On rational torsion points of central $\mathbb{Q}$-curves

Fumio Sairaiji (Hiroshima International University)
Takuya Yamauchi $^1$ (Hiroshima University)

Abstract

Let $E$ be a central $\mathbb{Q}$-curve over a polyquadratic field $k$. In this paper we give an upper bound for prime divisors of the order of the $k$-rational torsion subgroup $E_{\text{tors}}(k)$. (See Theorems 1.7 and 1.8.) The notion of central $\mathbb{Q}$-curves is a generalization to that of elliptic curves over $\mathbb{Q}$. Our result is a generalization of Theorem 2 of Mazur [12], and it is a precision of the upper bound of Merel [15].

1 Introduction

We review some known results. Let $E$ be an elliptic curve over a number field $k$ of degree $d$. Let $E(k)$ be the group of $k$-rational points on $E$ and let $E_{\text{tors}}(k)$ be its torsion subgroup. The Mordell-Weil Theorem asserts that $E(k)$ is a finitely generated abelian group, and thus $\#E_{\text{tors}}(k)$ is finite.

When $k$ is equal to either $\mathbb{Q}$ or a quadratic field, the group structure of $E_{\text{tors}}(k)$ is completely determined.

**Theorem 1.1 (Mazur [12]).** Assume that $k$ is equal to $\mathbb{Q}$. Then the group $E_{\text{tors}}(\mathbb{Q})$ is isomorphic to one of the following 15 abelian groups.

$$
\begin{align*}
\mathbb{Z}/N\mathbb{Z} & \quad (1 \leq N \leq 10, \ N = 12) \\
\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \quad (1 \leq N \leq 4)
\end{align*}
$$

Specially, each prime divisor of $\#E_{\text{tors}}(\mathbb{Q})$ is less than or equal to 7. For each finite abelian group $G$ in Theorem 1.1, Kubert [11] gives a defining equation parameterizing elliptic curves $E$ such that $E_{\text{tors}}(\mathbb{Q})$ contains $G$. For example, if $E_{\text{tors}}(\mathbb{Q})$ contains $\mathbb{Z}/6\mathbb{Z}$, $E$ is isomorphic to

$$y^2 + (1 - s)xy - (s^2 + s)y = x^3 - (s^2 + s)x^2$$

for some $s$ in $\mathbb{Q}$ such that $\Delta = s^6(s + 1)^3(9s + 1) \neq 0$. Then the point $(0,0)$ is of order 6.

$^1$The author is supported by the Japan Society for the Promotion of Science Research Fellowships for Young Scientists.
Theorem 1.2 (Kenku-Momose [10], Kamienny [9]). Let $k$ be a quadratic field. Then the group $E_{\text{tors}}(k)$ is isomorphic to one of the following 25 abelian groups.

- $\mathbb{Z}/N\mathbb{Z}$ \((1 \leq N \leq 14, \ N = 16, 18)\)
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ \((1 \leq N \leq 6)\)
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N\mathbb{Z}$ \((N = 1, 2) \ (k = \mathbb{Q}(\sqrt{-3}))\)
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ \((k = \mathbb{Q}(\sqrt{-1}))\)

Specially, each prime divisor of $\mathbb{Z}E_{\text{tors}}(k)$ is less than or equal to 13.

For elliptic curves over number fields of degree greater than two, there exist some results on the group structure of $E(k)_{\text{tors}}$ under some conditions (cf. e.g. [6], [21]).

Merel [15] obtains an effective upper bound for prime divisors of $\mathbb{Z}E_{\text{tors}}(k)$ depending only the degree $d$ of $k$ over $\mathbb{Q}$.

Theorem 1.3 (Merel [15]). Let $k$ be a number field of degree $d > 1$. Each prime divisor of $\mathbb{Z}E_{\text{tors}}(k)$ is less than $d^{3d^2}$.

Theorem 1.3 implies the following corollary (cf. e.g. [2]), what is called, the universal boundness conjecture.

