RIMS Kôkyûroku Bessatsu
B90 (2022), 17–37

Supersingular abelian varieties and quaternion hermitian lattices

By

Tomoyoshi Ibukiyama*

Abstract

This note gives a survey on relations between the theory of quaternion hermitian lattices and that of supersingular abelian varieties, including relations between polarizations, moduli loci, automorphism groups, curves with many rational points, and class numbers, type numbers, lattice automorphisms, algebraic modular forms. For readers' convenience, we give some explicit formulas for related numbers and give a slightly big list of related references. The last section is an announcement of new results on supersingular loci of low dimensions.

§ 1. A review on supersingular elliptic curves

First we review classical results on supersingular elliptic curves due to Deuring and Eichler. In this article, we fix a prime number p and we always mean by k an algebraically closed field of characteristic p. An elliptic curve E is said to be supersingular, if E has no p-torsion point, or equivalently if $D = End(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is the quaternion algebra over $\mathbb{Q}$ such that $D_\infty = D \otimes_{\mathbb{Q}} \mathbb{R}$ and $D_p = D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ are division and $D_q = D \otimes_{\mathbb{Q}} \mathbb{Q}_q \cong M_2(\mathbb{Q}_q)$ for any prime $q \neq p$. Here $\mathbb{Q}_q$ is the field of q-adic numbers and $M_2(\mathbb{Q}_q)$ is the 2×2 matrix algebra over $\mathbb{Q}_q$. For any supersingular E, it is known that $End(E)$ is a maximal order of D. This fact is proved first in [3] and also proved in [42] by other methods, but the proof is seldom given in any other popular books on elliptic curves as far as the author knows. The algebra D has finitely many non-isomorphic (equivalently, non-conjugate) maximal orders, but in general, maximal orders are not unique even up to conjugation. The number of non-isomorphic maximal

Received December 25, 2020. Revised March 26, 2021.
2020 Mathematics Subject Classification(s): 11E41, 11F72, 11F46, 14K15
Key Words: *supersingular abelian variety, quaternion hermitian lattice*
Supported by JSPS Kakenhi JP19K03424

*Department of Math. Graduate School of Science, Osaka University, Machikaneyama 1-1, 560-0043 Japan.
e-mail: `ibukiyam@math.sci.osaka-u.ac.jp`

orders of D is called the type number $T(p)$ of D. We fix a supersingular elliptic curve E and put $End(E) = O$. A left O module L in D is called a left O ideal if $L \otimes_{\mathbb{Z}} \mathbb{Q} = D$ and there exists $0 \neq a \in \mathbb{Q}$ such that $aL \subset O$. Two left O ideals L_1 and L_2 are said to be equivalent if $L_1 = L_2\alpha$ for some $\alpha \in D^{\times}$. The number of inequivalent left O ideals is finite and called the class number $H(p)$ of D. This does not depend on a choice of O or E. We always have $T(p) \leq H(p) \leq 2T(p)$.

We say that E has a model over $\mathbb{F}_p$ if there exists an elliptic curve E_1 defined over $\mathbb{F}_p$ such that $E \cong E_1$ over k.

Theorem 1.1 (Deuring [3]). *(1) Supersingular elliptic curves are all isogenous over k. The number of isomorphism classes of supersingular elliptic curves over k is equal to the class number $H(p)$.*
(2) A supersingular elliptic curve E always has a model over $\mathbb{F}_{p^2}$. It has a model over $\mathbb{F}_p$ if and only if $End(E)$ has a two sided principal ideal (π) with $\pi^2 = -p$. The number of isomorphism classes of E that has a model over $\mathbb{F}_p$ is equal to $2T(p) - H(p)$.

By (2), when E has a model over $\mathbb{F}_p$, the maximal order $End(E)$ contains an element π with $\pi^2 = -p$. Such maximal orders are not unique in general, but can be all explicitly written down (see [14]). The following orders exhaust all such maximal orders.

We take a prime q such that $q \equiv 3 \bmod 8$ and that

$$\left(\frac{-q}{p}\right) = -1 \qquad (\text{ or equivalently } \left(\frac{-p}{q}\right) = 1.\ )$$

We assume that α, β satisfies $\alpha^2 = -p$, $\beta^2 = -q$, and $\alpha\beta = -\beta\alpha$. Then by an easy application of the class field theory, we have

$$D = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta.$$

We take an integer r such that $r^2 + p \equiv 0 \bmod q$. We define

$$O(q,r) = \mathbb{Z} + \mathbb{Z}\frac{1+\beta}{2} + \mathbb{Z}\frac{\alpha(1+\beta)}{2} + \mathbb{Z}\frac{(r+\alpha)\beta}{q}.$$

If $p \equiv 3 \bmod 4$ besides, then by taking r' such that $r'^2 + p \equiv 0 \bmod 4q$, we define another module $O'(q,r')$ by

$$O'(q,r') = \mathbb{Z} + \mathbb{Z}\frac{1+\alpha}{2} + \mathbb{Z}\beta + \mathbb{Z}\frac{(r'+\alpha)\beta}{2q}.$$

Then $O(q,r)$ and $O'(q,r')$ are maximal orders. The essential point of the proof of this fact is to show that these are rings and the discriminant is p^2. Isomorphism classes of $O(q,r)$ and $O'(q,r')$ do not depend on the choice of r, r' but depend on q, so we write them by $O(q)$ and $O'(q)$ for fixed r and r'. Then we have $O(q) \cong O(q')$ if and only if $x^2 + py^2 = 4qq'$ for some $x, y \in \mathbb{Z}$, and $O'(q) \cong O'(q')$ if and only if $x^2 + 4py^2 = qq'$ for some $x, y \in \mathbb{Z}$. By the way, $O(q) \cong O'(q')$ for some q and q' if and only if $O(q)^\times \cong O'(q)^\times = \{\pm 1, \pm\sqrt{-1}\}$. Such maximal order whose unit group is of order 4 is known to be unique. For more ideal theoretic description, see [14].

Theorem 1.2 (Eichler [5], Deuring [4]). *(1) We have*

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

where $(-1/p) = -1$ *if* $p \equiv 3 \bmod 4$, $(-1/p) = 1$ *if* $p \equiv 1 \bmod 4$, $(-1/2) = 0$, *and* $(-3/p) = 1$ *if* $p \equiv 1 \bmod 3$, $(-3/p) = -1$ *if* $p \equiv 2 \bmod 3$ *and* $(-3/3) = 0$.
(2) We have

$$2T(p) - H(p) = \frac{1}{2}(h(-p) + h(-4p))$$

where $h(-d)$ *is the class number of positive definite primitive quadratic forms of discriminant* $-d$ *(or equivalently the class number of the quadratic order of discriminant* $-d$ *that might be non-maximal). In case* $-d \equiv 2$ *or* $3 \bmod 4$, *we put* $h(-d) = 0$.

