Tohoku Math. J.
71 (2019), 207–220

QUINARY LATTICES AND BINARY QUATERNION HERMITIAN LATTICES

TOMOYOSHI IBUKIYAMA

(Received August 26, 2016, revised February 1, 2017)

Abstract. In our previous papers, we defined the G-type number of any genera of quaternion hermitian lattices as a generalization of the type number of a quaternion algebra. Now we prove in this paper that the G-type number of any genus of positive definite binary quaternion hermitian maximal lattices in B^2 for a definite quaternion algebra B over $\mathbb{Q}$ is equal to the class number of some explicitly defined genus of positive definite quinary quadratic lattices. This is a generalization of a part of the results in 1982, where only the principal genus was treated. Explicit formulas for this type number can be obtained by using Asai's class number formula. In particular, in case when the discriminant of B is a prime, we will write down an explicit formula for T, H and $2T - H$ for the non-principal genus, where T and H are the type number and the class number. This number was known for the principal genus before. In another paper, our new result is applied to polarized superspecial varieties and irreducible components of supersingular locus in the moduli of principally polarized abelian varieties having a model over a finite prime field, where $2T - H$ plays an important role.

1. Introduction. The classical isomorphism $SU(2)/\{\pm 1\} \cong SO(3)$ suggests a relation between ternary lattices and the type number of quaternion algebras. (For example, see [13] or [14]). Also for the compact symplectic group $Sp(2)$ of complex rank 2, the isomorphism $Sp(2)/\pm 1 \cong SO(5)$ suggests a relation between the G-type number of binary quaternion hermitian forms and the class number of some quinary quadratic forms. But it seems there was no concrete general theory to tell which genus should correspond with which genus of lattices. It seems that this is a subtle arithmetic in general, and we need a careful proof for this kind of question. We will solve this for genera of maximal lattices.

Let B be a definite quaternion algebra over $\mathbb{Q}$ and G the group of similitudes of the positive definite quaternion hermitian form on B^2. Here we give a theorem on a relation between the G-type number of any genus of positive definite maximal lattices in B^2 and the class number of some positive definite quinary quadratic forms. When the genus in B^2 is the principal genus, this result was announced in [4] almost without proof. Our present result is its generalization. Our main theorem is Theorem 4.5. Some explicit formula will be explained in Theorem 5.1. Our application to a geometry is Theorem 5.2.

2. Quaternion hermitian forms and type numbers. We first review shortly the arithmetic theory of quaternion hermitian forms from [15] and G-type numbers from [5]. Let B be a definite quaternion algebra over $\mathbb{Q}$. We denote by D the product of finite primes such

2010 Mathematics Subject Classification. Primary 11E41; Secondary 14K10, 11E12.
Key words and phrases. Quinary lattice, Quaternion hermitian lattice, supersingular abelian variety.
This work was supported by JSPS KAKENHI Grant Number JP25247001.

that $B_p = B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a division algebra, where $\mathbb{Q}_p$ is the field of p-adic numbers. We call it a discriminant of B. For $\alpha \in B$, we denote by $N(\alpha)$ and $Tr(\alpha)$ the reduced norm and the reduced trace of α. We denote by $\alpha \to \overline{\alpha}$ the main involution of B. For any matrix $b = (b_{ij}) \in M_{mn}(B)$ of any size, we write $b^* = (\overline{b_{ji}})$. A positive definite quaternion hermitian form on B^2 is unique up to a base change over B, and for $x = (x_1, x_2)$ and $y = (y_1, y_2) \in B^2$, we may assume that it is given by

$$(x, y) = xy^* = x_1\overline{y_1} + x_2\overline{y_2}\,.$$

We denote by G the group of similitudes with respect to (x, y), that is,

$$G = \{g \in M_2(B); gg^* = n(g)1_2 \text{ for some } n(g) \in \mathbb{Q}^\times\},$$

where 1_n is the $n \times n$ unit matrix. Here obviously we have $n(g) > 0$. In the same way, for any places $v \leq \infty$ of $\mathbb{Q}$, we write

$$G_v = \{g \in M_2(B_v); gg^* = n(g)1_2 \text{ for some } n(g) \in \mathbb{Q}_v^\times\},$$

where we put $B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ for $\mathbb{Q}_v = \mathbb{Q}_p$ if $v = p$ is a prime or for $\mathbb{Q}_\infty = \mathbb{R}$ if $v = \infty$. Here of course $n(g) > 0$ if $v = \infty$. We denote by G_A the adelization of G. Let O be a maximal order of B. A lattice L in B^2 is said to be a left O-lattice if it is a left O module. We define $N(L)$ the two sided O ideal spanned by (x, y) for all x, $y \in L$. A left O-lattice L is said to be maximal if any left O lattice $L_1 \supset L$ such that $N(L_1) = N(L)$ is equal to L. Maximal left O_p lattices are defined similarly. A left O-lattice L is maximal if and only if $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is maximal for every prime p. We say that two left O-lattices L_1 and L_2 are in the same class if $L_1 g = L_2$ for some $g \in G$. We say that L_1 and L_2 belong to the same genus if $L_{1,p}g_p = L_{2,p}$ for some $g_p \in G_p$ for all primes p. For a left O-lattice L, we denote by $\mathcal{L}(L)$ the set of left O lattices which belong to the same genus as L and call it the genus of L. If $p \nmid D$, then the G_p-orbits of left O_p maximal lattices in B_p^2 is unique and represented by O_p^2. If $p|D$, then there are exactly two G_p orbits of maximal lattices, one is represented by O_p^2 and the other is represented by

$$L_p^{(np)} = O_p^2 \begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix} \xi$$

where π is a prime element of O_p with $\pi^2 = -p$ and ξ is a fixed element in $GL_2(B_p)$ such that $\xi\xi^* = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. For a divisor D_1 of D and $D_2 = D/D_1$, we define a genus $\mathcal{L}(D_1, D_2)$ as the set of left O-lattices such that $L_p = O_p^2 g_p$ for some $g_p \in G_p$ for primes $p \nmid D_2$, and $L_p = L_p^{(np)} g_p$ for some $g_p \in G_p$ for primes $p|D_2$. So if t is the number of prime divisors of D, then there are exactly 2^t different genera of maximal lattices. The genus $\mathcal{L}(D, 1) = \mathcal{L}(O^2)$ is called a principal genus. The number of classes in $\mathcal{L}(D_1, D_2)$ is called the class number of $\mathcal{L}(D_1, D_2)$. For a fixed $L \in \mathcal{L}(D_1, D_2)$, we put

$$U_p = U_p(L_p) = \{g \in G_p; L_p g_p = L_p\}$$

and $U(L) = U = G_\infty \prod_p U_p$. Then the class number $h = H(D_1, D_2)$ of $\mathcal{L}(D_1, D_2)$ is given by $\#(U \backslash G_A / G)$ which is finite. An explicit formula for $H(D_1, D_2)$ are all given in [4] (I) and (II).

