Tôhoku Math. J.
45 (1993), 311–329

ON RATIONAL POINTS OF CURVES OF GENUS 3 OVER FINITE FIELDS

TOMOYOSHI IBUKIYAMA*

(Received January 29, 1992, revised September 9, 1992)

Abstract. Let F be any finite field with q elements such that q is the square of an odd prime. For each extension F' of odd (resp. even) degree over F, we shall show that there exists a curve of genus 3 defined over F' such that the number of F'-rational points attains the maximum (resp. minimum) of the Weil estimation.

For any curves C defined over finite fields $\boldsymbol{F}_q$ ($q=p^d$; p: prime), Weil [20] gave an estimate for the cardinality of the set $C(\boldsymbol{F}_q)$ of $\boldsymbol{F}_q$-rational points of C as follows:

$$|\sharp(C(\boldsymbol{F}_q))-1-q|\leq 2g\sqrt{q}$$

where $g=g(C)$ is the genus of the curve C. When q is a square, for a fixed q and variable g, very interesting phenomena occur and the upper bound and asymptotic behaviour for $g\rightarrow\infty$ were studied for example by Ihara [11], Manin-Valdut [12]. Now, Serre [19], [18] studied the bound for a fixed g and variable q. A part of his results says that for any square $q=p^{2e}$ when $g=1$, and for each square $q\neq 4$ or 9 when $g=2$, there exist curves C_1 and C_2 defined over $\boldsymbol{F}_q$ such that

$$\sharp(C_1(\boldsymbol{F}_q))=1+q+2gp^e\,,\qquad \sharp(C_2(\boldsymbol{F}_q))=1+q-2gp^e\,,$$

that is, there exist curves such that the number of $\boldsymbol{F}_q$-rational points attains Weil's maximum, or minimum. But it remained open, except for several small q and g, whether this is also true for any $g\geq 3$ and for almost all q. (Serre, loc. cit. When q is some power of 2, see also Oort [14].) In this paper, we shall show the following:

THEOREM 1. *For each odd prime p and each positive integer e, there exists a nonsingular irreducible curve C of genus* 3 *defined over $\boldsymbol{F}_p$ such that the number of $\boldsymbol{F}_{p^{2e}}$ rational points attains the maximum* (*resp. the minimum*) *of the Weil inequality for odd* (*resp. even*) *e, that is,*

$$\sharp(C(\boldsymbol{F}_{p^{2e}}))=1+p^{2e}+(-1)^{e+1}6p^e\,.$$

More precisely, there exists a curve C defined over $\boldsymbol{F}_p$ such that the Jacobian variety $J(C)$ of C is isomorphic over $\boldsymbol{F}_{p^2}$ to the product of three copies of a supersingular elliptic curve

* Partly supported by the Grants-in-Aid for Scientific as well as Co-operative Research, The Ministry of Education, Science and Culture, Japan.

1991 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G15, 14G05, 11E41.

E defined over $\boldsymbol{F}_p$.

This work is motivated by Professor Serre's letter [17], where he pointed out that, to obtain the above theorem, it is sufficient to show the existence of an (irreducible nonsingular) hyperelliptic curve (over any field) whose Jacobian is the product of supersingular elliptic curves. When $p \equiv 3 \bmod 4$, it is easy to show the existence of such curve, using the class number formula of ternary quaternion Hermitian forms by Hashimoto [3] (cf. Oort [14], [5]). In this case, we need not assume that e is odd. Also, when $p \equiv 3 \bmod 4$, it is known that the curve C: $x^4 + y^4 = z^4$ satisfies the conditions in our Theorem ([17], [14]). On the contrary, for general p, we do not know whether we can take a curve C in the above theorem so that C is hyperelliptic. Hence, we do not know whether there exists a curve C such that $\sharp(C(\boldsymbol{F}_{p^{2e}}))$ attains the minimum (resp. maximum) for odd (resp. even) e. The outline of the proof of the above theorem is as follows: We fix an odd prime number p and take a supersingular elliptic curve E defined over $\boldsymbol{F}_p$ such that $F^2 = -p\,\mathrm{id}_E$, where we denote by F the Frobenius endomorphism over $\boldsymbol{F}_p$ of E. (The existence of such a curve is due to Deuring [1].) Any principal polarization Θ on E^3 is defined over $\boldsymbol{F}_{p^2}$ (e.g. [9]). We can give a number-theoretical criterion whether (E^3, Θ) has a model (A, Θ') over $\boldsymbol{F}_p$ which is isomorphic to (E^3, Θ) *over* $\boldsymbol{F}_{p^2}$. It is known by Oort and Ueno [15] that any 3-dimensional principally polarized abelian variety is the Jacobian of a 'good' curve (which is, in general, reducible). If (A, Θ') as above is the Jacobian of an irreducible curve C, (i.e., if Θ is indecomposable), then by Serre [17] or Oort [14], we can take a model C_0 of C such that C_0 is defined over $\boldsymbol{F}_p$ and that the Jacobian variety $J(C)$ is isomorphic to (A, Θ') over $\boldsymbol{F}_{p^2}$. By calculating the *mass formula* for elements of a certain type of the group G of quaternion hermitian similitudes, we can show the existence of such a principal polarization on E^3. Incidentally, a similar method cannot be applied in general for further study. That is, when $p \equiv 1 \bmod 4$, there exists no curve C of genus 3 defined over $\boldsymbol{F}_{p^2}$ such that the Jacobian variety $J(C) \cong E^3$ and that its Frobenius over $\boldsymbol{F}_{p^4}$ induces $-p^2$ in $J(C)$. (This is caused by the fact that, in this case, the automorphism group of $J(C)$ does not contain an element with characteristic polynomial $(x^2+1)^3$, cf. [3]).

In §1, we shall review algebraic geometry and give the criterion mentioned above. In §2, we shall give explicit results on the mass formula for some elements of the group G in Theorem 2. Sections 3 and 4 are devoted to the proof of Theorem 2. The calculation of local data we need for a calculation of the above mass will be given in §3. We encountered similar kind of calculations, for example, in [6], [3], [8]. Although this calculation is fairly elaborate, it is lengthy and the proof will be omitted here. The proofs of Theorem 2 and the above Theorem 1 will be completed in §4.

I would like to thank Professor Jean-Pierre Serre for explaning this problem and its subtle point in his letter [17] and also for valuable comments, and also Professor Toshiyuki Katsura for valuable discussions.

1. Review on algebraic geometry. We fix an odd prime p and a supersingular elliptic curve E such that the Frobenius endomorphism F of E over $\boldsymbol{F}_p$ satisfies $F^2 = -p\,\mathrm{id}_E$.

