RATIONAL TORSION POINTS ON JACOBIANS OF MODULAR CURVES

HWAJONG YOO

ABSTRACT. Let $p$ be a prime greater than 3. Consider the modular curve $X_0(3p)$ over $\mathbb{Q}$ and its Jacobian variety $J_0(3p)$ over $\mathbb{Q}$. Let $T(3p)$ and $C(3p)$ be the group of rational torsion points on $J_0(3p)$ and the cuspidal group of $J_0(3p)$, respectively. We prove that the 3-primary subgroups of $T(3p)$ and $C(3p)$ coincide unless $p \equiv 1 \pmod{9}$ and $3^{p-1} \not\equiv 1 \pmod{p}$.

CONTENTS

1. Introduction 1
2. Eisenstein ideals of level $pq$ 3
3. Case where $\ell$ does not divide $pq$ 5
4. Case where $\ell = p$ or $\ell = q$ 6
References 7

1. INTRODUCTION

Let $N$ be a square-free integer. Consider the modular curve $X_0(N)$ and its Jacobian variety $J_0(N) = \text{Pic}^0(X_0(N))$. Let $T(N)$ denote the group of rational torsion points on $J_0(N)$ and let $C(N)$ denote the cuspidal group of $J_0(N)$. By Manin and Drinfeld [Dri73, Man72], we have $C(N) \subseteq T(N)$ and they are both finite abelian groups.

When $N$ is prime, Ogg conjectured that $T(N) = C(N)$ [Ogg75, Conjecture 2]. In his article [Maz77], Mazur proved this conjecture by studying the Eisenstein ideal of level $N$. Recently, Ohta proved a generalization of the result of Mazur [Oht14]. More precisely, he proved the following.

Theorem 1.1 (Ohta). For a prime $\ell \geq 5$, we have $T(N)[\ell^\infty] = C(N)[\ell^\infty]$. Moreover, if 3 does not divide $N$, then $T(N)[3^\infty] = C(N)[3^\infty]$.

(For a finite abelian group $A$, $A[\ell^\infty]$ denotes the $\ell$-primary subgroup of $A$.)
We briefly sketch the proof of this theorem. Let $T_r$ (resp. $U_p$ and $w_p$) denote the $r$-th Hecke operator (resp. the $p$-th Hecke operator and the Atkin-Lehner operator with respect to $p$) acting on $J_0(N)$ for a prime $r$ not dividing $N$ (resp. a prime divisor $p$ of $N$). Let $\mathbb{T}(N)$ (resp. $\mathbb{T}(N)'$) be the $\mathbb{Z}$-subalgebra of $\text{End}(J_0(N))$ generated by $T_r$'s and $U_p$'s (resp. $T_r$'s and $w_p$'s) for primes $r \nmid N$ and $p \mid N$. Let 

$$\mathcal{I}_0 := (T_r - r - 1 : \text{for primes } r \nmid N)$$

be the (minimal) Eisenstein ideal of $\mathbb{T}(N)$ (or $\mathbb{T}(N)'$). Then, $\mathcal{I}_0$ annihilates $\mathbb{T}(N)$ and $\mathcal{C}(N)$ by the Eichler-Shimura relation. Thus, $\mathbb{T}(N)[\ell^{\infty}]$ is a module over $\mathbb{T}(N)_\ell/\mathcal{I}_0$ (or $\mathbb{T}(N)_\ell'/\mathcal{I}_0'$), where $\mathbb{T}(N)_\ell := \mathbb{T}(N) \otimes \mathbb{Z}_\ell$. Note that since $w_p^2 = 1$, for a prime $\ell \geq 3$ we have the following decomposition:

$$\mathbb{T}(N)_\ell/\mathcal{I}_0 = \prod_{M \mid N, M \neq N} \mathbb{T}(N)_\ell'/\mathcal{I}_M,$$

where $\mathcal{I}_M := (w_p - 1, w_q + 1, \mathcal{I}_0 : \text{for primes } p \mid M \text{ and } q \mid N/M)$. Thus, we have 

$$\mathbb{T}(N)[\ell^{\infty}] = \bigoplus \mathbb{T}(N)[\ell^{\infty}][\mathcal{I}_M] \text{ and } \mathcal{C}(N)[\ell^{\infty}] = \bigoplus \mathcal{C}(N)[\ell^{\infty}][\mathcal{I}_M].$$

