

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Fumio SAIRAJI et Takuya YAMAUCHI

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

Tome 20, n° 2 (2008), p. 465-483.

http://jtnb.cedram.org/item?id=JTNB_2008__20_2_465_0

© Université Bordeaux 1, 2008, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

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

par FUMIO SAIRAJI et TAKUYA YAMAUCHI

RÉSUMÉ. Soit E une \mathbb{Q} -courbe centrale sur un corps polyquadratique k . Dans cet article, nous donnons une borne supérieure des diviseurs premiers de l'ordre du sous-groupe de torsion k -rationnel $E_{tors}(k)$ (voir Théorèmes 1.1 et 1.2). La notion de \mathbb{Q} -courbe centrale est une généralisation de celle de courbe elliptique sur \mathbb{Q} . Notre résultat est une généralisation du Théorème de Mazur [12], et c'est une précision des bornes supérieures de Merel [15] et Oesterlé [17].

ABSTRACT. Let E be a central \mathbb{Q} -curve over a polyquadratic field k . In this article we give an upper bound for prime divisors of the order of the k -rational torsion subgroup $E_{tors}(k)$ (see Theorems 1.1 and 1.2). The notion of central \mathbb{Q} -curves is a generalization of 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 bounds of Merel [15] and Oesterlé [17].

1. Introduction

Let E be an elliptic curve over an algebraic 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. The Mordell-Weil Theorem asserts that $E(k)$ is a finitely generated abelian group and thus the order $\#E_{tors}(k)$ of $E_{tors}(k)$ is finite. We discuss about prime divisors of the order $\#E_{tors}(k)$.

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. Each prime divisor of $\#E_{tors}(\mathbb{Q})$ is less than or equal to 7. When k is a quadratic field, after Kenku-Momose [10], Kamienny [9] shows that $E_{tors}(k)$ is isomorphic to one of 25 abelian groups. Each prime divisor of $\#E_{tors}(k)$ is less than or equal to 13.

When d is greater than one, Merel [15] shows that each prime divisor of $\#E_{tors}(k)$ is less than or equal to d^{3d^2} . The bound is improved by Oesterlé [17]. He shows that $\#E_{tors}(k)$ is less than or equal to $(1 + 3^{d/2})^2$. We want to improve Oesterlé's bound in case where we restrict E to \mathbb{Q} -curves.

Manuscrit reçu le 11 septembre 2008.

The authors are partially supported by JSPS Core-to-Core Program No.18005. The first and second authors are also partially supported by JSPS Grant-in-Aid for Scientific research No.18740021 and No.19740017, respectively.

Definition. We call an 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 squarefree degree for each σ in $G_{\mathbb{Q}}$.

Elkies [3] shows that each non-CM \mathbb{Q} -curve is isogenous to a central \mathbb{Q} -curve and that each non-CM central \mathbb{Q} -curve is defined over a polyquadratic field. In this paper we always assume that each \mathbb{Q} -curve is non-CM.

Let $X_0^*(N)$ be the quotient curve of the modular curve $X_0(N)$ by the group $W(N)$ 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 squarefree integers.

Let E be a central \mathbb{Q} -curve defined over a polyquadratic field k of degree d . In this paper we always assume that k is the minimal field of definition of E . Since E is a central \mathbb{Q} -curve, there exists an isogeny ϕ_σ from ${}^\sigma E$ to E with squarefree degree d_σ for each σ in $G_{\mathbb{Q}}$.

Theorem 1.1. *If a prime number N divides $\sharp E_{tors}(k)$, then N satisfies at least one of the following conditions.*

- (1) $N \leq 13$.
- (2) $N = 2^{m+2} + 1, 3 \cdot 2^{m+2} + 1$ for some integer $m \leq \log_2 d$.
- (3) *The character ε of $G_{\mathbb{Q}}$, associated with E , defined in (3.4), is real quadratic, and N divides the generalized Bernoulli number $B_{2,\varepsilon}$.*

Corollary 1.1. *Assume the scalar restriction A of E from k to \mathbb{Q} is of GL_2 -type with real multiplications. If a prime number N divides $\sharp E_{tors}(k)$, then N is less than or equal to 13.*

Theorem 1.2. *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. There is a family of infinitely many \mathbb{Q} -curves with rational torsion points corresponding to each element in the above list except for $N = 14$. The case of $[k : \mathbb{Q}] = 1$ is due to Kubert [11]. The case of $[k : \mathbb{Q}] = 2$ and $N = 2, 3$ is given by Hasegawa [6]. The case of $N = 6$ is given by Quer [20] (see also Appendix 1). When $N = 14$, there is only one \mathbb{Q} -curve corresponding to the above list. More

precisely, $k = \mathbb{Q}(\sqrt{-7})$ and the corresponding \mathbb{Q} -curve has the j -invariant

$$j = \frac{56437681 - 1875341\sqrt{-7}}{32768}$$

and the global minimal model:

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

It is a $\overline{\mathbb{Q}}$ -simple factor of $J_0^{new}(98)$.

Let π be the natural projection from $X_1(N)$ to $X_0(M)/W$ via $X_0(N)$, where M is the least common multiple of d_σ and W is a subgroup of the group $W(M)$ of order $[k : \mathbb{Q}]$. We note that M is a divisor of N by the assumption of Theorem 1.2. Each element in the list of Theorem 1.2 corresponds to the existence of a non-cuspidal non-CM point of $X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}(X_0(M)/W)(\mathbb{Q})$.

In Section 2 we review basic facts on modular curves and in Section 3 we investigate fields of torsion points of central \mathbb{Q} -curves over polyquadratic fields. In Sections 4 and 5 we prove Theorems 1.1 and 1.2, respectively.

2. Preliminaries

Let \mathbb{H} be the complex upper half plane. For any positive integer N , let

$$\Gamma_1(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\},$$

and

$$\Gamma_0(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

The group $\Gamma_1(N)$ acts on $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$ via fractional linear transformations. The quotient $X_1(N)$ (resp. $X_0(N)$) of \mathbb{H}^* by $\Gamma_1(N)$ (resp. $\Gamma_0(N)$) has a structure as a compact Riemann surface and it also has a canonical structure as an algebraic curve over \mathbb{Q} . For $i = 0, 1$, each element in $\Gamma_i(N) \backslash \mathbb{Q} \cup \{i\infty\}$ is so called cusp and $Y_i(N) := X_i(N) \backslash (\Gamma_i(N) \backslash \mathbb{Q} \cup \{i\infty\})$ is an open affine curve.

The modular curve $X_1(N)$ is the coarse moduli space of the isomorphism classes of pairs (E, P) where E is a generalized elliptic curve and P is a point of E of order N and the modular curve $X_0(N)$ is the coarse moduli space of the isomorphism classes of pairs (E, C) where E is a generalized elliptic curve and C is a cyclic subgroup of E of order N . For a subfield k of the complex number field \mathbb{C} , each k -rational point of $Y_0(N)$ (resp. $Y_1(N)$) corresponds to a pair (E, C) (resp. (E, P)) where E is an elliptic curve over k and C (resp. P) is a k -rational subgroup (resp. point) of order N .

