THE INDEX OF AN EISENSTEIN IDEAL AND MULTIPLICITY ONE

HWAJONG YOO

ABSTRACT. Mazur's fundamental work on Eisenstein ideals for prime level has a variety of arithmetic applications. In this article, we generalize some of his work to square-free level. More specifically, we compute the index of an Eisenstein ideal and the dimension of the $\mathfrak{m}$-torsion of the modular Jacobian variety, where $\mathfrak{m}$ is an Eisenstein maximal ideal. In many cases, the dimension of the $\mathfrak{m}$-torsion is 2, in other words, multiplicity one theorem holds.

CONTENTS

1. INTRODUCTION

In the early 20th century, Ramanujan found the following congruences

$$\tau(p) \equiv 1 + p^{11} \pmod{691}$$

for any prime $p \neq 691$, where $\tau(p)$ is the p-th Fourier coefficient of the cusp form $\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}$ of weight 12 and level 1. Many mathematicians further found congruences between $\tau(p)$ and some arithmetic functions (such as $\sigma_k(p) = 1 + p^k$) modulo small prime powers. Serre and Swinnerton-Dyer [S73], [Sw73] recognized that these congruences between Eisenstein series and cusp forms can be understood by making use of Galois representations associated to Δ, and using this interpretation, they determined all possible congruences of $\tau(p)$.

In the case of weight 2, Mazur discussed Eisenstein ideals, which detect the congruences between Eisenstein series and cusp forms. (An ideal of a Hecke ring is called *Eisenstein* if it contains $T_r - r - 1$ for all but finitely many primes r not dividing the level.) For a prime N, he proved Ogg's conjecture (Conjecture 1.2) via a careful study of subgroups of the Jacobian variety $J_0(N)$ annihilated by the Eisenstein ideal. More precisely, in his paper [M77], he proved that $\mathbb{T}_N/I \simeq \mathbb{Z}/n\mathbb{Z}$, where $\mathbb{T}_N$ is the Hecke ring of level N, I is the Eisenstein ideal of $\mathbb{T}_N$, and n is the numerator of $\frac{N-1}{12}$. Moreover, for each prime $\ell \mid n$, he further proved that $\dim J_0(N)[\mathfrak{m}] = 2$, where $\mathfrak{m}$ is an Eisenstein maximal ideal generated by I and ℓ, and

$$J_0(N)[\mathfrak{m}] := \{x \in J_0(N)(\overline{\mathbb{Q}}) \ : \ Tx = 0 \ \text{ for all } T \in \mathfrak{m}\}.$$

Using this result he proved a classification theorem of the rational torsion subgroups of elliptic curves over the rational number field.

After his work, the dimension of $J_0(N)[\mathfrak{m}]$ has been studied by several mathematicians for the case that $\mathfrak{m}$ is non-Eisenstein. Assume that $\mathfrak{m}$ is a non-Eisenstein ideal of the Hecke ring $\mathbb{T}$ of

Date: September 29, 2014.
2010 *Mathematics Subject Classification.* 11G18 (Primary); 11F80(Secondary).
Key words and phrases. Cuspidal groups, Shimura subgroups, Eisenstein ideals, Multiplicity one.

level N. Then, by Boston-Lenstra-Ribet [BLR91], $J_0(N)[\mathfrak{m}] \simeq V^{\oplus r}$, where V is the underlying irreducible module for the Galois representation $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{T}/\mathfrak{m})$ associated to $\mathfrak{m}$. In most cases, for instance, when the characteristic of $\mathbb{T}/\mathfrak{m}$ is prime to $2N$, the multiplicity r is one. This result played an important role in the proof of Fermat's Last Theorem by Wiles. On the other hand, for an Eisenstein maximal ideal $\mathfrak{m}$, the dimension of $J_0(N)[\mathfrak{m}]$ has not been discussed when the level N is composite.

In this paper, we generalize some part of results of Mazur [M77] to square-free level. In §2, we introduce some Eisenstein modules that are used later.