§ 2. Supersingular abelian varieties

Products of more than two supersingular elliptic curves are all isomorphic over k, due to the results of Deligne, Ogus, Shioda. So we fix a supersingular elliptic curve E and consider E^n. Then of course we have

$$End(E^n) = M_n(O)$$

where $O = End(E)$. An abelian variety A of $\dim A = n$ is called superspecial if A is isomorphic to E^n and supersingular if A is isogenous to E^n. The class number of $M_n(O)$ is known to be 1 when $n \geq 2$ and the fact that superspecial abelian variety with $\dim A \geq 2$ is unique over k is a reflection of this fact. The fact that the class number of $M_n(O)$ is 1 for $n \geq 2$ is proved as follows. If we denote by $SL_n(D)$ the group of reduced norm 1, then the strong approximation theorem holds for $SL_n(D)$ for $n \geq 2$, that is, we have

$$SL_n(D_A) = SL_n(D)SL_n(D_\infty)\prod_q SL_n(O_q), \tag{2.1}$$

where D_A is the adelization of D, $O_q = O \otimes_{\mathbb{Z}} \mathbb{Z}_q$, and the group $SL_n(D)$ is embedded in $SL_n(D_A)$ diagonally. This property (2.1) does not hold in general when $n = 1$. The group $GL_n(D)$ does not satisfy the strong approximation property even for $n \geq 2$, but since we have

$$N(D_A^\times) = \mathbb{Q}_+^\times \mathbb{R}_+^\times \prod_q \mathbb{Z}_q^\times,$$

where $\mathbb{Q}_+^\times$ and $\mathbb{R}_+^\times$ are positive rational and real numbers respectively and N denotes the reduced norm, we also have

$$GL_n(D_A) = GL_n(D)GL_n(D_\infty) \prod_q GL_n(O_q)$$

for $n \geq 2$. This means that the class number of $M_n(O)$ is 1 for $n \geq 2$. (Note that if we take a smaller order than $M_n(O)$, the similar relation does not hold in general even for $n \geq 2$ and the class number might be bigger than 1. For $n = 1$, the class number of O is greater than 1 in general as the class number formula suggests.)

This class number one property for $n \geq 2$ gives another important fact. Let A be a supersingular abelian variety with $\dim A \geq 2$. Then by definition there exists an isogeny $\delta : E^n \to A$. Let assume that δ is an isogeny with minimal degree. Assume that $n \geq 2$. Then by the fact that $M_n(O)$ is of class number 1, we can show that any endomorphism ϕ of A has a pullback to $End(E^n)$. That is, for $\phi \in End(A)$, there exists an endomorphism $\psi \in End(E^n)$ such that $\phi \circ \delta = \delta \circ \psi$. This gives an injective homomorphism from $End(A)$ to $End(E^n)$, so the endomorphism ring of any supersingular abelian variety A can be regarded as a subring of $End(E^n) = M_n(O)$. Indeed, when $n = 2$, all the possible endomorphism is known (e.g. [29], [45]) and we can count the principal polarizations of A through this method ([27]).

For the sake of simplicity, hereafter we choose E such that E is defined over $\mathbb{F}_p$. For any effective divisor L of E^n, we define an isogeny ϕ_L of E^n to the dual $(E^n)^t$ by

$$\phi_L(t) = Cl(L_t - L) \in (E^n)^t,$$

where L_t is the translation of L by t and Cl means the linear equivalence class. If we define a divisor X of E^n by

$$X = E^{n-1} \times \{0\} + E \times \{0\} \times E^{n-2} + \cdots + \{0\} \times E^{n-1},$$

then ϕ_X is an isomorphism and defines a principal polarization. So we have $(E^n)^t \cong E^n$. For any element $\phi \in End(E^n)$, denote by ϕ^t the dual map from $(E^n)^t$ to E^n. Then $\phi \to \phi_X^{-1}\phi^t\phi_X$ is a positive involution of $M_n(D)$ and given for $\phi = g = (g_{ij})_{1 \leq i,j \leq n} \in M_n(O)$ by

$$g^* = {}^t(\overline{g_{ij}}) = (\overline{g_{ji}})$$

where $\overline{x}$ is the main involution of D. Here the main involution means the unique anti-automorphism of D such that $x + \overline{x} \in \mathbb{Q}$, $x\overline{x} \in \mathbb{Q}$. For any polarization $\lambda : E^n \to (E^n)^t$, we have $\phi_X^{-1}\lambda \in End(E^n)$. By this, we can identify the Neron-Severi group of E^n with the quaternion hermitian matrices $g^* = g \in M_n(O)$. The polarizations are identified with positive definite quaternion hermitian matrices in $M_n(O)$. So it is natural that quaternion hermitian matrices appear in the theory of supersingular abelian varieties.

§ 3. Quatnion hermitian matrices and lattices

For the rest of the paper, we assume that $n \geq 2$. A free finite submodule L over $\mathbb{Z}$ of D^n is called a lattice if $L \otimes_{\mathbb{Z}} \mathbb{Q} = D^n$. We fix a maximal order O of D that contains π such that $\pi^2 = -p$. A lattice of D^n that is a left O module is called a left O lattice. Because of the class number 1 property of $M_n(O)$ for $n \geq 2$, for any left O lattice, there exists $h \in GL_n(D) := M_n(D)^\times$ such that $L = O^n h$. Here h is not unique and we can change it by any element in $GL_n(O)h$ where $GL_n(O) := M_n(O)^\times$. For L, we define a quaternion hermitian matrix hh^*. We say that positive definite quaternion hermitian matrices H_1 and $H_2 \in M_n(D)$ are equivalent if $H_2 = \epsilon H_1 \epsilon^*$ for some $\epsilon \in GL_n(O)$. For any positive definite quaternion hermitian matrix H, there exists $h \in GL_n(D)$ such that $H = hh^*$ as in the usual linear algebra. This h is not unique, and if $h_1 h_1^* = h_2 h_2^*$, then we have $(h_1^{-1}h_2)(h_1^{-1}h_2)^* = 1_n$. So we define groups G^1 and G by

$$\begin{aligned} G &= \{g \in M_n(D); gg^* = n(g)1_n \text{ for some } n(g) \in \mathbb{Q}_+^\times\}, \\ G^1 &= \{g \in G; n(g) = 1\}. \end{aligned}$$

The group G is the group of all similitudes of quaternon hermitian metric defined by

$$(x, y) = \sum_{i=1}^{n} x_i \overline{y_i}, \quad x = (x_i), y = (y_i) \in D^n.$$

So for a quaternion hermitian matrix H, the right G^1-orbit of h such that $H = hh^*$ is unique. We say that two lattices L_1 and L_2 are equivalent if there exists $g \in G$ such that $L_2 = L_1 g$. If we write $L_2 = O^n h_2$ and $L_1 = O^n h_1$ and if we put $H_i = h_i h_i^*$, then the above equivalence is the same as $H_1 = m\epsilon H_2 \epsilon^*$ for some positive rational number m and $\epsilon \in GL_n(O)$. If $L_2 = L_1 g$ for $g \in G^1$, then we have $m = 1$. This also means that the reduced norms of H_1 and H_2 are the same. The equivalence by G and the equivalence by G^1 are not different so much in our cases, since $\{n(g) : g \in G\} = \mathbb{Q}_+^\times$ and $N(D^\times) = \mathbb{Q}_+^\times$. Arithmetically G is often better, so we use G equivalence in most cases, but often G^1 equivalence matches geometric properties.

We define the completions of G at ∞ and primes q by

$$\begin{aligned} G_\infty &= \{g \in M_n(D_\infty); gg^* = n(g)1_n \text{ for some } n(g) \in \mathbb{R}_+^\times\}, \\ G_q &= \{g \in M_n(D_q); gg^* = n(g)1_n \text{ for some } n(g) \in \mathbb{Q}_q^\times\}. \end{aligned}$$

We denote by G_A the adelization of G. By definition, an element $g = (g_v) \in G_A$ is an element in $\prod_v G_v$ such that $g_q \in GL_n(O_q)$ for almost all primes q.

For any left O lattie L in D^n and any prime q, we put $L_q = L \otimes_{\mathbb{Z}} \mathbb{Z}_q$. For any $g \in G_A$, we can define a left O lattice Lg of D^n by

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

We denote by $\mathcal{G}(L)$ the set of G_A orbits of L:

$$\mathcal{G}(L) = \{Lg; g \in G_A\}.$$

We say that $\mathcal{G}(L)$ is a genus. This is the set of left O lattices which are mutually equivalent by G_q at all q. The number of G equivalence classes in $\mathcal{G}(L)$ is finite and this number is called the class number of $\mathcal{G}(L)$. The class number is expressed by adelic double cosets as follows. We write

$$U(L_q) = \{g_q \in G_q; L_q g_q = L_q\}.$$

This is a compact subgroup of G_q. We put $U(L) = G_\infty \prod_q U(L_q)$. Then we obviously have the following bijection.

$$\mathcal{G}(L)/G \cong U(L)\backslash G_A/G.$$

So if we write

$$G_A = \bigcup_{i=1}^{h} U(L) g_i G \qquad (disjoint),$$

then $h = h(\mathcal{G}(L))$ is the class number of the genus $\mathcal{G}(L)$.