Corollary 1.4. Let $d$ be a positive integer. Then there exists a constant $C_d$ depending only on $d$ such that $\mathbb{Z}E_{\text{tors}}(k) < C_d$ for any number field $k$ of degree $d$ and for any elliptic curve $E$ over $k$.

The Merel’s bound $d^{3d^2}$ is effective, but it is large. For example, when $d = 2$, we have $d^{3d^2} = 2^{12} = 4096$. So we want to improve Merel’s bound in case where we restrict $E$ to central $\mathbb{Q}$-curves.

We introduce the notion of $\mathbb{Q}$-curves.

Definition 1.5. We call a non-CM elliptic curve $E$ over $\overline{\mathbb{Q}}$ a $\mathbb{Q}$-curve if there exists an isogeny $\phi_\sigma$ from $^\sigma E$ to $E$ for each $\sigma$ in the absolute Galois group $G_\mathbb{Q}$ of $\mathbb{Q}$. Furthermore, we call a $\mathbb{Q}$-curve $E$ central if we can take an isogeny $\phi_\sigma$ with square-free degree for each $\sigma$ in $G_\mathbb{Q}$.

Theorem 1.6 (Elkies [3]). Each $\mathbb{Q}$-curve is isogenous to a central $\mathbb{Q}$-curve defined over a polyquadratic field.

Let $E$ be a central $\mathbb{Q}$-curve. As below in this paper we always assume that $E$ is defined over a polyquadratic field $k$ and that $\phi_\sigma = \phi_\tau$ if and only if $\sigma|_k = \tau|_k$. 

2
Since $E$ is a central $\mathbb{Q}$-curve, there exists an isogeny $\phi_\sigma$ from $^\sigma E$ to $E$ with square-free degree $d_\sigma$ for each $\sigma$ in $G_\mathbb{Q}$. We put
\[ c(\sigma, \tau) := \phi_\sigma^\sigma \phi_\tau \phi_{\sigma \tau}^{-1} \quad \text{for each } \sigma, \tau \text{ in } G_\mathbb{Q}. \quad (1) \]

Then a mapping $c$ is a two-cocycle of $G_\mathbb{Q}$ with values in $\mathbb{Q}^*$. By taking the degree of both sides, we have $c(\sigma, \tau)^2 = d_\sigma d_\tau d_{\sigma \tau}^{-1}$. Since it follows from $H^1(G_\mathbb{Q}, \mathbb{Q}^*) = \{1\}$ that there exists a mapping $\beta$ from $G_\mathbb{Q}$ to $\mathbb{Q}$ such that
\[ c(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma \tau)^{-1} \quad \text{for each } \sigma, \tau \text{ in } G_\mathbb{Q}, \quad (2) \]
we see that
\[ \varepsilon(\sigma) := d_\sigma \beta(\sigma)^{-2} \quad (3) \]
is a character of $G_\mathbb{Q}$.

We introduce our main theorems.

**Theorem 1.7.** If a prime number $N$ divides $\sharp E_{\text{tors}}(k)$, then $N$ satisfies at least one of the following conditions.

(i) $N \leq 13$.

(ii) $N = 2^{m+2} + 1, \ 3 \cdot 2^{m+2} + 1$ for some positive integer $m \leq \log_2 d$.

(iii) $\varepsilon$ is real quadratic and $N$ divides the generalized Bernoulli number $B_{2,\varepsilon}$.

If the scalar restriction of $E$ from $k$ to $\mathbb{Q}$ is of $\text{GL}_2$-type with real multiplications, $\varepsilon$ is trivial and thus $N$ is bounded by the constant depending only on the degree $d$. We conjecture that $N$ always satisfies the condition (i).

Furthermore, under the assumption that each $d_\sigma$ divides $\sharp E_{\text{tors}}(k)$, we completely determine the square-free divisor of $E_{\text{tors}}(k)$.

**Theorem 1.8.** Assume that each $d_\sigma$ divides $\sharp E_{\text{tors}}(k)$. Let $N$ be the product of all prime divisors of $\sharp E_{\text{tors}}(k)$. Then $[k : \mathbb{Q}]$ and $N$ satisfy the following.

