

## CYCLIC TORSION OF ELLIPTIC CURVES

TETSUO NAKAMURA

(Communicated by William W. Adams)

*Dedicated to Professor Tsuneo Kanno on his seventieth birthday*

ABSTRACT. Let  $E$  be an elliptic curve over a number field  $k$  such that  $\text{End}_k E = \mathbf{Z}$  and let  $w(k)$  denote the number of roots of unity in  $k$ . Ross proposed a question: Is  $E$  isogenous over  $k$  to an elliptic curve  $E'/k$  such that  $E'(k)_{\text{tors}}$  is cyclic of order dividing  $w(k)$ ? A counter-example of this question is given. We show that  $E$  is isogenous to  $E'/k$  such that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/w(k)^2\mathbf{Z}$ . In case  $E$  has complex multiplication and  $\text{End}_k E = \mathbf{Z}$ , we obtain certain criteria whether or not  $E$  is isogenous to  $E'/k$  such that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/2\mathbf{Z}$ .

### INTRODUCTION

Let  $k$  be a field finitely generated over its prime field, and let  $w(k)$  denote the number of roots of unity in  $k$ . For an elliptic curve  $E$  over  $k$ , Ross [2] proposed the following question:

**Question 1.** If  $\text{End}_k E = \mathbf{Z}$ , then is  $E$  isogenous over  $k$  to an elliptic curve  $E'/k$  such that  $E'(k)_{\text{tors}}$ , the  $k$ -rational torsion points of  $E'$ , is cyclic of order dividing  $w(k)$ ?

In this paper we assume that  $k$  is a finite extension of the rationals  $\mathbf{Q}$ . An example in Section 4 shows that Question 1 does not hold in general. Put  $D = \text{Min} |E'(k)_{\text{tors}}|$ , where the minimum is taken over those  $E'/k$  which are isogenous to  $E$  over  $k$ . We will show in Section 2 that if  $\text{End}_k E = \mathbf{Z}$ , then  $D | w(k)^2$  and  $E$  is isogenous over  $k$  to an elliptic curve  $E'/k$  such that  $E'(k)_{\text{tors}}$  is cyclic of order  $D$  (Theorem 1). In Section 3 we treat an elliptic curve  $E$  over  $k$  with  $\text{End}_k E = \mathbf{Z}$ , but which has complex multiplication by an imaginary quadratic field  $K$ . We will prove that  $E$  is  $k$ -isogenous to  $E'/k$  such that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/4\mathbf{Z}$ . We will also give certain criteria for  $E'$  to be chosen so that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/2\mathbf{Z}$  (Theorem 2, Proposition 1). In Section 4 we will give some examples concerning other questions in Ross [2].

**Notations:** For a number field  $k$  and a prime number  $p$ , denote by  $w(k)$  ( $w_p(k)$ , resp.) the number of roots ( $p$ th-power roots, resp.) of unity in  $k$ . The Galois

---

Received by the editors December 11, 1996 and, in revised form, September 8, 1997.

1991 *Mathematics Subject Classification.* Primary 11G05.

*Key words and phrases.* Elliptic curve, torsion point, isogeny, complex multiplication.

The author was supported by Grant-Aid for Scientific Research No. 09640003, Ministry of Education, Science and Culture, Japan.

group  $\text{Gal}(\bar{k}/k)$  is simply denoted by  $G_k$  or  $G(\bar{k}/k)$ . If  $A$  is an abelian group, we denote by  $A[n]$  the subgroup of  $A$  annihilated by  $n$ . For an elliptic curve  $E$  over  $k$ , the  $p$ -Sylow subgroup of  $E(k)_{\text{tors}}$  is denoted by  $E(k)_{(p)}$ . We write  $\mathcal{C}(E)$  for the  $k$ -isogeny class of  $E$ .  $\text{End } E$  is the endomorphism ring of  $E$  and  $\text{End}_k$  is the subring of  $\text{End } E$  consisting of endomorphisms defined over  $k$ .

### 1. MINIMAL CYCLIC TORSION

Let  $E$  be an elliptic curve over  $k$ . For a prime number  $p$ , we denote by  $T_p(E)$  the  $p$ -adic Tate module of  $E$  and by  $\rho$  the corresponding representation of  $G_k$  on  $T_p(E)$ .

