arXiv:1502.06873v4 [math.NT] 11 Mar 2015

ON THE CYCLIC TORSION OF ELLIPTIC CURVES OVER CUBIC NUMBER FIELDS.

JIAN WANG

ABSTRACT. Let E be an elliptic 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 will discuss the cyclic torsion subgroup of elliptic curves over cubic number fields.

1. INTRODUCTION

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

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

For a fixed E/K, the torsion component $E(K)_{tor}$ can be calculated. Actually, for an elliptic curve E/K with Weierstrass equation

$$y^2 = x^3 + Ax + B$$

such that $A, B \in \mathcal{O}_K$. Let $\Delta = 4A^2+27B^2$ and let $P \in E(K)_{tor}$ be a point. Then $y(P)^2$ is essentially bounded by Δ (See [23] Exercise 8.11). However, for a general class of elliptic curves, it is usually difficult to list all the possible structures of $E(K)_{tor}$. We can consider the following:

Problem 1.1. *For a natural number d, what are the possible structures of $E(K)_{tor}$ with $[K : \mathbb{Q}] = d$?*

For $d = 1$, i.e. $K = \mathbb{Q}$, Mazur [18] proved that the torsion group $E(\mathbb{Q})_{tor}$ of an elliptic curve E over the rational number field must be 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 $d = 2$, the possible structures of the torsion of an elliptic curve over quadratic number fields were determined by Kenku-Momose [12] and Kamienny [6]:

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

Date: March 12, 2015.
2010 *Mathematics Subject Classification.* 11G05,11G18.
Key words and phrases. torsion, elliptic curves, modular curves.

For $d = 3$, Jeon, Kim, Schweizer [5] found all the torsion structures that appears infinitely often when one runs through all elliptic curve 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 [19] found a sporadic point on $X_1(21)$, so that $\mathbb{Z}/21\mathbb{Z}$ can also serve as torsion of elliptic curves over cubic fields. We can conjecture that:

Conjecture 1.2. *The possible structures of the torsion of an elliptic curve over cubic number fields are:*

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

In this paper, we will discuss the cyclic case. The main results are Theorem 1.3 and Theorem 1.4.

Theorem 1.3. *Suppose E is an elliptic curve over an cubic field K. If $N = p^n$ is a prime power, then the cyclic group $\mathbb{Z}/N\mathbb{Z}$ does not occur as a subgroup of $E(K)_{tor}$ for N =32, 27, 25, 49, 121, 169.*

Theorem 1.3 is a complete result since Parent [21] showed that the prime divisors of $E(K)_{tor}$ are ≤ 13. In order to prove that a cyclic subgroup of $E(K)_{tor}$ is exactly one of those shown in Conjecture 1.2, we need to eliminate the case $N = 2 \cdot 13, 3 \cdot 13, 5 \cdot 13, 7 \cdot 13, 11 \cdot 13; 2 \cdot 11, 3 \cdot 11, 5 \cdot 11, 7 \cdot 11; 4 \cdot 7, 5 \cdot 7, 6 \cdot 7; 8 \cdot 5, 6 \cdot 5, 9 \cdot 5; 8 \cdot 3, 4 \cdot 9$.. Theorem 1.4 gives a partial result.

Theorem 1.4. *Suppose E is an elliptic curve over an cubic field K. If N has more than one prime divisors, then the cyclic group $\mathbb{Z}/N\mathbb{Z}$ does not occur as a subgroup of $E(K)_{tor}$ for N =143, 91, 65, 77, 55, 22, 40, 24.*

As is done for $d = 1$ and 2, the key idea is to consider the modular curves $X_1(N)$ and the map $\pi : X_1(N) \longrightarrow X_0(N)$. We want to prove the nonexistence of cubic points on $X_1(N)$ for certain N.

For this purpose, we will use the Igusa's theorem [3] which states that $X_1(N)$ and $X_0(N)$ have good reduction at $p \nmid N$.

Let $J_1(N)$ (respectively, $J_0(N)$) be the Jacobian of $X_1(N)$ (respectively, $X_0(N)$). Then we have a canonical embedding: $X_1(N) \hookrightarrow J_1(N)$ (respectively, $X_0(N) \hookrightarrow J_0(N)$). Suppose A is a quotient of $J_0(N)$, and $L(A, s)$ is the L series associated to A (See [22] for the definition). Kolyvagin and Logachëv [16] proves a Birch-Swinnerton-Dyer conjecture for modular abelian varieties, which states that A has Mordel-Weil rank 0 if $L(A, 1) \neq 0$. For abelian varieties that are a quotient of $J_1(N)_{\mathbb{Q}}$, the same result was proved by Kato [9].

With the increasing of degree d, the bound $(1 + \sqrt{p^d})^2$ predicted by the Riemann hypothesis increases drastically. If we do reduction for $X_1(N)$ modulo p, the points on $\widetilde{X}_1(N)$ may represents not only cusps even for the small $N's$ we are interested in. Therefore, the methods used for $d = 1$ and 2 are not enough. We will use three methods:

Method A: If N is big enough such that elliptic curves over $\mathbb{F}_{p^3}$ for a suitable p can not admit $\mathbb{Z}/N\mathbb{Z}$ as a subgroup, and if the decomposition

$$J_1(N) \longrightarrow A_1 \times \cdots \times A_n$$

has all A_i finite, i.e. $L(A_i, 1) \neq 0, 1 \leq i \leq n$, we can show the nonexistence of cubic points on $X_1(N)$ in a relatively easy way.

Method B: If we can not show all the quotients of $J_1(N)$ are finite, we can consider the decomposition

$$J_0(N) \longrightarrow B_1 \times \cdots \times B_m$$

and collect the B_i such that $L(B_i, 1) \neq 0$. Then investigate Hecke correspondences T_1, T_2, T_3 on the finite quotient and make use of Kamienny's criterion.

Method C: If none of the two methods above work, we have make use of reduction of the defining equations of $X_0(N)$. By investigating the Atkin-Lehner involutions, we may find some contradiction.

2. Elliptic curves over finite fields.

Let $k = \mathbb{F}_q$ be the finite field with $q = p^n$ elements. Let E/k be an elliptic curve over k. We can define the zeta function of E:

$$Z_E(x) = \frac{1 - a_q(E)x + qx^2}{(1-x)(1-qx)}$$

Here $a_q(E) = q + 1 - N_q(E)$ and $N_q(E) = \#E(k)$, the number of points of E over k.

The *Riemann hypothesis* for E is then the assertion that if $Z_E(q^{-s}) = 0$, then $Re(s) = \frac{1}{2}$. We can also rephrase the Riemann Hypothesis as a bound on a_q. In fact, the bound

$$|N_q - q - 1| \leq 2\sqrt{q}$$

is equivalent to the Riemann hypothesis for E. Let $a_q(E) = t$, E is called ordinary if $(t, q) = 1$, otherwise it is called supersingular. In the range proposed by Riemann Hypothesis, all the ordinary t appear, while the supersingular t only appears in restricted case. Explicitly, we have:

Theorem 2.1 (Waterhouse [26])**.** *The isogeny classes of elliptic curves over k are in one-to-one correspondence with the rational integers t having $|t| \leq 2\sqrt{q}$ and satisfying one of the following conditions:*

(1) $(t, p) = 1$;

(2) If n is even: $t = \pm 2\sqrt{q}$;

(3) If n is even and $p \not\equiv 1 \mod 3$: $t = \pm\sqrt{q}$;

(4) If n is odd and $p = 2$ or 3: $t = \pm p^{\frac{n+1}{2}}$;

(5) If either (i) n is odd or (ii) n is even and $p \not\equiv 1 \mod 4$: $t = 0$.

The first of these are ordinary; the second are supersingular and have all their endomorphisms defined over k; the rest are supersingular but do not have all their endomorphisms defined over k.