<table>
<thead>
<tr>
<th>$[k : \mathbb{Q}]$</th>
<th>$N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 2, 3, 5, 6, 7, 10</td>
</tr>
<tr>
<td>2</td>
<td>2, 3, 6, 14</td>
</tr>
<tr>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>$\geq 8$</td>
<td>empty</td>
</tr>
</tbody>
</table>
We note that each case in the above list occurs. Specially, there is a family of infinitely many $\mathbb{Q}$-curves with rational torsion points corresponding to each element in the above list except for $N = 14$. In the case of $[k : \mathbb{Q}] = 1$ it is given by Kubert [11]. In the case of $[k : \mathbb{Q}] = 2$ and $N = 2, 3$ it is given by Hasegawa [5].

For example, when $[k : \mathbb{Q}] = 4$ and $N = 6$, $E$ is isomorphic to

$$y^2 + (1 - s)xy - (s^2 + s)y = x^3 - (s^2 + s)x^2$$

$$s = \frac{1}{12}(\sqrt{a} + \sqrt{4 + a})(3\sqrt{a} + \sqrt{4 + 9a})$$

for $a$ in $\mathbb{Q}$ such that $\Delta = s^6(s + 1)^3(9s + 1) \neq 0$.

When $N = 14$, there is only one $\mathbb{Q}$-curve corresponding to the above list. More precisely, $k = \mathbb{Q}(\sqrt{-7})$ and $E$ is defined by the global minimal model:

$$y^2 + (2 + \sqrt{-7})xy + (5 + \sqrt{-7})y = x^3 + (5 + \sqrt{-7})x^2.$$ 

Furthermore $E$ is a $\overline{\mathbb{Q}}$-simple factor of $J_{0}^{new}(98)$ and there exists an isogeny of degree 2 between $E$ and its non-trivial Galois conjugate curve.

Finally, we explain Theorem 1.8 in terms of modular curves. The existence of a non-CM elliptic curve over $k$ with a $k$-rational torsion of order $N$ is equivalent to that of a non-cuspidal non-CM $k$-rational point of the modular curve $X_1(N)$.

Let $X_0^*(N)$ be the quotient curve of the modular curve $X_0(N)$ by the group of Atkin-Lehner involutions of level $N$. Let $\pi$ be the natural projection from $X_0(N)$ to $X_0^*(N)$. The isomorphism classes of central $\mathbb{Q}$-curves are obtained from $\pi^{-1}(P)$ where $P$ is a non-cuspidal non-CM point of $X_0^*(N)(\mathbb{Q})$ and $N$ runs over the square-free integers.

Hence each element in the list of Theorem 1.8 corresponds to the existence of a non-cuspidal non-CM point of $X_1(N)(k) \times_{\mathbb{Q}(1)(\mathbb{Q})} \pi^{-1}X_0^*(M)(\mathbb{Q})$, where $M$ is the least common multiple of $d_\sigma$, which is a divisor of $N$ by the assumption of Theorem 1.8.

2 Central $\mathbb{Q}$-curves over polyquadratic fields

Let $N$ be a prime number. Let $E$ be a central $\mathbb{Q}$-curve over a polyquadratic field $k$ with a $k$-rational torsion point $Q_1$ of order $N$. We denote the group of $N$-torsion points on $E$ by $E[N]$. We take a point on $E[N]$ such that $\{Q_1, Q_2\}$ is a $\mathbb{Z}/NZ\mathbb{Z}$-basis of $E[N]$. Let $G$ be the Galois group of $k$ over $\mathbb{Q}$.

If $Q_1$ is in the kernel of $\phi_\sigma$ for some $\sigma$ in $G_\mathbb{Q}$, we can see that the $N$-th root $\zeta_N$ of unity is in the definition field of $\phi_\sigma$. Thus we have:
Proposition 2.1. If $N$ divides $d_\sigma$ for some $\sigma$ in $G_Q$, then $N$ is either 2 or 3.

