^t & \xrightarrow{\varphi_X^{-1}} & E \times E. \\ \psi \downarrow & & \uparrow \psi^t & & \\ A & \xrightarrow[\varphi_C]{} & A^t & & \end{array} \tag{2.10}$$

Since we have $1 = \dim_k \mathrm{Hom}(\alpha_p, A) = \dim_k \mathrm{Hom}(\alpha_p, A^t)$ (cf. Oort [18], Theorem 2), the subgroup schemes which are isomorphic to α_p are unique in A and A^t, respectively. Since φ_C and φ_X are isomorphisms, we have by (2.7)

$$\mathrm{Ker}\ \varphi_X^{-1} \cdot \varphi_{\psi^* C} = \mathrm{Ker}\ \varphi_{\psi^* C} = \mathrm{Ker}\ \psi^t \cdot \varphi_C \cdot \psi = \alpha_p \times \alpha_p. \tag{2.11}$$

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be the image of C by the homomorphism in (2.8). Since $(\psi^* C)^2 = pC^2 = 2p$, by (2.10) and Corollary 2.9, we have

$$a,\ d \in Z,\ a,\ d > 0,\ c = \bar{b} \text{ and } ad - cb = p. \tag{2.12}$$

By (2.11), we have $a,\ b,\ c,\ d \equiv 0 \pmod{\pi\mathcal{O}}$. Since a and b are integers, we conclude that a and b are divisible by p. Hence, the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is contained in Λ. Conversely, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of Λ. Then, by Corollary 2.9, there exists an effective divisor D such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \varphi_X^{-1} \circ \varphi_D$ with $D^2 = 2p$. By the definition of Λ, we have

$$\mathrm{Ker}\ \varphi_D = \mathrm{Ker}\ \varphi_X^{-1} \cdot \varphi_D \supset \alpha_p \times \alpha_p.$$

On the other hand, we have $\deg(\mathrm{Ker}\ \varphi_D) = (D^2/2)^2 = p^2$. Therefore,

$$\mathrm{Ker}\ \varphi_D = \alpha_p \times \alpha_p.$$

Therefore, using the descent theory in Mumford [14], Corollary to Theorem 2 on page 231, we see that there exists an effective divisor C such that $D = \psi^* C$. Since $2p = D^2 = (\deg \psi) C^2$, we have $C^2 = 2$, that is, the polarization C is a principal polarization on A. It is clear that the image of C by the homomorphism in (2.8) is $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Q.E.D.

THEOREM 2.15: *The group* $\mathrm{Aut}(E^2) = GL_2(\mathcal{O})$ *acts on the set of principal polarizations on* A *by*

$$\Lambda \ni g \mapsto \bar{\gamma}' g \gamma \quad \text{for } \gamma \in GL_2(\mathcal{O}). \tag{2.13}$$

The number of orbits under this action is equal to the class number $H_2(1, p)$ *of the non-principal genus in* B^2.

PROOF: This follows from Proposition 2.14, Lemmas 2.6 and 2.7. Q.E.D.

REMARK 2.16: This theorem will be used to show that the number of irreducible components of the locus of supersingular abelian surfaces in the coarse moduli scheme $A_{2,1}$ of principally polarized abelian surfaces is equal to $H_2(1, p)$ (cf. Katsura and Oort [10]).

REMARK 2.17: By Hashimoto and Ibukiyama [6], (II) and (III), we have the following explicit formula for $H' = H_2(1, p)$:

If $p = 2$, 3 or 5, then $H' = 1$, and if $p \geqslant 7$, then

$$\begin{aligned} H' = {} & (p^2 - 1)/2880 + (p+1)\left(1 - \left(\frac{-1}{p}\right)\right)/64 \\ & + 5(p-1)\left(1 + \left(\frac{-1}{p}\right)\right)/192 + (p+1)\left(1 - \left(\frac{-3}{p}\right)\right)/72 \\ & + (p-1)\left(1 + \left(\frac{-3}{p}\right)\right)/36 \\ & + \begin{cases} 2/5 \ldots p \equiv 2 & \text{or } 3 \pmod 5 \\ 0 \quad \ldots p \equiv 1 & \text{or } 4 \pmod 5 \end{cases} \\ & + \begin{cases} 1/4 \ldots p \equiv 3 & \text{or } 5 \pmod 8 \\ 0 \quad \ldots p \equiv 1 & \text{or } 7 \pmod 8 \end{cases} \\ & + \begin{cases} 1/6 \ldots p \equiv 5 & \pmod{12} \\ 0 \quad \ldots p \equiv 1, & 7 \text{ or } 11 \pmod{12}, \end{cases} \end{aligned}$$

where $\left(\frac{1}{p}\right)$ denotes the Legendre symbol.

Finally we give a remark on the structure of the endomorphism ring of an abelian surface A with $j \neq 0$, and $i/j \notin \mathbb{F}_{p^4}$. First, we need the following general lemma.

LEMMA 2.18: *Let E be a supersingular elliptic curve. Assume that A is an abelian variety of dimension $n \geqslant 2$ which is isogenous to E^n. Then, we can choose an isogeny $\varphi: E^n \to A$ such that for any $\alpha \in \mathrm{End}(A)$, there exists $\beta \in \mathrm{End}(E^n)$ which satisfies $\alpha \circ \varphi = \varphi \circ \beta$.*

PROOF: By tensoring with $\mathbb{Q}$, the group $\mathrm{Hom}(E^n, A)$ can be embedded into $M_n(B)$. Since $\mathrm{Hom}(E^n, A)$ is a right $\mathrm{End}(E^n)$-ideal, by Theorem 2.1 we can find an element φ of $\mathrm{Hom}(E^n, A)$ such that

$$\mathrm{Hom}(E^n, A) = \varphi\, \mathrm{End}(E^n). \tag{2.14}$$

Hence, for any $\alpha \in \mathrm{End}(A)$, we have $\alpha \cdot \varphi \in \varphi\, \mathrm{End}(E^n)$. Q.E.D.

Now, let E be a supersingular elliptic curve defined over $\mathbb{F}_p$ such that $\mathrm{End}(E)$ is defined over the finite field $\mathbb{F}_{p^2}$ (for the existence of such an elliptic curve, see Waterhouse [22], Theorem 4.1.5), and let A be an abelian surface with $j \neq 0$, and $i/j \notin \mathbb{F}_{p^4}$. Then, we can take ψ in (2.7) as φ in Lemma 2.18.

PROPOSITION 2.19: *Under the above notations,*

$$\varphi\, \mathrm{End}(A)\varphi^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathcal{O}) : b,\ c,\ a - d \in \pi\mathcal{O} \right\}. \tag{2.15}$$

PROOF: Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an element of $\mathrm{End}(E^2)$. Then, there exists an element h of $\mathrm{End}(A)$ such that $\varphi \cdot h = g \cdot \varphi$ if and only if $g(\varepsilon(\alpha_p)) \subset \varepsilon(\alpha_p)$. On the other hand, the endomorphism g induces a homomorphism on $\alpha_p \times \alpha_p$, and it is given by a matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathbb{F}_{p^2})$ (cf. Oort [18], Lemma 5). Therefore, we have $g(\varepsilon(\alpha_p)) \subset \varepsilon(\alpha_p)$ if and only if $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} = \lambda \begin{pmatrix} i \\ j \end{pmatrix}$ with a suitable element λ of $\mathbb{F}_{p^4}$. By assumption, we have $j \neq 0$ and $i/j \notin \mathbb{F}_{p^4}$. Hence, we have $\alpha = \delta = \lambda$ and $\beta = \gamma = 0$. Q.E.D.

