Abelian varieties over Q associated with an imaginary quadratic field

By Tetsuo NAKAMURA

Mathematical Institute, Tohoku University, Sendai 980-8578, Japan

(Communicated by Heisuke HIRONAKA, M.J.A., Oct. 12, 2007)

Abstract: For an imaginary quadratic field K with class number h, we shall characterize h-dimensional CM abelian varieties over K which descend to abelian varieties over $\mathbf{Q}$. These CM abelian varieties have minimal dimension h both over K and over $\mathbf{Q}$.

Key words: abelian variety; ellptic curve; complex multiplication; Hecke character.

Let K be an imaginary quadratic field with class number h. We shall characterize h-dimensional CM abelian varieties over K which descend to abelian varieties over the rational number field $\mathbf{Q}$ by their algebraic Hecke characters. If an abelian variety A over K has complex multiplication, then the dimension of A is $h\,[H_g(\mathrm{Im}\,\epsilon) : H_g]$ or $2h\,[H_g(\mathrm{Im}\,\epsilon) : H_g]$. Here H_g is the genus class field of K (Proposition 2). Hence our CM abelian varieties have minimal dimension h both over K and over $\mathbf{Q}$. Under the conditions that $\mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ are maximal real subfields of $\mathrm{End}_K(A) \otimes \mathbf{Q}$ and some restrictions on the conductors of A, such abelian varieties are investigated in Yang [5]. In this note removing the above conditions, we treat these abelian varieties in general. We shall give a characterization of the associated characters of them (Theorem 1). In the final section we explicitely determine such characters.

Notation:

K : an imaginary quadratic field.
D : the discriminant of K.
H : the Hilbert class field of K.
h : the class number of K.
$I(\mathfrak{f})$: the group of fractional ideals of K prime to $\mathfrak{f}$. ($\mathfrak{f}$ is an integral ideal of K)
$P(\mathfrak{f})$: the group of principal ideals of K prime to $\mathfrak{f}$.
ρ : the complex conjugation of $\mathbf{C}$.

For an abelian variety A over a number field k, we put $\mathcal{E}_k(A) = \mathrm{End}_k(A) \otimes \mathbf{Q}$, the endomorphism algebra of A over k. All number fields are considered as subfields of $\mathbf{C}$.

1. CM Abelian varieties over *K*. Let A be a CM abelian variety over an imaginary quadratic field K. We suppose that A is simple over K. Let ψ_A be the associated algebraic Hecke character of A over K, of conductor $\mathfrak{f}$. Then there is a character ϵ of $(O_K/\mathfrak{f})^\times$ such that

$$\psi_A((\alpha)) = \epsilon(\alpha)\alpha \qquad ((\alpha) \in P(\mathfrak{f})).$$

We say that A is of type ϵ or ϵ is associated to A (or to ψ_A). Clearly ϵ satisfies $\epsilon(-1) = -1$ and for ideal class characters χ of K, $\psi_A\chi$ are the algebraic Hecke characters associated to ϵ (see [5, § 3]). Let $I_g(\mathfrak{f}) = \{\mathfrak{a} \in I(\mathfrak{f});\ \mathfrak{a}^2 \text{ is principal}\}$. We put

$$T = K(\{\psi_A(\mathfrak{a}) \mid \mathfrak{a} \in I(\mathfrak{f})\})$$

and

$$T_g = K(\{\psi_A(\mathfrak{a}) \mid \mathfrak{a} \in I_g(\mathfrak{f})\}).$$

Let $r+1$ be the number of prime factors of D. Applying the argument in [3], we obtain ([5, Prop. 3.2])

Proposition 1. *We have:*
$[T_g : K] \geqq 2^r$, $[T : T_g] = h/2^r$ *and* $T_g \supset \mathrm{Im}\,\epsilon$.

