

COMPOSITIO MATHEMATICA

TOMOYOSHI IBUKIYAMA

TOSHIYUKI KATSURA

**On the field of definition of superspecial polarized
abelian varieties and type numbers**

Compositio Mathematica, tome 91, n° 1 (1994), p. 37-46

http://www.numdam.org/item?id=CM_1994__91_1_37_0

© Foundation Compositio Mathematica, 1994, tous droits réservés.

L'accès aux archives de la revue « Compositio Mathematica » (<http://www.compositio.nl/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

On the field of definition of superspecial polarized abelian varieties and type numbers

TOMOYOSHI IBUKIYAMA¹ and TOSHIYUKI KATSURA²

¹*Department of Mathematics, College of General Education, Osaka University, Toyonaka 560, Japan*

²*Department of Mathematical Sciences, The University of Tokyo, Tokyo 153, Japan*

Received 17 August 1990; accepted in final form 12 January 1993

Many algebro-geometrical phenomena on an abelian variety A which is the product of supersingular elliptic curves over the field of characteristic $p > 0$ are related to the arithmetic theory on quaternion hermitian lattices, as was shown, for example, in [3], [10], [11], [8]. Now, in this paper, we shall study the relation between the field of definition of principally polarized abelian varieties (A, Θ) , where A is as above, and some arithmetic nature on quaternion hermitian lattices, for example, Hecke operators, type numbers and so on. When $\dim A = 1$, that is, when A is a supersingular elliptic curve, Deuring [3] has shown that A has a model defined over the finite field \mathbb{F}_{p^2} and the number of those which have a model over \mathbb{F}_p is expressed by the class number and the type number of $\text{End}(A)$. But, when $\dim A \geq 2$, all the abelian varieties as above are isomorphic with each other and have a model defined over \mathbb{F}_p (This fact is due to Shioda, Deligne and Ogus). In this case, the arithmetic of quaternion hermitian lattices is mainly reflected on the nature of polarizations on A . For example, the number of isomorphism classes of principally polarized abelian varieties (A, Θ) is equal to the class number of some n -ary quaternion hermitian lattices (cf. [10]). In this paper, first, we shall show that every principally polarized abelian variety (A, Θ) (A : as above) is isomorphic to one defined over \mathbb{F}_{p^2} and give a criterion on having a model defined over \mathbb{F}_p (§1. Theorem 1), and secondly, we shall show that the number of isomorphism classes of principally polarized abelian variety which has a model defined over \mathbb{F}_p is equal to the trace of some Hecke operator of quaternion hermitian group and that it is also expressed by the class number and the ‘type number’ of quaternion hermitian group (§1. Theorem 2). When $\dim A = 2$, these numbers can be explicitly calculated (§1. Remark 3). As a corollary to these results, we also get the results on the field of definitions of supersingular curves (§1. Remark 1, 3). In the forthcoming paper [9], similar (but slightly finer) problem as above will be treated with the application to the number of rational points of curves over finite fields. More precise statement of our main results will be given in Section 1, together with reviews on notations and precise definitions.

In Section 2, we shall prepare some algebro-geometrical Lemmas, and in Section 3, we shall complete the proofs of Theorems 1 and 2. We thank Professor M. Ohta for valuable discussions and the referee for useful comments.