§3. Supersingular curves of genus two

3.1. The mass formula

Let k be an algebraically closed field of characteristic $p > 0$, and E a supersingular elliptic curve. Let $\{\Theta_i \ (i = 1, 2, \ldots, H_n(p, 1))\}$ be a set of

representatives of isomorphism classes of principal polarizations on E^n. We denote by Γ_i the group of automorphisms of a principally polarized abelian variety (E^n, Θ_i). The formula for

$$\sum_{i=1}^{H_n(p,1)} (1/|\Gamma_i|)$$

is known as the mass formula for general n. In case $n = 1$, we have

$$\sum_{i=1}^{h} (1/|\Gamma_i|) = (p-1)/24 \tag{3.1}$$

(cf. Eichler [2], Satz 1, and Deuring [1], §5, §10). In case $n = 2$, we have

$$\sum_{i=1}^{H} (1/|\Gamma_i|) = (p-1)(p^2+1)/5760 \tag{3.2}$$

(cf. Hashimoto and Ibukiyama [6], (I), Section 3, and see also Katsura and Oort [10], Theorem 5.6).

PROPOSITION 3.1: (*mass formula for curves of genus two*).

$$\sum_{C} (1/|\mathrm{RA}(C)|) = (p-1)(p-2)(p-3)/2880,$$

where C runs through isomorphism classes of non-singular irreducible curves of genus two whose Jacobian varieties $J(C)$ are isomorphic to a product of two supersingular elliptic curves.

PROOF: In case $n = 2$, the group of automorphisms of a principally polarized abelian surface $(E \times E, \Theta)$ is isomorphic to the group of automorphisms of Θ. Using the notations in 2.2, we see that the order of the group of automorphisms of a principally polarized abelian surface $(E_i \times E_j, E_i \times \{0\} + \{0\} \times E_j)$ is given by $|\mathrm{Aut}(E_i)|\,|\mathrm{Aut}(E_j)|$ if $i \neq j$, and by $2\,|\mathrm{Aut}(E_i)|^2$ if $i = j$. Therefore, we have

$$\sum_{i>j} \left(1/|\mathrm{Aut}(E_i)|\,|\mathrm{Aut}(E_j)|\right) + \sum_{i=1}^{h} \left(1/2\,|\mathrm{Aut}(E_i)|^2\right) =$$

$$= \Big(\sum_{i=1}^{h} 1/|\mathrm{Aut}(E_i)|\Big)^2/2 = ((p-1)/24)^2/2. \tag{3.3}$$

Therefore, subtracting this from the mass formula in (3.2), we complete our proof. Q.E.D.

3.3. *The number of supersingular curves of genus two*

In this section, we examine the number of isomorphism classes of supersingular curves of genus two with reduced group Γ of automorphisms. First, we need the following proposition.

PROPOSITION 3.2: *Assume* char. $k = p \geqslant 5$. *The number of isomorphism classes of curves of genus two with* Γ *such that* $S_3 \subset \Gamma$ (*resp.* $\mathbb{Z}/2 \times \mathbb{Z}/2 \subset \Gamma$) *whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves is given by* $[([p/3]+1)/2]$ (*resp.* $[([p/4]+1)/2]$).

PROOF: Since the degree of the polynomial $g(x)$ (resp. $h(x)$) is equal to $[p/3]$ (resp. $[p/4]$), this proposition follows from Lemma 1.5, Propositions 1.8, 1.9 and 1.14. Q.E.D.

THEOREM 3.3: *The number of isomorphism classes of curves of genus two with reduced group* Γ *of automorphisms whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves can be listed as follows*:

(I) $p \geqslant 7$.