Now let $L_1, \dots, L_h$ be a complete set of representatives of classes in $\mathcal{L}(D_1, D_2)$. We denote by R_i the right order of L_i defined by

$$R_i = \{g \in M_2(B); L_i g \subset L_i\} .$$

If $a^{-1} R_i a = R_j$ for some $a \in G$, then we say that R_i and R_j have the same G-type. The number of different types in $\{R_1, \dots, R_h\}$ is called a type number $T(D_1, D_2)$ of $\mathcal{L}(D_1, D_2)$. For the right order R of $L = L_1$ and $g = (g_p) \in G_A$, we write

$$g^{-1} R g = \bigcap_{p<\infty} \left(g_p^{-1} R_p g_p \cap M_2(B)\right) .$$

Then the type number is equal to the number of G-conjugacy classes in this set $\{g^{-1} R g; g \in G_A\}$. Main purpose of this paper is to show that the type number $T(D_1, D_2)$ is equal to the class number of some quinary lattices. Locally, the right order of O_p^2 is $M_2(O_p)$ and the right order of $L_p^{(np)}$ is given by

$$\xi^{-1} \begin{pmatrix} O_p & \pi^{-1} O_p \\ \pi O_p & O_p \end{pmatrix} \xi .$$

3. Quinary quadratic space over a field. Take two positive rational integers $a_i > 0$ for $i = 1, 2$. We take a quinary quadratic space $W = \sum_{i=1}^{5} \mathbb{Q} e_i$ over $\mathbb{Q}$ where the metric Q of W is given so that e_i are orthogonal with each other and $Q(e_1) = 1$, $Q(e_2) = 1$, $Q(e_3) = a_1$, $Q(e_4) = a_2$, $Q(e_5) = a_1 a_2$. The even Clifford algebra $C_2(W)$ of W is by definition given by

$$C_2(W) = \mathbb{Q} \oplus \left(\sum_{1 \le i < j \le 5} \mathbb{Q}\, e_i e_j \right) \oplus \left(\sum_{1 \le i < j < k < l \le 5} \mathbb{Q}\, e_i e_j e_k e_l \right)$$

with relations $e_i^2 = Q(e_i) 1 \in \mathbb{Q}$ and $e_i e_j + e_j e_i = 0$ $(i \neq j)$. If we put $\alpha = (e_4 e_5)/a_2$, $\beta = (e_3 e_5)/a_1$, then $\alpha\beta = e_3 e_4 = -\beta\alpha$ and we have $\alpha^2 = -a_1$, $\beta^2 = -a_2$. So the algebra $B = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$ is a definite quaternion algebra over $\mathbb{Q}$ and any definite quaternion algebra is written in this way. Also the subspace

$$C_0 = \mathbb{Q} + \mathbb{Q} e_1 e_2 + \mathbb{Q} e_2 e_3 e_4 e_5 + \mathbb{Q} e_1 e_3 e_4 e_5 \subset C_2(W)$$

is an algebra isomorphic to $M_2(\mathbb{Q})$ by identifying

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad e_1 e_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$(e_2 e_3 e_4 e_5)/(a_1 a_2) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad (e_1 e_3 e_4 e_5)/(a_1 a_2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$$

Inside $C_2(W)$, the above B and C_0 commute with each other and by these identifications, we can regard $C_2(W) = B \otimes_{\mathbb{Q}} C_0 = M_2(B)$. Natural involution on the whole Clifford algebra $C(W)$ is defined by $e_{i_1} \dots e_{i_r} \to e_{i_r} \dots e_{i_1}$ and we can see that for $b \in M_2(B) \cong C_2(W)$, this is given by $b \to b^*$. By definition, the even Clifford group Γ_2 of (W, Q) is the group of elements $g \in C_2(W)^\times$ such that $g^{-1} w g \in W$ for any $w \in W$, where we regard W as a subspace of

Clifford algebra $C(W)$. It is well known that $gg^* \in \mathbb{Q}^\times$ for any $g \in \Gamma_2$. If we embed W to $V = e_1e_2e_3e_4e_5W \subset C_2(W)$, then since $e_1e_2e_3e_4e_5$ generates the center of $C(W)$, we also have $g^{-1}vg \in V$ for all $v \in V$ and $g \in \Gamma_2$. By the above identification, we see that

$$W \cong V = \left\{ \begin{pmatrix} t & r \\ \overline{r} & -t \end{pmatrix} ; t \in \mathbb{Q}, r \in B \right\} .$$

We denote by G the group of hermitian similitudes of B^2 as before. This can be regarded as a subset of $M_2(B) = C_2(W)$, and for any $v \in V$, we have $g^{-1}vg = n(g)g^*vg$. Since this is invariant by $*$ and its reduced trace is zero, we have $g^{-1}vg \in V$ again. This means that $G = \Gamma_2$ as well known. The inner automorphism $w \longrightarrow g^{-1}wg$ induces a homomorphism of G to $SO(W)$. Actually we have an isomorphism $G/\mathbb{Q}^\times \cong SO(W)$, where $\mathbb{Q}^\times$ means the center $\{c1_2; c \in \mathbb{Q}^\times\}$ of G. (See for example [3] Chapter I §5, or [10]).

The natural quadratic form on this space V induced from $C_2(W)$ is given by $Q(v) = vv^* = t^2 + N(r)$ for $v \in V$. Even if we change the quadratic form Q by a constant multiple, which we will do later, obviously the relation $G/\mathbb{Q}^\times \cong SO(V)$ does not change.