LEMMA 1.1. *Let $n \geq 2$ be a positive integer. An n-dimensional principally polarized abelian variety (E^n, Θ) rational over $\boldsymbol{F}_{p^2}$ has a model (A, Θ') such that it is both defined over $\boldsymbol{F}_p$ and also isomorphic to (E^n, Θ) over $\boldsymbol{F}_{p^2}$, if and only if there exists an endomorphism α of E^n which satisfies the following three conditions* (1), (2) *and* (3):

(1) $\alpha \in \mathrm{Aut}(E^n)\cdot F$,

(2) $\alpha^2 = -p\,\mathrm{id}_E$, *and*

(3) $\alpha^*(\Theta) \approx p\Theta$, *where we denote by $\approx$ the algebraic equivalence of divisors.*

PROOF. First, assume that there exists such a model (A, Θ'), and denote by f the isomorphism of (A, Θ') onto (E^n, Θ) defined over $\boldsymbol{F}_{p^2}$. Denote by σ the generator of the Galois group $\mathrm{Gal}(\boldsymbol{F}_{p^2}/\boldsymbol{F}_p)$. Then, if we set $\alpha = f\cdot f^{-\sigma}F$, this α satisfies the above conditions. In fact, we get $\Theta' \approx f^*(\Theta) \approx (f^\sigma)^*(\Theta^\sigma)$, which implies (3). On the other hand, for any endomorphism β of E^n, we get $F\cdot\beta = \beta^\sigma F$. Hence, we get (2). Conversely, assume that there exists an endomorphism α which satisfies (1), (2), and (3). By (1), we can put $\alpha = \varepsilon\cdot F$, where $\varepsilon \in \mathrm{Aut}(E^n)$. By (2), we get $\varepsilon^\sigma\varepsilon = \mathrm{id}_E$. By (3), we get $F^*\varepsilon^*(\Theta) \approx p\Theta = F^*(\Theta^\sigma)$, which implies $\varepsilon^*(\Theta) \approx \Theta^\sigma$ and ε is an isomorphism of (E^n, Θ) onto (E^n, Θ^σ). Hence, by the Weil criterion, we get a model (A, Θ') defined over $\boldsymbol{F}_p$ and an $\boldsymbol{F}_{p^2}$-rational isomorphism f of (A, Θ') onto (E^n, Θ). q.e.d.

LEMMA 1.2. *Assume that a principally polarized abelian variety (E^3, Θ) satisfies the conditions in Lemma* 1.1, *and that Θ is an indecomposable polarization. Then, there exists an irreducible curve C of genus three rational over $\boldsymbol{F}_p$ such that*

$$\sharp(C(\boldsymbol{F}_{p^2})) = p^2 + 1 + 6p\,.$$

PROOF. By Oort and Ueno [15], any (E^3, Θ) is the Jacobian of a good curve, and if Θ is indecomposable, then C is irreducible. Now, it has been shown by Serre [17] and Oort [14], using the Torelli Theorem, that, if any principally polarized abelian variety (A_0, Θ_0) rational over a field k is the Jacobian variety of a curve C_0 (over the algebraic closure of k), then we can take a model C of C_0 such that C is rational over k and that the Jacobian variety $J(C)$ of C is isomorphic to (A_0, Θ_0) over a quadratic extension of k. Going back to our situation, we get an irreducible curve C rational over $\boldsymbol{F}_p$ whose Jacobian is isomorphic to (A, Θ') and hence to (E^3, Θ) over $\boldsymbol{F}_{p^2}$. This means that the Frobenius endomorphism of $J(C)$ over $\boldsymbol{F}_{p^2}$ is $-p\,\mathrm{id}_{E^3}$. q.e.d.

2. Relation to the mass formula. In this section, we shall interpret Lemma 1.1 into an arithmetic theory of the quaternion Hermitian forms, explain how to show Theorem 1 by the mass formula, and then state the results on masses.

We put $\mathcal{O} = \mathrm{End}(E)$ and $B = \mathrm{End}(E) \otimes \boldsymbol{Q}$. Then, B is a definite quaternion algebra over $\boldsymbol{Q}$ with discriminant p, and $\mathcal{O}$ is a maximal order of B. As has been shown in [10], principal polarizations on E^n (E: the supersingular elliptic curve over $\boldsymbol{F}_p$ which we fixed) correspond bijectively to the set of classes of lattices in the principal genus $\mathscr{L}(n)$ of the n-ary positive definite quaternion Hermitian space B^n (with standard metric). We need notation to interpret the conditions in Lemma 1.1. We denote by $G=G(n)$ the group of quaternion Hermitian similitudes on B^n:

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

where $\lambda(g)$ is a positive rational number depending only on g. We denote by $G_A=G_A(n)$ the adelization of $G(n)$. For any place v of $\boldsymbol{Q}$, we denote by $G_v=G_v(n)$ the v-component of G_A. For any finite place v, denote by $\mathcal{O}_v$ the v-adic completion of $\mathcal{O}$ and define a compact subgroup U_v of G_v by

$$U_v=G_v\cap GL_n(\mathcal{O}_v)\,.$$

We also define a subgroup U of G_A by

$$U=G_\infty\times\prod_{v<\infty}U_v\,.$$

Now take the double coset decomposition

$$G_A=\coprod_{i=1}^{H}Ug_iG\qquad\text{(disjoint)}\,.$$

Then, the number H of these double cosets is equal to the class number of $\mathscr{L}(n)$ and a complete set of representatives $L_1,\dots,L_H$ of the classe of $\mathscr{L}(n)$ is given by

$$L_i=\mathcal{O}^n g_i\cap B^n\,.$$

LEMMA 2.1. *If $P=(E^n,\Theta)$ satisfies the condition in Lemma* 1.1, *then for the lattice L_i which corresponds to this P, there exists an element $g\in G(n)$ with $g^2=-p1_n$ such that $L_ig\subset L_i$ and that $g_igg_i^{-1}\in\pi U$.*

The proof is obvious.

Now, we shall review some mass formulas for G. We denote by Γ_i the automorphism group of the lattice L_i:

$$\mathrm{Aut}(L_i)=\Gamma_i=\{g\in G\,;L_ig=L_i\}\,.$$

In the adelic language, we get $\Gamma_i=G\cap g_i^{-1}Ug_i$. To simplify notation, for each $i\,(1\le i\le H)$, we denote by $T_i^n(\pi)$ the subset of $G(n)$ defined by:

$$T_i^n(\pi)=\{g\in G;\ g_igg_i^{-1}\in\pi U\text{ and }g^2=-p1_n\}\,,$$

and we denote by $M(n, L_i)$ the rational number

$$M(n, L_i)=\frac{\sharp(T_i^n(\pi))}{\sharp(\Gamma_i)} .$$

For each positive integer n, we denote by $M(n)$ the following rational number (which is a kind of "mass" of some subset of G_A):

$$M(n)=\sum_{i=1}^{H} \frac{\sharp(T_i^n(\pi))}{\sharp(\Gamma_i)} .$$

In the above summation, some lattices L_i are decomposable and hence correspond to decomposable polarizations. Now, changing the indices if necessary, we assume that the lattices $L_1, \dots, L_{H'}$ are indecomposable and that for any $i > H'$, the lattice L_i is decomposable. Now, we define $M'(n)$ by

$$M'(n)=\sum_{i=1}^{H'} \frac{\sharp(T_i^n(\pi))}{\sharp(\Gamma_i)} .$$

It is obvious that the following two conditions are equivalent:

(1) There exists an indecomposable lattice L such that $Lg \subset L$for some $g \in T_i^n(\pi)$.

(2) We get $M'(n) > 0$.

On the other hand, it is known which kind of calculation is needed in order to obtain $M(n)$ (cf. Hashimoto [4]), although actual calculations are somewhat elabolate. If we get $M(1)$, $M(2)$, and $M(3)$, then we can calculate $M'(3)$ by using the following lemma.