**Lemma 1.** *There exists an elliptic curve  $E'$  in  $\mathcal{C}(E)$  such that  $E$  has an isogeny over  $k$  onto  $E'$  of  $p$ -power degree such that  $E'(k)_{(p)}$  is cyclic.*

*Proof.* If  $\text{End}_k E = \mathbf{Z}$ , then  $V_p(E) = T_p(E) \otimes \mathbf{Q}_p$  is irreducible as a  $G_k$ -space (see [3, IV § 2]). If  $E$  has complex multiplication by an imaginary quadratic field  $K$  over  $k$ , then  $V_p(E)$  is reducible if and only if  $p$  splits in  $K$ .

(1) The case  $V_p(E)$  is reducible. We may assume that  $\text{End } E$  is isomorphic to the maximal order of  $K$ . Then the decomposition  $K \otimes \mathbf{Q}_p = \mathbf{Q}_p \oplus \mathbf{Q}_p$  gives that of  $T_p(E) = T_1 \oplus T_2$  as a  $G_k$ -module. Therefore we have representations  $\chi_i : G_k \rightarrow \text{Aut } T_i = \mathbf{Z}_p^\times$  ( $i = 1, 2$ ) and  $\rho = \chi_1 \oplus \chi_2$ . The theory of complex multiplication shows that  $\text{Im } \rho$  is open in  $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ . Hence we can choose an integer  $n$  such that for all  $\sigma \in G_k$

$$\chi_1(\sigma) \equiv \chi_2(\sigma) \pmod{p^n},$$

and for some  $\sigma \in G_k$ ,

$$\chi_1(\sigma) \not\equiv \chi_2(\sigma) \pmod{p^{n+1}}.$$

Let  $T' = \mathbf{Z}_p e_1 + \mathbf{Z}_p \frac{e_1 + e_2}{p^n}$ , where  $T_i = \mathbf{Z}_p e_i$ . Then  $T'$  is a  $G_k$ -module and we obtain an elliptic curve  $E'/k$  and an isogeny  $f : E \rightarrow E'$  defined over  $k$  with  $\text{Ker } f = \langle e_1 + e_2 \pmod{p^n} \rangle$ . Let  $\rho'$  be the  $p$ -adic representation associated with  $E'$ . Then we get

$$\rho'(\sigma) \equiv \begin{pmatrix} \chi_1(\sigma) & 0 \\ u & \chi_2(\sigma) \end{pmatrix} \pmod{p^n}, \quad u \not\equiv 0 \pmod{p}.$$

This implies that  $E'(k)_{(p)}$  is cyclic.

(2) The case  $V_p(E)$  is irreducible. In this case it is clear that  $\mathbf{Z}_p x$  is not  $G_k$ -stable for a basis  $\{x, y\}$  of  $T_p(E)$ . Thus there is  $\sigma \in G_k$  such that

$$x^\sigma = ax + p^r uy, \quad u \not\equiv 0 \pmod{p} \quad (a \in \mathbf{Z}_p).$$

We choose  $r$  ( $\geq 0$ ) minimal under this condition. Then since the subgroup  $\langle x \pmod{p^r} \rangle$  of  $E[p^r]$  is  $G_k$ -stable,  $T' = \mathbf{Z}_p p^{-r} x + \mathbf{Z}_p y$  is  $G_k$ -stable. Then as in (1),  $T'$  defines  $E' \in \mathcal{C}(E)$  such that  $E'(k)_{(p)}$  is cyclic. This proves our assertion.  $\square$

**Lemma 2.** *Assume that  $V_p(E)$  is irreducible. If  $E$  contains a  $k$ -rational point of order  $p^{2n+1}$  with  $p^n = w_p(k)$ , then there is  $E' \in \mathcal{C}(E)$  such that  $E'(k)_{(p)} \subset \mathbf{Z}/p^n \mathbf{Z}$ .*