Let $0 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and $i\infty := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ be the \mathbb{Q} -rational cusps on $X_0(N)$. Then they are represented by $(\mathbb{G}_m, \mathbb{Z}/N\mathbb{Z})$ and (\mathbb{G}_m, μ_N) respectively, where \mathbb{G}_m

is the multiplicative group. In fact, 0 (resp. $i\infty$) corresponds to Kodaira's symbol I_N (resp. I_1).

Let d be a positive divisor d of N with $d \neq 1, N$ and let m be the greatest common divisor of d and N/d . For a positive integer i , coprime to N , with $1 \leq i \leq m$, we denote by $\left(\frac{i}{d}\right)$ the cusps on $X_0(N)$. Then they are represented by

$$(\mathbb{G}_m \times \mathbb{Z}/(N/d)\mathbb{Z}, \langle \zeta_N \rangle \times \langle i \rangle).$$

Each cusp $\left(\frac{i}{d}\right)$ is defined over $\mathbb{Q}(\zeta_m)$. In particular, if N is squarefree, then all cusps on $X_0(N)$ are defined over \mathbb{Q} .

Let n be a positive divisor of N such that $(n, \frac{N}{n}) = 1$, and put $W_n := \begin{bmatrix} nx & y \\ Nz & nw \end{bmatrix}$, where x, y, z, w are in \mathbb{Z} and $\det(W_n) = n$. Then $\Gamma_0(N) \cup W_n\Gamma_0(N)$ is a normalization of $\Gamma_0(N)$ in $\text{GL}_2^+(\mathbb{Q})$ and W_n induces an involution on $X_0(N)$. The group $W(N)$ generated by involutions W_n on $X_0(N)$ is an elementary abelian 2-group of order 2^r , where r is the number of distinct prime divisors of N . It is well known that all elements of $W(N)$ are defined over \mathbb{Q} . So the quotient modular curve $X_0^*(N)$ of $X_0(N)$ by $W(N)$ is defined over \mathbb{Q} .

3. The field $k(\mathbf{E}[N])$ of N -torsion points

3.1. The minimal field of definition of E . Let E be a central \mathbb{Q} -curve over $\overline{\mathbb{Q}}$ with the j -invariant j_E . We call the field $\mathbb{Q}(j_E)$ the *minimal field of definition* of E . By taking a model defined over $\mathbb{Q}(j_E)$, we assume that E is defined over $\mathbb{Q}(j_E)$. We put $k := \mathbb{Q}(j_E)$. We denote by G the Galois group of k over \mathbb{Q} .

According to Ribet [22], we introduce the 2-cocycle c associated with E . Since E is a central \mathbb{Q} -curve, there exists an isogeny ϕ_σ from ${}^\sigma E$ to E with squarefree degree d_σ for each σ in $G_{\mathbb{Q}}$. We put

$$(3.1) \quad c(\sigma, \tau) := \phi_\sigma^\sigma \phi_\tau \phi_{\sigma\tau}^{-1} \quad \text{for each } \sigma, \tau \text{ in } G_{\mathbb{Q}}.$$

Then the mapping c is a 2-cocycle of $G_{\mathbb{Q}}$ with values in \mathbb{Q}^* . By taking the degree of both sides, we have

$$(3.2) \quad c(\sigma, \tau)^2 = d_\sigma d_\tau d_{\sigma\tau}^{-1} \quad \text{for each } \sigma, \tau \text{ in } G_{\mathbb{Q}}.$$

Proposition 3.1. *The mapping*

$$G_{\mathbb{Q}} \rightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 : \sigma \mapsto d_\sigma$$

is a homomorphism with the kernel G_k .

Proof. It follows from (3.2) that the above mapping is a homomorphism. Since ${}^\sigma j_E = j_{\sigma E}$, we see

$$j_{\sigma E} = j_E \quad \text{if and only if} \quad \sigma \in G_k.$$

Thus we have

$$d_\sigma = 1 \quad \text{if and only if} \quad \sigma \in G_k.$$

□

Proposition 3.2. *k is a polyquadratic field.*

Proof. By Proposition 3.1 we see that σ^2 is in G_k for each σ in $G_{\mathbb{Q}}$. □

3.2. The case of N dividing d_σ for some σ . Let N be a prime number. Let E be a central \mathbb{Q} -curve defined over a polyquadratic field k of degree d with a k -rational N -torsion point Q_1 .

Let $k(\phi_\sigma)$ be the field of definition of ϕ_σ over k , and let $k^{(\sigma)}$ be the fixed subfield of k by σ .

Proposition 3.3. *The extension $k(\phi_\sigma)/k^{(\sigma)}$ is a Galois extension. Furthermore its Galois group is an elementary abelian 2-group of order two or four.*

Proof. Since E is non-CM, the automorphism group

$$\text{Aut Hom}({}^\sigma E, E) = \{\pm 1\}.$$

Since $\text{Hom}({}^\sigma E, E) = \mathbb{Z}\phi_\sigma$, we have an exact sequence

$$1 \rightarrow G_{k(\phi_\sigma)} \rightarrow G_k \rightarrow \text{Aut Hom}({}^\sigma E, E).$$

Thus $G_{k(\phi_\sigma)}$ is a normal subgroup of G_k with the index dividing two.

Similarly we have an exact sequence

$$1 \rightarrow G_{k(\sigma\phi_\sigma)} \rightarrow G_k \rightarrow \text{Aut Hom}(E, {}^\sigma E).$$

Since the transpose mapping

$$\text{Hom}({}^\sigma E, E) \rightarrow \text{Hom}(E, {}^\sigma E) : \psi \mapsto \psi^*$$

is a G_k -module isomorphism, we see

$$G_{k(\phi_\sigma)} = G_{k(\sigma\phi_\sigma)} = \sigma G_{k(\phi_\sigma)} \sigma^{-1}.$$

Since $G_{k^{(\sigma)}}$ is generated by σ and G_k , $G_{k(\phi_\sigma)}$ is a normal subgroup of $G_{k^{(\sigma)}}$.

We may put ${}^\sigma \phi_\sigma = \epsilon \phi_\sigma^*$ for some ϵ in $\{\pm 1\}$. Then we have

$$\sigma^2 \phi_\sigma = \epsilon^\sigma \phi_\sigma^* = \epsilon(\epsilon \phi_\sigma^*)^* = \phi_\sigma.$$

Thus σ^2 is in $G_{k(\phi_\sigma)}$. Thus the order of $G_{k^{(\sigma)}}/G_{k(\phi_\sigma)}$ divides four, and its exponent of is at most two. This completes the proof. □

Let ζ_N be a primitive N -th root of unity. We determine prime divisors of $\#E_{tors}(k)$ which divide d_σ for some σ in $G_{\mathbb{Q}}$.