LEMMA 2.2. *Notation and assumptions being as above, we get*

$$M'(3)=M(3)-M(1)M(2)+\frac{1}{3} M(1)^3 .$$

PROOF. Assume that a lattice $L \in \mathscr{L}(n)$ is decomposable. So, for some positive integer $r > 1$ and some positive integers $d_1, \dots, d_r$ such that $\sum_{j=1}^{r} d_j = n$, there exists non zero *indecomposable* left $\mathcal{O}$-lattices $M_1, \dots, M_r$ such that, for each j $(1 \le j \le r)$, the left B-vector space $V_j = B \otimes M_j$ is of dimension d_j, and that

$$L = M_1 \perp \cdots \perp M_r ,$$

where we denote by $\perp$ the orthogonal splitting of lattices with respect to the metric we fixed. It is trivial that each M_j belongs to $\mathscr{L}(d_j)$, if we identify V_j with B^{d_j}. It can also be proved easily in the same way as in O'Meara [13, p. 321] that the above orthogonal splitting is unique up to order. Now, we set $L = L_i$ for some i with $1 \le i \le H$, and assume that $Lg \subset L$ for some $g \in G$ such that $g^2 = -p1_3$ and that $g_i g g_i^{-1} = \pi u$ for some $u \in U$. Then, we get also

$$Lg = M_1 g \perp \cdots \perp M_r g ,$$

and

$$Lg=\mathcal{O}^n\pi u g_i=\pi\mathcal{O}^n g_i=\pi L\,.$$

Hence, we get the following orthogonal splitting of L into left $\mathcal{O}$-lattices:

$$L=\pi^{-1}M_1 g\perp\cdots\perp\pi^{-1}M_r g\,.$$

Hence, by the uniqueness of the orthogonal splittings, it is shown that for each j with $1\leq j\leq r$, there exists j' *with* $1\leq j'\leq r$ such that

$$M_j=\pi^{-1}M_{j'}g\,.$$

The above lattice M_j is not necessarily isometric to $M_{j'}$ as quaternion Hermitian lattices. Now, we assume that $L\in\mathscr{L}(3)$. Then, we have two cases:

(1) $r=2$, $d_1=1$, and $d_2=2$, or

(2) $r=3$, $d_1=d_2=d_3=1$.

In the case (1), we get $M_j=\pi^{-1}M_j g$ for each $j=1$, 2. Hence, as $\mathrm{Aut}(L)=\mathrm{Aut}(M_1)\times\mathrm{Aut}(M_2)$, we get

$$M(3, L)=M(1, M_1)\times M(2, M_2)$$

in this case.

In the case (2), there are several possibilities. We shall say that the nonisometric left $\mathcal{O}$-lattices M and N of rank 1 (but not necessarily left $\mathcal{O}$-free) are conjugate with each other, if $\pi M=Nb$ for some $b\in B^\times$. In other words, M and N correspond to supersingular elliptic curves defined over $\boldsymbol{F}_{p^2}$ which are conjugate with each other.

(i) If M_j $(1\leq j\leq 3)$ are not isometric with each other and M_2 is conjugate to M_3, then we get

$$M(3, L)=M(1, M_1)\times\frac{1}{\sharp(\mathrm{Aut}(M_2))}\,.$$

(ii) If any M_j $(1\leq j\leq 3)$ are not isometric and not conjugate with each other, then we get

$$M(3, L)=M(1, M_1)\times M(1, M_2)\times M(1, M_3)\,.$$

(iii) If M_1 and M_2 are isometric and if M_3 is not isometric and not conjugate to the others, then $\sharp(\mathrm{Aut}(L))=2\times(\sharp(\mathrm{Aut}(M_1)))^2\sharp(\mathrm{Aut}(M_3))$ and we get

$$M(3, L)=\left(\frac{1}{2}M(1, M_1)^2+\frac{\sharp(\{b\in B;\ M_1 b\subset M_1\ \text{ and }\ n(b)=p\})}{2\cdot(\sharp(\mathrm{Aut}(M_1))^2}\right)\times M(1, M_3)\,,$$

where we identify M_1 with left $\mathcal{O}$-ideal of B and denote by $n(b)$ the reduced norm of b.

(iv) If all M_j are isometric with each other, then $\sharp(\mathrm{Aut}(L))=6\cdot(\sharp(\mathrm{Aut}(M_1)))^3$, and by easy calculation, we get

$$M(3, L)=\frac{1}{6}M(1, M_1)^3+M(1, M_1)\times\frac{\sharp(\{b\in B;\ M_1b\subset M_1 \text{ and } n(b)=p\})}{2\cdot(\sharp(\mathrm{Aut}(M_1))^2)},$$

where the notation is as in (iii).

(v) In the remaining cases, we get $M(3, L)=0$. Hence, by easy combinatorial argument, we get our lemma. q.e.d.

It is wellknown (Deuring [2]) that when $p=3$,

$$M(1)=\frac{2}{3}$$

and for any $p\geq 5$,

$$M(1)=\frac{1}{2}(h(-p)+h(-4p))=\begin{cases} h(\sqrt{-p})/2 & \text{if } p\equiv 1 \bmod 4 \\ 2h(\sqrt{-p}) & \text{if } p\equiv 3 \bmod 8 \\ h(\sqrt{-p}) & \text{if } p\equiv 7 \bmod 8\,, \end{cases}$$

where $h(d)$ is the class number of the order of $Q(\sqrt{d})$ with discriminant d and $h(\sqrt{d})$ is the class number of the maximal order of $Q(\sqrt{d})$.

To get $M(2)$ and $M(3)$, we must calculate various complicated data. Here, we just state the results and the proof will be given in later sections.

THEOREM 2. *We assume that the discriminant p of B is an odd prime. Then, we get*

$$M(2)=\begin{cases} 19/72 & \textit{if } p=3\,, \\ (1/48)h(\sqrt{-p})(4p-1) & \textit{if } p\equiv 1 \bmod 4\,, \\ (1/24)h(\sqrt{-p})(8p-5) & \textit{if } p\equiv 3 \bmod 8\,, \quad p\neq 3\,, \\ (1/6)h(\sqrt{-p})(p-1) & \textit{if } p\equiv 7 \bmod 8\,, \end{cases}$$

and

$$M(3)=\begin{cases} 77/2^3\cdot 3^4 & \textit{if } p=3\,, \\ (1/2^5\cdot 3^2)h(\sqrt{-p})B_{3,\chi} & \textit{if } p\equiv 1 \bmod 4\,, \\ (77/2^4\cdot 3^2)h(\sqrt{-p})B_{3,\chi} & \textit{if } p\equiv 3 \bmod 8\,, \quad p\neq 3\,, \\ (13/2^4\cdot 3)h(\sqrt{-p})B_{3,\chi} & \textit{if } p\equiv 7 \bmod 8\,, \end{cases}$$

where we denote by χ the quadratic character which corresponds to the imaginary quadratic field $Q(\sqrt{-p})$ and by $B_{3,\chi}$ the generalized third Bernoulli number with respect to χ.

The proof will be postponed until the final section.

