ACTA ARITHMETICA
172.4 (2016)

Rational torsion points on Jacobians of modular curves

by

HWAJONG YOO (Pohang)

1. Introduction. Let N be a square-free integer. Consider the modular curve $X_0(N)$ and its Jacobian variety $J_0(N) = \mathrm{Pic}^0(X_0(N))$. Let $\mathcal{T}(N)$ denote the group of rational torsion points on $J_0(N)$ and let $\mathcal{C}(N)$ denote the cuspidal group of $J_0(N)$. By Manin and Drinfeld [2, 3], we have $\mathcal{C}(N) \subseteq \mathcal{T}(N)$ and they are both finite abelian groups.

When N is prime, Ogg conjectured that $\mathcal{T}(N) = \mathcal{C}(N)$ [5, Conjecture 2]. In his article [4], Mazur proved this conjecture by studying the Eisenstein ideal of level N. Recently, Ohta [6] proved a generalization of the result of Mazur. More precisely, he proved the following.

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

(For a finite abelian group A, $A[\ell^\infty]$ denotes its ℓ-primary subgroup.)

We briefly sketch the proof of this theorem. Let T_r (resp. U_p and w_p) denote the rth Hecke operator (resp. the pth 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 $\mathrm{End}(J_0(N))$ generated by the 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

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

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

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

2010 *Mathematics Subject Classification*: 11G10, 11G18, 14G05.
Key words and phrases: rational points, modular curves, Eisenstein ideals.
Received 19 April 2015.
Published online 3 December 2015.

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

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

Finally, he proved that $\mathcal{T}(N)[\ell^\infty][\mathcal{I}_M] = \mathcal{C}(N)[\ell^\infty][\mathcal{I}_M]$ by computing the index of $\mathcal{I}_M$ (up to 2-primary parts).

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 in the method by Ohta.) When ℓ satisfies some conditions, we get a 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 ℓ not dividing $2pq\gcd(p-1,\ q-1)$, we have $\mathcal{T}(pq)[\ell^\infty] = \mathcal{C}(pq)[\ell^\infty]$. Moreover, $\mathcal{T}(pq)[p^\infty] = \mathcal{C}(pq)[p^\infty]$ if one of the following holds:*

$$(1)\ p \geq 5 \ \textit{and} \begin{cases} \textit{either } q \not\equiv 1 \pmod{p} \textit{ or} \\ q \equiv 1 \pmod{p} \textit{ and } p^{(q-1)/p} \not\equiv 1 \pmod{q}. \end{cases}$$

$$(2)\ p = 3 \ \textit{and} \begin{cases} \textit{either } q \not\equiv 1 \pmod{9} \textit{ or} \\ q \equiv 1 \pmod{9} \textit{ and } 3^{(q-1)/3} \not\equiv 1 \pmod{q}. \end{cases}$$

Note that most cases above are special cases 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 $3^{(p-1)/3} \not\equiv 1 \pmod{p}$. Then*

$$\mathcal{T}(3p)[3^\infty] = \mathcal{C}(3p)[3^\infty].$$

1.1. Notation. For $x = a/b \in \mathbb{Q}$, we denote by $\mathrm{num}(x)$ the numerator of x, i.e.,

$$\mathrm{num}(x) := a/(a, b).$$

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 ℓ dividing

$$M_p := \mathrm{num}\left(\frac{(p-1)(q^2-1)}{3}\right) \quad \left(\text{resp. } M_q := \mathrm{num}\left(\frac{(p^2-1)(q-1)}{3}\right)\right).$$

2. Eisenstein ideals of level pq. Throughout this section, we fix two distinct primes p and q; and ℓ denotes a prime not dividing $2pq(q-1)$. Let $\mathbb{T} := \mathbb{T}(pq)$ and $\mathbb{T}_\ell := \mathbb{T}(pq) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. We say that an ideal of $\mathbb{T}$ is *Eisenstein* if it contains

$$\mathcal{I}_0 := (T_r - r - 1 : r \text{ prime},\ r \nmid pq).$$

DEFINITION 2.1. We define Eisenstein ideals as follows:

$$\mathcal{I}_1 := (U_p - 1, U_q - 1, \mathcal{I}_0),$$
$$\mathcal{I}_2 := (U_p - 1, U_q - q, \mathcal{I}_0), \quad \mathcal{I}_3 := (U_p - p, U_q - 1, \mathcal{I}_0).$$