Finally, he proved that $\mathbb{T}(N)[\ell^{\infty}][\mathcal{I}_M] = \mathcal{C}(N)[\ell^{\infty}][\mathcal{I}_M]$ by computing the index of $\mathcal{I}_M$.

In this paper, we discuss the case where $N = pq$ for two distinct primes $p$ and $q$. In contrast to the discussion above, we use $\mathbb{T}(pq)$ instead of $\mathbb{T}(pq)'$ and hence the corresponding decomposition of $\mathbb{T}(pq)/\mathcal{I}_0$ as above does not always exist. (However, other computations are relatively easier than the method by Ohta.) When $\ell$ satisfies some conditions, we get the similar decomposition of the quotient ring $\mathbb{T}(pq)/\mathcal{I}_0$ and we can prove the following.

**Theorem 1.2** (Main Theorem). For a prime $\ell$ not dividing $2pq \gcd(p - 1, q - 1)$, we have $\mathbb{T}(pq)[\ell^{\infty}] = \mathcal{C}(pq)[\ell^{\infty}]$. Moreover, $\mathbb{T}(pq)[p^{\infty}] = \mathcal{C}(pq)[p^{\infty}]$ if one of the following holds:

1. $p \geq 5$ and $\begin{cases} \text{either } q \not\equiv 1 \pmod{p} \text{ or } \\ q \equiv 1 \pmod{p} \text{ and } p^{\frac{q-1}{2}} \not\equiv 1 \pmod{q}. \end{cases}$

2. $p = 3$ and $\begin{cases} \text{either } q \not\equiv 1 \pmod{9} \text{ or } \\ q \equiv 1 \pmod{9} \text{ and } 3^{\frac{p-1}{2}} \not\equiv 1 \pmod{q}. \end{cases}$

Note that most cases are special ones of Theorem 1.1. The new result is as follows:

**Theorem 1.3.** Let $p$ be a prime greater than 3. Assume that either $p \not\equiv 1 \pmod{9}$ or $3^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. Then, we get 

$$\mathbb{T}(3p)[3^{\infty}] = \mathcal{C}(3p)[3^{\infty}].$$
1.1. **Notation.** For $x = a/b \in \mathbb{Q}$, we denote by $\text{num}(x)$ the numerator of $x$, i.e.,
\[
\text{num}(x) := \frac{a}{(a, b)}.
\]

From now on, we denote by $\ell^\alpha := \ell^{\alpha(p, q, \ell)}$ (resp. $\ell^\beta := \ell^{\beta(p, q, \ell)}$) the exact power of $\ell$ dividing
\[
M_p := \text{num}\left(\frac{(p-1)(q^2-1)}{3}\right) \quad \text{(resp. num}\left(\frac{(p^2-1)(q-1)}{3}\right)\right).
\]

2. **Eisenstein ideals of level $pq$**

Throughout this section, we fix distinct primes $p$ and $q$; and $\ell$ denotes a prime not dividing $2pq(q-1)$. Let $\mathcal{T} := \mathcal{T}(pq)$ and $\mathcal{T}_\ell := \mathcal{T}(pq) \otimes \mathbb{Z}_{\ell}$. We say an ideal of $\mathcal{T}$ *Eisenstein* if it contains
\[
\mathcal{I}_0 := (T_r - r - 1 : \text{for primes } r \nmid pq).
\]

**Definition 2.1.** We define Eisenstein ideals as follows:
\[
\mathcal{I}_1 := (U_p - 1, U_q - 1, \mathcal{I}_0);
\]
\[
\mathcal{I}_2 := (U_p - 1, U_q - q, \mathcal{I}_0) \quad \text{and} \quad \mathcal{I}_3 := (U_p - p, U_q - 1, \mathcal{I}_0).
\]

Moreover, we set $m_i := (\ell, \mathcal{I}_i)$. They are all possible Eisenstein maximal ideals in $\mathcal{T}_\ell$ by the result in [Yoo3, §2]. For ease of notation, we set $\mathcal{T}_i := \mathcal{T}_{m_i}$.

