

ON THE RATIONAL CUSPIDAL SUBGROUP
AND THE RATIONAL TORSION POINTS OF $J_0(pq)$

SENG-KIAT CHUA AND SAN LING

(Communicated by William W. Adams)

ABSTRACT. For two distinct prime numbers p, q , we compute the rational cuspidal subgroup $C(pq)$ of $J_0(pq)$ and determine the ℓ -primary part of the rational torsion subgroup of the old subvariety of $J_0(pq)$ for most primes ℓ . Some results of Berkovič on the nontriviality of the Mordell-Weil group of some Eisenstein factors of $J_0(pq)$ are also refined.

1. INTRODUCTION

Let p, q be two distinct prime numbers, and let $X_0(p), X_0(q)$ and $X_0(pq)$ denote the classical modular curves over \mathbb{Q} . Let $J_0(p), J_0(q)$ and $J_0(pq)$ denote the corresponding Jacobian varieties, also defined over \mathbb{Q} .

On $X_0(p)$ (resp. $X_0(q)$), there are two (rational) cusps P_1 and P_p (resp. P_1 and P_q). It is well-known that the cuspidal subgroup $C(p)$ (resp. $C(q)$), generated by the class of the cuspidal divisor $P_1 - P_p$ (resp. $P_1 - P_q$), is cyclic of order $\frac{p-1}{(p-1, 12)}$ (resp. $\frac{q-1}{(q-1, 12)}$) (cf. [7]).

There are exactly four cusps, denoted P_1, P_p, P_q and P_{pq} , on $X_0(pq)$, and they are all rational. Let $C_p = P_1 - P_p$, $C_q = P_1 - P_q$ and $C_{pq} = P_1 - P_{pq}$ be the cuspidal divisors of degree 0. For a degree-0 divisor D on $X_0(pq)$, we shall denote the divisor class it defines by \overline{D} .

The cuspidal subgroup $C(pq)$ of $J_0(pq)$ is clearly generated by $\overline{C_p}, \overline{C_q}$ and $\overline{C_{pq}}$. Manin [5] has shown that $\overline{C_p}, \overline{C_q}$ and $\overline{C_{pq}}$ are of finite order. For each prime ℓ , we shall let r_ℓ, s_ℓ and t_ℓ be the non-negative integers such that ℓ^{r_ℓ} (resp. $\ell^{s_\ell}, \ell^{t_\ell}$) is the exact power of ℓ dividing the order of $\overline{C_p}$ (resp. $\overline{C_q}, \overline{C_{pq}}$). For an integer x , let $v_\ell(x)$ be the valuation of x at ℓ , i.e., $\ell^{v_\ell(x)}$ is the exact power of ℓ dividing x . Then we also set, for each prime ℓ ,

$$m_\ell \stackrel{\text{def}}{=} \min \left(v_\ell \left(\frac{p-1}{(p-1, 12)} \right), v_\ell \left(\frac{q-1}{(q-1, 12)} \right) \right),$$
$$M_\ell \stackrel{\text{def}}{=} \max(v_\ell(p-1), v_\ell(q-1)).$$

In this article, we compute the rational cuspidal subgroup $C(pq)$ of $J_0(pq)$. Here, for a finite group G , the notation G_ℓ represents the ℓ -primary part of G .

Received by the editors September 8, 1995 and, in revised form, March 10, 1996.

1991 *Mathematics Subject Classification*. Primary 11G18, 11F03, 11F20, 14H40.

The authors would like to thank Ken Ribet for private communication. We are also grateful to the referee for comments which helped improve the presentation of the paper.

Theorem 1. (i) Let $p, q \geq 5$ be two distinct primes. For any prime ℓ , the ℓ -primary part of the cuspidal subgroup $C(pq)$ of $J_0(pq)$ is given by:

$$\begin{aligned} C(pq)_\ell &\cong \mathbb{Z}/\ell^{r_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{s_\ell}\mathbb{Z} && \text{if } \ell \nmid \left(\frac{p-1}{2}, \frac{q-1}{2}\right), \\ C(pq)_\ell &\cong \mathbb{Z}/\ell^{r_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{M_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{m_\ell}\mathbb{Z} && \text{if } \ell \mid \left(\frac{p-1}{2}, \frac{q-1}{2}\right), \quad \ell \geq 5, \\ C(pq)_\ell &\cong \mathbb{Z}/\ell^{r_\ell}\mathbb{Z} \times \mathbb{Z}/\ell^{M_\ell-1}\mathbb{Z} \times \mathbb{Z}/\ell^{m_\ell}\mathbb{Z} && \text{if } \ell \mid \left(\frac{p-1}{2}, \frac{q-1}{2}\right), \quad \ell = 2, 3. \end{aligned}$$