Now we look the structure of T_g more closely. Let $\mathfrak{f}$ be the conductor of ϵ. Let $p_1, \ldots, p_{r+1}$ be the set of prime divisors of D. Let $\mathfrak{p}_i$ denote the prime ideal of K such that $\mathfrak{p}_i^2 = (p_i)$ and $\mathfrak{l}_i$ a prime ideal of K prime to $\mathfrak{f}$, which belongs to the same ideal class of $\mathfrak{p}_i$ ($i = 1, \ldots, r+1$). It is well known that the genus ideal class group $I_g(\mathfrak{f})/P(\mathfrak{f})$ is generated by $\mathfrak{l}_1, \ldots, \mathfrak{l}_{r+1}$. We denote by H_g the genus class field of K. Note that $[H_g : K] = 2^r$. Denote by w_0 a generator of 2-Sylow subgroup of $\mathrm{Im}\,\epsilon$. Since $\mathfrak{l}_i^2 = a_i^2\mathfrak{p}_i^2$ ($i = 1, \ldots, r+1$) for some $a_i \in K^\times$, we have

$$\psi_A(\mathfrak{l}_i) = \sqrt{\epsilon(p_i a_i^2) p_i a_i^2} = \sqrt{w_i p_i}\, a_i' z,$$

2000 Mathematics Subject Classification. Primary 11G05, 11G10, 11G15.

where $a_i' \in K^\times,\ w_i \in \langle w_0 \rangle,\ z \in \mathrm{Im}\ \epsilon$. Putting $t_{p_i} = \sqrt{w_i p_i}$, we get

$$T_g = K(\mathrm{Im}\ \epsilon,\ t_p\ (p|D)).$$

We easily have the following relations:

$$\prod_{p|D} t_p \in K(\mathrm{Im}\ \epsilon)^\times \qquad (\text{if } D \not\equiv 4 \mod 8)$$

$$\prod_{p|(D/4)} t_p \in K(\mathrm{Im}\ \epsilon)^\times \qquad (\text{if } D \equiv 4 \mod 8).$$

In the following Proposition 2 we give an expression of dimension of A. Its proof is essentially those of Theorem 3.4 and Theorem 3.5 in [5].

Proposition 2. *We suppose $h > 1$. Let A be a simple CM abelian variety over K and ϵ the associated character of A over K, of order m. Let w_0 be as above. Then we have*

$$\dim A = \begin{cases} h\,[H_g(\mathrm{Im}\ \epsilon) :\ H_g] & \text{if } \sqrt{w_0} \notin T_g \\ 2h\,[H_g(\mathrm{Im}\ \epsilon) :\ H_g] & \text{if } \sqrt{w_0} \in T_g. \end{cases}$$

In particular $\dim A = h$ *if and only if one of the following conditions holds*:
(1) $m = 2$. *A is isogenous to the scalar restriction* $\mathrm{Res}_{H/K}(E)$ *of an elliptic curve E over H.*
(2) $m = 6,\ 3 \mid D$ *and* $\epsilon_0(3a_1^2) = -1$.
(3) $m = 4,\ 2 \mid D$ *and* $\epsilon_0(2a^2)$ *is of order* 4.
(4) $m = 12,\ 6 \mid D,\ 4 \mid h,\ \epsilon_0(3a_1^2) = \pm 1$ *and* $\epsilon_0(2a^2)$ *is of order* 4.
Here ϵ_0 denotes the 2-power order part of ϵ and $a_1,\ a \in K^\times$ are chosen such that $3a_1^2$ and $2a^2$ are prime to the conductor of ϵ_0. (Clearly the choices do not affect the statements above.)

Remark 1. The condition $\epsilon_0(3a_1^2) = \pm 1$ in (4) of Proposition 2 is missing in [5, Th 3.5 (4)]. It is necessary.

Remark 2. For $h = 1$ we have a result similar to Proposition 2 and Theorem 1. It is a little bit different.

Proof. Suppose $D \not\equiv 4 \mod 8$. Then $\sqrt{-1} \notin H_g$ and $T_g(\sqrt{w_0}) = H_g(\sqrt{w_0},\ \mathrm{Im}\ \epsilon)$. We can check that $[H_g(\sqrt{w_0},\ \mathrm{Im}\ \epsilon) : H_g(\mathrm{Im}\ \epsilon)] = 2$. Suppose $D \equiv 4 \mod 8$. Then $\sqrt{-1} \in H_g,\ \sqrt{2} \notin H_g$ and $T_g(\sqrt{w_0}) = H_g(\sqrt{w_0},\ \sqrt{2},\ \mathrm{Im}\ \epsilon)$. We also have $[H_g(\sqrt{w_0},\ \sqrt{2},\ \mathrm{Im}\ \epsilon) : H_g(\mathrm{Im}\ \epsilon)] = 2$. Noting $\dim A = [T : K] = h\,[T_g : K]/[H_g : K]$, we obtain our first assertion.