*Proof.* By assumption, we may assume that

$$\rho(G_k) \subset \begin{pmatrix} 1 + p^{2n+1} \mathbf{Z}_p & \mathbf{Z}_p \\ p^{2n+1} \mathbf{Z}_p & \mathbf{Z}_p^\times \end{pmatrix}.$$

Let  $\tau \in G_k$  be such that  $\tau$  induces a generator in  $G(k(\zeta_{p^{n+1}})/k)$ , where  $\zeta_{p^{n+1}}$  is a primitive  $p^{n+1}$ th root of unity. Since  $\det \rho$  is the  $p$ -adic cyclotomic character of  $G_k$ , we can write

$$\rho(\tau) = \begin{pmatrix} 1 + p^{2n+1}a & b \\ p^{2n+1}c & d \end{pmatrix},$$

where  $a, b, c, d \in \mathbf{Z}_p$  and  $d \equiv 1 \pmod{p^n}$  and  $d \not\equiv 1 \pmod{p^{n+1}}$ . The characteristic polynomial  $f(t)$  of  $\rho(\tau)$  satisfies  $f(t) \equiv (t-1)(t-d) \pmod{p^{2n+1}}$ . Putting  $t = 1 + p^n s$ , we have

$$p^{-2n} f(t) \equiv s(s - p^{-n}(d - 1)) \pmod{p}.$$

By Hensel's lemma,  $f(t)$  has solutions  $\lambda_1, \lambda_2 \in \mathbf{Z}_p$  such that  $\lambda_1 \equiv 1, \lambda_2 \equiv d \pmod{p^{n+1}}$ . We can choose  $P = \begin{pmatrix} 1 & b' \\ p^{n+1}c' & p^n \end{pmatrix}$  ( $b', c' \in \mathbf{Z}_p$ ) such that  $P^{-1}\rho(\tau)P = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ . Choose a basis  $\{x_1, x_2\}$  of  $T_p(E)$  such that  $x_1 \pmod{p^{2n+1}}$  is a  $k$ -rational point of order  $p^{2n+1}$ . Put  $y_1 = x_1 + p^{n+1}c'x_2$  and  $y_2 = b'x_1 + p^n x_2$ . Then the lattice  $T' = \mathbf{Z}_p y_1 + \mathbf{Z}_p y_2 = \mathbf{Z}_p x_1 + p^n \mathbf{Z}_p x_2$  is  $G_k$ -stable and  $T'$  determines an elliptic curve  $E' \in \mathcal{C}(E)$  such that  $\rho'(\tau) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$ , where  $\rho'$  is the  $p$ -adic representation associated with  $E'$ . Since  $T'$  is irreducible, there is  $\sigma \in G_k$  such that  $\rho'(\sigma) = \begin{pmatrix} \alpha & * \\ p^r u & \beta \end{pmatrix}$ , with  $u \not\equiv 0 \pmod{p}$  and  $r \geq 1$ . Choose  $r$  minimal under the above condition. Put  $T'' = \mathbf{Z}_p y'_1 + \mathbf{Z}_p y_2$  with  $y'_1 = p^{-r} y_1$ . Then  $T''$  also defines  $E'' \in \mathcal{C}(E)$  and the corresponding representation  $\rho''$  satisfies

$$\rho''(\tau) = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \rho''(\sigma) \equiv \begin{pmatrix} \alpha & * \\ u & \beta \end{pmatrix} \pmod{p}.$$

We see that  $E''(k)_{(p)}$  is cyclic. Let  $P = ay'_1 + by_2 \pmod{p^{n+1}}$ . Then  $P = P^\tau$  and  $P = P^\sigma$  implies  $a \equiv 0, b \equiv 0 \pmod{p}$ . This shows that  $E''(k)$  does not contain any point of order  $p^{n+1}$ . This completes the proof.  $\square$

**Lemma 3.** *Put  $p^n = w_p(k)$  and  $p^m = \text{Min}_{E' \in \mathcal{C}(E)} |E'(k)_{(p)}|$ . If  $V_p(E)$  is irreducible, then  $m \leq 2n$  and there exists  $E' \in \mathcal{C}(E)$  such that  $E'(k)_{(p)}$  is cyclic of order  $p^m$ .*