4. Quinary lattices over integers. From now on, for the sake of simplicity, we assume that the discriminant D of B is odd throughout the paper. We fix a positive divisor D_1 of D and put $D_2 = D/D_1$. We sometimes identify V in the last section with $V_0 = \mathbb{Q} \oplus B$. We slightly change the quadratic form Q on V and define it by $Q(t, r) = (t^2 + N(r))/D_2$ for $t \in \mathbb{Q}$ and $r \in B$. We define the binary form B_Q associated with Q by

$$B_Q((t_1, r_1), (t_2, r_2)) = (2t_1t_2 + Tr(r_1\overline{r_2}))/D_2$$

for $(t_i, r_i) \in \mathbb{Q} \oplus B$, so we have $B_Q((t, r), (t, r)) = 2Q(t, r)$. The discriminant of (V, Q) is defined to be $\det(B_Q(f_i, f_j))$ for a basis $\{f_i\}$ of V over $\mathbb{Q}$ up to a multiple of $(\mathbb{Q}^\times)^2$. It is obvious that the discriminant of $(V, \mathbb{Q})$ is $2D^2/D_2^5 \equiv 2D_2 \bmod (\mathbb{Q}^\times)^2$. If we write $v \in V$ by a matrix as in the last secton, then for $v \in V$, we have $Q(v) = -\det(v)/D_2$ and we also have $v^2/D_2 = vv^*/D_2 = Q(v)1_2$. Now in order to define a genus of this quadratic space, we consider several $\mathbb{Z}_p$ lattices in $V_p = V \otimes_{\mathbb{Q}} \mathbb{Q}_p$. To establish a connection with G type numbers, we must consider the stablizers of these lattices in G_p and their actions on the right orders of quaternion hermitian lattices. First we consider the case $p \nmid D_2$. In this case, we put

$$M_p = \left\{ \begin{pmatrix} t & r \\ \overline{r} & -t \end{pmatrix} ;\ t \in \mathbb{Z}_p, r \in O_p \right\} \cong \mathbb{Z}_p \oplus O_p \subset V_p . \tag{1}$$

LEMMA 4.1. *Assume that $p \nmid D_2$ and fix $g \in G_p$. Then $gM_pg^{-1} = M_p$ if and only if $gM_2(O_p)g^{-1} = M_2(O_p)$.*

PROOF. Denote by R_p^* the ring generated by M_p and 1_2 over $\mathbb{Z}_p$. We will show that $R_p^* = M_2(O_p)$. Since $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in M_p$, we have $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in R_p^*$. In the same way we have $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 2 \end{smallmatrix}\right) \in R_p^*$. We have

$$\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & r \\ \overline{r} & 0 \end{pmatrix} = \begin{pmatrix} 0 & 2r \\ 0 & 0 \end{pmatrix} \in R_p^*,$$

$$\begin{pmatrix} 0 & r \\ \overline{r} & 0 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 2\overline{r} & 0 \end{pmatrix} \in R_p^*$$

for any $r \in O_p$. In particular we have $\left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right) \in R_p^*$ and we have

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & r \\ \overline{r} & 0 \end{pmatrix} = \begin{pmatrix} 2\overline{r} & 0 \\ 0 & 0 \end{pmatrix} \in R_p^*,$$

$$\begin{pmatrix} 0 & r \\ \overline{r} & 0 \end{pmatrix}\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 2\overline{r} \end{pmatrix} \in R_p^*$$

for any $r \in O_p$. So we have $2M_2(O_p) \subset R_p^*$. So if $p \neq 2$, then we have $M_2(O_p) = R_p^*$. Next, we assume that $p = 2$. Since we assumed that D is odd, we have $B_2 \cong M_2(\mathbb{Q}_2)$ and we may assume $O_2 = M_2(\mathbb{Z}_2)$. We have

$$\begin{pmatrix} 0 & \overline{r_1} \\ r_1 & 0 \end{pmatrix}\begin{pmatrix} 0 & r_2 \\ \overline{r_2} & 0 \end{pmatrix} = \begin{pmatrix} \overline{r_1} \cdot \overline{r_2} & 0 \\ 0 & r_1 r_2 \end{pmatrix} \in R_2^*,$$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & r_3 \\ \overline{r_3} & 0 \end{pmatrix} = \begin{pmatrix} \overline{r_3} & 0 \\ 0 & r_3 \end{pmatrix} \in R_2^*,$$

$$\begin{pmatrix} \overline{r_1} \cdot \overline{r_2} & 0 \\ 0 & r_1 r_2 \end{pmatrix}\begin{pmatrix} \overline{r_3} & 0 \\ 0 & r_3 \end{pmatrix} = \begin{pmatrix} \overline{r_1} \cdot \overline{r_2} \cdot \overline{r_3} & 0 \\ 0 & r_1 r_2 r_3 \end{pmatrix} \in R_2^*.$$

Here if we put $r_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $r_2 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $r_3 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, then we have $r_1 r_2 r_3 = 1_2$ and

$$\overline{r_1} \cdot \overline{r_2} \cdot \overline{r_3} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

So if we put

$$u = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

then we have $u \in R_2^*$. Adding -1_4 to this, we see that

$$u_1 = -1_4 + u = \begin{pmatrix} U & 0 \\ 0 & 0 \end{pmatrix} \in R_2^*$$

where $U = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right) \in GL_2(\mathbb{Z}_2)$. Multiplying u_1 to $\left(\begin{smallmatrix} 0 & r \\ \overline{r} & 0 \end{smallmatrix}\right)$ from left or right and making r run over $O_2 = M_2(\mathbb{Z}_2)$, we see that $\left(\begin{smallmatrix} 0 & O_2 \\ 0 & 0 \end{smallmatrix}\right) \subset R_2^*$ and $\left(\begin{smallmatrix} 0 & 0 \\ O_2 & 0 \end{smallmatrix}\right) \subset R_2^*$. By this, we see easily that $M_2(O_2) \subset R_2^*$ by taking a suitable multiplication. But since $M_2 \subset M_2(O_2)$, we have $R_2^* \subset M_2(O_2)$, so $R_2^* = M_2(O_2)$. Now for any $p \nmid D_2$, if $gM_pg^{-1} = M_p$, obviously we have

