Functiones et Approximatio
47.1 (2012), 89–93
doi: 10.7169/facm/2012.47.1.7

ON TORSION POINTS OF CERTAIN CM ELLIPTIC CURVES

Naoki Murabayashi

Abstract: Let E be a CM elliptic curve defined over an algebraic number field F with CM by an imaginary quadratic field K. We determine the group of $K_{ab}F$-rational torsion points of E. In some cases we also determine the group of F or KF-rational torsion points of E.

Keywords: modularity, CM elliptic curves, torsion points.

1. Introduction

Let E be a CM elliptic curve defined over an algebraic number field $F \subseteq \mathbb{C}$ such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$, the ring of endomorphisms of E defined over $\overline{\mathbb{Q}}$, is isomorphic to an order R of an imaginary quadratic field $K \subseteq \mathbb{C}$. It is known by work of Shimura [6] that there exists a normalized newform f of weight two on $\Gamma_1(N)$ for some N, such that E admits a non-zero homomorphism $\varphi : E \to J_f$ defined over $\overline{\mathbb{Q}}$, where J_f is the $\mathbb{Q}$-simple factor of the Jacobian variety $J_1(N)$ corresponding to f.

In the previous paper [1], we gave necessary and sufficient conditions for E to be modular over F, i.e., such a non-zero homomorphism φ can be defined over F. It holds that E is modular over F if and only if the group $E_{\mathrm{tors}}(\mathbb{C})$ of torsion points of E rational over $\mathbb{C}$, i.e. the group of all torsion points of E, is contained in $E(K_{ab}F)$, where the subscript ab denotes the maximal abelian extension. Therefore, if E is modular over F, it holds that $E_{\mathrm{tors}}(K_{ab}F) = E_{\mathrm{tors}}(\mathbb{C})$.

In this paper we determine $E_{\mathrm{tors}}(K_{ab}F)$ in the case where E is not modular over F. We also determine $E_{\mathrm{tors}}(F)$ and $E_{\mathrm{tors}}(KF)$ in some cases.

2. Main results

We put $K' := K_{ab}F$. Let

$$\Phi : \mathrm{Gal}(\overline{K}/K') \longrightarrow \mathrm{Aut}(E_{\mathrm{tors}}(\mathbb{C})) \qquad (\text{resp. } \Psi : R^{\times} \longrightarrow \mathrm{Aut}(E_{\mathrm{tors}}(\mathbb{C})))$$

This research was financially supported by the Kansai University Grant-in-Aid for progress of research in graduate course, 2010.

2010 Mathematics Subject Classification: primary: 11G15; secondary: 11G18 be the homomorphism corresponding to the canonical action of $\mathrm{Gal}(\overline{K}/K')$ (resp. $R^\times$) on $E_{\mathrm{tors}}(\mathbb{C})$. Then there exists a homomorphism $\chi : \mathrm{Gal}(\overline{K}/K') \longrightarrow R^\times$ such that $\Phi = \Psi \circ \chi$. We explain the definition of χ. Fix a complex uniformization $\xi : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$, where $\mathfrak{a}$ is a proper R ideal in K. Applying Theorem 5.4 in [5] (p. 117) with $\sigma \in \mathrm{Gal}(\overline{K}/K')$ and $s = 1$, we obtain the unique isomorphism $\xi' : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathbb{C})$ such that $\xi(u)^\sigma = \xi'(u)$ for every $u \in K/\mathfrak{a}$. Putting $\chi(\sigma) := \xi' \circ \xi^{-1} \in \mathrm{Aut}(E) = R^\times$, we have $\xi(u)^\sigma = \xi'\xi^{-1}(\xi(u))$, i.e., $P^\sigma = \chi(\sigma)(P)$ for every $P = \xi(u) \in E_{\mathrm{tors}}(\mathbb{C})$. Let N be the size of the image of χ. By Theorem 5.1 in [1], E is modular over F if and only if $N = 1$. In particular, the condition that E is not modular over F implies $N \geqslant 2$, especially $N = 2$ in the case of $R^\times = \{\pm 1\}$.

Theorem 1. *Assume that E is not modular over F. Then we have*

$$E_{\mathrm{tors}}(K_{ab}F) = \begin{cases} E[2] & \text{if } N = 2, \\ E[\sqrt{-3}] \ (\subseteq E[3]) & \text{if } N = 3, \\ E[1+\sqrt{-1}] \ (\subseteq E[2]) & \text{if } N = 4, \\ \{O\} & \text{if } N = 6, \end{cases}$$

where $E[a]$ ($a \in R$) denotes the kernel of the endomorphism corresponding to a and O denotes the identity element of E.