Next we define G-type numbers (or just type numbers if no confusion is likely). We fix a genus $\mathcal{G}(L)$ and fix a set of representatives $\{L_1, \ldots, L_h\}$ of classes in $\mathcal{G}(L)$. We define the right order of L_i by

$$R_i = \{g \in M_n(D); L_i g \in L_i\}.$$

When $n = 1$ and $\mathcal{G}$ consists of left O ideals, then the right orders are maximal orders and any maximal orders of O is realized as some right order. So the number of isomorphism classes of the right orders (i.e. $D^\times$ conjucacy classes) is just the usual type number that we have already defined. When $n \geq 2$, since we can write $L_i = O^n h_i$, we have $R_i = h_i^{-1} M_n(O) h_i$, so they are all $GL_n(D)$ conjugate and they are all maximal orders. Actually since the class number of $M_n(O)$ is 1 (for $n \geq 2$), maximal orders of $M_n(D)$ are all conjugate to $M_n(O)$. In this sense, the type number in the classical sense is always 1. But here we will define another nice number. We say that R_i and R_j are equivalent if there exists $g \in G$ such that $R_j = g^{-1}R_i g$. The number of inequivalent right orders in $\{R_i\}$ is called the G-type number and we denote it by $T(\mathcal{G})$. When $n = 1$, this definition is the same as the classical one. Naturally we have $T(\mathcal{G}) \leq H(\mathcal{G})$, but we can show that $H(\mathcal{G}) \leq 2T(\mathcal{G})$.

Next we explain some important genera. We define the norm $N(L)$ of a left O lattice L by the two sided O ideal spanned by xy^* for any $x, y \in L$. We note that for $g \in G$, we have $N(Lg) = n(g)N(L)$, so G-equivalence does not preserve the norms, but the norm is determined up to $\mathbb{Q}_+^\times$ multiplication. We say that a left O lattice L is maximal if any left O lattice M with $N(M) = N(L)$ and $L \subset M$ is equal to L. For our D^n, when $n \geq 2$, maximal lattices are divided into two genera. One is called the principal genus and it is the genus containing O^n. The another one is represented by a maximal lattice L such that $N(L) = O\pi$ where $\pi^2 = -p$. This genus has no standard name, but we often call this non-principal genus. (When the discriminant of the quatenrion algebra D is not a prime and given by $p_1 \cdots p_t$, then there are 2^t genera of maximal lattices, so the word "non-principal" is not so nice in that case, but for geometry, we treat only the case $t = 1$, so we have no problem.) We will denote these two genera by $\mathcal{G}_{princ}$ and $\mathcal{G}_{nonp}$ respectively. To make degree clearer, we denote by $H_n(\mathcal{G}_{princ})$ the class number of $\mathcal{G}_{princ}$ for the genus of lattices in D^n. We define $H_n(\mathcal{G}_{nonp})$, $T_n(\mathcal{G}_{princ})$, $T_n(\mathcal{G}_{nonp})$ similarly.

The non-principal genus is a bit complicated to describe. Locally at $q \neq p$, it is equivalent to O_q^n. At p, a representative of the corresponding hermitian matrix for $O_p^n h$ is written by

$$\begin{pmatrix} 0 & \pi 1_{n/2} \\ -\pi 1_{n/2} & 0 \end{pmatrix}$$

if n is even, and by

$$\begin{pmatrix} 0 & 0 & \pi 1_{\frac{n-1}{2}} \\ 0 & p & 0 \\ -\pi 1_{\frac{n-1}{2}} & 0 & 0 \end{pmatrix}$$

if n is odd. More abstractly, a quaternion hermitian matrix $H \in M_n(O)$ corresponds with lattices L with $N(L) = \pi O$ in the non-principal genus if and only if $H \in \pi M_n(O)$ and $Hm(H) = p^{\lceil n/2 \rceil}$, where $\lceil x \rceil$ is the minimum integer which is not less than x and Hm is the Haupt norm of quaternion hermitian matrices. The Haupt norm is the notion of the norm for Jordan algebras and in this case, it is a multiplicative polynomial function on quaternion hermitian matrices which takes value 1 for 1_n and $Hm(x)^2 = N(x)$, where $N(x)$ is the reduced norm.

Example. When $n = 2$, quaternon hermitian matrices associated with $\mathcal{G}_{princ}$ are represented by

$$\begin{pmatrix} t & r \\ \bar{r} & s \end{pmatrix}, \quad 0 < t, s \in \mathbb{Z}, r \in O, ts - N(r) = 1.$$

Those associated with $\mathcal{G}_{nonp}$ are represented by

$$\begin{pmatrix} pt & \pi r \\ \overline{\pi r} & ps \end{pmatrix}, \qquad 0 < t, s \in \mathbb{Z}, r \in O, pts - N(r) = 1.$$

§ 4. Some arithmetical results on supersingular ableian varieties

We denote by $\mathcal{S}_{n,1}$ the locus of principally polarized supersingular abelian varieties (A, λ) in the moduli $\mathcal{A}_{n,1}$ of principally polarized abelian varieties.

Theorem 4.1 ([29]). *The number of isomorphism classes over k of principal polarizations on E^n is equal to the class number $H_n(\mathcal{G}_{princ})$.*

For $x \in \mathbb{R}$, we denote by $\lfloor x \rfloor$ the maximum integer that does not exceed x.

Theorem 4.2 ([33], [37]).
(1) In general, the locus $\mathcal{S}_{n,1}$ is (connected but) not irreducible. Every irreducible component of $\mathcal{S}_{n,1}$ has dimension $\lfloor n^2/4 \rfloor$.
(2) The number of irreducible components of $\mathcal{S}_{n,1}$ is equal to the class number $H_n(\mathcal{G}_{princ})$ if n is odd and to $H_n(\mathcal{G}_{nonp})$ if n is even.

When $n = 2$, then any principal polarization of E^2 corresponds to either a sum of supersingular elliptic curves or an irreducible curve C of genus two such that the Jacobian $J(C)$ is isomorphic to a principally polarized superspecial abelian surface. The latter corresponds with an indecomposable lattice class in $\mathcal{G}_{princ}$. The number of decomposable lattices is equal to $h(h+1)/2$ where h is the class number of D. So the number of isomorphism classes of irreducible curves C of genus two such that $J(C) \cong E^2$ is $H(\mathcal{G}_{princ}) - h(h+1)/2$.

Next we consider the field of definition. We say that a polarized abelian variety (A, λ) has a model over $\mathbb{F}_p$ if there exists another polarized abelian variety (B, μ) such that B and μ are defined over $\mathbb{F}_p$ and $(A, \lambda) \cong (B, \mu)$ over k.

Theorem 4.3 ([21], [25]). *(1) Any principally polarized abelian varieties (E^n, λ) has a model over $\mathbb{F}_{p^2}$. The number of isomorphism classes of (E^n, λ) over k that have models over $\mathbb{F}_p$ is equal to $2T_n(\mathcal{G}_{princ}) - H_n(\mathcal{G}_{princ})$.*

(2) Any irreducible components of the locus $\mathcal{S}_{n,1}$ is defined over $\mathbb{F}_{p^2}$. The number of irreducible components that have models over $\mathbb{F}_p$ is equal to $2T_n(\mathcal{G}_{princ}) - H_n(\mathcal{G}_{princ})$ if n is odd, and to $2T_n(\mathcal{G}_{nonp}) - H_n(\mathcal{G}_{nonp})$ if n is even.