$gM_pg^{-1} \subset M_2(O_p)$, and since M_p generates $M_2(O_p)$, we have $gM_2(O_p)g^{-1} \subset M_2(O_p)$. Since $gM_2(O_p)g^{-1}$ is maximal, we have $gM_2(O_p)g^{-1} = M_2(O_p)$. So we proved "only if" part. On the other hand, since $M_2(O_p) \cap V_p = M_p$ and V_p is invariant by G_p, the converse is also true. □

Now we consider the case $p \mid D_2$, which we should relate to $L_p^{(np)}$. In order to simplify treatment of $L_p^{(np)}$ for $p|D_2|D$, we define

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

Taking $\xi \in GL_2(O_p)$ such that $\xi\xi^* = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ as before, we have $G_p = \xi^{-1}G_p^*\xi$. We put $V_p^* = \xi V_p \xi^{-1}$. Then it is clear that G_p^* acts on V_p^* by gvg^{-1} for $v \in V_p^*$ and $g \in G_p^*$. If we put $B_p^0 = \{b \in B_p;\ Tr(b) = 0\}$, then we have

$$V_p^* = \left\{ \begin{pmatrix} y & t \\ s & -y \end{pmatrix};\ t, s \in \mathbb{Q}_p, y \in B_p^0 \right\}.$$

Indeed, put $v_1 = \xi v \xi^{-1}$ for $v \in V_p$. Then since $v = v^*$, we have $v = \xi^{-1}v_1\xi = \xi^* v_1^* \xi^{-*}$, so $v_1\xi\xi^* = \xi\xi^* v_1^*$. If we write $v_1 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(B_p)$, then the above relation means that $\overline{b} = b$, $\overline{c} = c$, $d = \overline{a}$. Since $Tr(v) = 0$, we also have $Tr(v_1) = 0$ and we have $0 = Tr(a + d) = 2Tr(a)$, so we are done. Here the quadratic form Q^* on V_p^* is induced from v^2/D_2 so we should put

$$Q^*(v_1) = v^2/D_2 = v_1^2/D_2 = (st + y^2)/D_2 .$$

The associated bilinear form B_Q^* is given by

$$B_Q^*\left(\begin{pmatrix} y_1 & t_1 \\ s_1 & -y_1 \end{pmatrix}, \begin{pmatrix} y_2 & t_2 \\ s_2 & -y_2 \end{pmatrix} \right) = (y_1y_2 + y_2y_1 + s_1t_2 + t_1s_2)/D_2 .$$

For $g \in G_p^*$, we have $g^{-1}V_p^*g = V_p^*$ and $B_Q^*(g^{-1}v_1g, g^{-1}v_2g) = B_Q^*(v_1, v_2)$ for any v_1, $v_2 \in V_p^*$. Now we put $O_p^0 = \{y \in O_p : Tr(y) = 0\}$ and define a lattice K_p^* in V_p^* by

$$K_p^* = \left\{ \begin{pmatrix} y & t \\ ps & -y \end{pmatrix};\ t, s \in \mathbb{Z}_p, y \in O_p^0 \right\}.$$

We also define the dual lattice of K_p^* by

$$K_p = \left\{ v_2 = \begin{pmatrix} y & t \\ s & -y \end{pmatrix} \in V_p^*; B^*(v_2, v_1) \in \mathbb{Z}_p \text{ for any } v_1 \in K_p^* \right\}.$$

Since $p \neq 2$ by our assumption, we have $O_p^0 = \mathbb{Z}_p\varepsilon + \mathbb{Z}_p\pi + \mathbb{Z}_p\pi\varepsilon$ for some ε with $\pi\varepsilon = -\varepsilon\pi$ and $\varepsilon^2 \in \mathbb{Z}_p^\times$. So if we note that $D_2 \in p\mathbb{Z}_p^\times$, it is easy to see that

$$(2) \qquad K_p = \left\{ \begin{pmatrix} y & t \\ ps & -y \end{pmatrix};\ t, s \in \mathbb{Z}_p, y \in \pi O_p \cap B_p^0 \right\} \subset V_p^* .$$

For $g \in G_p^*$, it is obvious that we have $g^{-1}K_p g = K_p$ if and only if $g^{-1}K_p^* g = K_p^*$. We put

$$R_p^{'} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} O_p & O_p \\ pO_p & O_p \end{pmatrix} ; a - \overline{d} \in \pi O_p \right\} .$$

LEMMA 4.2. *Assume p is odd. Then the subring of $M_2(B_p)$ generated over $\mathbb{Z}_p$ by the unit matrix 1_2 and K_p^* is $R_p^{'}$.*

PROOF. It is obvious that R_p' is a ring, noting that $xy - yx \in \pi O_p$ for any $x, y \in O_p$. We also have $K_p^* \subset R_p'$. Denote by R_p^* the subring of R_p' generated by 1_2 and K_p^* over $\mathbb{Z}_p$. Since $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) \in K_p^*$, we have $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} y & 0 \\ 0 & -y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & -y \\ 0 & 0 \end{smallmatrix}\right) \in R_p^*$ for any $y \in O_p^0$. Since we assumed that p is odd, we have $O_p = \mathbb{Z}_p + O_p^0$. Since we have $\left(\begin{smallmatrix} 0 & t-y \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & t \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 & -y \\ 0 & 0 \end{smallmatrix}\right) \in R_p^*$ for any $t \in \mathbb{Z}_p$ and $y \in O_p^0$, we have $\left(\begin{smallmatrix} 0 & O_p \\ 0 & 0 \end{smallmatrix}\right) \subset R_p^*$. Since we have $\left(\begin{smallmatrix} 0 & 0 \\ p & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} y & 0 \\ 0 & -y \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ py & 0 \end{smallmatrix}\right) \in R_p^*$ for any $y \in O_p^0$, we see $\left(\begin{smallmatrix} 0 & 0 \\ pO_p & 0 \end{smallmatrix}\right) \in R_p^*$ in the same way. Since p is odd, O_p is written as

$$\mathbb{Z}_p + \mathbb{Z}_p\varepsilon + \mathbb{Z}_p\pi + \mathbb{Z}_p\varepsilon\pi$$

where $\varepsilon^2 = u \in \mathbb{Z}_p^\times$ such that $\mathbb{Q}_p(\varepsilon)$ is unramified over $\mathbb{Q}_p$, $\pi^2 = -p$ and $\pi\varepsilon = -\varepsilon\pi$. So we have

$$\begin{pmatrix} \varepsilon & 0 \\ 0 & -\varepsilon \end{pmatrix} \begin{pmatrix} \pi & 0 \\ 0 & -\pi \end{pmatrix} = \begin{pmatrix} \varepsilon\pi & 0 \\ 0 & \varepsilon\pi \end{pmatrix} \in R_p^* .$$