The Frobenius endomorphism $\pi : (x, y) \longmapsto (x^q, y^q)$ of E satisfies

$$\pi^2 - t\pi + q = 0$$

The algebra $A = \mathbb{Q} \otimes End_k(E)$ is semisimple with center $\Phi = \mathbb{Q}(\pi)$. Deuring [1] also classified the endomorphism rings of elliptic curves over finite fields. Here we use the results of Waterhouse [26] instead.

Theorem 2.2 (Waterhouse [26])**.** *Let $A = \mathbb{Q} \otimes End_k(E)$ be the endomorphism algebra of an isogeny class of elliptic curves. The orders in A which are endomorphism rings of curves in the class are as follows:*

(1) If the curves are ordinary: all orders containing π;

(2) If the curves are supersingular with all endomorphisms defined: the maximal orders;

(3) If the curves are supersingular with not all endomorphisms defined: the orders which contain π and are maximal at p, i.e. have conductors prime to p.

If E is ordinary, then $A = \mathbb{Q}(\pi)$. So End$(E) \cong \mathcal{O}(D)$ for some $D|t^2 - 4q$, where

$$\mathcal{O}(D) = \mathbb{Z} + \frac{D + \sqrt{D}}{2}\mathbb{Z}$$

is the imaginary quadratic order of some discriminant D. There are $h'(D)$ isomorphism classes of elliptic curves defined over $\mathbb{F}_q$ with $\mathcal{O}(D)$ as the endomorphism ring. Here $h'(D)$ is the class number of the order $\mathcal{O}(D)$.

Kohel [15] gives the method to calculate End(E). We call an isogeny ϕ an ℓ-isogeny if $|\ker \phi| = \ell$. We restrict to prime ℓ. The classical modular polynomial $\phi_\ell \in \mathbb{Z}[X, Y]$ has the property

$$\phi_\ell(j(E_1), j(E_2)) = 0 \Longleftrightarrow j(E_1) \text{ and } j(E_2) \text{ are } \ell \text{ isogenous}$$

The ℓ-isogeny graph $G_\ell(\mathbb{F}_q)$ has vertex set

$$\mathcal{E}(\mathbb{F}_q) = \{j(E/\mathbb{F}_q)\} = \mathbb{F}_q$$

and edges (j_1, j_2) for $\phi_\ell(j_1, j_2) = 0$. The ordinary connected components of $G_\ell(\mathbb{F}_q)$ are ℓ-volcanoes. An ℓ-volcano of height h has vertices in level $V_0, \cdots, V_h$. Vertices in V_0 have endomorphism ring $\mathcal{O}(D_0)$ with $\ell \nmid D_0$. Vertices in V_k have endomorphism ring $\mathcal{O}(\ell^{2k} D_0)$.

Proposition 2.3 (Kohel [15])**.** *The ℓ-volcano can be described as:*

(a) The subgraph on V_0 is a cycle. All other edges lie between V_k and V_{k+1} for some k.

(b) For $k > 0$, each vertex in V_k has one neighbor in V_{k-1}.

(c) For $k < h$, every vertex in V_k has degree $\ell + 1$.

3. Kamienny's criterion on cubic points of $X_1(N)$.

For N prime, Kamienny [7] established an criterion for the nonexistence of rational points of modular curves over number fields. This criterion can be *mutatis mutandis* generalized to the cases

when $N =$ prime power [8] or square free composite. In this section, we assume N is *a prime power or square free*.

The abelian varieties $J_1(N)_{/\mathbb{Q}}$ and $J_0(N)_{/\mathbb{Q}}$ are semistable and have good reduction at all primes $\ell \nmid N$. By Manin [17] and Drinfeld [2], the class of $(0-\infty)$ generates a $\mathbb{Q}$-rational subgroup C of $J_0(N)_{/\mathbb{Q}}$. Let $J_{/\mathbb{Q}}$ be a quotient of $J_0(N)_{/\mathbb{Q}}$ with finite Mordell-Weil group.

Let $X^{(d)}$ denote the d-th symmetric power of $X_0(N)$, i.e. the quotient space of the d-fold product $X_0(N) \times X_0(N) \times \cdots \times X_0(N)$ by the action of S_d permuting the factors. Then $X^{(d)}$ is a smooth scheme over $S' = \text{Spec}\mathbb{Z}[1/N]$. Let $J_{/S'}$ be the Néron model of $J_{/\mathbb{Q}}$.

Let K be a number field of degree d over $\mathbb{Q}$. Let $(E,P) \in X_1(N)(K)$ and $x = \pi(E,P) \in X_0(N)(K)$. Let $x_1, \cdots, x_d$ be the images of x under the distinct embeddings

$$\varphi_i : K \hookrightarrow \mathbb{C}, \quad 1 \le i \le d$$

We may view $(x_1, \cdots, x_d)$ as a $\mathbb{Q}$-rational point of $X^{(d)}$.

A smooth projective curve X over an algebraically closed field $\overline{k}$ is called d-gonal if there exists a finite morphism $f : X \longrightarrow \mathbb{P}$ over $\overline{k}$ of degree d. For $d = 3$ we say that the curve is trigonal. Also the smallest possible d is called the gonality of the curve. Considering the modular curve $X_0(N)$ over $\mathbb{C}$, we denote its gonality as $Gon(X_0(N))$.

Lemma 3.1. *Suppose $Gon(X_1(N)) > 3$, $J_1(N)/_{\mathbb{Q}}$ is finite, $p > 2$ is a prime not dividing N, and every point of degree 3 on $X_1(N)$ reduces modulo p to the image of a cusp which is of degree ≤ 3. Then $X_1(N)$ has no noncuspidal point of degree 3.*

Proof. If p does not divide the order of $J_1(\mathbb{Q})$, then the reduction map is injective:

$$J_1(N)/_{\mathbb{Q}} \hookrightarrow J_1(N)/_{\mathbb{F}_p} \tag{3.1}$$

If p divides the order of $J_1(\mathbb{Q})$, i.e. there is a rational point of order p in $J_1(N)$, we look at its Zariski closure G in the Néron model of $J_1(N)$ over Spec$\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers. By Oort-Tate [25] the group scheme G must be the constant group scheme $\mathbb{Z}/p\mathbb{Z}$, and hence it is étale. As such it must map isomorphically onto its reduction modulo p. In other words, reduction modulo p is injective on any possible rational p-torsion. Therefore the reduction map (3.1) is always injective.

Now suppose there is a noncuspidal point P of degree 3 on $X_1(N)$. Pick an element σ of order 3 in Gal$(K/\mathbb{Q})$, where K is the normal closure of the defining field of P. Let Q be the cusp such that $P/_{\mathbb{F}_p} = Q/_{\mathbb{F}_p}$. So

$$((P) + (P^\sigma) + (P^{\sigma^2}) - (Q) - (Q^\sigma) - (Q^{\sigma^2}))/_{\mathbb{F}_p} = O \in J_1(N)/_{\mathbb{F}_p}$$

hence by the injectivity of the reduction map above

$$(P) + (P^\sigma) + (P^{\sigma^2}) - (Q) - (Q^\sigma) - (Q^{\sigma^2}) = O \in J_1(N)/_{\mathbb{Q}}$$

Then $X_1(N)$ has a degree 3 function. Since $Gon(X_1(N)) > 3$, this in impossible. □

Assume that N is large enough so that $Gon(X_0(N)) > d$. Then we may define an embedding $h : X^{(d)} \hookrightarrow J_0(N)$ by

$$h(y_1, \cdots, y_d) = (y_1 + \cdots + y_d - d\infty)$$

We compose this with the natural projection $J_0(N) \longrightarrow J$ to obtain a map $f : X^{(d)} \longrightarrow J$.

