ON THE CYCLIC TORSION OF ELLIPTIC CURVES OVER CUBIC NUMBER FIELDS (III)

JIANG ANG

ABSTRACT. This is the third part of a series of papers discussing the cyclic torsion subgroup of elliptic curves over cubic number fields. For $N = 39$, we show that $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{\text{tor}}$ for any elliptic curve $E$ over a cubic number field $K$.

In [12], the author conjectured that $\mathbb{Z}/N\mathbb{Z}$ is not a cyclic torsion subgroup of the Mordell-Weil group of any elliptic curve over a cubic number field for 24 values of $N$: 22, 24, 25, 26, 27, 28, 30, 32, 33, 35, 36, 39, 40, 42, 45, 49, 55, 63, 65, 77, 91, 121, 143, 169.

The cases $N = 55, 65, 77, 91, 143, 169$ were proved in the first part [12] of this series of papers using refinements of a criterion originally due to Kamienny. The cases $N = 22, 25, 40, 49$ were proved in the second part [13] of this series of papers with the help of Kato’s result about the Birch and Swinnerton-Dyer conjecture on modular abelian varieties. In this paper, we prove the $N = 39$ case, which is

Theorem 0.3.

Let $N$ be a positive integer. Throughout this paper, $X_1(N)$ (resp. $X_0(N)$) denotes the modular curve over $\mathbb{Q}$ associated to the congruence subgroup $\Gamma_1(N)$ (resp. $\Gamma_0(N)$). $Y_1(N)$ (resp. $Y_0(N)$) denotes the corresponding affine curve without cusps. $J_1(N)$ (resp. $J_0(N)$) denotes the Jacobian of $X_1(N)$ (resp. $X_0(N)$).

Let $X_0(N)^{(d)}$ be the $d$-th symmetric power of $X_0(N)$. Suppose $K$ is a number field of degree $d$ over $\mathbb{Q}$ and $x \in X(K)$. Let $x_1, \ldots, x_d$ be the images of $x$ under the distinct embeddings $\tau_i : K \rightarrow \mathbb{C}, 1 \leq i \leq d$. Define

$$\Phi : X_0(N)^{(d)} \rightarrow J_0(N)$$

by $\Phi(P_1 + \cdots + P_d) = [P_1 + \cdots + P_d - d\mathfrak{x}]$ where $[ \ ]$ denotes the divisor class.

Any point of $Y_1(N)$ is represented by $(E, \pm P)$, where $E$ is an elliptic curve and $P \in E$ is a point of order $N$. Any point of $Y_0(N)$ is represented by $(E, C)$, where $E$ is an elliptic curve and $C \subset E$ is a cyclic subgroup of order $N$. The covering map $\pi : X_1(N) \rightarrow X_0(N)$ sends $(E, \pm P)$ to $(E, \langle P \rangle)$, where $\langle P \rangle$ is the cyclic subgroup generated by $P$.

Let $K$ be a number field with ring of integers $\mathcal{O}_K$, $\varphi \subset \mathcal{O}_K$ a prime ideal lying above $p$, $k = \mathbb{F}_q = \mathcal{O}_K/\varphi$ its residue field. Let $A$ be an abelian variety over $K$ and $P \in A(K)$ a point of order $N$. Let $\tilde{A}$ be the fibre over $k$ of the Néron model of $A$.
and let $\tilde{P} \in \tilde{A}(k)$ be the reduction of $P$. The following lemma (see, for instance, \cite{Li} §7.3 Proposition 3) shows that $\tilde{P}$ has order $N$ when $p \nmid N$.

**Lemma 0.1.** Let $m$ be a positive integer relatively prime to $\text{char}(k)$. Then the reduction map $A(K)[m] \rightarrow \tilde{A}(k)$ is injective.

For a square-free $N$, the order $h_0(N)$ of $J_0(N)^c$ can be calculated by the following formula due to Takagi \cite{11}:

\begin{equation}
(0.1) 
 h_0(N) = \frac{2^f 12a_2a_3}{d} \prod_{\chi \neq 1} \frac{1}{24} \prod_{p|N} (p + \chi([p]))
\end{equation}

where $f$ is the number of the prime factors of $N = p_1 \cdots p_f$, $d = (12, p_1 - 1, \cdots, p_f - 1)$, $a_2 = 2$ if $2|N$ and $N$ has a prime factor $p$ with $p \equiv 3$ mod 4, $a_2 = 1$ otherwise, $a_3 = 3$ if $3|N$ and $N$ has a prime factor $p$ with $p \equiv 2$ mod 3, $a_3 = 1$ otherwise, $\chi$ runs through all nontrivial characters of the group $T$ (consisting of all the positive divisors of $N$ and isomorphic to $(\mathbb{Z}/2\mathbb{Z})^f$) and $p$ runs through all prime factors of $N$.