Proposition 3.4. *If N divides d_σ for some σ in $G_\mathbb{Q}$, then N is either 2 or 3.*

Proof. Firstly we show that ζ_N is in $k(\phi_\sigma)$. If $\ker \phi_\sigma \neq \langle {}^\sigma Q_1 \rangle$, then $E[N] = \langle Q_1 \rangle \oplus \langle \phi_\sigma({}^\sigma Q_1) \rangle$. Thus we see that ζ_N is in $k(\phi_\sigma)$. Suppose that $\ker \phi_\sigma = \langle {}^\sigma Q_1 \rangle$. Since ${}^\sigma Q_1$ is $k(\phi_\sigma)$ -rational, the Weil pairing e on ${}^\sigma E[N]$ induces an exact sequence of $G_{k(\phi_\sigma)}$ -modules

$$1 \rightarrow \langle {}^\sigma Q_1 \rangle \rightarrow {}^\sigma E[N] \xrightarrow{e(\langle {}^\sigma Q_1, * \rangle)} \mu_N \rightarrow 1.$$

Since we have an exact sequence of $G_{k(\phi_\sigma)}$ -modules

$$1 \rightarrow \langle {}^\sigma Q_1 \rangle \rightarrow {}^\sigma E[N] \xrightarrow{\phi_\sigma} \langle Q_1 \rangle \rightarrow 1,$$

we see that μ_N is $G_{k(\phi_\sigma)}$ -isomorphic to $\langle Q_1 \rangle$, which has trivial action. This implies that ζ_N is in $k(\phi_\sigma)$.

Secondly we show that $N = 2, 3$. Since the field $k(\phi_\sigma)$ is at most quadratic extension of the polyquadratic field k , we have $N = 2, 3, 5$. Assume that $N = 5$. Since ζ_5 is not in k , we have $k(\phi_\sigma) = k(\zeta_5)$ and $\sqrt{5} \in k$. Since $k(\phi_\sigma)/k^{(\sigma)}$ is polyquadratic, we have $\sqrt{5} \in k^{(\sigma)}$. We have

$$\#\{\sigma \in G \setminus \{1\} \mid \sqrt{5} \in k^{(\sigma)}\} = \#\{\sigma \in G \setminus \{1\} \mid \sigma(\sqrt{5}) = \sqrt{5}\} = [k : \mathbb{Q}]/2 - 1,$$

where G is the Galois group of k over \mathbb{Q} . By using Proposition 3.1, we have

$$\#\{\sigma \in G \setminus \{1\} \mid 5 \mid d_\sigma\} = [k : \mathbb{Q}]/2.$$

This leads to a contradiction. Thus N is not equal to 5. □

3.3. The field $k(E[N])$ for $N > 3$. Until the end of this subsection, we assume $N > 3$. Then the isogeny ϕ_σ induces the isomorphism from ${}^\sigma E[N]$ to $E[N]$ for each σ in $G_\mathbb{Q}$, since N does not divide d_σ for any σ in $G_\mathbb{Q}$ by Proposition 3.4.

Furthermore, we have $\phi_\sigma \langle {}^\sigma Q_1 \rangle \subset \langle Q_1 \rangle$. Indeed, if $\phi_\sigma \langle {}^\sigma Q_1 \rangle$ is not contained in $\langle Q_1 \rangle$, then $E[N] = \langle Q_1 \rangle \oplus \langle \phi_\sigma({}^\sigma Q_1) \rangle$ and thus ζ_N is in $k(\phi_\sigma)$. This contradicts Proposition 3.4. We define the element a_σ in $(\mathbb{Z}/N\mathbb{Z})^*$ by

$$\phi_\sigma({}^\sigma Q_1) = a_\sigma Q_1.$$

Proposition 3.5. *The congruence $c(\sigma, \tau) \equiv a_\sigma a_\tau a_{\sigma\tau}^{-1} \pmod N$ holds for each σ, τ in $G_\mathbb{Q}$.*

Proof. We have ${}^\sigma \phi_\tau({}^{\sigma\tau} Q_1) = a_\tau {}^\sigma Q_1$ by the definition of a_τ . Thus we have $\phi_\sigma {}^\sigma \phi_\tau({}^{\sigma\tau} Q_1) = a_\tau a_\sigma Q_1$. On the other hand, $c(\sigma, \tau) \phi_{\sigma\tau}({}^{\sigma\tau} Q_1) = c(\sigma, \tau) a_{\sigma\tau} Q_1$. Thus we have the assertion. □

Proposition 3.6. *The 2-cocycle c is symmetric, that is, $c(\sigma, \tau) = c(\tau, \sigma)$ for each σ, τ in $G_\mathbb{Q}$.*

Proof. Since E is non-CM, we have $c(\sigma, \tau) = \pm c(\tau, \sigma)$. By Proposition 3.5 we have $c(\sigma, \tau) \equiv c(\tau, \sigma) \pmod N$. Since N is odd, $c(\sigma, \tau) = c(\tau, \sigma)$. □

Proposition 3.7. *E is completely defined over k , that is, the isogeny ϕ_σ is defined over k for each σ in $G_{\mathbb{Q}}$.*

Proof. Since c is symmetric, we have

$$\phi_1^\tau \phi_\sigma \phi_\sigma^{-1} = c(\tau, \sigma) = c(\sigma, \tau) = \phi_\sigma^\sigma \phi_1 \phi_\sigma^{-1} = \phi_1$$

for τ in G_k . Thus we have ${}^\tau \phi_\sigma = \phi_\sigma$ for τ in G_k . □

By Proposition 3.7, we may consider that c is a 2-cocycle of the Galois group G of k over \mathbb{Q} . Since the 2-cocycle c is symmetric and G is commutative, there exists a mapping β from G to $\overline{\mathbb{Q}}$ such that

$$(3.3) \quad c(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1} \quad \text{for each } \sigma, \tau \text{ in } G$$

(cf. e.g. [7], Theorem 3.2). The splitting map β is uniquely determined up to multiplication by characters of G . Together with (3.2), we see that

$$(3.4) \quad \varepsilon(\sigma) := d_\sigma \beta(\sigma)^{-2}$$

is a character of G . Since G is of exponent less than or equal to two, the character ε does not depend on the choice of β . As below we consider that the splitting mapping β and the character ε are mappings from $G_{\mathbb{Q}}$ through the projection from $G_{\mathbb{Q}}$ to G .

Proposition 3.8. *The character ε is quadratic, and $\phi_\sigma^\sigma \phi_\sigma = \varepsilon(\sigma)d_\sigma$ holds for each σ in $G_{\mathbb{Q}}$.*

Proof. It follows from (3.1) and (3.3) that $c(1, 1) = \phi_1 = \beta(1)$. Since $c(\sigma, \sigma) = \phi_\sigma^\sigma \phi_\sigma \phi_1^{-1} = \beta(\sigma)^2 \beta(1)^{-1}$, it follows from (3.4) that $\phi_\sigma^\sigma \phi_\sigma = \varepsilon(\sigma)^{-1} d_\sigma$. Since E is non-CM, the signature $\varepsilon(\sigma) = \pm 1$, and the assertion follows. □

Proposition 3.9. *The character ε is real, that is, $\varepsilon(\rho) = 1$, where ρ is the complex conjugation.*

Proof. We fix an invariant differential ω_E of E over k . We have $\phi_\rho^* \omega_E = \alpha^\rho \omega_{\rho E}$ for some α in k . Then we have

$$\varepsilon(\rho) d_\rho \omega_E = (\phi_\rho^\rho \phi_\rho)^* \omega_E = \alpha^\rho \alpha \omega_E.$$

It follows from $\alpha^\rho \alpha > 0$ that $\varepsilon(\rho) = 1$. □

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.