Let

$$f_i = \sum_{n=1}^{\infty} a_n(f_i) q^n, \quad 1 \leq i \leq d$$

be weight-two cusp forms on $\Gamma_0(N)$. We will say that $f_1, \cdots, f_d$ satisfy the *linear independence condition mod* p if the vectors $(a_1(f_1), \cdots, a_d(f_1)), \cdots, (a_1(f_d), \cdots, a_d(f_d))$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$.

Proposition 3.2 (Kamienny [7])**.** *Suppose $p > 2$ and $p \nmid N$. The following are equivalent:*

(1) The map $f : X^{(d)}_{/S'} \longrightarrow J_{/S'}$ is a formal immersion along the section $(\infty, \cdots, \infty)$ in characteristic p.
(2) There exist d weight-two cusp forms, associated to J, that satisfy the linear independence condition mod p.
(3) The first d Hecke operators $T_1, \cdots, T_d$ on $H_1(J, \mathbb{Z})$ are linearly independent mod p.

Lemma 3.3. *Let $p \nmid N$ be a prime number with $N > (1 + \sqrt{p^d})^2$ and $N \nmid p^{2d} - 1$. Suppose that E is an elliptic curve over K possessing a K-rational point P of order N, and let $x = \pi(E, P)$ be the corresponding point in $X_0(N)(K)$. Let $\wp$ be a prime of $\mathcal{O}_K$ above p and let k be the residue field of $\wp$. Then $x_{1/\wp} = \cdots = x_{d/\wp} = \infty_{/\wp}$.*

Proof. By the Kodaira-Néron Theroem [13, 14, 20, 24], we need to check that E has multiplicative reduction at $\wp$, but P does not specialize to $(E_{/k})^0$.

If E has good reduction at $\wp$, then $E_{/k}$ is an elliptic curve with a k-rational point $P_{/k}$ of order N. By the Riemann hypothesis $E(k)$ 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 the index of $(E_{/k})^0$ in $E_{/k}$ is ≤ 4. So P must specialize to $(E_{/k})^0 \cong \mathbb{G}_{a/k}$. Then N divide the cardinality p^d of k, which is impossible since $p \nmid N$.

If E has multiplicative reduction at $\wp$, and P specialize to $(E_{/k})^0$, then over an extension $\mathscr{K}/k$ of degree at most 2, we have an isomorphism $(E_{/\mathscr{K}})^0 \cong \mathbb{G}_{m/\mathscr{K}}$. Then N must divide the cardinality of $\mathscr{K}^*$ which itself must divide $p^{2d} - 1$. This contradicts our assumption of N. □

Theorem 3.4 (Kamienny's creterion [7])**.** *Let N be prime power or square free composite natural number such that $Gon(X_0(N)) > d$. Suppose there is a prime $p \nmid N, p > 2$ satisfying:*

(1) $N \nmid p^{2d} - 1$ and $N > (1 + \sqrt{p^d})^2$
(2) The first d Hecke operators $T_1, \cdots, T_d$ on $H_1(J, \mathbb{Z})$ are linearly independent mod p.

Then there does not exist any elliptic curve with a point of order N rational over any field of degree d.

4. PRIME POWER CASES.

4.1. **case** $X_1(169)$**.** Calculations in Magma shows the decomposition

$$J_0(169) = A_1 \times A_2 \times A_3$$

with $\dim A_1 = 2, \dim A_2 = 3, \dim A_3 = 3$, and $L(A_i, 1) \neq 0$ for $i = 1, 3$. So by Kolyvagin-Logachëv [16], $A_1(\mathbb{Q})$ and $A_3(\mathbb{Q})$ are all finite. Take $J = A_1 \times A_3$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_1, \mathbb{Z}) \times H_1(A_3, \mathbb{Z}) = \mathbb{Z}^4 \times \mathbb{Z}^6$ as following:

$$T_1 = I_{10}$$

$$T_2 = diag\left\{ \begin{pmatrix} 2 & 1 & 0 & -1 \\ -1 & -1 & 1 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 3 & -1 & 0 & 1 & -2 \\ 0 & 4 & -3 & 2 & -1 & -1 \\ 0 & 1 & -1 & 1 & -1 & 0 \\ 0 & 2 & -1 & 1 & 0 & -1 \\ 1 & 3 & -2 & 0 & 1 & -2 \\ 0 & 6 & -4 & 2 & -1 & -2 \end{pmatrix} \right\}$$

$$T_3 = diag\left\{ \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 1 & -1 & 0 & -1 \\ 1 & 0 & -1 & -1 & -1 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ 0 & 2 & -2 & 0 & -1 & -1 \\ 1 & 3 & -2 & -2 & -1 & -2 \end{pmatrix} \right\}$$

They are linearly independent mod 3. Since $169 \nmid 3^6 - 1$ and $169 > (1 + \sqrt{3^3})^2$, then by Theorem 3.4, we are done.

4.2. **case** $X_1(121)$**.** We have the decomposition

$$J_0(121) = A_1 \times \cdots \times A_6$$

with $\dim A_i = 1, 1 \leq i \leq 6$, and $L(A_i, 1) \neq 0$ for $2 \leq i \leq 6$. Take $J = A_2 \times \cdots \times A_6$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_2, \mathbb{Z}) \times \cdots \times H_1(A_6, \mathbb{Z}) = \mathbb{Z}^2 \times \cdots \times \mathbb{Z}^2$ as following:

$$T_1 = I_{10}$$

$$T_2 = diag\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix} \right\}$$

$$T_3 = diag\left\{ \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

Unfortunately, they are linearly dependent mod 3. So we need to reprove Lemma 3.3 for $p = 5$. We have $121 \nmid 5^6 - 1$, but $121 < (1 + \sqrt{5^3})^2 \approx 148.4$. By Theorem 2.1, any elliptic curve E over $k = \mathbb{F}_{125}$ can not have an k-rational points P of order 121. So, Lemma 3.3 is true for $p = 5, d = 3, N = 121$. Then by Theorem 3.4, we are done.

4.3. **case** $X_1(49)$**.** $J_1(49)$ has decomposition:

$$J_1(49) \longrightarrow A_1 \times \cdots \times A_5$$

where A_i has dimensions: $1, 48, 6, 12, 2$ and $L(A_i, 1) \neq 0$ for all i. So $J_1(49)(\mathbb{Q})$ is finite.

Let K be a cubic field. Let $\wp$ be a prime in $\mathcal{O}_K$ lying above 3. Suppose $x = (E, P) \in X_1(49)(K)$. Since $49 > (1 + \sqrt{3^3})^2$, then $x_\wp$ is a cusp. We also know $Gon(X_1(49) > 3$. Therefore by Lemma 3.1, there are no noncuspidal cubic points on $X_1(49)$.

4.4. **case** $X_1(25)$**.** $J_1(25)$ has decomposition:

$$J_1(25) \longrightarrow A_1 \times A_2$$

where A_i has dimensions: $8, 4$ and $L(A_i, 1) \neq 0$ for all i. So $J_1(25)(\mathbb{Q})$ is finite.

We have $25 < (1 + \sqrt{3^3})^2 \approx 38.4$. So we need to show any elliptic curve E over $k = \mathbb{F}_{27}$ can not have an k-rational points P of order 25. Suppose $E(k)$ has a point of order 25, then $E(k) \cong \mathbb{Z}/25\mathbb{Z}$ since $25m > (1 + \sqrt{3^3})^2$ for any $m > 1$. But by Theorem 2.1, $E(k) \ncong \mathbb{Z}/25\mathbb{Z}$.

Let K be a cubic field. Let $\wp$ be a prime in $\mathcal{O}_K$ lying above 3. If $x = (E, P) \in X_1(25)(K)$, then $x_\wp$ is a cusp. We also know $Gon(X_1(25) > 3$. Therefore by Lemma 3.1, there are no noncuspidal cubic points on $X_1(25)$.