(0) $(p-1)(p^2-35p+346)/2880 - \left(1-\left(\frac{-1}{p}\right)\right)/32$
$-\left(1-\left(\frac{-2}{p}\right)\right)/8 - \left(1-\left(\frac{-3}{p}\right)\right)/9$
$+\begin{cases} 0 & \dots \quad p \equiv 1, 2 \text{ or } 3 \pmod 5 \\ -1/5 & \dots \quad p \equiv 4 \pmod 5, \end{cases}$
if $\Gamma \cong \{1\}$,

(1) $(p-1)(p-17)/48 + \left(1-\left(\frac{-1}{p}\right)\right)/8 + \left(1-\left(\frac{-2}{p}\right)\right)/2$
$+\left(1-\left(\frac{-3}{p}\right)\right)/2$, if $\Gamma \cong \mathbb{Z}/2$,

(2) $(p-1)/6 - \left(1-\left(\frac{-2}{p}\right)\right)/2 - \left(1-\left(\frac{-3}{p}\right)\right)/3$, if $\Gamma \cong S_3$,

(3) $(p-1)/8 - \left(1-\left(\frac{-1}{p}\right)\right)/8 - \left(1-\left(\frac{-2}{p}\right)\right)/4$
$-\left(1-\left(\frac{-3}{p}\right)\right)/2$, if $\Gamma \cong \mathbb{Z}/2 \times \mathbb{Z}/2$,

(4) $\left(1-\left(\frac{-3}{p}\right)\right)/2$, if $\Gamma \cong D_{12}$, which is equal to 0
if $p \equiv 1 \pmod 6$
(resp. 1 if $p \equiv 5 \pmod 6$),

(5) $\left(1-\left(\frac{-2}{p}\right)\right)/2$, if $\Gamma \cong S_4$, which is equal to 0
if $p \equiv 1$ or $3 \pmod 8$
(resp. 1 if $p \equiv 5$ or $7 \pmod 8$),

$$(6)\quad \begin{cases} 0 & \dots \quad p \equiv 1, 2 \text{ or } 3 \pmod 5 \\ 1 & \dots \quad p \equiv 4 \pmod 5. \end{cases} \quad \text{if } \Gamma \cong \mathbb{Z}/5.$$

(II) $p = 5$.
There exists only one such curve, and its reduced group Γ *of automorphisms is isomorphic to* PGL(2, 5).

(III) $p = 2$ or 3. *No such curves.*

PROOF: (II) and (III) follow from Corollary 2.12 and Proposition 1.12. Using Propositions 1.11, 1.12 and 1.13, we have the numbers in (4), (5) and (6). Using Proposition 3.2 and the above results, we have the numbers in (2) and (3). We denote by a (resp. b) the number of isomorphism classes of curves of genus two with reduced group $\Gamma \cong \{1\}$ (resp. $\Gamma = \mathbb{Z}/2$) of automorphisms whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves. Then, using Corollary 2.12 and Proposition 3.1, we have two equations with respect to a and b. Since we have the explicit formulas for h and H (cf. Deuring [1], p. 266, Igusa [8], Hashimoto and Ibukiyama [6], (I)), solving these equations we have the numbers in (0) and (1). Q.E.D.

REMARK 3.4: As for the number of isomorphism classes of curves of genus two with reduced group Γ whose Jacobian varieties are isomorphic to a product of two supersingular elliptic curves, we have the following list for small p.

p \ Γ	1	$\mathbb{Z}/2$	S_3	$\mathbb{Z}/2\times\mathbb{Z}/2$	D_{12}	S_4	$\mathbb{Z}/5$	$H-\{h(h+1)/2\}$
7	0	0	0	0	0	1	0	1
11	0	0	1	0	1	0	0	2
13	0	0	1	1	0	1	0	3
17	0	1	2	1	1	0	0	5
19	0	1	3	2	0	0	1	7
23	0	5	2	1	1	1	0	10
29	1	9	3	2	1	1	1	18
31	2	10	4	3	0	1	0	20
37	5	16	5	4	0	1	0	31
41	8	21	6	4	1	0	0	40
43	10	23	7	5	0	0	0	45
47	14	31	6	4	1	1	0	57
53	23	41	7	5	1	1	0	78
59	35	52	9	6	1	0	1	104
61	40	56	9	7	0	1	0	113

References

[1] M. DEURING: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Univ. Hamburg 14 (1941) 197–272.