In §3, we compute the index of an Eisenstein ideal of square-free level. More precisely, let N be a square-free integer and $M > 1$ be a divisor of N. Let

$$I_M := (U_p - 1,\ U_q - q,\ T_r - r - 1\ :\ \text{for primes } p \mid M,\ q \mid N/M, \text{ and } r \nmid N)$$

be an Eisenstein ideal of $\mathbb{T}_N$. For a square-free integer $N = \prod p_i$, let $\varphi(N) = \prod(p_i - 1)$ and $\psi(N) = \prod(p_i + 1)$. Then, we prove the following theorem.

Theorem 1.1. *For a prime $y \nmid 2N$, we have*

$$\mathbb{T}_N/I_M \otimes \mathbb{Z}_y \simeq \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}_y,$$

where m is the numerator of $\frac{\varphi(N)\psi(N/M)}{3}$.

The author expects that this theorem will shed light on the generalized Ogg's conjecture, which is the following.

Conjecture 1.2 (Generalized Ogg's conjecture)**.** *The rational torsion subgroup of $J_0(N)$ is the cuspidal group.*

(About the definition of the cuspidal group, see §2.3.)

For an Eisenstein maximal ideal $\mathfrak{m}$ of level N, we define

$$S_{\mathfrak{m}} := \text{ the set of primes at which } J[\mathfrak{m}] \text{ is ramified},$$

$$S_N := \text{ the set of prime divisors of } N,$$

$$s(\mathfrak{m}) := \#\{p \mid N\ :\ p \equiv 1 \pmod{\mathfrak{m}}\},$$

$$s_0(\mathfrak{m}) := \#\{p \mid N\ :\ U_p \equiv 1 \pmod{\mathfrak{m}}\}, \quad \text{and}$$

$$\varpi_0(\mathfrak{m}) := \begin{cases} s(\mathfrak{m}) & \text{if } s(\mathfrak{m}) = s_0(\mathfrak{m}) \\ 0 & \text{otherwise.} \end{cases}$$

For a finite set S of primes, we define

$$\varpi_\ell(S) := \#\{p \in S\ :\ p \equiv \pm 1 \pmod{\ell}\}.$$

In §4, we study the dimension of $J_0(N)[\mathfrak{m}]$ for an Eisenstein maximal ideal $\mathfrak{m}$ of residue characteristic $\ell \nmid 6N$. So, assume that $\ell \nmid 6N$.

Theorem 1.3. *Assume that $\varpi_\ell(S_N) = 1$. Then,*

$$\dim J_0(N)[\mathfrak{m}] = 2.$$

In other words, multiplicity one holds for an Eisenstein maximal ideal $\mathfrak{m}$.

We further prove a bound for $\dim J_0(N)[\mathfrak{m}]$ involves the two numbers $\varpi_0(\mathfrak{m})$ and $\varpi_\ell(S_{\mathfrak{m}})$.

Theorem 1.4. *We have*

$$\max\{1 + \varpi_0(\mathfrak{m}), 2\} \le \dim J_0(N)[\mathfrak{m}] \le 1 + \varpi_0(\mathfrak{m}) + \varpi_\ell(S_{\mathfrak{m}}).$$

Note that $\varpi_\ell(S_\mathfrak{m}) \leq \varpi_\ell(S_N)$ since $S_\mathfrak{m} \subseteq S_N \cup \{\ell\}$, so we can have an explicit bound of the dimension without further information about ramification of $J_0(N)[\mathfrak{m}]$. Recently, Ribet and the author proved that the above upper bound is *optimal* if $\varpi_0(\mathfrak{m}) = 0$. In other words, if $\varpi_0(\mathfrak{m}) = 0$, then

$$\dim J_0(N)[\mathfrak{m}] = 1 + \varpi_\ell(S_\mathfrak{m}).$$

The author expects that the above upper bound is optimal unless $\varpi_0(\mathfrak{m}) = 1$.