If $\dim A = h$, then $\sqrt{w_0} \notin T_g$ and $H_g(\mathrm{Im}\ \epsilon) = H_g$. This implies $m \mid 12$. Furthermore if $3 \mid m$, then $\sqrt{-3} \in H_g(\sqrt{-1})$ or $H_g(\sqrt{2})$ and this shows $3 \mid D$. If $4 \mid m$ and $D \not\equiv 4 \mod 8$, then $H_g(\sqrt{-1}) = T_g(\sqrt{-1},\ \sqrt{2})$ and this shows $D \equiv 0 \mod 8$.

(1) $m = 2$. Then ϵ determines an elliptic curve E over H and $A = \mathrm{Res}_{H/K}(E)$ (the restriction of scalars of E from H to K) is an abelian variety of dimension h over K of type ϵ.

(2) $m = 6$. In this case $3 \mid D$ and $\sqrt{-3} \in T_g$. Then $[T : K] = h$ is equivalent to $\sqrt{-1} \notin T_g$. Hence $t_3 = \sqrt{-3}$, so that $\epsilon_0(3a_1^2) = -1$.

(3) $m = 4$. Since $w_0 = \sqrt{-1},\ [T : K] = h$ is equivalent to $T_g(\sqrt{w_0}) = H_g(\sqrt{w_0}) \supsetneqq H_g$, hence $\sqrt{2} \notin T_g$. Noting $t_2 = \sqrt{\epsilon_0(2a^2)2} \in T_g$, it follows that $\dim A = h$ is equivalent to $\epsilon_0(2a^2) = \pm\sqrt{-1}$.

(4) $m = 12$. In this case $6 \mid D$ and $T_g = K(\sqrt{-1},\ t_p\ (p|D))$. As in (3), if $[T : K] = h$, we have $\epsilon_0(2a^2) = \pm\sqrt{-1}$. Since $(t_3/\sqrt{3})^2 = \epsilon_0(3a_1^2)$ and $\sqrt{w_0} \notin T_g$, we obtain $\epsilon_0(3a_1^2) = \pm 1$. The converse is obvious.

2. Descent of abelian varieties.

Lemma 1. *Let B be an abelian variety over a number field M. Let L/M be a quadratic extension in the algebraic closure $\overline{M}$ of M. Let $\langle \tau \rangle = \mathrm{Gal}(L/M)$ and τ is extended to an automorphism of $\overline{M}$. Assume that over L, B is a simple abelian variety with complex multiplication by a CM field $T(\subset \overline{M})$. Let ψ_B be the Hecke character of $(B,\ \theta)$ with an isomorphism $\theta : T \to \mathcal{E}_L(B)$. Then $\psi_B^\tau(= \tau\psi_B\tau^{-1})$ is the Hecke character of $(B,\ \theta\tau_0\tau)$ where $\tau_0 : T \to T$ is an automorphism induced by $\psi_B(\mathfrak{P}) \to \psi_B(\mathfrak{P}^\tau)$ for prime ideals $\mathfrak{P}$ of L prime to the conductor of ψ_B.*

Proof. By [4, Prop. 1], ψ_B^τ is the Hecke character of $(B,\ \tau\theta\tau^{-1})$. Since $\theta(\psi_B(\mathfrak{P})^\tau)$ is the Frobenius endomorphism of B mod $\mathfrak{P}^\tau$, we have $\theta(\psi_B(\mathfrak{P}^\tau)) = \theta(\psi_B(\mathfrak{P}))^\tau$, so that $\tau\theta = \theta\tau_0$.

Theorem 1. *The notation being as in Proposition 2 and assume $h > 1$. Let A be an h-dimensional CM abelian variety over K. Let ϵ be the associated character of A. (Hence ϵ satisfies the conditions of Proposition 2.) Then A can be descended to an abelian variety over* **Q** *if and only if ϵ satisfies one of the following conditions.*
(1) $m = 2,\ \epsilon^\rho = \epsilon$.
(2) $m = 6$.
(2-i) $\epsilon^\rho = \epsilon$ *and* $\epsilon_0(3a_1a_1^\rho) = 1$.
(2-ii) $\epsilon^\rho = \epsilon^{-1}$ *and* $\epsilon_0(3a_1a_1^\rho) = -1$.
(3) $m = 4$. (3-i) $\epsilon^\rho = \epsilon$ *and* $\epsilon(2aa^\rho) = 1$.
(3-ii) $\epsilon^\rho = \epsilon^{-1}$ *and* $\epsilon(2aa^\rho) = \epsilon(2a^2)$ *is of order* 4.
(4) $m = 12$.
(4-i) $\epsilon^\rho = \epsilon,\ \epsilon_0(2aa^\rho) = 1$ *and* $\epsilon_0(3a_1a_1^\rho) = 1$.
(4-ii) $\epsilon^\rho = \epsilon^5,\ \epsilon_0(2aa^\rho) = 1$ *and* $\epsilon_0(3) = -1$.