(ii) For $p \geq 5$, the cuspidal subgroup $C(3p)$ of $J_0(3p)$ is given by:

$$C(3p) \cong \begin{cases} \mathbb{Z}/\frac{p-1}{3}\mathbb{Z} \times \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z} & \text{if } p \equiv 1 \pmod{3}, \\ \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z} & \text{if } p \equiv 2 \pmod{3}. \end{cases}$$

(iii) For $p \geq 5$, the cuspidal subgroup $C(2p)$ of $J_0(2p)$ is given by:

$$C(2p) \cong \begin{cases} \mathbb{Z}/\frac{p-1}{(p-1,8)}\mathbb{Z} \times \mathbb{Z}/\frac{p^2-1}{24}\mathbb{Z} & \text{if } p \not\equiv 1 \pmod{8}, \\ \mathbb{Z}/\frac{p-1}{4}\mathbb{Z} \times \mathbb{Z}/\frac{p^2-1}{24}\mathbb{Z} & \text{if } p \equiv 1 \pmod{8}. \end{cases}$$

and $C(6) = 0$.

After some general discussion on the generators of $C(pq)$ and establishing some relations among these generators, we prove Theorem 1 (i) in Section 3.3. The proofs of Theorem 1 (ii) and (iii) are left to the reader.

Recall that there are degeneracy maps $v_1, v_q : X_0(pq) \rightarrow X_0(p)$ and $v_1, v_p : X_0(pq) \rightarrow X_0(q)$. They induce via Pic functoriality the maps $v_1^*, v_q^* : J_0(p) \rightarrow J_0(pq)$ and $v_1^*, v_p^* : J_0(q) \rightarrow J_0(pq)$, and via Albanese functoriality the maps $(v_1)_*, (v_q)_* : J_0(pq) \rightarrow J_0(p)$ and $(v_1)_*, (v_p)_* : J_0(pq) \rightarrow J_0(q)$. Let γ be the map

$$(1) \quad \gamma = (v_1^* \times v_q^*) \times (v_1^* \times v_p^*) : J_0(p)^2 \times J_0(q)^2 \rightarrow J_0(pq).$$

The image of γ is the old subvariety of $J_0(pq)$, which we denote by J_{old} . The group of \mathbb{Q} -rational torsion points of this old subvariety is denoted by $J_{\text{old}}(\mathbb{Q})_{\text{tor}}$. We prove in Section 4

Theorem 2. Let ℓ be an odd prime not dividing $\left(\frac{p-1}{(p-1,24)}, \frac{q-1}{(q-1,24)}\right)$; then the restriction of γ to $C(p)_\ell^2 \times C(q)_\ell^2$ defines an isomorphism

$$C(p)_\ell^2 \times C(q)_\ell^2 \cong (J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell.$$

Theorems 1 and 2 can be used to refine some results of Berkovič [1] on the nontriviality of the Mordell-Weil group of some Eisenstein factors of $J_0(pq)$.

2. THE DEDEKIND η -FUNCTIONS AND CUSPIDAL DIVISORS

2.1. The Dedekind η -functions. Let N be a positive integer, and let δ denote a positive divisor of N . Let $\mathbf{r} = (r_\delta)$ be a family of rational numbers $r_\delta \in \mathbb{Q}$ indexed by all the positive divisors δ of N . Let

$$(2) \quad g_{\mathbf{r}} = \prod_{\delta \mid N} \eta_\delta^{r_\delta}$$

be made up from the Dedekind η -functions, where $\eta_\delta(z) \stackrel{\text{def}}{=} \eta(\delta z)$. We recall without proof the following proposition (cf. [2, Proposition 3.2.1] or [3, Proposition 1]):

Proposition 1. *The function $g_{\mathbf{r}}$ in (2) is a modular function on the modular curve $X_0(N)$ if and only if the following conditions are satisfied:*

- (0) *all the r_δ are rational integers;*
- (1) $\sum_{\delta|N} r_\delta \equiv 0 \pmod{24};$
- (2) $\sum_{\delta|N} r_\delta \frac{N}{\delta} \equiv 0 \pmod{24};$
- (3) $\sum_{\delta|N} r_\delta = 0;$
- (4) $\prod_{\delta|N} \delta^{r_\delta}$ *is the square of a rational number.*