Moreover, we set $\mathfrak{m}_i := (\ell, \mathcal{I}_i)$. They are all possible Eisenstein maximal ideals in $\mathbb{T}_\ell$ by the result in [9, §2]. For ease of notation, we set $\mathbb{T}_i := \mathbb{T}_{\mathfrak{m}_i} = \lim_{\leftarrow n} \mathbb{T}/\mathfrak{m}_i^n$.

Since $\mathbb{T}_\ell$ is a semi-local ring, we have

$$\mathbb{T}_\ell = \prod_{\ell \in \mathfrak{m} \text{ maximal}} \mathbb{T}_\mathfrak{m}.$$

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

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

This theorem is crucial to deduce our Main Theorem. In general, the author expects that $\mathbb{T}_\ell/\mathcal{I}_0$ should be isomorphic to

$\{(x, y, z) \in \mathbb{T}_\ell/\mathcal{I}_1 \times \mathbb{T}_\ell/\mathcal{I}_2 \times \mathbb{T}_\ell/\mathcal{I}_3 : x \equiv y \pmod{p-1} \text{ and } x \equiv z \pmod{q-1}\}$.

To prove the theorem above, we need several lemmas.

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

Proof. Since $q \not\equiv 1 \pmod{\ell}$, no maximal ideal containing $\mathcal{I}_0$ can be p-old. Therefore $\mathbb{T}_\ell/\mathcal{I}_0 \simeq \mathbb{T}_\ell^{p\text{-new}}/\mathcal{I}_0$. Since $U_p^2 = 1$ in $\mathbb{T}_\ell^{p\text{-new}}$, the result follows. ∎

LEMMA 2.4. *Suppose that $\mathfrak{m}_2$ is maximal. Then*

$$\mathbb{T}_2/\mathcal{I}_0 = \mathbb{T}_2/\mathcal{I}_2 \simeq \mathbb{T}_\ell/\mathcal{I}_2.$$

If $\mathfrak{m}_1$ is maximal, then $p \equiv 1 \pmod{\ell}$ and hence $\mathfrak{m}_1 = \mathfrak{m}_3$; moreover, $\mathbb{T}_1/\mathcal{I}_0 = \mathbb{T}_3/\mathcal{I}_0 \simeq \mathbb{T}_\ell/\mathcal{I}_3$. If $p \not\equiv 1 \pmod{\ell}$, then $\mathfrak{m}_1$ is not maximal and $\mathbb{T}_3/\mathcal{I}_0 \simeq \mathbb{T}_\ell/\mathcal{I}_3$.

Proof. Since $U_p - 1 \in \mathfrak{m}_2$ and ℓ is odd, $U_p + 1 \notin \mathfrak{m}_2$ and hence it is a unit in $\mathbb{T}_2$. By the lemma above, $(U_p - 1)(U_p + 1) \in \mathcal{I}_0\mathbb{T}_\ell$ and hence $U_p - 1 \in \mathcal{I}_0\mathbb{T}_2$. Similarly, $U_q - q \in \mathcal{I}_0\mathbb{T}_2$ because $q \not\equiv 1 \pmod{\ell}$ and $(U_q - 1)(U_q - q) \in \mathcal{I}_0\mathbb{T}_2$ by the next lemma. Thus, we have $\mathbb{T}_2/\mathcal{I}_0 = \mathbb{T}_2/\mathcal{I}_2$. Since the index of $\mathcal{I}_2$ in $\mathbb{T}$ is finite (cf. [7, Lemma 3.1]), we have $\mathfrak{m}_2^n \subseteq \mathcal{I}_2$ for large enough n. Therefore $\mathbb{T}_\ell/(\mathfrak{m}_2^n, \mathcal{I}_2) \simeq \mathbb{T}_\ell/\mathcal{I}_2$ and hence $\mathbb{T}_2/\mathcal{I}_2 \simeq \mathbb{T}_\ell/\mathcal{I}_2$.