Proof. If $N = 2$, then we have $\mathrm{Im}\chi = \{\pm 1\} = \langle -1 \rangle$. We have

$$\begin{aligned} E_{\mathrm{tors}}(K_{ab}F) &= (E_{\mathrm{tors}}(\mathbb{C}))^{\Psi(-1)} \ (:= \{P \in E_{\mathrm{tors}}(\mathbb{C}) | \Psi(-1)(P) = P\}) \\ &= E[2]. \end{aligned}$$

If $N = 3$, then we have $\mathrm{Im}\chi = \{1, \omega, \omega^2\} = \langle \omega \rangle$, where $\omega = \dfrac{-1+\sqrt{-3}}{2}$. So $E_{\mathrm{tors}}(K_{ab}F) = (E_{\mathrm{tors}}(\mathbb{C}))^{\Psi(\omega)} = E[1-\omega] = E[\sqrt{-3}]$. This is applied to the other cases. ■

By contraposition of Theorem 1, we have the following:

Theorem 2. *If there exists a point of $E_{\mathrm{tors}}(F)$ whose order is greater than or equal to* 4*, E is modular over F. In the case of $R^\times = \{\pm 1\}$, we can replace* 4 *with* 3.

3. Further results

In this section we determine $E_{\mathrm{tors}}(F)$ and $E_{\mathrm{tors}}(KF)$ in some cases. We put $F' := KF$.

Proposition 3. *Assume that if the conductor of R is odd, 2 does not remain prime in K. Then $E_{\mathrm{tors}}(F')$ contains a subgroup of order 2.*

Proof. Except the case where the conductor of R is odd and 2 remains prime in K, we can take a prime ideal $\mathfrak{q}$ of R (not necessarily proper) lying above 2 such that $R/\mathfrak{q} \cong \mathbb{Z}/2\mathbb{Z}$. Lemma 1 in [4] implies that $E[2] \cong R/2R$ as R-module. Let M be the subgroup of $E[2]$ corresponding to $\mathfrak{q}/2R$ by this identification. The action of $\mathrm{Gal}(\overline{F'}/F')$ on $E[2]$ is R-linear, so M is stable under this. Since $E[2]/M \cong R/\mathfrak{q} \cong \mathbb{Z}/2\mathbb{Z}$, $M \cong \mathbb{Z}/2\mathbb{Z}$. Therefore the unique generator of M is fixed by the action of $\mathrm{Gal}(\overline{F'}/F')$, so F'-rational, hence $E_{\mathrm{tors}}(F') \supseteq M \cong \mathbb{Z}/2\mathbb{Z}$. ■

Proposition 4. *Assume that*

(i) *E is not modular over F;*
(ii) *$K \neq \mathbb{Q}(\sqrt{-1})$;*
(iii) *2 is ramified in K, i.e. $(2) = \mathfrak{q}^2$ ($\mathfrak{q}$ is a prime ideal of K);*
(iv) *there exists a prime ideal $\mathfrak{Q}$ of F' lying above $\mathfrak{q}$ such that $\mathfrak{Q}$ is unramified over $\mathfrak{q}$.*

Then $E_{\mathrm{tors}}(F') \subsetneqq E[2]$.

Proof. By assumption (ii) and (iii), $R^\times = \{\pm 1\}$. Hence, Theorem 1 implies that $E_{\mathrm{tors}}(F') \subseteq E[2]$. By the theory of complex multiplication there exists a unique homomorphism

$$\alpha_{E/F'} : F'^{\times}_{\mathbb{A}} \longrightarrow K^\times$$

(where $F'^{\times}_{\mathbb{A}}$ denotes the idele group of F') such that

- $\mathrm{Ker}(\alpha_{E/F'})$ is open in $F'^{\times}_{\mathbb{A}}$;
- For any $x \in F'^{\times}_{\mathbb{A}}$, $\alpha_{E/F'}(x)N_{F'/K}(x)^{-1}\mathfrak{a} = \mathfrak{a}$, where $N_{F'/K}$ is the norm map from $F'^{\times}_{\mathbb{A}}$ to $K^{\times}_{\mathbb{A}}$;
- For any $x \in F'^{\times}_{\mathbb{A}}$, $\alpha_{E/F'}(x)\alpha_{E/F'}(x)^\rho = N(il(x))$, where z^ρ is the complex conjugate of a complex number z and $il(x)$ is the fractional ideal of F' associated to an idele element x;
- For any $x \in F'^{\times}_{\mathbb{A}}$ and $w \in K/\mathfrak{a}$ ($\subseteq \mathbb{C}/\mathfrak{a}$),

  $$\xi(w)^{[x,\, F']} = \xi(\alpha_{E/F'}(x)N_{F'/K}(x)^{-1}w),$$

  where $[x,\, F']$ is the element of $\mathrm{Gal}(F'_{ab}/F')$ corresponding to x by the reciprocity law of class field theory (see Theorem 19.8, p. 134 in [7]).