Since $\mathcal{T}_\ell$ is a semi-local ring, we have
\[
\mathcal{T}_\ell = \prod_{\ell \in m \text{ maximal}} \mathcal{T}_m.
\]

Using the above description of Eisenstein maximal ideals, we prove the following:

**Theorem 2.2.** The quotient $\mathcal{T}_\ell / \mathcal{I}_0$ is isomorphic to $\mathcal{T}_\ell / \mathcal{I}_2 \times \mathcal{T}_\ell / \mathcal{I}_3$.

This theorem is crucial to deduce our main theorem. In general, the author expects that $\mathcal{T}_\ell / \mathcal{I}_0$ should be isomorphic to
\[
\{(x, y, z) \in \mathcal{T}_\ell / \mathcal{I}_1 \times \mathcal{T}_\ell / \mathcal{I}_2 \times \mathcal{T}_\ell / \mathcal{I}_3 : x \equiv y \pmod{p - 1} \text{ and } x \equiv z \pmod{q - 1}\}.
\]

Before proving the theorem above, we need several lemmas.

**Lemma 2.3.** We have $(U_p - 1)(U_p + 1) \in \mathcal{I}_0 \mathcal{T}_\ell$.

**Proof.** Since $q \not\equiv 1 \pmod{\ell}$, any maximal ideal containing $\mathcal{I}_0$ cannot be $p$-old. Therefore $\mathcal{T}_\ell / \mathcal{I}_0 \simeq \mathcal{T}_\ell^{p\text{-new}} / \mathcal{I}_0$. Since $U_p^2 = 1$ in $\mathcal{T}_\ell^{p\text{-new}}$, the result follows. \qed
Lemma 2.4. Suppose that $m_2$ is maximal. Then, we have

$$\mathbb{T}_2/I_0 = \mathbb{T}_2/I_2 \simeq \mathbb{T}_\ell/I_2.$$  

If $m_1$ is maximal, then $p \equiv 1 \pmod{\ell}$ and hence $m_1 = m_3$; moreover, we have $\mathbb{T}_1/I_0 = \mathbb{T}_3/I_0 \simeq \mathbb{T}_\ell/I_3$. If $p \not\equiv 1 \pmod{\ell}$, then $m_1$ is not maximal and $\mathbb{T}_3/I_0 \simeq \mathbb{T}_\ell/I_3$.

Proof. Suppose that $m_2$ is maximal. Since $U_p - 1 \in m_2$ and $\ell$ is odd, $U_p + 1 \not\in m_2$ and hence it is a unit in $\mathbb{T}_2$. By the lemma above, $(U_p - 1)(U_p + 1) \in I_0\mathbb{T}_\ell$ and hence $U_p - 1 \in I_0\mathbb{T}_2$. Similarly, we have $U_q - q \in I_0\mathbb{T}_2$ because $q \not\equiv 1 \pmod{\ell}$ and $(U_q - 1)(U_q - q) \in I_0\mathbb{T}_2$ by the following lemma. Thus, we have $\mathbb{T}_2/I_0 = \mathbb{T}_2/I_2$. Since the index of $I_2$ in $\mathbb{T}$ is finite (cf. [Yoo1 Lemma 3.1]), we have $m_2^q \subseteq I_2$ for large enough $n$. Therefore $\mathbb{T}_\ell/(m_2^q, I_2) \simeq \mathbb{T}_\ell/I_2$ and hence $\mathbb{T}_2/I_2 \simeq \mathbb{T}_\ell/I_2$.