Proposition 3.10. *N splits completely in F , that is, the Legendre symbol $(\varepsilon(\sigma)d_\sigma/N)$ is equal to 1 for each σ in $G_{\mathbb{Q}}$.*

Proof. Since σ^2 is in G_k , we have

$$\varepsilon(\sigma)d_\sigma = \phi_\sigma^\sigma \phi_\sigma = c(\sigma, \sigma)\phi_1 = a_\sigma^2 a_1^{-1} a_1 = a_\sigma^2$$

on $\langle Q_1 \rangle$ by using $\phi_1 = c(1, 1) = a_1$. Thus we have $\varepsilon(\sigma)d_\sigma \equiv a_\sigma^2 \pmod{N}$. □

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 $\text{End}_{\mathbb{Q}}^0 A = F$. The abelian variety A is of GL_2 -type with real multiplications if and only if the character ε is trivial.

By the definition of the Weil restriction, $A(\mathbb{Q})$ and $E(k)$ are in bijection. 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 ideal λ in \mathcal{O}_F dividing N such that R_1 is in $A[\lambda]$.

We take R_2 in $A[\lambda]$ such that (R_1, R_2) is a $\mathbb{Z}/N\mathbb{Z}$ -basis of $A[\lambda]$. For the basis (R_1, R_2) the image of the representation of $G_{\mathbb{Q}}$ on $A[\lambda]$ consists of matrices of the form $\begin{bmatrix} 1 & b \\ 0 & \varepsilon\chi \end{bmatrix}$, where χ is the cyclotomic character modulo N . We denote by k_{ε} the fixed subfield of k by the action of the kernel of ε . By Propositions 3.8 and 3.9 k_{ε} is a real field of degree at most two.

The action of $\text{Gal}(k_{\varepsilon}(\zeta_N)/\mathbb{Q})$ on $\text{Gal}(k_{\varepsilon}(A[\lambda])/k_{\varepsilon}(\zeta_N))$ is via $\varepsilon\chi^{-1}$ since

$$\begin{bmatrix} 1 & 0 \\ 0 & \varepsilon(\kappa)\chi(\kappa) \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & \varepsilon(\tau)\chi(\tau) \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & \varepsilon(\kappa)\chi(\kappa) \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \varepsilon(\kappa)\chi^{-1}(\kappa)b \\ 0 & \varepsilon(\tau)\chi(\tau) \end{bmatrix}.$$

Thus $k_{\varepsilon}(A[\lambda])/k_{\varepsilon}(\zeta_N)$ is an $\varepsilon\chi^{-1}$ -extension.

Proposition 3.11. *The equation $k(E[N]) = k(A[N])$ holds.*

Proof. Since ϕ_{σ} induces an isomorphism from ${}^{\sigma}E[N]$ to $E[N]$, we have $k({}^{\sigma}E[N]) = k(E[N])$ for each σ in $G_{\mathbb{Q}}$. Thus $k(E[N]) = k(A[N])$. □

Proposition 3.12. *The equation $k(E[N]) = k(A[\lambda])$ holds.*

Proof. If $\langle R_2 \rangle$ is \mathbb{Q} -rational, then $k_{\varepsilon}(A[\lambda]) = k_{\varepsilon}(\zeta_N)$. Since the group $\langle R_2 \rangle$ determines a k -rational subgroup of $E[N]$ which is not $\langle Q_1 \rangle$, we see that $k(E[N]) = k(\zeta_N) = k(A[\lambda])$. If $\langle R_2 \rangle$ is not \mathbb{Q} -rational, $k_{\varepsilon}(A[\lambda])$ is a cyclic extension of $k_{\varepsilon}(\zeta_N)$ of degree N . Since N is prime to $[k(\zeta_N) : k_{\varepsilon}(\zeta_N)]$, we have $[k(A[\lambda]) : k(\zeta_N)] = N$. Since $k(E[N])$ is a cyclic extension of $k(\zeta_N)$ of degree N containing $k(A[\lambda])$, we have $k(A[\lambda]) = k(E[N])$. □

Proposition 3.13. *If $k(E[N])/k(\zeta_N)$ is unramified and N does not divide the generalized Bernoulli number $B_{2,\varepsilon}$, then $k(E[N]) = k(\zeta_N)$.*

Proof. Since $k(\zeta_N)/k_{\varepsilon}(\zeta_N)$ is polyquadratic and $k(E[N])/k(\zeta_N)$ is unramified, the ramification index of each prime at $k(E[N])/k_{\varepsilon}(\zeta_N)$ is a power of two. Thus $k_{\varepsilon}(A[\lambda])/k_{\varepsilon}(\zeta_N)$ is unramified. By Proposition 7.4 in Appendix 2, there exists no non-trivial unramified $\varepsilon\chi^{-1}$ -extension of $k_{\varepsilon}(\zeta_N)$, which leads to $k_{\varepsilon}(A[\lambda]) = k_{\varepsilon}(\zeta_N)$. Thus $k(E[N]) = k(\zeta_N)$. □

3.4. The reduction type of E modulo \mathfrak{p} . We assume that $N > 3$. We denote the p -factor of the L-series attached to l -adic (resp. λ -adic) representations of $G_{\mathbb{Q}}$ on A by $L_p(A/\mathbb{Q}, u)$ (resp. $L_p(A/\mathbb{Q}, F, u)$). Then $L_p(A/\mathbb{Q}, u)$

(resp. $L_p(A/\mathbb{Q}, F, u)$) is a polynomial with coefficients in \mathbb{Z} (resp. \mathcal{O}_F). We denote the \mathfrak{p} -factor of the L-series attached to l -adic representations of G_k on E by $L_p(E/k, u)$.

Proposition 3.14. *Let \mathfrak{p} be a prime in k . If \mathfrak{p} ramifies in k over \mathbb{Q} , then E has good or additive reduction at \mathfrak{p} .*

Proof. Since A is the Weil restriction of E and it is of GL_2 -type, we have

$$(3.5) \quad N_{F/\mathbb{Q}}L_p(A/\mathbb{Q}, F, u) = L_p(A/\mathbb{Q}, u) = N_{\mathfrak{p}|p}L_p(E/k, u^{f_p}),$$

where f_p is the residue degree for \mathfrak{p} .

