Journal of Number Theory 183 (2018) 291–308

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the cyclic torsion of elliptic curves over cubic number fields

Jian Wang [1]

Department of Mathematics, University of Southern California, Los Angeles, CA 90089, USA

ARTICLE INFO

Article history:
Received 21 April 2017
Accepted 1 August 2017
Available online 30 August 2017
Communicated by S.J. Miller

MSC:
11G05
11G18

Keywords:
Torsion subgroup
Elliptic curves
Modular curves

ABSTRACT

Let E be an elliptic curve defined over a number field K. Then its Mordell–Weil group $E(K)$ is finitely generated: $E(K) \cong E(K)_{tor} \times \mathbb{Z}^r$. In this paper, we discuss the cyclic torsion subgroup of elliptic curves over cubic number fields. For $N = 169, 143, 91, 65, 77$ or 55, we show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$ for any elliptic curve E over a cubic number field K.

1. Introduction

Let E be an elliptic curve defined over a number field K. Then its Mordell–Weil group $E(K)$ is finitely generated:

$$E(K) \cong E(K)_{tor} \times \mathbb{Z}^r$$

E-mail address: blandye@gmail.com.

[1] Current address: Department of Mathematical Sciences, Tsinghua University, Beijing, 100084, China.

http://dx.doi.org/10.1016/j.jnt.2017.08.001

For a fixed elliptic E over a field K, the torsion component $E(K)_{tor}$ can be calculated due to the Nagell–Lutz–Cassels theorem [3]. However, if we consider a class of elliptic curves, it is usually difficult to list exactly all the possible group structures of $E(K)_{tor}$. The following problem is one of this kind.

Problem 1.1. For an integer $d \geq 1$, what are the possible group structures of $E(K)_{tor}$ with $[K : \mathbb{Q}] = d$?

For $d = 1$, i.e. $K = \mathbb{Q}$, by the work of Kubert [20] and Mazur [23], the torsion group $E(\mathbb{Q})_{tor}$ of an elliptic curve E over the rational number field is isomorphic to one of the following:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && m = 1 - 10, 12; \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, && m = 1 - 4. \end{aligned}$$

For $d = 2$, by the work of Kenku–Momose [18] and Kamienny [14], the torsion group $E(K)_{tor}$ of an elliptic curve over a quadratic number field is isomorphic to one of the following:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && m = 1 - 16, 18; \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, && m = 1 - 6; \\ &\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}, && m = 1 - 2; \\ &\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

For $d = 3$, Parent [33,34] showed that the prime divisors of the order of $E(K)_{tor}$ are ≤ 13. Jeon–Kim–Schweizer [13] determined all the torsion structures that appear infinitely often when we run through all elliptic curves over all cubic fields:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && m = 1 - 16, 18, 20; \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, && m = 1 - 7. \end{aligned}$$

Najman [27] discovered a *sporadic* elliptic curve over a cubic field with torsion group isomorphic to $\mathbb{Z}/21\mathbb{Z}$. In view of these facts, our ultimate aim is to show that the torsion group $E(K)_{tor}$ of an elliptic curve E over a cubic number field is isomorphic to one of the following:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && m = 1 - 16, 18, 20 - 21; \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, && m = 1 - 7. \end{aligned}$$

For the cyclic case, it suffices to show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$ for any elliptic curve E over a cubic number field K when N is among the following list

$$N = 169, 121, 49, 25, 27, 32;$$

$$N = 143, 91, 65, 39, 26, 77, 55, 33, 22, 35, 63, 42, 28, 45, 30, 40, 36, 24.$$

The main result of this paper is the following:

Theorem 1.2. *If $N = 169, 143, 91, 65, 77$ or 55, then $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$ for any elliptic curve E over a cubic number field K.*

2. Preliminaries

Let $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im} z > 0\}$ be the upper half plane. Let $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the extended upper half plane by adjoining cusps $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$ to $\mathbb{H}$. Let N be a positive integer. Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})/(\pm 1) | c \equiv 0 \mod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) | a \equiv d \equiv 1 \mod N \right\}$$

be the congruence subgroups and let $X_1(N)$ (resp. $X_0(N)$) be the modular curve which corresponds to the modular group $\Gamma_1(N)$ (resp. $\Gamma_0(N)$). We denote by $Y_1(N) = X_1(N)\backslash\{cusps\}$, $Y_0(N) = X_0(N)\backslash\{cusps\}$ the corresponding affine curves. Denote by $J_1(N)$ (respectively, $J_0(N)$) the jacobian of $X_1(N)$ (respectively, $X_0(N)$).

For a modular curve X, let $X^{(d)}$ be the d-th symmetric power of X, i.e. the quotient space of the d-fold product X^d by the action of the symmetric group S_d permuting the factors. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$. Then $X^{(d)}(\overline{\mathbb{Q}})$, the set of algebraic points of $X^{(d)}$, corresponds one-to-one to the set $\{P_1 + \cdots + P_d; P_i \in X(\overline{\mathbb{Q}})\}$ of positive $\overline{\mathbb{Q}}$-rational divisors of degree d of X.

Let K be a number field of degree d over $\mathbb{Q}$. Let $x \in X(K)$. Let $x_1, \cdots, x_d$ be the images of x under the distinct embeddings $\tau_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq d$. We may view $x_1 + \cdots + x_d$ is a $\mathbb{Q}$-rational point of $X^{(d)}$. Define

$$\Phi : X^{(d)} \longrightarrow J_X$$

by $\Phi(P_1 + \cdots + P_d) = [P_1 + \cdots + P_d - d\infty]$ where J_X is the jacobian of X, and $[\ ]$ denotes the divisor class.

For a modular curve X over $\mathbb{C}$, X is called d-gonal if there exists a finite $\mathbb{C}$-morphism $\pi : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ of degree d. The minimum d is called the *gonality* of X, which we denote as $\mathrm{Gon}(X)$. The following lemma is a generalization of proposition 1(i) in Frey [8].

Lemma 2.1 *(Frey). Assume that $Gon(X) > d$. Then Φ is injective.*

Proof. Suppose otherwise Φ is not injective, i.e. there exist different $P_1 + \cdots + P_d$ and $Q_1 + \cdots + Q_d$ in $X^{(d)}$ such that $\Phi(P_1 + \cdots + P_d) = \Phi(Q_1 + \cdots + Q_d)$, then

$$[P_1 + \cdots + P_d - d\infty] = [Q_1 + \cdots + Q_d - d\infty] \in J_X$$

then there is a nonconstant function $f \in \mathbb{C}(X)^*$ such that

$$\begin{aligned}\operatorname{div}(f) &= (P_1 + \cdots + P_d - d\infty) - (Q_1 + \cdots + Q_d - d\infty)\\ &= P_1 + \cdots + P_d - Q_1 - \cdots - Q_d\end{aligned}$$

which means f has a pole divisor of degree $\leq d$. Consider the map $\pi : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ defined by $P \longmapsto [f(P), 1]$. Then the degree of π is equal to the degree of pole divisor of f. This contradicts the assumption $\operatorname{Gon}(X) > d$. □

We are interested in the gonality of the modular curve $X_0(N)$ over $\mathbb{C}$. Since the 1-gonal curves are precisely the curves of genus 0, then $X_0(N)$ is 1-gonal if and only if N is among the fifteen values $N = 1 - 10, 12, 13, 16, 18, 25$ with genus 0. The complete list of 2-gonal $X_0(N)$ was determined by Ogg [30], and that of 3-gonal ones by Hasegawa–Shimura [11].