As below we assume that $N > 3$. Then $Q_1$ is not in the kernel of $\phi_\sigma$ for any $\sigma$ in $G_Q$. Using the fact that $\phi_\sigma$ induces the isomorphism from $^\sigma E[N]$ to $E[N]$, we have Propositions 2.2 and 2.3.

Proposition 2.2. $\phi_\sigma$ is defined over $k$ for each $\sigma$ in $G_Q$. Specially, $E$ is completely defined over $k$.

Proposition 2.3. The 2-cocycle $c$ is symmetric. That is, $c(\sigma, \tau) = c(\tau, \sigma)$ for each $\sigma, \tau$ in $G_Q$.

Since $c$ is symmetric and $G$ is commutative, we may consider that $\beta$ is a mapping from $G$ to $Q^*$ (cf. e.g. [7]). By (3) the character $\varepsilon$ is either trivial or quadratic. Since we can see $\phi_\sigma^* \phi_\sigma = \varepsilon(\sigma) d_\sigma$, we have:

Proposition 2.4. The character $\varepsilon$ is even, that is, $\varepsilon(\rho) = 1$, where $\rho$ is the complex conjugation.

We denote by $F$ the extension of $Q$ adjoining all values $\beta(\sigma)$. Since $\beta(\sigma) = \pm \sqrt[3]{\varepsilon(\sigma)d_\sigma}$, $F$ is a polyquadratic field. We denote by $A$ the scalar restriction of $E$ from $k$ to $Q$. Since $E$ is a central $Q$-curve completely defined over $k$, $A$ is an abelian variety of $GL_2$-type with $End_0^0 A = F$. By using the isomorphisms $V_i(A) \cong \bigoplus \lambda \in \Lambda^i(\lambda)$ and $V_i(A) \cong \bigoplus \tau \in G^i(\tau E)$, we have:

Proposition 2.5. Let $k_\varepsilon$ be a field corresponding to the kernel of $\varepsilon$. If $E$ is semistable, $k$ is an unramified extension of $k_\varepsilon$.

For $\tau$ in $G_Q$ we have

$$\tau[R_1, R_2] = [R_1, R_2] \begin{bmatrix} 1 & * \\ 0 & \varepsilon(\tau) \chi(\tau) \end{bmatrix},$$

where $\chi$ is the cyclotomic character modulo $N$. Thus $k_\varepsilon(A[\lambda])/k_\varepsilon(\zeta_N)$ is an $\varepsilon\chi^{-1}$-extension (cf. [8], p.547). By modifying Herbrand’s Theorem (cf. e.g. [20], p.101), we have:

Proposition 2.7. If $k(E[N])/k(\zeta_N)$ is unramified and $N$ does not divide the generalized Bernoulli number $B_{2,\varepsilon}$, then $k(E[N]) = k(\zeta_N)$.
3 Proof of Theorem 1.7

Throughout this section we always assume the following:

(i) $N > 13$
(ii) $N \neq 2^{m+2} + 1, 3 \cdot 2^{m+2} + 1$
(iii) $N \nmid B_{2,\varepsilon}$

In this section we give a proof of Theorem 1.7 by modifying the result of Kamienny [8].

Let $S$ be the spectrum of the ring of integers in $k$. Let $p$ be a prime ideal of $k$ above a prime integer $p$.

**Proposition 3.1.** $E$ is semistable over $S$.

**Proof.** Let $k_p$ be the completion of $k$ at $p$ and let $\mathcal{O}_p$ be its ring of integers. Let $E/\mathcal{O}_p$ be the Néron model of $E/k_p$ over Spec $\mathcal{O}_p$. By the universal property of Néron models the morphism from $\mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p$ to $E/k_p$ extends to a morphism from $\mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p$ to $E/\mathcal{O}_p$ which maps to the Zariski closure in $E/\mathcal{O}_p$ of $\mathbb{Z}/N\mathbb{Z}/k_p \subset E/k_p$. This group scheme extension $H/\mathcal{O}_p$ is a separated quasi-finite group scheme over $\mathcal{O}_p$ whose generic fibre is $\mathbb{Z}/N\mathbb{Z}$. Since it admits a map from $\mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p$ which is an isomorphism on the generic fibre, it follows from that $H/\mathcal{O}_p$ is a finite flat group scheme of order $N$. Since $k$ is polyquadratic and $N$ is odd, the absolute ramification index $e_p$ over Spec $\mathbb{Z}$ is equal to 1 or 2. Since $e_p$ is less than $N - 1$, by the theorem of Raynaud [17, Cor. 3.3.6] we have $H/\mathcal{O}_p \cong \mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p$. Therefore we shall identify $H/\mathcal{O}_p$ with $\mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p$.

