J. Math. Soc. Japan
Vol. 72, No. 4 (2020) pp. 1161–1180
doi: 10.2969/jmsj/82528252

Principal polarizations of supersingular abelian surfaces

By Tomoyoshi IBUKIYAMA

(Received May 2, 2019)

Abstract. We consider supersingular abelian surfaces A over a field k of characteristic p which are not superspecial. For any such fixed A, we give an explicit formula of numbers of principal polarizations λ of A up to isomorphisms over the algebraic closure of k. We also determine all the automorphism groups of (A, λ) over algebraically closed field explicitly for every prime p. When $p \geq 5$, any automorphism group of (A, λ) is either $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$ or $\mathbb{Z}/10\mathbb{Z}$. When $p = 2$ or 3, it is a little more complicated but explicitly given. The number of principal polarizations having such automorphism groups is counted exactly. In particular, for any *odd* prime p, we prove that the automorphism group of any generic (A, λ) is $\{\pm 1\}$. This is a part of a conjecture by Oort that the automorphism group of any generic principally polarized supersingular abelian variety should be $\{\pm 1\}$. On the other hand, we prove that the conjecture is false for $p = 2$ in case of dimension two by showing that the automorphism group of any (A, λ) (with $\dim A = 2$) is never equal to $\{\pm 1\}$.

1. Introduction.

We say that an abelian variety A defined over a field k of characteristic p is supersingular if it is isogenous over the algebraic closure $\overline{k}$ of k to E^n where E is a supersingular elliptic curve. We say that A is superspecial if it is isomorphic over $\overline{k}$ to a product of supersingular elliptic curves. By Deligne, Ogus, Shioda, it is known that any products of two supersingular elliptic curves are isomorphic. It has been known that the number of principal polarizations of E^n for $n \geq 2$ is equal to the class number of quaternion hermitian lattices of rank n belonging to the principal genus ([**8**]) and explicit values were given in [**3**] for $n = 2$ and in [**4**] for $n = 3$. The problem treated in this paper is the number of isomorphism classes of principal polarizations of any fixed supersingular abelian surface which is *not* superspecial. By virtue of Oort [**13**], any such abelian surface A is written as $E^2/\iota(\alpha_p)$ where E is a supersingular elliptic curve defined over $\mathbb{F}_p$ and α_p is the finite group scheme $Spec\ \mathbb{F}_p[x]/(x^p)$ and ι is an embedding

$$\iota : \alpha_p \to \alpha_p^2.$$

We denote exclusively by t the tangent of this embedding ι. If t is in $\mathbb{F}_{p^2} \cup \{\infty\}$, then $E^2/\iota(\alpha_p)$ is superspecial ([**13**]), so we exclude this case. Corresponding to the structures of $\mathrm{End}(A)$, we consider two different cases: the case $t \notin \mathbb{F}_{p^4}$ and the case $t \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$. We call them the first case (I) and the second case (II), respectively. We call that A is

2010 *Mathematics Subject Classification.* Primary 14K15; Secondary 11R52, 14K10, 11R58.
Key Words and Phrases. abelian variety, supersingular, polarization, quaternion.
This work was supported by JSPS KAKENHI JP25247001 and JP19K03424.

generic if t is transcendental. This case belongs to the case (I). We state the results for each case. We fix a supersingular abelian surface A which is not superspecial.

THEOREM 1.1. *The number h of principal polarizations of A up to* $\mathrm{Aut}(A)$ *is given as follows*:

(1) *In the case* (I), *i.e. when $t \notin \mathbb{F}_{p^4}$, we have*

$$h = \begin{cases} 1 & \text{if } p = 2, \\ \dfrac{p^2(p^4-1)(p^2-1)}{5760} & \text{for any } p \geq 3. \end{cases}$$

(2) *In the case* (II), *i.e. when $t \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$, we have*

$$h = \begin{cases} 1 & \text{if } p = 2, \\ \dfrac{p^2(p^2-1)^2}{2880} & \text{if } p \equiv \pm 1 \bmod 5 \text{ or } p = 5, \\ 1 + \dfrac{(p-3)(p+3)(p^2-3p+8)(p^2+3p+8)}{2880} & \text{if } p \equiv \pm 2 \bmod 5. \end{cases}$$

For any principal polarization λ of A, we denote by $\mathrm{Aut}(A,\lambda)$ the automorphism group of the principally polarized abelian surface (A,λ) and by $\#(\mathrm{Aut}(A,\lambda))$ its cardinality.

THEOREM 1.2. (1) *In the case* (I), *when $p = 2$, the principal polarization of A is unique up to* $\mathrm{Aut}(A)$, *and we have* $\#(\mathrm{Aut}(A,\lambda)) = 32$. *When p is odd, we have* $\mathrm{Aut}(A,\lambda) = \{\pm 1\}$ *for any principal polarization λ of A.*

(2) *In the case* (II), *when $p = 2$, the principal polarization of A is again unique up to* $\mathrm{Aut}(A)$ *and* $\#(\mathrm{Aut}(A,\lambda)) = 160$. *When $p \equiv \pm 1 \bmod 5$ or $p = 5$, we have* $\mathrm{Aut}(A,\lambda) = \{\pm 1\}$ *for any principal polarization of A. When $p \equiv \pm 2 \bmod 5$, there is the unique principal polarization λ of A up to isomorphism such that* $\mathrm{Aut}(A,\lambda) \cong \mathbb{Z}/10\mathbb{Z}$, *and for all the other principal polarizations λ of A, we have* $\mathrm{Aut}(A,\lambda) = \{\pm 1\}$.

It is stated in [**1**] as a conjecture of Oort that we should have $\mathrm{Aut}(A,\lambda) = \{\pm 1\}$ for any generic principally polarized supersingular abelian variety (A,λ). The above theorem tells us that this conjecture is false for $p = 2$, since we see that the groups $\mathrm{Aut}(A,\lambda)$ are never equal to $\{\pm 1\}$ when $p = 2$. (By the way, the same is true also for superspecial case.) On the other hand, the above claim (1) also means that his conjecture is true for any odd prime p when the dimension is two. A precise description of automorphism groups for $p = 2$ and 3 for the cases (I), (II) will be given in Section 4. (By the way, [**9**, Proposition 7.6] claims that for odd p the proportion of (A,λ) with $\mathrm{Aut}(A,\lambda) \ncong \{\pm 1\}$ tends to zero as the corresponding points in the moduli belong to bigger fields.)

We give a table of the numbers h of principal polarizations for small primes p below. For $t \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$, we have

p	2	3	5	7	11	13	17	19	23	29	31
h	1	1	5	40	605	1657	8324	16245	51208	206045	307520

For $t \notin \mathbb{F}_{p^4}$, we have

p	2	3	5	7	11	13	17	19	23
h	1	1	65	980	36905	140777	1206864	2940345	13569908

The proofs of the theorems are based on explicit description of endomorphisms of A, mass formulas of principal polarizations, and previously known results in [**6**] on the automorphism groups of the pullbacks (E^2, λ_0) of (A, λ). As was explained in [**8**], any endomorphism of A is lifted to $\mathrm{End}(E^2)$ and it is easy to give a structure of $\mathrm{End}(A)$ according to the cases (I) and (II). (See [**8**, Lemma 2.18 and Proposition 2.19] and [**18**].) Also the mass formula for $M(A) = \sum_\lambda (1/\#(\mathrm{Aut}(A, \lambda)))$ for isomorphism classes of principal polarizations λ of A will be given. (There is a similar formula in [**18**], but they treated there a mass of polarizations of p-divisible groups. Although the number is the same as a result in this case, their definition is different from ours.) Then by some simple arithmetic on quaternion hermitian forms and by a little more deep results in [**6**], we can give structures of automorphism groups and can count how many isomorphism classes of principal polarizations have that automorphism group. Then based on the mass formula, we are able to give the number of principal polarizations of A up to $\mathrm{Aut}(A)$.

The paper is organized as follows. In Section 2, we review previously known geometric facts on A and reduce the problem to an arithmetic on quaternion hermitian matrix. We add a remark there that abelian varieties in the case (II) are all isomorphic. In Section 3, first, for general n we consider $n \times n$ quaternion hermitian matrices in $M_n(O)$ and their equivalence over $R^\times$ for an order R which are not necessarily maximal in $M_n(D)$. Then we give a mass formula for $M(A)$ for $n = 2$ which fits our formulation. Secondly we give remarks on relations between $R^\times$ equivalence classes of quaternion hermitian matrices and an arithmetic of the adelized quaternion hermitian group. This also explains a (non-canonical) relation with [**18**]. Logically, this Subsection 3.2 is unnecessary for the rest of the proofs, except for the point that we define a mapping ϕ_0 from $\mathrm{Aut}(A, \lambda)$ to $SL_2(\mathbb{F}_{p^2})$ for $n = 2$ which is injective for $p \geq 5$. However, we inserted this partly for aesthetic reason and partly for possible future applications. In Section 4, we give all possible candidates of automorphism groups when $p \geq 5$ and prove the main theorems in the introduction for $p \geq 5$. In Section 5, we explain how to obtain results for $p = 2$ and 3.