If $\mathfrak{m}_1$ is maximal, the index of $\mathcal{I}_1$ in $\mathbb{T}$ is divisible by ℓ. By [9, Theorem 1.4], it is $\mathrm{num}((p-1)(q-1)/3)$ up to powers of 2 and hence $p \equiv 1 \pmod{\ell}$.

Assume that $p \equiv 1 \pmod{\ell}$. Let α be the number in §1.1. Since ℓ does not divide $(p+1)(q-1)$, ℓ^α divides $(p-1)$. Note that the index of $\mathcal{I}_3$ in $\mathbb{T}_\ell$ is equal to ℓ^α (cf. [9, Theorem 1.4]) and hence $\mathcal{I}_3\mathbb{T}_\ell$ contains $p-1$. Thus, $U_p - 1 = (U_p - p) + (p-1) \in \mathcal{I}_3\mathbb{T}_\ell$. In other words, $\mathcal{I}_1\mathbb{T}_\ell \subseteq \mathcal{I}_3\mathbb{T}_\ell$. Similarly, $\mathcal{I}_3\mathbb{T}_\ell \subseteq \mathcal{I}_1\mathbb{T}_\ell$. Therefore $\mathcal{I}_1\mathbb{T}_\ell = \mathcal{I}_3\mathbb{T}_\ell$. By the same argument as above, $\mathcal{I}_0\mathbb{T}_3$

contains $U_p - 1$ and $(U_q - 1)(U_q - q)$. Since $q \not\equiv 1 \pmod{\ell}$ and $U_q - 1 \in \mathfrak{m}_3$, we have $U_q - q \notin \mathfrak{m}_3$ and hence $\mathbb{T}_3/\mathcal{I}_0 = \mathbb{T}_3/\mathcal{I}_3$. By the same argument as above, we get $\mathbb{T}_3/\mathcal{I}_3 \simeq \mathbb{T}_\ell/\mathcal{I}_3$.

If $p \not\equiv 1 \pmod{\ell}$, then $\mathfrak{m}_3$ is neither p-old nor q-old. If $p \not\equiv -1 \pmod{\ell}$, then $\mathfrak{m}_3$ is not maximal. Thus, $\mathbb{T}_\ell/\mathcal{I}_3 = \mathbb{T}_3/\mathcal{I}_0 = 0$. If $p \equiv -1 \pmod{\ell}$, then the result follows by [8, Proposition 2.3]. ∎

Lemma 2.5. *Let $I := (U_p - 1, \mathcal{I}_0) \subseteq \mathbb{T}_\ell$. Then $(U_q - 1)(U_q - q) \in I$.*

Proof. We closely follow the argument in [4, §II.5].

Let $f(z) := \sum_{n\geq 1}(T_n \bmod I)x^n$ be the Fourier expansion (at ∞) of a cusp form of weight 2 and level pq over $\mathbb{T}_\ell/I$, where $x = e^{2\pi i z}$. (Here, we often denote by T_p (resp. T_q) the Hecke operator U_p (resp. U_q).) Let $E := E_{p,pq}$ be an Eisenstein series of weight 2 and level pq in [7, §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 $U_q - q \notin I$, then by Ohta [6, 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 $b_r \equiv 1 + r \pmod{I'}$ for primes $r \neq p$, where I' is the Eisenstein ideal of level p. Thus, we have $(U_q - q)(a_q - b_q) \equiv (U_q - q)(U_q - 1) \in I$. ∎

Proof of Theorem 2.2. If $p \equiv 1 \pmod{\ell}$, then $\mathfrak{m}_1 = \mathfrak{m}_3$. Otherwise $\mathfrak{m}_1$ is not maximal. Therefore,

$$\mathbb{T}_\ell/\mathcal{I}_0 \simeq \mathbb{T}_2/\mathcal{I}_0 \times \mathbb{T}_3/\mathcal{I}_0 = \mathbb{T}_2/\mathcal{I}_2 \times \mathbb{T}_3/\mathcal{I}_3 \simeq \mathbb{T}_\ell/\mathcal{I}_2 \times \mathbb{T}_\ell/\mathcal{I}_3. \ ∎$$