Since we have $\left(\begin{smallmatrix} \varepsilon\pi & 0 \\ 0 & -\varepsilon\pi \end{smallmatrix}\right) \in R_p^*$ and p is odd, we have

$$\begin{pmatrix} \varepsilon\pi & 0 \\ 0 & 0 \end{pmatrix} = \frac{1}{2}\left(\begin{pmatrix} \varepsilon\pi & 0 \\ 0 & \varepsilon\pi \end{pmatrix} + \begin{pmatrix} \varepsilon\pi & 0 \\ 0 & -\varepsilon\pi \end{pmatrix} \right) \in R_p^* .$$

So we also have $\left(\begin{smallmatrix} 0 & 0 \\ 0 & \varepsilon\pi \end{smallmatrix}\right) \in R_p^*$. Since $\varepsilon(\varepsilon\pi) = u\pi \in \mathbb{Z}_p^\times\pi$, we see that $\left(\begin{smallmatrix} \pi & 0 \\ 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 0 \\ 0 & \pi \end{smallmatrix}\right) \in R_p^*$ by the same argument. Taking squares of these, we see $\left(\begin{smallmatrix} p\mathbb{Z}_p & 0 \\ 0 & p\mathbb{Z}_p \end{smallmatrix}\right) \in R_p^*$. Since $p\left(\begin{smallmatrix} \varepsilon & 0 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \varepsilon\pi & 0 \\ 0 & \varepsilon\pi \end{smallmatrix}\right)\left(\begin{smallmatrix} -\pi & 0 \\ 0 & 0 \end{smallmatrix}\right) \in R_p^*$, we also have $\left(\begin{smallmatrix} p\mathbb{Z}_p\varepsilon & 0 \\ 0 & 0 \end{smallmatrix}\right) \subset R_p^*$ and we also have $\left(\begin{smallmatrix} 0 & 0 \\ 0 & p\mathbb{Z}_p \end{smallmatrix}\right) \subset R_p^*$. So we have $\left(\begin{smallmatrix} a+\pi O_p & O_p \\ pO_p & \overline{a}+\pi O_p \end{smallmatrix}\right) \subset R_p^*$ for $a \in \mathbb{Z}_p + \mathbb{Z}_p\varepsilon$. Here the set of the left hand side is nothing but $R_p^{'}$, so $R_p^{'} \subset R_p^*$ and hence $R_p' = R_p^*$. □

We also put

$$R_p = \begin{pmatrix} O_p & \pi^{-1}O_p \\ \pi O_p & O_p \end{pmatrix} .$$

LEMMA 4.3. *If $gR_p^{'}g^{-1} \subset R_p^{'}$ for $g \in G_p^*$, then we have $gR_pg^{-1} \subset R_p$.*

PROOF. For any $g \in G_p^*$ and $x \in B_p$, we put

$$u(g,x) = g \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} g^{-1}, \qquad v(g,x) = g \begin{pmatrix} 0 & 0 \\ x & 0 \end{pmatrix} g^{-1}.$$

If we assume that g satifies the condition in the Lemma, then we have $u(g,x) \in R_p'$ for any $x \in O_p$. Now we show $u(g,y) \in R_p$ for any $y \in \pi^{-1}O_p$ for such g. Since $g \in G_p^*$, we have $g \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) {}^t\overline{g} = n(g) \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for some $n(g) \in \mathbb{Q}_p^\times$. So if we put $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then $g^{-1} = n(g)^{-1} \left(\begin{smallmatrix} \overline{d} & \overline{b} \\ \overline{c} & \overline{a} \end{smallmatrix}\right)$. Writing $n(g)^{-1} = \lambda$, we have

$$u(g,y) = \lambda \begin{pmatrix} ay\overline{c} & ay\overline{a} \\ cy\overline{c} & cy\overline{a} \end{pmatrix} .$$

By the condition $u(g,1) \in R_p'$, it is necessary that the following conditions are satisfied.

$$\begin{aligned} \mathrm{ord}(\lambda) + \mathrm{ord}(a) + \mathrm{ord}(c) &\geq 0\,, \\ \mathrm{ord}(\lambda) + 2\,\mathrm{ord}(a) &\geq 0\,, \\ \mathrm{ord}(\lambda) + 2\,\mathrm{ord}(c) &\geq 2\,, \end{aligned}$$

where we denote by ord(*) the order of the elements with respect to the prime element π of O_p. Adding the second and the third inequality, we have

$$\mathrm{ord}(\lambda) + \mathrm{ord}(a) + \mathrm{ord}(c) \geq 1\,.$$

Then for $y \in \pi^{-1}O_p$, we have

$$\begin{aligned} \mathrm{ord}(\lambda) + \mathrm{ord}(a) + \mathrm{ord}(c) + \mathrm{ord}(y) &\geq 1 - 1 = 0\,, \\ \mathrm{ord}(\lambda) + 2\mathrm{ord}(a) + \mathrm{ord}(y) &\geq -1\,, \\ \mathrm{ord}(\lambda) + 2\mathrm{ord}(c) + \mathrm{ord}(y) &\geq 1\,, \end{aligned}$$

so we have $u(g,y) \in R_p$. In the same way we can show that if $v(g,p) \in R_p'$ then $v(g,y) \in R_p$ for any $y \in \pi O_p$. Indeed, we have

$$v(g,y) = \lambda \begin{pmatrix} by\overline{d} & by\overline{b} \\ dy\overline{d} & dy\overline{b} \end{pmatrix} .$$

So if $v(g,p) \in R_p'$, then since $\mathrm{ord}(p) = 2$ we have

$$\begin{aligned} \mathrm{ord}(\lambda) + \mathrm{ord}(b) + \mathrm{ord}(d) + 2 \geq &\quad 0\,, \\ \mathrm{ord}(\lambda) + 2\mathrm{ord}(b) + 2 \geq &\quad 0\,, \\ \mathrm{ord}(\lambda) + 2\mathrm{ord}(d) + 2 \geq &\quad 2\,. \end{aligned}$$