Proposition 2.2 *(Ogg). The modular curve $X_0(N)$ is 2-gonal if and only if N is one of the following:*

$$\begin{aligned}
&N = 1 - 10, 12, 13, 16, 18, 25 && (g = 0);\\
&N = 11, 14, 15, 17, 19 - 21, 24, 27, 32, 36, 49 && (g = 1);\\
&N = 22, 23, 26, 28, 29, 31, 37, 50 && (g = 2);\\
&N = 30, 33, 35, 39, 40, 41, 48 && (g = 3);\\
&N = 47 && (g = 4);\\
&N = 46, 59 && (g = 5);\\
&N = 71 && (g = 6).
\end{aligned}$$

Proposition 2.3 *(Hasegawa–Shimura). The modular curve $X_0(N)$ is 3-gonal if and only if N is one of the following:*

$$\begin{aligned}
&N = 1 - 10, 12, 13, 16, 18, 25 && (g = 0);\\
&N = 11, 14, 15, 17, 19 - 21, 24, 27, 32, 36, 49 && (g = 1);\\
&N = 22, 23, 26, 28, 29, 31, 37, 50 && (g = 2);\\
&N = 34, 43, 45, 64 && (g = 3);\\
&N = 38, 44, 53, 54, 61, 81 && (g = 4).
\end{aligned}$$

The moduli interpretation of a noncuspidal point of $X_1(N)$ is $(E, \pm P)$, where E is an elliptic curve and $P \in E$ is a point of order N. The moduli interpretation of a noncuspidal point of $X_0(N)$ is (E, C), where E is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N. The map $\pi : X_1(N) \longrightarrow X_0(N)$ sends $(E, \pm P)$ to $(E, \langle P \rangle)$, where $\langle P \rangle$ is the cyclic subgroup generated by P.

Let p be a prime such that $p \nmid N$. Igusa's theorem [12] says that the modular curves $X_1(N)$ and $X_0(N)$ have good reduction at prime p. Moreover, reducing the modular curve is compatible with reducing the moduli interpretation (see for example [31, Theorem 1]). And the description of the cusps is the same in characteristic p as in characteristic 0.

Let $k = \mathbb{F}_q$ be the finite field with $q = p^n$ elements. Let E/k be an elliptic curve over k. Let $|E(k)|$ be the number of points of E over k. Then Hasse's theorem states that

$$||E(k)| - q - 1| \leq 2\sqrt{q}$$

i.e.

$$(1 - \sqrt{p^n})^2 \leq |E(k)| \leq (1 + \sqrt{p^n})^2$$

The description of the reduction types of elliptic curves in terms of the language of Néron models can be summarized as the Kodaira–Néron theorem [19], [28]. A complete proof of this theorem can be found in [36, IV §8 §9].

Theorem 2.4 *(Kodaira–Néron). Let R be a Dedekind domain with field of fractions K, let $\mathcal{E}$ be a Néron model over R for an elliptic curve E/K, and let $\wp \subset R$ be any nonzero prime ideal with residue field k. Let $\widetilde{E}$ be the fiber over k of $\mathcal{E}$.*

(1): If E has good reduction at $\wp$, then $\widetilde{E}(k) = \widetilde{E}(k)^0$ is an elliptic curve, where $\widetilde{E}(k)^0$ denotes the connected component of the identity.
(2): If E has additive reduction at $\wp$, then $\widetilde{E}(k)^0 \cong \mathbb{G}_{a/k}$, and $\widetilde{E}(k)/\widetilde{E}(k)^0 = G$ is a finite group of order at most four.
(3): If E has multiplicative reduction at $\wp$, then there exists an extension $\mathscr{K}$ of k of degree at most two so that $\widetilde{E}(\mathscr{K})^0 \cong \mathbb{G}_{m/\mathscr{K}}$ and $\widetilde{E}(\mathscr{K})/\widetilde{E}(\mathscr{K})^0 \cong \mathbb{Z}/n\mathbb{Z}$ for some positive integer n.

Let K be a number field with ring of integers $\mathcal{O}_K$, $\wp \subset \mathcal{O}_K$ a prime ideal lying above p, $k = \mathbb{F}_q = \mathcal{O}_K/\wp$ its residue field. Let E be an elliptic curve over K and $P \in E(K)$ a point of order N. Let $\widetilde{E}$ be the fiber over k of the Néron model of E, and let $\widetilde{P} \in \widetilde{E}(k)$ be the reduction of P. Suppose that $p \nmid N$. Then elementary theory of group schemes shows that $\widetilde{P}$ has order N due to the following well-known result (see for example [2, §7.3 Proposition 3]).

Proposition 2.5. *Let m be a positive integer relatively prime to char(k). Then the reduction map*

$$E(K)[m] \longrightarrow \widetilde{E}(k)$$

is injective.

The Néron–Kodaira theorem leads to Deligne–Rapoport's treatment of modular curves as moduli scheme of generalized elliptic curves [5]. Katz–Mazur [17] developed the theory of Drinfeld level structures on elliptic curves. Conrad [4] improved this theory by extending it on to generalized elliptic curves. We explain here the notions and results in these theories that are necessary in Section 3.

Let $n \geq 1$ be an integer and let k be a field. The *Néron n-gon* over k, denoted C_n, is the quotient of $(\mathbb{P}^1)_k \times \mathbb{Z}/n\mathbb{Z}$ where (∞, i) is identified with $(0, i+1)$. It has n irreducible components $(\mathbb{P}^1)_k \times d$, $d \in \mathbb{Z}/n\mathbb{Z}$, of which $(\mathbb{P}^1)_k \times 0$ is called the identity component. The smooth locus $C_n^{sm} = \mathbb{G}_m \times \mathbb{Z}/n\mathbb{Z}$ of C_n is a group. Furthermore, the action of C_n^{sm} on itself extends to an action of C_n^{sm} on all of C_n: the $\mathbb{G}_m$ part fixes the singular points. The N-torsion part $C_n^{sm}[n]$ has order n^2. In fact, there is a natural short exact sequence

$$0 \longrightarrow \mu_n \longrightarrow C_n^{sm}[n] \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

where the μ_n sits in the identity component of C_n^{sm}.

A *generalized elliptic curve* over a base scheme S is a tuple $(E, +, e)$, where E/S is a proper flat curve, $e \in E(S)$, and $+$ is a map $E^{sm} \times E \longrightarrow E$ such that: (1) $+$ (with e) gives E^{sm} the structure of a group and defines an action on E; (2) the geometric fibers of E are elliptic curves or Néron n-gons.

Denote $S = \operatorname{Spec} \mathbb{Z}$. For $N \geq 5$, $X_1(N)_{/S}$ is the fine moduli scheme which classify the generalized elliptic curves E with a torsion point P of order N; $X_0(N)_{/S}$ is the coarse moduli scheme which classify the generalized elliptic curves E with a cyclic subgroup C of order N. There is a natural morphism $X_1(N)_{/S} \longrightarrow X_0(N)_{/S} : (E, \pm P) \longmapsto (E, \langle P \rangle)$, where $\langle P \rangle$ is the cyclic subgroup generated by P.