1. Main results

We fix a prime number p once and for all throughout this paper. An elliptic curve defined over a field of characteristic p is called supersingular, if it has no p -torsion (étale) point. We fix a supersingular elliptic curve E defined over the prime field F_p such that $\pi^2 = -p \cdot \text{id}_E$, where π is the Frobenius endomorphism of E over F_p . (The existence of such E is due to Deuring [2]. Incidentally, the last condition is automatically satisfied when $p \geq 5$.) Then, if A is a product of (various) supersingular elliptic curves, and if $\dim A = n \geq 2$, then A is isomorphic to E^n (Shioda, Deligne and Ogus). Hereafter, we assume always that $n \geq 2$ and put $A = E^n$ (where E is fixed as above.) For any abelian variety A_1 , we shall say that an algebraic equivalence class Θ of divisors of A_1 is a principal polarization, if Θ is represented by an effective divisor D such that the n -fold intersection number $(D^n) = n!$. We shall say that two principally polarized abelian varieties (A_1, Θ_1) and (A_2, Θ_2) are isomorphic with each other, when there exists an isomorphism f of A_1 to A_2 (as abelian varieties) such that $f^*(\Theta_2) = \Theta_1$. Denote by $\mathcal{O} = \text{End}(E)$ the endomorphism ring of E as an abelian variety and put $B = \text{End}(E) \otimes Q$. Then, it is well known that B is the (unique) definite quaternion algebra over Q with discriminant p , and \mathcal{O} is a maximal order of B which contains an element π with $\pi^2 = -p$, where the isomorphism class of \mathcal{O} depends on the choice of E .

Now, we review on some definitions on quaternion hermitian lattices according to Shimura [14] and also on some results in [10]. We regard B^n as a left B -vector space. Every positive definite quaternion hermitian metric on B^n is equivalent to the following ϕ up to base change:

$$\phi(x, y) = \sum_{i=1}^n x_i \bar{y}_i \text{ for } x = {}^t(x_1, \dots, x_n), y = {}^t(y_1, \dots, y_n) \in B^n.$$

Then by definition, the group G of similitudes of (B^n, ϕ) is given by:

$$G = \{g \in M_n(B); g^t \bar{g} = n(g)1_n, n(g) \in Q^\times \}$$

where $n(g)$ is a positive rational number depending on g , and for $g = (g_{ij})$, we put $\bar{g} = (\bar{g}_{ij})$, \bar{g}_{ij} being the image of g_{ij} under the main involution of B . We denote by $G_{\mathcal{A}}$ the adelization of G and for any place v of Q , we denote by G_v

the v -component of $G_{\mathcal{L}}$. We also put $B_p = B \otimes \mathbf{Q}_p$ and $\mathcal{O}_p = \mathcal{O} \otimes \mathbf{Z}_p$. A \mathbf{Z} -submodule L of B^n is called a left \mathcal{O} -lattice, when it is a \mathbf{Z} -lattice and a left \mathcal{O} -module. We denote by \mathcal{L} the set of all left \mathcal{O} -lattices L such that, for every prime p , $L \otimes \mathbf{Z}_p = \mathcal{O}_p^n g_p$ for some element $g_p \in G_p$. According to Shimura (loc. cit.), we call this set \mathcal{L} the principal genus of B^n . The natural right action of G on \mathcal{L} is defined by: $\mathcal{L} \ni L \rightarrow Lg \in \mathcal{L}$, and each G -orbit in \mathcal{L} is called a class. The number of classes in \mathcal{L} is finite and called the class number of \mathcal{L} .

Now, we review on relations between these classes and principal polarizations on A (cf. [10]). Denote by X the divisor of A defined by $X = 0 \times E^{n-1} + E \times 0 \times E^{n-2} + \dots + E^{n-1} \times 0$. This divisor defines a principal polarization on A . For any divisor D of A , we denote by ϕ_D the morphism of A to $\text{Pic}^0(A)$ defined by: $\phi_D(t) = Cl(D_t - D)$ for any $t \in A$, where D_t is the translation of D by t , and Cl denotes the linear equivalence class. This ϕ_D depends only on the algebraic equivalence class of D , and we may write $\phi_D = \phi_\Theta$, where Θ is the algebraic equivalence class to which D belongs. Now, the mapping $\Theta \rightarrow \phi_{\bar{x}}^{-1} \phi_\Theta$ of the Néron-Severi group $NS(A)$ to $\text{End}(A)$ induces a bijection of principal polarizations of A onto positive definite quaternion hermitian matrices in $M_n(\mathcal{O})$ with Hauptnorm 1, where we identify $\text{End}(A)$ with $M_n(\mathcal{O})$. Here, we say that a matrix $K \in M_n(B)$ is quaternion hermitian if ${}^t \bar{K} = K$, and positive definite, if ${}^t \bar{x} K x \geq 0$ for any $x \in B^n$ and > 0 unless $x = 0$. For any positive definite quaternion hermitian matrix $K \in M_n(B)$, there exists $g \in GL_n(B)$ such that $K = g {}^t \bar{g}$. If the Hauptnorm of K is one, then the lattice $L = \mathcal{O}^n g$ belongs to \mathcal{L} for any g as above, and the class of L depends only on K and not on the choice of g . So, we get a mapping of the set of all principally polarized abelian varieties (A, Θ) to the classes $L(\Theta)$ in \mathcal{L} . This induces the bijection of the set of all isomorphism classes of principally polarized abelian varieties to the classes in \mathcal{L} . For any principally polarized abelian variety (A, Θ) , we fix a representative of the lattice class $L(\Theta) \in \mathcal{L}$, and denote it also by $L(\Theta)$. For any left \mathcal{O} -lattice L in \mathcal{L} , we denote by R_L the right order of L :

