ACTA ARITHMETICA
XCVII.4 (2001)

On abelian varieties associated with elliptic curves with complex multiplication

by

TETSUO NAKAMURA (Sendai)

1. Introduction. Let K be an imaginary quadratic field and H the Hilbert class field of K. Let E be an elliptic curve over H with complex multiplication by K. We suppose that E is a K-curve, that is, for each $\sigma \in \mathrm{Gal}(H/K)$, E^σ and E are H-isogenous. We denote by $B = R_{H/K}(E)$ the abelian variety over K which is obtained from E by restriction of scalars. We will show that one of the following three cases holds (see Theorem 3):

(i) B is a simple CM-type abelian variety over K.

(ii) B is isogenous to a product $A \times \ldots \times A$ of a simple non-CM abelian variety A such that $\mathrm{End}_K A \otimes \mathbb{Q}$ is commutative.

(iii) B is isogenous to a product $A \times \ldots \times A$ of a simple non-CM abelian variety A such that $\mathrm{End}_K A \otimes \mathbb{Q}$ is a division quaternion algebra.

Some examples of these cases are discussed in Section 4. In [B-Gr] and [Gr], $\mathbb{Q}$-curves are treated under the assumption that the class number h of K is odd. Such a curve E is a K-curve satisfying the condition: E^τ and E are H-isogenous, where τ is the complex conjugation. In this case, it is shown that B is a simple CM-type abelian variety (see [Gr], § 15).

Throughout the paper elliptic curves have complex multiplication by K and the following notation is used:

- K — an imaginary quadratic field,
- $Cl(K)$ — the ideal class group of K,
- h — the class number of K,
- H — the Hilbert class field of K,
- $G(L/k)$ — the Galois group of a Galois extension L/k,
- I_k, C_k — the idele group and the idele class group of a number field k,
- $R_{k/M}(E)$ — the abelian variety over M which is obtained from an elliptic curve E over k by restriction of scalars to M.

2000 *Mathematics Subject Classification*: 11G05, 11G10, 11G15.

2. ***K*-curves and descending characters.** Let M be a finite extension of K and L be a finite Galois extension of M. Let E be an elliptic curve over L with complex multiplication by K. Denote by J the set of $\sigma \in G(L/M)$ such that E^σ is isogenous to E over L. Clearly J is a subgroup of $G(L/M)$ and we obtain (cf. [Gr], Chap. 4)

$$\dim_K \mathrm{End}_M R_{L/M}(E) \otimes \mathbb{Q} = |J|.$$

DEFINITION. 1. If $J = G(L/M)$, then we call E an *M-curve*.

2. Let ψ_E be the Hecke character of an elliptic curve E over L. If there exists a Hecke character ϕ of M such that $\psi_E = \phi \circ N_{L/M}$, we say that ψ_E *descends* to M or simply that E has an *M-character* ϕ.

REMARK. 1. The following fact is well known: ψ_E descends to M if and only if all the points of E of finite order are rational over $M^{\mathrm{ab}}L$, where M^{ab} is the maximal abelian extension of M (see [S1], Theorem 7.44).

2. For an elliptic curve E over H there exists an elliptic curve E_0 over H such that $j_E = j_{E_0}$ and E_0 has a K-character (see [S2], Prop. 5, p. 525).

THEOREM 1. *Let E, L, M be as above and assume that L is abelian over M. Then the following conditions are equivalent*:

(i) $L(E_{\mathrm{tors}})$ *is an abelian extension of M.*

(ii) *The abelian variety $B = R_{L/M}(E)$ has complex multiplication over M in the sense that*

$$\mathrm{End}_M B \otimes \mathbb{Q} \cong \prod_{i=1}^{r} T_i$$

where T_i $(i = 1, \ldots, r)$ are (CM) fields over K such that

$$\sum_i [T_i : K] = [L : M] \ (= \dim B).$$

(iii) *E has an M-character.*

In case $K = M$, the theorem is Théorème 4.1 in [G-Sch] and since our assertion is proved similarly, we omit its proof. If $L = H$, we have the following:

THEOREM 2. *Let M be a subfield of H containing K. If E is an elliptic curve over H with an M-character, then $B = R_{H/M}(E)$ is a simple CM type abelian variety over M, which means that* $\mathrm{End}_M B \otimes \mathbb{Q}$ *is a field over K of degree $[H : M]$.*