Suppose that the component $(E/p)^0$ is an additive group. Then the index of $(E/p)^0$ in $E/p$ is less than or equal to 4. It follows that $\mathbb{Z}/N\mathbb{Z}/p \subset (E/p)^0$. Thus, the residue characteristic $p$ is equal to $N$. By Serre-Tate [18] there exists a field extension $k'_p/k_p$ whose relative ramification index is less than or equal to 6, and such that $E/k'_p$ possess a semi-stable Néron model $\mathcal{E}/\mathcal{O}_p'$ where $\mathcal{O}_p'$ is the ring of integers in $k'_p$. Then we have a morphism $\psi$ from $E/\mathcal{O}_p'$ to $\mathcal{E}/\mathcal{O}_p'$ which is an isomorphism on generic fibres, using the universal Néron property of $\mathcal{E}/\mathcal{O}_p'$. The mapping $\psi$ is zero on the connected component of the special fibre of $E/\mathcal{O}_p'$ since there are no non-zero morphisms from an additive to a multiplicative type group over a field. Consequently, the mapping $\psi$ restricted to the special fibre of $\mathbb{Z}/N\mathbb{Z}/\mathcal{O}_p'$ is zero. Using Raynaud [17, Cor. 3.3.6], again, we see that this is impossible. Indeed, since $k$ is polyquadratic and $N$ is odd, the absolute ramification index of $k'_p$ is less than or equal to 12, which leads to a contradiction to the assumption $N - 1 > 12$. 

\[ \square \]
Proposition 3.2. Assume that $p$ is neither 2 nor 3. Then $p$ a multiplicative prime of $E$. Furthermore the reduction $Q_1$ does not specialize mod $p$ to $(E/p)^0$.

Proof. If $p$ is a good prime of $E$, then $E/p$ is an elliptic curve over $O/p$ containing a rational torsion point of order $N$. By the Riemann hypothesis of elliptic curves over the finite field $O/p$, $N$ must be less than or equal to $(1 + p^{h/2})^2$, where $f_p$ is the degree of residue field. Since $k$ is polyquadratic, we have $f_p = 1, 2$. Thus we have $(1 + p^{h/2})^2 \geq 16$. Since $N$ is prime, $N \geq 17$ follows from the assumption $N > 13$. Hence this is impossible, and $E$ has multiplicative reduction at $p$.

Suppose that $Q_1$ specialize to $(E/p)^0$. Over a quadratic extension $k_{/p}$ we have an isomorphism $E_{/k} \cong \mathbb{G}_{m/k}$, so that $N$ divides the cardinality of $k^*$. Since it follows from $f_p = 1, 2$ that the cardinality of $k^*$ is one of 3,8,15,80, this is impossible by the assumption $N > 13$.

The pair $(E,(Q_1))$ defines a $k$-rational point on the modular curve $X_0(N)_k$. If $p \neq N$, we denote by $x_{/p}$ the image of $x$ on the reduced curve $X_0(N)/(Q_{h/p})$. When $p$ is a potentially multiplicative prime of $E$, we know that $x_{/p} = \infty_{/p}$ if the point $Q_1$ does not specialize to the connected component $(E/p)^0$ of the identity (cf. [8], p.547).