We note that for any genus $\mathcal{G}$, we have $2T(\mathcal{G})-H(\mathcal{G})=H(\mathcal{G})$ if and only if $T(\mathcal{G})=H(\mathcal{G})$. By comparing the main terms of the trace formulas, we see that $2T(\mathcal{G})-H(\mathcal{G})$ is much smaller than $H(\mathcal{G})$ for big p for usual $\mathcal{G}$, but often the difference is apt to be small (or there are no difference) for small p.

§ 5. Examples of the Class numbers and the type numbers

We give here explicit formulas for class numbers and type numbers for $n=2$. The formula for $H(\mathcal{G}_{princ})$ for $n=3$ is known by Hashimoto [9], but it seems that the formula for $H(\mathcal{G}_{nonp})$ for $n\geq 3$ has never been calculated (except possibly for sporadic small p).

Hereafter in this section, we assume that $n=2$. A reference of the class number formulas below are [10]. We write the class numbers of genera $\mathcal{G}_{princ}$ and $\mathcal{G}_{nonp}$ of maximal lattices by $H(p,1)=H_2(\mathcal{G}_{princ})$ and $H(1,p)=H_2(\mathcal{G}_{nonp})$, respectively. We also write type numbers by $T(p,1)=T_2(\mathcal{G}_{princ})$ and $T(1,p)=T_2(\mathcal{G}_{nonp})$.

Theorem 5.1 ([10]). *We have $H(p,1)=1$ for $p=2$, 3, and for $p\geq 5$, it is given by*

$$\begin{aligned}
H(p,1) = {} & \frac{(p-1)(p^2+1)}{2880}+\frac{7(p-1)^2}{576}+\frac{1}{48}(p-1)\left(1-\left(\frac{-1}{p}\right)\right)\\
&+\frac{1}{36}(p-1)\left(1-\left(\frac{-3}{p}\right)\right)+\frac{5(p-1)}{96}+\frac{1}{32}\left(1-\left(\frac{-1}{p}\right)\right)\\
&+\frac{1}{9}\left(1-\left(\frac{-3}{p}\right)\right)^2+\frac{1}{36}\left(1-\left(\frac{-3}{p}\right)\right)+\frac{(p-1)}{18}\\
&+\frac{1}{12}\left(1-\left(\frac{-1}{p}\right)\right)\left(1-\left(\frac{-3}{p}\right)\right)+\left\{\begin{array}{ll}1/5 & \textit{if}\ p=5\\ 4/5 & \textit{if}\ p\equiv 4 \bmod 5\\ 0 & \textit{otherwise}\end{array}\right\}\\
&+\left\{\begin{array}{ll}0 & \textit{if}\ p\equiv 1 \bmod 8\\ 1/4 & \textit{if}\ p\equiv 3,5 \bmod 8\\ 1/2 & \textit{if}\ p\equiv 7 \bmod 8\end{array}\right\}+\left\{\begin{array}{ll}0 & \textit{if}\ p\equiv 1 \bmod 6\\ 1/6 & \textit{if}\ p\equiv 5 \bmod 6\end{array}\right\}.
\end{aligned}$$

For $p=2$, 3, we have $H(1,p)=1$ and for $p\geq 5$, it is given by

$$
\begin{aligned}
H(1,p) &= \frac{p^2-1}{2880} + \frac{1}{2^3\cdot 3}\left(p - \left(\frac{-1}{p}\right)\right) + \frac{1}{2^5\cdot 3}\left(p\left(\frac{-1}{p}\right) - 1\right) \\
&\quad + \frac{1}{2^3\cdot 3}\left(p - \left(\frac{-3}{p}\right)\right) + \frac{1}{2^3\cdot 3^2}\left(p\left(\frac{-3}{p}\right) - 1\right) \\
&\quad + \frac{1}{5}\times\left\{\begin{matrix} 1 & \textit{if}\ p=5 \\ 2 & \textit{if}\ p\equiv 2,3 \bmod 5 \\ 0 & \textit{if}\ p\equiv \pm 1 \bmod 5 \end{matrix}\right\} + \frac{1}{2^2}\left\{\begin{matrix} 0 & \textit{if}\ p\equiv 1,7 \bmod 8 \\ 1 & \textit{if}\ p\equiv 3,5 \bmod 8 \end{matrix}\right\} \\
&\quad + \frac{1}{2^3\cdot 3}\left(1 - \left(\frac{3}{p}\right)\right) + \frac{1}{2^3\cdot 3}\left(\left(\frac{-1}{p}\right) - \left(\frac{-3}{p}\right)\right).
\end{aligned}
$$

A table is given as follows.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$H(p,1)$	1	1	2	2	5	4	8	10	16	24	26	37	50	55	72
$H(1,p)$	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4

To explain the type number formula, we use the following definition. For any Dirichlet character χ, we define the n-th generalized Bernoulli number by

$$\sum_{a=1}^{f_\chi} \frac{\chi(a)te^{at}}{e^{f_\chi t}-1} = \sum_{n=0}^{\infty} \frac{B_{n,\chi}}{n!}t^n.$$

where f_χ is the conductor of χ (see [1]). For example, more explicitly we have

$$B_{2,\chi} = \frac{1}{f_\chi}\sum_{a=1}^{f_\chi}\chi(a)a^2 - \sum_{a=1}^{f_\chi}\chi(a)a.$$

In the following theorem, we assume that χ is the Dirichlet character associated with the real quadratic field $\mathbb{Q}(\sqrt{p})$, so we have $\chi(-1)=1$ and hence $\sum_{a=1}^{f_\chi}\chi(a)a = 0$, so we can omit this part from the above formula for $B_{2,\chi}$. For any squarefree positive integer, we denote by $h(\sqrt{-d})$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$.

Theorem 5.2 ([21], [25], [26]). *(1) For $p = 2$, 3, 5, we have $T(p,1) = 1$, 1, 2 and $2T(p,1) - H(p,1) = 1$, 1, 2. When $p \equiv 1 \bmod 4$ and $p \geq 11$, we have*

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

For $p \equiv 3 \bmod 4$ and $p \geq 7$, we have

$$
\begin{aligned}
&2T(p,1) - H(p,1) = \\
&\frac{1}{2^5 \cdot 3} B_{2,\chi} + \frac{1}{8} h(\sqrt{-2p}) + \frac{1}{12} h(\sqrt{-3p}) \\
&\quad + \left\{ \frac{1}{48}(p-1)\left(9 - 4\left(\frac{2}{p}\right)\right) + \frac{1}{16}\left(p - \left(\frac{2}{p}\right)\right) + \frac{1}{12}\left(1 - \left(\frac{p}{3}\right)\right)\left(3 - \left(\frac{2}{p}\right)\right)\right\} h(\sqrt{-p})
\end{aligned}
$$

(2) For $p = 2$, 3, 5, we have $T(1,p) = 2T(1,p) - H(1,p) = 1$. When $p \equiv 1 \bmod 4$ and $p \geq 11$, we have

$$
\begin{aligned}
2T(1,p) - H(1,p) = {}& \frac{1}{2^5 \cdot 3}\left(9 - 2\left(\frac{2}{p}\right)\right) B_{2,\chi} + \frac{1}{2^4} h(\sqrt{-p}) \\
&+ \frac{1}{2^3} h(\sqrt{-2p}) + \frac{1}{2^2 \cdot 3}\left(3 + \left(\frac{2}{p}\right)\right) h(\sqrt{-3p}).
\end{aligned}
$$

When $p \equiv 3 \bmod 4$ and $p \geq 7$, we have

$$
\begin{aligned}
&2T(1,p) - H(1,p) = \\
&\qquad \frac{1}{2^5 \cdot 3} B_{2,\chi} + \frac{1}{2^4}\left(1 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}) + \frac{1}{2^3} h(\sqrt{-2p}) + \frac{1}{2^2 \cdot 3} h(\sqrt{-3p}).
\end{aligned}
$$

A numerical table are given as follows.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$2T(p,1) - H(p,1)$	1	1	2	2	5	4	8	8	14	18	18	11	32	19	44
$2T(1,p) - H(1,p)$	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4

Comparing the numerical table of $2T(1,p) - H(1,p)$ with the table of $H(1,p)$, it is surprising that $T(1,p) = H(1,p)$ for so many p. Actually the minimum p such that these are different is $p = 167$, where $H(1,p) = 20$ and $T(1,p) = 19$. We have the following easy corollary of the above table on geometry.