$$R_L = \{x \in M_n(B); Lx \subset L\}.$$

We denote by P_L the unique two-sided R_L -(prime)ideal in R_L on p , that is, P_L is the two sided ideal such that reduced norm of $P_L = p^n$. We also denote by P'_L the set of generators of P_L : $P'_L = \{\gamma \in P_L; \gamma R_L = P_L\}$.

THEOREM 1. *Let A be as above and assume that $\dim A \geq 2$. Then, any principally polarized abelian variety (A, Θ) is \mathbf{F}_p -rational. Besides, there exists a principally polarized abelian variety (A_0, Θ_0) defined over \mathbf{F}_p which is isomorphic to (A, Θ) over $\bar{\mathbf{F}}_p$, if and only if*

$$P'_{L(\Theta)} \cap G \neq \emptyset.$$

REMARK 1. Let k be a perfect field. Assume that C is a (not necessarily irreducible) algebraic curve such that the Jacobian variety $J(C)$ is isomorphic over the algebraic closure \bar{k} of k to a principally polarized abelian variety (A_1, Θ) defined over a field k . Then, by the Torelli Theorem, it is clear that C has also a model defined over k (Serre [13]). In particular, if C is a curve such that $J(C) \cong E^n$, then C has a model defined over F_{p^2} .

To count the numbers of principal polarizations defined over F_p , we need some more definitions. We denote by \mathcal{R} the set of maximal orders of $M_n(B)$ defined by:

$$\mathcal{R} = \{R \subset M_n(B); R = g^{-1}M_n(\mathcal{O})g \text{ for some } g \in G_{\mathcal{L}}\},$$

where $g^{-1}M_n(\mathcal{O})g = \bigcap_{v < \infty} (g_v^{-1}M_n(\mathcal{O}_v)g_v \cap M_n(B))$ and for each prime v , g_v is the v -component of g . We define an equivalence relation of \mathcal{R} by: $R_1 \sim R_2$ if and only if $R_1 = g^{-1}R_2g$ for some $g \in G$. As in [7], we call the number of the above equivalence classes in \mathcal{R} the type number of G (or of \mathcal{L}) and denote it by T . When $n = 1$, this is the classical type number of the algebra B , that is, the number of isomorphism classes of maximal orders of B . Now, we shall define a Hecke operator $R(\pi)$ acting on automorphic forms on $G_{\mathcal{L}}$ of weight 0. For that purpose, first we review on automorphic forms. For each prime q , we denote by U_q the subgroup of G_q defined by $U_q = GL_n(\mathcal{O}_q) \cap G_q$, where $GL_n(\mathcal{O}_q)$ is the group of invertible elements of $M_n(\mathcal{O}_q)$, and we also define a subgroup U of $G_{\mathcal{L}}$ by: $U = G_{\infty} \times \prod_{v > \infty} U_v$. A \mathbf{C} -valued function f on $G_{\mathcal{L}}$ is called automorphic form of weight 0 with respect to U , when it satisfies $f(uga) = f(g)$ for every $u \in U$, $g \in G_{\mathcal{L}}$, and $a \in G$. We denote by $M_0(U)$ the set of all automorphic forms of weight 0 with respect to U . This is an H -dimensional \mathbf{C} -linear vector space, where we denote by H the class number of \mathcal{L} . For any U -double coset UhU in $G_{\mathcal{L}}$, we define the action of UgU on $M_0(U)$ as follows: take the left U -coset decomposition of UhU as follows:

$$UhU = \prod_{i=1}^d Uh_i. \quad (\text{disjoint.})$$

For any $f \in M_0(U)$, we write

$$(f|[UhU])(g) = \sum_{i=1}^d f(h_i g)$$

This defines a linear endomorphism of $M_0(U)$. We define a special U -double coset $U(\pi)$ by: $U(\pi) = G_{\infty} \times \pi U_p \times \prod_{q \neq p, \infty} U_q$. We denote by $T(1)$, or $R(\pi)$ the linear endomorphism on $M_0(U)$ defined by the U -double coset U , or $U(\pi)$, respectively.

THEOREM 2. *Notations being as above, the number of isomorphism classes of principally polarized abelian varieties (A, Θ) which have models over \mathbf{F}_p is equal to*

$$\text{tr}(R(\pi)) = 2T - H,$$

and the number of those which are defined over \mathbf{F}_{p^2} but do not have models over \mathbf{F}_p is equal to

$$\text{tr}(T(1)) - \text{tr}(R(\pi)) = 2H - 2T.$$

REMARK 2. In the above Theorem 2, polarizations Θ might be decomposable. Of course, it is easy to get a formula for the number of indecomposable ones, subtracting decomposable ones (which consist of the products of polarizations in E^m ($m \leq n$)). We omit the details here. As for the case $n = 2$, see below.

REMARK 3. When $\dim A = 2$, the class number H was explicitly calculated in Hashimoto and Ibukiyama [7]. On the other hand, the type number T is equal to the class number of some quinary quadratic forms, as was shown in [7]. Hence, using the class number formula in Asai [1], we can calculate $\text{tr}(R(\pi))$ explicitly. The result is as follows: If $p = 2, 3$, or 5 , then $\text{tr}(R(\pi)) = 1, 1$, or 2 , respectively. As for primes $p \geq 7$, when $p \equiv 3 \pmod{4}$, we get

$$\begin{aligned} \text{tr}(R(\pi)) &= \frac{1}{2^5 \cdot 3} B_{2,x} + \frac{1}{8} h(\sqrt{-2p}) + \frac{1}{12} h(\sqrt{-3p}) \\ &\quad + \left\{ \frac{1}{48} (p-1) \left(9 - 4 \left(\frac{2}{p} \right) \right) + \frac{1}{16} \left(p - \left(\frac{2}{p} \right) \right) \right. \\ &\quad \left. + \frac{1}{12} \left(1 - \left(\frac{p}{3} \right) \right) \left(3 - \left(\frac{2}{p} \right) \right) \right\} h(\sqrt{-p}) \end{aligned}$$

and when $p \equiv 1 \pmod{4}$, then

$$\begin{aligned} \text{tr}(R(\pi)) &= \frac{1}{2^5 \cdot 3} (9 - 2\chi(2)) B_{2,x} + \frac{4p-1}{48} h(\sqrt{-p}) + \frac{1}{8} h(\sqrt{-2p}) \\ &\quad + \frac{1}{12} \left(3 + \left(\frac{-2}{p} \right) \right) h(\sqrt{-3p}) + \frac{1}{12} \left(1 - \left(\frac{p}{3} \right) \right) h(\sqrt{-p}), \end{aligned}$$

where χ is the Dirichlet character which corresponds to the real quadratic field $Q(\sqrt{p})$, $B_{2,x}$ is the second generalized Bernoulli number, $h(-D)$ is the class number of the imaginary quadratic field $Q(\sqrt{-D})$, and $(*/*)$ is the Legendre

symbol. It is obvious that the number of isomorphism classes of decomposable polarizations Θ such that (E^2, Θ) has a model over \mathbb{F}_p is given by $(h + h^2)/2$, where h is the number of isomorphism classes of supersingular elliptic curves, and h' is the number of those defined over \mathbb{F}_p . The explicit values of h and h' are known by Eichler [4] and Deuring [3], [2], and given by:

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

and

$$h' = \begin{cases} \frac{1}{2}h(\sqrt{-p}) & \text{if } p \equiv 1 \pmod{4}, \\ h(\sqrt{-p}) & \text{if } p \equiv 7 \pmod{8}, \\ 2 \cdot h(\sqrt{-p}) & \text{if } p \equiv 3 \pmod{8} \text{ and } p \neq 3. \end{cases}$$

So, we can calculate the number of irreducible curves such that the Jacobian variety $J(C) \cong E^2$ and that C has a model over \mathbb{F}_p . Numerical examples of such numbers (denoted by $\#(C/\mathbb{F}_p)$ below) will be given in the following table.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
H	1	1	2	2	5	4	8	10	16	24	26	37	50	55	72	93
$2T - H$	1	1	2	2	5	4	8	8	14	18	18	11	32	19	44	33
h	1	1	1	1	2	1	2	2	3	3	3	3	4	4	5	5
h'	1	1	1	1	2	1	2	2	3	3	3	1	4	2	5	3
$\#(C/\mathbb{F}_p)$	0	0	1	1	2	3	5	5	8	12	12	9	22	15	29	26

2. Geometric lemmas

First, we shall introduce several notations and then we shall give two Lemmas which are obtained by algebro-geometrical method.

2.1. Preliminaries

We denote by σ the Frobenius automorphism of the algebraic closure $\bar{\mathbb{F}}_p$ of \mathbb{F}_p : $x^\sigma = x^p$ for any $x \in \bar{\mathbb{F}}_p$. For any variety V defined over $\bar{\mathbb{F}}_p$ and any $\tau \in \text{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, denote by V^τ so called “transform of V under τ ”. That is, the fibre product of $V \rightarrow \text{Spec}(\bar{\mathbb{F}}_p)$ and $\text{Spec}(\bar{\mathbb{F}}_p) \xrightarrow{\tau} \text{Spec}(\bar{\mathbb{F}}_p)$ over $\text{Spec}(\bar{\mathbb{F}}_p)$.

We also denote by F the Frobenius endomorphism of A over \mathbb{F}_p . It is easy to see that, for any divisor D of A defined over $\bar{\mathbb{F}}_p$, we get

$$F^*(D^\sigma) = pD.$$

The following Lemma 2.1 seems more or less known to the experts. The short proof below of this lemma was suggested by the referee. (Our original proof was somewhat longer.)

LEMMA 2.1. *Let Θ be a principal polarization of A . Then, Θ is defined over \mathbb{F}_{p^2} , and the polarization Θ contains an effective divisor D_0 of A rational over \mathbb{F}_{p^2} .*

Proof. The set of line bundles giving rise to a fixed polarization forms a principal homogeneous space over the Picard variety $\text{Pic}^0(A)$. Since the \mathbb{F}_{p^2} -Frobenius is $-p \text{id}_A$, this is defined over \mathbb{F}_{p^2} , and by Lang's theorem, the set of \mathbb{F}_{p^2} -rational points is non empty. In the case of Θ , there is a unique effective divisor in its linear system and hence it is also defined over \mathbb{F}_{p^2} . \square

LEMMA 2.2. *Let Θ be a principal polarization of A . Then, there exists a principally polarized abelian variety (A_0, Θ_0) defined over \mathbb{F}_p and isomorphic to (A, Θ) , if and only if there exists an automorphism ε of A (as an abelian variety) such that*

$$\varepsilon(D) \approx D^\sigma$$

for some divisor D in Θ defined over $\bar{\mathbb{F}}_p$.