By applying [4, Proposition 2] to the case $N = pq$, we have a bijection Λ from $\left\{ \prod_{\delta|pq} \eta_\delta^{r_\delta} : r_\delta \in \mathbb{Q} \text{ and } \sum_{\delta|pq} r_\delta = 0 \right\}$ to $\left\{ \sum_{d|pq} m_d P_d : m_d \in \mathbb{Q} \text{ and } \sum_{d|pq} m_d = 0 \right\}$. Identifying the first set with

$$\left\{ \begin{pmatrix} r_1 \\ r_p \\ r_q \\ r_{pq} \end{pmatrix} \in \mathbb{Q}^4 : r_1 + r_p + r_q + r_{pq} = 0 \right\}$$

and identifying the second set with

$$\left\{ \begin{pmatrix} m_1 \\ m_p \\ m_q \\ m_{pq} \end{pmatrix} \in \mathbb{Q}^4 : m_1 + m_p + m_q + m_{pq} = 0 \right\},$$

the map Λ may be represented as a matrix

$$\Lambda = \frac{1}{24} \begin{pmatrix} pq & q & p & 1 \\ q & pq & 1 & p \\ p & 1 & pq & q \\ 1 & p & q & pq \end{pmatrix},$$

so

$$\Lambda^{-1} = \frac{24}{(p^2 - 1)(q^2 - 1)} \begin{pmatrix} pq & -q & -p & 1 \\ -q & pq & 1 & -p \\ -p & 1 & pq & -q \\ 1 & -p & -q & pq \end{pmatrix}.$$

2.2. **Orders of cuspidal divisors.** Using the identification above, we have

$$\begin{aligned}
 C_p &= \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \quad \text{and} \quad \Lambda^{-1}C_p = \frac{24}{(p-1)(q^2-1)} \begin{pmatrix} q \\ -q \\ -1 \\ 1 \end{pmatrix}; \\
 C_q &= \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \quad \text{and} \quad \Lambda^{-1}C_q = \frac{24}{(p^2-1)(q-1)} \begin{pmatrix} p \\ -1 \\ -p \\ 1 \end{pmatrix}; \\
 C_{pq} &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} \quad \text{and} \quad \Lambda^{-1}C_{pq} = \frac{24}{(p^2-1)(q^2-1)} \begin{pmatrix} pq-1 \\ p-q \\ q-p \\ 1-pq \end{pmatrix}.
 \end{aligned}$$

Proposition 1 can then be used to determine the orders of the divisor classes $\overline{C}_p, \overline{C}_q$ and \overline{C}_{pq} . We summarize the results of our computations as follows:

	order of \overline{C}_p	order of \overline{C}_q	order of \overline{C}_{pq}
$q = 2$	$\frac{p-1}{(p-1,8)}$ if $p \not\equiv 1 \pmod{8}$	$\frac{p^2-1}{24}$	$\frac{p^2-1}{8}$ if $p \equiv 1 \pmod{3}$
$p \geq 5$	$\frac{p-1}{4}$ if $p \equiv 1 \pmod{8}$		$\frac{p^2-1}{24}$ if $p \equiv 2 \pmod{3}$
$q = 3$	$\frac{p-1}{3}$ if $p \equiv 1 \pmod{3}$	$\frac{p^2-1}{12}$	$\frac{p^2-1}{12}$ if $p \equiv 3 \pmod{4}$
$p \geq 5$	$p-1$ if $p \equiv 2 \pmod{3}$		$\frac{p^2-1}{6}$ if $p \equiv 1 \pmod{4}$
$q \geq 5$	$\frac{(q^2-1)(p-1)}{24}$	$\frac{(p^2-1)(q-1)}{24}$	$\frac{(p^2-1)(q^2-1)}{m}$
$p \geq 5$			

where $m \stackrel{\text{def}}{=} ((p^2-1)(q^2-1), 24(pq-1), 24(p-q), 12(p-1)(q+1), 12(q-1)(p+1))$.

3. RELATIONS AMONG THE GENERATORS $\overline{C}_p, \overline{C}_q, \overline{C}_{pq}$

3.1. **The general strategy.** To establish relations among the generators \overline{C}_i of $C(pq)$ we first apply the maps $v_1^*, v_q^* : J_0(p) \rightarrow J_0(pq)$ and $v_1^*, v_p^* : J_0(q) \rightarrow J_0(pq)$ to translate any known relations in $J_0(p)$ and $J_0(q)$ to some relations in $J_0(pq)$. Next, we note that a relation $\sum \lambda_i \overline{C}_i = 0$ exists if and only if $\Lambda^{-1}(\sum \lambda_i C_i)$ satisfies the conditions of Proposition 1. Using this criterion, one can easily check the validity of any relation. In addition, we can simplify the checking process by applying the maps $(v_1)_*, (v_q)_* : J_0(pq) \rightarrow J_0(p)$ (resp. $(v_1)_*, (v_p)_* : J_0(pq) \rightarrow J_0(q)$) to translate a relation in $J_0(pq)$ to a relation in $J_0(p)$ (resp. $J_0(q)$).

In this section, we will apply this strategy to establish the relations among the generators $\overline{C}_p, \overline{C}_q, \overline{C}_{pq}$. Note that a similar strategy has been used in [4, Section 2] to establish the relations among the generators of $C(p^r)$, where $p \geq 5$ is a prime. Consequently, we will only state the key lemmas in Section 3.2 since most of the details are similar to those in [4, Section 2].