THEOREM 3. *For every odd prime p, we get*

$$M'(3)>0\,.$$

Besides, $\lim_{p\to\infty} M'(3)=+\infty$, *and the number of curves over* $\boldsymbol{F}_p$ *such that* $\sharp C(\boldsymbol{F}_{p^2})=1+p^2+6p$ *tends to infinity as* $p\to\infty$.

PROOF. By Lemma 2.2 and the above Theorem, we get an estimate for $M'(3)$ from below. It is fairly easy to show that

$$B_{3,\chi}>p^2\sqrt{p} \qquad \text{if} \quad p\equiv 1 \bmod 4\,,$$

and

$$B_{3,\chi}>\frac{1}{25}p^2\sqrt{p} \quad \text{if} \quad p\equiv 3 \bmod 4\,.$$

In fact, it is wellknown that

$$B_{3,\chi}=\frac{3f^2\sqrt{f}}{2\pi^3}L(3,\chi)\,,$$

where f is the conductor of χ, and also that

$$L(3,\chi)=\zeta_{\boldsymbol{Q}(\sqrt{-p})}(3)/\zeta(3)\,,$$

where the L functions and zeta functions are defined as usual. As $\zeta(3)<1.21$ and $\zeta_{\boldsymbol{Q}(\sqrt{-p})}(3)>\zeta(6)=\pi^6/945$, we get the above estimate for $B_{3,\chi}$. Hence, as $h(\sqrt{-p})<p$, we can always show that $M'(3)>0$ for sufficiently large p. For example, if $p\equiv 1 \bmod 4$, then the above estimate gives that $M'(3)>0$ for $p\geq 150$. As for $p<150$, we calculate the exact value of $M'(3)$ directly, and we can see that $M'(3)>0$. For those primes with $p\equiv 3 \bmod 4$, we can show in a similar way that $M'(3)>0$. It is also obvious by the above estimate that $M'(3)\to\infty$ as $p\to\infty$. For each lattice L, it is obvious that $M(3, L)\leq 1$. Hence, the number of indecomposable lattices L such that $M(3, L)\neq 0$ increases to infinity as $p\to\infty$. q.e.d.

3. Review on the mass formula.

From now on, we shall calculate $M(2)$ and $M(3)$. In this section, first we shall review the general (but not explicit) formula for $M(n)$, and secondly, we shall review conjugacy classes.

PROPOSITION 3.1 (Hashimoto [4], see also [6, §1]). *We have*

$$M(n)=\sum_{\{g\}_G}\sum_{L_G(\Lambda)} M_G(\Lambda)\prod_{q<\infty} c_q(g, \Lambda_q, \pi U_q)\,,$$

where the notation will be explained below.

NOTATION. (1) $\{g\}_G$ runs over G-conjugacy classes of elements of G such that $g^2=-p1_n$.

(2) Here, we shall explain the meaning of $L_G(\Lambda)$. For each element $g\in G$, we denote by $Z(g)$ the commutant of $\boldsymbol{Q}(g)$ in $M_n(B)$: $Z(g)=\{z\in M_n(B);\, zg=gz\}$. We put

$Z_G(g)=Z(g)\cap G$. Now take an order Λ of $Z(g)$. For any prime q, we denote by $Z_G(g)_q$ the q-adic component of the adelization $Z_G(g)_A$, and put $\Lambda_q=\Lambda\otimes \boldsymbol{Z}_q$. We denote by $L_G(\Lambda)$ the G-genus containing Λ:

$$L_G(\Lambda)=\{\Lambda'\subset Z(g);\ \Lambda' \text{ is an order of } Z(g) \text{ and for every prime } q,\ \Lambda'_q=y_q^{-1}\Lambda_q y_q \text{ for some } y_q\in Z_G(g)_q\}\,.$$

In the second summation of the above Proposition, $L_G(\Lambda)$ runs over all the G-genera.

(3) $M_g(\Lambda)$ is the mass of the G-genus Λ defined below.

Take a double coset decomposition of $Z_G(g)_A$ as follows:

$$Z_G(g)_A=\coprod_{k=1}^{h(\Lambda)} Z_G(g)y_k(\Lambda_A^\times\cap Z_G(g)_A)\,.$$

For each k with $1\leq k\leq h(\Lambda)$, define an order Λ_k of $Z(g)$ by

$$\Lambda_k=\bigcap\nolimits_q(y_k\Lambda_q y_k^{-1}\cap Z(g))\,.$$

The G-mass $M_G(\Lambda)$ is defined by

$$M_G(\Lambda)=\sum_{k=1}^{h(\Lambda)}\frac{1}{\#(\Lambda_k^\times\cap G)}\,.$$

(4) The quantity in the last product is now defined. For each prime q, we set

$$M(g,\Lambda_q,\pi U_q)=\{x\in G_q;\ x^{-1}gx\in\pi U_q \text{ and } Z(g)\cap xM_n(\mathcal{O}_q)x^{-1}=a\Lambda_q a^{-1} \text{ for some } a\in Z_G(g)_q\}\,.$$

The "local datum" c_q is defined by

$$c_q(g,\Lambda_q,\pi U_q)=\#(Z_G(g)\backslash M(g,\Lambda_q,\pi U_q)/U_q)\,.$$

To get $M(2)$ and $M(3)$, we must calculate every datum in the above propostion explicitly. Here, we review conjugacy classes of elements of G (cf. [6]). For each n and each prime q, we define a subset $C_q(n)$ of $G_q(n)$, and a subset $C(n)$ of G, respectively as follows:

$$C_q(n)=\{g\in G_q(n);\ g^2=-p1_n, \text{ and } g^t\bar{g}=p1_n\}\,,$$

$$C(n)=\{g\in G(n);\ g^2=-p1_n \text{ and } g^t\bar{g}=p1_n\}\,.$$

When $n=3$, put

$$g=\begin{pmatrix}\pi&0&0\\0&\pi&0\\0&0&\pi\end{pmatrix}.$$

Then, any element g' of $C(3)$, or $C_q(3)$, is G-conjugate, or G_q-conjugate, to g, respectively.

When $n=2$, for an element $g\in C(2)$, set $F=\boldsymbol{Q}(g)\cong\boldsymbol{Q}(\sqrt{-p})$. Then, $Z(g)$ is a quaternion algebra over F with $Z(g)\otimes F\cong M_2(B)$ and there exists a unique quaternion subalgebra $Z_0(g)$ over $\boldsymbol{Q}$ of $Z(g)$ such that $Z_G(g)=F^\times\cdot Z_0(g)^\times$ (an amalgamated product with $F\cap Z_0(g)=\boldsymbol{Q}^\times$.) The mapping $C(2)\to Z_0(g)$ gives a bijection from the set of G-conjugacy classes in $C(2)$ onto the set of definite quaternion algebra D with $D\otimes_{\boldsymbol{Q}}F\cong B\otimes F$. (As for a more precise statement, see [6].) As for $C_q(2)$, the same holds, if we replace each global object above by the corresponding local one, e.g. $Z(g)$ by $Z(g)_q$ etc. Hence, the set $C_q(2)$ consists of *at most* two G_q-conjugacy classes.