Proof. The only "if" part is obvious. In fact, denote by f an isomorphism of (A_0, Θ_0) to (A, Θ) , and by D_0 a divisor in Θ_0 rational over \mathbb{F}_p . Define a divisor in Θ by $D = f(D_0)$. Then, we get $f^\sigma f^{-1}(D) = f^\sigma(D_0) = f(D_0)^\sigma = D^\sigma$, and the automorphism $\varepsilon = f^\sigma f^{-1}$ of A satisfies the desired property. Next, we shall show the "if" part. By the condition on D , we get $\varepsilon(D) \sim D_t^\sigma$ for some $\bar{\mathbb{F}}_p$ -rational point $t \in A$. Since D represents a principal polarization, we get $\varepsilon(D) = D_t^\sigma$. As $F - \varepsilon$ is obviously an isogeny, we get $t = s^\sigma - \varepsilon(s)$ for some $\bar{\mathbb{F}}_p$ -rational point $s \in A$. Hence, if we put $D_1 = D_s$, we get $\varepsilon(D_1) = D_1^\sigma$, and $\varepsilon^\sigma \varepsilon(D_1) = D_1^{\sigma^2}$. Now, assume that D_1 is defined over $\mathbb{F}_{p^{2m}}$. As is well known, every element of $\text{End}(A)$ is defined over \mathbb{F}_{p^2} , and so, we get

$$D_1 = (\varepsilon^\sigma \varepsilon)^m(D_1).$$

Hence, the automorphism $(\varepsilon^\sigma \cdot \varepsilon)^m$ of A fixes the principal polarization Θ and hence a torsion element. We denote by l the order of $\varepsilon^\sigma \cdot \varepsilon$. Now, put $f_\sigma = \varepsilon$. For each integer i with $1 \leq i \leq 2l$, we also define an automorphism f_{σ^i} of A by:

$$f_{\sigma^i} = f_\sigma^{\sigma^{i-1}} \cdot f_\sigma^{\sigma^{i-2}} \cdots f_\sigma^\sigma \cdot f_\sigma.$$

Then, $f_{\sigma^{2l}}$ is the identity id_A , and the set $\{f_{\sigma^i}; 1 \leq i \leq 2l\}$ defines a 1-cocycle. Hence by Weil's criterion, there exists an abelian variety A_0 defined over \mathbb{F}_p and an isomorphism f of A_0 onto A such that $f_\sigma = f^\sigma f^{-1}$. Define a divisor

D_0 of A_0 by: $D_0 = f^{-1}(D_1)$. Then, we get

$$\begin{aligned} D_0^\sigma &= (f^{-1})^\sigma(D_1^\sigma) \\ &= f^{-1}\varepsilon^{-1}(D_1^\sigma) = f^{-1}(D_1) = D_0. \end{aligned}$$

