数理解析研究所講究録
1521巻 2006年 139-149

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

Fumio Sairaiji (Hiroshima International University)
Takuya Yamauchi [1] (Hiroshima University)

1 Introduction

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 $E_{tors}(k)$ be its torsion subgroup. When k is the rational number field $\mathbb{Q}$, Mazur [12] shows that $E_{tors}(\mathbb{Q})$ is isomorphic to one of 15 abelian groups. Kunku-Momose [10] and Kamienny [9] generalize the result of Mazur to the case where k is a quadratic field.

Assume that the degree d is greater than one. Then Merel [15] shows that each prime divisor of the order $\sharp E_{tors}(k)$ is less than d^{3d^2}. Merel's bound is effective, but it is large.

In this paper we discuss about prime divisors of the order $\sharp E_{tors}(k)$ in case where we restrict E to a central $\mathbb{Q}$-curve over a polyquadratic field k. Our results assert that each prime divisor of $\sharp E_{tors}(k)$ is less than or equal to 13 or that it belongs to a finite set of prime numbers depending on k.

In Section 2, we review some known results on $E_{tors}(k)$. In Section 3, we give the definition of central $\mathbb{Q}$-curves and we introduce our results. In Sections 4-6, we give outline of proofs of our results.

2 Known Results

Let E be an elliptic curve over a number field k. Let $E(k)$ be the group of k-rational points on E.

Theorem 2.1 (Mordell-Weil Theorem). *The group $E(k)$ is a finitely generated abelian group. Specially, $E_{tors}(k)$ is a finite abelian group.*

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

Theorem 2.2 (Mazur [12]). *Assume that k is equal to $\mathbb{Q}$. Then the group $E_{tors}(\mathbb{Q})$ is isomorphic to one of the following 15 abelian groups.*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & (1 \le N \le 10,\ N = 12) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & (1 \le N \le 4) \end{array}$$

[1]The auther is supported by the Japan Society for the Promotion of Science Research Fellowships for Young Scientists.

Specially, each prime divisor of $\sharp E_{tors}(\mathbb{Q})$ is less than or equal to 7. For each group G in Theorem 2.2, Kubert [11] gives a defining equation parameterizing elliptic curves E such that $E_{tors}(\mathbb{Q})$ contains G. For example, if $E_{tors}(\mathbb{Q})$ 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.

The existance of an elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational torsion of order N is equivalent to that of a non-cuspidal $\mathbb{Q}$-rational point of the modular curve $X_1(N)$.

Theorem 2.3 (Kenku-Momose [10], Kamienny [9]). *Let k be a quadratic field. Then the group $E_{tors}(k)$ is isomorphic to one of the following 25 abelian groups.*

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

Specially, each prime divisor of $\sharp E_{tors}(k)$ is less than or equal to 13. For elliptic curves over number fields of degree greater than two, there exist some reuslts on the group structure of $E(k)_{tors}$ under some conditions (cf. e.g. [6], [21]).

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

Theorem 2.4 (Merel [15]). *Let k be a number field of degree $d > 1$. Each prime divisor of $\sharp E_{tors}(k)$ is less than d^{3d^2}.*

Theorem 2.4 implies the following corollary (cf. e.g. [2]), what is called, the universal boundness conjecture.

Corollary 2.5. *Let d be a positive integer. Then there exists a constant C_d depending only on d such that $\sharp E_{tors}(k) < C_d$ for any number field k of degree d and for any elliptic curve E over k.*

3 Our Results

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

Definition 3.1. *We call a non-CM elliptic curve E over $\overline{\mathbb{Q}}$ a $\mathbb{Q}$-curve if there exists an isogeny ϕ_σ from ${}^\sigma E$ to E for each σ 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 ϕ_σ with square-free degree for each σ in $G_\mathbb{Q}$.*

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 π 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.

Theorem 3.2 (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 of degree 2^d and that $\phi_\sigma = \phi_\tau$ if and only if $\sigma_{|k} = \tau_{|k}$.