Corollary 5.3 ([27], [48]). *For any n, there exists a component of $\mathcal{S}_{n,1}$ defined over $\mathbb{F}_p$. When $n = 2$ and $p < 167$, all the irreducible components of $\mathcal{S}_{2,1}$ are defined over $\mathbb{F}_p$.*

I was informed by Cris Poor that this prime 167 appears also as the smallest prime such that there exists non-lift paramodular cusp form of weight 3 with plus sign of Atkin-Lehner ([6]). Such correspondence is naturally expected by the conjecture between paramodular forms of weight k and the algebraic modular forms of weight $k-3$ associated with non-principal genus (see [18], [22], [31]).

The calculation above of $T(p,1)$ or $T(1,p)$ is based on an equality between the type numbers and class numbers of quinary quadratic forms ([26]). The latter class numbers have been calculated in [2], so we can use this. In general, $2T(\mathcal{G})-H(\mathcal{G})$ is also given by the trace formula for the Hecke operator $U\pi U$ (see [25]), though actual calculation would be very hard.

§ 6. Remark on algebraic modular forms

Our class numbers can be regarded as dimensions of certain algebraic automorphic forms of some weight. So we explain algebraic modular forms and some related things in this section. Let (ρ, V) be an irreducible representation of $G_\infty^1 := \{g \in G_\infty; n(g)=1\}$. We assume here that $\rho(\pm 1_n)=1$ for the sake of simplicity. Here G_∞^1 is a compact group and a theory of representations are classical. The irreducible rational representations correspond with certain Young diagrams and character formulas are also known. We define a representation of G_A associated with ρ by

$$G_A \to G_\infty \to G_\infty/\mathbb{R}_+^\times \cong G_\infty^1/\{\pm 1_n\} \xrightarrow{\rho} GL(V).$$

We define the space $\mathfrak{M}_\rho(U)$ of algebraic modular forms of weight ρ with respect to an open subgroup U of G_A by

$$\mathfrak{M}_\rho(U) := \{f : G_A \to V; f(uga) = \rho(u)f(g) \text{ for any } u \in U, g \in G_A, a \in G\}.$$

If we write $G_A = \bigcup_{i=1}^h Ug_iG$, then it is clear that $f \in \mathfrak{M}_\rho(U)$ is determined by the vector $(f(g_1), \ldots, f(g_h))$. For example, if ρ is the trivial representation (denoted by 0 for simplicity), then f is nothing but a function which takes a constant on each double coset. So in this case, we have

$$\mathfrak{M}_0(U) \cong \mathbb{C}^h.$$

This is often called algebraic modular forms of weight 0. So the class number of U (the number of double cosets) is nothing but the dimension of algebraic modular forms of weight 0. More generally, we have the following isomorphism (see [8], [10]).

$$\mathfrak{M}_\rho(U) \cong \oplus_{i=1}^h V^{\Gamma_i} \tag{6.1}$$

where we define $\Gamma_i = G \cap g_i^{-1}Ug_i$ (which is a finite group) and

$$V^{\Gamma_i} = \{v \in V; \rho(\gamma)v = v \text{ for all } \gamma \in \Gamma_i\}. \tag{6.2}$$

The isomorphism of (6.1) is given by $f \to (\rho(g_1^{-1})f(g_1), \ldots, \rho(g_h^{-1})f(g_h))$.

When $n=1$, algebraic modular forms are *disguised* forms of the classical “Brandt matrices”. Since G_∞^1 is compact, we can realize V as a certain space of polynomials, and algebraic modular forms are vectors of polynomials invariant by the actions of certain finite groups. It is not difficult to give concrete examples for such polynomials. This is often much easier to give holomorphic modular forms, so by using the correspondence between algebraic modular forms of $U(2)$ and holomorphic modular forms of $GL(2)$ or its product known by Eichler, Shimuzu, Jacquet-Langlands, some people use algebraic modular forms instead of holomorphic modular forms to give examples. The spaces beyond classical Brandt matrices were first introduced by Y. Ihara [32]. Some abstract general theory for Hecke algebra etc on algebraic modular forms for our case was well explained in Hashimoto [8]. Later B. H. Gross defined algebraic modular forms for general reductive group such that G_∞ is compact, so we are using his naming here.

The dimension formula for $\mathfrak{M}_\rho$ is an easy corollary for the class number formula and the classical character formula, which we omit here(see [10], [18], [11], [22], [31], [24]). For any double coset UzU, the Hecke operator action on $\mathfrak{M}_\rho(U)$ is defined by

$$((UzU)f)(g) = \sum_{i=1}^{d} \rho(z_j^{-1})f(z_i^{-1}g)$$

where $UzU = \cup_{i=1}^{d} z_i U$. Through the isomorphism (6.2), the Hecke operator is identified with certain $h \times h$ matrices(see [8]). This has some application to the geometry. For example if $L = O^n$ and $T(m) = \bigcup_{g \in G_A \cap M_n(O_A); n(g)=m} UgU$, then $T(m)$ describes isogenies of degree n between principally polaraized superspecial abelian varieties. A general theory of such Hecke operators for big U is in Satake [38], and explicit shape of Euler factors are known in [32] and [12].

The proof of the class number formulas in the previous section is based on a calculation of the trace of some Hecke operators on algebraic modular forms. It is essentially a summation of some type of masses associated with conjugacy classes in G with some complicated local correction data.

We have a similar mass formula for elements in any ℓ-fold self-product G^ℓ of G (see [19]). We can apply this to vectors of generators of any subgroup in G and hence to generators of Γ_i. Then this formula enables us to calculate Γ_i in principle. More precisely, let Γ be some abstract group. Then this new mass formula can be in principle used to count the number of Γ_i such that $\Gamma \cong \Gamma_i$. Of course in most cases, the actual calculations are hard, but a precise result for $n = 2$ of $\mathcal{G}_{nonp}$ is given in [19]. Such groups Γ_i for $\mathcal{G}_{nonp}$ is the automorphism group of the irreducible components of $\mathcal{S}_{2,1}$. In this case, the possible groups for $\Gamma_i/\{\pm 1_2\}$ are

$$\{1\} \quad \mathbb{Z}/2\mathbb{Z} \quad \mathbb{Z}/3\mathbb{Z} \quad (\mathbb{Z}/2\mathbb{Z})^2 \quad S_3 \quad A_4 \quad S_4 \quad D_{12} \quad A_5$$

where S_n and A_n are the symmetric group and the alternating group, respectively and D_{12} is the dihedral group of order 12. On the other hand, the list of automorphism groups for the principal genus $\mathcal{G}_{princ}$ for $n = 2$ is in [29] for indecomposable lattices. Automorphism groups of decomposable lattices are easily given. If the lattice corresponds with $E_1 + E_2$ for non-isomorphic supersingular elliptic curves E_1 and E_2, then the automorphism group is $Aut(E_1) \times Aut(E_2)$. The automorphism group of the lattice corresponding to $E + E$ is generated by $Aut(E) \times Aut(E)$ and the interchange of both components.