Hence, D_0 is rational over \mathbf{F}_p . □

3. Proofs of Theorems 1 and 2

3.1 The first part of Theorem 1 has already been proved in Lemma 2.1. Now, we prove the second part. Let (A, Θ) be as in Theorem 1. Assume that (A, Θ) has a model defined over \mathbf{F}_p . Then, by Lemma 2.2, we get $\varepsilon(D) \approx D^\sigma$ for $\varepsilon \in \text{Aut}(A)$ and a divisor $D \in \Theta$. Hence, $F^*\varepsilon(D) \approx F^*(D^\sigma) = pD$. We get $\phi_{F^*\varepsilon(D)} = \varepsilon^{-1}F\phi_D\varepsilon^{-1}F$, where for any element $\eta \in \text{End}(A)$, we denote by $\hat{\eta}$ the dual endomorphism of the dual abelian variety \hat{A} of A . Hence, $p\phi_{\bar{x}}^{-1}\phi_D = (\varepsilon^{-1}F)^*\phi_{\bar{x}}^{-1}\phi_D(\varepsilon^{-1}F)$, where $*$ is the standard involution of $M_n(B)$ defined by $h^* = {}^t\bar{h}$. Now, take $g \in GL_n(B)$ such that $gg^* = \phi_{\bar{x}}^{-1}\phi_D$, and put $L = \mathcal{O}^n g$. If we put $\gamma = g^{-1}(\varepsilon^{-1}F)^*g$, then $\gamma\gamma^* = p1_n$, hence $\gamma \in G$, and $L\gamma \subset L$. Besides, $\gamma R_L = g^{-1}\pi M_n(\mathcal{O})g$ is the unique two-sided ideal of R_L on p . Hence, the condition is necessary. Conversely, if there exists $\gamma \in G \cap P_{L(\Theta)}$, then taking g as before, we get $\gamma = g^{-1}\varepsilon^{-1}Fg$ for some $\varepsilon \in GL_n(\mathcal{O}) \cong \text{Aut}(A)$. Comparing the reduced norm of both sides, we get $\gamma\gamma^* = p1_n$. Hence, we get $pgg^* = (\varepsilon^{-1}F)^*gg^*(\varepsilon^{-1}F)$, and $\phi_{pD}(x) = \phi_{F^*\varepsilon(D)}$. This means that we get $F^*\varepsilon(D) \approx F^*(D^\sigma)$ for some $\varepsilon \in \text{Aut}(A)$. As F is an isogeny, we get $\varepsilon(D) \approx D^\sigma$. Hence, Theorem 1 was proved.

3.2 Next, we shall prove Theorem 2. First, we shall show that the number of isomorphism classes which have a model over \mathbf{F}_p is equal to $\text{tr}(R(\pi))$. For that purpose, we review on classical interpretation of the Hecke operators on $M_0(U)$ (cf. Hashimoto [6]). We decompose $G_{\mathcal{A}}$ into the disjoint union as follows:

$$G_{\mathcal{A}} = \prod_{i=1}^H U g_i G.$$

For each i with $1 \leq i \leq H$, denote by e_i the function on $G_{\mathcal{A}}$ defined by:

$$e_i(g) = \begin{cases} 1, \dots, & \text{if } g \in U g_i G, \\ 0, \dots, & \text{otherwise.} \end{cases}$$

Then, each $e_i \in M_0(U)$ and the elements e_1, \dots, e_H form a basis of $M_0(U)$. Now, we shall write down the $H \times H$ -representation matrix (c_{ij}) ($1 \leq i, j \leq H$) of

$R(\pi)$ with respect to this basis. For each i with $1 \leq i \leq H$, define a left O -lattice L_i in \mathcal{L} and a finite subgroup Γ_i of G by:

$$L_i = \mathcal{O}^n g_i = \bigcap_{v < \infty} (B^n \cap \mathcal{O}_v^n g_{i,v}) \text{ and } \Gamma_i = G \cap g_i^{-1} U g_i,$$

where $g_{i,v}$ is the v -component of g_i . If we denote by R_{L_i} the right order of L_i (in $M_n(B)$), then $\Gamma_i = R_{L_i}^\times \cap G$. Now, for each i, j with $1 \leq i, j \leq H$, the coefficients c_{ij} of the representation matrix of $R(\pi)$ are given by:

$$c_{ij} = \#(\Gamma_i \backslash (g_i^{-1} U(\pi) g_j \cap G)).$$

where $U(\pi)$ is as in Section 1 (cf. Hashimoto loc.cit.).