(4-iii) $\epsilon^\rho = \epsilon^7$, $\epsilon_0(3a_1a_1^\rho) = -1$ *and* $\epsilon_0(2aa^\rho) = \epsilon_0(2a^2)$ *is of order* 4.
(4-iv) $\epsilon^\rho = \epsilon^{-1}$ *and* $\epsilon_0(2aa^\rho) = \epsilon_0(2a^2)$ *is of order* 4.
(*In case* (4-ii) *and* (4-iv), *the conductor of* ϵ_0 *is prime to* 3.)

Proof. Let ψ_A be the Hecke character over K associated to (A, θ) with $\theta : T \to \mathcal{E}_K(A)$. Assume that A descends to an abelian variety over $\mathbf{Q}$. By Lemma 1, $\psi_A^\rho (= \rho\psi_A\rho^{-1})$ is the Hecke character of $(A, \theta\tau_0\rho^{-1})$ for some $\tau_0 : T \to T$. Then we have $\rho\psi_A\rho^{-1} = \rho\tau_0^{-1}\psi_A$. Since $\rho\tau_0^{-1}\epsilon = \epsilon^i$ for an integer i prime to m, we get $\epsilon^\rho = \epsilon^i$.

(1) $m = 2$. Assume $\epsilon^\rho = \epsilon$. Let E be an elliptic curve over H associated to ϵ. We may assume that $\rho(j_E) = j_E$. By [1, § 10], E descends to $F = \mathbf{Q}(j_E) \subset H$. Then $\mathrm{Res}_{H/K}(E)$ is an h-dimensional abelian variety over K of type ϵ and descends to $\mathrm{Res}_{F/\mathbf{Q}}(E)$.

(2) $m = 6$. In this case we must have $\epsilon^\rho = \epsilon^{\pm 1}$. As in (1) let E be an elliptic curve over H associated to ϵ_0. Let k_1/H be the extension of degree 3 corresponding to $\epsilon_1 = \epsilon_0\epsilon$. k_1 is Galois over $\mathbf{Q}$. Then $\mathrm{Res}_{k_1/H}(E)$ is isogenous to $E \times A_0$ where A_0 is a 2-dimensional abelian variety over H, which is of type ϵ. We see that $\psi_{A_0} = \psi_A \circ N_{H/K}$ has values in $S = K(\sqrt{-3}) \subset T$ and A_0 can be descended to $F = \mathbf{Q}(j_E)$. By Lemma 1 there exists $\tau_0 \in \mathrm{Aut}\, S$ such that $\psi_{A_0}\rho = \tau_0\psi_{A_0}$ and $\tau_0 = \rho$ on K.

Claim. If $\epsilon^\rho = \epsilon$, then $\tau_0 = \rho$ on S. If $\epsilon^\rho = \epsilon^{-1}$, then $\tau_0(\sqrt{-3}) = \sqrt{-3}$.

Proof of Claim. Assume first $\epsilon^\rho = \epsilon$. Since there exists $\alpha \in K$ such that $\psi_{A_0}((\alpha)) = \epsilon(\alpha)\alpha$ where $\epsilon(\alpha)$ is a primitive 3rd root of unity, $\psi_{A_0}((\alpha^\rho)) = \epsilon(\alpha^\rho)\alpha^\rho = \epsilon(\alpha)\alpha^\rho$, so that $\tau_0 = \rho$. If $\epsilon^\rho = \epsilon^{-1}$, then $\psi_{A_0}((\alpha^\rho)) = \epsilon(\alpha)\alpha^\rho = \psi_{A_0}((\alpha))^{\tau_0}$. Hence $\tau_0(\epsilon(\alpha)) = \epsilon(\alpha)$. This proves Claim.