2. Review on supersingular abelian surfaces.

We fix a supersingular elliptic curve E defined over $\mathbb{F}_p$. We may assume that $\mathrm{End}(E)$ has an element π (Frobenius) such that $\pi^2 = -p$. We write $O = \mathrm{End}(E)$ and $O \otimes_{\mathbb{Z}} \mathbb{Q} = D$. Then $D = D_{p,\infty}$ is the definite quaternion algebra over $\mathbb{Q}$ with discriminant $p\infty$ and O is a maximal order of D. We assume that A is a supersingular abelian surface isogenous to E^2 but not superspecial. Then by [**13**], there is an embedding $\iota : \alpha_p \to \alpha_p^2$ such that its tangent is not in $\mathbb{F}_{p^2} \cup \{\infty\}$ and $A \cong E^2/\iota(\alpha_p)$. The natural projection $\psi : E^2 \to A$ is an isogeny of minimal degree. By [**10**] and [**12**], the following result is well known.

Lemma 2.1 ([**10**], [**12**]). *For any principal polarization λ of A, there exists a pullback $\lambda_0 = \psi^*(\lambda)$ to E^2 such that $\mathrm{Ker}(\lambda_0) = \mathrm{Ker}(F)$, where F is the Frobenius of E^2 over $\mathbb{F}_p$. Conversely if there is a polarization λ_0 of E^2 such that $\mathrm{Ker}(\lambda_0) = \mathrm{Ker}(F)$, then*

there exists a principal polarization λ of A such that $\lambda_0 = \psi^*(\lambda)$.

We take a divisor X of E^2 defined by

$$X = \{0\} \times E + E \times \{0\}$$

and define a map φ_X from E^2 to $(E^t)^2 \cong E^2$ by $\varphi_X(y) = Cl(X_y - X)$ for $y \in E^2$. Then this gives a principal polarization of E^2. For any polarization λ_0 of E^2, the endomorphism $\varphi_X^{-1}\lambda_0$ of E^2 is identified with a positive definite quaternion hermitian matrix $H \in M_2(O)$. We may write $H = gg^*$ for some $g = (g_{ij}) \in M_2(D)^\times$, where $g^* = (\overline{g_{ji}})$ and the bar is the main involution of D. We say that H belongs to the non-principal genus if the lattice defined by $O^2 g$ belongs to the non-principal genus. (This does not depend on the choice of g.) When $\mathrm{Ker}(\lambda_0) = \mathrm{Ker}(F)$, then H belongs to the non-principal genus, and the set of such H is given by

$$\mathcal{P} = \left\{ \begin{pmatrix} pt & r \\ \bar{r} & ps \end{pmatrix}; 0 < t, s \in \mathbb{Z}, r \in \pi O, p^2 ts - N(r) = p \right\}$$

where $N(r)$ is the reduced norm of r. For any positive integer n, we write $GL_n(D) = M_n(D)^\times$ and denote by $SL_n(D)$ the subgroup of $GL_n(D)$ of elements of reduced norm 1. We also write $GL_n(O) = M_n(O)^\times$, the group of all elements of $M_n(O)$ invertible in $M_n(O)$. The reduced norm of any element of $GL_n(O)$ is 1. Indeed, denoting the reduced norm of $M_n(D)$ by N, if $\epsilon \in GL_n(O)$, then $\epsilon^{-1} \in M_n(O)$, so $N(\epsilon)$, $N(\epsilon^{-1}) \in \mathbb{Z}$ and $N(\epsilon)N(\epsilon^{-1}) = N(1_n) = 1$, so $N(\epsilon) = \pm 1$. However, we have $N(GL_n(D)) = N(D^\times) = \mathbb{Q}_+^\times$ where $\mathbb{Q}_+^\times$ is the multiplicative group of positive rational numbers (cf. [**17**, Chapter IX, Section 2, Corollary 3 and Chapter XI, Section 3, Proposition 3]), so we have $N(\epsilon) = 1$. So we may write $GL_n(O) = SL_n(O)$. For H_1, $H_2 \in \mathcal{P}$, we say that H_1 is $SL_2(O)$-equivalent to H_2 if $H_2 = \epsilon H_1 \epsilon^*$ for some $\epsilon \in SL_2(O)$. Then the number of such equivalence classes in $\mathcal{P}$ is equal to the class number of the non-principal genus and also to the number of isomorphism classes of polarizations λ_0 of E^2 belonging to the non-principal genus. This number is known explicitly in [**3**]. For any $H \in \mathcal{P}$ corresponding to λ_0, we write

$$\Gamma_H = \{\epsilon \in SL_2(O); \epsilon H \epsilon^* = H\}.$$

Then we have

$$\mathrm{Aut}(E^2, \lambda) \cong \Gamma_H.$$

It is also known that for each abstract group Δ, how many classes $H \in \mathcal{P}$ satisfy $\Delta \cong \Gamma_H$ (see [**6**]).

Now to describe the equivalence class of principal polarizations of A, we need structures of $\mathrm{End}(A)$. We express these by the pullback of $\mathrm{End}(A)$ by ψ in $\mathrm{End}(E^2) = M_2(O)$. The following results are well known and easy to see.

LEMMA 2.2 ([**8**], [**18**]). (1) *If $t \notin \mathbb{F}_{p^4}$ then $\psi^{-1}\mathrm{End}(A)\psi = R_1$, where*

$$R_1 = \left\{ \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(O); a \equiv d \bmod \pi, b \equiv c \equiv 0 \bmod \pi \right\}.$$

(2) *If* $t \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$*, then there exists a certain subfield* K *of* $M_2(\mathbb{F}_p^2)$ *with* $K \cong \mathbb{F}_{p^4}$ *and* $\{a1_2 : a \in \mathbb{F}_{p^2}\} \subset K$ *such that* $\psi^{-1}\mathrm{End}(A)\psi = R_2$*, where*

$$R_2 = \{\alpha \in M_2(O); \alpha \equiv \beta \bmod \pi \text{ for some } \beta \in K\}.$$

Here 1_2 *denotes the* 2×2 *unit matrix.*

The first claim (1) is in [**8**] and (2) is in [**18**]. Here K of course depends on ι and ψ but we need not explicit description of K in the paper. By the Skolem–Noether theorem, all such K are conjugate by $GL_2(\mathbb{F}_{p^2})$, but we should be careful that they are not the same subset of $M_2(\mathbb{F}_{p^2})$.

We say that principally polarized abelian surfaces (A, λ_1) and (A, λ_2) are isomorphic if there is an automorphism $\epsilon \in \mathrm{Aut}(A)$ such that $\epsilon^t \lambda_1 \epsilon = \lambda_2$, where ϵ^t is a dual morphism of the dual abelian variety A^t to A^t. For an order $R \subset M_2(O)$, we say that H_1 and $H_2 \in \mathcal{P}$ are $R^\times$ equivalent if

$$\epsilon H_1 \epsilon^* = H_2$$

for some $\epsilon \in R^\times$. Denote by H_1 and H_2 the quaternion hermitian matrices in $\mathcal{P}$ corresponding to the pullback to E^2 of principal polarizations λ_1 and λ_2 of A. Then $(A, \lambda_1) \cong (A, \lambda_2)$ if and only if H_1 is $R_1^\times$ equivalent to H_2 in the case (I) and $R_2^\times$ equivalent in the case (II), respectively. So our aim is to count the number of $R_i^\times$ equivalence classes of $\mathcal{P}$ for each $i = 1, 2$. A $SL_2(O)$ equivalence class of $\mathcal{P}$ is just a usual class of non-principal genus, so to consider $R_i^\times$ equivalence classes is to take a finer division of the usual class. We will consider this in more general setting in the next section.

Here for curiosity, we add a remark for the case of (II). There we may ask if we can replace t to any other element in $\mathbb{F}_{p^4} - \mathbb{F}_{p^2}$ by changing A only by an isomorphism. The answer is yes as can been seen below. This proposition is not used in the rest of the paper and can be skipped.

Proposition 2.3. *All supersingular abelian varieties* A *whose tangent belong to* $\mathbb{F}_{p^4} - \mathbb{F}_{p^2}$ *are isomorphic with each other over an algebraically closed field.*

Proof. It is clear that tangents t_1 and $t_2 \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$ are mutually mapped by an element of $\mathrm{End}(E^2) \bmod \pi \cong M_2(\mathbb{F}_{p^2})$, but the point is if we can take such a map from $\mathrm{Aut}(E^2) = GL_2(O)$ and this is not trivial, so we carefully see this. We fix one such A and let $t \in \mathbb{F}_{p^4} - \mathbb{F}_{p^2}$ be the tangent to define A. Let η be a fixed generator of $\mathbb{F}_{p^4}$ over $\mathbb{F}_{p^2}$. We will show that we can change A by an isomorphism to $A_0 = E^2/\iota'(\alpha_p)$ such that the tangent of $\iota'(\alpha)$ is η. We put $O_p = O \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Since $O_p/\pi O_p \cong \mathbb{F}_{p^2}$, we may assume that $\eta^2 + (c_1 \bmod \pi)\eta + (c_2 \bmod \pi) = 0$, where $c_i \in O_p$. Then we may write $t = (c_0 \bmod \pi)\eta + (d_0 \bmod \pi)$ for some $c_0 \in O_p^\times$, $d_0 \in O_p$. Then we have

$$\begin{pmatrix} 1 & -d_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t \\ 1 \end{pmatrix} \equiv \begin{pmatrix} \overline{c_0}\eta \\ 1 \end{pmatrix} \bmod \pi,$$

where $\overline{c_0} := c_0 \bmod \pi$. So by this we may change t to $\overline{c_0}\eta$. Now we see that $\overline{c_0}\eta$ can be changed to η. For any c, $d \in O_p$ such that $(c,d) \notin (\pi O_p)^2$, we put