Theorem 1.3 can be applied to the study of the structure of $J_0(N)[\mathfrak{m}]$. If multiplicity one holds, it gives one of the models of the associated Galois representation $\rho_\mathfrak{m}$ to $\mathfrak{m}$. Moreover, $J_0(N)[\mathfrak{m}]$ can only be ramified at ℓ and a prime divisor p of N such that $p \equiv \pm 1 \pmod{\ell}$. In the case when N is the product of two distinct primes p and q, we prove a more precise result on $\dim J_0(N)[\mathfrak{m}]$. This result also gives the description of the Galois module $J_0(N)[\mathfrak{m}]$ by computing its dimension as a vector space over $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_\ell$.

1.1. **Notation.** Let $X_0(N)$ be the modular curve for $\Gamma_0(N)$ and let $J_0(N)$ be the Jacobian variety of $X_0(N)$. By Igusa [Ig59], Deligne-Rapaport [DR73], Katz-Mazur [KM85], and Raynaud [Ra70], there exists the Néron model of $J_0(N)$ over $\mathbb{Z}$, we denote it by $J_0(N)_{/\mathbb{Z}}$. We denote by $J_0(N)_{/\mathbb{F}_p}$ the special fiber of $J_0(N)_{/\mathbb{Z}}$ over $\mathbb{F}_p$. We denote by $M_2(\Gamma_0(N))$ (resp. $S_2(\Gamma_0(N))$) the space of modular (resp. cusp) forms of weight 2 and level $\Gamma_0(N)$ over $\mathbb{C}$.

From now on, we assume that ℓ is a prime larger than 3. And we assume that the level N is square-free and prime to ℓ.

For a square-free number N, we define

$$\varphi(N) := \prod_{p|N \text{ primes}} (p-1) \quad \text{and} \quad \psi(N) := \prod_{p|N \text{ primes}} (p+1).$$

For any group or module X, we denote by $\mathrm{End}(X)$ its endomorphism ring. We denote by $\mathbb{Z}/\ell\mathbb{Z}$ the constant group scheme of order ℓ. We denote by μ_ℓ the multiplicative group scheme of order ℓ. For a finite set S of primes, we denote by $\mathrm{Ext}_S(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ the group of extensions of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$, which are unramified outside S and are annihilated by ℓ.

Acknowledgements. The author would like to thank his advisor Kenneth Ribet. This paper would not exist if it were not for his inspired suggestions and his constant enthusiasm for the work. The author would like to thank Chan-Ho Kim, Sara Arias-de-Reyna, Sug Woo Shin, and Gabor Wiese for many suggestions toward the correction and improvement of this paper. The author would also like to thank Samsung scholarship for supporting him during the course of graduate research.

2. Eisenstein series and Eisenstein modules

2.1. **Hecke operators.** Throughout this section, we assume that p is a prime not dividing N and q is a prime divisor of N.

2.1.1. *Degeneracy maps on modular curves.* For a field K of characteristic not dividing Np, the points of $X_0(Np)$ over K are isomorphism classes of the triples (E, C, D), where E is a (generalized) elliptic curve over K, C is a cyclic subgroup of E of order N, and D is a cyclic subgroup of E of order p. Similarly, the points of $X_0(N)$ over K are isomorphism classes of the pairs (E, C). We can consider natural maps between modular curves

$$X_0(Np) \underset{\beta_p}{\overset{\alpha_p}{\rightrightarrows}} X_0(N),$$

where $\alpha_p(E, C, D) := (E, C)$ and $\beta_p(E, C, D) := (E/D, C + D/D)$. In other words, the map α_p is "forgetting level p structure" and the map β_p is "dividing by level p structure". As a map

$X_0(Np)(\mathbb{C}) \simeq \mathfrak{h}^*/\Gamma_0(Np) \to \mathfrak{h}^*/\Gamma_0(N) \simeq X_0(N)(\mathbb{C})$ on the complex points, α_p (resp. β_p) sends z to z (resp. to pz), where $\mathfrak{h}$ is the complex upper half plane and $\mathfrak{h}^* = \mathfrak{h} \bigcup \mathbb{P}^1(\mathbb{Q})$.