Let L_1 be the subfield of H corresponding to $\langle\mathfrak{p}_3\rangle$ in the ideal class group $\mathrm{Cl}(K)$ of K with $\mathfrak{p}_3^2 = (3)$. Denote by F_1 the fixed subfield of L_1 by ρ. Put $B = \mathrm{Res}_{F/F_1}(A_0)$. Then B is isogenous to $A_1 \times A_1'$ over L_1 with $\psi_{A_1} = \psi_A \circ N_{H/L_1}$ and $\psi_{A_1'} = \psi_{A_1}\chi_1$, where χ_1 is a character of $\mathrm{Cl}(K)$ such that $\chi(\mathfrak{p}_3) = -1$. We have

$$\mathcal{E}_{L_1}(B) \cong S[T]/(T^2 - {t_3}^2) \cong S \oplus S$$

where $t_3 = \sqrt{-3}$. The conditions (2-i) and (2-ii) are equivalent to $\psi_{A_1}\rho = \tau_0\psi_{A_1}$. If this holds, we have $\psi_{A_1'}\rho = \tau_0\psi_{A_1'}$ and $\mathcal{E}_{F_1}(B) \cong S_0 \oplus S_0$ with $S_0 = \mathcal{E}_F(A_0)$. This implies that A_1 and A_1' can be descended to F_1 and hence $A = \mathrm{Res}_{L_1/K}(A_1)$ can be descended to $\mathbf{Q}$. Conversely if A is descended to $\mathbf{Q}$, then $\psi_A\rho = \tau\psi_A$ for some $\tau \in \mathrm{Aut}\mathbf{C}$. This shows $\psi_{A_1}\rho = \tau\psi_{A_1}$. Then $\mathcal{E}_{F_1}(B) \cong S_1 \oplus S_1$ with $S_1 = \{a \in S \mid \tau(a) = a\}$. Since $\mathcal{E}_{F_1}(B)$ is S_0-algebra, we find $S_0 = S_1$, so that $\tau = \tau_0$. Hence (2-i) or (2-ii) holds.

(3) $m = 4$. We have $\epsilon^\rho = \epsilon^{\pm 1}$. Let k/H be the quadratic extension corresponding to ϵ^2 and let E be an elliptic curve defined over k corresponding to ϵ. Since $k/\mathbf{Q}$ is Galois and $\mathbf{Q}(j_E)$ has a real place, we may assume that E is defined over F' ($\mathbf{Q}(j_E) \subset F' \subset k$), which is fixed by ρ (cf. [1; §10]). Put $A_0 = \mathrm{Res}_{k/H}(E)$. Then A_0 descends to $\mathrm{Res}_{F'/F}(E)$ over F. By analogous argument as in (2), we obtain; $\mathcal{E}_H(A_0) \cong K(\sqrt{-1})$ and there exists $\tau_0 \in \mathrm{Aut}(K(\sqrt{-1}))$ such that $\psi_{A_0}\rho = \tau_0\psi_{A_0}$ with $\tau_0 = \rho$ on K. Let L be the subfield of H corresponding to $\langle\mathfrak{p}_2\rangle$ in $\mathrm{Cl}(K)$ with $\mathfrak{p}_2^2 = (2)$. Denote by F_2 the fixed subfield of L by ρ. Put $B = \mathrm{Res}_{F/F_2}(A_0)$. Then B is isogenous over L to a direct product $A_1 \times A_1'$ of abelian varieties and $\mathcal{E}_L(B) \cong S \oplus S$ with $S = K(\sqrt{-1})$. As in (2) we see that $A = \mathrm{Res}_{L/K}(A_1)$ can be descended to $\mathbf{Q}$ if and only if A_1 can be descended to F_2. Also this is equivalent to $\psi_{A_1}\rho = \tau_0\psi_{A_1}$, and we can check easily that this is equivalent to our statement (3) in Theorem 1.