$$\epsilon = \begin{pmatrix} c_0(d - cc_1) & -c_0cc_2 \\ c & d \end{pmatrix}.$$

For any element $h = \begin{pmatrix} x_0 & y_0 \\ z_0 & w_0 \end{pmatrix} \in GL_2(\mathbb{F}_{p^2})$, we write

$$h \circ \eta = \frac{x_0\eta + y_0}{z_0\eta + w_0}.$$

Then we have

$$(\epsilon \bmod \pi) \circ \eta = \overline{c_0}\eta,$$

since

$$c_0\eta(c\eta + d) \equiv c_0((d - cc_1)\eta - cc_2) \bmod \pi.$$

We also have

$$\det(\epsilon \bmod \pi) \equiv c_0(d^2 - cc_1d + c^2c_2) \bmod \pi.$$

Now we may embed $\mathbb{F}_{p^4}$ in $M_2(\mathbb{F}_{p^2})$ so that the subfield $\mathbb{F}_{p^2}$ of $\mathbb{F}_{p^4}$ is equal to the center of $M_2(\mathbb{F}_{p^2})$. So we have an element $\eta_0 \in M_2(\mathbb{F}_{p^2})$ such that $\eta_0^2 + (c_1 \bmod \pi)\eta_0 + (c_2 \bmod \pi) = 0$. Since $M_2(O_p)/\pi M_2(O_p) \cong M_2(\mathbb{F}_{p^2})$, we may take $y \in M_2(O_p)$ such that $y \bmod \pi = \eta_0$. Since $N_{\mathbb{F}_{p^4}^\times/\mathbb{F}_{p^2}}(\mathbb{F}_{p^4}^\times) = \mathbb{F}_{p^2}^\times$, we have $\det((cy+d) \bmod \pi) \equiv c_0^{-1} \bmod \pi$ for some c, $d \in O_p$. Here we have $\det(cy + d) \equiv d^2 - c_1cd + c^2c_2 \bmod \pi$, so defining ϵ by using this c and d, we have $\det(\epsilon \bmod \pi) \equiv 1 \bmod \pi$. Now we show that we may replace ϵ by an element in the norm one subgroup $SL_2(O_p)$ of $GL_2(O_p)$. Since $N(\epsilon) \equiv N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\det(\epsilon \bmod \pi)) = 1 \bmod p$, we have $N(\epsilon) \in 1 + p\mathbb{Z}_p$. The ring O_p contains the ring o_F of integers of the unramified quadratic extension F of $\mathbb{Q}_p$, and we have $1 + po_F \subset 1 + \pi O_p$. It is well known that $N(1 + po_F) = 1 + p\mathbb{Z}_p$ (cf. [**14**]), so take $\beta \in 1 + po_F$ such that $N(\beta)N(\epsilon) = 1$ and put

$$\epsilon_0 = \begin{pmatrix} \beta & 0 \\ 0 & 1 \end{pmatrix} \epsilon.$$

Then since $\beta \equiv 1 \bmod \pi$, we have $\beta^{-1} \in O_p$, $\epsilon_0 \in SL_2(O_p)$ and

$$(\epsilon_0 \bmod \pi) \circ \eta = \overline{c_0}\eta.$$

Finally we show that we can replace ϵ_0 by an element of $SL_2(O)$. We put

$$W_p = (1 + \pi M_2(O_p)) \cap SL_2(O_p).$$

Denote by D_A the adelization of D and by D_v the v-adic completion of D for any $v \leq \infty$.

Then by the strong approximation theorem ([**2**], [**11**]), we have

$$SL_2(D_A) = SL_2(D) \cdot SL_2(D_\infty) W_p \prod_{q \neq p} SL_2(O_q),$$

where $SL_2(D)$ is embedded in $SL_2(D_A)$ diagonally as usual. Hence, for $\epsilon_0 \in SL_2(O_p) \subset SL_2(D_A)$, there exist $\gamma \in SL_2(D)$ and $w \in SL_2(D_\infty) W_p \prod_{q \neq p} SL_2(O_q)$ such that $\epsilon_0 = \gamma w$. Then we have $\gamma = \epsilon_0 w^{-1} \in SL_2(D_\infty) \prod_q SL_2(O_q)$, so $\gamma \in SL_2(O)$. By definition of W_p, we have $(w \bmod \pi) \circ \eta \equiv \eta$, so

$$(\gamma \bmod \pi) \circ \eta = (\epsilon_0 \bmod \pi) \circ \eta = \overline{c_0}\eta.$$

So by the isomorphism γ^{-1} of E^2, we can change the tangent $c_0\eta$ to η, and this induces an isomorphism of A to $E^2/\iota'(\alpha_p)$ where the tangent of ι' is η. □

3. Quaternion hermitian matrices and lattices.

Expecting a future application, here we treat a theory in slightly more general setting. Throughout the paper, we assume that n is a positive integer such that $n \geq 2$.

3.1. Quaternion hermitian matrices.

Let $R \subset M_n(O)$ be an order of $M_n(D)$. For any prime q, we write $R_q = R \otimes_{\mathbb{Z}} \mathbb{Z}_q$ and $R_\infty = M_n(D_\infty)$. For any place $v \leq \infty$, we denote by R_v^1 the subgroup of elements of $R_v^\times$ with reduced norm 1. We put $R_A = \prod_{v \leq \infty} R_v$ and $R_A^1 = \prod_{v \leq \infty} R_v^1$. We put

$$\mathbb{Q}_{A,+}^\times = \mathbb{R}_+^\times \mathbb{Q}_{A,fin}^\times$$

where $\mathbb{Q}_{A,fin}^\times$ is the finite part of the idele group $\mathbb{Q}_A^\times$. We denote by $\mathbb{Q}_+^\times$ the set of positive rational numbers. If $R = M_n(O)$, then by the strong approximation theorem for $SL_n(D)$ for $n \geq 2$ and the fact that

$$\mathbb{Q}_{A,+} = \mathbb{Q}_+^\times \mathbb{R}_+^\times \prod_q \mathbb{Z}_q^\times = N(GL_n(D)) N(GL_n(D_\infty)) \prod_q N(GL_n(O_q)), \tag{1}$$

we have

$$GL_n(D_A) = GL_n(D) \cdot R_A^\times \tag{2}$$

for $n \geq 2$. When a lattice L in D^n is a left O-module, we call L a left O lattice. For any prime q, we write $L_q = L \otimes_{\mathbb{Z}} \mathbb{Z}_q$. For any $g_A = (g_v) \in GL_n(D_A)$, we define

$$Lg_A = \bigcap_{q:prime} (L_q g_q \cap D^n).$$

Then this is again a left O lattice in D^n. It is easy to see that for any left O lattice L, there exists $g_A \in GL_n(D_A)$ such that $L = O^n g_A$. So by (2), there exists $g \in GL_n(D)$ such that $L = O^n g$.

Even if $R \subsetneq M_n(O)$, we have

$$SL_n(D_A) = SL_n(D) \prod_v R_A^1. \tag{3}$$

However, (2) does not hold for general R, because $N(R_q^\times)$ might be a proper subset of $\mathbb{Z}_q^\times$ for some q and the equality corresponding to (1) fails. We note that $N(R^\times) = 1$ and $R^\times \subset SL_n(O)$ as explained before.

For any positive definite quaternion hermitian matrix H, there exists $g \in GL_n(D)$ such that $H = gg^*$ ([**15**]). For two positive definite quaternion hermitian matrices H_1 and H_2, we say that H_1 and H_2 are $R^\times$ equivalent if $H_2 = \epsilon H_1 \epsilon^*$ for some $\epsilon \in R^\times$. For a fixed positive definite quaternion hermitian matrix H, we write

$$S_H(R) = \{\epsilon H \epsilon^*; \epsilon \in R^\times\}.$$

We write

$$\Gamma_H(R) = \{\epsilon \in R^\times; \epsilon H \epsilon^* = H\}.$$

Then $S_H(R)$ is bijective to $R^\times/\Gamma_H(R)$. When $R = M_n(O)$, we write shortly as $\Gamma_H = \Gamma_H(R)$. Now we assume that R, R_0 are orders of $M_n(D)$ with $R \subset R_0 \subset M_n(O)$. Then the $R^\times$ equivalence classes of matrices in $S_H(R_0)$, denoted by $S_H(R_0)/\sim_R$, correspond bijectively with $R^\times \backslash R_0^\times / \Gamma_H(R_0)$. The proof is obvious and we omit it here. We write the double coset decomposition as

$$R_0^\times = \bigcup_{i=1}^{d} R^\times e_i \Gamma_H(R_0).$$

Then representatives of $S_H(R_0)/\sim_R$ are given by $H_i = e_i H e_i^*$ for $i = 1, \ldots, d$. Now we consider the "mass" of $R^\times$ equivalence classes. We denote by $H_1, \ldots, H_d$ the representatives of $S_H(R_0)/\sim_R$.