3.2. **The case $p, q \geq 5$.** We now determine the relations involving the generators $\overline{C}_p, \overline{C}_q$ and \overline{C}_{pq} of $C(pq)$ by finding such relations at each prime ℓ . For each prime ℓ , we may write

$$(3) \quad \frac{(q^2-1)(p-1)}{24} = \ell^{r_\ell} \ell_1, \quad \frac{(p^2-1)(q-1)}{24} = \ell^{s_\ell} \ell_2, \quad \frac{(q^2-1)(p^2-1)}{m} = \ell^{t_\ell} \ell_3$$

where $\ell \nmid \ell_1, \ell \nmid \ell_2, \ell \nmid \ell_3$. We also set

$$C_{p,\ell} = \ell_1 \ell_2 \ell_3 C_p, \quad C_{q,\ell} = \ell_1 \ell_2 \ell_3 C_q, \quad C_{pq,\ell} = \ell_1 \ell_2 \ell_3 C_{pq}.$$

Since $(\ell_1 \ell_2, \ell) = (\ell_2 \ell_3, \ell) = (\ell_1 \ell_3, \ell) = 1$, it is clear that $\overline{C}_{p,\ell}, \overline{C}_{q,\ell}$ and $\overline{C}_{pq,\ell}$ generate $C(pq)_\ell$. By applying the maps $v_1^*, v_q^* : J_0(p) \rightarrow J_0(pq)$ and $v_1^*, v_p^* : J_0(q) \rightarrow J_0(pq)$ as described in Section 3.1, we get

Lemma 1. (i) *If ℓ does not divide $\left(\frac{q-1}{(q-1,12)}, \frac{p-1}{(p-1,12)}\right)$, then $C(pq)_\ell$ is generated by $\overline{C}_{p,\ell}$ and $\overline{C}_{q,\ell}$.*

(ii) *If ℓ divides $\left(\frac{q-1}{(q-1,12)}, \frac{p-1}{(p-1,12)}\right)$, then $\ell^{m_\ell} \overline{C}_{pq,\ell} = \alpha \overline{C}_{p,\ell} + \beta \overline{C}_{q,\ell}$ for some α, β .*

Furthermore, by applying the maps $(v_1)_*, (v_q)_* : J_0(pq) \rightarrow J_0(p)$ and $(v_1)_*, (v_p)_* : J_0(pq) \rightarrow J_0(q)$ together with the criterion stated in Section 3.1, we have

Lemma 2. *There is no non-trivial relation*

$$(4) \quad \nu_\ell \overline{C}_{pq,\ell} = \lambda_\ell \overline{C}_{p,\ell} + \mu_\ell \overline{C}_{q,\ell}$$

with $0 \leq \lambda_\ell < \ell^{r_\ell}, 0 \leq \mu_\ell < \ell^{s_\ell}$ and $0 \leq \nu_\ell < \ell^{m_\ell}$.

To help the reader in reconstructing the proof, we include the following formulas:

$$\begin{aligned} v_1^*(C_p) &= -C_q + qC_p + C_{pq}, \\ v_q^*(C_p) &= -qC_q + C_p + qC_{pq}, \\ (v_1)_*(C_p) &= C_p, \\ (v_1)_*(C_q) &= 0, \\ (v_1)_*(C_{pq}) &= C_p. \end{aligned}$$

In addition, the two maps v_1 and v_q are related by the formula $v_1 = v_q \circ w_q$ where w_q is an Atkin-Lehner involution (see the remark after Theorem 3).

From Lemma 1 (ii) and Lemma 2, if there is any relation

$$\nu_\ell \overline{C}_{pq,\ell} = \lambda_\ell \overline{C}_{p,\ell} + \mu_\ell \overline{C}_{q,\ell}$$

relating $\overline{C}_{pq,\ell}, \overline{C}_{p,\ell}$ and $\overline{C}_{q,\ell}$, we may assume $\nu_\ell(\nu_\ell) \geq m_\ell$. Together with Lemma 1 (ii), this relation can be reduced to

$$(5) \quad 0 = \lambda_\ell \overline{C}_{p,\ell} + \mu_\ell \overline{C}_{q,\ell}.$$

Therefore, we shall next study relations of this type.

Lemma 3. *Suppose (5) is satisfied.*

(i) *If $\ell \nmid (p-1, q-1)$ (hence $\ell \neq 2$), then $\lambda_\ell = \mu_\ell = 0$.*

(ii) *If $\ell \mid (p-1, q-1)$ and $\ell \neq 2$, then λ_ℓ and μ_ℓ satisfy*

$$\begin{aligned} \lambda_\ell \ell_2 q &\equiv -\mu_\ell \ell_1 \equiv \lambda_\ell \ell_2 \pmod{\ell^{r_\ell}} \quad (\ell \geq 3) \\ \text{and } \lambda_\ell &\equiv \mu_\ell \equiv 0 \pmod{\ell^{M_\ell}} \quad (\ell \geq 5) \quad \text{or } \lambda_3 \equiv \mu_3 \equiv 0 \pmod{3^{M_3-1}}. \end{aligned}$$