Another interesting thing for algebraic modular form is that by Langlands functoriality and the isomorphism $G^1(\mathbb{C}) \cong Sp(n, \mathbb{C})$ (where $Sp(n, \mathbb{C})$ is the symplectic group of rank n, i.e. a subgroup of $GL_{2n}(\mathbb{C})$), we can expect that algebraic modular forms are isomorphic to Siegel modular forms Hecke equivariantly. This was the motivation of Ihara [32]. Although he did not formulate any precise conjecture and said nothing about which kind of discrete subgroups are suitable for the comparison, he developped some lifting theory to algebraic modular forms of Saito-Kurokawa type for $n = 2$.

A precise formulation of this sort of conjectures for parahoric subgroups as discrete subgroups are given in [15], [18], [11], [22], [31], [24]. A proof for some of them is given in [13].

§ 7. Curves with many rational points

Let C be a smooth projective curve of genus g defined over the finite field $\mathbb{F}_q$ of q elements. Then the number of $\mathbb{F}_q$ rational points $C(\mathbb{F}_q)$ is evaluated by A. Weil as

$$1 + q - 2g\sqrt{q} \leq |C(\mathbb{F}_q)| \leq 1 + q + 2g\sqrt{q}.$$

If q is not a square, the equality never holds, but when q is a square, it is an interesting problem to ask if there exists a curve C which attains the maximum or the minimum of the above bound. The case $g = 1$ is classical. The problem for $g \geq 2$ is started by J. P. Serre and he proved the existence for any square $q \neq 4$, 9 for $g = 2$. For the existence theorem for such curves for $p \neq 2$, 3, his point is to show that there exists a curve of genus 2 such that $J(C) \cong E^2$ for a supersingular elliptic curve E, since the Frobenius of E^2 is suitable to show the maximality of the number of rational points. He also used the fact that a curve of genus 2 is always a hyperelliptic curve.

When the genus is 3, all the abelian varieties of dimension 3 are Jacobian varieties if we include reduced curves ([35]), so principally polarized superspecial abelian variety (E^3, λ) with indecomposable λ is a Jacobian $J(C)$ of a smooth irreducible curve C. We can easily count the number of indecomposable lattices in the principal genus by using class number formulas for $n = 1$, 2, 3 and when $p \geq 3$, there exists an irreducible curve C over k of genus 3 such that $J(C) \cong E^3$. But this is far from showing the existence of maximum or minimum curve. Here we have the following problem. For general g, if C is not hyperelliptic, the Torelli theorem has some problem. In case when C is non-hyperelliptic, even if there exists an isomorphism $J(C) \cong E^3$ over an algebraically closed field, we cannot descend this to an isomorphism over the field of definition of both sides. The obstruction is that for non-hyperelliptic curve C, there is a difference between $Aut(C)$ and $Aut(J(C))$, and we only have

$$Aut(C) \cong Aut(J(C))/\{\pm 1\}.$$

What we can say is that we have an isomorphism over a quadratic extension of the base field of definition but may not have it over the base field itself. (I learned this from J. P. Serre by a private letter.) So we must have a special care for this point.

Here we have the following theorem.

Theorem 7.1 ([20]). *For any odd prime, there exists a smooth irreducible curve of genus 3 defined over $\mathbb{F}_p$ such that $J(C) \cong E^3$ for a supersingular elliptic curve E defined over $\mathbb{F}_p$, where the isomorphism is defined over $\mathbb{F}_{p^2}$ and we have*

$$|C(\mathbb{F}_{p^2})| = 1 + p^2 + 6p,$$

which is the maximum possible number.

By seeing the Frobenius of E^3 over $\mathbb{F}_{p^{2e}}$, this theorem obviously means that for odd e, we have $|C(\mathbb{F}_{p^{2e}})| = 1 + p^{2e} + 6p^e$ and for even e, we have $|C(\mathbb{F}_{p^{2e}})| = 1 + p^{2e} - 6p^e$.

This is an existence theorem and not a theorem to give C concretely. If we write any concrete relatively simple C over $\mathbb{Z}$ and consider the condition such that C mod p is superspecial, then it usually happens that for some p in certain arithmetic progressions, this is superspecial, but not for the rest of progressions. (Of course we can give many such examples, e. g. $x^4 + y^4 = z^4$.) If so, this means that there is no hope to prove the existence of maximal curves for all big p by giving examples, since finite numbers of such arithmetic progressions do not cover all the primes.

The ingredient of the proof of Theorem 7.1 is as follows. We consider a condition that (E^3, λ) has a model (A, μ) over $\mathbb{F}_p$ and at the same time an isomorphism $(E^3, \lambda) \cong (A, \mu)$ can be taken over $\mathbb{F}_{p^2}$. By the Weil criterion of descent of the field of definition, this condition is interpreted as the existence of quaternion hermitian lattices L in $\mathcal{G}_{princ}$ such that there is some nice element $g \in G$ satisfying $Lg \subset L$. Then we prove this existence of such L by showing the positivity of certain mass of such g in the trace formula.

When the genus is more than 3, abelian varieties are not necessarily Jacobians and it seems there is no easy way to reduce the problem to the theory of lattices.

§ 8. Moduli and parahoric subgroups

We will explain that the arithmetic of G_A is also powerful for the study of moduli. First we consider the case $n = \dim A = 2$. We have already explained the following

things.
(1) Each irreducible component V of $\mathcal{S}_{1,2}$ corresponds to a (class of) quaternion hermitian lattice in the non-principal genus $\mathcal{G}_{nonp}$.
(2) Each principally polarized superspecial abelian surface (E^2, λ) corresponds to a (class of) quaternion hermitan lattice in the principal genus $\mathcal{G}_{princ}$.

Since *superspecial* is also *supersingular*, the above (E^2, λ) should correspond to some point in $\mathcal{S}_{2,1}$. To which component does this belong? In particular, since such points and irreducible components are both described by quaternion hermitian lattices, how can we describe the condition that a point is on a component by the lattice theoretic terminology? We will answer this question below.

First we review some theory on directions from Oort [36] and [34]. We denote by α_p the finite group scheme of order p given by

$$\alpha_p = Spec(k[x]/(x^p)),$$

where the multiplication is given by $x \to 1 \otimes x + x \otimes 1$. We have an embedding $\alpha_p \to E$. Any supersingular abelian surface A can be written as

$$A \cong E^2/\iota(\alpha_p)$$

where ι is an embedding $(i, j) : \alpha_p \to E^2$. We put ${}_F E = \{Ker(F : E \to E^{(p)})\}$ for the Frobenius map F and define $t \in k \cup \{\infty\}$ as

$$\{\alpha_p \xrightarrow{\overset{i}{\sim}} {}_F E \xrightarrow{j^{-1}} \alpha_p\} = \frac{i}{j} = t \in k = End(\alpha_p),$$

where we regard $t = \infty$ when $j = 0$. We call t a direction of the embedding. Oort proved in [36] that A is isomorphic to E^2 if and only if $t \in \mathbb{F}_{p^2} \cup \{\infty\}$. In this case, t is called a good direction. So there are $p^2 + 1$ good directions. Let ϕ be the natural projection of E^2 to $E^2/\iota(\alpha_p)$ for a good direction. Although E^2 and $E^2/\iota(\alpha_p)$ are isomorphic, we are taking ϕ as an isogeny of degree p. Since $E^2/\iota(\alpha_p) \cong E^2$, we can identify ϕ with an element in the Hecke algebra

$$T(1, \pi) := GL_2(O) \begin{pmatrix} 1 & 0 \\ 0 & \pi \end{pmatrix} GL_2(O).$$

(Because of the strong approximation theorem, the local Hecke algebra and the global Hecke algebra do not differ essentially.) So we can show that the directions can be regarded as cosets $GL_2(O)\backslash T(1, \pi)$ by seeing concrete coset representatives.