LEMMA 3.1. *Notation being as above, we have*

$$\frac{[R_0^\times : R^\times]}{\#(\Gamma_H(R_0))} = \sum_{i=1}^{d} \frac{1}{\#(\Gamma_{H_i}(R))}.$$

PROOF. It is well known and easy to see (e.g. [**16**]) that

$$R^\times e_i \Gamma_H(R_0) = \bigcup_{h \in (e_i^{-1} R^\times e_i \cap \Gamma_H(R_0)) \backslash \Gamma_H(R_0)} R^\times e_i h.$$

It is obvious that

$$R^\times \cap e_i \Gamma_H(R_0) e_i^{-1} = \Gamma_{H_i}(R).$$

So counting $R^\times$ cosets in $R_0^\times$, we have

$$[R_0^\times : R^\times] = \sum_{i=1}^{d} \frac{\#(\Gamma_H(R_0))}{\#(e_i R^\times e_i^{-1} \cap \Gamma_H(R_0))} = \sum_{i=1}^{d} \frac{\#(\Gamma_H(R_0))}{\#(\Gamma_{H_i}(R))}. \qquad \square$$

For a genus $\mathcal{G}$ of left O lattices, we say that a quaternion hermitian matrix $H = gg^*$ ($g \in GL_n(D)$) belongs to $\mathcal{G}$ if $O^n g$ belongs to $\mathcal{G}$. We denote by S the set of all quaternion hermitian matrices in $M_n(O)$ belonging to a fixed genus $\mathcal{G}$. Then the mass of S for $GL_n(O)$ equivalence classes is defined by

$$\sum_{H \in S/\sim_{GL_n(O)}} \frac{1}{\#(\Gamma_H)}$$

and the explicit value is essentially given in [**3**]. So for $R_0 = M_n(O)$, the calculation of the mass for $R^\times$-equivalence classes is reduced to the calculation of $[GL_n(O) : R^\times]$. For example, when $n = 2$ and $\mathcal{G}$ is the non-principal genus, the mass of $GL_2(O)$-equivalence classes in $\mathcal{G}$ is given by $(p^2 - 1)/5760$ (see [**3**]). For a supersingular abelian surface A, assume that $R = \mathrm{End}(A)$, and for any principal polarization λ of A, assume that $\varphi_X^{-1}\psi^*(\lambda) = H_\lambda$. Then it is clear that $\mathrm{Aut}(A, \lambda) \cong \Gamma_{H_\lambda}(R)$. So if we define the mass of principal polarizations of A by

$$M(A) = \sum_{\lambda} \frac{1}{\#(\mathrm{Aut}(A, \lambda))}$$

where λ runs over principal polarizations of A up to isomorphism, then we have

$$M(A) = \frac{[GL_2(O) : R^\times](p^2 - 1)}{5760}.$$

Coming back to the general $n \geq 2$, we explain that we can calculate $[R_0^\times : R^\times]$ locally. Since we have

$$SL_n(D_A) = SL_n(D)R_{0,A}^1 = SL_n(D)R_A^1$$

and $R^\times = SL_n(D) \cap R_A^1$, $R_0^\times = SL_n(D) \cap R_{0,A}^1$, we have the following bijections

$$SL_n(D)\backslash SL_n(D_A) = R_0^\times \backslash R_{0,A}^1 = R^\times \backslash R_A^1.$$

So we have

$$[R_0^\times : R^\times] = [R_{0,A}^1 : R_A^1].$$

Since $R_{0,q} = R_q$ for almost all primes q, this is equal to

$$\prod_{q:prime} [R_{0,q}^1 : R_q^1].$$

Since $O_p/\pi O_p = \mathbb{F}_{p^2}$, it is easy to see that

$$SL_n(O_p) \bmod \pi = \{x \in GL_n(\mathbb{F}_{p^2}); N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\det(x)) = 1\}.$$

So if R_p^1 contains $(1_n + \pi M_n(O_p)) \cap SL_n(O_p)$, then we have $[SL_n(O_p) : R_p^1] = [SL_n(O_p) \bmod \pi : R_p^1 \bmod \pi]$. Returning to the case $n = 2$ and using the same notation as in Lemma 2.2, we have $M_2(O_q) = R_{1,q} = R_{2,q}$ for $q \neq p$. We have

$\#(SL_2(O_p) \bmod \pi) = p^2(p^4-1)(p+1)$ and

$$R_1^1 \bmod \pi = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}; a \in \mathbb{F}_{p^2}^\times, N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a^2) = 1 \right\},$$
$$R_2^1 \bmod \pi = \{\beta \in K; N_{\mathbb{F}_{p^4}/\mathbb{F}_p}(\beta) = 1\}.$$

If $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a)^2 = 1$ then we have $N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a) = \pm 1$ for $p \neq 2$ and $= 1$ when $p = 2$. So we have $\#(R_{1,p}^1 \bmod \pi) = 2(p+1)$ if $p \neq 2$ and $= (p+1)$ if $p = 2$. We also have $\#(R_{2,p}^1 \bmod \pi) = \#\{x \in \mathbb{F}_{p^4}; N_{\mathbb{F}_{p^4}/\mathbb{F}_p}(x) = 1\} = (p^4-1)/(p-1)$. Hence we have

LEMMA 3.2.

$$[GL_2(O) : R_1^\times] = \begin{cases} p^2(p^4-1) = 60 & \text{if } p = 2, \\ p^2(p^4-1)/2 & \text{if } p \neq 2, \end{cases}$$
$$[GL_2(O) : R_2^\times] = p^2(p^2-1).$$

This leads to the following formula for $M(A)$.

PROPOSITION 3.3. *In the case* (I)*, we have*

$$M(A) = \begin{cases} \dfrac{1}{32} & \text{if } p = 2, \\ \dfrac{p^2(p^2-1)(p^4-1)}{2 \cdot 5760} & \text{if } p \text{ is odd.} \end{cases}$$

In the case (II)*, we have*

$$M(A) = \frac{p^2(p^2-1)^2}{5760}.$$

3.2. Quaternion hermitian groups.

In the last subsection, we explained everything in terms of $SL_n(D)$. However, usually it is more natural to use quaternion hermitian groups when we consider quaternion hermitian metrics. So we see the relation to that in this subsection. We define quaternion hermitian groups G and G^1 by

$$G = \{\gamma \in M_n(D); \gamma\gamma^* = n(\gamma)1_n \text{ for some } n(\gamma) \in \mathbb{Q}_+^\times\},$$
$$G^1 = \{\gamma \in G; n(\gamma) = 1\}.$$

We denote by G_A and G_A^1 their adelizations, and by G_v and G_v^1 the v-adic components for $v \leq \infty$. We say that left O lattices L_1 and L_2 in D^n are in the same class if $L_2 = L_1\gamma$ for some $\gamma \in G$, and we say that L_1 and L_2 belong to the same genus if $L_2 = L_1\gamma_A$ for some $\gamma_A \in G_A$. If we define $U(L) = \{\gamma \in G_A; L\gamma_A = L\}$, then the classes in the genus $\mathcal{G}(L)$ which contains L is bijective to $U(L)\backslash G_A/G$. This is called the class number of L. We have $\{n(u); u \in U(L)\} = \mathbb{R}_+^\times \prod_q \mathbb{Z}_q^\times$ for any L ([**7**, Corollary 2.3]), and writing $U^1(L) = U(L) \cap G_A^1$, we have a bijection

$$U(L)\backslash G_A/G = U^1(L)\backslash G_A^1/G^1 \tag{4}$$

because of (1). So usually we do not care so much about the difference between G and G^1, since they are essentially the same. However, in our problems when R is not maximal, this is sometimes subtle, and mainly we formulate the problem by G^1, since this is suitable for our purpose. Since $L = O^n g$ for some $g \in GL_n(D)$ if $n \geq 2$, we interpret the class of L as an equivalent class of $H = gg^*$ with respect to $GL_n(O)$. For example, if we take another g_1 with $O^n g = O^n g_1$, then $g_1 = \epsilon g$ for some $\epsilon \in GL_n(O)$ and $\epsilon(gg^*)\epsilon^* = g_1 g_1^*$. However, if we consider an equivalent class of H with respect to $R \subsetneq M_n(O)$, then this cannot be interpreted directly to lattice classes. Since we are treating such cases, we are tempted to explain an equivalence class over R by a certain double coset of G_A, though there is no a priori reason that this is possible. We consider this problem in this subsection.

Since we would like to consider matrices H belonging to a certain fixed genus, we should fix a local condition on those g such that $H = gg^*$. We fix an element $g_{0,A} = (g_{0,v}) \in GL_n(D_A)$ and consider a left O lattice $L_0 = O^n g_{0,A}$. (We do not assume that $g_{0,A} \in SL_n(D_A)$.) Assume that $N(g_{0,q}) \in q^{e_q}\mathbb{Z}_q^\times$. Put $m = \prod_q q^{e_q} \in \mathbb{Q}^\times$. Then $m^{-1}N(g_{0,v}) \in \mathbb{Z}_q^\times$. Since $N(GL_n(O_q)) = \mathbb{Z}_q^\times$, there exists an element $g_1 \in GL_n(O_A)$ such that $N(g_1 g_{0,A}) = m \in \mathbb{Q}$. Since $O^n g_1 g_{0,A} = O^n g_{0,A}$, we may assume that $N(g_{0,A}) \in \mathbb{Q}_+^\times$ (diagonally embedded in $\mathbb{Q}_A^\times$) without changing the lattece L_0. We fix a lattice $L_0 g_A = O^n g_{0,A} g_A$ ($g_A \in G_A^1$) in a genus of L_0. This lattice class corresponds with the double coset $U^1(L)g_A G^1$. We have an element $g \in GL_n(D)$ such that $O^n g = O^n g_{0,A} g_A$. We fix an order $R_0 \subset M_n(O)$. Since we have $N(g_{0,A} g_A) = m$, and there exists an element $h \in GL_n(D)$ such that $N(h) = m$, and we have $g_{0,A} g_A h^{-1} \in SL_n(D_A)$. Then by (3), we have $g_{0,A} g_A h^{-1} = w_0^{-1} g_0$ for some $w_0 \in R_{0,A}^1$ and $g_0 \in SL_n(D)$. So replacing g by $g_0 h$ if necessary, we may assume that $L_0 g_A = O^n g$ and

$$g = w_0 g_{0,A} g_A, \qquad w_0 \in R_{0,A}^1.$$

We fix such g and w_0. For any order $R \subset M_n(O)$, we put

$$U^1(R) = g_{0,A}^{-1} w_0^{-1} R_A^1 w_0 g_{0,A} \cap G_A^1.$$

LEMMA 3.4. *For $H = gg*$, we have*

$$\Gamma_H(R) = gG^1 g^{-1} \cap R^\times = g(g_A^{-1} U^1(R) g_A \cap G^1) g^{-1}.$$