(iii) *If at least one of $p, q \equiv 3 \pmod{4}$, then $\lambda_2 = \mu_2 = 0$.*

(iv) *If $p \equiv q \equiv 1 \pmod{4}$, then λ_2 and μ_2 satisfy*

$$\lambda_2 \ell_2 q \equiv -\mu_2 \ell_1 \equiv \lambda_2 \ell_2 \pmod{2^{r_2}} \quad \text{and } \lambda_2 \equiv \mu_2 \equiv 0 \pmod{2^{M_2-1}}.$$

3.3. Proof of Theorem 1 (i). To prove Theorem 1 (i), note that if ℓ does not divide $(\frac{p-1}{2}, \frac{q-1}{2})$, then ℓ does not divide $(\frac{p-1}{(p-1,12)}, \frac{q-1}{(q-1,12)})$. Therefore $C(pq)_\ell$ is generated by $\overline{C}_{p,\ell}$ and $\overline{C}_{q,\ell}$. By Lemma 3 (i) and (iii), there is no relation between $\overline{C}_{p,\ell}$ and $\overline{C}_{q,\ell}$ in this case. The orders of $\overline{C}_{p,\ell}$ and $\overline{C}_{q,\ell}$ are given by (3). In the remaining case, Lemma 1 (ii) and Lemma 2 show that

$$C(pq)_\ell \cong \langle \overline{C}_{p,\ell}, \overline{C}_{q,\ell} \rangle \times \mathbb{Z}/\ell^{m_\ell} \mathbb{Z}.$$

If ℓ divides $(\frac{p-1}{2}, \frac{q-1}{2})$, then ℓ divides $(p-1, q-1)$.

If $\ell \geq 5$, Lemma 3 (ii) shows that $\langle \overline{C}_{p,\ell}, \overline{C}_{q,\ell} \rangle \cong \mathbb{Z}/\ell^{r_\ell} \mathbb{Z} \times \mathbb{Z}/\ell^{M_\ell} \mathbb{Z}$.

If $\ell = 3$, Lemma 3 (ii) shows that $\langle \overline{C}_{p,3}, \overline{C}_{q,3} \rangle \cong \mathbb{Z}/3^{r_3} \mathbb{Z} \times \mathbb{Z}/3^{M_3-1} \mathbb{Z}$.

If $\ell = 2$, Lemma 3 (iv) shows that $\langle \overline{C}_{p,2}, \overline{C}_{q,2} \rangle \cong \mathbb{Z}/2^{r_2} \mathbb{Z} \times \mathbb{Z}/2^{M_2-1} \mathbb{Z}$.

This completes the proof of Theorem 1 (i).

3.4. Additional remarks on Theorem 1. Consider the following cuspidal divisors (cf. [8]):

divisor	order of divisor class
$D^{+,-} = P_1 + P_p - P_q - P_{pq}$	$\frac{(p+1)(q-1)}{((p+1)(q-1), 24)}$
$D^{-,+} = P_1 - P_p + P_q - P_{pq}$	$\frac{(p-1)(q+1)}{((p-1)(q+1), 24)}$
$D^{-,-} = P_1 - P_p - P_q + P_{pq}$	$\frac{(p-1)(q-1)}{((p-1)(q-1), 24)}$

Note that we have the inclusions of groups

$$\langle 2\overline{C}_p, 2\overline{C}_q, 2\overline{C}_{pq} \rangle \subseteq \langle \overline{D}^{+,-}, \overline{D}^{-,+}, \overline{D}^{-,-} \rangle \subseteq C(pq) = \langle \overline{C}_p, \overline{C}_q, \overline{C}_{pq} \rangle.$$

If we are only interested in the odd part of $C(pq)$, we may as well consider the odd part of $\langle \overline{D}^{+,-}, \overline{D}^{-,+}, \overline{D}^{-,-} \rangle$. Using techniques employed in the earlier sections, we can show that there are no non-trivial relations among $\overline{D}^{+,-}, \overline{D}^{-,+}$ and $\overline{D}^{-,-}$ (even at the 2-primary part). Therefore the odd part of $C(pq)$ is isomorphic to that of $\langle \overline{D}^{+,-} \rangle \times \langle \overline{D}^{-,+} \rangle \times \langle \overline{D}^{-,-} \rangle$.