Of the remaining 14 cases of $N$, 6 are square-free. The order $h_0(N)$ of $J_0(N)^c$ is calculated and listed in Table 1.

| $N$   | 26  | 30  | 33  | 35  | 39  | 42  |
|-------|-----|-----|-----|-----|-----|-----|
| $h_0(N)$ | $3 \cdot 7$ | $2^6 \cdot 3$ | $2^4 \cdot 5^2$ | $2^4 \cdot 3$ | $2^3 \cdot 7$ | $2^8 \cdot 3^2$ |

The following specialization lemma follows from the classification of Oort-Tate \cite{10} on finite flat group schemes of rank $p$ (or more generally the classification of finite flat group schemes of type $(p, \cdots, p)$ by Raynaud \cite{9}). If the group scheme is contained in an abelian variety, this lemma follows from elementary properties of formal Lie groups (see, for example, the Appendix of Katz\cite{5}).

**Lemma 0.2 (Specialization Lemma).** Let $K$ be a number field. Let $\wp \subset O_K$ be a prime above $p$. Let $A/K$ be an abelian variety. Suppose the ramification index $e_\wp(K/Q) < p - 1$. Then the reduction map $\Psi : A(K)_{\text{tor}} \rightarrow A(\overline{\mathbb{F}_p})$ is injective.

Using the same method as that in \cite{13} to show the finiteness of $J_1(N)(\mathbb{Q})$, we can verify that $J_0(N)(\mathbb{Q})$ is finite for certain $N$. For the 24 cases we are interested in, Table 2 is the result of calculations in Magma \cite{6}. The second column $t$ is the number of non-isogenous modular abelian varieties in the decomposition $J_0(N) = \bigoplus_{i=1}^t A_i^{m_i}$. The third column list the dimension $d_i$ and multiplicity $m_i$ of each $A_i$ (we omit $m_i$ if $m_i = 1$). The fourth column verifies non-vanishing of $L$-series at 1 (a mark $T$ means $L(A_i, 1) \neq 0$ is verified, otherwise we place a mark $F$).

**Theorem 0.3.** If $N = 39$, then $\mathbb{Z}/N\mathbb{Z}$ is not a subgroup of $E(K)_{\text{tor}}$ for any elliptic curve $E$ over a cubic number field $K$. 
Table 2. Decomposition of $J_0(N)$

| $N$  | $t$ | $d_i(m_i)$ | $L(A_i, 1) \neq 0$ |
|------|-----|------------|------------------|
| 169  | 3   | 2, 3, 3    | $T, F, T$        |
| 121  | 6   | 1, 1, 1, 1, 1 | $F, T, T, T, T, T$ |
| 49   | 1   | 1          | $T$              |
| 25   | 1   | 0          | $-$              |
| 27   | 1   | 1          | $T$              |
| 32   | 1   | 1          | $T$              |
| 143  | 5   | 1, 4, 6, 1, 1 | $F, T, T, T, T$ |
| 91   | 4   | 1, 1, 2, 3 | $F, F, T, T$    |
| 65   | 3   | 1, 2, 2   | $F, T, T$       |
| 39   | 2   | 1, 2      | $T, T$          |
| 26   | 2   | 1, 1      | $T, T$          |
| 77   | 6   | 1, 1, 2, 1, 1 | $F, T, T, T, T, T$ |
| 55   | 4   | 1, 2, 1, 1 | $T, T, T$      |
| 33   | 3   | 1, 1, 1   | $T, T, T$      |
| 22   | 2   | 1, 1      | $T, T$         |
| 35   | 2   | 1, 2      | $T, T$         |
| 63   | 4   | 1, 2, 1, 1 | $T, T, T, T$   |
| 42   | 5   | 1, 1, 1, 1, 1 | $T, T, T, T, T$ |
| 28   | 2   | 1, 1      | $T, T$        |
| 45   | 3   | 1, 1, 1   | $T, T, T$      |
| 30   | 3   | 1, 1, 1   | $T, T, T$      |
| 40   | 3   | 1, 1, 1   | $T, T, T$      |
| 36   | 1   | 1          | $T$            |
| 24   | 1   | 1          | $T$            |

Proof. Let $p = 3$ and $N' = N/p$. Let $K$ be a cubic field and $\wp$ a prime of $K$ over $p$. As shown in the proof of Lemma 3.6 of [12], we can always choose $\wp$ such that the residue field $k = O_K/\wp$ has degree 1 or 3 over $F_p$. Suppose $x = \pi(E, \pm P) \in Y_0(N)(K)$, then $E$ cannot have additive reduction since $N > 4$.