(4) $m = 12$. Let $\epsilon = \epsilon_0\epsilon_1$. If A is defined over $\mathbf{Q}$, then $\epsilon_0^\rho = \epsilon_0^{\pm 1}$ and $\epsilon_1^\rho = \epsilon_1^{\pm 1}$. Let k and k_1 be the extensions of H corresponding to ϵ_0^2 and ϵ_1, respectively. Using ϵ_0, we define E and $A_0 = \mathrm{Res}_{k/H}(E)$ as in (3). Then $\mathrm{Res}_{k_1/H}(A_0)$ is isogenous to $A_0 \times A_0'$ over H, where A_0' is a 4-dimensional abelian variety corresponding to ϵ with $\mathcal{E}_H(A_0') = K(\sqrt{-1}, \sqrt{-3})$. Since A_0 is defined over F, we may assume that A_0' is defined over F. As in case (2) and (3), there exists $\tau_0 \in \mathrm{Aut}(K(\sqrt{-1}, \sqrt{-3}))$ such that $\psi_{A_0'}\rho = \tau_0\psi_{A_0'}$. Let L_0 be the subfield of H corresponding to $\langle\mathfrak{p}_2, \mathfrak{p}_3\rangle$ in $\mathrm{Cl}(K)$ and denote by F_0 the fixed subfield of L_0 by ρ. Put $B = \mathrm{Res}_{F/F_0}(A_0')$. Then over L_0, B is isogenous to a product $C_1 \times C_2 \times C_3 \times C_4$ of four abelian varieties. It follows that $A_i = \mathrm{Res}_{L_0/K}(C_i)$ ($i = 1, 2, 3, 4$) are abelian varieties over K of type ϵ and $\psi_{A_i} = \psi_{A_1}\chi_i$ ($i = 2, 3, 4$), where χ_i are characters of $\mathrm{Cl}(K)$ such that they induce on $\langle\mathfrak{p}_2, \mathfrak{p}_3\rangle$ distinct non-trivial characters. A is isogenous to one of A_i ($i = 1, 2, 3, 4$). As in case (2) and (3), A can be descended to $\mathbf{Q}$ if and only if $\psi_{C_1}\rho = \tau_0\psi_{C_1}$. We can check that this is equivalent to the statement (4) in Theorem 1. For example, in case (4-ii), we have $\epsilon_0(3a_1^2) = \epsilon_0(3a_1a_1^\rho) = -1$. If the conductor

of ϵ_0 is not prime to 3, write $\epsilon_0 = \eta_3 \cdot \eta$, where η_3 has conductor $\mathfrak{p}_3$ (see [2; §3]) and η has conductor prime to 3. Putting $a_1 = \sqrt{D}/3$, we see $3a_1^2 = -3a_1a_1^\rho$. Since $\eta_3(-1) = -1$, it follows that $\epsilon_0(3a_1^2) = \eta_3(3a_1^2)\eta(3) = \eta_3(-3a_1a_1^\rho)\eta(3) = -\epsilon_0(3a_1a_1^\rho)$, a contradiction. Hence the conductor of ϵ_0 is prime to 3.

3. Construction of characters. We are going to construct explicitely characters ϵ over K with the following property; the CM abelian variety A over K of type ϵ can be descended to $\mathbf{Q}$ and has dimension h. The characterization of such ϵ is given in Theorem 1. Let m be the order of ϵ.

1. $m = 2$. Then ϵ corresponds to a $\mathbf{Q}$-curve over H whose Hecke character satisfy the condition (Sh) in [2, §4]. Such ϵ exists only when D is divisible by 8 or D has a prime divisor q with $q \equiv -1 \bmod 4$. A classification of ϵ is given in [2, Theorem 2 and Theorem 3].

2. $m = 6$. Let $\epsilon = \epsilon_0\epsilon_1$ be the decomposition such that ϵ_0 has order 2 and ϵ_1 has order 3. Then ϵ_0 is a character in Case 1. Since $\epsilon_1^\rho = \epsilon_1^{\pm 1}$, ϵ_1 corresponds to a cubic extension k_1/H such that $k_1/\mathbf{Q}$ is Galois.

3. $m = 4$. For a rational prime ℓ, we denote by U_ℓ the local unit group $U(K \otimes \mathbf{Q}_\ell)$ at ℓ. We can think of ϵ as a character of $U_K = \prod_\ell U_\ell$. Then we can write uniquely $\epsilon = \prod_\ell \epsilon_\ell$, where ϵ_ℓ is a character of U_ℓ of order dividing 4. It is obvious that $\epsilon^\rho = \epsilon$ (resp. $\epsilon^\rho = \epsilon^{-1}$) if and only if $\epsilon_\ell^\rho = \epsilon_\ell$ (resp. $\epsilon_\ell^\rho = \epsilon_\ell^{-1}$) for every ℓ. Let us ask for a local character λ of U_ℓ of order 4 such that $\lambda^\rho = \lambda^{\pm 1}$ and $\lambda(2a^2)$ is of order 4, where $2a^2$ ($a \in K^\times$) is prime to ℓ.