4.5. **case** $X_1(32)$**.** The cyclic covering $X_1(32) \longrightarrow X_0(32)$ can be factorised over $\mathbb{Q}$ into maps of degree 2 as follows:

$$X_1(32) \xrightarrow{\alpha_1} X_2 \xrightarrow{\alpha_2} X_3 \xrightarrow{\alpha_3} X_4 = X_0(32)$$

where $X_i = X_1(32)/\gamma_5^{2^{4-i}}$.

By the work of Igusa [3] we know that X_2 has good reduction modulo $p \neq 2$. The isomorphism class of each elliptic curve E defined over $\mathbb{F}_q$ with a point P satisfying $(\pi \pm 1)P = 0$ or $(\pi \pm 17)P = 0$ contributes 8 points to the reduction $\widetilde{X}_2$ of X_2 over $\mathbb{F}_q$.

TABLE 1. Elliptic curves over $\mathbb{F}_{27}$

t	π $= \frac{t+\sqrt{t^2-4q}}{2}$	$N(\pi+1)$ $= q+t+1$	$N(\pi-1)$ $= q-t+1$	$N(\pi+17)$ $= q+17t+289$	$N(\pi-17)$ $= q-17t+289$
0	$3\sqrt{-3}$	28	28	316	316
1	$\frac{1+\sqrt{-107}}{2}$	29	27	333	299
2	$1+\sqrt{-26}$	30	26	350	282
4	$2+\sqrt{-23}$	32	24	384	248
5	$\frac{5+\sqrt{-83}}{2}$	33	23	401	231
7	$\frac{7+\sqrt{-59}}{2}$	35	21	435	197
8	$4+\sqrt{-11}$	36	20	452	180
9	$\frac{9+3\sqrt{-3}}{2}$	37	19	469	163
10	$5+\sqrt{-2}$	38	18	486	146

Table 1 listed the ordinary case and super singular case of elliptic curves over $\mathbb{F}_{27}$. We find that noncuspidal points on $\widetilde{X}_2$ over $\mathbb{F}_{27}$ comes from elliptic curves with endomorphism ring $\mathbb{Z}[\sqrt{-23}]$ or $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.

Lemma 4.1. *Let x be a point of degree 3 on X_2, then it does not reduce modulo 3 to any point coresponding to an elliptic curve E with endomorphism ring $\mathbb{Z}[\sqrt{-23}]$ or $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$.*

Proof. Ishii [4] showed that $X_0(32)$ has a defining equation:

$$Y^2 + 2XY - 14Y - X^3 + 4X^2 - 21X + 54 = 0 \tag{4.1}$$

with j-invariant given by

$$j = (X^8 - 16X^4 + 16)^3/X^4(X^4 - 16)$$

Reduction modulo 3 we have

$$Y^2 + 2XY + Y - X^3 + X^2 = 0$$

$$j = (X^8 - X^4 + 1)^3/X^4(X^4 - 1)$$

Let $\mathbb{F}_{27} = \mathbb{F}_3[u]/(u^3-u+1)$. Table 2 list the points on the reduction of $X_0(32)$ modulo 3 which are rational over $\mathbb{F}_{27}$. For each j, we set $a_6 = -1/j$ and have the following elliptic curve with $j(E) = j$

$$E : y^2 = x^3 + x^2 + a_6$$

TABLE 2. Points on the reduction of $X_0(32)$ modulo 3 which are rational over $\mathbb{F}_{27}$

X	Y_1	Y_2	j
∞	∞	∞	$-$
0	-1	0	$-$
1	0	0	$-$
u	u^2+u	$-u^2-1$	$-u^2-u-1$
$u+1$	u^2-1	$-u^2+u+1$	$-u^2$
$u-1$	u^2-u	$-u^2-u+1$	$-u^2+u-1$
u^2+1	u	u^2-u	$-u^2-u+1$
u^2+u-1	$u-1$	u^2-1	$-u^2+u+1$
u^2-u-1	$u+1$	u^2+u	$-u^2-1$
$-u^2$	$-u^2+1$	1	$-u^2+u-1$
$-u^2-1$	u^2+u	u^2-u+1	$-u^2-u+1$
$-u^2+u+1$	u^2-1	u^2+u+1	$-u^2-1$
$-u^2+u-1$	$-u^2+u$	1	$-u^2-u-1$
$-u^2-u+1$	u^2-u	u^2	$-u^2+u+1$
$-u^2-u-1$	$-u^2-u$	1	$-u^2$

To calculate the endomorphism ring End(E), we use

$$\begin{aligned}\phi_2(X,Y) =&(X+Y)^3 - X^2Y^2 + 1485XY(X+Y) - 162000(X+Y)^2 \\ &+ 41097375XY + 8748000000(X+Y) - 157464000000000\end{aligned}$$

Reduction modulo 3, we have

$$\phi_2(X,Y) = (X+Y)^3 - X^2Y^2$$

Then we can calculate $E(\mathbb{F}_{27})$,π and End(E) as listed in Table 3.

TABLE 3. Endomorphism rings

j	a_6	$E(\mathbb{F}_{27})$	π	$End(E)$
$-u^2-u-1(F)$	$-u^2+u+1$	$\mathbb{Z}/24$	$2+\sqrt{-23}$	$\mathbb{Z}[\sqrt{-23}]$
$-u^2(E)$	$-u^2-u+1$	$\mathbb{Z}/24$	$2+\sqrt{-23}$	$\mathbb{Z}[\sqrt{-23}]$
$-u^2+u-1(D)$	$-u^2-1$	$\mathbb{Z}/24$	$2+\sqrt{-23}$	$\mathbb{Z}[\sqrt{-23}]$
$-u^2-u+1(A)$	$-u^2$	$\mathbb{Z}/2\times\mathbb{Z}/12$	$2+\sqrt{-23}$	$\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$
$-u^2+u+1(B)$	$-u^2-u-1$	$\mathbb{Z}/2\times\mathbb{Z}/12$	$2+\sqrt{-23}$	$\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$
$-u^2-1(C)$	$-u^2+u-1$	$\mathbb{Z}/2\times\mathbb{Z}/12$	$2+\sqrt{-23}$	$\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$

Consider the Atkin-Lehner involution ω on $X_0(32)$. Then $\omega(P) = P_0 \pm P$ where $P_0 = \omega(P_\infty)$. The reduction of ω modulo 3 has the same modular interpretation as over $\mathbb{Q}$. By using the additive law on $X_0(32)$, the $\omega(P)$ is calculated as listed in table 4. We can see if P corresponds to an elliptic curve with endomorphism ring $\mathbb{Z}[\sqrt{-23}]$, then $\omega(P)$ always corresponds to an elliptic curve with endomorphism ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$. If P corresponds to an elliptic curve with endomorphism ring $\mathbb{Z}[\frac{1+\sqrt{-23}}{2}]$, then $\omega(P)$ always corresponds to an elliptic curve with endomorphism ring $\mathbb{Z}[\sqrt{-23}]$

On the other hand, if P were the projection of any of those points on X_2 rational in $\mathbb{F}_{27}$, $\omega(P)$ should correspond to an elliptic curve with the same endomorphism ring as P. We have a contradiction.

□

Theorem 4.2. *There is no non-cusp point of degree 3 on* $X_1(32)$

Proof. Kenku [10] shows that $J(X_2)_{\mathbb{Q}}$ is finite of order dividing $2^9 \times 5^2$. Let K be a cubic field. Let $\wp$ be a prime in $\mathcal{O}_K$ lying above 3. If $x \in X_2(K)$, then $x_\wp$ is a cusp. We also know $Gon(X_2) > 3$. Therefore by Lemma 3.1, there is no noncuspidal cubic points on X_2.