2.1.2. *Degeneracy maps on modular forms.* The maps α_p and β_p above induce maps α_p^* and β_p^* between cusp forms of weight two, respectively as follows.

$$S_2(\Gamma_0(N)) \underset{\beta_p^*}{\overset{\alpha_p^*}{\rightrightarrows}} S_2(\Gamma_0(Np)),$$

where $\alpha_p^*(f(\tau)) = f(\tau)$ and $\beta_p^*(f(\tau)) = pf(p\tau)$. On its Fourier expansions at $i\infty$, $\alpha_p^*(\sum a_n x^n) = \sum a_n x^n$ and $\beta_p^*(\sum a_n x^n) = p\sum a_n x^{pn}$. (Note that we use x-expansions instead of q-expansions because we denote by q a prime divisor of the level N.) These maps can also be extended to $M_2(\Gamma_0(N))$ via the same formula.

2.1.3. *Hecke operators on modular curves and modular forms.* The above degeneracy maps induce maps between divisor groups of modular curves. More specifically, we have

$$\mathrm{Div}(X_0(N)) \underset{\beta_p^*}{\overset{\alpha_p^*}{\rightrightarrows}} \mathrm{Div}(X_0(Np)) \underset{\beta_{p,*}}{\overset{\alpha_{p,*}}{\rightrightarrows}} \mathrm{Div}(X_0(N)),$$

where

$$\alpha_p^*(E,C) = \sum_{D \subset E[p]} (E, C, D),\ \beta_p^*(E,C) = \sum_{D \subset E[p]} (E/D, C + D/D, E[p]/D),$$

$$\alpha_{p,*}(E,C,D) = (E,C), \text{ and } \beta_{p,*}(E,C,D) = (E/D, C + D/D).$$

In the summation of the above formula, D runs through all cyclic subgroups of order p. We define T_p acting on $\mathrm{Div}(X_0(N))$ to be $\alpha_{p,*} \circ \beta_p^*$ or $\beta_{p,*} \circ \alpha_p^*$. In terms of divisors we have

$$T_p(E,C) = \sum_{D \subset E[p]} (E/D, C + D/D),$$

where D runs through all cyclic subgroups of order p. This map induces an endomorphism of the Jacobian $J_0(N)$, which is also denoted by T_p.

Since $S_2(\Gamma_0(N))$ can be identified with the cotangent space at 0 of $J_0(N)$, T_p acts on $S_2(\Gamma_0(N))$. The above definition is compatible with the action of Hecke operators on modular forms $M_2(\Gamma_0(N))$, which is (on their Fourier expansions at $i\infty$)

$$T_p(\sum a_n x^n) := \sum a_{np} x^n + p \sum a_n x^{np}.$$

2.1.4. *Atkin-Lehner operators and more on Hecke operators.* Let q be a prime divisor of N. Since N is square-free, q^2 does not divide N. Thus, $M := N/q$ is prime to q. We have an endomorphism w_q of $X_0(N)$ such that

$$w_q(E,C,D) = (E/D, C + D/D, E[q]/D),$$

where E is a (generalized) elliptic curve, C is a cyclic subgroup of E of order M, and D is a cyclic subgroup of order q. It induces an Atkin-Lehner involution on $J_0(N)$, which is also denoted by w_q. There is also the Hecke operator T_q in $\mathrm{End}(\mathrm{Div}(X_0(N)))$, which acts by

$$T_q(E,C,D) = \sum_{L \subset E[q]} (E/L, C + L/L, E[q]/L),$$

where L runs through all cyclic subgroups of E of order q, which are different from D. This operator also induces an endomorphism of $J_0(N)$ (via Albanese functoriality), which is also denoted by T_q.