Suppose that E has multiplicative reduction at \mathfrak{p} . Since E is a \mathbb{Q} -curve, it follows from (3.5) that

$$N_{F/\mathbb{Q}}(1 - au + \eta pu^2) = (1 - a_p u^{f_p})^{[k:\mathbb{Q}]/e_p f_p}$$

for some a in \mathcal{O}_F , $\eta = 0, 1$ and $a_p = \pm 1$, where e_p is the ramification index for \mathfrak{p} . By comparing the degree of the both sides, we have a contradiction to $e_p \geq 2$. □

Proposition 3.15. *Assume that the residue degree of \mathfrak{p} is two. Then E does not have multiplicative reduction at \mathfrak{p} .*

Proof. Assume that E has multiplicative reduction at \mathfrak{p} . By the assumption it follows from (3.5) that

$$N_{F/\mathbb{Q}}(1 - au) = N_{\mathfrak{p}|p}(1 - a_p u^2)$$

for some a in \mathcal{O}_F and $a_p = \pm 1$. Since the zero of the right hand side is $u = \pm 1$ or $u = \pm\sqrt{-1}$. Thus we have $a = \pm\sqrt{-1}$ and hence $\sqrt{-1}$ is in F .

Since F is generated by $\sqrt{\varepsilon(\sigma)d_\sigma}$ over \mathbb{Q} , there exists σ in $G_{\mathbb{Q}}$ such that $\varepsilon(\sigma)d_\sigma = -1$. Thus we have $d_\sigma = 1$ and $\varepsilon(\sigma) = -1$. By Proposition 3.1, σ is in G_k and thus $\varepsilon(\sigma)$ must be one. This is a contradiction. □

Proposition 3.16. *If E is semistable, k is an unramified extension of k_ε .*

Proof. Let \mathfrak{p} be a prime in k . Assume that \mathfrak{p} ramifies in k over \mathbb{Q} . Since E is semistable, it follows from Proposition 3.14 that \mathfrak{p} is a good prime of E . For each element σ in the inertia group I_p of \mathfrak{p} , the reduction of ϕ_σ modulo \mathfrak{p} is an endomorphism of the reduction of E modulo \mathfrak{p} . It is a complex multiplication, since d_σ is squarefree. Thus for a non-trivial element σ in I_p we have $\varepsilon(\sigma) = -1$. This implies $I_p \cap \ker \varepsilon = \{1\}$ and k is an unramified extension of k_ε . □

4. Proof of Theorem 1.1

Let N be a prime number. Let E be a central \mathbb{Q} -curve over a polyquadratic field k with k -rational N -torsion point Q_1 . Throughout this section we always assume the following:

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

In this section we give a proof of Theorem 1.1 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 4.1. *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 $\text{Spec } \mathcal{O}_{\mathfrak{p}}$. By the universal property of the Néron model 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 this 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 $\text{Spec } \mathbb{Z}$ is equal to 1 or 2. Since $e_{\mathfrak{p}}$ is less than $N - 1$, by Raynaud [21], Corollary 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 [23] 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 semistable 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 isomorphism on generic fibres, using the universal property of the Néron model 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 [21], Corollary 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 4.2. *Assume that p is either 2 or 3. Then \mathfrak{p} is 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 $(1 + p^{f_{\mathfrak{p}}/2})^2 \leq 16$. 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 specializes to $(E/\mathfrak{p})^0$. Over a quadratic extension κ of \mathcal{O}/\mathfrak{p} we have an isomorphism $(E/\kappa)^0 \cong \mathbb{G}_{m/\kappa}$, so that N divides the cardinality of κ^* . Since it follows from $f_{\mathfrak{p}} = 1, 2$ that the cardinality of κ^* is one of $3, 8, 15, 80$, this is impossible by the assumption $N > 13$. \square

The pair $(E, \langle Q_1 \rangle)$ defines a k -rational point on the modular curve $X_0(N)_{\mathbb{Q}}$. Let us call this point x . 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 by $J_0(N)_{/\mathbb{Q}}$ the Jacobian of $X_0(N)_{/\mathbb{Q}}$. The abelian variety $J_0(N)$ is semistable and has good reduction at all primes $p \neq N$ ([2]). 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 4.3. Q_1 does not specialize to $(E/\mathfrak{p})^0$ for any bad prime \mathfrak{p} of E .

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 4.2 we have $\sigma x_{/\mathfrak{p}} = \infty_{/\mathfrak{p}}$ for each σ and \mathfrak{p} dividing 2, so we have

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

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 such that Q_1 specializes to $(E/\mathfrak{p})^0$, then $x_{/\mathfrak{p}} = 0_{/\mathfrak{p}}$. By Proposition 4.2 we may assume that the residue characteristic p is neither 2 nor 3. Since E is a \mathbb{Q} -curve completely defined over k , the types of reduction at $\sigma\mathfrak{p}$ are the same for any σ and thus we have $\sigma x_{/\mathfrak{p}} = 0_{/\mathfrak{p}}$ for each σ . We have

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

Since $h(0 - \infty)$ is a \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 (2). \square

Proposition 4.4. $k(E[N])/k(\zeta_N)$ 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 [23]).

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 $\mathcal{O}_{\mathfrak{p}}$:

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

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

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

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. [5]), and fits into a short exact sequence

$$0 \rightarrow \mathbb{Z}/N\mathbb{Z} \rightarrow E[N] \rightarrow \bar{\mu}_N \rightarrow 0,$$

where $\bar{\mu}_N$ 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 $\bar{\mu}_N$. Thus, $\bar{\mu}_N$ 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 $\mu_N = \bar{\mu}_N$ by Raynaud [21], Corollary 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} . \square

Under the assumption (3), we see that $k(E[N]) = k(\zeta_N)$ by using Propositions 3.13 and 4.4. Since $E[N] = \langle Q_1 \rangle \oplus \langle Q_2 \rangle$, the subgroup $\langle Q_2 \rangle$ is k -rational.

Proposition 4.5. *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 the following diagram is commutative.*

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

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 $\phi_\sigma(\sigma Q_2) \in \langle Q_2 \rangle$. 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 τ 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 a 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 a central \mathbb{Q} -curve. □

Proof of Theorem 1.1. By Proposition 4.5 we get a sequence of central \mathbb{Q} -curves over k

$$E \rightarrow E^{(1)} \rightarrow E^{(2)} \rightarrow E^{(3)} \rightarrow \dots$$

each obtained from the previous one 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 classes of elliptic curves represented. Consequently, for some indices $j > j'$ we must have $E^{(j)} \cong E^{(j')}$. But $E^{(j)}$ maps to $E^{(j')}$ by a nonscalar isogeny. Therefore $E^{(j)}$ is a CM elliptic curve and so is E . This contradicts the assumption that E is non-CM.

Proof of Corollary 1.1. Assume the condition (1) in Theorem 1.1 does not hold, that is, $N > 13$. Since A has real multiplications, the character ε is trivial and thus $k_\varepsilon = \mathbb{Q}$. We recall that the proof of Proposition 4.1 is independent of the conditions (2) and (3). Since E is semistable by Proposition 4.1, we have $k = \mathbb{Q}$ by Proposition 3.16. The conditions (2) and (3) in Theorem 1.1 mean that $N = 5, 13$, or, N divides the second Bernoulli number $B_2 = 1/6$. This leads to a contradiction to $N > 13$.