Since γ_5^4 takes non-cusp point of degree 3 to a non cusp point of degree 3 on $X_1(32)$, we can conclude there is no non-cusp point of degree 3 on $X_1(32)$. □

4.6. **case** $X_1(27)$**.** Consider the cyclic covering $X_1(27) \longrightarrow X_0(27)$. The isomorphism class of each elliptic curve E defined over $\mathbb{F}_q$ with a point P satisfying $(\pi \pm 1)P = 0$ contributes 9 points to the reduction $\widetilde{X_1(27)}$ over $\mathbb{F}_q$.

We find that noncuspidal points on $\widetilde{X_1(27)}$ over $\mathbb{F}_{125}$ comes from elliptic curves with endomorphism ring $\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$, $\mathbb{Z}[\sqrt{-44}]$, $\mathbb{Z}[\sqrt{-11}]$ or $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.

TABLE 4. Points on the reduction of 4.1 modulo 3 which are rational over $\mathbb{F}_{27}$

P	$\omega(P)$
$P_\infty = (\infty, \infty)$	$P_0 = (1, 0)$
$P_1 = (0, -1)$	$P_2 = (0, 0)$
$P_3 = (u, u^2 + u)*$	$P_{24} = (-u^2 - u + 1, u^2)$
$P_4 = (u, -u^2 - 1)*$	$P_{23} = (-u^2 - u + 1, u^2 - u)$
$P_5 = (u + 1, u^2 - 1)*$	$P_{18} = (-u^2 - 1, u^2 - u + 1)$
$P_6 = (u + 1, -u^2 + u + 1)*$	$P_{17} = (-u^2 - 1, u^2 + u)$
$P_7 = (u - 1, u^2 - u)*$	$P_{20} = (-u^2 + u + 1, u^2 + u + 1)$
$P_8 = (u - 1, -u^2 - u + 1)*$	$P_{19} = (-u^2 + u + 1, u^2 - 1)$
$P_9 = (u^2 + 1, u)$	$P_{26} = (-u^2 - u - 1, 1)*$
$P_{10} = (u^2 + 1, u^2 - u)$	$P_{25} = (-u^2 - u - 1, -u^2 - u)*$
$P_{11} = (u^2 + u - 1, u - 1)$	$P_{22} = (-u^2 + u - 1, 1)*$
$P_{12} = (u^2 + u - 1, u^2 - 1)$	$P_{21} = (-u^2 + u - 1, -u^2 + u)*$
$P_{13} = (u^2 - u - 1, u + 1)$	$P_{16} = (-u^2, 1)*$
$P_{14} = (u^2 - u - 1, u^2 + u)$	$P_{15} = (-u^2, -u^2 + 1)*$

TABLE 5. Elliptic curves over $\mathbb{F}_{125}$

t	$t^2 - 4q$	$N(\pi + 1) = q + t + 1$	$N(\pi - 1) = q - t + 1$
9	-419	135	117
18	-176	144	108

Lemma 4.3. *Let x be a point of degree 3 on $X_1(27)$, then it does not reduce modulo 3 to any point corresponding to an elliptic curve E with endomorphism ring $\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$, $\mathbb{Z}[\sqrt{-44}]$, $\mathbb{Z}[\sqrt{-11}]$ or $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$.*

Proof. Ishii [4] showed that $X_0(27)$ has a defining equation:

$$Y^2 + 2XY + 3Y - X^3 + X^2 + 3X + 9 = 0 \tag{4.2}$$

with j-invariant given by

$$j = (A + BY)/C$$

where

$$\begin{aligned} A =& X^{19} - 12X^{18} + 27X^{16} + 441X^{15} - 1782X^{13} - 3159X^{12} + 9018X^{10} \\ & - 810X^9 - 7290X^7 + 22626X^6 - 20412X^3 + 729X + 4374 \\ B =& X^{18} + 27X^{15} - 1782X^{12} + 9018X^9 - 7290X^6 + 729 \\ C =& X^6 - 27X^3 \end{aligned}$$

Reduction modulo 5 we have

$$\begin{aligned} A =& X^{19} - 2X^{18} + 2X^{16} + X^{15} - 2X^{13} + X^{12} + 3X^{10} + X^6 - 2X^3 + 4X + 4 \\ B =& X^{18} + 2X^{15} - 2X^{12} + 3X^9 + 4 \\ C =& X^6 - 2X^3 \end{aligned}$$

For $j \neq 0$, we set $A = -\frac{1}{j-3}$ and have the following elliptic curve with $j(E) = j$

$$E : y^2 + xy = x^3 + Ax + A$$

For $j = 0$, we have the following elliptic curve with $j(E_0) = 0$

$$E_0 : y^2 + y = x^3$$

To calculate the endomorphism ring $\mathrm{End}(E)$, we use

$$\begin{aligned} \phi_2(X, Y) =& (X + Y)^3 - X^2Y^2 + 1485XY(X + Y) - 162000(X + Y)^2 \\ &+ 41097375XY + 8748000000(X + Y) - 157464000000000 \end{aligned}$$

Reduction modulo 5, we have

$$\phi_2(X, Y) = (X + Y)^3 - X^2Y^2$$

Then we can calculate $E(\mathbb{F}_{125})$ and $\mathrm{End}(E)$ as listed in Table 6.

Consider the Atkin-Lehner involution ω on $X_0(27)$. Then $\omega(P) = P_0 + P$ where $P_0 = \omega(P_\infty)$. The reduction of ω modulo 5 has the same modular interpretation as over $\mathbb{Q}$. By using the additive law on $X_0(27)$, We can see $\omega(P)$ corresponds to an elliptic curve with different endomorphism ring as P. This is a contradiction. □

Theorem 4.4. *There is no non-cusp point of degree 3 on $X_1(27)$.*

Proof. We know $X_1(27)$ is not trigonal. And by Kenku [11], $J_1(27)(\mathbb{Q})$ is finite and its order is not divisible by 5. So the argument in the case $N = 32$ works as well. □

5. Composite cases.

Since we have shown there is no torsion points of order $N = 32, 25, 27, 49, 121, 169$, it suffices to prove there are no cubic points on $X_1(N)$ for $N = 2 \cdot 13, 3 \cdot 13, 5 \cdot 13, 7 \cdot 13, 11 \cdot 13; 2 \cdot 11, 3 \cdot 11, 5 \cdot 11, 7 \cdot 11; 4 \cdot 7, 5 \cdot 7, 6 \cdot 7; 8 \cdot 5, 6 \cdot 5, 9 \cdot 5; 8 \cdot 3, 4 \cdot 9$.

5.1. case $X_1(143)$.