Lemma 2.1. *As endomorphisms of $J_0(N)$, we have $T_q + w_q = \beta_q^* \circ \alpha_{q,*}$, where*

$$J_0(N) \underset{\beta_{q,*}}{\overset{\alpha_{q,*}}{\rightrightarrows}} J_0(M) \underset{\alpha_q^*}{\overset{\beta_q^*}{\rightrightarrows}} J_0(N).$$

Proof. On $\mathrm{Div}(X_0(N))$, $\alpha_{q,*}(E, C, D) = (E, C)$ and hence,

$$\beta_q^* \circ \alpha_{q,*}(E, C, D) = \sum_{L \subset E[q]} (E/L, C + L/L, E[q]/L),$$

where L runs through all cyclic subgroups of E of order q. It is equal to $(T_q + w_q)(E, C, D)$, therefore they induce the same map on $J_0(N)$. □

Remark 2.2. Note that $\alpha_q^* \circ \beta_{q,*} = w_q(\beta_q^* \circ \alpha_{q,*})w_q$ and $T_q^t = w_q T_q w_q$, where T_q^t is the transpose of T_q. If we use Picard functoriality of Jacobian varieties, the formula will be written as $T_q^t + w_q = \alpha_q^* \circ \beta_{q,*}$ (cf. on pages 444-446 in [R90]). From now on, we will use the Picard functoriality.

2.1.5. *Hecke algebras.* We define $\mathbb{T}_N$ as a $\mathbb{Z}$-subalgebra of $\mathrm{End}(J_0(N))$ generated by all T_n. Note that $\mathbb{T}_N$ is finite over $\mathbb{Z}$. Therefore all maximal ideals of $\mathbb{T}_N$ are of finite index. From now on, we will denote by U_q the Hecke operator T_q for primes q dividing the level N.

2.2. **Eisenstein series of $\Gamma_0(N)$.** The space $M_2(\Gamma_0(N))$ of modular forms naturally decomposes into its subspace of cusp forms $S_2(\Gamma_0(N))$ and the quotient space $M_2(\Gamma_0(N))/S_2(\Gamma_0(N))$, the *Eisenstein space* $E_2(\Gamma_0(N))$. We can pick a natural basis of $E_2(\Gamma_0(N))$ that consists of eigenfunctions for all Hecke operators. Since the number of cusps of $X_0(N)$ is 2^t, where t is the number of distinct prime factors of N, the dimension of $E_2(\Gamma_0(N))$ is $2^t - 1$.

Definition 2.3. We define e to be the normalized Eisenstein series of weight two and level 1,

$$e(\tau) := -\frac{1}{24} + \sum_{n=1}^{\infty} \sigma(n) x^n,$$

where $\sigma(n) = \sum_{d|n, d>0} d$ and $x = e^{2\pi i \tau}$.

Remark 2.4. Note that though e is an eigenfunction for all Hecke operators, e is not a classical modular form. And $e \pmod{\ell}$ is not a mod ℓ modular form of weight two (for a prime $\ell > 3$), which means that it cannot be expressed as a sum of mod ℓ modular forms of weight two of any level prime to ℓ. (In other words, the filtration of e is $\ell + 1$, not 2.) About this fact, see [M77], [S73], or [Sw73].

With the above function e, we can make Eisenstein series of weight two and level N by raising the level.

Definition 2.5. For any modular form g of level N and a prime p not dividing N,

$$[p]^+(g)(z) := (\alpha_p^* - \beta_p^*)(g) = g(z) - pg(pz) \quad \text{and}$$

$$[p]^-(g)(z) := (\alpha_p^* - \beta_p^*/p)(g) = g(z) - g(pz),$$

where α_p^* and $\beta_p^* : M_2(\Gamma_0(N)) \to M_2(\Gamma_0(Np))$ are the two degeneracy maps in the previous section.