3. Case where ℓ 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 ℓ 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 $M_p = \ell^\alpha \times x$ and $M_q = \ell^\beta \times y$ as in §1.1. (Thus, $(\ell, xy) = 1$.) 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 $\mathbb{T}_\ell/\mathcal{I}_2 \simeq \mathbb{Z}/\ell^\alpha\mathbb{Z}$ (resp. $\mathbb{T}_\ell/\mathcal{I}_3 \simeq \mathbb{Z}/\ell^\beta\mathbb{Z}$) (cf. [9, Theorem 1.4]).

Proof of Theorem 3.1. By the Eichler–Shimura relation, $\mathcal{T}[\ell^\infty]$ is a module over $\mathbb{T}_\ell/\mathcal{I}_0$. Therefore $\mathcal{T}[\ell^\infty]$ decomposes into $\mathcal{T}[\ell^\infty][\mathcal{I}_2] \times \mathcal{T}[\ell^\infty][\mathcal{I}_3]$ by Theorem 2.2. Hence it suffices to show that $\mathcal{T}[\ell^\infty][\mathcal{I}_2] = \langle D_p\rangle$ and $\mathcal{T}[\ell^\infty][\mathcal{I}_3] = \langle D_q\rangle$.

If $\alpha = 0$, then $\mathbb{T}_\ell/\mathcal{I}_2 = 0$ and hence $\mathcal{T}[\ell^\infty][\mathcal{I}_2] = \langle D_p\rangle = 0$. Thus, we may assume that $\alpha \geq 1$. Note that

$$\mathcal{T}[\ell^\infty][\mathcal{I}_2] \simeq \prod_{i=1}^{t} \mathbb{Z}/\ell^{a_i}\mathbb{Z},$$

where $1 \leq a_i \leq \alpha$ because $\mathbb{T}_\ell/\mathcal{I}_2 \simeq \mathbb{Z}/\ell^\alpha\mathbb{Z}$ (and $\mathcal{T}$ is finite). Since D_p is in $\mathcal{T}[\ell^\infty]$, we have $\langle D_p\rangle \subseteq \mathcal{T}[\ell^\infty][\mathcal{I}_2]$ and hence $t \geq 1$; and $\mathcal{T}[\ell^\infty][\ell, \mathcal{I}_2] \simeq (\mathbb{Z}/\ell\mathbb{Z})^{\oplus t} \subseteq J_0(N)[\mathfrak{m}_2]$. By the same argument in [4, §II, Corollary 14.8] (cf. [7, Theorem 4.2]), we have $t = 1$ and $\mathcal{T}[\ell^\infty][\mathcal{I}_2] = \langle D_p\rangle$. By symmetry, $\mathcal{T}[\ell^\infty][\mathcal{I}_3] = \langle D_q\rangle$, and the result follows. ∎

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

$$\ell = p \quad \text{and} \quad \begin{cases} \text{either } q \not\equiv 1 \pmod{P} \text{ or} \\ q \equiv 1 \pmod{P} \text{ and } p^{(q-1)/p} \not\equiv 1 \pmod{q}. \end{cases} \tag{4.1}$$

THEOREM 4.1. *We have $\mathcal{T}[p^\infty] = \mathcal{C}[p^\infty]$.*

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 $\mathcal{I}_1$, $\mathcal{I}_2$ and $\mathcal{I}_3$ are not divisible by 3 (cf. [9, Theorem 1.4]). Therefore there are no Eisenstein maximal ideals containing 3, and $\mathbb{T}_p/\mathcal{I}_0 = 0$. Thus, $\mathcal{T}[3^\infty] = \mathcal{C}[3^\infty] = 0$.