*Proof.* The first assertion follows from Lemma 2. Hence we may assume that

$$E(k)_{(p)} \cong \mathbf{Z}/p^r \mathbf{Z} \oplus \mathbf{Z}/p^{r'} \mathbf{Z}, \quad 1 \leq r \leq r', \quad r + r' = m \leq 2n.$$

Choose a basis  $\{x, y\}$  of  $T_p(E)$  such that  $x \pmod{p^r}$  and  $y \pmod{p^{r'}}$  are  $k$ -rational points of  $E$ . As in the proof of Lemma 1, there exists an integer  $s (\geq r)$  such that the subgroup  $X = \langle x \pmod{p^s} \rangle$  is  $G_k$ -stable and  $\langle x \pmod{p^{s+1}} \rangle$  is not  $G_k$ -stable; if  $r = r'$ , changing  $x$  and  $y$  if necessary, we may assume that  $\langle y \pmod{p^s} \rangle$  is  $G_k$ -stable. Putting  $E' = E/X$ , we obtain  $E' \in \mathcal{C}(E)$  such that  $E'(k)_{(p)}$  is cyclic. It suffices to show that each point  $P$  in  $E'(k)_{(p)}$  is of order dividing  $p^m$ . We may suppose that  $T_p(E') = \mathbf{Z}_p x' + \mathbf{Z}_p y$  with  $x' = p^{-s} x$ . A point  $P$  of  $E'[p^{m+1}]$  can be written in the form  $\alpha x' + \beta y \pmod{p^{m+1}}$ .

(i) First assume  $s > r$ . Since  $x \bmod p^{r+1}$  is not  $k$ -rational in  $E$ , there is  $\sigma \in G_k$  such that  $x^\sigma \equiv x + p^r vx \bmod p^{r+1}$  with  $v \in \mathbf{Z}_p^\times$ . If  $r \nmid n$ , then  $\det \rho(\sigma) \equiv 1 \bmod p^n$  shows that  $r = r'$ , and with respect to the basis  $\{x', y\}$ ,  $\rho'(\sigma)$  takes the form

$$\begin{pmatrix} 1 + p^r v & p^{r+s} b \\ c & 1 + p^r v' \end{pmatrix} \quad (v' \equiv -v \pmod p).$$

If  $P^\sigma = P$ , then

$$p^r v \alpha \equiv 0, \quad c \alpha + p^r v' \beta \equiv 0 \pmod{p^{m+1}}.$$

Therefore  $\alpha \equiv \beta \equiv 0 \pmod p$ . If  $r = n$ , then  $r = r'$  and there is  $\sigma \in G_k$  such that  $y^{\sigma'} \equiv y + p^r uy \bmod p^{r+1}$  with  $u \in \mathbf{Z}_p^\times$ . Clearly  $P^\sigma = P$  and  $P^{\sigma'} = P$  imply  $\alpha \equiv \beta \equiv 0 \pmod p$ .

(ii) Next assume  $s = r$ . In this case there is  $\sigma \in G_k$  such that  $x^\sigma = x + p^r ax + p^r uy$  with  $u \in \mathbf{Z}_p^\times$ . If  $P^\sigma = P$ , then  $u \alpha + p^r d \beta \equiv 0 \pmod{p^{m+1}}$ , which shows that  $\alpha x' + \beta y = \gamma x + \beta y (= z, \text{ say})$  with  $\gamma \in \mathbf{Z}_p$ . Now  $z^\sigma \equiv z \bmod p^{m+1} T_p(E')$  for  $\sigma \in G_k$  implies  $z^\sigma \equiv z \bmod p^{r'+1} T_p(E)$ , because  $p^{m+1} T_p(E') \subset p^{r'+1} T_p(E)$ . As  $E(k)$  contains no point of order  $p^{r'+1}$ , we have  $\alpha \equiv \beta \equiv 0 \pmod p$ . Therefore every point of  $E'(k)_{(p)}$  is of order dividing  $p^m$ . This proves our assertion.  $\square$