Proposition 2.6. *Let g be an Eisenstein series of level N that is an eigenform for all Hecke operators. Then, for a prime p not dividing N, $[p]^+(g)$ and $[p]^-(g)$ are Eisenstein series of level Np such that the eigenvalues of U_p are 1 and p, respectively. They are eigenforms for all Hecke operators as well.*

Proof. On the p-old subvariety of $J_0(Np)$, U_p and T_p satisfy the following equality (cf. "Formulaire" 4 in [R89])

$$U_p \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} T_p & p \\ -1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

The first (resp. second) row maps into $J_0(Np)$ by the map α_p^* (resp. β_p^*). Since on g, T_p acts by $p+1$, U_p acts by 1 on $\left(\begin{smallmatrix} x \\ -x \end{smallmatrix}\right)$ and by p on $\left(\begin{smallmatrix} px \\ -x \end{smallmatrix}\right)$. Thus, the result follows. □

Remark 2.7. On the p-old subvariety of $J_0(Np)$, U_p satisfies the quadratic equation

$$X^2 - T_p X + p = 0$$

by the Cayley-Hamilton theorem.

Definition 2.8. For $1 \le s \le t$, let $N = \prod_{i=1}^{t} p_i$ and $M = \prod_{j=1}^{s} p_j$. We define

$$E_{M,N} := [p_t]^- \circ \cdots \circ [p_{s+1}]^- \circ [p_s]^+ \circ \cdots \circ [p_1]^+(e).$$

For given $N = \prod_{i=1}^{t} p_i$ and each $1 \le s \le t$, there are $\binom{t}{s}$ different choices for M. Thus, the number of all possible $E_{M,N}$ is $2^t - 1$. Since they are all eigenforms for the Hecke operators and their eigensystems are different, they form a basis of $E_2(\Gamma_0(N))$.

Remark 2.9. Note that $E_{1,N}$ is not a modular form of weight two because of the same reason as the case of $e = E_{1,1}$. When $N = p$, $E_{p,p} = [p]^+(e)$ is a unique eigenform (up to constant multiple) of level p, which is $-\frac{1}{24}e'$, where e' is the modular form on page 78 in [M77].

Later we will use these functions for computing the index of an Eisenstein ideal. For doing it, we need an information about constant terms of Fourier expansions of an Eisenstein series at various cusps, in particular, 0 or $i\infty$. Recall Proposition 3.34 in [FJ95].

Proposition 2.10 (Faltings-Jordan)**.** *Suppose that $N = pN'$ with $(N', p) = 1$. Let g be a modular form of weight k and level N', so $w_p g$ has level N.*

1. *The modular form $(\alpha(p) - w_p)g$ has constant term $\alpha(p)(1 - p^{k-1})a_0(g; c)$ at a p-multiplicative cusp c, $\alpha(p)(1 - 1/p)a_0(g; c)$ at a p-etale cusp c.*
2. *The modular form $(\beta(p)p^{k-1} - w_p)g$ has constant term 0 at a p-multiplicative cusp, $(p^{k-1}\beta(p) - \alpha(p)/p)a_0(g; c)$ at a p-etale cusp c.*

In our situation, $\alpha = \beta = 1$ (the trivial character), $k = 2$, and $w_p g(z) = pg(pz) = \beta_p^*(g)(z)$. Using the above result, we compute constant term of $E_{M,N}$ of level N at the multiplicative cusp $i\infty$, and the etale cusp 0. First recall that $E_{p,p}$ has constant term $-\frac{1-p}{24}$ at $i\infty$ and $-\frac{p-1}{24p}$ at 0 (cf. page 78 in [M77]).