We have the decomposition

$$J_0(143) = A_1 \times \cdots \times A_5$$

TABLE 6. Endomorphism rings

j	$E(\mathbb{F}_{125})$	$End(E)$	$j(w(E))$	$End(w(E))$
2	$\mathbb{Z}/4\times\mathbb{Z}/36$	$\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$	$-$	
a^2+3a+2	$\mathbb{Z}/135$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+2a/3a^2+2a+4$	$\mathbb{Z}[\sqrt{-44}]$
a^2+3a+4	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$2a^2+2a+1/3a^2+4a+4$	$\mathbb{Z}[\sqrt{-44}]$
a^2+4a+2	$\mathbb{Z}/135$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+a/4a^2+4a+1$	$\mathbb{Z}[\sqrt{-44}]$
a^2+4a+4	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+2a/3a^2+2a+4$	$\mathbb{Z}[\sqrt{-44}]$
$2a^2+2a$	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+4a+4/3a^2+4a+2$	$\mathbb{Z}[\sqrt{-11}]$
$2a^2+2a+1$	$\mathbb{Z}/144$	$\mathbb{Z}[\sqrt{-44}]$	$a^2+3a+4/3a^2+3a+1$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$3a^2+2a+2$	$\mathbb{Z}/2\times\mathbb{Z}/72$	$\mathbb{Z}[\sqrt{-11}]$	$4a^2+a+4/4a^2+2a+4$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$3a^2+2a+4$	$\mathbb{Z}/108$	$\mathbb{Z}[\sqrt{-44}]$	a^2+3a+2/a^2+4a+4	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$3a^2+3a+1$	$\mathbb{Z}/135$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$3a^2+4a+4/2a^2+2a+1$	$\mathbb{Z}[\sqrt{-44}]$
$3a^2+3a+3$	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+4a+1/4a^2+a$	$\mathbb{Z}[\sqrt{-44}]$
$3a^2+4a+2$	$\mathbb{Z}/2\times\mathbb{Z}/72$	$\mathbb{Z}[\sqrt{-11}]$	$2a^2+2a/4a^2+2a+4$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$3a^2+4a+4$	$\mathbb{Z}/108$	$\mathbb{Z}[\sqrt{-44}]$	$a^2+3a+4/3a^2+3a+1$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$4a^2+a$	$\mathbb{Z}/144$	$\mathbb{Z}[\sqrt{-44}]$	$a^2+4a+2/3a^2+3a+3$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$4a^2+a+4$	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$4a^2+4a+4/3a^2+2a+2$	$\mathbb{Z}[\sqrt{-11}]$
$4a^2+2a$	$\mathbb{Z}/144$	$\mathbb{Z}[\sqrt{-44}]$	a^2+3a+2/a^2+4a+4	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$4a^2+2a+4$	$\mathbb{Z}/117$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$	$3a^2+2a+2/3a^2+4a+2$	$\mathbb{Z}[\sqrt{-11}]$
$4a^2+4a+1$	$\mathbb{Z}/108$	$\mathbb{Z}[\sqrt{-44}]$	$a^2+4a+2/3a^2+3a+3$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$
$4a^2+4a+4$	$\mathbb{Z}/2\times\mathbb{Z}/72$	$\mathbb{Z}[\sqrt{-11}]$	$2a^2+2a/4a^2+a+4$	$\mathbb{Z}[\frac{1+\sqrt{-419}}{2}]$

with $\dim A_1 = 1, \dim A_2 = 4, \dim A_3 = 6, \dim A_4 = 1, \dim A_5 = 1$, and $L(A_i, 1) \neq 0$ for $i = 2, \cdots, 5$. Take $J = A_2$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_2, \mathbb{Z}) = \mathbb{Z}^8$ as following:

$$T_1 = I_8$$

$$T_2 = \begin{pmatrix} 1 & 2 & 1 & -2 & -2 & 3 & 2 & -1 \\ 0 & 0 & 0 & 0 & 1 & 1 & -3 & -2 \\ -1 & 0 & 0 & 1 & 1 & 0 & -1 & -2 \\ 0 & 1 & 1 & 0 & -1 & 1 & 2 & -1 \\ 0 & 0 & 1 & -1 & 1 & 2 & -1 & 0 \\ 1 & 1 & 1 & -2 & -1 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & -1 & 1 & 2 & 1 \\ 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$T_3 = \begin{pmatrix} -1 & 1 & 2 & 0 & -2 & 3 & 0 & 0 \\ 2 & 0 & 0 & -1 & 1 & -3 & 2 & 0 \\ 1 & -1 & -2 & 3 & 2 & -4 & -1 & 3 \\ 0 & 0 & 2 & -1 & -1 & 2 & 0 & -1 \\ -1 & 1 & 2 & -1 & -1 & 2 & 2 & -1 \\ -1 & 0 & 2 & -1 & -1 & 3 & 0 & -2 \\ -1 & 1 & 1 & -1 & -1 & 2 & 1 & -1 \\ 1 & -1 & 0 & 0 & 1 & -2 & 0 & 1 \end{pmatrix}$$

They are linearly independent mod 3. Since $143 \nmid 3^6 - 1$ and $143 > (1 + \sqrt{3^3})^2$, then by Theorem 3.4, we are done.

5.2. **case** $X_1(91)$**.** We have the decomposition

$$J_0(91) = A_1 \times \cdots \times A_4$$

with $\dim A_1 = 1, \dim A_2 = 1, \dim A_3 = 2, \dim A_4 = 3$, and $L(A_i, 1) \neq 0$ for $i = 3, 4$. Take $J = A_4$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_4, \mathbb{Z}) = \mathbb{Z}^6$ as following:

$$T_1 = I_6, T_2 = \begin{pmatrix} 1 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 2 & 1 & 0 & -1 & 2 & -2 \\ -1 & -1 & 0 & 1 & -2 & 1 \\ -1 & -1 & 0 & -1 & 1 & -1 \\ 0 & -1 & -1 & -1 & 0 & -1 \end{pmatrix}, T_3 = \begin{pmatrix} -1 & -2 & 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 & 0 & -1 \\ 1 & 0 & -2 & 0 & 1 & -1 \\ -1 & -1 & 2 & 1 & 0 & -1 \\ 0 & -2 & 0 & 0 & -2 & 0 \\ 1 & -2 & -2 & -2 & -1 & -1 \end{pmatrix}$$

They are linearly independent mod 5. Since $91 \nmid 5^6 - 1$ and $91 < (1 - \sqrt{5^3})^2 < (1 + \sqrt{5^3})^2 < 2 \cdot 91$, then by Theorem 3.4, we are done.

5.3. **case** $X_1(65)$**.** We have the decomposition

$$J_0(65) = A_1 \times \cdots \times A_3$$

with $\dim A_1 = 1, \dim A_2 = 2, \dim A_3 = 2$, and $L(A_i, 1) \neq 0$ for $i = 2, 3$. Take $J = A_2 \times A_3$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_2 \times A_3, \mathbb{Z}) = \mathbb{Z}^4 \times \mathbb{Z}^4$ as following:

$$T_1 = I_8$$

$$T_2 = diag\left\{ \begin{pmatrix} 2 & 0 & 0 & -1 \\ 1 & -2 & 1 & -1 \\ 1 & -1 & 2 & -3 \\ 1 & 0 & 0 & -2 \end{pmatrix}, \begin{pmatrix} 1 & -2 & 0 & 0 \\ 1 & -3 & 0 & 0 \\ 1 & -1 & -2 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix} \right\}$$

$$T_3 = diag\left\{ \begin{pmatrix} -1 & 0 & 0 & 1 \\ -1 & 3 & -1 & 1 \\ -1 & 1 & -1 & 3 \\ -1 & 0 & 0 & 3 \end{pmatrix}, \begin{pmatrix} 2 & -2 & 0 & 0 \\ 1 & -2 & 0 & 0 \\ 1 & -1 & -1 & 1 \\ 0 & -1 & 1 & 1 \end{pmatrix} \right\}$$

They are linearly independent mod 3. Since $65 \nmid 3^6 - 1$ and $65 > (1 + \sqrt{3^3})^2$, then by Theorem 3.4, we are done.

5.4. **case** $X_1(77)$**.** We have the decomposition

$$J_0(77) = A_1 \times \cdots \times A_6$$

with $\dim A_1 = \dim A_2 = \dim A_3 = \dim A_5 = \dim A_6 = 1, \dim A_4 = 2$, and $L(A_i, 1) \neq 0$ for $i = 2, \cdots, 6$. Take $J = A_4 \times A_5$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_4 \times A_5, \mathbb{Z}) = \mathbb{Z}^4 \times \mathbb{Z}^2$ as

following:

$$T_1 = I_6$$

$$T_2 = diag\left\{\left(\begin{array}{cccc} 0 & 2 & -1 & -2 \\ 2 & -1 & 0 & -2 \\ 1 & -2 & 2 & -2 \\ -1 & 0 & -1 & -1 \end{array}\right), \left(\begin{array}{cc} -2 & 0 \\ 0 & -2 \end{array}\right)\right\}$$

$$T_3 = diag\left\{\left(\begin{array}{cccc} 1 & -2 & 1 & 2 \\ -2 & 2 & 0 & 2 \\ -1 & 2 & -1 & 2 \\ 1 & 0 & 1 & 2 \end{array}\right), \left(\begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array}\right)\right\}$$

They are linearly independent mod 3. Since $77 \nmid 3^6 - 1$ and $77 > (1 + \sqrt{3^3})^2$, then by Theorem 3.4, we are done.