**Theorem 1.** *Put  $D = \text{Min}_{E' \in \mathcal{C}(E)} |E'(k)_{\text{tors}}|$ . If  $\text{End}_k E = \mathbf{Z}$ , then  $D$  is a divisor of  $w(k)^2$  and there exists an elliptic curve  $E'$  in  $\mathcal{C}(E)$  such that  $E'(k)_{\text{tors}}$  is cyclic of order  $D$ .*

*Proof.* Let  $p$  be a prime divisor of  $|E(k)_{\text{tors}}|$ . By the above three lemmata,  $E$  is  $k$ -isogenous to  $E'$  of  $p$ -power degree such that  $E'(k)_{(p)}$  is cyclic of the minimal  $p$ -power order. Repeating this process we obtain Theorem 1.  $\square$

## 2. ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

Let  $E$  be an elliptic curve over  $k$  with complex multiplication by an imaginary quadratic field  $K$  and suppose that  $k \not\supset K$ .

**Lemma 4** (Aoki [1, Theorem 9.1]). *If  $w_p(k) = w_p(Kk)$ , then  $E(k)_{(p)} = 0$  for  $p > 2$  and  $E(k)_{(2)} \subset \mathbf{Z}/2\mathbf{Z}$  for  $p = 2$ .*

*Proof.* For the sake of completeness we sketch the proof in [1]. By Tchebotarev's density theorem, there is a prime ideal  $\mathfrak{l}$  of  $k$  satisfying the following conditions:

- $(\mathfrak{l}, p) = 1$  and  $E$  has good reduction modulo  $\mathfrak{l}$ .
- The Frobenius automorphism associated with  $\mathfrak{l}$  in  $G(Kk(\zeta_{p^{n+1}})/k)$  acts trivially on  $\zeta_{p^{n+1}}$  and non-trivially on  $K$ .

Then we have  $|\tilde{E}(F)| = 1 + N\mathfrak{l}$  and  $N\mathfrak{l} \equiv 1 \pmod{p^{n+1}}$ , where  $\tilde{E}$  is the reduction of  $E$  modulo  $\mathfrak{l}$  over the residue field  $F$  and  $N\mathfrak{l}$  is the norm of  $\mathfrak{l}$ . Since  $N\mathfrak{l} + 1 \equiv 2 \pmod{p^{n+1}}$ , we see that  $|\tilde{E}(F)|$  is prime to  $p$  for  $p > 2$  and  $4 \nmid |\tilde{E}(F)|$  for  $p = 2$ . As the reduction map  $E(k) \rightarrow \tilde{E}(F)$  is injective, we get our assertion.  $\square$

**Theorem 2.** *Let  $E$  be an elliptic curve over  $k$  with complex multiplication by an imaginary quadratic field  $K$  and suppose that  $k \not\supset K$ , i.e.  $\text{End}_k E = \mathbf{Z}$ . Then  $E$  is  $k$ -isogenous to an elliptic curve  $E'/k$  such that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/4\mathbf{Z}$ . If  $Kk \neq k(\sqrt{-1})$ , then  $E'$  can be chosen such that  $E'(k)_{\text{tors}} \subset \mathbf{Z}/2\mathbf{Z}$ .*