Proposition 2.11. *The constant term of $E_{M,N}$ at $i\infty$ is either 0 if $M \neq N$ or $(-1)^{t+1}\frac{\varphi(N)}{24}$ if $M = N$. And its constant term at 0 is $-\frac{\varphi(N)\psi(N/M)}{24N(N/M)}$.*

Proof. Since $[p]^+(g)(z) = g(z) - pg(z) = (\alpha(p) - w_p)g$, its constant term at $i\infty$ (resp. at 0) is $(1-p)a_0(g)$ (resp. $\frac{1}{p}(p-1)b_0(g)$), where $a_0(g)$ (resp. $b_0(g)$) is the constant term of g at $i\infty$ (resp. at 0). Moreover, because $[p]^-(g)(z) = g(z) - g(pz) = \frac{1}{p}(\beta(p)p - w_p)g$, its constant term at $i\infty$ (resp. at 0) is 0 (resp. $\frac{1}{p^2}(p-1)(p+1)b_0(g)$). Thus, the result follows by induction. □

2.3. **The cuspidal group of $J_0(N)$.** Let P_n be the cusp corresponding to $\left(\begin{smallmatrix}1\\n\end{smallmatrix}\right)$ as in [Og74]. (It corresponds to $\frac{1}{n}$ in $\mathbb{P}^1(\mathbb{Q})$, so $P_1 = 0$ and $P_N = i\infty$.) Then the cusps of $X_0(N)$ are those of the form P_n for all possible positive divisors n of N. The cuspidal group of $J_0(N)$ is the group generated by all these cusps. We introduce some special elements of the cuspidal group of $J_0(N)$.

Definition 2.12. As in the previous section, let $N = \prod_{i=1}^{t} p_i$ and $M = \prod_{j=1}^{s} p_j$ for some $1 \le s \le t$. We define

$$C_{M,N} := \sum_{n|M} (-1)^{\omega(n)} P_n = P_1 - (\sum_{i=1}^{s} P_{p_i}) + \cdots + (-1)^s P_M \in J_0(N),$$

where $\omega(n)$ is the number of distinct prime divisors of n. And we denote by $\langle C_{M,N} \rangle$ the cyclic subgroup of $J_0(N)$ generated by $C_{M,N}$.

Proposition 2.13. *On the group $\langle C_{M,N} \rangle$, U_{p_i} acts by 1 for $1 \le i \le s$ and U_{p_j} acts by p_j for $s < j \le t$. For any prime r not dividing N, T_r acts by $r+1$ on $\langle C_{M,N} \rangle$. The order of $\langle C_{M,N} \rangle$ is the numerator of $\frac{\varphi(N)\psi(N/M)}{3}$ up to powers of 2.*

Proof. First, recall that for a prime divisor p of N, $U_p + w_p$ acts on $J_0(N)$ by $\alpha_p^* \circ \beta_{p,*}$, where α_p and β_p are the two degeneracy maps

$$X_0(N) \underset{\beta_p}{\overset{\alpha_p}{\rightrightarrows}} X_0(N/p)$$

and w_p is the Atkin-Lehner involution. (See Remark 2.2.) For some $D \mid N$ with $p \nmid D$, $\alpha_{p,*}(P_D) = \alpha_{p,*}(P_{pD}) = \beta_{p,*}(P_D) = \beta_{p,*}(P_{pD}) = P_D$. And $\alpha_p^*(P_D) = pP_D + P_{pD}$, $\beta_p^*(P_D) = P_D + pP_{pD}$. Moreover $w_p(P_D) = P_{pD}$, $w_p(P_{pD}) = P_D$. (cf. §5 in [R89].)

Let $p = p_i$ for some $1 \le i \le s$. Then $\beta_{p,*}(C_{M,N}) = 0$, hence $(U_p + w_p)(C_{M,N}) = \alpha_p^* \circ \beta_{p,*}(C_{M,N}) = 0$. Since $w_p(C_{M,N}) = -C_{M,N}$, $U_p(C_{M,N}) = C_{M,N}$.

Let $q = p_j$ for some $s < j \le t$. Then

$$w_q(C_{M,N}) = P_q - (\sum_{i=1}^{s} P_{qp_i}) + (\sum_{i<j}^{s} P_{qp_ip_j}) + \cdots + (-1)^s P_{qM} (=: C_{M,N}^{(q)})$$

and $\beta_{q,*}(C_{M,N}) = C_{M,N/q}$. Thus,

$$(U_q + w_q)(C_{M,N}) = \alpha_q^*(C_{M,N/q}) = qC_{M,N} + C_{M,N}^{(q)} = qC_{M,N} + w_q(C_{M,N}),$$

so $U_q(C_{M,N}) = qC_{M,N}$.