Adding the second and the third inequality, we have

$$\mathrm{ord}(\lambda) + \mathrm{ord}(b) + \mathrm{ord}(d) \geq -1\,.$$

So for $y \in \pi O_p$, we have

$$\mathrm{ord}(\lambda) + \mathrm{ord}(b) + \mathrm{ord}(d) + \mathrm{ord}(y) \geq 0\,,$$

$$\mathrm{ord}(\lambda) + 2\mathrm{ord}(b) + \mathrm{ord}(y) \geq -1\,,$$
$$\mathrm{ord}(\lambda) + 2\mathrm{ord}(d) + \mathrm{ord}(y) \geq 1\,.$$

This means that $v(g, y) \in R_p$. Now for any $x \in \pi^{-1}O_p$ and $y \in \pi O_p$, we have

$$g \begin{pmatrix} xy & 0 \\ 0 & 0 \end{pmatrix} g^{-1} = u(g, x)v(g, y) \in R_p$$
$$g \begin{pmatrix} 0 & 0 \\ 0 & yx \end{pmatrix} g^{-1} = v(g, y)u(g, x) \in R_p\,.$$

Since $(\pi O_p)(\pi^{-1}O_p) = O_p$, we have shown that $gR_pg^{-1} \subset R_p$. □

COROLLARY 4.4. *Fix an element $g \in G_p^*$. Then the following three conditions are equivalent.*

(i) $gK_pg^{-1} = K_p$. (ii) $gK_p^*g^{-1} = K_p^*$. (iii) $gR_pg^{-1} = R_p$.

PROOF. The equivalence of (i) and (ii) is obvious since they are dual. So we see equivalence of (ii) and (iii). If $gK_p^*g^{-1} \subset K_p^*$, then $gR_p^{'}g^{-1} \subset R_p^{'}$ by Lemma 4.2. So by Lemma 4.3, we have $gR_pg^{-1} \subset R_p$, but since R_p is a maximal order, we have $gR_pg^{-1} = R_p$. Conversely if $gR_pg^{-1} = R_p$, then since $R_p \cap V_p^* = K_p^*$ and $gV_p^*g^{-1} = V_p^*$, we have $gK_p^*g^{-1} = K_p^*$. □

For any $0 < D_1|D$ and $D_2 = D/D_1$, the quadratic form Q on V is taken to be $Q(v) = v^2/D_2$ as before. We define the set $\mathcal{M}(D_1, D_2)$ of lattices M_0 in V such that for each prime p, the lattice $g_p^{-1}(M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p)g_p$ for some $g_p \in G_p$ is equal to the lattice given as follows.

(i) For $p \nmid D_2$, the lattice M_p in V_p defined by (1).

(ii) For $p|D_2$, the lattice $\xi^{-1}K_p\xi$, where K_p is defined by (2).

The global lattice $\mathbb{Z}+O$ in V is of course equivalent to M_p locally for all primes p, and since the collection of local lattices (i) and (ii) differs from this at only a finite number of primes, there exists a global lattice M_0 in V whose localizations are M_p and $\xi^{-1}K_p\xi$ for $p \nmid D_2$ and $p|D_2$ respectively by a well known theorem (for example, see [16] Chapter V Section 2 Theorem 2). So the set $\mathcal{M}(D_1, D_2)$ is non empty and there exists $M_0 \in \mathcal{M}(D_1, D_2)$ such that elements of G_A which fix M_0 are exactly those elements which fix the right order of a lattice in the genus $\mathcal{L}(D_1, D_2)$ of maximal lattices in B^2 which is O_p^2 for $p|D_1$ and $(\pi O_p, O_p)\xi$ for $p|D_2$. Here we note that the right order of O_p^2 is $M_2(O_p)$ and the right order of $(\pi O_p, O_p)\xi$ is $\xi^{-1}R_p\xi$. We say that two lattices M and $M' \in \mathcal{M}(D_1, D_2)$ are in the same class if $M = M'g$ for some $g \in O(V)$ and in the same proper class if $M = M'g$ for some $g \in SO(V)$, where $O(V)$ and $SO(V)$ are the orthogonal group and the special orthogonal group over $\mathbb{Q}$, respectively. Since $\dim V = 5$ is odd, we have $O(V)/SO(V) = \{\pm id.\}$ and the class and the proper class are the same. Since the natural map $G_p \longrightarrow SO(V_p)$ is surjective, the set $\mathcal{M}(D_1, D_2)$ is a genus in the usual sense of the quadratic space V, and the number of classes in $\mathcal{M}(D_1, D_2)$ is called the class number of this genus. By the above lemmas, we have the following theorem.

THEOREM 4.5. *The G-type number of the genus $\mathcal{L}(D_1, D_2)$ in B^2 is equal to the class number of the genus $\mathcal{M}(D_1, D_2)$ in V.*

To compare the above results with Asai's class number formula in [2], we study the above local lattices a little more closely. The discriminant of a lattice $M_{0,p} = M_0 \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is defined to be $\det(B(e_i, e_j))$ for a basis $\{e_i\}$ of $M_{0,p}$ over $\mathbb{Z}_p$ and this is determined up to a multiple of $(\mathbb{Z}_p^\times)^2$. The discriminant of M_p for $p \nmid D_2$ is $2D^2/D_2^5 \equiv 2D_1^2 D_2 \bmod (\mathbb{Z}_p^\times)^2$ since we assumed $D_2 \in \mathbb{Z}_p^\times$ here. In particular, if $p \nmid D$ and $p \neq 2$, then M_p is unimodular and uniquely determined by the discriminant ([9]). When $p = 2$, since we are assuming that D is odd, we have $2 \nmid D$. So $O_2 = M_2(\mathbb{Z}_2)$, and M_2 is a lattice isomorphic to

$$(2D_2^{-1}) \perp D_2^{-1}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp D_2^{-1}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \cong (2D_2) \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

if we express it by the Gram matrix. For p such that $p|D_2$, we define K_p^* and K_p as before, taking the quadratic form as $(pst + y^2)/D_2 = -\det(v_1)/D_2$ for $v_1 = \left(\begin{smallmatrix} y & t \\ ps & -y \end{smallmatrix}\right) \in K_p^*$. The discriminant of K_p^* is $2p^4/D_2^5$ up to $(\mathbb{Z}_p^\times)^2$. Since $p|D_2$, p is odd, and D_2/p is coprime to p, we have $2p^4/D_2^5 \equiv 2/(D_2(D_2/p)^4) \equiv 2/D_2 \equiv 1/2D_2 \bmod (\mathbb{Z}_p^\times)^2$ up to $(\mathbb{Z}_p^\times)^2$. The discriminant of K_p is obviously the inverse of that of K_p^*, so it is equal to $2D_2 \equiv 2D_1^2 D_2$ up to $(\mathbb{Z}_p^\times)^2$.