Now we can describe the moduli interpretation of the cusps on the generic fiber $X_1(N)$ (resp. $X_0(N)$) of $X_1(N)_{/S}$ (resp. $X_0(N)_{/S}$). The moduli interpretation of cusps of $X_1(N)$ is that for each $d \mid N$, one has cusps $(C_d, (\zeta_N^r, b))$ where $b \in (\mathbb{Z}/d\mathbb{Z})^\times$ and $r \in \mathbb{Z}/N\mathbb{Z}$ maps to a unit in $\mathbb{Z}/(N/d)\mathbb{Z}$. It is easy to see (ζ_N^r, b) is a point of order N in the smooth locus $C_d^{sm} = \mathbb{G}_m \times \mathbb{Z}/d\mathbb{Z}$. The moduli interpretation of cusps of $X_0(N)$ is that for each $d \mid N$, one has cusps (C_d, G), where G is a cyclic subgroup of order N in the smooth locus $C_d^{sm} = \mathbb{G}_m \times \mathbb{Z}/d\mathbb{Z}$ that meets all the irreducible components. Especially for $d = 1$ and $d = N$, we have the cusps (C_1, μ_N) and $(C_N, \mathbb{Z}/N\mathbb{Z})$, which we denote as 0 and ∞ respectively. Note that 0 is distinguished from ∞ by the fact that μ_N lives in the identity component.

In the following section, we use a specialization lemma in Appendix of Katz [16] and a theorem of Manin [21] and Drinfeld [7].

Lemma 2.6 *(Specialization lemma). Let K be a number field. Let $\wp \subset \mathcal{O}_K$ be a prime above p. Let A/K be an abelian variety. Suppose the ramification index $e_\wp(K/\mathbb{Q}) < p-1$. Then the reduction map*

$$\Psi : A(K)_{tor} \longrightarrow A(\overline{\mathbb{F}}_p)$$

is injective.

Theorem 2.7 *(Manin–Drinfeld). Let $C \subset SL_2(\mathbb{Z})/(\pm 1)$ be a congruence subgroup. $x, y \in \mathbb{P}^1(\mathbb{Q})$ and $\overline{x}, \overline{y}$ are the images of x and y respectively, on $\overline{\mathbb{H}}/C$. Then the class of divisors $(\overline{x}) - (\overline{y})$ on curve $\overline{\mathbb{H}}/C$ has finite order.*

3. Method

When N is a rational prime number, Kamienny [15] established a criterion for the nonexistence of elliptic curves E with a point of order N over a number field of degree d. This criterion is refined by Merel [26] in which the Eisenstein quotient is replaced by the winding quotient and the linear independence condition of weight-two cusp forms is replaced by the linear independence of the Hecke operators on the winding element. This type of Kamienny's criterion for the general N is proved by Parent [32]. (In Parent's paper, he assumed N to be a prime power for practical reason. But as he mentioned on page 86, Théorème 1.7 and the Kamienny's criterion Théorème 1.8 are also true by taking directly at any positive integer level N.) Before giving this criterion, we have to explain the necessary knowledge.

Considering the first absolute singular homology group $H_1(X_0(N);\mathbb{Z})$ and the homology group relative to the cusps $H_1(X_0(N), cusps; \mathbb{Z})$ of $X_0(N)$, the first being seen as a subgroup of the second. For $(\alpha, \beta) \in \mathbb{P}^1(\mathbb{Q})^2$, the *modular symbol* $\{\alpha, \beta\}$ is the element of $H_1(X_0(N), cusps; \mathbb{Z})$ defined by the image in $X_0(N)$ of geodesic path of $\mathbb{H}$ connecting α to β in $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$. When $\Gamma_0(N)\alpha = \Gamma_0(N)\beta$, we have $\{\alpha, \beta\} \in H_1(X_0(N);\mathbb{Z})$. Integration defines a classical isomorphism of real vector spaces:

$$H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{R} \longrightarrow \mathrm{Hom}_{\mathbb{C}}(H^0(X_0(N);\Omega^1), \mathbb{C})$$
$$\gamma \otimes 1 \longmapsto (\omega \longmapsto \int_\gamma \omega)$$

The following lemma is a generalization of Lemma 18.6 in Mazur [23].

Lemma 3.1. *The inverse image e of the linear form*

$$\omega \longmapsto \int_{\{0,\infty\}} \omega$$

in $H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{R}$ is actually in $H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{Q}$.

Proof. Consider the exact sequence of topological groups:

$$\begin{tikzcd} 0 \arrow[r] & H_1(X_0(N);\mathbb{Z}) \arrow[r] & U \arrow[r, "\pi"] & J_0(N) \arrow[r] & 0 \end{tikzcd}$$

where U is the universal covering group of the jacobian $J_0(N)$ of $X_0(N)$. As a real Lie group, U is isomorphic to $H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{R}$ and $J_0(N)$ is canonically isomorphic to $H_1(X_0(N);\mathbb{Z}) \otimes (\mathbb{R}/\mathbb{Z})$. From the definition, it is clear that $\pi(e) = c = ((0) - (\infty))$ in $J_0(N)$. By Theorem 2.7, c has finite order, i.e. there is $n \in \mathbb{Z}_{\geq 0}$ such that $n \cdot c = 0$. It follows that $n \cdot e \in H_1(X_0(N);\mathbb{Z})$. So $e \in (1/n)H_1(X_0(N);\mathbb{Z}) \subset H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{Q}$. □

This element e in Lemma 3.1 was first defined by Mazur [23] as the *winding element.* Denote $\mathbb{T}$ the algebra generated over $\mathbb{Z}$ by the Hecke operators T_i ($i \geq 1$, integer), acting faithfully on $H_1(X_0(N);\mathbb{Z}) \otimes \mathbb{Q}$ and on the jacobian $J_0(N)$ of the modular curve. Let $\mathscr{A}_e$ be the annihilator ideal of e in $\mathbb{T}$; we then define the *winding quotient* J_0^e as the quotient abelian variety $J_0(N)/\mathscr{A}_e J_0(N)$. Parent [32, Theorem 1.7] showed that $J_0^e(\mathbb{Q})$ is finite.

The notion of *formal immersion* was introduced by Mazur [24] to indicate the morphism that satisfies the equivalent conditions of EGA IV Proposition 17.4.4 from [10]. If $f : X \longrightarrow Y$ is a morphism of finite type between Noetherian schemes, we shall say that f is a *formal immersion* at a point x if the induced map on the completions of local rings $\widehat{f^\sharp} : \widehat{\mathcal{O}}_{Y,f(x)} \longrightarrow \widehat{\mathcal{O}}_{X,x}$ is surjective.

The following Lemma was known for experts but used without proof. Parent [32] referred it to an unpublished paper of Oesterlé [29]. Arnold sketched a proof in a note [1]. For the sake of completeness, we write down his proof with more detailed clarification.

Lemma 3.2. *Suppose that X is separated and that $f : X \longrightarrow Y$ is a formal immersion at $x \in X$. Suppose that there is an integral Noetherian scheme T and two T-valued points $p_1, p_2 \in X(T)$ such that for some point $t \in T$ we have $x = p_1(t) = p_2(t)$. If moreover $f \circ p_1 = f \circ p_2$, then $p_1 = p_2$.*

Proof. The subscheme $A = \{s \in T \mid p_1(s) = p_2(s)\} \subseteq T$ is closed since X is separated. This is because in the following diagram i is a base change of Δ. So i is a closed immersion since Δ is a closed immersion and the property of closed immersion is stable under base change.

$$\begin{tikzcd} A = X \times_{X \times X} T \arrow[r, "i"] \arrow[d] & T \arrow[d, "p_1 \times p_2"] \\ X \arrow[r, "\Delta"] & X \times X \end{tikzcd}$$

We consider the canonical morphisms [9, EGA I, §2.4]

$$\phi_{T,t} : \mathrm{Spec}\mathcal{O}_{T,t} \longrightarrow T, \qquad \phi_{X,x} : \mathrm{Spec}\mathcal{O}_{X,x} \longrightarrow X.$$

By [9, EGA I, Proposition 2.4.2], they are monomorphisms of ringed spaces. The image of $\phi_{T,t}$ (resp. $\phi_{X,x}$) is exactly the set of all those generic points of the closed irreducible subschemes of T (resp. X) passing through t (resp. x).