PROOF. We have $h \in \Gamma_H(R)$ if and only if $h \in R^\times$ and $hgg^*h^* = gg^*$, or equivalently $g^{-1}hg \in G^1$. Since we have

$$g^{-1}hg = g_A^{-1}(g_{0,A}^{-1} w_0^{-1} h w_0 g_{0,A}) g_A,$$

this belongs to G^1 if and only if $g_{0,A}^{-1} w_0^{-1} h w_0 g_{0,A} \in G_A^1$ and belongs to $g_A^{-1} U^1(R) g_A$ if and only if $h \in R^\times$. □

Now we assume that $R \subset R_0$. We define a mapping ϕ from $U^1(R_0)$ to $R^\times \backslash R_0^\times$ as follows. For any element $u \in U^1(R_0)$, write

$$k = w_0 g_{0,A} u g_{0,A}^{-1} w_0^{-1}.$$

Then by definition of $U^1(R_0)$, we have $k \in R^1_{0,A}$. Then by (3), we have $\epsilon = rk$ for some elements $r \in R^1_A$ and $\epsilon \in SL_n(D)$. Since $\epsilon \in R^1_A \cdot R^1_{0,A} = R^1_{0,A}$, we have $\epsilon \in R_0^\times$. Then we define a map $\phi : U^1(R_0) \to R^\times \backslash R_0^\times$ by

$$\phi(u) = R^\times \epsilon \in R^\times \backslash R_0^\times.$$

This mapping ϕ is well defined. Indeed, if $\epsilon_1 = r_1 k$, $\epsilon_2 = r_2 k$ for $r_i \in R^1_A$ and $\epsilon_i \in R_0^\times$, then $\epsilon_2 \epsilon_1^{-1} = r_2 r_1^{-1} \in R^\times$, so we have $R^\times \epsilon_1 = R^\times \epsilon_2$.

PROPOSITION 3.5. *The mapping ϕ induces following injections.*

(1) $\phi_1 : U^1(R) \backslash U^1(R_0) \to R^\times \backslash R_0^\times$,
(2) $\phi_2 : U^1(R) \backslash U^1(R_0) g_A G^1 / G^1 \to R^\times \backslash R_0^\times / \Gamma_H(R_0)$.

PROOF. We prove (1). Since the claim that ϕ induces a mapping ϕ_1 from $U^1(R) \backslash U^1(R_0)$ is almost trivial, we prove only the injectivity of ϕ_1. For $u_i \in U^1(R_0)$ $(i = 1, 2)$, assume that $\phi(u_1) = \phi(u_2)$. For $i = 1, 2$, write $k_i = w_0 g_{0,A} u_i g_{0,A}^{-1} w_0^{-1}$ and $\epsilon_i = r_i k_i$ where $r_i \in R^1_A$, $\epsilon_i \in R_0^\times$. By definition, we have

$$R^\times \epsilon_1 = \phi(u_1) = \phi(u_2) = R^\times \epsilon_2.$$

Then we have $\epsilon_2 = r_0 \epsilon_1$ for some $r_0 \in R^\times$. So we have $r_2 k_2 = r_0 r_1 k_1$, and

$$w_0 g_{0,A} u_2 g_{0,A}^{-1} w_0^{-1} = k_2 = (r_2^{-1} r_0 r_1) k_1 = (r_2^{-1} r_0 r_1) w_0 g_{0,A} u_1 g_{0,A}^{-1} w_0^{-1}.$$

So we have

$$u_2 = (g_{0,A}^{-1} w_0^{-1} (r_2^{-1} r_0 r_1) w_0 g_{0,A}) u_1.$$

Since $u_1, u_2 \in G^1_A$, we have $u_2 u_1^{-1} = g_{0,A}^{-1} w_0^{-1} (r_2^{-1} r_0 r_1) w_0 g_{0,A} \in G^1_A$ and since $r_2^{-1} r_0 r_1 \in R^1_A$, we have $u_2 u_1^{-1} \in U^1(R)$. So the map ϕ_1 in (1) is injective. Next we see (2). For any element $u g_A \gamma \in U^1(R_0) g_A G^1$, we define $\phi_2(u g_A \gamma) = R^\times \phi(u) G^1$. First we see that this mapping is well defined. For $u_1, u_2 \in U^1(R_0)$, we define k_i and $\epsilon_i = r_i k_i$ for $i = 1, 2$ as before, and we put $\phi(u_i) = \epsilon_i$ as above. Assume that $u_1 g_A \gamma_1 = u_2 g_A \gamma_2$ for $u_i \in U^1(R_0)$ and $\gamma_i \in G^1$ for $i = 1, 2$, then

$$\gamma_1 \gamma_2^{-1} = g_A^{-1} u_1^{-1} u_2 g_A = g_A^{-1} g_{0,A}^{-1} w_0^{-1} k_1^{-1} k_2 w_0 g_{0,A} g_A = g^{-1} k_1^{-1} k_2 g.$$

Since $\gamma_1 \gamma_2^{-1} \in G^1$, $g \in GL_2(D)$ and $k_1^{-1} k_2 \in R^1_{0,A}$, we have $k_1^{-1} k_2 = g(\gamma_1 \gamma_2) g^{-1} \in R_0^\times$ and $\gamma_1 \gamma_2^{-1} \in G^1 \cap g^{-1} R_0^\times g$. So we have $k_1^{-1} k_2 = g \gamma_1 \gamma_2^{-1} g^{-1} \in \Gamma_H(R_0)$. However, we have

$$\epsilon_2 = r_2 k_2 = (r_2 r_1^{-1})(r_1 k_1)(k_1^{-1} k_2) = (r_2 r_1^{-1}) \epsilon_1 (k_1^{-1} k_2).$$

Since $k_1^{-1} k_2 \in \Gamma_H(R_0)$ and $\epsilon_i \in R_0^\times$, we have $r_2 r_1 \in R^1_A \cap R_0^\times = R^\times$. So we have $\epsilon_2 \in R^\times \epsilon_1 \Gamma_H(R_0)$. So the mapping ϕ_2 from $U^1(R_0) g_A G$ to $R^\times \backslash R_0^\times / \Gamma_H(R_0)$ is well

defined. We see that ϕ_2 is injective. Assume that $\phi_2(u_1 g_A \gamma_1) = \phi_2(u_2 g_A \gamma_2)$. For $k_i = w_0 g_{0,A} u_i g_{0,A}^{-1} w_0^{-1}$ and $\epsilon_i = r_i k_i$, we assume that $\epsilon_2 = r_0 \epsilon_1 h$ for some $r_0 \in R^\times$ and $h \in \Gamma_H(R_0)$. Then we have $k_2 = r_2^{-1}\epsilon_2 = r_2^{-1} r_0 r_1 k_1 h$ and

$$\begin{aligned} u_2 g_A &= g_{0,A}^{-1} w_0^{-1} k_2 w_0 g_{0,A} g_A \\ &= (g_{0,A}^{-1} w_0^{-1} (r_2^{-1} r_0 r_1) w_0 g_{0,A}) \times (g_{0,A}^{-1} w_0^{-1} k_1 w_0 g_{0,A}) g_A \times g_A^{-1} g_{0,A}^{-1} w_0^{-1} h w_0 g_{0,A} g_A \\ &= (g_{0,A}^{-1} w_0^{-1} (r_2^{-1} r_0 r_1) w_0 g_{0,A}) \times u_1 g_A (g^{-1} h g). \end{aligned}$$

So $g_{0,A}^{-1} w_0^{-1} (r_2^{-1} r_0 r_1) w_0 g_{0,A} \in G_A^1$, hence this belongs to $U^1(R)$. Since $g^{-1} h g \in G^1$, we have $u_2 g_A \in U^1(R) u_1 g_A G^1$. □

It seems that ϕ_1 and ϕ_2 are not surjective in general, and in fact we have no reason to expect surjectivity. However, for the case we treat in this paper, we can show it.