If $m_1$ is maximal, the index of $I_1$ in $\mathbb{T}$ is divisible by $\ell$. By [Yoo3 Theorem 1.4], it is num $(\frac{(p-1)(q-1)}{4})$ up to powers of $2$ and hence $p \equiv 1 \pmod{\ell}$.

Assume that $p \equiv 1 \pmod{\ell}$. Let $a$ be the number in [1.1] Since $\ell$ does not divide $(p+1)(q-1)$, $\ell^a$ divides $(p-1)$. Note that the index of $I_3$ in $\mathbb{T}_\ell$ is equal to $\ell^a$ (cf. [Yoo3 Theorem 1.4]) and hence $I_3\mathbb{T}_\ell$ contains $p - 1$. Thus, $U_p - 1 = (U_p - p) + (p - 1) \in I_3\mathbb{T}_\ell$. In other words, $I_1\mathbb{T}_\ell \subseteq I_3\mathbb{T}_\ell$. Similarly, we have $I_3\mathbb{T}_\ell \subseteq I_1\mathbb{T}_\ell$. Therefore we have $I_1\mathbb{T}_\ell = I_3\mathbb{T}_\ell$. By the same argument as above, $I_0\mathbb{T}_3$ contains $U_p - 1$ and $(U_q - 1)(U_q - q)$. Since $q \not\equiv 1 \pmod{\ell}$ and $U_q - 1 \in m_3$, we have $U_q - q \not\in m_3$ and hence $\mathbb{T}_3/I_0 = \mathbb{T}_3/I_3$. Thus, we get $\mathbb{T}_3/I_3 \simeq \mathbb{T}_\ell/I_3$ as above.

If $p \not\equiv 1 \pmod{\ell}$, then $m_3$ is neither $p$-old nor $q$-old. If $p \not\equiv -1 \pmod{\ell}$, then $m_3$ is not maximal. Thus, we have $\mathbb{T}_\ell/I_3 = \mathbb{T}_3/I_0 = 0$. If $p \equiv -1 \pmod{\ell}$, then the result follows by [Yoo2 Proposition 2.3].

Lemma 2.5. Let $I := (U_p - 1, I_0) \subseteq \mathbb{T}_\ell$. Then, we get $(U_q - 1)(U_q - q) \in I$.

Proof. We closely follow the argument in [MaZ77, §II. 5].

Let $f(z) := \sum_{n \geq 1} (T_n \mod I) x^n$ be a cusp form of weight 2 and level $pq$ over $\mathbb{T}_\ell/I$, where $x = e^{2\pi iz}$. Let $E := E_{p, pq}$ be an Eisenstein series of weight 2 and level $pq$ in [Yoo1 §2.3]. Note that

$$(f - E)(z) \equiv (U_q - q) \sum_{n \geq 1} a_n x^{qn} \pmod{I},$$

where $a_p = 1$ and $a_r = 1 + r$ for all primes $r \neq pq$ and $a_q = U_q + q$. If $U_q - q \not\in I$, then by Ohta [Oht14 Lemma 2.1.1], there is a cusp form $g(z) = \sum_{n \geq 1} b_n x^n$ of weight 2 and level $p$ such that

$$(f - E)(z) \equiv (U_q - q) \sum_{n \geq 1} a_n x^{qn} \equiv (U_q - q)g(qz) \pmod{I}.$$
Therefore \( p \equiv 1 \pmod{\ell} \) and \( b_r \equiv 1 + r \pmod{l'} \) for primes \( r \neq p \), where \( l' \) is the Eisenstein ideal of level \( p \). Thus, we have \( (U_q - q)(a_q - b_q) \equiv (U_q - q)(U_q - 1) \in I. \]

Now, we are ready to prove Theorem 2.2.