Since T is integral, then $T = \overline{(0)}$, where (0) is the unique generic point of T. So we will have an inclusion sequence

$$\overline{(0)} \subseteq \overline{\mathrm{Spec}\mathcal{O}_{T,t}} \subseteq A \subseteq T = \overline{(0)}$$

if we can show that $\mathrm{Spec}\mathcal{O}_{T,t} \longrightarrow T$ factors through A. Hence we can assume that T is local with closed point t. The maps $p_i : T \longrightarrow X$ then factor (uniquely) through $\mathrm{Spec}\mathcal{O}_{X,x} \longrightarrow X$, so we may assume that X is local with closed point x. Now we have the following commutative diagram

$$\begin{tikzcd}
& \mathrm{Spec}\mathcal{O}_{T,t} \arrow[r, shift left, "p_1"] \arrow[r, shift right, "p_2"'] \arrow[d, "\phi_{T,t}"'] & \mathrm{Spec}\mathcal{O}_{X,x} \arrow[d, "\phi_{X,x}"] \\
A \arrow[r, "i"] & T \arrow[r, shift left, "p_1"] \arrow[r, shift right, "p_2"'] & X
\end{tikzcd}$$

In order to show that $p_1 = p_2 : T \rightrightarrows X$, it suffices to show that $p_1 = p_2 : \mathrm{Spec}\mathcal{O}_{T,t} \rightrightarrows \mathrm{Spec}\mathcal{O}_{X,x}$. This is equivalent to show that $p_1^\sharp = p_2^\sharp : \mathcal{O}_{X,x} \rightrightarrows \mathcal{O}_{T,t}$. Consider the commutative diagram

$$\begin{tikzcd}
\widehat{\mathcal{O}}_{Y,f(x)} \arrow[r, "\widehat{f}^\sharp"] & \widehat{\mathcal{O}}_{X,x} \arrow[r, shift left, "\widehat{p}_1^\sharp"] \arrow[r, shift right, "\widehat{p}_2^\sharp"'] & \widehat{\mathcal{O}}_{T,t} \\
& \mathcal{O}_{X,x} \arrow[u, "\sigma_{X,x}"] \arrow[r, shift left, "p_1^\sharp"] \arrow[r, shift right, "p_2^\sharp"'] & \mathcal{O}_{T,t} \arrow[u, "\sigma_{T,t}"']
\end{tikzcd}$$

Since T is an integral Noetherian scheme, then $\mathcal{O}_{T,t}$ is a Noetherian integral domain. So the rightmost map $\sigma_{T,t} : \mathcal{O}_{T,t} \longrightarrow \widehat{\mathcal{O}}_{T,t}$ is injective since $\ker(\sigma_{T,t}) = \bigcap_n \mathfrak{m}_{T,t}^n = 0$ by [22, Theorem 8.10(ii)]. Hence it will suffice to show that $\widehat{p}_1^\sharp = \widehat{p}_2^\sharp$. The condition $f \circ p_1 = f \circ p_2$ implies $\widehat{p}_1^\sharp \circ \widehat{f}^\sharp = \widehat{p}_2^\sharp \circ \widehat{f}^\sharp$. And $\widehat{f}^\sharp : \widehat{\mathcal{O}}_{Y,f(x)} \longrightarrow \widehat{\mathcal{O}}_{X,x}$ is surjective since f is a formal immersion at x. Therefore $\widehat{p}_1^\sharp = \widehat{p}_2^\sharp$. □

Assume that N is large enough so that $Gon(X_0(N)) > d$. Then by Lemma 2.1, we may define an embedding $\Phi : X_0(N)^{(d)} \hookrightarrow J_0(N)$. We compose this with the natural projection $J_0(N) \longrightarrow J_0^e$ to obtain a map $f : X_0(N)^{(d)} \longrightarrow J_0^e$. Denote $S' = \mathrm{Spec}\mathbb{Z}[1/N]$. Since $X_0(N)$ is a smooth scheme over S', then $X_0(N)^{(d)}$ is also a smooth scheme over S'. Since J_0^e is an abelian variety over $\mathbb{Q}$, it has a Néron model $J_{0/S'}^e$. We also use f to denote the map $f : X_0(N)_{/S'}^{(d)} \longrightarrow J_{0/S'}^e$. Parent [32] proved the following Kamienny's criterion.

Proposition 3.3 *(Kamienny's criterion). Suppose $p > 2$ and $p \nmid N$. The following (1) and (2) are equivalent. Furthermore, these two conditions are satisfied if (3) is true.*

(1) The map $f : X_0(N)^{(d)}_{/S'} \longrightarrow J^e_{0/S'}$ is a formal immersion along the section $(\infty, \cdots, \infty)$ in characteristic p.
(2) $T_1 e, \cdots, T_d e$ are $\mathbb{F}_p$-linearly independent in $\mathbb{T}e/p\mathbb{T}e$.
(3) $T_1\{0,\infty\}, \cdots, T_{sd}\{0,\infty\}$ are $\mathbb{F}_p$-linearly independent in $H_1(X_0(N), cusps, \mathbb{Z}) \otimes \mathbb{F}_p$ (here s is the smallest prime number not dividing N).

In order to apply this criterion in our cases, we need the following Lemma 3.4 and Lemma 3.6.

Lemma 3.4. *Let $N = q_1^{e_1} \cdots q_n^{e_n}$ be a positive integer with $q_1, \cdots, q_n$ distinct prime numbers. Let $p \nmid N$ be a prime number with $N > (1+\sqrt{p^d})^2$ and $q_j^{e_j} \nmid p^{2i}-1$, for all $1 \le j \le n$ and all $1 \le i \le d$. Suppose that E is an elliptic curve over a number field K of degree d with P a K-rational point of order N, i.e. $(E, \pm P) \in Y_1(N)(K)$. Let $x = \pi(E, \pm P)$ be the projection of $(E, \pm P)$ on $Y_0(N)(K)$. Let $\wp$ be a prime of $\mathcal{O}_K$ above p and let k be the residue field of $\wp$. Then $x_{1/\tau_1(\wp)} = \cdots = x_{d/\tau_d(\wp)} = \infty_{/\wp}$.*

Proof. Let $(\widetilde{E}, \widetilde{P})$ be the reduction of (E, P). It suffices to verify that E has multiplicative reduction at $\wp$ and $\pi(E, \pm P)$ specialize to ∞.

If E has good reduction at $\wp$, then $\widetilde{E}$ is an elliptic curve with a k-rational point $\widetilde{P}$ of order N. By the Hasse's theorem, $\widetilde{E}(k)$ has order at most $(1+\sqrt{p^d})^2$. This is impossible under our assumption of N.

If E has additive reduction at $\wp$, then $\widetilde{E}(k)^0 \cong \mathbb{G}_{a/k}$ with $|\mathbb{G}_{a/k}| = p^i$, $i \le d$ and $\widetilde{E}(k)/\widetilde{E}(k)^0 \cong G$ with $|G| \le 4$. Since $\widetilde{P}$ is a k-rational point of order N in $\widetilde{E}$, then N divides $|\widetilde{E}(k)| = |\mathbb{G}_{a/k}||G|$, which is impossible under our assumption.

So E has multiplicative reduction at $\wp$, then over a quadratic extension $\mathscr{K}$ of k, we have an isomorphism $\widetilde{E}(\mathscr{K})^0 \cong \mathbb{G}_{m/\mathscr{K}}$.