Since E is a central $\mathbb{Q}$-curve, there exists an isogeny ϕ_σ from ${}^\sigma E$ to E with square-free degree d_σ for each σ in $G_\mathbb{Q}$. We put

$$c(\sigma,\tau) = \phi_\sigma {}^\sigma\phi_\tau \phi_{\sigma\tau}^{-1} \quad \text{for each } \sigma,\tau \text{ in } G_\mathbb{Q}. \tag{1}$$

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 $\mathrm{H}^1(G_\mathbb{Q}, \overline{\mathbb{Q}}^*) = \{1\}$ that there exists a mapping β from $G_\mathbb{Q}$ to $\overline{\mathbb{Q}}$ such that

$$c(\sigma,\tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1} \quad \text{for each } \sigma,\tau \text{ in } G_\mathbb{Q}, \tag{2}$$

we see that

$$\varepsilon(\sigma) := \frac{d_\sigma}{\beta(\sigma)^2} \tag{3}$$

is a character of $G_\mathbb{Q}$. We obtain:

Theorem 3.3. *If a prime number N divides $\sharp E_{tors}(k)$, then N satisfies at least one of the following conditions.*

(i) $N \leqq 13$.

(ii) $N = 2^{m+2}+1,\ 3\cdot 2^{m+2}+1$ *for some* $m \leqq d$.

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

The condition (iii) depends on the definition field k of E. If the scalar restriction of E from k to $\mathbb{Q}$ is of GL_2-type with real multiplications, we have $\varepsilon = 1$ and thus N is bounded by the constant depending only on the degree of k.

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

Theorem 3.4. *Assume that each d_σ divides $\sharp E_{tors}(k)$. Let N be the product of all prime divisors of $\sharp E_{tors}(k)$. Then $[k : \mathbb{Q}]$ and N satisfy the following.*

$[k:\mathbb{Q}]$	N
1	1, 2, 3, 5, 6, 7, 10
2	2, 3, 6, 14
4	6
≥ 8	*empty*

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.

Let π be the natural projection from $X_1(N)$ to $X_0^*(N)$ via $X_0(N)$. Each element in the list of Theorem 3.4 corresponds to the existance of a non-cuspidal non-CM point of $X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}X_0^*(M)(\mathbb{Q})$, where M is the least common multiple of d_σ, which is a divisor of N by the assumption of Theorem 3.4.

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

Let notations and assumptions be the same as in the previous section. We denote the group of N-torsion points on E by $E[N]$. We take a $\mathbb{Z}/N\mathbb{Z}$-basis $\{Q_1, Q_2\}$ of $E[N]$ such that Q_1 is k-rational. Let G be the Galois group of k over $\mathbb{Q}$.

If Q_1 is in the kernel of ϕ_σ for some σ in $G_\mathbb{Q}$, we can see that the N-th root ζ_N of unity is in the definition field of ϕ_σ. Thus we have:

Proposition 4.1. *If N divides d_σ for some σ in $G_\mathbb{Q}$, then N is either 2 or 3.*

As below we assume that $N > 3$. Then Q_1 is not in the kernel of ϕ_σ for any σ in $G_\mathbb{Q}$. Using the fact that ϕ_σ induces the isomorphism from ${}^\sigma E[N]$ to $E[N]$, we have Propositions 4.2 and 4.3.

Proposition 4.2. *ϕ_σ is defined over k for each σ in $G_\mathbb{Q}$. Specially, E is completely defined over k.*

Proposition 4.3. *The 2-cocycle c is symmetric. That is, $c(\sigma, \tau) = c(\tau, \sigma)$ for each σ, τ in $G_\mathbb{Q}$.*

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

Proposition 4.4. *The character ε is even, that is, $\varepsilon(\rho) = 1$, where ρ is the complex conjugation.*