We denote $J_0(N)/\mathbb{Q}$ the jacobian of $X_0(N)/\mathbb{Q}$. The abelian variety $J_0(N)$ is semi-stable and has good reduction at all primes $p \neq N$ ([1]). We denote by $J/Q$ the Eisenstein quotient of $J_0(N)/\mathbb{Q}$. Then Mazur [13] shows that $J(Q)$ is finite of order the numerator of $(N - 1)/12$, which is generated by the image of the class $0 - \infty$ by the projection from $J_0(N)$ to $J$

Proposition 3.3. Assume that $N$ is not of the form $2^{m+2} + 1$, $3 \cdot 2^{m+2} + 1$. If $p$ is any bad prime of $E$, then $Q_1$ does not specialize to $(E/p)^0$.

Proof. Define a map $g$ from $J_0(N)(k)$ to $J_0(N)(\mathbb{Q})$ by $g(x) = \sum_{\sigma \in G} \sigma x - d \cdot \infty$, where $d := [k : \mathbb{Q}]$. Let $f$ be the composition of $g$ with the projection $h$ from $J_0(N)$ to $J$. Then $f(x)$ is a torsion point, since $J(Q)$ is a finite group and $f(x)$ is $\mathbb{Q}$-rational. By Proposition 3.2 we have $\sigma x_{/p} = \infty_{/p}$ for each $\sigma$ and $p$ dividing 2, so we have

$$f(x)/p = h(\sum_{\sigma \in G} \sigma x_{/p} - d \cdot \infty_{/p}) = 0,$$

so $f(x)$ has order a power of 2. However, $f(x)/p = 0$ for $p$ dividing 3 by the same reasoning. Thus, $f(x)$ has order a power of 3, and so $f(x) = 0$.

If $p$ is a bad prime of $E$ which $Q_1$ does not specialize to $(E/p)^0$, then $x_{/p} = 0/p$. By Proposition 3.2 we may assume that the residue characteristic
Proof. If $E$ has good reduction at $p$ and $p \neq N$, then $k(E[N])/k(\zeta_N)$ is unramified at the primes lying above $p$ (cf. Serre-Tate[18]).

If $E$ has good reduction at $p$ and $p = N$, then $E[N]$ is a finite flat group scheme over $\mathcal{O}_p$. Then there is a short exact sequence of finite flat group schemes over $\mathcal{O}_p$:

$$0 \to \mathbb{Z}/N\mathbb{Z} \to E[N] \to \mu_N \to 0.$$ 

However, $E[N]$ also fits into a short exact sequence

$$0 \to E[N]^0 \to E[N] \to E[N]^\text{ét} \to 0,$$

where $E[N]^0$ is the largest connected subgroup of $E[N]$ and $E[N]^\text{ét}$ is the largest étale quotient (cf. [14], p.134-138). Clearly we have $E[N]^0 = \mu_N$, and this gives us splitting of the above exact sequences. Since $[k(E[N]) : k(\zeta_N)]$ divides $N$, the action of the inertia subgroup for $p$ in $G_{k(\zeta_N)}$ on $E[N]$ is trivial. Namely, $k(E[N])/k(\zeta_N)$ is unramified at the primes lying above $p$.

Assume that $E$ has bad reduction at $p$. Since $J_0(N)$ is semistable, $E[N]/p$ is a quasi-finite flat group scheme over $\mathcal{O}_p$ (cf. [4]), and fits into a short exact sequence

$$0 \to \mathbb{Z}/N\mathbb{Z} \to E[N] \to \overline{\mu}_N \to 0,$$

where $\overline{\mu}_N$ is a quasi-finite flat group with generic fibre isomorphic to $\mu_N$. Since $Q_1$ does not specialize to $(E/p)^0$, we see that the kernel of multiplication by $N$ on $(E/p)^0$ maps injectively to $\overline{\mu}_N$. Thus, $\overline{\mu}_N$ is actually a finite flat group scheme. If $p \neq N$, then $E[N]$ is étale, and so $k(E[N])/k(\zeta_N)$ is unramified at the primes above $p$. If $p = N$, then $\mu_N = \overline{\mu}_N$ by Raynaud [17, Cor. 3.3.6] and $e_N \leq 2 < N - 1$. We see that $E[N]/\mathcal{O}_p = \mathbb{Z}/N \oplus \mu_N$, so $k(E[N])/k(\zeta_N)$ is unramified at the primes above $p$. 