Suppose (E, P) specialize to $(C_n, (\zeta_N^r, b)))$ where C_n is a Néron n-gon with $n < N$ and (ζ_N^r, b) is a point of order N in the smooth locus $C_n^{sm} = \mathbb{G}_{m/\mathscr{K}} \times \mathbb{Z}/n\mathbb{Z}$. Then the order of b in $\mathbb{Z}/d\mathbb{Z}$ is $\le n < N$. Therefore, for a prime $q_j|(N/n)$, one has that $(N/q_j)P$ specialize into the identity component $\widetilde{E}(\mathscr{K})^0 \cong \mathbb{G}_{m/\mathscr{K}}$.

Now consider the point $P' := (N/q_j^{e_j})P$, whose specialization is of order $q_j^{e_j}$ on $\mathbb{G}_{m/\mathscr{K}} \times \mathbb{Z}/n\mathbb{Z}$. Write $\widetilde{P}' = (\widetilde{P}'_1, \widetilde{P}'_2)$ with $\widetilde{P}'_1$ a point of $\mathbb{G}_{m/\mathscr{K}}$ and $\widetilde{P}'_2$ a point of $\mathbb{Z}/n\mathbb{Z}$. The fact that $q_j^{e_j-1}P' = (N/q_j)P$ specializes into the identity component means that $\widetilde{P}'_2$ has order dividing $q_j^{e_j-1}$. So, the only possibility for $\widetilde{P}'$ to have order $q_j^{e_j}$ is then for $\widetilde{P}'_1$ to be of that order. So $q_j^{e_j}$ must divide the cardinality of $\mathscr{K}^*$, which itself must divide $p^{2i}-1$, where i is the degree of k over $\mathbb{F}_p$. This contradicts our assumption of N.

So (E, P) must specialize to $(C_n, (\zeta_N^r, b)))$ where C_n is the Néron n-gon with $n = N$ and (ζ_N^r, b) is a point of order N in the smooth locus $C_N^{sm} = \mathbb{G}_{m/\mathscr{K}} \times \mathbb{Z}/N\mathbb{Z}$. Hence $\pi(E, \pm P)$ specialize to $\infty := (C_N, \mathbb{Z}/N\mathbb{Z})$. □

Theorem 3.5. *Let $N = q_1^{e_1} \cdots q_n^{e_n}$ be an odd positive integer such that $Gon(X_0(N)) > d$. Suppose there is a prime $p \nmid N$, $p > 2$ satisfying:*

(1) $N > (1 + \sqrt{p^d})^2$ and $q_j^{e_j} \nmid p^{2i} - 1$, for all $1 \le j \le n$ and all $1 \le i \le d$.
(2) $T_1\{0, \infty\}, \cdots, T_{2d}\{0, \infty\}$ are linearly independent mod p in $H_1(X_0(N), cusps, \mathbb{Z})$.

Then for any elliptic curve E defined over a number field K with $[K : \mathbb{Q}] = d$, the cyclic group $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$.

Proof. The proof of this theorem is in essence the same as that of Theorem 3.3 in Kamienny [15]. Suppose we have a number field K with $[K : \mathbb{Q}] = d$ and an elliptic curve E defined over K such that $\mathbb{Z}/N\mathbb{Z} \subseteq E(K)_{tor}$. Take a generator P of $\mathbb{Z}/N\mathbb{Z}$, then we have a noncuspidal point $x = \pi(E, \pm P)$ on $X_0(N)$ of degree d. By Lemma 3.4, we have that the S-sections $(x_1, \cdots, x_d)$ and $(\infty, \cdots, \infty)$ meet at the prime p. Consequently, we have that $f(x_1, \cdots, x_d)_{/p} = f(\infty, \cdots, \infty)_{/p}$. However, the points $f(x_1, \cdots, x_d)$ and $f(\infty, \cdots, \infty)$ are both $\mathbb{Q}$-rational. And we know $J_0^e(\mathbb{Q})$ is finite [32, Theorem 1.7]. So by Lemma 2.6, the S-sections $f(x_1, \cdots, x_d)$ and $f(\infty, \cdots, \infty)$ coincide. And by Proposition 3.3, f is a formal immersion at $(\infty, \cdots, \infty)_p$. Therefore by Lemma 3.2, the sections $(x_1, \cdots, x_d)$ and $(\infty, \cdots, \infty)$ coincide. This contradicts our assumption that x is noncuspidal. □

In the special case when N is square free, and K is cubic, we can weaken the condition in Lemma 3.4 and get the following:

Lemma 3.6. *Let N be a square free positive integer with $g(X_0(N)) > 0$. Let $p \nmid N$ be a prime number with $N > (1 + \sqrt{p^3})^2$ and N is coprime with $p^2 - 1$. Suppose that E is an elliptic curve over a cubic number field K with P a K-rational point of order N, i.e. $y = (E, \pm P) \in Y_1(N)(K)$. Let $x = \pi(E, \pm P)$ be the projection of y on $Y_0(N)(K)$. Then there is a prime $\wp$ of $\mathcal{O}_K$ above p with residue field k, such that either $x_{1/\tau_1(\wp)} = \cdots = x_{3/\tau_3(\wp)} = \infty_{/\wp}$, or there is an Atkin–Lehner involution w_n on $X_0(N)$ with $w_n(x_1)_{/\tau_1(\wp)} = \cdots = w_n(x_3)_{/\tau_3(\wp)} = \infty_{/\wp}$.*

Proof. We can always choose $\wp$ such that the residue field $k = \mathcal{O}_K/\wp$ has degree 1 or 3 over $\mathbb{F}_p$. In fact, the decomposition of p in $\mathcal{O}_K$ has the following five types

$$\begin{array}{llllll} I: & p\mathcal{O}_K = \wp & II: & p\mathcal{O}_K = \wp^3 & III: & p\mathcal{O}_K = \wp_1\wp_2 \\ IV: & p\mathcal{O}_K = \wp_1\wp_2^2 & V: & p\mathcal{O}_K = \wp_1\wp_2\wp_3 & & \end{array}$$

In type II, IV, V, all the primes over p have degree 1 residue field. In type I, the prime over p has degree 3 residue field. In type III, the degree of the residue fields of the two primes $\wp_1$, $\wp_2$ is 1 and 2 respectively. We choose the one with degree 1 residue field as $\wp$.

By the same reason as in the proof of Lemma 3.4, E has multiplicative reduction at $\wp$. If the degree of k over $\mathbb{F}_p$ is 1, since we assume N is coprime with $p^2 - 1$, then the same reasoning as that in the proof of Lemma 3.4 leads to $x_{1/\tau_1(\wp)} = \cdots = x_{3/\tau_3(\wp)} = \infty_{/\wp}$.

If the degree of k over $\mathbb{F}_p$ is 3, consider the Galois closure L of K. Then either $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$ or $\mathrm{Gal}(L/\mathbb{Q}) = S_3$. We claim that there is an element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ of order 3, such that (after a necessary rearrangement) the embeddings $\tau_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq 3$ satisfy

$$\tau_i = \sigma^i|_K$$

In fact, if $\mathrm{Gal}(L/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$, then $L = K$, i.e. $K/\mathbb{Q}$ is a Galois extension. So $\mathrm{Gal}(K/\mathbb{Q}) = \{\tau_1, \tau_2, \tau_3\}$. Let σ be a generator of $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$. Then, after a necessary rearrangement of τ_1, τ_2 and τ_3, we have $\tau_i = \sigma^i$.