5.5. **case** $X_1(55)$**.** We have the decomposition

$$J_0(55) = A_1 \times \cdots \times A_4$$

with $\dim A_1 = \dim A_3 = \dim A_4 = 1, \dim A_2 = 2$, and $L(A_i, 1) \neq 0$ for $i = 1, \cdots, 4$. Take $J = A_2 \times A_3$. T_1, T_2, T_3 acts on $H_1(J, \mathbb{Z}) \cong H_1(A_2 \times A_3, \mathbb{Z}) = \mathbb{Z}^4 \times \mathbb{Z}^2$ as following:

$$T_1 = I_6$$

$$T_2 = diag\left\{\left(\begin{array}{cccc} 1 & 0 & -1 & 2 \\ -2 & -1 & 2 & -2 \\ -2 & -2 & 3 & 0 \\ 0 & -1 & 1 & 1 \end{array}\right), \left(\begin{array}{cc} -2 & 0 \\ 0 & -2 \end{array}\right)\right\}$$

$$T_3 = diag\left\{\left(\begin{array}{cccc} 0 & 0 & 2 & -4 \\ 4 & 4 & -4 & 4 \\ 4 & 4 & -4 & 0 \\ 0 & 2 & -2 & 0 \end{array}\right), \left(\begin{array}{cc} -1 & 0 \\ 0 & -1 \end{array}\right)\right\}$$

They are linearly independent mod 3. Since $55 \nmid 3^6 - 1$ and $55 > (1 + \sqrt{3^3})^2$, then by Theorem 3.4, we are done.

5.6. **case** $X_1(40)$**.** $J_1(40)$ has decomposition:

$$J_1(40) \longrightarrow A_1 \times \cdots \times A_9$$

where A_i has dimensions: $1, 1, 1, 4, 2, 2, 8, 2, 4$ and $L(A_i, 1) \neq 0$ for all i. So $J_1(40)(\mathbb{Q})$ is finite.

Let K be a cubic field. Let $\wp$ be a prime in $\mathcal{O}_K$ lying above 3. Suppose $x = (E, P) \in X_1(40)(K)$. Since $40 > (1 + \sqrt{3^3})^2$, then $x_\wp$ is a cusp. We also know $Gon(X_1(40) > 3$. Therefore by Lemma 3.1, there are no noncuspidal cubic points on $X_1(40)$.

5.7. **case** $X_1(22)$**.** $J_1(22)$ has decomposition:

$$J_1(22) \longrightarrow A_1 \times A_2 \times A_3$$

where A_i has dimensions: $1, 1, 4$ and $L(A_i, 1) \neq 0$ for all i. So $J_1(22)(\mathbb{Q})$ is finite.

We have $22 < (1+\sqrt{3^3})^2 \approx 38.4$. So we need to show any elliptic curve E over $k = \mathbb{F}_{27}$ can not have an k-rational points P of order 22. Suppose $E(k)$ has a point of order 22, then $E(k) \cong \mathbb{Z}/22\mathbb{Z}$ since $22m > (1+\sqrt{3^3})^2$ for any $m > 1$. But by Theorem 2.1, $E(k) \ncong \mathbb{Z}/22\mathbb{Z}$.

Let K be a cubic field. Let $\wp$ be a prime in $\mathcal{O}_K$ lying above 3. If $x = (E, P) \in X_1(22)(K)$, then $x_\wp$ is a cusp. We also know $Gon(X_1(22)) > 3$. Therefore by Lemma 3.1, there are no noncuspidal cubic points on $X_1(22)$.

5.8. **case** $X_1(24)$**.**

Lemma 5.1. *Let E be an elliptic curve (over a field k with base point O) and φ an involution on E. Then either $\varphi(P) = Q + P$ for a point $Q \in E$ of order 2, or $\varphi(P) = Q - P$ for some point $Q \in E$.*

Proof. By Silverman [23, III.4.7], Every morphism φ can be written as $\varphi = \tau_Q\phi$, where ϕ is an isogeny and τ_Q is translation by $Q \in E$. If φ is an involution with $\varphi = \tau_Q\phi$, then it is an automorphism, i.e. $\varphi \in Aut(E)$. So $\phi \in Aut(E, O)$. We have

$$Id = \varphi^2 = (\tau_Q\phi)^2 = \tau_Q(\phi\tau_Q)\phi = \tau_Q(\tau_{\phi(Q)}\phi)\phi = \tau_{Q+\phi(Q)}\phi^2$$

Take the value of O, we have

$$O = Id(O) = \tau_{Q+\phi(Q)}\phi^2(O) = \tau_{Q+\phi(Q)}(O) = Q + \phi(Q)$$

This means $\tau_{Q+\phi(Q)} = Id$, hence $\phi^2 = Id$.

Consider the structure of $Aut(E, O)$

$$Aut(E,O) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & j(E) \neq 0, 1728 \\ \mathbb{Z}/4\mathbb{Z}, & j(E) = 0, & char(k) \neq 2, 3 \\ \mathbb{Z}/6\mathbb{Z}, & j(E) = 1728, & char(k) \neq 2, 3 \\ SL_2(\mathbb{F}_3), & j(E) = 0 = 1728, & char(k) = 2 \\ \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}, & j(E) = 0 = 1728, & char(k) = 3 \end{cases}$$

we see there is only one element in $Aut(E, O)$ of order 2. Therefore, $\phi = \pm Id$.

If $\phi = Id$, then $\varphi(P) = Q + P$ for a point $Q \in E$ of order 2. If $\phi = -Id$, then $\varphi(P) = Q - P$ for some point $Q \in E$. □

Consider the cyclic covering $X_1(24) \longrightarrow X_0(24)$. The isomorphism class of each elliptic curve E defined over $\mathbb{F}_q$ with a point P satisfying $(\pi \pm 1)P = 0$ contributes 4 points to the reduction $\widetilde{X_1(24)}$ over $\mathbb{F}_q$.

TABLE 7. Elliptic curves over $\mathbb{F}_{7^3}$

t	$t^2 - 4q$	$N(\pi + 1) = q + t + 1$	$N(\pi - 1) = q - t + 1$
8	-1308	352	$24 \cdot 14$
16	-1116	$24 \cdot 15$	328
32	-348	376	$24 \cdot 13$

We find that noncuspidal points on $\widetilde{X_1(24)}$ over $\mathbb{F}_{7^3}$ comes from elliptic curves with endomorphism ring $\mathbb{Z}[\sqrt{-1308}]$, $\mathbb{Z}[\frac{1+\sqrt{-327}}{2}]$, $\mathbb{Z}[\sqrt{-1116}]$, $\mathbb{Z}[\frac{1+\sqrt{-279}}{2}]$, $\mathbb{Z}[\sqrt{-124}]$, $\mathbb{Z}[\frac{1+\sqrt{-31}}{2}]$, $\mathbb{Z}[\sqrt{-348}]$, $\mathbb{Z}[\frac{1+\sqrt{-87}}{2}]$.