4. Local data. We shall give the most delicate term $c_q(g, \Lambda, \pi U_q)$ in the mass formula for $n=2$ and 3. The proof consists of fairly long calculation on matrices which is similar to that in [6] and will be omitted here. The above data are determined locally, and we calculate them for each G_q-conjugacy class in $C_q(n)$, $n=2$, or 3. When $n=2$, we shall also calculate some numbers $d_q=d_q(g, \Lambda)$ and $e_q=e_q(g, \Lambda)$ which are necessary for the calculation of $M_G(\Lambda)$ and defined by

$$d_q=[\Lambda_{0,\max}^\times:\Lambda_0^\times]\cdot[\mathfrak{o}_q^\times:\boldsymbol{Z}_q[g]^\times],$$

and

$$e_q=[\Lambda^\times\cap G:\boldsymbol{Z}_q[g]^\times\Lambda_0^\times],$$

where we put $\Lambda_0=Z(g)\cap\Lambda$, and denote by Λ any maximal order of $Z_0(g)$ which contains Λ_0 and by $\mathfrak{o}_q$ the maximal order of $\boldsymbol{Q}_q(g)$. Throughout this section, we assume that the discriminant p of B is an odd prime.

4.1. The case $n=2$. In this subsection, we treat the case $n=2$. For the sake of convenience, we put

$$G_q^*=\left\{g\in M_2(B_q);\ g\begin{pmatrix}0&1\\1&0\end{pmatrix}{}^t\bar{g}=\begin{pmatrix}0&1\\1&0\end{pmatrix}\right\},$$

and

$$U_q^*=G_q^*\cap GL_2(\mathcal{O}_q).$$

As we can choose an element $\xi\in GL_2(\mathcal{O}_q)$ such that

$$\xi{}^t\bar{\xi}=\begin{pmatrix}0&1\\1&0\end{pmatrix},$$

the mapping $G_q\ni g\to\xi g\xi^{-1}\in G_q^*$ induces isomorphisms $G_q\cong G_q^*$ and $U_q\cong U_q^*$. We fix ξ for each prime q and we shall often identify G_q with G_q^* through the above isomorphism. When $q\neq p$, it is also convenient in some case to use generalized symplectic group $GSp(2, \boldsymbol{Q}_2)$:

$$GSp(2, \boldsymbol{Q}_2)=\left\{g\in M_4(\boldsymbol{Q}_q);\ g\begin{pmatrix}0&-1_2\\-1_2&0\end{pmatrix}{}^tg=\begin{pmatrix}0&-1_2\\-1_2&0\end{pmatrix}\right\}.$$

For $q \neq p$, we get $GSp(2, \mathbf{Q}_q) \cong G_q$, and we fix this isomorphism and identify these groups sometimes.

For each prime q, we fix an element π of $\mathcal{O}_q$ such that $\pi^2 = -p$, and put

$$g_1 = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix} \in G_q^* .$$

Then, $\xi g_1 \xi^{-1}$ belongs to $C_q(2)$, and the corresponding algebra $Z_0(g_1)$ (defined in the preceding section, or [6]) is given by

$$Z_0(g_1) = \left\{ \begin{pmatrix} a & b\pi \\ c\pi & d \end{pmatrix} \in M_2(B_q);\ a, b, c, d \in \mathbf{Q}_q \right\},$$

and is isomorphic to $M_2(\mathbf{Q}_q)$. When $\mathbf{Q}_q(\sqrt{-p}) \cong \mathbf{Q}_q \oplus \mathbf{Q}_q$, then $\xi g_1 \xi^{-1}$ represents the unique G_q-conjugacy class in $C_q(2)$. Besides, if $q \neq 2$ and $\mathbf{Q}_q(\sqrt{-p})$ is an unramified quadratic extension of $\mathbf{Q}_q$, then for any $g \in C_q$ such that $Z_0(g)$ is a division algebra, namely, if g belongs to the other G_q-conjugacy class in $C_q(g)$ than $\xi g_1 \xi^{-1}$, we have $c_q(g, \Lambda, U_q) = 0$ for any order $\Lambda \subset Z(g)$ (see [6, Proposition 4]). First we assume that $q \neq 2$ and $\mathbf{Q}_q(\sqrt{-p}) \cong \mathbf{Q}_q \oplus \mathbf{Q}_q$.

PROPOSITION 4.1. *Notation and assumptions being as above, we get*

$$c_q(\xi g_1 \xi^{-1}, \Lambda, U_q) = \begin{cases} 1 & \text{if } \Lambda \sim \Lambda_1 = M_2(\mathbf{Z}_q[\pi]), \\ 0 & \text{for any other } \Lambda, \end{cases}$$

and $d_q(\Lambda_1) = e_q(\Lambda_1) = 1$.

Now, we assume that $q \neq 2$ and that $\mathbf{Q}_q(\sqrt{-p})$ is an unramified quadratic extension of $\mathbf{Q}_q$.

PROPOSITION 4.2. *Notation and assumptions being as above, we get*

$$c_q(\xi g_1 \xi^{-1}, \Lambda, U_q) = \begin{cases} 1 & \text{if } \Lambda \sim \Lambda_1 = M_2(\mathbf{Z}_q[\pi]), \\ 0 & \text{for any other } \Lambda, \end{cases}$$

and $d_q(\Lambda_1) = e_q(\Lambda_1) = 1$.

Next, we assume that $q = p$. In this case, $\mathbf{Q}_p(g)$ is a ramified quadratic extension of $\mathbf{Q}_p$. We fix an element π of $\mathcal{O}_p$ such that $\pi^2 = -p$. Then, there are two G_q-conjugacy classes in $C_q(2)$, each of which is represented by g_1 defined before, or g_2 defined as follows: When $p \equiv 1 \bmod 4$, we put

$$g_2 = \begin{pmatrix} \pi & 0 \\ 0 & \pi \end{pmatrix} \in G_q ,$$

and if $p \equiv 3 \bmod 4$, we put

$$g_2=\begin{pmatrix}\pi & 0\\ 0 & -\pi\end{pmatrix}\in G_q\,.$$

PROPOSITION 4.3. *Let the notation be as above.*

(i) *As for g_1 we get*

$$c_p(\xi g_1\xi^{-1}, \Lambda, U_q)=\begin{cases}1 & \textit{if}\ \ \Lambda\sim\Lambda_1=M_2(\boldsymbol{Z}_q[\pi])\,,\\ 0 & \textit{for the other}\ \Lambda\,,\end{cases}$$

and $d_p(\Lambda_1)=p+1$, $e_p(\Lambda_1)=2$.

(ii) *As for g_2, we get*

$$c_p(g_2, \Lambda, U_q)=\begin{cases}1 & \textit{if}\ \ \Lambda\sim\Lambda_2=M_2(\boldsymbol{Z}_q[\pi])\,,\\ 0 & \textit{for the other}\ \Lambda\,,\end{cases}$$

and $d_p(\Lambda_2)=1$, $e_p(\Lambda_2)=2$.