Proof. Since $R = \mathrm{End}_K B \otimes \mathbb{Q}$ is commutative by Theorem 1, it suffices to show that R is a field of degree $[H : M]$ over K. If $M = K$ and h is odd, the proof is given in [Gr], Chap. 4. Our proof proceeds similarly. Let Y be the subgroup of $Cl(K)$ corresponding to M. Let $\mathfrak{a}$ be an integral ideal in Y. One can associate with $\mathfrak{a}$ an M-endomorphism $t(\mathfrak{a})$ of B with the following property: If $\mathfrak{a}^n \sim 1$, then $t(\mathfrak{a})^n \in K$ and $\mathfrak{a}^n = (t(\mathfrak{a})^n)$ (see [Gr], Chap. 4). For a prime number p, let Y_p be the p-Sylow subgroup of Y and put $p^r = |Y_p|$. For a set of independent generators $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ for Y_p, let X_p be the subgroup of $K^\times/K^{\times p^r}$ generated by $\{t(\mathfrak{a}_i)^{p^r} \mid 1 \le i \le s\}$. Then Y_p is isomorphic to X_p. Let $T_p = K(\{t(\mathfrak{a}_i) \mid 1 \le i \le s\})$. It suffices to show that T_p is a field over K of degree p^r, because we then have $\dim_K R = \dim_K \prod_p T_p$. Write $\mu(p^r)$ for the group of p^rth roots of unity and put $K' = K(\mu(p^r))$. Now we use the following lemma which follows from [W], Lemma 13.27.

Lemma 1. *If p is odd, then $H^1(G(K'/K), \mu(p^r)) = (0)$. If $p = 2$, then $H^1(G(K'/K(\sqrt{-1})), \mu(p^r)) = (0)$.*

If p is odd, then $K^\times/K^{\times p^r} \to K'^\times/K'^{\times p^r}$ is injective by Lemma 1. Since $K' T_p$ is a Kummer extension of K' corresponding to the subgroup X_p, it follows that T_p is a field over K of degree p^r. Now assume $p = 2$. It suffices to consider the case when $h > 1$ and the exponent of the group Y_2 is greater than 2. Then $K(\sqrt{-1})$ $(= K_1$ say$) \ne K$ and $\mu(4) = \mu(2^r)^{G(\overline{K}/K_1)}$. In the restriction inflation sequence

$$0 \to H^1(G(K_1/K), \mu(4)) \ (\cong \mathbb{Z}/2\mathbb{Z}) \xrightarrow{i} K^\times/K^{\times 2^r} \to K_1^\times/K_1^{\times 2^r}$$

the image of i corresponds to the extension K_1/K. From this we see that T_2 is a field over K of degree 2^r, since $K_1^\times/K_1^{\times 2^r} \to K'^\times/K'^{\times 2^r}$ is injective by Lemma 1. This completes the proof of Theorem 2. ∎

3. The abelian variety $R_{H/K}(E)$

Lemma 2. *Let M be a subfield of H containing K. Let E_0 be an elliptic curve over H with an M-character. Let E be a twist of E_0 corresponding to a quadratic extension k/H. Then*

(i) *E is an M-curve if and only if k/M is Galois.*
(ii) *E has an M-character if and only if k/M is abelian.*

Proof. Let ψ_0, ψ be Hecke characters of E_0, E, respectively. Then by [Gr], Lemma 9.2.5, we have $\psi = \psi_0 \cdot \chi$, where $\chi : I_H \to \{\pm 1\}$ is the character associated with the extension k/H.

(i) E is an M-curve if and only if $\psi^\sigma = \psi$ $(\sigma \in G(H/M))$ (see [Gr], §11). Our assertion follows from the equivalence of the following assertions:

(1) $\psi^\sigma = \psi$ $(\sigma \in G(H/M))$.
(2) $\chi^\sigma = \chi$ $(\sigma \in G(H/M))$.
(3) $\operatorname{Ker} \chi$ is $G(H/M)$-stable.
(4) k/M is Galois.