Claim 1. *The condition that $E_{\mathrm{tors}}(F') = E[2]$ is equivalent to the condition $(*)$:*

$$\alpha_{E/F'}(x)N_{F'/K}(x)_{\mathfrak{q}}^{-1} \in 1 + \mathfrak{q}^2 \qquad \textit{for any} \;\; x \in F'^{\times}_{\mathbb{A}}$$

(where $N_{F'/K}(x)_{\mathfrak{q}}$ denotes the $\mathfrak{q}$-component of $N_{F'/K}(x)$).

Proof of Claim 1. It is clear that $E_{\mathrm{tors}}(F') = E[2]$ is equivalent to the condition:

$$\xi(\alpha_{E/F'}(x)N_{F'/K}(x)^{-1}w) = \xi(w) \qquad \text{for any } \ x \in F_{\mathbb{A}}'^{\times} \ \text{ and } \ w \in \frac{1}{2}\mathfrak{a}/\mathfrak{a}.$$

Putting $w = \dfrac{1}{2}a$ $(a \in \mathfrak{a})$, $\xi(\alpha_{E/F'}(x)N_{F'/K}(x)^{-1}w) = \xi(w)$ is equivalent to the condition (∗∗):

$$\frac{\alpha_{E/F'}(x)N_{F'/K}(x)_{\mathfrak{r}}^{-1}}{2}a \equiv \frac{1}{2}\,a \mod \mathfrak{a} \otimes_R \mathcal{O}_{\mathfrak{r}} \qquad \text{for any prime ideal } \ \mathfrak{r} \text{ of } K$$

(where $\mathcal{O}_{\mathfrak{r}}$ denotes the ring of integers in $K_{\mathfrak{r}}$, the completion of K with respect to the valuation associated to $\mathfrak{r}$). If $\mathfrak{r} \neq \mathfrak{q}$, $2 \in \mathcal{O}_{\mathfrak{r}}^{\times}$. We also have that $\alpha_{E/F'}(x)N_{F'/K}(x)_{\mathfrak{r}}^{-1} \in \mathcal{O}_{\mathfrak{r}}^{\times}$ because of $\alpha_{E/F'}(x)N_{F'/K}(x)^{-1}\mathfrak{a} = \mathfrak{a}$. So if $\mathfrak{r} \neq \mathfrak{q}$, the congruence relations in the condition (∗∗) hold. Therefore we have

$$\begin{aligned} E_{\mathrm{tors}}(F') = E[2] &\Longleftrightarrow \frac{\alpha_{E/F'}(x)N_{F'/K}(x)_{\mathfrak{q}}^{-1} - 1}{2}a \equiv 0 \mod \mathfrak{a} \otimes_R \mathcal{O}_{\mathfrak{q}} \\ &\qquad\qquad \text{for any } x \in F_{\mathbb{A}}'^{\times} \text{ and } a \in \mathfrak{a} \\ &\Longleftrightarrow \frac{\alpha_{E/F'}(x)N_{F'/K}(x)_{\mathfrak{q}}^{-1} - 1}{2} \in \mathcal{O}_{\mathfrak{q}} \qquad \text{for any } x \in F_{\mathbb{A}}'^{\times}. \end{aligned}$$

Since $(2) = \mathfrak{q}^2$, the last condition is equivalent to the condition (∗). This completes the proof. ■

Claim 2. *The condition* (∗) *does not hold.*

Proof of Claim 2. Let π be a prime element of $\mathcal{O}_{\mathfrak{q}}$, i.e. $(\pi) = \mathfrak{q}$ in $\mathcal{O}_{\mathfrak{q}}$. By assumption, $F'_{\mathfrak{Q}}/K_{\mathfrak{q}}$ is an unramified extension, so $N_{F'_{\mathfrak{Q}}/K_{\mathfrak{q}}}(\mathcal{O}_{\mathfrak{Q}}^{\times}) = \mathcal{O}_{\mathfrak{q}}^{\times}$, where $\mathcal{O}_{\mathfrak{Q}}$ denotes the ring of integers in $F'_{\mathfrak{Q}}$. Therefore there exists $x_0 \in \mathcal{O}_{\mathfrak{Q}}^{\times}$ such that $N_{F'_{\mathfrak{Q}}/K_{\mathfrak{q}}}(x_0) = (1+\pi)^{-1}$. We consider the restriction of $\alpha_{E/F'}$ to $\mathcal{O}_{\mathfrak{Q}}^{\times}$ and let $\mathfrak{Q}^f$ $(f \geqslant 0)$ be the conductor of it. Putting $m := \sharp(\mathcal{O}_{\mathfrak{Q}}/\mathfrak{Q}^f)^{\times}$ if $f \geqslant 1$ and $m := 1$ if $f = 0$, $x_0^m \equiv 1 \mod \mathfrak{Q}^f$, hence $\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0)^m = 1$, where $\iota_{\mathfrak{Q}}x_0$ denotes the element of $F_{\mathbb{A}}'^{\times}$ whose $\mathfrak{Q}$-component is x_0 and all the other components are one. Therefore we have