Finally, we assume that $q=2$. Recall that we assumed $p\neq 2$. When $p\equiv 1 \bmod 4$, we define $g_1\in G_2^*$ as before. When $p\equiv 3 \bmod 8$, we get

$$\pi=\begin{pmatrix}1 & 2\\ -(p+1)/2 & -1\end{pmatrix}.$$

This setting is convenient, because $\boldsymbol{Q}_2(\pi)\cap M_2(\boldsymbol{Z}_2)=\boldsymbol{Z}_2[(1+\pi)/2]=$ the maximal order of $\boldsymbol{Q}_2(\pi)$. When $p\equiv 7 \bmod 8$, we set

$$g_1=\begin{pmatrix}\omega 1_2 & 0\\ 0 & -\omega 1_2\end{pmatrix}\in GSp(2, \boldsymbol{Q}_2)\,,$$

where ω is an element of $\boldsymbol{Z}_2$ such that $\omega^2=-p$. We also define g_2 for each characteristic (or discriminant) p as follows:

When $p\equiv 1 \bmod 4$, put

$$g_2=\begin{pmatrix}0 & 0 & -1 & 0\\ 0 & 0 & 0 & -1\\ p & 0 & 0 & 0\\ 0 & p & 0 & 0\end{pmatrix}\in GSp(2, \boldsymbol{Q}_2)\,,$$

and when $p\equiv 3 \bmod 8$, then put

$$g_2=\begin{pmatrix}1 & 0 & 2 & 0\\ 0 & 1 & 0 & 4\\ 2\varepsilon & 0 & -1 & 0\\ 0 & \varepsilon & 0 & -1\end{pmatrix}\in GSp(2, \boldsymbol{Q}_2)\,,$$

where $\varepsilon=-(p+1)/4$.

PROPOSITION 4.4. *Notation and assumptions being as above, we get*
(i) *if* $p\equiv 1 \bmod 4$, *then*

$$c_q(g_1, \Lambda, U_q)=\begin{cases} 1 & \textit{if } \ \Lambda\sim\Lambda_1=M_2(\mathbf{Z}_2(\pi))\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_2=Z(g_1)\cap\begin{pmatrix}1 & \beta\\ 0 & 1\end{pmatrix}, \\ 0 & \textit{for any other } \Lambda\,, \end{cases}$$

where

$$\beta=\frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},$$

and $d_q(\Lambda_1)=1$, $e_q(\Lambda_1)=1$, *and* $d_q(\Lambda_2)=3$, $e_q(\Lambda_2)=2$,

$$c_q(g_2, \Lambda, U_q)=\begin{cases} 1 & \textit{if } \ \Lambda\sim\Lambda_1=Z(g_2)\cap M_4(\mathbf{Z}_2)\,, \\ 1 & \textit{for any other } \Lambda\,, \end{cases}$$

and $d_q(\Lambda_2)=3$, $e_q(\Lambda_2)=2$.

(ii) *If* $p\equiv 3 \bmod 8$, *then*

$$c_q(g_1, \Lambda, U_q)=\begin{cases} 1 & \textit{if } \ \Lambda\sim\Lambda_1=Z(g)\cap M_2(\mathcal{O}_2)\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_2=Z(g)\cap xM_2(\mathcal{O}_2)x^{-1}\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_3=Z(g)\cap yM_2(\mathcal{O}_2)y^{-1}\,, \\ 0 & \textit{for any other } \Lambda\,, \end{cases}$$

where

$$x=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 1/2 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{pmatrix}, \qquad y=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 2 & 1 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 2\end{pmatrix}\in G_2^*\,,$$

and $d_q(\Lambda_1)=3$, $e_q(\Lambda_1)=3$, $d_q(\Lambda_2)=9$, $e_q(\Lambda_2)=1$, $d_q(\Lambda_3)=3$, $e_q(\Lambda_3)=1$.

$$c_q(g_2, \Lambda, U_q)=\begin{cases} 1 & \textit{if } \ \Lambda\sim\Lambda_1=Z(g)\cap M_2(\mathcal{O}_2)\,, \\ 0 & \textit{for any other } \Lambda\,, \end{cases}$$

and $d_q(\Lambda_1)=9$, $e_q(\Lambda_1)=3$.
(iii) *If* $p\equiv 7 \bmod 8$, *then*

$$c_q(g_1, \Lambda, U_q)=\begin{cases} 1 & \textit{if } \ \Lambda\sim\Lambda_1=Z(g)\cap M_2(\mathcal{O}_2)\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_2=Z(g)\cap xM_2(\mathcal{O}_2)x^{-1}\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_3=Z(g)\cap yM_2(\mathcal{O}_2)y^{-1}\,, \\ 1 & \textit{if } \ \Lambda\sim\Lambda_4=Z(g)\cap zM_2(\mathcal{O}_2)z^{-1}\,, \\ 0 & \textit{for any other } \Lambda\,, \end{cases}$$

where

$$x=\begin{pmatrix}1&0&0&1/2\\0&1&1/2&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad y=\begin{pmatrix}1&0&1/2&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\quad z=\begin{pmatrix}1&0&1/2&0\\0&1&0&1/2\\0&0&1&0\\0&0&0&1\end{pmatrix},$$

and $d_q(\Lambda_1)=1$, $e_q(\Lambda_1)=1$, $d_q(\Lambda_2)=1$, $e_q(\Lambda_2)=1$, $d_q(\Lambda_3)=3$, $e_q(\Lambda_3)=1$, $d_q(\Lambda_4)=3$, $e_q(\Lambda_4)=1$.

4.2. The case $n=3$. It is not difficult to show that for each prime q, there exists an element $\xi\in GL_3(\mathcal{O}_q)$ such that

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

We set

$$G_q^*=\left\{g\in M_3(B_q);\ g\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}{}^t\bar{g}=\begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}\right\},$$

and

$$U_q^*=G_q^*\cap GL_3(\mathcal{O}_q)\,.$$

Then, $G_q\ni g\mapsto\xi g\xi^{-1}\in G_q^*$ induces isomorphisms $G_q\cong G_q^*$ and $U_q\cong U_q^*$. Now, we put

$$g=\begin{pmatrix}\pi&0&0\\0&\pi&0\\0&0&\pi\end{pmatrix},$$

where π is any fixed element of $\mathcal{O}_q$ with $\pi^2=-p$. Then, any element $g'\in C_q(3)$ is G_q-conjugate to $\xi g\xi^{-1}$. Hence, we shall treat everything in G_q^* and use g as a representative of $C_q(3)$. To calculate $M_G(\Lambda)$, we need some local mass, which is denoted by $d_q(\Lambda)$ and defined by

$$d_q(\Lambda)=\frac{[\Lambda^\times\cap G_q^\times:\Lambda_0^\times\cap\Lambda^\times\cap G_q^*]}{[\Lambda_0^\times\cap G_q^*:\Lambda_0^\times\cap\Lambda^\times\cap G_q^*]},$$

where we put $\Lambda_0=M_3(\mathfrak{o}_q)$.