(ii) If k/M is abelian, our assertion is clear by Theorem 1, since $R_{k/M}(E_0) \cong R_{k/M}(E)$. Now assume that ψ descends to M. Then $\psi = \phi \circ N_{H/M}$ and

$\psi_0 = \phi_0 \circ N_{H/M}$, where ϕ and ϕ_0 are characters of I_M. As E_0 and E are isomorphic over k, ϕ and ϕ_0 coincide on the norm subgroup $P_k = N_{k/M}(C_k)$ of C_M. Since χ is non-trivial, ϕ and ϕ_0 differ on $P_H = N_{H/M}(C_H)$ ($\supset P_k$). This implies that $P_H \neq P_k$, which shows that k/M is abelian. ∎

THEOREM 3. *Let E be a K-curve over H and put $B = R_{H/K}(E)$ and $R = \mathrm{End}_K B \otimes \mathbb{Q}$. If E has a K-character, R is a field of degree h over K. If E has no K-characters, then the center Z of R is a field of degree h_0 over K with $h = 2^{2m}h_0$ ($m \geq 1$) and one of the following two cases holds*:

(i) $R \cong \mathrm{M}_{2^m}(Z)$. *In this case, B is isogenous over K to a product of A with itself 2^m times, where A is K-simple, $2^m h_0$-dimensional and $Z = \mathrm{End}_K A \otimes \mathbb{Q}$.*

(ii) $R \cong \mathrm{M}_{2^{m-1}}(D)$, *where D is a division quaternion algebra over Z. In this case, B is isogenous over K to a product of A with itself 2^{m-1} times, where A is K-simple, $2^{m+1}h_0$-dimensional and $D = \mathrm{End}_K A \otimes \mathbb{Q}$.*

Proof. Choose an elliptic curve E_0 over H with a K-character such that $j_E = j_{E_0}$ (see Remark 2). If E and E_0 are isomorphic over H, our assertion follows from Theorem 2. Assume that E and E_0 are not isomorphic over H. Since it suffices to consider the case $h > 1$, there exists a unique quadratic extension k of H such that E and E_0 are isomorphic over k. Then k/K is Galois by Lemma 2 and we have an exact sequence

$$1 \to G(k/H)\ (\cong \{\pm 1\}) \to G(k/K) \to G(H/K)\ (\cong Cl(K)) \to 1.$$

LEMMA 3. *Let C be the center of $G = G(k/K)$. Then C contains $G(k/H)$ and G/C is an elementary abelian group of order 2^{2m} ($m \geq 0$) with $2m \leq \dim Cl(K) \otimes \mathbb{F}_2$. If G is non-commutative, there exist $x_1, \dots, x_m, y_1, \dots, y_m \in G$ which induce a basis of G/C and satisfy the following commutator relations*:

$$[x_i, y_i] = -1, \qquad [x_i, x_j] = [y_i, y_j] = [x_i, y_j] = 1 \qquad (i \neq j).$$

Proof of Lemma 3. Since the commutator map

$$G \times G \ni (x, y) \to [x, y] \in \{\pm 1\}$$

induces a non-degenerate alternating form on $G/C \times G/C$, our assertion follows easily. ∎

If E has a K-character, then $R = \mathrm{End}_K(R_{H/K}(E)) \otimes \mathbb{Q}$ is a field of degree h over K by Theorem 2. Now we assume that E is a K-curve but has no K-characters, which means that G is non-commutative by Lemma 2. Let $m \geq 1$ be as in Lemma 3 and put $h_0 = h/2^{2m} = |C/\{\pm 1\}|$. Write M_0 and M_i for the subfields of H corresponding to C and $\langle x_i, y_i, C\rangle$, respectively. As $G(k/M_0) = C$ is commutative, we see that E has an M_0-character by Lemma 2 and $Z = \mathrm{End}_{M_0}(R_{H/M_0}(E)) \otimes \mathbb{Q}$ is a field over K of degree h_0

by Theorem 2. On the other hand as $G(k/M_i)$ is non-commutative, E has no M_i-characters by Lemma 2. Then by taking $L = H$ in Theorem 1, we see that $D_i = \mathrm{End}_{M_i}(R_{H/M_i}(E)) \otimes \mathbb{Q}$ is not a direct product of fields. As D_i is semisimple, this means that D_i is a non-commutative subring of R containing Z. By the map $G \to G(H/K) \cong Cl(K)$, x_i and y_i determine elements of $Cl(K)$ and as in the proof of Theorem 2, they correspond to elements s, t of D_i. We see that $D_i = Z[s,t]$ and $s^2, t^2 \in Z$. According to [Gr], p. 47, st and ts differ by a root of unity in K; we get $st = -ts$. Therefore D_i is a quaternion algebra over Z. For $j \neq i$, we also have