$$\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0) \in K^{\times} \cap \{\text{roots of unity}\} = \{\pm 1\}.$$

If $\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0) = 1$,

$$\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0)N_{F'/K}(\iota_{\mathfrak{Q}}x_0)_{\mathfrak{q}}^{-1} = 1 + \pi \notin 1 + \mathfrak{q}^2$$

and if $\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0) = -1$,

$$\alpha_{E/F'}(\iota_{\mathfrak{Q}}x_0)N_{F'/K}(\iota_{\mathfrak{Q}}x_0)_{\mathfrak{q}}^{-1} = -1 - \pi = 1 + \pi - 2(1+\pi) \notin 1 + \mathfrak{q}^2$$

because of $2(1+\pi) \in \mathfrak{q}^2$. Hence the condition (∗) does not hold. ■

By Claim 1 and 2, $E_{\mathrm{tors}}(F') \subsetneqq E[2]$. This completes the proof of Proposition 4. ■

Theorem 5. *Let K be an imaginary quadratic field with expression $\mathbb{Q}(\sqrt{-p_1 \cdots p_r})$, where $p_1, \dots, p_r$ $(r \geqslant 1)$ are distinct prime numbers such that $p_i \equiv 1 \bmod 4$ $(1 \leqslant i \leqslant r)$. Let $\mathfrak{q}$ be the prime ideal of K lying above 2 (then $(2) = \mathfrak{q}^2$ in K). Let E be an elliptic curve defined over $\mathbb{Q}(j_E)$ such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E)$ is isomorphic to the maximal order of K. Let H be the Hilbert class field of K (hence $H = K(j_E)$). Then we have*

$$E_{\mathrm{tors}}(\mathbb{Q}(j_E)) = E_{\mathrm{tors}}(H) = E[\mathfrak{q}] \cong \mathbb{Z}/2\mathbb{Z}.$$

Proof. By Theorem 7.1 in [2], E is not modular over $\mathbb{Q}(j_E)$. So Theorem 1 implies that $E_{\mathrm{tors}}(H) \subseteq E[2]$. Since $(2) = \mathfrak{q}^2$, M in the proof of Proposition 3 coincides with $E[\mathfrak{q}]$. Combining with Proposition 4, $E_{\mathrm{tors}}(H) = E[\mathfrak{q}] \cong \mathbb{Z}/2\mathbb{Z}$. Since E is defined over $\mathbb{Q}(j_E)$, $\mathrm{Gal}(H/\mathbb{Q}(j_E))$ acts on $E_{\mathrm{tors}}(H) \cong \mathbb{Z}/2\mathbb{Z}$. Therefore the unique generator of $E_{\mathrm{tors}}(H)$ is $\mathbb{Q}(j_E)$-rational. Hence we get the assertion. ■

Acknowledgements. The presentation of Theorem 1 owes to the referee's comments. I wish to express my sincere thanks to the referee.

References

[1] N. Murabayashi, *On the field of definition for modularity of CM elliptic curves*, J. Number Theory **108** (2004), 268–286.

[2] N. Murabayashi, *On construction of certain CM elliptic curves*, J. Number Theory **128** (2008), 576–588.

[3] N. Murabayashi, *Modularity of CM elliptic curves over division fields*, J. Number Theory **128** (2008), 895–897.

[4] J.L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. Number Theory **33** (1989), 257–265.

[5] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton University Press, 1971.

[6] G. Shimura, *On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields*, Nagoya Math. J. **43** (1971), 199–208.

[7] G. Shimura, *Abelian varieties with complex multiplication and modular functions*, Princeton University Press, Princeton, NJ, 1998.

Address: Naoki Murabayashi: Department of Mathematics, Faculty of Engineering Science, Kansai University, 3-3-35, Yamate-cho, Suita-shi, Osaka, 564-8680, Japan.

E-mail: murabaya@kansai-u.ac.jp

Received: 31 May 2011; **revised:** 22 July 2011