4. RATIONAL TORSION POINTS OF THE OLD SUBVARIETY

The goal of this section is to establish Theorem 2. Let γ be the map in (1), let K denote the kernel of γ and let ℓ be an odd prime. Let $\Sigma(p)$ (resp. $\Sigma(q)$) denote the Shimura subgroup of $J_0(p)$ (resp. $J_0(q)$); it is a cyclic group of order $\frac{p-1}{(p-1,12)}$ (resp. $\frac{q-1}{(q-1,12)}$). Let $\overline{C}(p)$ be the image of the anti-diagonal $C(p)$ in $J_0(pq)$, i.e.,

$$\overline{C}(p) = \{x \in J_0(pq) : x = (v_1^* - v_q^*)(c) \text{ for } c \in C(p)\},$$

and $\overline{C}(q)$ is similarly defined. It is shown in [9] that

$$(6) \quad K_\ell \cong \Sigma(p)_\ell \times \Sigma(q)_\ell \times (\overline{C}(p)_\ell \cap \overline{C}(q)_\ell).$$

Moreover, it is known that the group $\overline{C}(p) \cap \overline{C}(q)$ has order $(\frac{p-1}{(p-1,24)}, \frac{q-1}{(q-1,24)})$.

Let $P \subseteq J_0(p)^2 \times J_0(q)^2$ be defined as $P = \gamma^{-1}(J_{\text{old}}(\mathbb{Q})_{\text{tor}})$. For each odd prime ℓ , we have an exact sequence of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -modules

$$(7) \quad 0 \longrightarrow K_\ell \longrightarrow P_\ell \xrightarrow{\gamma} (J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell \longrightarrow 0.$$

Now let r be a prime distinct from p and q . Let T_r be the r th Hecke operator on $J_0(pq)$. Since $(r, pq) = 1$, T_r acts on $J_0(p)^2 \times J_0(q)^2$ (hence on P) diagonally, i.e., it acts on $J_0(p)$ (resp. $J_0(q)$) like the usual Hecke operator T_r in $\mathbb{T}_p = \text{End}_{\mathbb{Q}}(J_0(p))$ (resp. $\mathbb{T}_q = \text{End}_{\mathbb{Q}}(J_0(q))$) (cf. [9], “Formulaire”).

Since $\Sigma(p)$ and $C(p)$ (resp. $\Sigma(q)$ and $C(q)$) are Eisenstein, i.e., they are annihilated by $T_r - (1 + r)$ for all primes $r \neq p$ (resp. $r \neq q$), it follows from the isomorphism (6) that $(T_r - (1 + r))K_\ell = 0$ for all primes $r \neq p, q$. By considering the action of T_r on the Néron model of $J_0(pq)$ over \mathbb{Z} and restricting to characteristic r , the Eichler-Shimura relation yields the equation

$$T_r = \text{Frob}_r + r/\text{Frob}_r$$

on $J_0(pq)/\mathbb{F}_r$ where Frob_r denotes the Frobenius at r . This implies, in particular, $(T_r - (1 + r))(J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell = 0$. Since $T_r - (1 + r)$ kills K_ℓ and $(J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell$, and $T_r - (1 + r)$ commutes with the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $T_r - (1 + r)$ induces (using the Snake Lemma) a homomorphism $\delta_r : (J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell \rightarrow K_\ell^{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$. When ℓ does not divide $\left(\frac{p-1}{(p-1, 24)}, \frac{q-1}{(q-1, 24)}\right)$, $\overline{C(p)}_\ell \cap \overline{C(q)}_\ell$ is trivial, and (6) implies that $K_\ell^{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}$ is trivial. Therefore δ_r is the trivial homomorphism. This means that $T_r - (1 + r)$ annihilates P_ℓ , for all primes $r \neq p, q$.

Lemma 4 (cf. [11]). *Let S be a set of primes of density one that does not contain p . The ideal in $\mathbb{T}_p = \text{End}_{\mathbb{Q}}(J(p))$ generated by $\{T_r - (1 + r) : r \in S\}$ is the Eisenstein ideal I_p .*

Proof. Let I denote the ideal in \mathbb{T}_p generated by $\{T_r - (1 + r) : r \in S\}$ and let \mathfrak{m} denote a maximal ideal of \mathbb{T}_p containing $\{T_r - (1 + r) : r \in S\}$. By [10, Theorem 5.2], \mathfrak{m} gives rise to a reducible Galois representation $\rho_{\mathfrak{m}} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}(2, \mathbb{T}_p/\mathfrak{m})$ satisfying

$$\text{Tr}(\rho_{\mathfrak{m}}(\text{Frob}_r)) \equiv T_r \pmod{\mathfrak{m}}, \quad \det(\rho_{\mathfrak{m}}(\text{Frob}_r)) \equiv r \pmod{\mathfrak{m}}$$

for almost all r . Proposition 14.1 of [6, Chapter II] shows that \mathfrak{m} is Eisenstein. Hence, if $\mathfrak{m} \subset \mathbb{T}_p$ is a maximal ideal, $\mathfrak{m} \supset \{T_r - (1 + r) : r \in S\}$ if and only if $\mathfrak{m} \supset I_p$.