Proof of Theorem 2.2 If \( p \equiv 1 \pmod{\ell} \), then \( m_1 = m_3 \). Otherwise \( m_1 \) is not maximal. Therefore, we have

\[
\mathbb{T}_\ell/I_0 \simeq \mathbb{T}_2/I_0 \times \mathbb{T}_3/I_0 = \mathbb{T}_2/I_2 \times \mathbb{T}_3/I_3 \simeq \mathbb{T}_\ell/I_2 \times \mathbb{T}_\ell/I_3.
\]

\[ \square \]

3. Case where \( \ell \) does not divide \( pq \)

From now on, let \( \mathcal{C} := \mathcal{C}(pq) \) and \( \mathcal{T} := \mathcal{T}(pq) \) be the cuspidal group of \( J_0(pq) \) and the group of rational torsion points on \( J_0(pq) \), respectively. For a prime \( r \) and a finite abelian group \( A \), we denote by \( A[r^\infty] \) the \( r \)-primary subgroup of \( A \). In this section, we prove the following theorem.

**Theorem 3.1.** For a prime \( \ell \) not dividing \( 2pq(q - 1) \), we have \( \mathcal{T}[\ell^\infty] = \mathcal{C}[\ell^\infty] \).

Before proving this theorem, we introduce some cuspidal divisors.

Let \( P_n \) be the cusp of \( X_0(pq) \) corresponding to \( 1/n \in \mathbb{P}^1(\mathbb{Q}) \). Let \( C_p := P_1 - P_p \) and \( C_q := P_1 - P_q \) denote the cuspidal divisors in \( \mathcal{C} \). Let \( M_p = \ell^a \times x \) and \( M_q = \ell^b \times y \) as in (3.1) (Thus, we have \((\ell, xy)=1\).) We define

\[ D_p := xC_p \quad \text{and} \quad D_q := yC_q. \]

Then, \( \langle D_p \rangle \) (resp. \( \langle D_q \rangle \)) is a free module of rank 1 over \( \mathbb{T}_\ell/I_2 \simeq \mathbb{Z}/\ell^a\mathbb{Z} \) (resp. \( \mathbb{T}_\ell/I_3 \simeq \mathbb{Z}/\ell^b\mathbb{Z} \)) (cf. [Yoo3, Theorem 1.4]).

Now we prove the Theorem above.

Proof of Theorem 3.1. By the Eichler-Shimura relation, \( \mathcal{T}[\ell^\infty] \) is a module over \( \mathbb{T}_\ell/I_0 \). Therefore \( \mathcal{T}[\ell^\infty] \) decomposes into \( \mathcal{T}[\ell^\infty][I_2] \times \mathcal{T}[\ell^\infty][I_3] \) by Theorem 2.2. Hence it suffices to show that \( \mathcal{T}[\ell^\infty][I_2] = \langle D_p \rangle \) and \( \mathcal{T}[\ell^\infty][I_3] = \langle D_q \rangle \).

If \( a = 0 \), then \( \mathbb{T}_\ell/I_2 = 0 \) and hence \( \mathcal{T}[\ell^\infty][I_2] = \langle D_p \rangle = 0 \). Thus, we may assume that \( a \geq 1 \). Note that

\[
\mathcal{T}[\ell^\infty][I_2] \simeq \prod_{i=1}^t \mathbb{Z}/\ell^{a_i}\mathbb{Z},
\]

where \( 1 \leq a_i \leq a \) because \( \mathbb{T}_\ell/I_2 \simeq \mathbb{Z}/\ell^a\mathbb{Z} \) (and \( \mathcal{T} \) is finite). Since \( D_p \in \mathcal{T}[\ell^\infty] \), we have \( \langle D_p \rangle \subseteq \mathcal{T}[\ell^\infty][I_2] \) and hence \( t \geq 1 \); and \( \mathcal{T}[\ell^\infty][\ell, I_2] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\oplus t} \subseteq J[m_2] \). By the same argument in [Maz77, II, Corollary 14.8] (cf. [Yoo1, Theorem 4.2]), we have \( t = 1 \) and \( \mathcal{T}[\ell^\infty][I_2] = \langle D_p \rangle \). By symmetry, \( \mathcal{T}[\ell^\infty][I_3] = \langle D_q \rangle \) and the result follows. \[ \square \]
4. Case where $\ell = p$ or $\ell = q$