PROPOSITION 4.5. (1) *When* $q\neq 2$, *we get*

$$c_q(g,\Lambda,\pi U_q^*)=\begin{cases}1 & \textit{if}\ \ \Lambda\sim\Lambda_0\,,\\ 0 & \textit{for any other}\ \Lambda\,.\end{cases}$$

(2) *When $q=2$, we get the following results*:

(i) *If* $p\equiv 1 \bmod 4$, *then*

$$c_2(g,\Lambda,\pi U_2^*)=\begin{cases}1 & \textit{if}\ \ \Lambda\sim\Lambda_0\,,\\ 0 & \textit{for any other}\ \Lambda\,.\end{cases}$$

(ii) *If* $p\equiv 7 \bmod 8$, *then*

$$c_2(g,\Lambda,\pi U_2^*)=\begin{cases}1 & \textit{if}\ \ \Lambda\sim\Lambda_0\,,\\ 1 & \textit{if}\ \ \Lambda\sim\Lambda_1=M_3(\boldsymbol{Q}_2(\pi))\cap x_1M_2(\mathcal{O}_2)x_1^{-1}\,,\\ 1 & \textit{if}\ \ \Lambda\sim\Lambda_2=M_3(\boldsymbol{Q}_2(\pi))\cap x_2M_2(\mathcal{O}_2)x_2^{-1}\,,\\ 1 & \textit{if}\ \ \Lambda\sim\Lambda_3=M_3(\boldsymbol{Q}_2(\pi))\cap x_3M_2(\mathcal{O}_2)x_3^{-1}\,,\\ 1 & \textit{if}\ \ \Lambda\sim\Lambda_4=M_3(\boldsymbol{Q}_2(\pi))\cap x_4M_2(\mathcal{O}_2)x_4^{-1}\,,\\ 0 & \textit{for any other}\ \Lambda\,,\end{cases}$$

where, for each i with $1\le i\le 4$, *we put*

$$x_i=\begin{pmatrix}1_3 & (1/2)S_i\\ 0 & 1_3\end{pmatrix},$$

and

$$S_1=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\qquad S_2=\begin{pmatrix}0&0&0\\0&1&0\\0&0&1\end{pmatrix},$$

$$S_3=\begin{pmatrix}0&0&0\\0&0&1\\0&1&0\end{pmatrix},\qquad S_4=\begin{pmatrix}0&0&0\\0&0&0\\0&0&1\end{pmatrix},$$

and $d_2(\Lambda_0)=1$, $d_2(\Lambda_1)=28$, $d_2(\Lambda_2)=21$, $d_2(\Lambda_3)=7$, $d_2(\Lambda_4)=21$.

When $p\equiv 3 \bmod 8$, the same kind of calculation seems fairly complicated, so we shall determine the local data at 2 for $n=3$ by another method as follows: We can reduce the problem to the case $p=3$ as we shall see later. When $p=3$, the class number of the principal genus in B^3 is two (cf. Hashimoto [3]). In this case, we can take the maximal order $\mathcal{O}$ as

$$\mathcal{O}=\boldsymbol{Z}+\boldsymbol{Z}\frac{1+\alpha}{2}+\boldsymbol{Z}\beta+\boldsymbol{Z}\frac{(1+\alpha)\beta}{2},$$

where $\alpha^2=-3$ and $\beta^2=-1$. Then, the unique indecomposable lattice class in the principal genus of B^3 is represented by $L=\mathcal{O}^3x$, where $x\in GL_3(B)$ such that

$$Y:=x^t\bar{x}=\begin{pmatrix}3 & \alpha & \alpha+\beta\\ -\alpha & 2 & 0\\ -\alpha-\beta & 0 & 3\end{pmatrix}.$$

The other lattice class is represented by $\mathcal{O}^3$. Since $\sharp(\mathrm{Aut}(\mathcal{O}^3))=1/12^3\cdot 6$ and since

$$\frac{13}{12^3\cdot 6\cdot 7}=\frac{1}{\sharp(\mathrm{Aut}(\mathcal{O}^3))}+\frac{1}{\sharp(\mathrm{Aut}(L))}$$

by the usual mass formula ([6, p. 568]), we get $\sharp(\mathrm{Aut}(L))=12^3\cdot 7$. Now, define a subset N of G by

$$N=\{g\in G;\ Lg\subset L,\ g^2=-3\cdot 1_3\}\ .$$

Then, it is easy to see that

$$\sharp(N)=\sharp\{g\in M_3(\mathcal{O});\ gY{}^t\bar{g}=3Y,\ g^2=-3\cdot 1_3\}\ .$$

The latter number was calculated by computer and we obtained $\sharp(N)=504$. Hence, we obtained $M'(3)=1/2^3\cdot 3$ and $M(3)=77/2^3 3^4$ for $p=3$. When $p\equiv 3 \bmod 8$, then we have $-p=-3\varepsilon^2$ for some $\varepsilon\in \boldsymbol{Z}_2^\times$. So, if $g^2=-p$, then $(g\varepsilon^{-1})^2=-3$. Hence, it is obvious that for any order $\Lambda_2\subset Z(g)_2$, the datum $c_2(g, \Lambda_2, \pi U_2)$ does not depend on p as long as $p\equiv 3 \bmod 8$. For $p=3$, and hence for any prime $p\equiv 3 \bmod 8$, we get

$$\sum_{\Lambda} d_2(\Lambda)c_2(g, \Lambda, \pi U_2^*)=154\ .$$

These data are enough for later use.

5. Proof of the main theorem. In this section, we complete the proof of Theorem 1 in §1 by showing Theorem 2 in §2. First, we treat $M(3)$. Let F be any imaginary quadratic field over $\boldsymbol{Q}$, and denote by $\mathfrak{o}_F$ the maximal order of F. For any natural number n, we define the generalized unitary group $GU(n, F)$ and the unitary group $U(n, F)$ as usual by

$$GU(n, F)=\{h\in M_n(F);\ h{}^t\bar{h}=n(h)1_n\}\ ,$$

and

$$U(n, F)=\{h\in GU(n, F);\ n(h)=1\}\ .$$

If we put

$$g=\begin{pmatrix}\pi & 0 & 0\\ 0 & \pi & 0\\ 0 & 0 & \pi\end{pmatrix}$$

as before, then

$$Z(g)=M_3(\boldsymbol{Q}(\pi))\ ,$$

and

$$Z_G(g)=GU(3, \boldsymbol{Q}(\pi))\ .$$

Hence, for $\Lambda_0 = M_3(\mathfrak{o}_F) \subset Z(g)$, where $F = \boldsymbol{Q}(\pi)$, the mass $M_G(\Lambda_0)$ is the *usual mass* of the generalized unitary group $GU(3, F)$. To get the mass $M_G(\Lambda_0)$ from the *usual mass* of the unitary group

$$Z_G(g)^1 = \{h \in Z_G(g);\ n(h) = 1\} = U(3, F)\,,$$

we shall compare the class numbers of both algebraic groups. We shall treat this problem in a slightly more general setting. Again, let F be any imaginary quadratic field over $\boldsymbol{Q}$.

LEMMA 5.1. *Notation being as above, assume that n is odd. Then, we get*

$$h(GU(n, F)) = 2^{t-1} \cdot h(U(n, F))\,,$$

where t is the number of prime divisors of the discriminant of F.