*Proof.* Since  $[Kk : k] = 2$ ,  $p \leq w_p(k) \langle w_p(Kk) \rangle$  never happens for  $p > 2$ . Hence by Theorem 1 and Lemma 4,  $E$  is isogenous to an elliptic curve  $E'$  over  $k$  such that  $E'(k)_{tors}$  is cyclic of 2-power order. If  $Kk = k(\sqrt{-1})$ , then  $w_2(k) < w_2(Kk)$ , which implies  $w_2(k) = 2$ . Therefore we get the first assertion by Lemma 3. Now assume that  $Kk \neq k(\sqrt{-1})$ . If  $w_2(k) = w_2(Kk)$ , our assertion follows from Lemma 4. Hence we may further assume that  $w_2(k) < w_2(Kk)$ . This implies that  $\sqrt{-1} \in k$ . Let  $\tau$  be an element of  $G_k$  which acts non-trivially on  $K$ . Then  $\alpha \rightarrow \alpha^\tau$  ( $\alpha \in \text{End } E$ ) induces a non-trivial automorphism of  $\text{End } E$ . Let  $\rho : G_k \rightarrow \text{Aut}(T_2(E))$  be the 2-adic representation associated with  $E$ . As  $\alpha^\tau = \rho(\tau)\alpha\rho(\tau)^{-1}$ ,  $\rho(\tau)$  induces the non-trivial automorphism of  $K \otimes \mathbf{Q}_2 = \text{End } E \otimes \mathbf{Q}_2$ . Then  $\rho(\tau)$  is conjugate to a matrix of the form  $\begin{pmatrix} a & b \\ mb & -a \end{pmatrix}$  where  $K = \mathbf{Q}(\sqrt{-m})$  and  $a, b \in \mathbf{Z}_2$ . By Lemma 1, we may assume that  $E(k)_{(2)}$  is cyclic. Now  $\sqrt{-1} \in k$  implies  $\det \rho(\tau) \equiv 1 \pmod{4}$ . If  $E(k)$  contains a point of order 4, then  $\rho(\tau)$  is conjugate to a matrix of the form  $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{4}$ . Since  $\text{tr} \rho(\tau) = 0$ , this is a contradiction. Therefore  $E(k)_{(2)} \subset \mathbf{Z}/2\mathbf{Z}$ . □

**Proposition 1.** *Let  $E/k, K$  be as in Theorem 2. Assume  $Kk = k(\sqrt{-1})$ . Let  $H(f)$  denote the ring class field of  $K$  of conductor  $f$  and choose  $n$  maximal such that  $H(2^n) \subset Kk$ . Assume further that  $4 \mid |E(k)_{tors}|$ ,  $E(Kk) \supset \mathbf{Z}/4\mathbf{Z}$ , and for any  $E' \in \mathcal{C}(E)$ ,  $\text{End } E'$  has conductor not divisible by  $2^n$ . Then for any  $E' \in \mathcal{C}(E)$ , we have  $E'(k) \supset \mathbf{Z}/4\mathbf{Z}$  or  $E'(k) \supset E'[2]$ .*

*Proof.* We divide the proof into three steps. □

*Step 1.*  $E'(Kk) \supset \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$  for any  $E' \in \mathcal{C}(E)$ .

*Proof of Step 1.* Let  $j'$  be the  $j$ -invariant of  $E'$ . If  $j' = 0$ , then  $K = \mathbf{Q}(\sqrt{-3})$  and  $E'$  is isomorphic to the curve  $y^2 = x^3 + a$ ,  $a \neq 0$ . As  $E'(k)_{(2)} \neq 0$ , our assertion is clear. If  $j' = 1728$ , then  $K = \mathbf{Q}(\sqrt{-1})$  and  $E'$  is isomorphic to the curve  $y^2 = x^3 + ax$ . If  $E'(Kk) \not\supset \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$ , then  $x^2 \pm a = 0$  has no solutions in  $Kk$ , hence  $E'(Kk) \cong \mathbf{Z}/2\mathbf{Z}$ . Let  $f : E' \rightarrow E''$  be a  $k$ -isogeny of degree 2. Since  $\text{Ker } f = \langle (0, 0) \rangle$ ,  $E''$  is  $Kk$ -isomorphic to the curve  $y^2 = x(x^2 - 4a)$ . Then we also have  $E''(Kk)_{(2)} = \mathbf{Z}/2\mathbf{Z}$ . This shows that  $E'(Kk)_{(2)} = \mathbf{Z}/2\mathbf{Z}$  for all  $E' \in \mathcal{C}(E)$ . This contradicts the condition  $4 \mid |E(k)_{tors}|$ . Now assume that  $j' \neq 0, 1728$ . Let the conductor of  $\text{End } E'$  be  $2^r d$ ,  $(2, d) = 1$ . Then we have

$$H(2^r d) = K(j'), \quad Kk \supset H(2^r d)H(2^n) \supset H(2^{r+1}d).$$

Since we have  $H(2^{r+1}d) = K(j', E'[2])$  by [4, Theorem 5.5], we get that  $E'(Kk) \supset \mathbf{Z}/2\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$ .

*Step 2.*  $E'(Kk) \supset \mathbf{Z}/4\mathbf{Z}$  for any  $E' \in \mathcal{C}(E)$ .