For any polarization λ of E^2, we say that λ belongs to a genus $\mathcal{G}$ if the quatenion hermitian matrix $\phi_X^{-1}\lambda$ is associated with a lattice in $\mathcal{G}$. Assume that a polarization λ of E^2 belongs to $\mathcal{G}_{nonp}$. Then it is clear that for any $g \in T(1, \pi)$, there exists $H = H^* \in$

$GL_2(O)$ (a quaternion hermitian matrix belonging to $\mathcal{G}_{princ}$) such that $\phi_X^{-1}\lambda = gHg^*$, and any such λ descends to a principal polarization of E^2. On the other hand, let λ_0 be a principal polarization of E^2 and consider the situation that $p\lambda_0$ descends to a polarization λ_1 of E^2 which belong to $\mathcal{G}_{nonp}$ by an element $g \in T(1,\pi)$. (The condition that λ_1 belongs to $\mathcal{G}_{nonp}$ is equivalent to the condition that $Ker(\lambda_1) \cong \alpha_p^2$.) Then by a direct calculation of cosets, we can show that there are $p+1$ cosets of $g \in T(1,\pi)$ such that $p\lambda_0 = g^*(\lambda_1)$ for some λ_1. This direction, i.e. a coset in $GL_2(O)\backslash T(1,\pi)$, is called a very good direction. We will see that these two notions are related to parahoric subgroups. To explain parahoric subgroups, we introduce another expression of G_p. Locally at p, we have an element $\xi \in GL_2(O_p)$ such that

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

By using this element, if we put $G_p^* = \xi G_p \xi^{-1}$, then we have

$$G_p^* = \left\{ g \in M_2(D_p); g \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} g^* = n(g) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ for some } n(g) \in \mathbb{Q}_p^\times \right\}.$$

For $i = 0$, 1, 2, we define

$$\begin{aligned} U_{2,p}^* &= GL_2(O_p) \cap G_p^*, \\ U_{1,p}^* &= \begin{pmatrix} O_p & \pi^{-1}O_p \\ \pi O_p & O_p \end{pmatrix}^\times \cap G_p^*, \\ U_{0,p}^* &= U_{1,p}^* \cap U_{2,p}^*, \end{aligned}$$

and put $U_{i,p} = \xi^{-1}U_{i,p}^*\xi$. Then these three groups are representatives of conjugacy classes of parahoric subgroups of G_p. (Roughly speaking, a parahoric subgroup is a group whose reduction modulo π contains a upper triangular subgroup.) We also define open subgroups of G_A by

$$U_i = G_\infty U_{i,p} \prod_{q \neq p} (GL_2(O_q) \cap G_q).$$

Then we have $[U_2 : U_0] = [U_{2,p} : U_{0,p}] = p^2 + 1$ and $[U_1 : U_0] = [U_{1,p} : U_{0,p}] = p + 1$. So it is natural to expect that good directions and very good directions have some connection to these subgroups. First we explain this only by using the quaternion hermitian matrices. Let H_0 and K_0 be quaternion hermitian matrices in $GL_2(O)$ (corresponding to the principal genus) and put $H_2 = pK_0$. We assume that H_1 is a quatenion hermitian matrix corresponding to the non-principal genus. Let L be a maximal lattice in $\mathcal{G}_{nonp}$ defined by

$$L = ((\pi O_p, O_p)\xi \cap D^2) \bigcap_{q \neq p} (O_q^2 \cap D^2).$$

For $h_i \in GL_2(D)$ such that $H_i = h_i h_i^*$ for $i = 0$, 1, 2, we may write

$$O^2 h_2 = O^2 \pi g_2, \qquad O^2 h_0 = O^2 g_0, \qquad O^2 h_1 = L g_1 \tag{8.1}$$

for some $g_i \in G_A$. For quatenion hermitian matrices H and K, we say that H is descendable to K if $H = gKg^*$ for some $g \in GL_2(D) \cap M_2(O)$.

Proposition 8.1. *Notation being as above, we have*
(1) H_2 is descendable to H_1 if and only if $U_1 g_1 G \cap U_2 g_2 G \neq \emptyset$.
(2) H_1 is descendable to H_0 if and only if $U_1 g_1 G \cap U_2 g_0 G \neq \emptyset$.

Note that here we are considering two possibly different double cosets $U_2 g_2 G$ and $U_2 g_0 G$ for the same U_2. Some more description between some orbit of directions and $U_i \cap g_i G g_i^{-1}$ -orbit of $U_0 \backslash U_i$ is possible but we omit it here. Please see another paper [28].

We write one geometric application of the above proposition. Any irreducible component of $\mathcal{S}_{2,1}$ corresponds with some polarization λ of E^2 that belongs to $\mathcal{G}_{nonp}$ (due to Katsura and Oort). Let's fix such polarization μ_1 and denote by $V(\mu_1)$ the irreducible component of $\mathcal{S}_{2,1}$ corresponding to μ_1. Let μ_0 be a principal polarization of E^2. Denote by H_1, H_0 the quatenion hermitian matrices corresponding to μ_1, μ_0, respectively and define g_i as in (8.1). Then we have

Theorem 8.2. *A principally polarized superspecial abelian surface (E^2, μ_0) is on $V(\mu_1)$ if and only if $U_2 g_0 G \cap U_1 g_1 G \neq \emptyset$. (Note that the mismatch of the subscripts of U_2 and g_0 are not typos.)*

For a supersingular abelian variety A, we define a-number by $a = \dim Hom(\alpha_p, A)$(e.g. see [37]). For example, $A \cong E^n$ if and only if $a = n$. For a generic A, we have $a = 1$. Irreducible components in $\mathcal{S}_{n,1}$ is controlled by a polarization λ of E^n in $\mathcal{G}_{princ}$ or in $\mathcal{G}_{nonp}$ as we have already explained. More precisely for $n = 3$ this is described as follows (see [35], [33], [37]). Let (A, λ) be a principally polarized supersingular abelian variety of dimension 3. Then there exists a principal polarization λ_0 of E^3 and a sequence

$$(E^3, p\lambda_0) \overset{\phi_2}{\to} (A_1, \mu_1) \overset{\phi_1}{\to} (A, \lambda)$$

such that $Ker(\phi_i) \cong (\alpha_p)^i$ and $p\lambda_0 = \phi_2^*(\mu_1)$, $\mu_1 = \phi_1^*(\lambda)$, and $Ker(\mu_1) \subset A_1[F]$, where F is the absolute Frobenius. Such sequence is called a polarized flag type quotient. When $a(A) = 1$, then this sequence is unique and (A, λ) belongs to the irreducible component of $\mathcal{S}_{3,1}$ defined by λ_0.

Then we may ask the similar thing for $n = 3$ as in $n = 2$. Since we have no space to state theorems for this, we give a very short sketch. When $\dim A = 3$, the a-number of A is 1, 2, 3. For $a = 3$, for a principal polarization μ_0, (E^3, μ_0) is a point in $\mathcal{S}_{3,1}$. For

$a = 2$, we can consider the family of principally polarized abelian varieties (A, λ) *below* $(E^3, p\lambda_0)$ for a fixed λ_0. So we have three families, i.e. irreducible components, $a = 2$ families, and points (E^3, μ_0). These three families correspond to adelic double cosets for certain explicitly described open subgroups of G_A, and all the inclusion relations of these three objects are described by non-emptyness of corresponding double cosets. Details will be published in [28].

Acknowledgment: We would like to thank the referee for the very careful reading and suggestions.

References

[1] T. Arakawa, T. Ibukiyama and M. Kaneko, *Bernoulli numbers and zeta functions*, with an appendix by Don Zagier, Springer Monographs in Math. Springer (2014), xi+274 pp.

[2] T. Asai, The class numbers of positive definite quadratic forms. *Japan. J. Math. (N.S.)* **3** (1977), 239–296.

[3] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.

[4] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl. *Jber. Deutsch. Math.-Verein.* **54** (1950), 24–41.