5. Proof of Theorem 1.2

In this section, we complete the proof of Theorem 1.2. We fix a k -rational N -torsion point Q_1 of E . Let M be the product of all prime divisors of d_σ for all σ . By the assumption of Theorem 1.2 we see that M divides N . Thus, by using Proposition 3.4 we see that M is a divisor of 6. Furthermore, (E, Q_1) is in $X_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}(X_0(M)/W)(\mathbb{Q})$ for some subgroup W of $W(M)$ such that $[k : \mathbb{Q}] = \#W$. We note that the isogenies ϕ_σ correspond bijectively to elements of W . Hence we see that $W = \langle 1 \rangle, \langle W_2 \rangle, \langle W_3 \rangle, \langle W_2, W_3 \rangle$. Namely $[k : \mathbb{Q}] = 1, 2, 4$.

If $[k : \mathbb{Q}] = 1$, then our assertion follows from the result of Mazur [12]. Suppose that $[k : \mathbb{Q}] = 2$. Then $M = 2, 3$ and $N = Mn$ for some squarefree integer n coprime to M . From the result of Kamienny [9] and Kenku-Momose [10], we have $(M, n) = (2, 1), (2, 3), (2, 5), (2, 7), (3, 1), (3, 2)$ such that $Y_1(N)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}(X_0(M)/W)(\mathbb{Q}) \neq \emptyset$. Furthermore, we see that $(M, n) \neq (2, 5)$ by Proposition 3.10 and $\left(\frac{\pm 2}{5}\right) = -1$.

Suppose that $[k : \mathbb{Q}] = 4$. Then $M = 6$ and $N = 6n$, $(6, n) = 1$, n is squarefree. We show $n = 1$.

Assume that $n > 1$. Then we have $N \geq 30$. By Proposition 3.4 we see that ζ_3 is in k , and by Proposition 3.7 E is completely defined over k .

Proposition 5.1. *Assume $N > 9$ and ζ_3 is in k . Then E has additive reduction at the finite places of k lying above (2).*

Proof. We assume E has good reduction at such places. Since $\mathbb{Q}(\sqrt{-3}) \subset k$, the ideal (2) decomposes as \mathfrak{p}^2 or $\mathfrak{p}\mathfrak{p}'$ in k . In either cases, the residue field at \mathfrak{p} is \mathbb{F}_4 . By the Weil bound we have $\sharp E_{\mathfrak{p}}(\mathbb{F}_4) \leq (\sqrt{4} + 1)^2 = 9$. But there exists an inclusion $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E_{tors}(k) \hookrightarrow E_{\mathfrak{p}}(\mathbb{F}_4)$. This is a contradiction. So E has bad reduction at such places. Furthermore by Propositions 3.14 and 3.15 E has additive reduction at such places. \square

Proposition 5.2. *The inequality $p \leq 13$ holds for any prime divisor p of n .*

Proof. If $p > 13$, then E is semistable over k by Proposition 4.1. This contradicts Proposition 5.1. \square

By Proposition 3.10, we have $p \neq 5, 13$, since $\left(\frac{\pm 2}{5}\right) = \left(\frac{\pm 2}{13}\right) = -1$. We also have $p \neq 3, 7$ since $\left(\frac{2}{3}\right) = -1$ and $\left(\frac{-2}{7}\right) = -1$. So we must show $n \neq 11$. For the proof we need the following proposition.

Proposition 5.3 ([4]). *The modular curve $X_0(66)/W_6$ is a hyperelliptic curve with W_{11} as the hyperelliptic involution and an affine model of $X_0(66)/W_6$ is as follows: $y^2 = (z^4 - 7z^3 + 11z^2 - 8z + 4)(z^6 - 9z^5 + 32z^4 - 57z^3 + 56z^2 - 33z + 11)$.*

Assume that $n = 11$. Let \mathfrak{p} be a prime of k lying above (3) and let R be the localization of the integer ring \mathcal{O}_k at \mathfrak{p} . Take $x := (E, Q_1)$ in $X_1(66)(k)$. If the prime ideal (3) is unramified in k , the ramification index $e_3 = 1 < 2 = 3 - 1$. By Raynaud’s theorem (see proposition (1.10) in [10]) and the universal property of the Néron model \mathcal{E}_R of E over R , $(\mathbb{Z}/66\mathbb{Z})_R \subset \mathcal{E}_R$. If the prime ideal (3) ramifies in k , $(\mathbb{Z}/22\mathbb{Z})_R \subset \mathcal{E}_R$. In both cases, \mathcal{E}_R has multiplicative reduction at \mathfrak{p} . Furthermore, $(\mathbb{Z}/11\mathbb{Z})_R \otimes k(\mathfrak{p})$ is not contained in the identity component $\mathcal{E}^0(k(\mathfrak{p}))$, since $\mathcal{E}^0(k(\mathfrak{p})) \simeq \mathbb{Z}/(q - \epsilon)\mathbb{Z}$, where $q := \sharp k(\mathfrak{p}) = 3$, or 9 (recall k is biquadratic !) and $\epsilon = \pm 1$. For each σ in $\text{Gal}(k/\mathbb{Q})$ we also denote by x^σ the image of x^σ under the natural projection from $X_1(66)$ to $X_0(66)$. For any σ in $\text{Gal}(k/\mathbb{Q})$, there exists a rational cusp C_σ represented by $\left(\frac{1}{d}\right)$ with $d|6$ such that $x^\sigma \equiv C_\sigma \pmod{\mathfrak{p}}$. Then the divisor $D := \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})} (x^\sigma - C_\sigma)$ is \mathbb{Q} -rational.

By Proposition 3.7 and the fact that $\sharp(\text{Gal}(k/\mathbb{Q}) \setminus \{1\}) = 3 > 1$, there exists a non-trivial element τ in $\text{Gal}(k/\mathbb{Q})$ such that the isogeny ϕ_τ from ${}^\tau E$ to E is defined over k . Then we have $C_\sigma \equiv C_{\tau\sigma} \pmod{\mathfrak{p}}$ for all σ in