Lemma 5.2. *Let x be a point of degree 3 on $X_1(24)$, then it does not reduce modulo 7 to any point corresponding to an elliptic curve E with endomorphism ring $\mathbb{Z}[\sqrt{-1308}]$, $\mathbb{Z}[\frac{1+\sqrt{-327}}{2}]$, $\mathbb{Z}[\sqrt{-1116}]$, $\mathbb{Z}[\frac{1+\sqrt{-279}}{2}]$,$\mathbb{Z}[\sqrt{-124}]$, $\mathbb{Z}[\frac{1+\sqrt{-31}}{2}]$,$\mathbb{Z}[\sqrt{-348}]$, $\mathbb{Z}[\frac{1+\sqrt{-87}}{2}]$.*

Proof. Ishii [4] showed that $X_0(24)$ has a defining equation:

$$Y^2 + 4Y - X^3 - 2X^2 + 3X + 4 = 0 \tag{5.1}$$

with j-invariant given by

$$j = (A + BY)/C$$

where

$$\begin{aligned} A =& (X^2 - 3)^3(X^6 - 9X^4 + 3X^2 - 3)^3 \\ B =& 0 \\ C =& X^4(X^2 - 9)(X^2 - 1)^3 \end{aligned}$$

For $j \neq 0$, we set $A = -\frac{1}{j-3}$ and have the following elliptic curve with $j(E) = j$

$$E : y^2 + xy = x^3 + Ax + A$$

For $j = 0$, we have the following elliptic curve with $j(E_0) = 0$

$$E_0 : y^2 + y = x^3$$

To calculate the endomorphism ring End(E), we use

$$\begin{aligned} \phi_2(X, Y) =& (X + Y)^3 - X^2Y^2 + 1485XY(X + Y) - 162000(X + Y)^2 \\ &+ 41097375XY + 8748000000(X + Y) - 157464000000000 \end{aligned}$$

Then we can calculate $E(\mathbb{F}_{7^3})$ and End(E).

Consider the Atkin-Lehner involution $\omega_i, i = 3, 8, 24$ on $X_0(24)$. By Lemma 5.1, we have $\omega_i(P) = P_i \pm P$ where $P_i = \omega_i(P_\infty)$. We claim that at least one of them takes the positive sign. Actually, suppose both ω_3 and ω_8 take the negative sign, i.e. $\omega_3(P) = P_3 - P$ and $\omega_8(P) = P_8 - P$. Then

$$\omega_{24}(P) = \omega_3 \circ \omega_8(P) = \omega_3(P_8 - P) = P_3 - (P_8 - P) = (P_3 - P_8) + P$$

Denote this involution as ω. Then $\omega(P) = Q + P$ for some point Q of order 2. We have 3 points on $(\widetilde{X_0(24)})(\mathbb{F}_{7^3})$ of order 2. They are $(0, -2), (1, -2)$ and $(4, -2)$.

The reduction of ω_i modulo 7 has the same modular interpretation as over $\mathbb{Q}$. By using the additive law on $X_0(24)$, We can see $\omega(P)$ corresponds to an elliptic curve with different endomorphism ring from that of P. This is a contradiction.

□

Theorem 5.3. *There is no non-cusp point of degree 3 on $X_1(24)$*

TABLE 8. Atkin-Lehner involution on $X_0(24)$ over $\mathbb{F}_{7^3}$.

P, (6 points)	$(0,-2)+P$	$(1,-2)+P$	$(4,-2)+P$
$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}$	$\mathbb{Z}/364\mathbb{Z}$	$\mathbb{Z}/370\mathbb{Z}$	$\mathbb{Z}/359\mathbb{Z}$
$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/120\mathbb{Z}$	$\mathbb{Z}/364\mathbb{Z}$	$\mathbb{Z}/359\mathbb{Z}$	$\mathbb{Z}/370\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/322\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/366\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/322\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/314\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/114\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/160\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/353\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/367\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/357\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/314\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/357\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/366\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/353\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/160\mathbb{Z}$
$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/156\mathbb{Z}$	$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/114\mathbb{Z}$	$\mathbb{Z}/342\mathbb{Z}$	$\mathbb{Z}/367\mathbb{Z}$

Proof. We know $X_1(24)$ is not trigonal. And $J_1(24)(\mathbb{Q})$ has decomposition:

$$J_1(24)(\mathbb{Q}) \longrightarrow A_1 \times A_2 \times A_3$$

with A_i of dimension 1, 2, 2. And $L(A_i, 1) \neq 0$ for all i which means $J_1(24)(\mathbb{Q})$ is finite. So the argument in $N = 32$ case works as well. □

Acknowledgements. The author would like to thank Prof. Sheldon Kamienny for introducing me to this research topic and for providing many valuable ideas and insightful comments throughout the research. The author would also like to thank Andrew Sutherland at MIT for pointing out several minor errors in an earlier version of this paper.

REFERENCES

[1] Deuring, Max *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* (German) Abh. Math. Sem. Hansischen Univ. 14, (1941). 197-272.

[2] Drinfel'd, V. G. *Two theorems on modular curves.* (Russian) Funkcional. Anal. i Priložen. 7 (1973), no. 2, 83-84.

[3] Igusa, Jun-ichi *Kroneckerian model of fields of elliptic modular functions.* Amer. J. Math. 81 1959 561-577.

[4] Ishii, Noburo *Rational expression for j-invariant function in terms of generators of modular function fields.* Int. Math. Forum 2 (2007), no. 37-40, 1877-1894.

[5] Jeon, Daeyeol; Kim, Chang Heon; Schweizer, Andreas *On the torsion of elliptic curves over cubic number fields.* Acta Arith. 113 (2004), no. 3, 291-301.

[6] Kamienny, S. *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. 109 (1992), no. 2, 221-229.

[7] Kamienny, S. *Torsion points on elliptic curves over fields of higher degree.* Internat. Math. Res. Notices 1992, no. 6, 129-133.

[8] Kamienny, S. *On the local boundedness of torsion in elliptic curves.* MSRI Preprint No. 036-94 (1994)

[9] Kazuya Kato. *p-adic Hodge theory and values of zeta functions of modular forms.* Astérisque, (295):ix, 117290, 2004. ISSN 0303-1179. Cohomologies p-adiques et applications arithmétiques. III.

[10] Kenku, M. A. *Certain torsion points on elliptic curves defined over quadratic fields.* J. London Math. Soc. (2) 19 (1979), no. 2, 233-240.

[11] Kenku, M. A. *Rational torsion points on elliptic curves defined over quadratic fields.* J. Nigerian Math. Soc. 2 (1983), 1-16.

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

[13] Kodaira, K. *On the structure of compact complex analytic surfaces. I.* Amer. J. Math. 86 1964 751-798.

[14] Kodaira, K. *On the structure of compact complex analytic surfaces. II.* Amer. J. Math. 88 1966 682-721.

[15] Kohel, David Russell *Endomorphism rings of elliptic curves over finite fields.* Thesis (Ph.D.)-University of California, Berkeley. 1996. 117 pp. ISBN: 978-0591-32123-4, ProQuest LLC

[16] Kolyvagin, V. A.; Logachev, D. Yu. *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. (Russian)* Algebra i Analiz 1 (1989), no. 5, 171–196; translation in Leningrad Math. J. 1 (1990), no. 5, 1229-1253

[17] Manin, Ju. I. *Parabolic points and zeta functions of modular curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 19-66.

[18] Mazur, B. *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33-186 (1978).

[19] Najman, F. *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(N)$. Math. Res. Letters. To appear.

[20] Néron, André *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux.* (French) Inst. Hautes Études Sci. Publ.Math. No. 21 1964 128 pp.

[21] Parent, Pierre *No 17-torsion on elliptic curves over cubic number fields.* J. Théor. Nombres Bordeaux 15 (2003), no. 3, 831-838.

[22] Shimura, Goro *Introduction to the arithmetic theory of automorphic functions.* Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. xiv+267 pp.

[23] Silverman, Joseph H. *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9

[24] Silverman, Joseph H. *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994. xiv+525 pp. ISBN: 0-387-94328-5

[25] Tate, John; Oort, Frans *Group schemes of prime order.* Ann. Sci. École Norm. Sup. (4) 3 1970 1-21.

[26] Waterhouse, William C. *Abelian varieties over finite fields.* Ann. Sci. École Norm. Sup. (4) 2 1969 521-560.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089, USA
E-mail address: wang50@usc.edu,blandye@gmail.com