Otherwise, if $\mathrm{Gal}(L/\mathbb{Q}) = S_3$, then L/K is a quadratic extension. There is an element $\sigma_2 \in \mathrm{Gal}(L/\mathbb{Q})$ of order 2 such that $\mathrm{Gal}(L/K) = \langle \sigma_2 \rangle$. Let $\sigma_3 \in \mathrm{Gal}(L/\mathbb{Q})$ be an element of order 3. Then $\mathrm{Gal}(L/\mathbb{Q}) = \langle \sigma_2, \sigma_3 \rangle$. On the other hand, each τ_i extends to two embedding $\tau_{i1}, \tau_{i2} : L \hookrightarrow \mathbb{Q}$ and $\mathrm{Gal}(L/\mathbb{Q}) = \{\tau_{11}, \tau_{12}, \tau_{21}, \tau_{22}, \tau_{31}, \tau_{32}\}$. Without loss of generality, suppose τ_3 is the identity embedding, then $\{\tau_{31}, \tau_{32}\} = \{id, \sigma_2\}$, and after a necessary rearrangement of τ_1 and τ_2, $\{\tau_{11}, \tau_{12}\} = \{\sigma_3, \sigma_3\sigma_2\}$, $\{\tau_{21}, \tau_{22}\} = \{\sigma_3^2, \sigma_3^2\sigma_2\}$. Let $\sigma = \sigma_3$. Then $\tau_i = \sigma^i|_K$.

Let $\wp'$ be a prime of L over $\wp$ with residue field $k' = \mathcal{O}_L/\wp'$ (which is an extension of k). It is known in algebraic number theory that the Frobenius $\phi \in \mathrm{Gal}(k'/\mathbb{F}_p)$ is the reduction from a Frobenius element $\sigma' = Frob_{\wp'}$ in $\mathrm{Gal}(L/\mathbb{Q})$. It is easy to see $k' = k$ since the highest order of an element in $\mathrm{Gal}(L/\mathbb{Q})$ is 3. Since the only elements of order 3 in $\mathrm{Gal}(L/\mathbb{Q})$ are σ and σ^2, then either $\sigma' = \sigma$ or $\sigma' = \sigma^2$. Without loss of generality, let's suppose $\sigma' = \sigma$. Then the following reduction diagram is commutative for all $1 \leq i \leq 3$:

$$\begin{tikzcd}
X_1(N) \arrow[r, "\otimes\overline{\mathbb{F}}_p"] \arrow[d, "\tau_i"] & \widetilde{X}_1(N) \arrow[r, "\pi"] \arrow[d, "\phi^i"] & \widetilde{X}_0(N) \arrow[d, "\phi^i"] \\
X_1(N) \arrow[r, "\otimes\overline{\mathbb{F}}_p"] & \widetilde{X}_1(N) \arrow[r, "\pi"] & \widetilde{X}_0(N)
\end{tikzcd}$$

Let y_1, y_2, y_3 (resp. x_1, x_2, x_3) be the images of y (resp. x) under the distinct embeddings $\tau_i : K \hookrightarrow \mathbb{C}$, $1 \leq i \leq 3$. Since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the covering $X_1(N) \longrightarrow X_0(N)$ is compatible, i.e. the following diagram is commutative, we have $x_i = \pi(y_i)$, $1 \leq i \leq 3$.

$$\begin{tikzcd}
X_1(N) \arrow[r, "\tau_i"] \arrow[d, "\pi"'] & X_1(N) \arrow[d, "\pi"] \\
X_0(N) \arrow[r, "\tau_i"] & X_0(N)
\end{tikzcd}$$

Let c be a cusp of $X_1(N)$ such that

$$y \otimes \overline{\mathbb{F}}_p = c \otimes \overline{\mathbb{F}}_p$$

then for $1 \leq i \leq 3$

$$y_i \otimes \overline{\mathbb{F}}_p = \tau_i(y) \otimes \overline{\mathbb{F}}_p = \phi^i(y \otimes \overline{\mathbb{F}}_p) = \phi^i(c \otimes \overline{\mathbb{F}}_p) = \tau_i(c) \otimes \overline{\mathbb{F}}_p$$

We know that the action of each τ_i on the cusps factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$. Suppose c is represented by $(C_n, (\zeta_N^r, b))$, then $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ acts on c as

$$(C_n, (\zeta_N^r, b))^a = (C_n, (\zeta_N^{ra}, b))$$

So all the $\tau_i(c)$ are in the form of $(C_n, (\zeta_N^{ra_i}, b))$ for some $a_i \in (\mathbb{Z}/N\mathbb{Z})^\times$. Since N is square free, we know they all map to the unique cusp of the form (C_n, G) on $X_0(N)$. Denote (C_n, G) as c_n. Then

$$x_i \otimes \overline{\mathbb{F}}_p = \pi(y_i) \otimes \overline{\mathbb{F}}_p = \pi(y_i \otimes \overline{\mathbb{F}}_p) = \pi(\tau_i(c) \otimes \overline{\mathbb{F}}_p) = \pi(\tau_i(c)) \otimes \overline{\mathbb{F}}_p = c_n \otimes \overline{\mathbb{F}}_p$$

We know the Atkin–Lehner involutions act transitively on the cusps of $X_0(N)$ if N is square free. In fact, by applying the Atkin–Lehner involution w_n one gets that $w_n(c_n) = \infty$. And because the reduction diagram

$$\begin{tikzcd}
X_0(N) \arrow[r, "w_n"] \arrow[d, "\otimes\overline{\mathbb{F}}_p"'] & X_0(N) \arrow[d, "\otimes\overline{\mathbb{F}}_p"] \\
\widetilde{X}_0(N) \arrow[r, "w_n"] & \widetilde{X}_0(N)
\end{tikzcd}$$

is commutative when the genus of $X_0(N)$ is positive (see Diamond–Shurman [6], Theorem 8.5.7). So we have

$$w_n(x_i) \otimes \overline{\mathbb{F}}_p = w_n(x_i \otimes \overline{\mathbb{F}}_p) = w_n(c_n \otimes \overline{\mathbb{F}}_p) = w_n(c_n) \otimes \overline{\mathbb{F}}_p = \infty \otimes \overline{\mathbb{F}}_p$$

i.e.

$$w_n(x_1)_{/\tau_1(\wp)} = \cdots = w_n(x_3)_{/\tau_3(\wp)} = w_n(c_n)_{/\wp} = \infty_{/\wp}. \qquad \square$$

Theorem 3.7. *Let N be an odd square free positive integer such that $Gon(X_0(N)) > d$ and the genus $g(X_0(N)) > 0$. Suppose there is a prime $p \nmid N$, $p > 2$ satisfying:*

(1) $N > (1 + \sqrt{p^3})^2$ and N is coprime with $p^2 - 1$.
(2) $T_1\{0, \infty\}, \cdots, T_{2d}\{0, \infty\}$ are linearly independent mod p in $H_1(X_0(N), cusps, \mathbb{Z})$.

Then for any elliptic curve E defined over a cubic number field K, the cyclic group $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$.

Proof. With Lemma 3.6 at hand, the proof of this theorem is exactly the same as that of Theorem 3.5 except replacing $(x_1, \cdots, x_d)$ by $(w_n(x_1), \cdots, w_n(x_d))$ when necessary. □

4. Proof of Theorem 1.2

The calculations in this section are done in Sage [35]. The elements in $H_1(X_0(N), cusps, \mathbb{Z})$ can be represented by the *Manin symbols* (detailed description of this treatment can be found in Stein's book [37, §3]). Under this representation, the element $\{0, \infty\}$ is represented by the Manin symbol $(0, 1)$. By Proposition 20 of Merel [25], the action of Hecke operators T_n on Manin symbols can be calculated by the formula:

$$T_n(x, y) = \sum_{a>b\geq 0,\quad d>c\geq 0,\quad ad-bc=n} (x, y)\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] = (x, y)h_n$$

where in the sum

$$h_n = \sum_{a>b\geq 0,\quad d>c\geq 0,\quad ad-bc=n} \left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right],$$

if

$$(x', y') = (x, y)\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right] \in (\mathbb{Z}/N\mathbb{Z})^2 \quad \text{and} \quad \gcd(x', y', N) \neq 1,$$

then we omit the corresponding summand.