We denote by F the extension of $\mathbb{Q}$ adjoining all values $\beta(\sigma)$. Since $\beta(\sigma) = \pm\sqrt{\varepsilon(\sigma)d_\sigma}$, F is a polyquadratic field. We denote by A the scalar restriction of E from k to $\mathbb{Q}$. Since E is a central $\mathbb{Q}$-curve completely defined over k, A is an abelian variety of GL_2-type with $\mathrm{End}^0_\mathbb{Q} A = F$. By using the isomorphisms l-adic (λ-adic) Tate modules, $V_l(A) \cong \oplus_{\lambda | l} V_\lambda(A)$ and $V_l(A) \cong \oplus_{\tau\in G} V_l({}^\tau E)$, we have:

Proposition 4.5. *Let k_ε be a field corresponding to the kernel of ε. If E is semistable, k is an unramified extension of k_ε.*

By the definition of the scalar restriction, $A(\mathbb{Q})$ and $E(k)$ are bijective. Since ζ_N is not in k, the group of k-rational N-torsion points on E must be $\langle Q_1\rangle$. Thus A has the unique $\mathbb{Q}$-rational N-torsion group $\langle R_1\rangle$. There exists the unique prime λ of F dividing N such that R_1 is in $A[\lambda]$.

Proposition 4.6. $k(E[N]) = k(A[\lambda])$.

For τ in $G_{\mathbb{Q}}$ we have

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

where χ 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 4.7. *If $k(E[N])/k(\zeta_N)$ is unramified and N does not divide the generalized Bernoulli number $B_{2,\varepsilon}$, then $k(E[N]) = k(\zeta_N)$.*

5 Proof of Theorem 3.3

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 3.3 by modifying the result of Kamienny [8].

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

Proposition 5.1. *E is semistable over S.*

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

Suppose that the component $(E_{/\mathfrak{p}})^0$ is an additive group. Then the index of $(E_{/\mathfrak{p}})^0$ in $E_{/\mathfrak{p}}$ is less than or equal to 4. It follows that $\mathbb{Z}/N\mathbb{Z}_{/\mathfrak{p}} \subset (E_{/\mathfrak{p}})^0$.

Thus, the residue characteristic p is equal to N. By Serre-Tate [18] there exists a field extension $k'_\mathfrak{p}/k_\mathfrak{p}$ whose relative ramification index is less than or equal to 6, and such that $E_{/k'_\mathfrak{p}}$ possess a semi-stable Néron model $\mathcal{E}_{/\mathcal{O}'_\mathfrak{p}}$ where $\mathcal{O}'_\mathfrak{p}$ is the ring of integers in $k'_\mathfrak{p}$. Then we have a morphism ψ from $E_{/\mathcal{O}'_\mathfrak{p}}$ to $\mathcal{E}_{/\mathcal{O}'_\mathfrak{p}}$ which is an isimorphism on generic fibres, using the universal Néron property of $\mathcal{E}_{/\mathcal{O}'_\mathfrak{p}}$. The mapping ψ is zero on the connected component of the special fibre of $E_{/\mathcal{O}'_\mathfrak{p}}$ since there are no non-zero morphisms from an additive to a multiplicative type group over a field. Consequently, the mapping ψ restricted to the special fibre of $\mathbb{Z}/N\mathbb{Z}_{/\mathcal{O}'_\mathfrak{p}}$ 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 $k'_\mathfrak{p}$ is less than or equal to 12, which leads to a contradiction to the assumption $N-1>12$. □

Proposition 5.2. *Assume that p is neither 2 nor 3. Then $\mathfrak{p}$ a multiplicative prime of E. Furthermore the reduction Q_1 does not specialize mod $\mathfrak{p}$ to $(E_{/\mathfrak{p}})^0$.*