*Proof of Step 2.* It suffices to show that for an isogeny  $f : E \rightarrow E'$  defined over  $k$  of degree 2,  $E(Kk) \supset \mathbf{Z}/4\mathbf{Z}$  implies  $E'(Kk) \supset \mathbf{Z}/4\mathbf{Z}$ . Let  $P$  be a  $Kk$ -rational point of  $E$  of order 4. If  $\text{Ker } f \neq \langle 2P \rangle$ , then  $f(P)$  is a  $Kk$ -rational point of  $E'$  of order 4. If  $\text{Ker } f = \langle 2P \rangle$ , then  $f(P')$  is a  $Kk$ -rational point of  $E'$  of order 4, where  $P' \in E[4]$  is such that  $2P' \neq 2P$ .

*Step 3.* For  $E_1, E_2 \in \mathcal{C}(E)$ , let  $f : E_1 \rightarrow E_2$  be an isogeny over  $k$  of degree 2. If  $|E_1(k)_{(2)}| \geq 4$ , then  $|E_2(k)_{(2)}| \geq 4$ .

*Proof of Step 3.* Let  $\text{Ker} f = \langle e \rangle$ , where  $\{e, e'\}$  is a basis of  $E_1[2]$ . Assume that  $E_1(k)_{(2)}$  is cyclic. Then  $E_1(k)$  contains a point  $P$  of order 4. If  $2P \neq e$ , our assertion is clear. If  $2P = e$ , then  $E_2(k) \supset \langle f(P), f(e') \rangle = E_2[2]$ . Next assume that  $E_1(k) \supset E_1[2]$ . Let  $P, P'$  be such that  $2P = e, 2P' = e'$ . Since  $E(Kk) \supset \mathbf{Z}/4\mathbf{Z} \otimes \mathbf{Z}/2\mathbf{Z}$ , we may assume that  $P$  or  $P' \in E_1(Kk)$ . If  $P^\sigma \neq P$  for some  $\sigma \in G_{Kk}$ , then  $\det \rho(\sigma) \equiv 1 \pmod{4}$  shows that  $P^\sigma = P + e'$ . Hence  $f(P)$  is not  $Kk$ -rational, which contradicts Step 1. Thus we get  $P \in E_1(Kk)$ . Similarly if  $P'^\sigma \neq P'$  for some  $\sigma \in G_{Kk}$ , we have  $P'^\sigma = P' + e$  and this implies that  $E'_1(Kk) \not\supset E'_1[2]$  with  $E'_1 = E_1/\langle e' \rangle$ . Consequently we have  $E_1(Kk) \supset E_1[4]$ . Let  $\langle \tau \rangle = G(Kk/k)$ . Since  $\det \rho(\tau) \equiv -1 \pmod{4}$ , we obtain

$$P^\tau = aP + me', \quad P'^\tau = bP' + ne$$

with  $ab \equiv -1 \pmod{4}$ . If  $b = 1$ , then  $f(P')$  is a  $k$ -rational point of order 4. If  $b = -1$  and  $m = 0$ , then  $\langle f(P), f(e') \rangle = E_2[2] \subset E_2(k)$ . If  $b = -1$  and  $m = 1$ , then we have  $(P + P')^\tau = P + P' + ne$ , which shows that  $f(P + P')$  is a  $k$ -rational point of order 4. This completes the proof.

### 3. EXAMPLES

The following is a counter-example of Question 1 in the Introduction.

**Example 1.** Let  $k = \mathbf{Q}(\sqrt{-2})$  and  $E : y^2 = x(x^2 - 16)$ . Notations being as in Proposition 1, we see that  $w(k) = 2$ ,  $K = \mathbf{Q}(\sqrt{-1})$  and  $Kk = H(2^2)$ . If  $E' \in \mathcal{C}(E)$ , then  $j(E') \in k$  has a real conjugate, hence  $j(E') \in \mathbf{Q}$  (cf. [4, p.124]). Therefore  $\text{End } E'$  has conductor 1 or 2. This shows that  $4 \mid |E(k)_{\text{tors}}|$  for all  $E' \in \mathcal{C}(E)$  by Proposition 1.