$\text{Gal}(k/\mathbb{Q})$. Put $D' := 2 \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})/\langle \tau \rangle} (x^\sigma - C_\sigma)$. Since $J_0(66)$ is isogenous to a product of elliptic curves of conductors 11, 33 and 66 by Theorem 1 in [25], we see that $J_0(66)(\mathbb{Q})$ is a finite group from Cremona's database [1]. Since $D' \equiv D \equiv 0 \pmod{\mathfrak{p}}$ and $\sharp J_0(66)(\mathbb{Q}) < \infty$, we have $D' \equiv 0$ in $J_0(66)$ by Raynaud's theorem (note that \mathfrak{p} does not divide 2). Denote by ϕ the natural projection from $J_0(66)$ to $\text{Jac}(X_0(66)/W_6)$. Since W_6 acts on the set $A := \{(\frac{1}{d}) \mid d|6\}$, we have $0 = \phi(D') = 2 \left(\sum_{\sigma \in \text{Gal}(k/\mathbb{Q})/\langle \tau \rangle} x^\sigma - C'_\sigma \right)$, where $C'_\sigma := \phi(C_\sigma)$ in A . Since by Proposition 5.3, $\text{Jac}(X_0(66)/W_6)$ has no nontrivial \mathbb{Q} -rational 2-torsion of the form $P + Q - \infty_+ - \infty_-$, where ∞_\pm are the points at infinity, we have

$$D'' := \sum_{\sigma \in \text{Gal}(k/\mathbb{Q})/\langle \tau \rangle} (x^\sigma - C'_\sigma) \equiv 0,$$

on $\text{Jac}(X_0(66)/W_6)$. Then we can see that $D'' = \text{div}\left(\frac{az + b}{cz + d}\right)$ where z is the (local) z -coordinate of $X_0(66)/W_6$ in Proposition 5.3 and $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ in $\text{GL}_2(\mathbb{Q})$. Since W_{11} induces the hyperelliptic involution on $X_0(66)/W_6$, W_{11} have to fix the pole part of D'' . On the other hand, $W_{11}(A) \cap A = \emptyset$. This gives a contradiction.

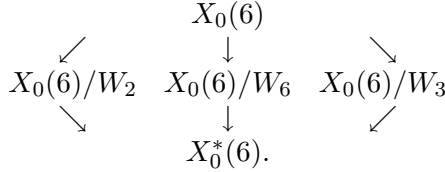
6. Appendix 1

In this appendix, we give an explicit model of the central \mathbb{Q} -curve associated to a non-cuspidal non-CM point of $X_0^*(6)(\mathbb{Q})$ and $X_0(6)/W_i(\mathbb{Q})$ for $i = 2, 3, 6$. A model of elliptic curve with $(0, 0)$ as a 6-torsion point is well known:

$$(6.1) \quad y^2 + (1 - s)xy - (s^2 + s)y = x^3 - (s^2 + s)x^2$$

$$\Delta := s^6(s + 1)^3(9s + 1) \neq 0,$$

where $\mathbb{Q}(X_1(6)) = \mathbb{Q}(X_0(6)) = \mathbb{Q}(s)$ (see [11]). We often regard a point of $X_0(6)$ as that of $X_1(6)$ through the natural isomorphism from $X_1(6)$ to $X_0(6)$. We can take a generator $s = \frac{\eta(\tau)^5\eta(3\tau)}{\eta(2\tau)\eta(6\tau)^5}$ of $\mathbb{Q}(X_0(6))$ where $\eta(\tau)$ is the eta function. Then we have the following commutative diagram where all maps are the natural projections between modular curves over \mathbb{Q} :



It is easy to see that $t_i := s + s|W_i$ is a generator of the function field $\mathbb{Q}(X_0(6)/W_i)$ for $i = 2, 3, 6$ and $t := s + s|W_2 + s|W_3 + s|W_6 = s + \frac{-s-1}{9s+1} + \frac{1}{9s} + \frac{-9s-1}{9(s+1)}$ is a generator of the function field $\mathbb{Q}(X_0^*(6))$. We also have

$$t_3|W_2 = \frac{-10t_3 - 4}{9t_3 + 10}, \quad t_2|W_3 = \frac{-t_2}{t_2 + 1}, \quad t_6|W_2 = \frac{-t_6}{9t_6 + 1}.$$

Let π be the projection from $X_0(6)$ to $X_0^*(6)$. For a general point a in $X_0^*(6)(\mathbb{Q})$, we can easily compute the solution of $\pi(s) = a$. These are the conjugations of $s = (\sqrt{a} + \sqrt{4+a})(3\sqrt{a} + \sqrt{4+9a})/12$. Thus a model of the central \mathbb{Q} -curve corresponding to some non-cuspidal non-CM point of $X_1(6)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}X_0^*(6)(\mathbb{Q})$ for some biquadratic field k is obtained by restricting s in (6.1) as follows:

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

where a is in \mathbb{Q} such that $\Delta \neq 0$ and $k = \mathbb{Q}(s)$ is a biquadratic field (cf. [20]). Since $t_2 + t_2|[W_3] = t_3 + t_3|[W_2] = t_6 + t_6|[W_2] = \pi(s) = a$, we also obtain models of \mathbb{Q} -curves corresponding to some non-cuspidal non-CM points of $X_1(6)(k) \times_{X_0(1)(\overline{\mathbb{Q}})} \pi^{-1}(X_0(M)/W_M)(\mathbb{Q})$ for $M = 2, 3, 6$ and for some quadratic field k . These models are obtained by restricting s in (6.1) as follows:

$$\begin{aligned}
 \text{if } M = 2, \quad s &= \frac{-3t_2 - \sqrt{9t_2^2 + 4t_2 + 4}}{6(t_2 + 1)} ; \\
 \text{if } M = 3, \quad s &= \frac{-1}{12(9t_3 + 10)}(6 + 3t_3 + \sqrt{9t_3^2 - 4})(2 + 9t_3 + \sqrt{9t_3^2 - 4}) ; \\
 \text{if } M = 6, \quad s &= \frac{1}{6}(3t_6 + \sqrt{9t_6^2 + 36t_6 + 4}) ;
 \end{aligned}$$

where t_2, t_3, t_6 is in \mathbb{Q} such that $\Delta \neq 0$ and $k = \mathbb{Q}(s)$ is a quadratic field.

7. Appendix 2

In this appendix we modify the Herbrand theorem. The general reference is Washington [26]. Let ε be a quadratic character of $G_{\mathbb{Q}}$ and let k_{ε} be its fixed field. Let N be an odd prime number and let ζ_N be the primitive N -th root of unity. Put $M := k_{\varepsilon}(\zeta_N)$. We take the minimal positive integer m such that $M \subset \mathbb{Q}(\zeta_m)$. Then m is equal to the conductor of $\varepsilon\chi^{-1}$, where χ is the N -th cyclotomic character of $G_{\mathbb{Q}}$.

$H := \text{Gal}(M/\mathbb{Q})$ may be regarded as a quotient of $(\mathbb{Z}/m\mathbb{Z})^*$. We define the Stickelberger element θ by

$$\theta := \sum_{\substack{1 \leq a \leq m \\ (a,m)=1}} \left\{ \frac{a}{m} \right\} \sigma_a^{-1} \in \mathbb{Q}[H],$$

where $\{x\}$ denote the fractional part of the real number x . We define the Stickelberger ideal I by $\mathbb{Z}[H] \cap \theta\mathbb{Z}[H]$.

Proposition 7.1 (Stickelberger’s Theorem). *The Stickelberger ideal annihilates the ideal class group Cl_M of M .*

Let I' be the ideal of $\mathbb{Z}[H]$ generated by elements of the form $c - \sigma_c$, with $(c, m) = 1$. Since

$$(c - \sigma_c)\theta = \sum_a \left(c \left\{ \frac{a}{m} \right\} - \left\{ \frac{ac}{m} \right\} \right) \sigma_a^{-1} \in \mathbb{Z}[H],$$

we have $I'\theta \subset I$.