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

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

The pair $(E, \langle Q_1\rangle)$ defines a k-rational point on the modular curve $X_0(N)_\mathbb{Q}$. If $p\neq N$, we denote by $x_{/\mathfrak{p}}$ the image of x on the reduced curve $X_0(N)_{/(\mathcal{O}_k/\mathfrak{p})}$ When $\mathfrak{p}$ is a potentially multiplicative prime of E, we know that $x_{/\mathfrak{p}}=\infty_{/\mathfrak{p}}$ if the point Q_1 does not specialize to the connected component $(E_{/\mathfrak{p}})^0$ 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 $\tilde{J}_{/\mathbb{Q}}$ the Eisenstein quotient of $J_0(N)_{/\mathbb{Q}}$. Then Mazur [13] shows that $\tilde{J}(\mathbb{Q})$ 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 $\tilde{J}$

Proposition 5.3. *Assume that N is not of the form $2^{m+2}+1,\ 3\cdot 2^{m+2}+1$. If $\mathfrak{p}$ is any bad prime of E, then Q_1 does not specialize to $(E_{/\mathfrak{p}})^0$.*

Proof. Define a map g from $X_0(N)(k)$ 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 $\tilde{J}$. Then $f(x)$ is a torsion point, since $\tilde{J}(\mathbb{Q})$ is a finite group and $f(x)$ is $\mathbb{Q}$-rational. By Proposition 5.2 we have ${}^{\sigma}x_{/\mathfrak{p}} = \infty_{/\mathfrak{p}}$ for each σ and $\mathfrak{p}$ dividing 2, so we have

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

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

If $\mathfrak{p}$ is a bad prime of E which Q_1 does not specialize to $(E_{/\mathfrak{p}})^0$, then $x_{/\mathfrak{p}} = 0_{/\mathfrak{p}}$. By Proposition 5.2 we may assume that the residue characteristic p is not 2, 3 or N. Since E is a $\mathbb{Q}$-curve completely defined over k, we have ${}^{\sigma}x_{/\mathfrak{p}} = 0_{/\mathfrak{p}}$ for each σ. Thus,

$$f(x)_{/\mathfrak{p}} = h(\sum_{\sigma\in G} {}^{\sigma}x_{/\mathfrak{p}} - d\cdot\infty_{/\mathfrak{p}}) = h(d(0-\infty))_{/\mathfrak{p}}.$$

Since $h(0-\infty)$ is $\mathbb{Q}$-rational point, the order of $h(0-\infty)$ divides d. Since the order of $h(0-\infty)$ is equal to the numerator of $(N-1)/12$, N is of the form $2^{m+2}+1,\ 3\cdot 2^{m+2}+1$, which is impossible by the assumption. □

Proposition 5.4. *$k(E[N])/k(\zeta_N)$ is everywhere unramified.*

Proof. If E has good reduction at $\mathfrak{p}$ and $p \neq N$, then $k(E[N])/k(\zeta_N)$ is unramified at the primes lying above $\mathfrak{p}$ (cf. Serre-Tate[18]).

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

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

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 $\mathfrak{p}$ in $G_{k(\zeta_N)}$ on $E[N]$ is trivial. Namely, $k(E[N])/k(\zeta_N)$ is unramified at the primes lying above $\mathfrak{p}$.

Assume that E has bad reduction at $\mathfrak{p}$. Since $J_0(N)$ is semistable , $E[N]_{/\mathfrak{p}}$ is a quasi-finite flat group scheme over $\mathcal{O}_{\mathfrak{p}}$ (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 μ_N. Since Q_1 does not specialize to $(E_{/\mathfrak{p}})^0$, we see that the kernel of multiplication by N on $(E_{/\mathfrak{p}})^0$ 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 $\mathfrak{p}$. 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 $E[N]_{/\mathcal{O}_\mathfrak{p}} = \mathbb{Z}/N \oplus \mu_N$, so $k(E[N])/k(\zeta_N)$ is unramified at the primes above $\mathfrak{p}$. □

By Propositions 4.7 and 5.4, we see that $k(E[N]) = k(\zeta_N)$. Thus $\langle Q_2 \rangle$ is k-rational.