**Question 2** ([2]). Let  $w_p(k) = p^n$  ( $n \geq 1$ ). If  $E/k$  contains a  $k$ -rational point of order  $p^d$  with  $d \leq n$ , then does every elliptic curve  $E' \in \mathcal{C}(E)$  contain a  $k$ -rational point of order  $p^d$ ?

If  $n \geq 1$  and  $d = 1$ , Question 2 is valid ([2, Proposition 2]). The following example shows that when  $p = 2, n = d = 2$ , Question 2 no longer holds.

**Example 2.** Let  $k = \mathbf{Q}(\sqrt{2 - 2i})$  ( $\ni i = \sqrt{-1}$ ) and

$$E : y^2 = x^3 - 2x^2 - x, \quad E' : y^2 = x^3 + 4x^2 + 8x.$$

There is an isogeny  $E \rightarrow E'$  of degree 2 defined over  $\mathbf{Q}$  and  $E$  has a  $k$ -rational point  $P = (i, \sqrt{2 - 2i})$  of order 4. Put  $c = 2 - 2i$  and  $c' = 2 + 2i$ . The points of  $E'$  of order 2 are

$$e = (0, 0), \quad e_1 = (-c, 0), \quad e_2 = (-c', 0).$$

Let  $P = (X, Y) \in E'$ . If  $2P = e$ , then  $X = \pm 2\sqrt{2} \notin k$ . If  $2P = e_1$ , then  $X = c \pm 2\sqrt{c'} \notin k$ . If  $2P = e_2$ , then  $X = c' \pm 2\sqrt{c}$  and  $Y = \pm 2\sqrt{-\sqrt{-1}X} \notin k$ . Therefore  $E'$  has no  $k$ -rational point of order 4.

The following example shows that Proposition 5 (hence Question 4) in [2, Section 4] is not valid in general.

**Example 3.** Let  $k = \mathbf{Q}(\sqrt[4]{-3}) \supset K = \mathbf{Q}(\sqrt{-3})$  and

$$E : y^2 = x^3 - 1, \quad E' : y^2 = x^3 - 6x^2 - 3x.$$

Then  $p = 2$  is inert in  $K$  and  $w_2(k) = 2$ . There is an isogeny  $E \rightarrow E'$  of degree 2 defined over  $\mathbf{Q}$  and  $E'$  has a  $k$ -rational point  $P = (-\sqrt{-3}, \sqrt[4]{-3}(3 - \sqrt{-3}))$  of order

4. We see that  $2\omega P = 0$  with  $\omega^2 + \omega + 1 = 0$ . But we have  $E(k)_{(2)} = E[2]$ . Let  $E_1 \in \mathcal{C}(E)$  and put  $j_1 = j(E_1)$ . Since  $K(j_1)/\mathbf{Q}$  is Galois, we have  $K = K(j_1)$  and this implies  $j_1 \in \mathbf{Q}$ , hence  $j_1 = j(E)$  or  $j(E')$ . It follows that  $E_1$  is  $k$ -isomorphic to  $E$  or to  $E'$ . Therefore if  $E_1(k)_{tors}$  is cyclic for  $E_1 \in \mathcal{C}(E)$ , then  $E_1(k)_{tors} \supset \mathbf{Z}/4\mathbf{Z}$ .

## REFERENCES

1. N. Aoki, *Torsion points on abelian varieties with complex multiplication*, In *Algebraic Cycles and Related Topics*, KITASAKADO 1994, F. Hazama, ed., World Scientific, Singapore, New Jersey, London, HongKong, 1995, 1-22. CMP 97:02
2. R. Ross, *Minimal torsion in isogeny classes of elliptic curves*, Trans. AMS **344**(1994), 203-215. MR **95b**:11058
3. J.-P. Serre, *Abelian  $l$ -adic representations and elliptic curves*, Benjamin, New York, 1968.
4. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton Univ. Press, 1971. MR **95e**:11048

MATHEMATICAL INSTITUTE, TOHOKU UNIVERSITY, SENDAI 980-8578, JAPAN  
*E-mail address*: nakamura@math.tohoku.ac.jp