Throughout this section, we set $P := p$ if $p \geq 5$; and $P := 9$ if $p = 3$. Suppose that

\begin{equation}
\ell = p \quad \text{and} \quad \left\{ \begin{array}{l}
\text{either } q \not\equiv 1 \pmod{P} \text{ or } \\
q \equiv 1 \pmod{P} \text{ and } p^{q-1} \not\equiv 1 \pmod{q}.
\end{array} \right.
\end{equation}

**Theorem 4.1.** We have $T[p^\infty] = C[p^\infty]$.

**Proof.** We divide the problem into three cases.

1. Suppose that $q \not\equiv 1 \pmod{P}$ and $q \equiv 1 \pmod{p}$. This happens when $\ell = p = 3$. In this case, the indices of $I_1$, $I_2$ and $I_3$ are not divisible by 3 (cf. [Yoo3, Theorem 1.4]). Therefore there are no Eisenstein maximal ideals containing 3 and $T_p/I_0 = 0$. Thus, we have $T[3^\infty] = C[3^\infty] = 0$.

2. Suppose that $q \equiv 1 \pmod{P}$ and $p^{q-1} \not\equiv 1 \pmod{q}$. Then, $m_1 = m_2$ is not new by [Yoo2, Theorem 3.1]. Since $U_p \equiv p \equiv 0 \pmod{m_3}$, $m_3$ is not new. Therefore $T_p/I_0 \simeq T_p^{\text{old}}/I_0$. Consider the following exact sequence:

\[
0 \longrightarrow J_{\text{old}}(Q)[p^\infty] \longrightarrow J(Q)[p^\infty] \longrightarrow J_{\text{new}}(Q)[p^\infty].
\]

If $J_{\text{new}}(Q)[p^\infty] \neq 0$, then there is a new Eisenstein maximal ideal containing $p$, which is a contradiction. Therefore we have $J_{\text{old}}(Q)[p^\infty] = J(Q)[p^\infty]$. Now, the result follows from [CL97, Theorem 2] because $p \nmid 2 \gcd(p - 1, q - 1)$.

3. Suppose that $q \not\equiv 1 \pmod{p}$. First, assume that $q \not\equiv -1 \pmod{P}$. Then, the indices of $I_1$, $I_2$ and $I_3$ are not divisible by $p$, there is no Eisenstein maximal ideal. Thus, $T_p/I_0 = 0$ and $T[p^\infty] = C[p^\infty] = 0$.

Next, assume that $q \equiv -1 \pmod{P}$. By the same reason as above, $m_1$ and $m_3$ are not maximal (but $m_2$ is). Note that $m_2$ is neither $p$-old nor $q$-old by Mazur. Therefore we get $T_2/I_0 \simeq T_2^{\text{new}}/I_0$. Since $(U_p - 1)(U_p + 1) = (U_q - 1)(U_q + 1) = 0$ in $T^{\text{new}}$, we get $T_2/I_0 = T_2/I_2 \simeq T_p/I_2$ by [Yoo2, Proposition 2.3]. As in the proof of Theorem 3.1, we get

\[
T[p^\infty] = T[p^\infty][I_2] = C[p^\infty][I_2] = C[p^\infty].
\]

\[\square\]

**Remark 4.2.** If $p > q$, then the assumption above holds and hence $T[p^\infty] = C[p^\infty]$. Since $C[p^\infty] = 0$, there are no rational torsion points of order $p$ on $J_0(pq)$.  

REFERENCES


E-mail address: hwajong@gmail.com

Université du Luxembourg, Faculté des Sciences, de la Technologie et de la Communication, 6, rue Richard Coudenhove-Kalergi, L-1359 Luxembourg, Luxembourg