Proposition 5.5. *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*

$$\begin{array}{ccc} {}^{\sigma}E & \xrightarrow{\phi_\sigma} & E \\ \downarrow & & \downarrow \\ {}^{\sigma}\Big(E/\langle Q_2 \rangle\Big) & \xrightarrow{\phi_\sigma} & E/\langle Q_2 \rangle \end{array}$$

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 $\phi_\sigma \langle {}^{\sigma}Q_2 \rangle \subset \langle Q_2 \rangle$. We may put $\phi_\sigma({}^{\sigma}Q_2) = aQ_1 + bQ_2$. Since Q_1 is k-rational, $\phi_\sigma({}^{\tau\sigma}Q_2) = aQ_1 + b^{\tau}Q_2$ 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 $\phi_\sigma \langle {}^{\sigma}Q_2 \rangle \subset \langle Q_2 \rangle$, we have the above diagram. Specially $E/\langle Q_2 \rangle$ is again central $\mathbb{Q}$-curve. □

Proof of Theorem 3.3. By Proposition 5.5 we get a sequence central $\mathbb{Q}$-curves over k

$$E \to E^{(1)} \to E^{(2)} \to E^{(3)} \to \cdots$$

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. □

6 Proof of Theorem 3.4

We recall that each element in the list of Theorem 3.4 corresponds to existance of a non-cuspidal non-CM point of $X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}X_0^*(M)(\mathbb{Q})$. By Proposition 4.1 we have $M = 2, 3$. By using Theorem 3.3 and Proposition 4.5 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

[1] P. Deligne and M. Rapoport, *Schémas de modules de courbes elliptiques,* Lect. Notes Math. **349**, Berlin-Heiderlberg-New York, Springer (1973).

[2] B. Edixhoven, *Rational torsion points on elliptic curves over number fields,* Séminaire Bourbaki, 46ème année, 1993-94, n° 782, 209-227.

[3] N.D. Elkies, *On elliptic K-curves,* Modular curves and abelian varieties., ed. J. Cremona etc, progress in math **224**, Birkhäuser, 81-91.

[4] A. Grothendieck, *Groupes de monodromie en géometrie algébrique* , Lecture Notes in Mathematics 288, 340, 1972/3.

[5] Y. Hasegawa, *$\mathbb{Q}$-curves over quadratic fields*, Manuscripta Math. **94** (1997), no. 3, 347–364.

[6] D. Jeon, C.H. Kim and A. Schwezer, *On the torsion of elliptic curves over cubic number fields*, Acta Arithmetica **113** (2004), 291-301.

[7] G. Karpilovsky, *Group representations,* Vol. 2 (Elsevier, Amsterdam, 1993).

[8] S. Kamienny, *On the torsion subgroups of elliptic curves over totally real field,* Invent. Math. **83** (1986), 545-551.

[9] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms,* Invent. Math. **109** (1992), 221-229.

[10] M. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[11] D.S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

[12] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 107–148. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977

[13] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1978), 33-186.

[14] B. Mazur, *Rational isogenies of prime degree*, Invent Math. **44** (1978), 129-162.

[15] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres,* Invent. Math. **124** (1996), 437-449.

[16] E.E. Pyle, *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$*. In J. Cremona, J.C. Lario, J. Quer and K. Ribet (ed.): Modular curves and abelian varieties, 189-239, Progress in Mathematics **224**, Birkhäuser, 2004.

[17] M. Raynaud, *Schémas en groupes de type $(p,\ldots,p)$,* Bull. Soc Math. Fr. **102** (1974), 241-280.

[18] J.-P. Serre and J. Tate, *Good reduction of abelian varieties,* Ann. Math. **88** (1968), 492-517.

[19] J. Tate, *Algorithm for determining the type of a singular fibre in an elliptic pencil,* B.J.Birch,W.Kuyk(editors), Modular Function of One Variable IV, Springer-Verlag, LNM 476 (1975).

[20] L.C. Washington, *Introduction to cyclotomic fields,* Springer GTM 83.

[21] H.G. Zimmer, *Torsion groups of elliptic curves over cubic and certain biquadratic number fields,* Contemp. Math. **174** (1994), 203-220.

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