If $k$ has degree 3, then $e_{\wp}(K/Q) = 1 < p - 1$, by Lemma [12] $E$ has multiplicative reduction since $N > (1 + \sqrt{3})^2$. If $k$ has degree 1, by Lemma 0.1 $E$ also has multiplicative reduction since $N' > (1 + \sqrt{3})^2$.

Since $E$ has multiplicative reduction at $\wp$, then $x$ specializes to a cusp of $\tilde{X}_0(N)$. Recall the notation of $\tau_i$ and $x_i$, $1 \leq i \leq 3$. Then $\tau_i(K)$ is also a cubic field with prime ideal $\tau_i(\wp)$ over $p$ and residue field $k_i = k$. And $\tau_i(E)$ also has multiplicative reduction at $\tau_i(\wp)$. This means all the images $x_1, x_2, x_3$ of $x$ specialize to cusps of $\tilde{X}_0(N)$. Let $c_1, c_2, c_3$ be the cusps such that

$$x_i \otimes \mathbb{F}_p = c_i \otimes \mathbb{F}_p, \quad 1 \leq i \leq 3$$

We know all the cusps of $X_0(N)$ are defined over $\mathbb{Q}(\zeta_N)$ [8]. As is seen in Table 1 the order of $J_0(N)^\vee$ is $2^3 \cdot 7$. Therefore by Lemma 0.1 the specialization map

$$\Psi : J_0(N)(\mathbb{Q}(\zeta_N))_{tor} \longrightarrow J_0(N)(\mathbb{F}_p)$$

is injective.
We know $x_1 + x_2 + x_3$ is $\mathbb{Q}$-rational. The data in Table 2 show the finiteness of $J_0(N)(\mathbb{Q})$. So $[x_1 + x_2 + x_3 - 3\infty]$ is in $J_0(N)(\mathbb{Q}(\zeta_N))_{\text{tor}}$. By a theorem of Manin [7] and Drinfeld [2], the difference of two cusps of $X_0(N)$ has finite order in $J_0(N)$. So $[c_1 + c_2 + c_3 - 3\infty]$ is also in $J_0(N)(\mathbb{Q}(\zeta_N))_{\text{tor}}$. Therefore

$$\Psi([x_1 + x_2 + x_3 - 3\infty]) = \Psi([c_1 + c_2 + c_3 - 3\infty])$$

implies

$$[x_1 + x_2 + x_3 - 3\infty] = [c_1 + c_2 + c_3 - 3\infty]$$

Since $X_0(N)$ is not trigonal [4], then similar reasoning as in the proof of Proposition 1 in Frey [3] shows that $x_1 + x_2 + x_3 = c_1 + c_2 + c_3$. This is a contradiction because we assume $x$ is a noncuspidal point.

\[\square\]

\textbf{References}

[1] S. Bosch, W. Lütkebohmert & M. Raynaud, \textit{Néron models.} Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 21, Springer-Verlag, Berlin, 1990.

[2] V. G. Drinfeld, \textit{Two theorems on modular curves.} Funkcional. Anal. i Priložen. 7 (1973), no. 2, 83–84.

[3] G. Frey, \textit{Curves with infinitely many points of fixed degree.} Israel J. Math. 85 (1994), no. 1–3, 79–83.

[4] Y. Hasegawa & M. Shimura, \textit{Trigonal modular curves.} Acta Arith. 88 (1999), no. 2, 129–140.

[5] N. M. Katz, \textit{Galois properties of torsion points on abelian varieties.} Invent. Math. 62 (1981), no. 3, 481–502.

[6] Magma: \url{http://magma.maths.usyd.edu.au/magma/}

[7] Y. I. Manin, \textit{Parabolic points and zeta functions of modular curves.} Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 19–66.

[8] A. P. Ogg, \textit{Rational points on certain elliptic modular curves.} Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), pp. 221–231. Amer. Math. Soc., Providence, R.I., 1973.

[9] M. Raynaud, \textit{Schémas en groupes de type \((p, \ldots, p)\).} Bull. Soc. Math. France 102 (1974), 241–280.

[10] J. Tate & F. Oort, \textit{Group schemes of prime order.} Ann. Sci. École Norm. Sup. (4) 3 (1970), 1–21.

[11] T. Takagi, \textit{The cuspidal class number formula for the modular curves $X_0(M)$ with $M$ square-free.} J. Algebra 193 (1997), 180–213.

[12] J. Wang, \textit{On the cyclic torsion of elliptic curves over cubic number fields.} J. Number Theory 183 (2018), 291–308.

[13] J. Wang, \textit{On the cyclic torsion of elliptic curves over cubic number fields (II).} The Journal de Théorie des Nombres de Bordeaux 31 (2019), 663–670.

JIAN WANG, \textit{College of Mathematics, Jilin Normal University, Siping, Jilin 136000, China}

\textit{E-mail address:} blandye@gmail.com