THEOREM 3.6. *In the above setting, assume that $n = 2$, L belongs to the non-principal genus, $R_0 = M_2(O)$, and $R = R_1$ or R_2 defined as in Lemma 2.2. Then the maps ϕ_1 and ϕ_2 in Proposition 3.5 are bijections. In particular, the number of isomorphism classes of principal polarizations of a fixed supersingular abelian variety A which is not superspecial is equal to*

$$\#(U^1(R_i) \backslash G_A^1 / G^1)$$

for $i = 1$ and 2 corresponding to the case (I) *and* (II)*, respectively.*

PROOF. It is enough to show that ϕ_1 is surjective. To do this, it is enough to show that

$$[GL_2(O) : R_i^\times] = [U^1(M_2(O)) : U^1(R_i)]$$

for $i = 1, 2$. Since the LHS index is known in Lemma 3.2, we calculate the RHS index and show that these indices are equal. Since $L = O^2 g$ belongs to the non-principal genus, we may take $g_{0.A} = (g_{0,v})$ so that $N(g_{0,A}) = p \in \mathbb{Q}_+^\times$, $g_{0,q} \in GL_n(O_q)$ for $q \neq p$ and

$$g_{0,p} = \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} \xi,$$

where $\xi \in GL_2(O_q)$ with $\xi \xi^* = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. (See [**15**].) We have

$$[U^1(M_2(O)) : U^1(R_i)] = [U^1(M_2(O_p)) : U^1(R_{i,p})],$$

where $U^1(R_{i,p})$ is the p-adic component of $U^1(R_i)$. We write $U_p^1 = U^1(M_2(O_p))$ for the sake of simplicity. Writing $w_0 = (w_{0,v})$, we have

$$\begin{aligned} U_p^1 &= (g_{0,p}^{-1} w_{0,p}^{-1} SL_2(O_p) w_{0,p} g_{0,p}) \cap G_p^1 \\ &= \xi^{-1} \begin{pmatrix} O_p & \pi^{-1} O_p \\ \pi O_p & O_p \end{pmatrix}^\times \xi \cap G_p^1. \end{aligned}$$

For $u = g_{0,p}^{-1} w_{0,p}^{-1} h w_{0,p} g_{0,p} \in U_p^1$, we write $\phi_0(u) = w_{0.p}^{-1} h w_{0,p} \bmod \pi \in M_2(\mathbb{F}_{p^2})$. First, we show that $\phi_0(u) \in SL_2(\mathbb{F}_{p^2})$. We write

$$w_{0,p}^{-1} h w_{0,p} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Then we have

$$\xi^{-1} \begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} \xi \in G_p^1.$$

So we have

$$\begin{pmatrix} \pi^{-1}a\pi & \pi^{-1}b \\ c\pi & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \overline{\pi^{-1}a\pi} & \overline{c\pi} \\ \overline{\pi^{-1}b} & \overline{d} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where $\overline{*}$ is the main involution. So comparing the $(1, 2)$ components, we see that $\pi^{-1}a\pi\overline{d} - \pi^{-1}b\pi\overline{c} = 1$. For any $x \in O_p$, we have $\pi^{-1}x\pi \equiv \overline{x} \bmod \pi$, so we have $ad - bc \equiv 1 \bmod \pi$. So we have $\det(h \bmod \pi) = \det(w_{0.p}^{-1} h w_{0,p} \bmod \pi) = 1$. So this gives a map from U_p^1 to $SL_2(\mathbb{F}_{p^2})$. Secondly we show that ϕ_0 is surjective to $SL_2(\mathbb{F}_{p^2})$. The maximal order O_p contains the ring o_F of integers of the unramified quadratic extension of $\mathbb{Q}_p$ and we may write $O_p = o_F + \pi o_F$, where $\pi\alpha = \overline{\alpha}\pi$ for any $\alpha \in o_F$. We have $o_F \bmod p = \mathbb{F}_{p^2}$ and $o_F^{\times} \bmod p = \mathbb{F}_{p^2}^{\times}$. It is easy to see that the following elements are in U_p^1.

$$\xi^{-1} \begin{pmatrix} 1 & \pi^{-1}\alpha \\ 0 & 1 \end{pmatrix} \xi, \qquad \alpha \in o_F,$$

$$\xi^{-1} \begin{pmatrix} 1 & 0 \\ \pi\alpha & 1 \end{pmatrix} \xi, \qquad \alpha \in o_F,$$

$$\xi^{-1} \begin{pmatrix} \beta & 0 \\ 0 & \overline{\beta}^{-1} \end{pmatrix} \xi, \qquad \beta \in o_F^{\times}.$$

It is well known that $SL_2(\mathbb{F}_{p^2})$ is generated by upper and lower triangular unipotent matrices and diagonal matrices, so $\phi_0(U_p^1)$ generates $SL_2(\mathbb{F}_{p^2})$. Hence ϕ_0 is surjective. The group $U(R_{i,p})$ for $i = 1, 2$ contains the kernel of this map ϕ_0 since $1 + \pi M_2(O_p) \subset R_{i,p}$. We have

$$\phi_0(U(R_{1,p})) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}; a \in \mathbb{F}_{p^2}, a^2 = 1 \right\}.$$

So $\#(\phi_0(U^1(R_{1,p}))) = 1$ if $p = 2$ and $= 2$ if $p \neq 2$. For $K \cong \mathbb{F}_{p^4}$ in the definition of R_2, we put $K_1 = (w_0 \bmod \pi)^{-1} K (w_0 \bmod \pi) \subset M_2(\mathbb{F}_{p^2})$. Then we have

$$\phi_0(U^1(R_{2,p})) = \{x \in K_1^{\times} \cong \mathbb{F}_{p^4}; \det(x) = 1\}.$$

Since $\det(x) = N_{\mathbb{F}_{p^4}/\mathbb{F}_{p^2}}(x) = x^{p^2+1} = 1$, we have $\#(\phi_0(U^1(R_{2,p})) = p^2 + 1$. So by Lemma 3.2, we have $[U_p^1 : U^1(R_{i,p})] = [GL_2(O) : R_i^{\times}]$ for $i = 1$ and 2. □

COROLLARY 3.7. *For a fixed supersingular abelian surface A which is not superspecial, the number of principal polarizations of A up to isomorphism is equal to the number of double cosets in $U^1(R_i)\backslash G_A^1/G^1$ where $i = 1$ for the case* (I) *and $i = 2$ for* (II).

4. Automorphism groups.

As before, let A be a supersingular surface which is not superspecial. By Corollary 3.7, the number of principal polarizations can be in principle calculated by the Selberg trace formula for $U^1(R_i)$. However, in this section, we will obtain this number by seeing possible cardinality of $\mathrm{Aut}(A, \lambda)$ concretely and using the mass formula. It is well known that $\mathrm{Aut}(A, \lambda)$ is a finite group. This group is isomorphic to $\Gamma_H(R_i) \cong g_A^{-1}U(R_i)g_A \cap G^1$ for some $g_A \in G_A^1$ and some quaternion hermitian matrix H. Of course $\Gamma_H(R_i) \subset \Gamma_H = \Gamma_H(M_2(O))$. The map ϕ_0 of U_p^1 to $SL_2(\mathbb{F}_{p^2})$ defined in the proof of Theorem 3.6 is essentially the same map given in [**6**, pp.312–313] , and there we have shown that the restriction of ϕ_0 to $\Gamma_H = \Gamma_H(M_2(O))$ through an embedding $\Gamma_H \to U_p^1$ is injective to $SL_2(\mathbb{F}_{p^2})$ for $p \geq 7$. By a comment of C.-F. Yu, this is also true for $p = 5$, which is explained below.

LEMMA 4.1. *If $p \geq 5$, the above mapping of Γ_H to $SL_2(\mathbb{F}_{p^2})$ is injective.*

PROOF. This has been proved in [**6**] in pages 312 and 313 when $p \geq 7$. (There we used the fact that prime factors of the order of any non-unit element in Γ_H are either 2, 3 or 5 and that the order of any torsion in $ker(\phi_0)$ is divisible by p.) Now we supply the proof for $p = 5$ given by C.-F. Yu. Since Γ_H is a finite group, any element $\gamma \in \Gamma_H$ is a torsion element. The kernel of ϕ_0 is in $1_2 + \pi M_2(O_p)$. The group $1_2 + \pi M_2(O_p)$ has no torsion element whose order is prime to p. Indeed, take $x \in 1_2 + \pi M_2(O_p)$. Then since $[1_2 + \pi M_2(O_p) : 1_2 + \pi^l M_2(O_p)] = p^{8(l-1)}$ for any integer $l \geq 1$, we have $x^{p^{8(l-1)}} \in 1_2 + \pi^l M_2(O_p)$ for all $l \geq 1$. If x is of order m and $(m, p) = 1$, then there exist r and $s \in \mathbb{Z}$ such that $1 = mr + sp^{8(l-1)}$ and we have $x = (x^m)^r(x^{p^{8(l-1)}})^s \in 1 + \pi^l M_2(O_p)$ for any l. This means that $x = 1$. So it is enough to show that there is no element in Γ_H of order p. Now assume that $p = 5$. If $\zeta \in 1_2 + \pi M_2(O_p)$ is of order 5, then since $\mathbb{Q}_5(\zeta)/\mathbb{Q}_5$ is totally ramified over $\mathbb{Q}_5$, the reduced norm of $1_2 - \zeta$ is $\prod_{i=1}^4(1 - \zeta^i) = 5$, while the reduced norm of any element of $\pi M_2(O_p)$ is divisible by $N(\pi)^2 = 5^2$. So this is a contradiction and there is no torsion element in the kernel. Hence the map ϕ_0 is injective on Γ_H also in this case. □

REMARK. C.-F. Yu proved that for any n and $p \geq 5$, $1_n + M_n(O_p)$ is torsion free by the same line of proof as above.

From now on, we assume that $p \geq 5$ in this section.