$$D_j = \mathrm{End}_{M_j}(R_{H/M_j}(E)) \otimes \mathbb{Q} = Z[s', t']$$

where s', t' are elements of D_j corresponding to x_j, y_j, respectively. Let N be the subfield of H corresponding to $\langle x_i, x_j, C\rangle$. Since $\langle x_i, x_j, C\rangle$ is commutative, E has an N-character by Lemma 2, so that $D' = \mathrm{End}_N(R_{H/N}(E)) \otimes \mathbb{Q}$ is a field by Theorem 2. As $s, s' \in D' \subset R$, we have $ss' = s's$. The same arguments show that elements of D_i commute with those of D_j. Consequently, $D_i \cdot D_j = D_i \otimes_Z D_j$ in R and in particular

$$R = D_1 \otimes_Z \ldots \otimes_Z D_m.$$

In the Brauer group, the class to which R belongs is a product of quaternion algebras; this implies that $R \cong \mathrm{M}_{2^m}(Z)$ or $R \cong \mathrm{M}_{2^{m-1}}(D)$, where D is a division quaternion algebra over Z. This completes the proof of Theorem 3. ∎

COROLLARY 1. *If the* 2*-Sylow subgroup of* $Cl(K)$ *is cyclic*, *i.e.*, *if the discriminant of* K *is divisible by at most two distinct primes*, *then every* K*-curve over* H *has a* K*-character.*

Proof. The inequality $2m \le \dim Cl(K) \otimes \mathbb{F}_2$ in Lemma 3 implies that $G(k/K)$ is commutative. Our assertion follows immediately from Lemma 2. ∎

4. Examples. We are going to discuss examples which show that both cases (i) and (ii) of Theorem 3 are possible.

Let p_1, p_2 and q be three rational primes such that

$$p_1 \equiv p_2 \equiv 1 \bmod 4, \quad q \equiv 3 \bmod 4.$$

The imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p_1 p_2 q})$ has discriminant $-p_1 p_2 q$. Let $\mathfrak{q}$ be the prime ideal of K with $\mathfrak{q}^2 = (q)$ and $\left(\frac{\alpha}{\mathfrak{q}}\right)$ denote the quadratic residue symbol mod $\mathfrak{q}$. Let ϕ_0 be a Hecke character of K such that for any principal ideal (α) of K prime to $\mathfrak{q}$,

$$\phi_0((\alpha)) = \left(\frac{\alpha}{\mathfrak{q}}\right)\alpha.$$

There are h such characters (see [S2], p. 527, Example 3). We assume that

(∗) the 2-Sylow subgroup of $Cl(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Let K_0 be the subfield of H over K such that $G(H/K_0) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and put $K_i = K_0(\sqrt{p_i})$ $(i = 1, 2)$. Let k be a quadratic extension of H such that k/K is Galois with non-commutative Galois group. Then $G(k/K_0)$ is of order 8 and is isomorphic to either the quaternion group or the dihedral group. Let E_0 be an elliptic curve over H which corresponds to the Hecke character $\psi_0 = \phi_0 \circ N_{H/K}$. We write E for a twist of E_0 with respect to k/H, so that the Hecke character of E over H is $\psi = \psi_0 \cdot \chi$, where χ is the character defined as in the proof of Lemma 2. If we put $D = \mathrm{End}_{K_0}(R_{H/K_0}(E)) \otimes \mathbb{Q}$, then we see that

$$R = \mathrm{End}_K(R_{H/K}(E)) \otimes \mathbb{Q} = Z \otimes_K D,$$

where Z is the center of R. For the prime ideal $\mathfrak{p}_i$ of K with $\mathfrak{p}_i^2 = (p_i)$ $(i = 1, 2)$, choose prime ideals $\mathfrak{l}_i$ of K such that $\mathfrak{p}_i$ and $\mathfrak{l}_i$ belong to the same class in $Cl(K)$ and the $\mathfrak{l}_i$ are unramified in k/K. Let $\mathfrak{L}_1$ be a prime ideal of H lying over $\mathfrak{l}_1$. The decomposition field Z_1 of $\mathfrak{L}_1$ is of index 2 in H. As k/Z_1 is abelian, there exists a Z_1-character ψ_1 such that $\psi = \psi_1 \circ N_{H/Z_1}$. Let $\mathcal{L}_1$ be the restriction of $\mathfrak{L}_1$ to Z_1. Then $\psi(\mathfrak{L}_1) = \psi_1(\mathcal{L}_1^2)$ and

$$\psi(\mathfrak{L}_1) = \psi_0(\mathfrak{L}_1)\chi(\mathfrak{L}_1) = \phi_0(\mathfrak{l}_1^2)\chi(\mathfrak{L}_1)$$