By Propositions 2.7 and 3.4, we see that $k(E[N]) = k(\zeta_N)$. Thus $\langle Q_2 \rangle$ is $k$-rational. 

8
Proposition 3.5. The quotient curve \( E/\langle Q_2 \rangle \) is again a central \( \mathbb{Q} \)-curve over \( k \) with \( N \)-rational torsion point. Furthermore the image of \( Q_1 \) is \( N \)-rational point of \( E/\langle Q_2 \rangle \) and

\[
\begin{array}{ccc}
\sigma E & \xrightarrow{\phi_\sigma} & E \\
\downarrow & & \downarrow \\
\sigma \left( E/\langle Q_2 \rangle \right) & \xrightarrow{\phi_\sigma} & E/\langle Q_2 \rangle
\end{array}
\]

Proof. Since \( \langle Q_2 \rangle \) is \( k \)-rational, the quotient curve \( E/\langle Q_2 \rangle \) is a \( \mathbb{Q} \)-curve over \( k \). We show that \( \phi_\sigma(\sigma Q_2) \subseteq \langle Q_2 \rangle \). We may put \( \phi_\sigma(\sigma Q_2) = aQ_1 + bQ_2 \). Since \( Q_1 \) is \( k \)-rational, \( \phi_\sigma(\tau^* Q_2) = aQ_1 + b^* Q_2 \) for each \( \tau \in G_k \). Since \( \langle Q_2 \rangle \) is \( k \)-rational, \( a \neq 0 \) implies \( \tau^* Q_2 = Q_2 \) and thus \( k(E[N]) = k \). Since \( k \) is polyquadratic and \( N > 3 \), this leads to contradiction.

Since \( \phi_\sigma(\sigma Q_2) \subseteq \langle Q_2 \rangle \), we have the above diagram. Specially \( E/\langle Q_2 \rangle \) is again central \( \mathbb{Q} \)-curve. \qed

Proof of Theorem 1.7. By Proposition 3.5 we get a sequence central \( \mathbb{Q} \)-curves over \( k \)

\[ E \rightarrow E^{(1)} \rightarrow E^{(2)} \rightarrow E^{(3)} \rightarrow \cdots \]

each obtained from the next by an \( N \)-isogeny, and such that the original group \( \mathbb{Z}/N\mathbb{Z} \) maps isomorphically into every \( E^{(j)} \).

It follows from Shafarevic theorem that among the set of \( E^{(j)} \) there can be only a finite number of \( k \)-isomorphism class of elliptic curve represented. Consequently, for some indecies \( j > j' \) we must have \( E^{(j)} \cong E^{(j')} \). But \( E^{(j)} \) maps to \( E^{(j')} \) by nonscalar isogeny. Therefore \( E^{(j)} \) is a CM elliptic curve and so is \( E \). This contradicts to the assumption that \( E \) is non-CM. \qed

4 Proof of Theorem 1.8

We recall that each element in the list of Theorem 1.8 corresponds to existence of a non-cuspidal non-CM point of \( X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1} X_0^*(M)(\mathbb{Q}) \). Suppose that there exists such a point. Then by Proposition 2.1 we have \( M = 2, 3 \). By using Theorem 1.7 and Proposition 2.5 we see that each divisor of \( N \) less than or equal to 13. Thus there are only finite couples \((N, M)\) such that \( X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1} X_0^*(M)(\mathbb{Q}) \) has a non-cuspidal non-CM point. For such \((N, M)\), by computing defining equations, we check whether there is a non-cuspidal non-CM point of \( X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1} X_0^*(M)(\mathbb{Q}) \) or not.
References


Fumio SAIRAIJI,
Hiroshima International University,
Hiro, Hiroshima 737-0112, Japan.
e-mail address: sairaiji@it.hirokoku-u.ac.jp

Takuya YAMAUCHI,
Hiroshima University,
Higashi-hiroshima, Hiroshima 739-8526, Japan.
e-mail address: yamauchi@math.sci.hiroshima-u.ac.jp