If $R = R_1$, then the condition $\epsilon \in R_{1,p}^\times$ is equivalent to the condition $w_{0,p}^{-1}\epsilon w_{0,p} \in R_{1,p}^\times$, where we write $w_0 = (w_{0,v})$ as in the last section. Then the image $\phi_0(\Gamma_H(R_1))$ is in

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \in SL_2(\mathbb{F}_{p^2}).$$

So we have $x^2 = 1$ and $x = \pm 1$. Since the map is injective for $p \geq 5$, this means that $\Gamma_H(R_1) = \{\pm 1_2\}$. This proves the case (I). Next we consider the case (II). We see that $w_{0,p}^{-1} R_2 w_{0,p} \bmod \pi$ is a conjugate of K so still isomorphic to $\mathbb{F}_{p^4}$. Since the determinant of the image of

$$\begin{pmatrix} \pi^{-1} & 0 \\ 0 & 1 \end{pmatrix} \epsilon_p^{-1} R_2 \epsilon_p \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}$$

by ϕ_0 is just the norm of elements of $\mathbb{F}_{p^4}$ over $\mathbb{F}_{p^2}$, the image of $\Gamma_H(R_2)$ is contained in the set of norm 1 elements

$$\mathbb{F}_{p^4}^{(1)} = \{x \in \mathbb{F}_{p^4}; N_{\mathbb{F}_{p^4}/\mathbb{F}_{p^2}}(x) = 1\}.$$

We have $\mathbb{F}_{p^4}^{(1)} = \{x \in \mathbb{F}_{p^4}; x^{p^2+1} = 1\}$ and this is a cyclic group of order $p^2 + 1$. By Lemma 4.1, we have an injective homomorphism of $\Gamma_H(R_2) = R_2^\times \cap \Gamma_H$ to the group $\mathbb{F}_{p^4}^{(1)}$, so $\Gamma_H(R_2)$ is a cyclic group whose order is a divisor of $p^2 + 1$. For any p, the number $p^2 + 1$ is not divisible by 3 so there are no elements of order 3 in $\Gamma_H(R_2)$. When $p \equiv \pm 1 \bmod 5$ or $p = 5$, we have $p^2 + 1 \equiv 1$ or $2 \bmod 5$, so there are no elements of order 5 in $\Gamma_H(R_2)$. For any odd p, we have $p^2 + 1 \equiv 2 \bmod 8$, so there are no elements of order 4 in $\Gamma_H(R_2)$. Since $\Gamma_H(R_2)$ is cyclic, there is only one element of order 2 which is given by -1_2. Since Γ_H has only elements of order 1, 2, 3, 4, 5, 6, 8, 10, 12 (cf. [**3**]), possible candidates of the groups $\Gamma_H(R_2)$ are $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}$. In particular, if $p = 5$ or $p \equiv \pm 1 \bmod 5$, the only candidate is $\mathbb{Z}/2\mathbb{Z}$. Next we see the case $p \equiv \pm 2 \bmod 5$. For the case (II), we have

$$M(A) = \frac{p^2(p^2-1)^2}{5760}.$$

Since $p^2(p^2-1)^2 \equiv 1 \bmod 5$ if $p \equiv \pm 2 \bmod 5$, the numerator is not divisible by 5 and there should exist at least one H such that $\Gamma_H(R_2) = \mathbb{Z}/10\mathbb{Z}$. Now we prove that there is only one such H up to $R_2^\times$ equivalence. Fix an element $H \in \mathcal{P}$ such that $\Gamma_H(R_2) = \mathbb{Z}/10\mathbb{Z}$. By [**6**, Theorem 7.1], we have $\Gamma_H/\{\pm 1_2\} \cong A_5$ in this case for $p \geq 7$, where A_5 is the alternating group of degree 5. Now assume that for $H_0 \in \mathcal{P}$, there exists an element of order 5 in $\Gamma_{H_0} \cap R_2^\times$. By the result of [**6**, Theorem 7.1], if Γ_{H_0} contains an element of order 5, then H_0 and H are $GL_2(O)$ equivalent. Our aim is to show that any such H_0 is $R_2^\times$ equivalent to H. So write $\epsilon_0 H \epsilon_0^* = H_0$ for some $\epsilon_0 \in GL_2(O)$. By assumption, we have $\epsilon \in R_2^\times$ of order 5 such that

$$\epsilon \epsilon_0 H \epsilon_0^* \epsilon^* = \epsilon_0 H \epsilon_0.$$

So we have

$$\epsilon_0^{-1} \epsilon \epsilon_0 \in \Gamma_H.$$

Now A_5 has 24 elements of order 5 and there are 6 different groups of order 5 in A_5. We can check directly that these groups are all conjugate by elements of A_5. The pullbacks of these groups to Γ_H are cyclic groups of order 10, and these are also conjugate by Γ_H

since if $\zeta \in \Gamma_H$ is of order 5, then $-\zeta$ is of order 10 and ζ and $-\zeta$ are not conjugate. So there is an element $\zeta \in \Gamma_H(R_2)$ of order 5 and an element $\gamma \in \Gamma_H$ such that

$$\epsilon_0^{-1}\epsilon\epsilon_0 = \gamma^{-1}\zeta\gamma. \tag{5}$$

Both elements $\epsilon, \zeta \in R_2^\times$ are of order 5. By injectivity of ϕ_0, the elements $\overline{\epsilon} := (\epsilon \bmod \pi)$ and $\overline{\zeta} := (\zeta \bmod \pi)$ are also of order 5. Since the subgroup of order 5 of $(\mathbb{F}_{p^4})^\times$ is unique, we have $\overline{\epsilon} = \overline{\zeta}^j$ for some j with $1 \le j \le 4$. By our assumption $p \equiv \pm 2 \bmod 5$, we have $\mathbb{F}_p[\overline{\zeta}] \cong \mathbb{F}_{p^4}$, and $\mathbb{F}_p[\overline{\zeta} + \overline{\zeta}^{-1}] \cong \mathbb{F}_{p^2}$. However, since $\zeta \in R_2$, we have $\mathbb{F}_p[\overline{\zeta} + \overline{\zeta}^{-1}] = \mathbb{F}_{p^2} \cdot 1_2 \subset M_2(\mathbb{F}_{p^2})$. By (5), elements $\overline{\epsilon}$ and $\overline{\zeta}$ are conjugate by elements of $GL_2(\mathbb{F}_{p^2})$. Since this conjugate is trivial on the center $\mathbb{F}_{p^2} \cdot 1_2 \subset M_2(\mathbb{F}_{p^2})$, we have $\overline{\epsilon} = \overline{\zeta}$ or $\overline{\epsilon} = \overline{\zeta}^{-1}$. So by the injectivity of ϕ_0, we have $\epsilon = \zeta$ or $\epsilon = \zeta^{-1}$. However, seeing the conjugacy classes of A_5 in details, we can see that the projections of ζ and ζ^{-1} in A_5 are conjugate in A_5 and hence ϵ and ζ are conjugate in Γ_H. So changing $\gamma \in \Gamma_H$ if necessary, we may assume that

$$\epsilon_0^{-1}\epsilon\epsilon_0 = \gamma^{-1}\epsilon\gamma.$$

This means that $\epsilon_0\gamma^{-1} \bmod \pi$ commutes with the fixed subfield $\mathbb{F}_{p^4} = \mathbb{F}_p[\overline{\epsilon}]$ of $M_2(\mathbb{F}_{p^2})$ containing $\mathbb{F}_{p^2} \cdot 1_2$. By the Skolem–Noether theorem, this means that $\epsilon_0\gamma^{-1} \bmod \pi \in (\mathbb{F}_{p^4})^\times$. By definition of R_2, this means that $\epsilon_0\gamma^{-1} \in R_2^\times$. So $\epsilon_0 \in R_2^\times\Gamma_H$ and H_0 is $R_2^\times$ equivalent to H. So there is only one $R_2^\times$ equivalence class in $\mathcal{P}$ such that the automorphism group is $\mathbb{Z}/10\mathbb{Z}$. So we prove the claims in the introduction for $p \ge 5$.

5. The cases $p = 2$ and $p = 3$.

We consider the remaining cases $p = 2$ and $p = 3$ and prove Theorems in these cases. We note that the class number of the non-principal genus (that is, the number of $GL_2(O)$ equivalence classes in $\mathcal{P}$) is 1 for both $p = 2$ and 3 (see [**3**]). For $p = 2$, we may write the maximal order of D as

$$O = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}\frac{1+i+j+k}{2},$$

where $i^2 = j^2 = -1$, $ij = -ji = k$. Then we know that the representative of lattices in the non-principal genus is given by

$$H = \begin{pmatrix} 2 & \overline{r} \\ r & 2 \end{pmatrix} = gg^*,$$

where $r = i - k$ and $g = \begin{pmatrix} 1 & -1 \\ 0 & r \end{pmatrix}$ (see [**3**]). The isomorphism group $\Gamma = g^{-1}M_2(O)^\times g \cap G$ considered in the quaternion hermitian group G is given by the following 1920 elements (see [**5**, p.592]).

$$\begin{pmatrix} ar^{-1} & -aa_0r^{-1} \\ ar^{-1} & aa_0r^{-1} \end{pmatrix}, \qquad \begin{pmatrix} ar^{-1} & aa_0r^{-1} \\ -ar^{-1} & aa_0r^{-1} \end{pmatrix},$$

$$\begin{pmatrix} a & 0 \\ 0 & aa_0 \end{pmatrix}, \qquad \begin{pmatrix} 0 & aa_0 \\ a & 0 \end{pmatrix}, \tag{6}$$
$$\begin{pmatrix} (1+r^{-1}x)a & r^{-1}xaa_0 \\ r^{-1}xa & (1+r^{-1}x)aa_0 \end{pmatrix},$$

where a, a_0 and x run respectively over the following sets

$$a \in O^\times = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\},$$
$$a_0 \in \{\pm 1, \pm i, \pm j, \pm k\},$$
$$x \in \{-i, k, (\pm 1 - i \pm j + k)/2\}.$$