When n is small enough such that $\gcd(x', y', N) = 1$ for all summands, the formula is independent of the level N. Under this assumption, the first six h_n's are

$$h_1 = \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$$

$$h_2 = \left[\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}\right]$$

$$h_3 = \left[\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}\right] + \left[\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 3 & 1 \\ 0 & 1 \end{pmatrix}\right]$$
$$+ \left[\begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}\right]$$

$$h_4 = \left[\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 1 & 4 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 2 & 4 \end{pmatrix}\right] + \left[\begin{pmatrix} 1 & 0 \\ 3 & 4 \end{pmatrix}\right] + \left[\begin{pmatrix} 4 & 0 \\ 0 & 1 \end{pmatrix}\right]$$
$$+ \left[\begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 4 & 2 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}\right] + \left[\begin{pmatrix} 2 & 0 \\ 1 & 2 \end{pmatrix}\right]$$

$$
\begin{aligned}
&+\left[\begin{pmatrix}2&1\\0&2\end{pmatrix}\right]+\left[\begin{pmatrix}2&1\\2&3\end{pmatrix}\right]+\left[\begin{pmatrix}3&2\\1&2\end{pmatrix}\right]\\
h_5={}&\left[\begin{pmatrix}1&0\\0&5\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\1&5\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\2&5\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\3&5\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\4&5\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}5&0\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}5&1\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}5&2\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}5&3\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}5&4\\0&1\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}2&1\\1&3\end{pmatrix}\right]+\left[\begin{pmatrix}3&1\\1&2\end{pmatrix}\right]+\left[\begin{pmatrix}2&1\\3&4\end{pmatrix}\right]+\left[\begin{pmatrix}4&3\\1&2\end{pmatrix}\right]+\left[\begin{pmatrix}3&2\\2&3\end{pmatrix}\right]\\
h_6={}&\left[\begin{pmatrix}1&0\\0&6\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\1&6\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\2&6\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\3&6\end{pmatrix}\right]+\left[\begin{pmatrix}1&0\\4&6\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}1&0\\5&6\end{pmatrix}\right]+\left[\begin{pmatrix}6&0\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}6&1\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}6&2\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}6&3\\0&1\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}6&4\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}6&5\\0&1\end{pmatrix}\right]+\left[\begin{pmatrix}2&0\\0&3\end{pmatrix}\right]+\left[\begin{pmatrix}2&0\\1&3\end{pmatrix}\right]+\left[\begin{pmatrix}2&0\\2&3\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}2&1\\0&3\end{pmatrix}\right]+\left[\begin{pmatrix}3&0\\0&2\end{pmatrix}\right]+\left[\begin{pmatrix}3&1\\0&2\end{pmatrix}\right]+\left[\begin{pmatrix}3&2\\0&2\end{pmatrix}\right]+\left[\begin{pmatrix}3&0\\1&2\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}2&1\\2&4\end{pmatrix}\right]+\left[\begin{pmatrix}4&2\\1&2\end{pmatrix}\right]+\left[\begin{pmatrix}2&1\\4&5\end{pmatrix}\right]+\left[\begin{pmatrix}5&4\\1&2\end{pmatrix}\right]+\left[\begin{pmatrix}3&2\\3&4\end{pmatrix}\right]\\
&+\left[\begin{pmatrix}4&3\\2&3\end{pmatrix}\right]
\end{aligned}
$$

For $N = 169, 143, 91, 65, 77, 55$, the Manin basis of $H_1(X_0(N), cusps, \mathbb{Z})$ is listed in Table 1. And the actions of $T_1, \cdots, T_6$ on the Manin symbol $(0, 1)$ in terms of the Manin basis are given in Table 2.

4.1. $N = 169$

It is seen in Table 2 that $T_1\{0, \infty\}, \cdots, T_6\{0, \infty\}$ are linearly independent mod 5. By Proposition 2.2 and 2.3, we know $Gon(X_0(169)) > 3$. Since $169 \nmid 5^{2i} - 1$, $i = 1, 2, 3$, and $169 > (1 + \sqrt{5^3})^2$, then by Theorem 3.5, $\mathbb{Z}/169\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$.

4.2. $N = 143, 91, 65, 77, 55$

It is seen in Table 2 that $T_1\{0, \infty\}, \cdots, T_6\{0, \infty\}$ are linearly independent mod 3. By Proposition 2.2 and 2.3, we know $Gon(X_0(N)) > 3$. Since $(N, 3^2 - 1) = 1$ and $N > (1 + \sqrt{3^3})^2$, then by Theorem 3.7, $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{tor}$.

Table 1
Manin basis of $H_1(X_0(N), cusps, \mathbb{Z})$.

N	dim	Manin basis of $H_1(X_0(N), cusps, \mathbb{Z})$
169	29	$(1,0),(1,133),(1,134),(1,135),(1,138),(1,139),(1,151),(1,152),(1,153),(1,158),$ $(1,159),(1,160),(1,163),(1,164),(1,165),(1,166),(1,167),(13,1),(13,2),(13,3),$ $(13,4),(13,5),(13,6),(13,7),(13,8),(13,9),(13,10),(13,11),(13,12)$
143	29	$(1,0),(1,83),(1,113),(1,127),(1,128),(1,135),(1,139),(1,140),(1,141),(11,3),$ $(11,4),(11,5),(11,6),(11,7),(11,8),(11,9),(11,10),(11,12),(13,1),(13,2),$ $(13,3),(13,4),(13,5),(13,6),(13,7),(13,8),(13,9),(13,10),(13,11)$
91	17	$(1,0),(7,1),(7,2),(7,4),(7,5),(7,8),(7,9),(7,10),(7,11),(7,12),$ $(13,1),(13,2),(13,3),(13,4),(13,5),(13,6),(13,7)$
65	13	$(1,0),(5,2),(5,3),(5,7),(5,9),(5,11),(5,12),(5,23),(13,1),(13,2),$ $(13,3),(13,4),(13,5)$
77	17	$(1,0),(1,74),(1,75),(7,1),(7,3),(7,5),(7,6),(7,8),(7,9),(7,10),$ $(11,1),(11,2),(11,3),(11,4),(11,5),(11,6),(11,7)$
55	13	$(1,0),(1,48),(5,2),(5,4),(5,7),(5,8),(5,9),(5,21),(11,1),(11,2),$ $(11,3),(11,4),(11,5)$

Table 2
Hecke operators on $\{0, \infty\}$ in terms of Manin symbols.