(2) Suppose that $q \equiv 1 \pmod{P}$ and $p^{(q-1)/p} \not\equiv 1 \pmod{q}$. Then $\mathfrak{m}_1 = \mathfrak{m}_2$ is not new by [8, Theorem 3.1]. Since $U_p \equiv p \equiv 0 \pmod{\mathfrak{m}_3}$, $\mathfrak{m}_3$ is not new. Therefore $\mathbb{T}_p/\mathcal{I}_0 \simeq \mathbb{T}_p^{\mathrm{old}}/\mathcal{I}_0$. Consider the exact sequence

$$0 \to J_{\mathrm{old}}(\mathbb{Q})[p^\infty] \to J(\mathbb{Q})[p^\infty] \to J^{\mathrm{new}}(\mathbb{Q})[p^\infty].$$

If $J^{\mathrm{new}}(\mathbb{Q})[p^\infty] \neq 0$, then there is a new Eisenstein maximal ideal containing p, a contradiction. Therefore $J_{\mathrm{old}}(\mathbb{Q})[p^\infty] = J(\mathbb{Q})[p^\infty]$. Now, the result follows from [1, Theorem 2] because p does not divide $2(p-1, q-1)$.

(3) Suppose that $q \not\equiv 1 \pmod{p}$. First, assume that $q \not\equiv -1 \pmod{P}$. Then the indices of $\mathcal{I}_1$, $\mathcal{I}_2$ and $\mathcal{I}_3$ are not divisible by p, so there is no Eisenstein maximal ideal. Thus, $\mathbb{T}_p/\mathcal{I}_0 = 0$ and $\mathcal{T}[p^\infty] = \mathcal{C}[p^\infty] = 0$.

Next, assume $q \equiv -1 \pmod{P}$. For the same reason as above, $\mathfrak{m}_1$ and $\mathfrak{m}_3$ are not maximal (but $\mathfrak{m}_2$ is). Note that $\mathfrak{m}_2$ is neither p-old nor q-old by Mazur. Therefore we obtain $\mathbb{T}_2/\mathcal{I}_0 \simeq \mathbb{T}^{\text{new}}_{\mathfrak{m}_2}/\mathcal{I}_0$. Since $(U_p - 1)(U_p + 1) = (U_q - 1)(U_q + 1) = 0$ in $\mathbb{T}^{\text{new}}$, we get $\mathbb{T}_2/\mathcal{I}_0 = \mathbb{T}_2/\mathcal{I}_2 \simeq \mathbb{T}_p/\mathcal{I}_2$ by [8, Proposition 2.3]. As in the proof of Theorem 3.1, we conclude that

$$\mathcal{T}[p^\infty] = \mathcal{T}[p^\infty][\mathcal{I}_2] = \mathcal{C}[p^\infty][\mathcal{I}_2] = \mathcal{C}[p^\infty]. \blacksquare$$

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

Acknowledgements. This work was supported by IBS-R003-D1.

References

[1] S.-K. Chua and S. Ling, *On the rational cuspidal subgroup and the rational torsion points of* $J_0(pq)$, Proc. Amer. Math. Soc. 125 (1997), 2255–2263.

[2] V. Drinfeld, *Two theorems on modular curves*, Funct. Anal. Appl. 7 (1973), 155–156.

[3] Yu. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), 19–66 (in Russian); English transl.: Math. USSR-Izv. 6 (1972), 19–64.

[4] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. I.H.É.S. 47 (1977), 33–186.

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

[6] M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. 37 (2014), 273–318.

[7] H. Yoo, *The index of an Eisenstein ideal and multiplicity one*, Math. Z., to appear; arXiv:1311.5275 (2015).

[8] H. Yoo, *Rational torsion points on Jacobians of Shimura curves*, arXiv:1502.07370 (2015).

[9] H. Yoo, *On Eisenstein ideals and the cuspidal group of* $J_0(N)$, Israel J. Math., to appear; arXiv:1502.01571 (2015).

Hwajong Yoo
Center for Geometry and Physics
Institute for Basic Science (IBS)
Pohang 37673, Republic of Korea
E-mail: hwajong@gmail.com