where $\chi(\mathfrak{L}_1) = \pm 1$ and $\phi_0(\mathfrak{l}_1^2) = \left(\frac{p_1}{q}\right) p_1 a_1^2$ with $\mathfrak{l}_1 = a_1 \mathfrak{p}_1$ $(a_1 \in K^\times)$. Now let $\psi_1(\mathcal{L}_1)$ be an element of $\mathrm{End}_{Z_1}(R_{H/Z_1}(E)) \subset D$ satisfying $\psi_1(\mathcal{L}_1)^2 = \psi(\mathfrak{L}_1)$. A similar argument also holds for $\mathfrak{l}_2$. Therefore D is a quaternion algebra over K generated by t_1 and t_2 with $t_i^2 = \widehat{p}_i = \pm p_i$ $(i = 1, 2)$ and $t_1 t_2 = -t_2 t_1$. This implies that the splitting of D is completely determined by the Hilbert norm residue symbol $\left(\frac{\widehat{p}_1,\, \widehat{p}_2}{\mathfrak{p}}\right)$. We easily get $\left(\frac{\widehat{p}_1,\, \widehat{p}_2}{\mathfrak{p}}\right) = 1$ for a prime ideal $\mathfrak{p}$ of K prime to 2. Therefore if 2 does not split in K, we obtain $D \cong \mathrm{M}_2(K)$ by the product formula of the norm residue symbol. From now on we suppose that 2 splits in K. Let $\mathfrak{p}$ be a prime ideal of K over 2. We seek a condition for $\left(\frac{\widehat{p}_1,\, \widehat{p}_2}{\mathfrak{p}}\right) = -1$. Since the localization of K with respect to $\mathfrak{p}$ is $\mathbb{Q}_2$, we have $\left(\frac{\widehat{p}_1,\, \widehat{p}_2}{\mathfrak{p}}\right) = -1$ if and only if $\widehat{p}_i = -p_i$ $(i = 1, 2)$.

1) If $G(k/K_0)$ is the quaternion group, then the $G(k/K_i)$ are cyclic and this implies $\chi(\mathfrak{L}_i) = -1$ $(i = 1, 2)$. Therefore if $\widehat{p}_i = -p_i$, then $\left(\frac{p_i}{q}\right) = 1$ $(i = 1, 2)$, which contradicts the assumption $(*)$ (see [R-R]).

2) If $G(k/K_0)$ is dihedral, then $G(k/K_0)$ has a unique cyclic subgroup of order 4. Assume that the $G(k/K_i)$ $(i = 1, 2)$ are not cyclic. Then we have $\chi(\mathfrak{L}_i) = 1$. Consequently, $\left(\frac{\widehat{p}_1,\, \widehat{p}_2}{\mathfrak{p}}\right) = -1$ if and only if $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = -1$.

Since $\left(\frac{p_1,\, p_2}{\mathfrak{p}}\right) = 1$ for all places $\mathfrak{p}$ of K, there exist $a,\ b,\ c\ (\neq 0)$ in K satisfying

$$a^2 = p_1 b^2 + p_2 c^2.$$

Put $x = \sqrt{a + b\sqrt{p_1}}$ and $k = H(x)$. Then k/K_0 is Galois, $G(k/K_0)$ is dihedral and $G(k/K_0(\sqrt{p_i}))$ $(i = 1, 2)$ is not cyclic (cf. [Se], 1.2). For example, take $p_1 = 5$, $p_2 = 17$, $q = 3$. Then $h = 12$ and 2 splits in K. Since $\left(\frac{p_i}{q}\right) = -1$ $(i = 1, 2)$, we see that R is a division quaternion algebra over a field Z of degree 3 over K.

References

[B-Gr] J. P. Buhler and B. H. Gross, *Arithmetic on elliptic curves with complex multiplication. II*, Invent. Math. 79 (1985), 11–29.

[G-Sch] C. Goldstein et N. Schappacher, *Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe*, J. Reine Angew. Math. 327 (1981), 184–218.

[Gr] B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Lecture Notes in Math. 776, Springer, 1980.

[R-R] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1934), 69–74.

[Se] J.-P. Serre, *Topics in Galois Theory*, Jones and Bartlett, Boston, 1993.

[S1] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton Univ. Press, 1971.

[S2] —, *On the zeta function of an abelian variety with complex multiplication*, Ann. of Math. 94 (1971), 504–533.

[W] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, New York, 1980.

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan
E-mail: nakamura@math.tohoku.ac.jp

Received on 28.5.1999
and in revised form on 3.7.2000 (3608)