For $\gamma \in \Gamma$, we see the condition that $g\gamma g^{-1} \equiv 1_2 \bmod \pi$, where $\pi = i - k$ is a prime element of O over p. This is the condition for the case (I), i.e. the case $t \notin \mathbb{F}_{p^4}$. For example, we see that

$$g \begin{pmatrix} a & 0 \\ 0 & aa_0 \end{pmatrix} g^{-1} = \begin{pmatrix} a & a(1-a_0)r^{-1} \\ 0 & raa_0 r^{-1} \end{pmatrix}.$$

This is $1_2 \bmod \pi (= -1_2 \bmod \pi)$ if and only if $a \equiv aa_0 \bmod \pi$ and $a_0 \equiv 1 \bmod 2$. This is satisfied if and only if $a_0 = \pm 1$ and $a \in \{\pm 1, \pm i, \pm j, \pm k\}$. In the same way we see that $g \begin{pmatrix} 0 & aa_0 \\ a & 0 \end{pmatrix} g^{-1}$ satisfies the condition if and only if a, a_0 satisfy the same conditions as above condition. For all the other $\gamma \in \Gamma$, we can see by direct calculation that $g\gamma g^{-1}$ does not satisfy the condition. So the automorphism group Γ_1 of this H in $R_1^\times$ is a group of order 32 and is isomorphic to the group given by

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & \pm a \end{pmatrix}, \begin{pmatrix} 0 & \pm a \\ a & 0 \end{pmatrix}; \quad a \in \{\pm 1, \pm i, \pm j, \pm k\} \right\}.$$

Since the mass for $p = 2$ in the case (I) is $1/32$, there are no other class and the number of $R_1^\times$ equivalence class is one.

Next we see that the number of $R_2^\times$ equivalence classes is also one for the case (II) when $p = 2$. As we have shown, there is a homomorphism ϕ_0 from Γ to $SL_2(\mathbb{F}_4)$. The latter group is of order $4 \cdot (4^2 - 1) = 60$. Since the order of the kernel is 32 as we have shown above, and $1920/32 = 60$, the map from Γ is surjective. So the inverse image of $\{x \in \mathbb{F}_{2^4}; x^{4+1} = 1\}$ in Γ is of order $5 \times 32 = 160$. Since the mass for the case (II) is $1/160$, again there is only one R_2 equivalence class and a group Γ_2 of automorphisms in $R_2^\times$ is of order 160. Of course we have $\Gamma_2 \subset \Gamma$ but the group Γ_2 depends on a choice of K (i.e. the tangent t). For example, if we take

$$K = \begin{pmatrix} a & b \\ b & a + b\eta \end{pmatrix}, \qquad a, b \in \mathbb{F}_4,$$

where $\eta \in \mathbb{F}_4$ is an element such that $\eta^2 + \eta + 1 = 0$, then among elements of Γ in (6), there are 16 elements of Γ_2 in each of the first 4 types in (6) and 96 elements in the last type in (6). So we see directly that $\#(\Gamma_2) = 16 \times 4 + 96 = 160$. We omit the details.

Next we consider the case $p = 3$. Also in this case, the automorphism group can be written down explicitly as in the case when $p = 2$. However, here we omit this description and we show the necessary results in a little more abstract way. When $p = 3$, the class number of the non-principal genus is again one ([**3**]), and we write the corresponding quaternion hermitian matrix by H. By [**10**], it is known that $\Gamma_H/\{\pm 1_2\} \cong A_6$ for $\Gamma_H = \Gamma_H(M_2(O)) \cong \mathrm{Aut}(E^2, \lambda_0)$ for the polarization λ_0 of E^2 in the non-principal genus. On the other hand, we have a homomorphism ϕ_0 of Γ_H to the group $SL_2(\mathbb{F}_9)$ of order 720. We also know that $PSL_2(\mathbb{F}_9) \cong A_6$. So it is likely that the image of Γ_H is exactly $SL_2(\mathbb{F}_9)$. Indeed, if we map Γ_H to $SL_2(\mathbb{F}_9)$ as before, then by definition, the element -1_2 is not in the kernel of the mapping. So if we denote by Γ_0 the kernel of this mapping, then $\Gamma_0 \cap \{\pm 1_2\} = \{1\}$. Since Γ_0 is a normal subgroup of Γ_H and $A_6 = \Gamma_H/\{\pm 1_2\}$ is a simple group, we have $\Gamma_0 = \{1_2\}$ or $\Gamma_H = \Gamma_0 \times \{\pm 1_2\}$. The latter case does not occur since we know that Γ_H contains an element γ of order 4 whose characteristic polynomial is $(x^2+1)^2$ (see [**3**]), and hence $\gamma^2 = -1_2$, which cannot happen for elements in $\Gamma_0 \times \{\pm 1_2\}$. So we see that the kernel is trivial and comparing the group order we see that $\Gamma \cong SL_2(\mathbb{F}_9)$. For the case (I), the image of $\Gamma_H(R_1) \to SL_2(\mathbb{F}_9)$ is $\{\pm 1\}$, so $\Gamma_H(R_1) \cong \mathrm{Aut}(A, \lambda)$ is equal to $\{\pm 1_2\}$ for the principal polarization λ of A such that $\lambda_0 = \psi^*(\lambda)$. However, we have

$$M(A) = \frac{3^2(3^4-1)(3^2-1)}{2 \cdot 5760} = \frac{1}{2}.$$

So there is only one isomorphism class of principal polarizations of A. For the case (II), the image of $\Gamma_H(R_2) \to SL_2(\mathbb{F}_9)$ is isomorphic to the group of norm one subgroup of $\mathbb{F}_{3^4}^{\times}$ over $\mathbb{F}_9$, which is a cyclic group of order $3^2 + 1 = 10$. However, the mass in this case is

$$M(A) = \frac{3^2(3^2-1)^2}{5760} = \frac{1}{10}.$$

So there is only one isomorphism class and the automorphism group is $\mathbb{Z}/10\mathbb{Z}$.

So all the claims in the theorems in the introduction are proved.

Acknowledgements. This work was finished during the author's stay in Academia Sinica in November 2018. The author would like to express his sincere thanks to their kind hospitality and ideal circumstances. He also thanks Professor Jiangwei Xue and Professor Chia-Fu Yu for fruitful discussions. In particular, a professor Yu's comment on the case $p = 5$ enables us to treat the case uniformly. The author also thanks Professor Rachel Pries for having questions to him in JAMI conference in 2017. This gave him a good motivation to come back to this area again after his long pause on the subject.

References

[1] S. J. Edixhoven, B. J. J. Moonen and F. Oort (Eds.), Open problems in algebraic geometry, Manuscript presented by M.-P. Malliavin, Bull. Sci. Math., **125** (2001), 1–22, Problem 4.

[2] M. Eichler, Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und ihre L-Reihen, J. Reine Angew. Math., **179** (1938), 227–251.

[3] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion Hermitian forms. I, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **27** (1980), 549–601; II, **28** (1982), 695–699; III, **30** (1983), 393–401.
[4] K. Hashimoto, Class numbers of positive definite ternary quaternion Hermitian forms, Proc. Japan Acad. Ser. A Math. Sci., **59** (1983), 490–493.
[5] T. Ibukiyama, On symplectic Euler factors of genus two, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **30** (1984), 587–614.
[6] T. Ibukiyama, On automorphism groups of positive definite binary quaternion Hermitian lattices and new mass formula, In: Automorphic Forms and Geometry of Arithmetic Varieties, Adv. Stud. Pure Math., **15**, Academic Press, Boston, MA, 1989, 301–349.
[7] T. Ibukiyama, Type numbers of quaternion hermitian forms and supersingular abelian varieties, Osaka J. Math., **55** (2018), 369–384.
[8] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math., **57** (1986), 127–152.
[9] V. Karemaker and R. Pries, Fully maximal and fully minimal abelian varieties, J. Pure Appl. Algebra, **223** (2019), 3031–3056.
[10] T. Katsura and F. Oort, Families of supersingular abelian surfaces, Compositio Math., **62** (1987), 107–167.
[11] M. Kneser, Strong approximation, In: Algebraic Groups and Discontinuous Subgroups, Proc. Sympos. Pure Math., **IX**, Amer. Math. Soc., Providence, RI, 1966, 187–196.
[12] L. Moret-Bailly, Familles de courbes et de variété abéliennes sur $\mathbb{P}^1$: I. Descente des polarisations, In: Séminaire sur les pinceaux de courbes de genre au moins deux, Astérisque, **86**, 1981, 109–124; II. Exemples, 125–140.
[13] F. Oort, Which abelian surfaces are products of elliptic curves?, Math. Ann., **214** (1975), 35–47.
[14] J.-P. Serre, Corps Locaux, Publications de l'Institut de Mathématique de l'Université de Nancago, **VIII**, Actualités Sci. Indust., **1296**, Hermann, Paris, 1962, 243 pp.
[15] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan, **15** (1963), 33–65.
[16] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions. Kanô Memorial Lectures, **1**, Publications of the Math. Soc. Japan, **11**, Iwanami Shoten, Publishers, Tokyo; Princeton Univ. Press, Princeton, NJ, 1971, xiv+267 pp.
[17] A. Weil, Basic Number Theory, Grundlehren Math. Wiss., **144**, Springer-Verlag New York, Inc., New York, 1967, xviii+294 pp.
[18] C.-F. Yu and J.-D. Yu, Mass formula for supersingular abelian surfaces, J. Algebra, **322** (2009), 3733–3743.

Tomoyoshi IBUKIYAMA
Department of Mathematics
Graduate School of Mathematics
Osaka University
Machikaneyama 1-1, Toyonaka
Osaka 560-0043, Japan
E-mail: ibukiyam@math.sci.osaka-u.ac.jp