PROOF. Put $\mathfrak{o}_A^\times = \boldsymbol{C}^\times \times \prod_{v<\infty} \mathfrak{o}_{F_v}^\times$, where $\mathfrak{o}_{F_v}$ is the maximal order of the v-adic completion F_v of F. If $g_1, g_2 \in GU(n, F_A)$ and if $n(g_1) \notin N(F^\times) n(g_2) N(\mathfrak{o}_A^\times)$, then it is clear that $g_1 \notin GU(n, F) g_2 GU(n, \mathfrak{o}_A)$. On the other hand, for each $R = F^\times$, $F_A^\times$, or $\mathfrak{o}_A^\times$, the set of multiplicators $n(g)$ of $GU(n, R)$ is $N(R)$, respectively, where we denote by N the usual norm over $\boldsymbol{Q}$ or $\boldsymbol{Q}_A$. Indeed, for any $a \in R$, $a1_n \in GU(n, R)$ and $N(a) = n(a1_n)$. On the other hand, for $g \in GU(n, R)$, we get $\det(g^t\bar{g}) = n(g)^n$, and since n is odd, we get $n(g) = N(\det(g)/n(g)^{(n-1)/2})$. So, if $n(g) \in N(F^\times) N(a) N(\mathfrak{o}_A^\times)$ for some $a \in F_A^\times$, then replacing g by some other representative in $GU(n, F) g GU(n, \mathfrak{o}_A)$ if necessary, we may assume that $n(g) = N(a)$. Now, for each $a \in F_A$, put $S(a) = \{g \in GU(n, F_A);\ n(g) \in N(F^\times) N(a) N(o_A^\times)\}$ and $T(a) = \{g \in GU(n, F_A);\ n(g) = N(a)\}$. We show that $\sharp(GU(n, F) \backslash S(a) / GU(n, \mathfrak{o}_A)) = \sharp(U(n, F) \backslash T(a) / U(n, \mathfrak{o}_A)) = h(U(n, F))$. Indeed, if $g \in S(a)$, then replacing g by some other representative in $GU(n, F) g GU(n, \mathfrak{o}_A)$ if necessary, we may assume that $n(g) = a$. So, take $g_1, g_2 \in S(a)$ such that $n(g) = a$. If $g_1 = k g_2 u$ for some $k \in GU(n, F)$ and $u \in GU(n, \mathfrak{o}_A)$, then $n(ku) = 1$. So, we get $n(k) \in N(F^\times) \cap N(\mathfrak{o}_A^\times) = 1$. This means that $a \in U(n, F)$ and $u \in U(n, \mathfrak{o}_A)$. Besides, for any $g \in T(a)$, we get $a^{-1} g \in U(n, F)$ and so $T(a) = a^{-1} T(1)$. So we get the above results. By the genus theory, it is wellknown that $\sharp(N(F^\times) \backslash N(F_A^\times) / N(\mathfrak{o}_A^\times)) = 2^{t-1}$. q.e.d.

By the above lemma and by using the fact that the unit group of a $GU(n, F)$-class is the same as those of $U(n, F)$-classes in that, it is obvious that

$$M_G(M_n(\mathfrak{o}_F)) = 2^{t-1} \cdot M(U(n, F))\,,$$

where $M(U(n, F))$ is the usual mass of the unitary group (with respect to the genus containing $\mathfrak{o}_F^n$). But, the explicit value of $M(U(n, F))$ is well-known (cf. Otremba [16], Hashimoto-Koseki [7]) and when $n = 3$, this is given by:

$$M(U(3, F)) = -\frac{1}{2^{t+4} \cdot 3^2} B_{1,\chi} B_{3,\chi}\,,$$

and hence, for $F = \boldsymbol{Q}(\sqrt{-p})$ (p: odd prime), we get

$$M(GU(3, F))=\begin{cases} 1/2^4\cdot 3^4 & \text{if} \quad p=3\,, \\ (1/2^5\cdot 3^2)h(\sqrt{-p})B_{3,\chi} & \text{for} \quad p\geq 5\,. \end{cases}$$

For any order $\Lambda\subset Z(g)$, we get $M_G(\Lambda)=M_G(\Lambda_0)\prod_q d_q(\Lambda)$. Hence, gathering the local data in §4 together, we get the result for $M(3)$ in Theorem 2.

As for the case where $n=2$, it is known (cf. [6, p. 572, Proposition 12]) that

$$M_G(\Lambda)=\frac{h(\sqrt{-p})}{12\#(\mathfrak{o}_F^\times)}\prod_{l\mid D(Z_0(g))}(l-1)\prod_q d_q(\Lambda)/e_q(\Lambda)$$

for any $\Lambda\subset Z(g)$. Hence, gathering local data in §4 together, we get the results for $M(2)$ in Theorem 2.

Thus, Theorem 2 was proved and hence Theorem 1 as well.

References

[1] M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, Jber. Deutsch. Math. Verein. 54 (1951), 24–41.

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

[3] K. Hashimoto, Class numbers of positive definite ternary quaternion hermitian forms, Proc. Japan Acad. Ser. A. Math. Sci. 59 (1983), 490–493.

[4] 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.

[5] K. Hashimoto and T. Ibukiyama, A letter to Serre, 1984.

[6] K. Hashimoto and T. Ibukiyama, On class numbers of positive definite binary quaternion hermitian forms, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 27 (1980), 549–601.

[7] K. Hashimoto and H. Koseki, Class numbers of definite unimodular Hermitian forms over the rings of imaginary quadratic fields, Tôhoku Math. J. (2) 41 (1989), 1–30.

[8] T. Ibukiyama, On automorphism groups of positive definite binary quaternion hermitian lattices and new mass formula, in Automorphic Forms and Geometry of Arithmetic Varieties, (K. Hashimoto, Y. Namikawa eds.), Advanced Studies in Pure Math. Vol. 15, Kinokuniya, Tokyo, and Academic Press, Orland, Florida, 1989, 301–349.

[9] T. Ibukiyama and T. Katsura, On the field of definition of superspecial polarized abelian varieties and type numbers, 1989. Preprint.

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

[11] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), 721–724.

[12] Yu. I. Manin and S. G. Vladut, Linear codes and modular curves, J. Soviet Math. 30 (1985), 2611–2643.

[13] O. O'Meara, Introduction to quadratic forms, Springer, Berlin, Heidelberg, New York, 1971.

[14] F. Oort, Hyperelliptic supersingular curves, in Arithmetic algebraic geometry, Texel, 1989 (G. van der Geer, F. Oort, J. Steenbrink, ed.) Progr. Math. 89, Birkhäuser Boston, Boston, MA, 1991, 247–284.

[15] F. Oort and K. Ueno, Principally polarized abelian varieties of dimension two or three are Jacobian varieties, J. Fac. Sci. Univ. Tokyo Sect. IA 20 (1973), 377–381.

[16] G. Otremba, Zur Theorie der Hermitischen Formen in imaginär-quadratischen Zahlkörpern, J. Reine Angew. Math. 249 (1971), 1–19.

[17] J. P. Serre, A letter to Hashimoto and Ibukiyama, February 1984.

[18] J. P. Serre, Nombre des points des courbes algébrique sur $\boldsymbol{F}_q$, Sém. Théor. Nombres Bordeaux (2) 1982/83, 22 (1983).

[19] J. P. Serre, Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini, C. R. Acad. Sci. Paris Sér. I Math. 296 (1983), 397–402.

[20] A. Weil, Courbes algébriques et variétés abéliennes, Hermann, Paris, 1971.

Department of Mathematics
College of General Education
Osaka University
Toyonaka 560
Japan