(i) $\ell \not| D$. Since $\lambda^\rho = \lambda^{\pm 1}$, we find that $\lambda(\mathbf{F}_\ell^\times) = \pm 1$ and $\lambda(2a^2) = \lambda(2) = \pm 1$.

(ii) $\ell \mid D$, $\ell \neq 2$. Since $\lambda^2(2) = \left(\dfrac{2}{\ell}\right) = -1$, we must have $\ell \equiv 5 \bmod 8$. In this case there exists only two characters $\lambda^{\pm 1}$ of order 4 such that $\lambda^\rho = \lambda^{-1}$ and $\lambda(2)$ is of order 4.

(iii) $\ell = 2$. We use the notation of [2, § 2]. Let X_2^0 be the set of characters $\nu : U_2 \to \pm 1$ such that $\nu^\rho = \nu$. We cosider in cases.

I. $D \equiv -4m$ with $m = 1 + 4k$. If we put $a = \frac{1+\sqrt{-m}}{2}$, then $2a^2 = \sqrt{-m} - 2k$ and $2aa^\rho = 1 + 2k$. Since $\lambda^2 \in X_2^0 = \langle \eta_{-4},\ \epsilon_8 \rangle$ by [2, Proposition 2], we have $\lambda(\mathbf{Z}_2^\times) = \pm 1$. Put $c_1 = \sqrt{-m}$ and $c_3 = 3 - 2\sqrt{-m}$ ($\in 1 + \mathfrak{p}_2^3$), then

$$(1 + \mathfrak{p}_2)/(1 + \mathfrak{p}_2^6) \cong \langle c_1 \rangle \times \langle c_3 \rangle \times \langle 5 \rangle$$

where $\langle c_1 \rangle$ and $\langle c_3 \rangle$ are cyclic of oeder 4. Let δ be a character of U_2 such that $\delta(c_1) = \sqrt{-1}$, $\delta(c_3) = \delta(5) = 1$. Then $\delta^\rho = \delta$, $\delta^2 = \eta_{-4}$, $\delta(-1) = -1$ and $\delta(2a^2)$ is of order 4. We have

$$\delta(2aa^\rho) = \begin{cases} 1 & \text{if } m \equiv 1 \bmod 8 \\ -1 & \text{if } m \equiv 5 \bmod 8. \end{cases}$$

Let ϕ be a character of U_2 such that $\phi(c_3) = \sqrt{-1}$ and Ker $\phi = \langle c_1,\ \mathbf{Z}_2^\times \rangle$. Then $\phi^\rho = \phi$ and $\phi(2aa^\rho) = 1$. Moreover we have; if $m \equiv 1 \bmod 8$, then $\phi^2 = \epsilon_8$ and $\phi(2a^2) = \pm 1$; if $m \equiv 5 \bmod 8$, then $\phi^2 = \epsilon_8\eta_{-4}$ and $\phi(2a^2)$ is of order 4. Therefore if $m \equiv 1 \bmod 8$, δ and $\delta\phi$ satisfy the condition (3-i) of Theorem 1. For an odd prime divisor p of D, η_p denotes the unique quadratic character of U_p. If $m \equiv 5 \bmod 8$, then m has a prime divisor p with $p \equiv 5 \bmod 8$ or a pair of prime divisors q_1, q_2 satisfying $q_1 \equiv 3 \bmod 8$ and $q_2 \equiv -1 \bmod 8$. We check easily that $\eta_p\delta$ and $\eta_{q_1}\eta_{q_2}\delta$ satisfy the condition (3-i) of Theorem 1. We denote by δ_0 either $\eta_p\delta$ or $\eta_{q_1}\eta_{q_2}\delta$. Further if m ($m \equiv 5 \bmod 8$) has a prime divisor q with $q \equiv 7 \bmod 8$, then $\eta_q\phi$ also satisfies the condition (3-i) of Theorem 1.

II. $D = -8m$. We put $a = \sqrt{-2m}/2$. Then $-m = 2a^2$ and $m = 2aa^\rho$. By [2, Proposition 2], $X_2^0 = \langle \eta_{-8},\ \epsilon_4 \rangle$ if $m \equiv 1 \bmod 4$ and $X_2^0 = \langle \eta_8,\ \epsilon_4 \rangle$ if $m \equiv -1 \bmod 4$. If $m \equiv 1 \bmod 4$, then $\lambda^2 = \epsilon_4$ because $\eta_{-8}(-1) = -1$. Since $\epsilon_4(-m) = 1$, we see $\lambda(-m) = \pm 1$. Hence there are no characters satisfying (3) of Theorem 1 in this case.