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

[6] V. Gritsenko, C. Poor and D. S. Yuen, Antisymmetric paramodular forms of weight 2 and 3. *Int. Math. Research Notices* (2020) **20**, 6926–6946.

[7] B. H. Gross, Algebraic modular forms. *Israel J. Math.* **113** (1999), 61–93.

[8] K. Hashimoto, On Brandt matrices associated with the positive definite quaternion Hermitian forms. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **27** (1980), 227–245.

[9] K. Hashimoto, Class numbers of positive definite ternary quaternion Hermitian forms. *Proc. Japan Acad. Ser. A Math. Sci.* **59** (1983), no. 10, 490–493.

[10] K. Hashimoto and T. Ibukiyama, On class numbers of binary quaternion hermitian forms (I), *J. Fac. Sci. Univ. Tokyo Sect. IA* **27** (1980), 549–601; (II) *ibid.* **28** (1982), 695–699; (III) *ibid.* **30** (1983), 393–401.

[11] K. Hashimoto and T. Ibukiyama, On relations of dimensions of automorphic forms of $Sp(2, \mathbb{R})$ and its compact twist $Sp(2)$. II. *Automorphic forms and number theory (Sendai, 1983)*, 31–102, Adv. Stud. Pure Math., **7**, North-Holland, Amsterdam, 1985.

[12] T. Hina and T. Sugano, On the local Hecke series of some classical groups over p-adic fields. *J. Math. Soc. Japan* **35** (1983), 133–152.

[13] P. van Hoften, A geometric Jacquet-Langlands correspondence for paramodular Siegel threefolds, Math. Z. **299** (2021), 2029–2061.

[14] T. Ibukiyama, On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings. *Nagoya Math. J.*, **88** (1982), 181–195.

[15] T. Ibukiyama, On symplectic Euler factors of genus two. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **30** (1984), 587–614.

[16] T. Ibukiyama. On automorphic forms of $Sp(2; \mathbb{R})$ and its compact form $Sp(2)$. *Séminaire de Théorie des nomble de Paris, 1982–1983*, Progr. Math. **51**, Birkhäuser Boston, Inc.(1984), 125–134.

[17] T. Ibukiyama, Construction of half integral weight Siegel modular forms of $Sp(2;\mathbb{R})$ from automorphic forms of the compact twist $Sp(2)$. *J. reine angew. Math.*, **359**. (1985), 188–220.

[18] T. Ibukiyama. On relations of dimensions of automorphic forms of $Sp(2;\mathbb{R})$ and its compact twist $Sp(2)$ (I). *Automorphic Forms and Number Theory(Sendai 1983)*, Advanced Studies in Pure Math., **7** (1985), 7–29.

[19] T. Ibukyama, On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, pages 301-349. *Automorphic Forms and Geometry of Arithmetic Varieties*, Advanced Studies in pure Math. **15**, Kinokuniya, Tokyo, 1989.

[20] T. Ibukiyama, On rational points of curves of genus three over finite fields. *Tõhoku Math. J.* **45**(1993), 311–329.

[21] T. Ibukiyama and T. Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers. *Compositio Math.* **91**(1994), 37–46.

[22] T. Ibukiyama, Paramodular forms and compact twist, *Automorphic Forms on GSp(4), Proceedings of the 9-th Autumn Workshop on Number Theory*, Ed. M. Furusawa (2007), 37–48.

[23] T. Ibukiyama, Dimension formulas of Siegel modular forms of weight 3 and supersingular abelian varieties, *Proceedings of the 4-th Spring Conference on modular forms and related topics, Siegel Modular Forms and Abelian Varieties* ed. by T. Ibukiyama (2007), 39–60.

[24] T. Ibukiyama, Conjectures on correspondence of symplectic modular forms of middle parahoric type and Ihara lifts. *Res. Math. Sci.* **5** (2018), no. 2, Paper No. 18, 36 pp.

[25] T. Ibukiyama, Type numbers of quaternion hermitian forms and supersingular abelian varieties. *Osaka J. Math.* **55** (2018), no. 2, 369–384.

[26] T. Ibukiyama, Quinary lattices and binary quaternion hermitian lattices, *Tohoku Math. J.* (2) **71** (2019), no. 2, 207–220.

[27] T. Ibukiyama, Principal polarizations of supersingular abelian surfaces, *J. Math. Soc. Japan* **72** (2020), 1161–1180.

[28] T, Ibukiyama, Supersingular loci of low dimensions and parahoric subgroups, to appear in Osaka J. Math. **59** no. 3 (2022).

[29] T. Ibukiyama, T. Katsura, and F. Oort, Supersingular curves of genus two and class numbers. *Compositio Math.*, **57** (1986), 127–152.

[30] T. Ibukiyama and Y. Ihara, On automorphic forms on the unitary symplectic group $Sp(n)$ and $SL_2(\mathbb{R})$, *Math. Ann.*, **278** (1987), 307–327.

[31] T. Ibukiyama and H. Kitayama, Dimension formulas of paramodular forms of squarefree level and comparison with inner twist, *J. Math. Soc. Japan* **69** (2017), no. 2, 597–671.

[32] Y. Ihara, On certain arithmetical Dirichlet series. *J. Math. Soc. Japan* **16** (1964), 214–225.

[33] T. Katsura and F. Oort, Supersingular abelian varieties of dimension two or three and class numbers. *Algebraic geometry, Sendai*, 1985, 253–281, Adv. Stud. Pure Math., **10**, North-Holland, Amsterdam, 1987.

[34] T. Katsura and F. Oort, Families of supersingular abelian surfaces. *Compositio Math.* **62** (1987), 107–167.

[35] T. Oda and F. Oort, Supersingular abelian varieties. *Proceedings of the International Symposium on Algebraic Geometry (Kyoto Univ., Kyoto, 1977)*, 595–621, Kinokuniya Book Store, Tokyo, 1978.

[36] F. Oort, Which abelian surfaces are products of elliptic curves? *Math. Ann.* **214** (1975), 35–47.

[37] Ke-Zheng Li and F. Oort, Moduli of supersingular abelian varieties. *Lecture Notes in*

Mathematics **1680**. Springer-Verlag, Berlin, 1998. iv+116 pp.

[38] I. Satake, Theory of spherical functions on reductive algebraic groups over p-adic fields. *Inst. Hautes Études Sci. Publ. Math.* **18** (1963), 5–69.

[39] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms. *J. Math. Soc. Japan* **15** (1963), 33–65.

[40] T. Shioda, Some remarks on abelian varieties, *J. Fac. Sci. Univ. Tokyo, Sect. IA* **24** (1977), 11–21.

[41] J. Tate, Endomorphisms of abelian varieties over finite fields, *Inventiones Math.* **2** (1966), 134–144.

[42] W. C. Waterhouse, Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.* **(4) 2** (1969), 521–560.

[43] W. C. Waterhouse and J. S. Milne, Abelian varieties over finite fields, *Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y.*, (1971), 53–64, Amer. Math. Soc., Providence, R.I.

[44] Chia-Fu Yu, The supersingular loci and mass formulas on Siegel modular varieties, *Doc. Math.* **11** (2006), 449–468.

[45] Chia-Fu Yu and Jeng-Daw Yu, Mass formula for supersingular abelian surfaces, *J. Algebra* **322**(2009), 3733-3743.

[46] Chia-Fu Yu, Superspecial abelian varieties over finite prime fields. *J. Pure Appl. Algebra* **216** (2012), no. 6, 1418–1427.

[47] U. Görtz and Chia-Fu Yu, The supersingular locus in Siegel modular varieties with Iwahori level structure. *Math. Ann.* **353** (2012), 465–498.

[48] Chia-Fu Yu, On fields of definition of components of the Siegel supersingular locus. *Proc. Amer. Math. Soc.* **145** (2017), no. 12, 5053–5058.