Let N be a prime number. Let $Cl_M[N]$ be the N -primary subgroup of Cl_M . Then $Cl_M[N]$ is an H -vector space over \mathbb{F}_N .

Since $\#H$ divides $2(N - 1)$, N does not divide $\#H$. Put

$$e_{\varepsilon\chi^{-1}} := \frac{1}{\#H} \sum_{\sigma \in H} \varepsilon(\sigma)\chi^{-1}(\sigma)\sigma^{-1} \in \mathbb{F}_N[H].$$

Then

$$Cl_M[N]^{\varepsilon\chi^{-1}} = e_{\varepsilon\chi^{-1}} Cl_M[N]$$

and

$$e_{\varepsilon\chi^{-1}}(c - \sigma_c)\theta = (c - \varepsilon(\sigma_c)\chi^{-1}(\sigma_c))B_{1,\varepsilon\chi}e_{\varepsilon\chi^{-1}}.$$

Since there exists c such that $\varepsilon(\sigma_c)\chi(\sigma_c) \neq c$, $B_{1,\varepsilon\chi^{-1}}$ annihilates $Cl_M[N]^{\varepsilon\chi^{-1}}$.

Proposition 7.2. *If $Cl_M[N]^{\varepsilon\chi^{-1}}$ is non-trivial, then N divides $B_{1,\varepsilon\chi}$.*

Proposition 7.3. *Assume that $\varepsilon\chi^2 \neq 1$. Then the congruence*

$$B_{1,\varepsilon\chi} \equiv \frac{B_{2,\varepsilon}}{2} \pmod{N}$$

holds.

Proof. By the definition of the p -adic L-function $L_p(s, \varepsilon\chi^2)$ (cf. e.g. [26], Theorem 5.11),

$$L_p(0, \varepsilon\chi^2) = -(1 - \varepsilon\chi(N)) \frac{B_{1, \varepsilon\chi}}{1} = -B_{1, \varepsilon\chi}$$

because of $\varepsilon\chi(N) = 0$. Since the odd part of the conductor of ε is squarefree, N^2 does not divide the conductor of $\varepsilon\chi^2$. Since $\varepsilon\chi^2 \neq 1$, we have

$$L_p(0, \varepsilon\chi^2) = L_p(-1, \varepsilon\chi^2) \pmod{N}$$

and both numbers are N -integral. (cf. e.g. [26], Corollary. 5.13). By the definition of the p -adic L-function $L_p(s, \varepsilon\chi^2)$ we have

$$L_p(-1, \varepsilon\chi^2) = -(1 - \varepsilon(N)N) \frac{B_{2, \varepsilon}}{2} \equiv -\frac{B_{2, \varepsilon}}{2} \pmod{N}$$

since $L_p(-1, \varepsilon\chi^2)$ is N -integral. Thus we have

$$B_{1, \varepsilon\chi} \equiv \frac{B_{2, \varepsilon}}{2} \pmod{N}.$$

□

By Propositions 7.2 and 7.3, the next proposition follows from class field theory.

Proposition 7.4. *If $k_\varepsilon(\zeta_N)$ has a non-trivial unramified $\varepsilon\chi^{-1}$ -extension over \mathbb{Q} , then N divides $B_{2, \varepsilon}$.*

Proof. If $\varepsilon\chi^2 \neq 1$, then the assertion follows from Propositions 7.2 and 7.3. Suppose that $\varepsilon\chi^2 = 1$. Then ε is trivial and $N = 3$, or ε is quadratic and $N = 5$. In any case we have $k_\varepsilon(\zeta_N) = \mathbb{Q}(\zeta_N)$, and its class number is one. Thus $k_\varepsilon(\zeta_N)$ does not have a non-trivial unramified $\varepsilon\chi^{-1}$ -extension over \mathbb{Q} . □

References

- [1] J. CREMONA, *Algorithms for modular elliptic curves*. Cambridge: Cambridge University Press, 1992.
- [2] P. DELIGNE, M. RAPOPORT, *Schémas de modules de courbes elliptiques*. Lecture Notes in Math. **349**, Springer, Berlin-Heidelberg-New York, 1973.
- [3] N.D. ELKIES, *On elliptic K-curves*. In *Modular curves and abelian varieties*, Birkhäuser, 2004.
- [4] M. FURUMOTO, Y. HASEGAWA, *Hyperelliptic quotients of modular curves $X_0(N)$* . Tokyo J. Math. **22** (1999), 105–125.
- [5] A. GROTHENDIECK, *Groupes de monodromie en géométrie algébrique*. In *Séminaire de Géométrie Algébrique*, Springer, 1972/3.
- [6] Y. HASEGAWA, *\mathbb{Q} -curves over quadratic fields*. Manuscripta Math. **94** (1997), 347–364.
- [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, 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. **33** (1976), 193–237.
- [12] B. MAZUR, *Rational points on modular curves*. In Modular functions of one variable V, 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] K. MURTY, *The addition law on hyperelliptic Jacobians*. Currents trends in number theory (Allahabad, 2000), 101–110, Hindustan Book Agency, New Delhi, 2002.
- [17] J. OESTERLÉ, *Torsion des courbes elliptiques sur les corps de nombres*, preprint.
- [18] P. PARENT, *Borne effective pour la torsion des courbes elliptiques sur les corps de nombres*. J. Reine Angew Math. **503** (1999), 129–160.
- [19] E.E. PYLE, *Abelian varieties over \mathbb{Q} with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$* . In Modular curves and abelian varieties, Birkhäuser, 2004.
- [20] J. QUER, *\mathbb{Q} -curves and abelian varieties of GL_2 -type*. Proc. London Math. Soc. **81** (2000), 285–317.
- [21] M. RAYNAUD, *Schémas en groupes de type (p, \dots, p)* . Bull. Soc Math. Fr. **102** (1974), 241–280.
- [22] K. RIBET, *A modular construction of unramified p -extension of $\mathbb{Q}(\mu_p)$* . Invent. Math. **34** (1976), 151–162.
- [23] J.-P. SERRE, J. TATE, *Good reduction of abelian varieties*. Ann. Math. **88** (1968), 492–517.
- [24] J. TATE, *Algorithm for determining the type of a singular fibre in an elliptic pencil*. In Modular Function of One Variable IV, Springer-Verlag, 1975.
- [25] T. YAMAUCHI, *On \mathbb{Q} -simple factors of Jacobian varieties of modular curves*. Yokohama Math. J. **53** (2007), no. 2, 149–160.
- [26] L.C. WASHINGTON, *Introduction to cyclotomic fields*. Springer-Verlag New-York, 1997.

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

Takuya YAMAUCHI
Faculty of Liberal Arts and Sciences,
Osaka Prefecture University,
1-1 Gakuen-cho, Nakaku, Sakai, Osaka
599-8531, Japan
E-mail: yamauchi@las.osakafu-u.ac.jp