Suppose $m \equiv -1 \bmod 4$. Let κ be a character of $(\mathbf{Z}/32\mathbf{Z})^\times$ such that $\kappa(5)$ is of order 8 and $\kappa(-1) = 1$. Define $\omega = \kappa \circ \mathrm{N}_{K/\mathbf{Q}}$. Then ω is a character of U_2 of order 4 with the following properties; if $m \equiv 3 \bmod 8$, then $\omega(\pm m)$ is of order 4 and $\omega^2 = \eta_8\epsilon_4$ and if $m \equiv 7 \bmod 8$, then $\omega(\pm m) = \pm 1$ and $\omega^2 = \eta_8$. Put $c_1 = 1 + \sqrt{-2m}$, then $U_2/\mathbf{Z}_2^\times U_2^4 \cong \langle c_1 \rangle$ is cyclic of order 4. Hence we can define a character ϕ of U_2 of order 4 by $\phi(c_1) = \sqrt{-1}$ and $\phi(\mathbf{Z}_2^\times) = 1$. We have $\phi^\rho = \phi$ and $\phi^2 = \epsilon_4$. Since $m \equiv 3 \bmod 8$, m has a prime divisor q with $q \equiv 3 \bmod 4$. Then $\lambda_1 = \eta_q\omega$ satisfies the condition (3-ii) of Theorem 1.

Summing up the above arguments, we obtain the following results.

(a) The set of characters $\mathcal{C}$ satisfying the condition (3-i).

Let Y be the set of quadratic characters χ of U_K such that

$$\chi^\rho = \chi, \quad \chi(-1) = \chi(2aa^\rho) = 1.$$

If $D = -4m$, $m \equiv 1 \bmod 8$, then $\mathcal{C} = \delta Y \cup \delta\phi Y$.

If $D = -4m$, $m \equiv 5 \mod 8$, then $\mathcal{C} = \delta_0 Y$. Furthermore if m has a prime divsor q with $q \equiv 7 \mod 8$, then $\mathcal{C} = \eta_q \phi Y$.

(b) The set of characters $\mathcal{C}'$ satisfying the condition (3-ii).

Let Y' be the set of characters χ of U_K of order dividing 4 such that

$$\chi^\rho = \chi^{-1}, \quad \chi(-1) = 1, \quad \chi(2a^2) = \chi(2aa^\rho) = \pm 1.$$

If D has a prime divisor p with $p \equiv 5 \mod 8$, we have $\mathcal{C}' = \lambda_p Y'$.

If $D = -8m$ with $m \equiv 3 \mod 8$, for a prime divisor q of D with $q \equiv 3 \mod 4$, we have $\mathcal{C}' = \eta_q \omega Y'$.

Remark 3. In case $D = -8m$ with $m \equiv 3 \mod 8$, the character $\lambda_2 = \eta_{-8} \phi \omega$ satisfies

$$\lambda_2^\rho = \lambda_2^{-1},\ \lambda_2(-1) = -1,\ \lambda_2(-m) : \text{of order } 4.$$

Since $\lambda_2(-m) \neq \lambda_2(m)$, λ_2 does not satisfy (3-ii).

4. $m = 12$. Let $\epsilon = \epsilon_0 \epsilon_1$ be the decomposition such that ϵ_0 has order 4 and ϵ_1 has order 3. According to $\epsilon_1^\rho = \epsilon_1$ or $\epsilon_1^\rho = \epsilon_1^{-1}$, it suffices to choose ϵ_0 from the characters constructed in case 3 to satisfy the conditions (4) of Theorem 1.

References

[1] B. H. Gross, *Arithmetic on elliptic curves with complex multiplication*, Lecture Notes in Math. 776, Springer, Berlin, 1980.

[2] T. Nakamura, A classification of **Q**-curves with complex multiplication, J. Math. Soc. Japan **56** (2004), no. 2, 635–648.

[3] D. E. Rohrlich, Galois conjugacy of unramified twists of Hecke characters, Duke Math. J. **47** (1980), no. 3, 695–703.

[4] G. Shimura, On the zeta-function of an abelian variety with complex multiplication, Ann. of Math. (2) **94** (1971), 504–533.

[5] T. Yang, On CM abelian varieties over imaginary quadratic fields, Math. Ann. **329** (2004), no. 1, 87–117.