As $\pi U_p = U_p \pi$, we get $c_{ij} = 0$, or 1. More precisely, it is very easy to see that, for a fixed i , there exists the unique j such that $c_{ij} = 1$ and that $c_{ik} = 0$ for any other $k \neq j$. Besides, we get $c_{ij} = c_{ji}$, since $\pi^{-1} = -\pi$ and $(g_i^{-1} U(\pi) g_j \cap G)^{-1} = (g_j^{-1} U(\pi) g_i \cap G)$. In any way, we get $c_{ii} = 1$, if and only if $P_{L_i} \cap G \neq \emptyset$. Hence, by Theorem 1, the number of isomorphism classes of principally polarized abelian variety (A, Θ) which has a model defined over F_p is equal to $\sum_{i=1}^H c_{ii} = \text{tr}(R(\pi))$. Next, we shall see that $\text{tr}(R(\pi)) = 2T - H$. When $n = 2$, this relation was announced in Hashimoto-Ibukiyama [7] Proposition 24 (in a slightly more general case). As the proof was omitted there, we shall give here the proof for general n for readers' convenience. Assume that $g^{-1} g_i^{-1} M_n(\mathcal{O}) g_i g = g_j^{-1} M_n(\mathcal{O}) g_j$ for some i, j with $1 \leq i, j \leq H$, $i \neq j$, and $g \in G$. Then, $M_n(\mathcal{O}_A) g_i g g_j^{-1}$ is the two sided ideal of $M_n(\mathcal{O}_A)$. But, for any finite prime $q \neq p$, any two sided ideal of $M_n(\mathcal{O}_p)$ is equal to $q^a M_n(\mathcal{O}_q)$ for some $a \in \mathbb{Z}$, and any two sided ideal of $M_n(\mathcal{O}_p)$ is equal to $\pi^b M_n(\mathcal{O}_p)$ for some $b \in \mathbb{Z}$. Hence, multiplying g by an element of Q^\times , we can assume that $g_i g g_j^{-1} \in U$, or $U(\pi)$. As $i \neq j$, the former case cannot occur, because each g_i or g_j belongs to a mutually different U - G -double coset. Hence, we get $c_{ij} = c_{ji} = 1$ and $c_{ik} = c_{ki} = 0$ for any $k \neq j$. Hence, for a fixed i , if $c_{ii} = 1$, there exists no j such that R_{L_i} is G -conjugate to R_{L_j} , and if $c_{ii} = 0$, then there exists unique j such that R_{L_i} is G -conjugate to R_{L_j} . Hence, $T = \text{tr} R(\pi) + (H - \text{tr}(R(\pi)))/2$, and we get $\text{tr}(R(\pi)) = 2T - H$. Thus, we proved Theorem 2. □

References

1. Asai, T., The class number of positive definite quadratic forms, *Japanese J. Math.*, 3 (1977) 239–296.
2. Deuring, M., Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primem Grundzahl, *Jahresberich Deutschen Math.*, 54 (1951) 24–41.
3. Deuring, M., Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Univ. Hamburg*, 14 (1941) 197–272.

4. Eichler, M., Über die Idealklassenzahl total definiten quaternionen algebren, *Math. Z.*, 43 (1938) 102–109.
5. Hartshorne, R., *Algebraic Geometry*, Springer, New York, Berlin, Heidelberg, 1977.
6. Hashimoto, K., On Brandt matrices associated with the positive definite quaternion hermitian forms, *J. Fac. Sci. Univ. Tokyo Sect. IA*, 27 (1980) 227–245.
7. Hashimoto, K. and Ibukiyama, T., On class numbers of positive definite binary quaternion hermitian forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, 27 (1980) 549–601.
8. Ibukiyama, T., On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, pp. 301–349, *Advanced Studies in Pure Math. Vol. 15*, Kinokuniya, Tokyo, 1989.
9. Ibukiyama, T., On rational points of curves of genus three over finite fields, to appear in *Tohoku Math. J.*
10. Ibukiyama, T., Katsura, T. and Oort, F., Supersingular curves of genus two and class numbers, *Compositio Math.*, 57 (1986) 127–152.
11. Katsura, T. and Oort, F., Families of supersingular abelian surfaces, *Compositio Math.*, 62 (1987) 107–167.
12. Mumford, D., *Abelian Varieties*, Oxford University Press, 1970.
13. Serre, J.-P., A letter to Hashimoto and Ibukiyama, 1984.
14. Shimura, G., Arithmetic of alternating forms and quaternion hermitian forms, *J. Math. Soc. Japan*, 15 (1963) 33–65.
15. Shimura, G. and Taniyama, Y., *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*, Publ. Math. Soc. Japan 6, 1961.