To show that $I = I_p$, it suffices to demonstrate that $I_{\mathfrak{m}} = I_{p, \mathfrak{m}}$ (in $\mathbb{T}_{\mathfrak{m}}$) for all Eisenstein primes \mathfrak{m} . By [6, Chapter II, Proposition 16.6], the ideal $I_{p, \mathfrak{m}}$ is a principal ideal in $\mathbb{T}_{p, \mathfrak{m}}$, generated by $T_r - (1 + r)$ for any “good” prime r . (For the definition of a “good” prime, see [6, Chapter II, Section 16].) The set of “good” primes has Dirichlet density $\frac{r-2}{r-1}$ if $r > 2$, and $\frac{1}{4}$ if $r = 2$. In particular, there is a good prime r_0 in S . Since $I_{\mathfrak{m}} \subset I_{p, \mathfrak{m}}$ evidently, $T_{r_0} - (1 + r_0) \in I$ shows that $I_{p, \mathfrak{m}} = I_{\mathfrak{m}}$. \square

Take S to be the set of all primes except p and q , and apply Lemma 4. It follows that P_ℓ is Eisenstein, i.e., $P_\ell \subseteq J_0(p)[I_p]_\ell^2 \times J_0(q)[I_q]_\ell^2$. In other words (cf. [6, Chapter II, Corollary 16.4]),

$$P_\ell \subseteq (\Sigma(p)_\ell \oplus C(p)_\ell)^2 \times (\Sigma(q)_\ell \oplus C(q)_\ell)^2.$$

Let $(\sigma_1 + c_1, \sigma_2 + c_2, \sigma_3 + c_3, \sigma_4 + c_4) \in P_\ell$ where $\sigma_1, \sigma_2 \in \Sigma(p), \sigma_3, \sigma_4 \in \Sigma(q)$, and $c_1, c_2 \in C(p), c_3, c_4 \in C(q)$. Since $C(p)$ and $C(q)$ consist only of \mathbb{Q} -rational torsion points of $J_0(p)$ and $J_0(q)$, respectively, we have $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in P_\ell$. For

any $\tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $(\sigma_1^\tau, \sigma_2^\tau, \sigma_3^\tau, \sigma_4^\tau) \in P_\ell$ and $\gamma(\sigma_1^\tau, \sigma_2^\tau, \sigma_3^\tau, \sigma_4^\tau) = \gamma(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$. Therefore,

$$(\sigma_1^\tau - \sigma_1, \sigma_2^\tau - \sigma_2, \sigma_3^\tau - \sigma_3, \sigma_4^\tau - \sigma_4) \in K_\ell \cong \Sigma(p)_\ell \times \Sigma(q)_\ell$$

since we are still in the case $\ell \nmid \left(\frac{p-1}{(p-1,24)}, \frac{q-1}{(q-1,24)} \right)$. It follows that (cf. [3, Theorem 1]) $\sigma_1^\tau - \sigma_1 = -(\sigma_2^\tau - \sigma_2)$ and $\sigma_3^\tau - \sigma_3 = -(\sigma_4^\tau - \sigma_4)$, i.e., $\sigma_1 + \sigma_2 \in \Sigma(p)_\ell(\mathbb{Q})$ and $\sigma_3 + \sigma_4 \in \Sigma(q)_\ell(\mathbb{Q})$. Therefore, we obtain $\sigma_1 = -\sigma_2$ and $\sigma_3 = -\sigma_4$, implying that $(\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in K_\ell$. This shows that $P_\ell = K_\ell \oplus (C(p)_\ell^2 \times C(q)_\ell^2)$. Putting this into (7) shows that γ induces an isomorphism

$$C(p)_\ell^2 \times C(q)_\ell^2 \cong (J_{\text{old}}(\mathbb{Q})_{\text{tor}})_\ell.$$

This completes the proof of Theorem 2.

5. A REMARK ON THE NONTRIVIALITY OF CERTAIN EISENSTEIN FACTORS OF $J_0(pq)$

Let $J^{\text{new}} \stackrel{\text{def}}{=} J_0(pq)/J_{\text{old}}$ be the new quotient of $J_0(pq)$. Let \mathbb{T} be the subring of $\text{End}_{\mathbb{Q}}(J^{\text{new}})$ generated over \mathbb{Z} by the Hecke operators. The Eisenstein ideal I_{pq} is the ideal in \mathbb{T} generated by $T_r - (1+r)$, for all primes $r \neq p, q$. It is of finite index in \mathbb{T} .