N	T_i	$T_i(0,1)$
169	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_3	$(-4,0,1,-1,1,-1,0,1,0,0,-1,0,0,0,1,0,1,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_4	$(-7,0,0,-1,1,-1,0,0,0,0,0,0,-1,1,1,0,2,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_5	$(-6,0,0,-2,0,0,0,1,0,0,-1,0,0,2,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_6	$(-12,0,3,-3,2,-2,0,2,0,0,-2,0,1,0,2,0,4,0,0,0,0,0,0,0,0,0,0,0,0)$
143	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_3	$(-4,0,0,0,0,0,0,0,1,1,0,0,0,0,0,0,1,-1,-1,-1,1,0,0,0,0,1,-1,0,1)$
	T_4	$(-7,0,0,0,1,0,1,-1,3,1,0,0,0,-1,0,1,1,-1,0,-1,0,0,0,0,0,1,-1,0,1)$
	T_5	$(-6,0,0,0,1,0,1,-1,1,1,-1,2,0,-1,2,0,1,-3,-2,-1,0,-1,2,2,-1,1,-1,0,1)$
	T_6	$(-12,0,0,0,1,0,1,-1,4,3,-1,0,1,0,0,0,3,-4,-3,-2,2,-1,1,1,-1,3,-2,0,2)$
91	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,0,1,-1,-1,-1,-1,1,1,0,0,0,1,0,0,0,-1)$
	T_3	$(-4,-1,1,-2,0,0,-2,2,1,-1,1,-1,2,0,-1,1,-2)$
	T_4	$(-7,-1,3,-3,-2,-2,-3,2,3,-1,1,-1,3,1,-1,1,-4)$
	T_5	$(-6,-1,1,-2,-1,-1,-2,2,1,-1,1,0,2,0,0,1,-4)$
	T_6	$(-12,-3,4,-6,-2,-2,-6,6,4,-3,3,-2,6,0,-2,3,-8)$
65	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,1,-1,0,1,0,-1,-1,-1,0,1,1,-1)$
	T_3	$(-4,1,-1,0,2,-1,-2,-1,-2,0,2,2,-2)$
	T_4	$(-7,3,-2,0,4,-1,-4,-2,-4,-1,3,4,-2)$
	T_5	$(-5,2,-2,0,2,-2,-4,-2,-3,-1,3,3,-1)$
	T_6	$(-12,5,-4,0,6,-2,-7,-4,-6,-1,6,7,-6)$
77	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_3	$(-4,0,1,0,0,1,1,0,-1,0,-1,0,0,0,1,-1,1)$
	T_4	$(-7,0,3,0,-1,1,1,-1,-1,0,-1,0,1,1,1,-1,-1)$
	T_5	$(-6,0,2,-1,0,2,2,0,-2,-1,-1,0,0,0,2,-1,0)$
	T_6	$(-12,0,4,-1,0,3,3,0,-2,-1,-2,0,0,0,2,-2,2)$
55	T_1	$(-1,0,0,0,0,0,0,0,0,0,0,0,0)$
	T_2	$(-3,0,0,1,1,-1,0,-1,-1,1,0,0,0)$
	T_3	$(-4,0,-1,2,2,0,-1,-2,-2,1,1,0,0)$
	T_4	$(-7,0,0,3,3,-2,0,-4,-3,2,0,1,0)$
	T_5	$(-5,0,-1,2,2,-2,-1,-4,-3,2,0,1,1)$
	T_6	$(-12,0,-2,6,6,-2,-2,-8,-6,4,2,2,-2)$

Acknowledgments

It is a pleasure to thank my PhD advisor Sheldon Kamienny for introducing this research topic and for providing many valuable ideas and insightful comments throughout the research. I wish to thank Maarten Derickx for correcting mistakes in Lemma 3.4 and Lemma 3.6. I also wish to thank Andrew Sutherland and Andreas Schweizer for pointing out several errors in an earlier version of this paper.

References

[1] T. Arnold, Formal immersions and quotients of modular jacobians, Talks at the 2003–04 VIGRE Number Theory Working Group at the University of Michigan.

[2] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergeb. Math. Grenzgeb. (3), vol. 21, Springer-Verlag, Berlin, 1990.

[3] J.W.S. Cassels, A note on the division values of $\wp(u)$, Proc. Cambridge Philos. Soc. 45 (1949) 167–172.

[4] B. Conrad, Arithmetic moduli of generalized elliptic curves, J. Inst. Math. Jussieu 6 (2) (2007) 209–278.

[5] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, in: Modular Functions of One Variable, II, Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, in: Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316 (in French).

[6] F. Diamond, J. Shurman, A First Course in Modular Forms, Grad. Texts in Math., vol. 228, Springer-Verlag, New York, 2005.

[7] V.G. Drinfeld, Two theorems on modular curves, Funktsional. Anal. i Prilozhen. 7 (2) (1973) 83–84 (in Russian).

[8] G. Frey, Curves with infinitely many points of fixed degree, Israel J. Math. 85 (1–3) (1994) 79–83.

[9] A. Grothendieck, Éléments de géométrie algébrique. I. Le langage des schémas, Inst. Hautes Études Sci. Publ. Math. (4) (1960) (in French).

[10] A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV, Inst. Hautes Études Sci. Publ. Math. (32) (1967) (in French).

[11] Y. Hasegawa, M. Shimura, Trigonal modular curves, Acta Arith. 88 (2) (1999) 129–140.

[12] J. Igusa, Kroneckerian model of fields of elliptic modular functions, Amer. J. Math. 81 (1959) 561–577.

[13] D. Jeon, C.H. Kim, A. Schweizer, On the torsion of elliptic curves over cubic number fields, Acta Arith. 113 (3) (2004) 291–301.

[14] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. 109 (2) (1992) 221–229.

[15] S. Kamienny, Torsion points on elliptic curves over fields of higher degree, Int. Math. Res. Not. IMRN (6) (1992) 129–133.

[16] N.M. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (3) (1981) 481–502.

[17] N.M. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Ann. of Math. Stud., vol. 108, Princeton University Press, Princeton, NJ, 1985.

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

[19] K. Kodaira, On compact analytic surfaces: II, Ann. of Math. (2) 77 (1963) 563–626.

[20] D.S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. Lond. Math. Soc. (3) 33 (2) (1976) 193–237.

[21] Y.I. Manin, Parabolic points and zeta functions of modular curves, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972) 19–66 (in Russian).

[22] H. Matsumura, Commutative Ring Theory, Cambridge Stud. Adv. Math., vol. 8, Cambridge University Press, Cambridge, 1986, translated from the Japanese by M. Reid.

[23] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. (47) (1977) 33–186.

[24] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (2) (1978) 129–162.

[25] L. Merel, Universal Fourier expansions of modular forms, in: On Artin's Conjecture for Odd 2-Dimensional Representations, in: Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, pp. 59–94.

[26] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1–3) (1996) 437–449 (in French).

[27] F. Najman, Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$, Math. Res. Lett. 23 (1) (2016) 245–272.

[28] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Inst. Hautes Études Sci. Publ. Math. (21) (1964) 1–128 (in French).

[29] J. Oesterlé, Torsion des courbes elliptiques sur les corps de nombres, unpublished.

[30] A.P. Ogg, Hyperelliptic modular curves, Bull. Soc. Math. France 102 (1974) 449–462.

[31] A.P. Ogg, Diophantine equations and modular forms, Bull. Amer. Math. Soc. 81 (1975) 14–27.

[32] P. Parent, Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres, J. Reine Angew. Math. 506 (1999) 85–116 (in French).

[33] P. Parent, Torsion des courbes elliptiques sur les corps cubiques, Ann. Inst. Fourier (Grenoble) 50 (3) (2000) 723–749 (in French).

[34] P. Parent, No 17-torsion on elliptic curves over cubic number fields, J. Théor. Nombres Bordeaux 15 (3) (2003) 831–838.

[35] Sage: http://www.sagemath.org/.

[36] J.H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 151, Springer-Verlag, New York, 1994.

[37] W. Stein, Modular Forms, a Computational Approach (with an Appendix by Paul E. Gunnells), Grad. Stud. Math., vol. 79, American Mathematical Society, Providence, RI, 2007.