5. Explicit formulas. When the discriminant D of B is odd, the class number formula of $\mathcal{M}(D_1, D_2)$ for $D_1 D_2 = D$ is given by Theorem 4.17 in Teruaki Asai [2]. Since the discriminant of our lattice is $2D_1^2 D_2$, we see that the conditions of [2] Theorem 4.17 on lattices are fulfilled by [2] Lemma 4.13. (For $p|D$ and for $p = 2$, we see easily that the Hasse invariant $S(V_p)$ of V_p is -1.) So we can also give the G-type number of $\mathcal{L}(D_1, D_2)$ by virtue of Theorem 4.5 in this paper. The general explicit results are complicated. The case when D is a prime, the result is slightly easier and we have an application to geometry. The formula for the type number of $\mathcal{L}(p, 1)$ was explained in [6]. Here we write down the type number of $\mathcal{L}(1, p)$.

We prepare some notation. We denote by χ the character associated with the quadratic field extension $Q(\sqrt{p})/Q$, that is,

$$\chi(n) = \left(\frac{Q(\sqrt{p})}{n}\right).$$

We denote by $B_{2,\chi}$ the generalized Bernoulli number associated with χ. This is given explicitly as follows (see [1]).

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

where f is the conductor of χ. For an integer $d > 0$, we denote by $h(\sqrt{-d})$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. We put $w(p) = 0$ if $p \equiv \pm 1 \bmod 8$ and $w(p) = 1$ if $p \equiv \pm 3 \bmod 8$. So we have $(-1)^{w(p)} = \left(\frac{2}{p}\right)$. Also we have $\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right)$. Teruaki Asai's class number formula in [2] Corollary 4.18 exactly gives the type number of $\mathcal{L}(1, p)$. We reproduce it below for the readers convenience.

THEOREM 5.1. *We have* $T(1,2) = T(1,3) = T(1,5) = 1$.
For $p \geq 7$ *such that* $p \equiv 1 \bmod 4$, *we have*

$$\begin{aligned}
T(1,p) = & \frac{p^2-1}{2^7 3^2 5} + \frac{1}{2^6 \cdot 3}\left(9 - 2\left(\frac{2}{p}\right)\right) B_{2,\chi} + \frac{1}{2^5} h(\sqrt{-p}) + \frac{1}{2^4} h(\sqrt{-2p}) \\
& + \frac{1}{2^3 \cdot 3}\left(3 + \left(\frac{2}{p}\right)\right) h(\sqrt{-3p}) + \frac{5}{2^6 \cdot 3}(p-1) \\
& + \frac{1}{2^4}\left(1 - \left(\frac{2}{p}\right)\right) + \frac{1}{2^4 3^2}\left(p - \left(\frac{-3}{p}\right)\right)\left(3 + \left(\frac{-3}{p}\right)\right) \\
& + \frac{1}{2^3 3}\left(1 - \left(\frac{-3}{p}\right)\right) + \frac{1}{2 \cdot 5}\left(1 - \left(\frac{p}{5}\right)\right).
\end{aligned}$$

For $p \geq 7$ *such that* $p \equiv 3 \bmod 4$, *we have*

$$\begin{aligned}
T(1,p) = & \frac{1}{2^7 \cdot 3^2 \cdot 5}(p^2-1) + \frac{1}{2^6 \cdot 3} B_{2,\chi} \\
& + \frac{1}{2^5}\left(1 - \left(\frac{2}{p}\right)\right) h(\sqrt{-p}) + \frac{1}{2^4} h(\sqrt{-2p}) + \frac{1}{2^3 \cdot 3} h(\sqrt{-3p}) \\
& + \frac{1}{2^6}(p+1) + \frac{1}{2^4}\left(1 - \left(\frac{2}{p}\right)\right) + \frac{1}{3^2 2^4}\left(p - \left(\frac{-3}{p}\right)\right)\left(3 + \left(\frac{-3}{p}\right)\right) \\
& + \frac{1}{2 \cdot 5}\left(1 - \left(\frac{p}{5}\right)\right).
\end{aligned}$$

On the other hand, the class number $H(1,p)$ of the non-principal genus is known in [4] (II). We have $H(1,2) = H(1,3) = H(1,5) = 1$ and for primes $p \geq 7$ we have

$$\begin{aligned}
H(1,p) = & \frac{1}{2^6 \cdot 3^2 \cdot 5}(p^2-1) + \frac{1}{2^3 3^2}(3p-1) + \frac{p-3}{2^3 3^2}\left(\frac{-3}{p}\right) \\
& + \frac{1}{5}\left(1 - \left(\frac{p}{5}\right)\right) + \frac{1}{2^3}\left(1 - \left(\frac{2}{p}\right)\right) \\
& + \begin{cases} \dfrac{5(p-1)}{2^5 3} + \dfrac{1}{2^2 3}\left(1 - \left(\dfrac{-3}{p}\right)\right) & \text{if } p \equiv 1 \bmod 4, \\ \dfrac{p+1}{2^5} & \text{if } p \equiv 3 \bmod 4. \end{cases}
\end{aligned}$$

For the proof, see [4] (II), (III).