Let Λ be a non-trivial ideal of \mathbb{T} containing I_{pq} and a prime number ℓ . Let $a_\Lambda = \bigcap_{n=1}^\infty \Lambda^n$. The Eisenstein factor $J^{(\Lambda)}$ of J^{new} associated with Λ is defined as

$$J^{(\Lambda)} \stackrel{\text{def}}{=} J^{\text{new}}/a_\Lambda J^{\text{new}}.$$

In [1], the following theorem is proved:

Theorem 3 (cf. [1, Theorem 4]). *Let p and q be distinct prime numbers, ℓ an odd prime with $\ell \mid (p+1)$ but $\ell \nmid (q-1)$ if $\ell > 3$, and $9 \mid (p+1)(q-1)$ but $9 \nmid (q-1)$ if $\ell = 3$. Then the ideal $\Lambda = \langle I_{pq}, \ell, 1 - W_p \rangle$ is a proper ideal of \mathbb{T} , and the group $J^{(\Lambda)}(\mathbb{Q})$ is finite.*

Remark. Here, W_p is induced by the Atkin-Lehner involution on $X_0(pq)$, which is derived from the transformation $\tau \mapsto g\tau$ of the Poincaré upper half plane, where $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is any matrix in $M_2(\mathbb{Z})$ such that $p \mid A, p \mid D, pq \mid C$ and $\det(g) = p$.

A key step in the proof of Theorem 3 in [1] is to produce a point of order ℓ in $J^{\text{new}}(\mathbb{Q})$ which is annihilated by Λ . Given the conditions on ℓ in Theorem 3, by proving that J_{old} has no \mathbb{Q} -rational point of order ℓ , Berkovič showed that the image of the divisor class of $D^{+,-} = P_1 + P_p - P_q - P_{pq}$ in $J^{\text{new}}(\mathbb{Q})$ has order divisible by ℓ . A suitable multiple of $\overline{D^{+,-}}$ would produce the point of $J^{\text{new}}(\mathbb{Q})$ with the desired properties. The constraint $\ell \nmid (q-1)$ if $\ell > 3$ and $9 \nmid (q-1)$ if $\ell = 3$ are necessary for the proof used in [1], because it depends on the following fact: the Galois module $J_0(p)(\overline{\mathbb{Q}})_\ell$ has a Jordan-Holder factor isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ or μ_ℓ if and only if $\ell \mid \frac{p-1}{(p-1,12)}$. A careful application of Theorems 1 and 2 above allows us to relax some of the constraints on ℓ in Theorem 3.

Theorem 4. *Let p and q be distinct prime numbers, ℓ an odd prime with $\ell \mid (p+1)$ if $\ell > 3$ and $9 \mid (p+1)(q-1)$ and $3 \mid (p+1)$ if $\ell = 3$. Then the ideal $\Lambda = \langle I_{pq}, \ell, 1 - W_p \rangle$ is a proper ideal of \mathbb{T} and the group $J^{(\Lambda)}(\mathbb{Q})$ is finite.*

The (relaxed) constraints on ℓ in Theorem 4 imply that ℓ satisfies the conditions in Theorem 2, so $(J_{\text{old}}(\mathbb{Q})_{\text{tor}})_{\ell}$ is known. It is easy to see that $(J_{\text{old}}(\mathbb{Q})_{\text{tor}})_{\ell}$ is strictly smaller than $C(pq)_{\ell}$, so an element in its complement in the latter yields an element of $J^{\text{new}}(\mathbb{Q})$ of the desired properties. The details of the proof are left to the reader.

REFERENCES

1. V. G. Berkovič, *The rational points on the Jacobian of modular curves.*, Math. USSR Sbornik **30** (1976), AMS Translations 478–500.
2. G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France Mémoire **43** (1975), 5–80. MR **54**:5121
3. S. Ling, *The old subvariety of $J_0(pq)$ and the Eisenstein kernel in Jacobians*, Israel J. of Math **84** (1993), 365–384. MR **94h**:11047
4. ———, *On the \mathbb{Q} -rational cuspidal subgroup and the component group of $J_0(p^r)$* , 1996, To appear in Israel J. of Math.
5. Ju. Manin, *Parabolic points and zeta function of modular curves.*, Izv. Akad. Nauk. SSSR **6** (1972), AMS Translations 19–64. MR **47**:3396
6. B. Mazur, *Modular curves and the Eisenstein ideal.*, Pub. Math. I.H.E.S. **47** (1978), 33–186.
7. A. P. Ogg, *Rational points on certain elliptic modular curves*, Proc. Sym. Pure Math, vol. 20, AMS, 1973, pp. 221–231. MR **49**:2743
8. ———, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR **51**:514
9. K. Ribet, *The old subvariety of $J_0(pq)$* , Arithmetic Algebraic Geometry, Birkhäuser, 1989, pp. 293–307. MR **92a**:11069
10. ———, *On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*, Invent. Math. **100** (1991), 431–476. MR **91g**:11066
11. ———, June 1994, Private communication.

DEPARTMENT OF MATHEMATICS, NATIONAL UNIVERSITY OF SINGAPORE, 10 KENT RIDGE CRES-
CENT, SINGAPORE 119260, REPUBLIC OF SINGAPORE

E-mail address: matchua@nus.sg

E-mail address: matlings@nus.sg