[2] M. EICHLER: Über die Idealklassenzahl total definiter Quaternionenalgebren. *Math. Z.* 43 (1938) 102–109.
[3] M. EICHLER: Über die Idealklassenzahl hyperkomplexer Systeme. *Math. Z.* 43 (1938) 481–494.
[4] M. EICHLER: Zur Zahlentheorie der Quaternionen-Algebren. *J. Reine Angew. Math.* 195 (1955) 127–151.
[5] K. HASHIMOTO: Class numbers of positive definite ternary quaternion hermitian forms. *Proceed. Japan Acad.* 59 Ser. A (1983) 490–493.
[6] K. HASHIMOTO and T. IBUKIYAMA: On class numbers of positive definite binary quaternion hermitian forms (I). *J. Fac. Sci.* Univ. Tokyo Sect IA, 27 (1980) 549–601, (II) ibid. 28 (1981) 695–699, (III) ibid. to appear.
[7] T. HAYASHIDA: A class number associated with the product of an elliptic curve with itself. *J. Math. Soc. Japan* 20 (1968) 26–43.
[8] J. IGUSA: Class number of a definite quaternion with prime discriminant. *Proc. Nat. Acad. Sci. U.S.A.* 44 (1958) 312–314.
[9] J. IGUSA: Arithmetic variety of moduli for genus two. *Ann. of Math.* 72 (1960) 612–649.
[10] T. KATSURA and F. OORT: Families of supersingular abelian surfaces. In preparation.
[11] N. KOBLITZ: *P*-adic variation of the zeta-function over families defined over finite fields. *Compositio Math.* 31 (1975) 119–218.
[12] S. LANG: *Abelian Varieties.* New York: Interscience-Wiley (1959).
[13] YU. I. MANIN: The theory of commutative formal groups over fields of finite characteristic. *Russian Math. Surveys* 18 (1963) 1–83.
[14] D. MUMFORD: *Abelian Varieties.* Oxford University Press (1970).
[15] P. NORMAN and F. OORT: Moduli of abelian varieties. *Ann. of Math. 112* (1980) 413–439.
[16] N.O. NYGAARD: Slopes of powers of frobenius on crystalline cohomology. *Ann. Sci. Ecole Norm.* Sup. 14 (1981) 369–401.
[17] F. OORT: Subvarieties of moduli spaces. *Invent. Math.* 24 (1974) 95–119.
[18] F. OORT: Which abelian surfaces are products of elliptic curves? *Math. Ann.* 214 (1975) 35–47.
[19] G. SHIMURA: Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan* 15 (1963) 33–65.
[20] T. SHIODA: Some results on unirationality of algebraic surfaces. *Math. Ann.* 230 (1977) 153–168.
[21] T. SHIODA: Supersingular K3 surfaces. *Lecture Notes in Math. 732.* Berlin-Heidelberg-New York: Springer (1979) 564–591.
[22] W.C. WATERHOUSE: Abelian varieties over finite fields. *Ann. Sci. Ecole Norm.* Sup. 2 (1962) 521–560.
[23] N. YUI: On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$. *Journ. of Alg.* 52 (1978) 378–410.

(Oblatum 27-XII-1983 & 11-XII-1984)

Tomoyoshi Ibukiyama
Max-Planck-Institut für Mathematik
5300 Bonn
West Germany

and

Department of Mathematics
College of General Education
Kyushu University
Fukuoka, 810
Japan

Toshiyuki Katsura
Department of Mathematics
Yokohama City University
Yokohama, 236
Japan

Frans Oort
Mathematical Institute
State University of Utrecht
Budapestlaan 6
3508 TA Utrecht
The Netherlands