Now we consider the superspecial abelian variety $A = E^2$, where E is any fixed supersingular elliptic curve such that $End(E) = O \subset B$, where B is the definite quaternion algebra of discriminant p. Then Néron-Severi group $NS(A)$ is identified with the set of quaternion hermitian matrices in $M_2(O)$. We can essentially identify genera of quaternion hermitian lattices in B^2 as a subset of $NS(A)$. Among isomorphism classes over $\overline{F_p}$ of polarized abelian surfaces (A, λ) with $\lambda \in \mathcal{L}(1,p)$, exactly $2T(1,p) - H(1,p)$ of them have a model over $\mathbb{F}_p$ (see [5]). We denote by $\mathcal{A}_{2,1}$ the moduli of principally polarized abelian surfaces and by $\mathcal{S}_{2,1}$ the locus in $\mathcal{A}_{2,1}$ of principally polarized supersingular abelian surfaces. The number of irreducible components defined over $\mathbb{F}_p$ of $\mathcal{S}_{2,1}$ is also equal to $2T(1,p) - H(1,p)$ (see [5]) and explicitly given in the following theorem.

THEOREM 5.2. *The number $2T(1,p) - H(1,p)$ is given explicitly as follows. When $p = 2$, 3, 5, it is one. If $p \geq 7$, then for $p \equiv 1 \bmod 4$, we have*

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

and for $p \equiv 3 \bmod 4$, we have

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

NUMERICAL EXAMPLES.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
H	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4
T	1	1	1	1	1	2	2	2	2	3	3	5	4	5	4

p	53	59	61	67	71	73	79	83	89	97	101	103	107
H	6	5	8	8	6	10	9	8	10	14	12	13	11
T	6	5	8	8	6	10	9	8	10	14	12	13	11

p	109	113	127	131	137	139	149	151	157	163	167
H	16	14	17	14	18	19	20	21	26	24	20
T	16	14	17	14	18	19	20	21	26	24	19

p	173	179	181	191	193	197	199	211	223	227	229
H	25	22	31	24	34	30	31	34	37	32	43
T	24	22	31	24	34	29	31	34	36	30	43

p	233	239	241	251	257	263	269	271	277	281
H	38	34	46	37	44	40	47	49	57	50
T	37	33	46	36	42	38	45	48	56	49

COROLLARY 5.3. (i) *If $p < 167$, then we have*

$$T(1,p) = H(1,p) = 2T(1,p) - H(1,p).$$

(ii) *We have $2T(1,p) - H(1,p) > 0$ for all primes p.*

PROOF. The first assertion follows from the above table. In the formula of Theorem 5.2 above, all the terms except for $B_{2,\chi}$ are obviously non-negative. We also have $B_{2,\chi} > 0$. This is proved by $L(2,\chi) > 0$ and the formula for $L(2,\chi)$ by $B_{2,\chi}$ for a real quadratic character χ (see [1]), . □

For the principal genus, a similar formula for $2T(p,1) - H(p,1)$ was given in [6] as well as some application to geometry. By the above corollary, we can show that there exists an irreducible component defined over $\mathbb{F}_p$ of supersingular locus in the moduli of principally polarized abelian varietis of any fixed dimension. Such applications to supersingular geometry is explained in [5] by using [7], [8], [11], [12].

REFERENCES

[1] T. ARAKAWA, T. IBUKIYAMA AND M. KANEKO, Bernoulli numbers and zeta functions. With an appendix by Don Zagier. Springer Monographs in Mathematics. Springer, Tokyo, 2014. xii+274 pp.

[2] T. ASAI, The class number of positive definite quadratic forms, Japan. J. Math. 3 (1977), 239–296.

[3] M. EICHLER, Quadratische Formen und orthogonale Gruppen. Zweite Auflage. Die Grundlehren der mathematischen Wissenschaften, Band 63. Springer-Verlag, Berlin-New York, 1974. xii+222 pp.

[4] K. HASHIMOTO AND T. IBUKIYAMA, On class numbers of positive definite binary quaternion hermitian forms (I), J. Fac. Sci. Univ. Tokyo, Sec. IA 27 (1980), 549–601; (II) ibid.28 (1982), 695–699 (1982); (III) ibid.30 (1983), 393–401.

[5] T. IBUKIYAMA, Type numbers of quatenion hermitian forms and supersingular abelian varieties, Osaka J. Math. 55 (2018), 369–382.

[6] T. IBUKIYAMA AND T. KATSURA, On the field of definition of superspecial polarized abelian varieties and type numbers, Compositio Math. 91(1994), 37–46.

[7] T. KATSURA AND F. OORT, Families of supersingular abelian surfaces, Compositio Math. 62(1987), 107–167.

[8] T. KATSURA AND F. OORT, The class number of the principal genus of a positive definite quaternion hermitian space of dimension two and three, Algebraic geometry, Sendai, 1985, 1, 253–281, Adv. Stud. Pure Math. 10, North-Holland Publishing Co., Amsterdam; Kinokuniya Company Ltd., Tokyo, 1987.

[9] Y. KITAOKA, Arithmetic of quadratic forms. Cambridge Tracts in Mathematics, 106. Cambridge University Press, Cambridge, 1993. x+268 pp.

[10] M. KNESER, Quadratische Formen. Revised and edited in collaboration with Rudolf Scharlau. Springer-Verlag, Berlin, 2002. viii+164 pp.

[11] K. Z. LI AND F. OORT, Moduli of supersingular abelian varieties. Lecture Notes in Mathematics, 1680. Springer-Verlag, Berlin, 1998. iv+116 pp.

[12] F. OORT, Newton polygon strata in the moduli space of abelian varieties. Moduli of abelian varieties (Texel Island, 1999), 417–440, Progr. Math., 195, Birkhäuser, Basel, 2001.

[13] M. PETERS, Ternäre quadratische Formen und Quaternionenalgebra, Acta Arith. 15, (1968/69), 329–365.

[14] T. R. SHEMANSKE, Ternary quadratic forms and quaternion algebras. J. Number Theory 23 (1986), 203–209.

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

[16] A. WEIL, Basic Number Theory, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen Band 144, Springer-Verlag Berlin-Heidelberg 1967, xviii+294 pp.

DEPARTMENT OF MATHEMATICS
GRADUATE SCHOOL OF SCIENCE
OSAKA UNIVERSITY
MACHIKANEYAMA 1–1
TOYONAKA, OSAKA, 560–0043
JAPAN

E-mail address: ibukiyam@math.sci.osaka-u.ac.jp