Next, let $r \nmid N$ be a prime. Then $T_r = \alpha_{r,*} \circ \beta_r^*$ on $J_0(N)$, where α_r and β_r are the two degeneracy maps

$$X_0(Nr) \underset{\beta_r}{\overset{\alpha_r}{\rightrightarrows}} X_0(N).$$

For any $D \mid N$, $\beta_r^*(P_D) = P_D + rP_{rD}$, so $\alpha_{r,*} \circ \beta_r^*(P_D) = (r+1)P_D$. Thus, $T_r(C_{M,N}) = (r+1)C_{M,N}$.

Finally, we compute the order of $C_{M,N}$ up to powers of 2. If $p = p_i$ for some $1 \le i \le s$, then

$$[p]^+(C_{M/p,N/p}) := (\alpha_p^* - \beta_p^*)(C_{M/p,N/p}) = (p-1)C_{M,N}.$$

If $p = p_j$ for some $s < j \le t$, then

$$[p]^-(C_{M,N/p}) := (p\alpha_p^* - \beta_p^*)(C_{M,N/p}) = (p^2-1)C_{M,N}.$$

Let $\gamma : J_0(N/p)^2 \to J_0(N)$, where $\gamma(x,y) = \alpha_p^*(x) + \beta_p^*(y)$. Then, the kernel of γ is the antidiagonal embedding of the Shimura subgroup of $J_0(N/p)$ by Ribet [R84]. Thus, the

restriction of γ to the cuspidal group is injective up to 2-torsion points because the cuspidal group is a constant group scheme and the Shimura subgroup is a multiplicative group scheme. Hence, $[p]^+$ and $[p]^-$ are both injective up to 2-torsion points. We prove the result on the order of $C_{M,N}$ up to powers of 2 by induction on t, the number of prime divisors of N.

When $t = 1$, the order of $C_{p,p} = P_1 - P_p$ in $J_0(p)$ is equal to the numerator of $\frac{p-1}{12}$. (cf. §11 of Chapter II in [M77]).

When $t = 2$, by Ogg [Og74], the orders of $C_{pq,pq}$ is the numerator of $\frac{(p-1)(q-1)}{24}$. By Chua and Ling [CL97], the order of $C_{p,pq}$ is the numerator of $\frac{(p-1)(q^2-1)}{24}$ unless $p \equiv 1 \pmod 8$ and $q = 2$, and the order of $C_{p,2p}$ is $\frac{p-1}{4}$ if $p \equiv 1 \pmod 8$. Thus, the orders of $C_{pq,pq}$ and $C_{p,pq}$ are the numerators of $\frac{(p-1)(q-1)}{3}$ and $\frac{(p-1)(q^2-1)}{3}$ up to powers of 2, respectively.

Let $N = pqr$ and consider the ℓ-primary part of the cyclic group $\langle C_{pqr,pqr}\rangle$, say A_ℓ, for a prime $\ell \geq 3$. For simplicity, we denote by $\mathrm{num}(n)$ the numerator of a rational number n. Since $(r-1)C_{pqr,pqr} = [r]^+(C_{pq,pq})$, the order of A_ℓ divides $\mathrm{num}(\frac{(p-1)(q-1)(r-1)}{3})$. Hence, assume that $\ell \mid \mathrm{num}(\frac{(p-1)(q-1)(r-1)}{3})$. If $r \not\equiv 1 \pmod \ell$, then the order of A_ℓ is equal to the ℓ-primary part of $\langle C_{pq,pq}\rangle$, so the result holds. Hence we assume that $p \equiv q \equiv r \equiv 1 \pmod \ell$. Let ℓ^a (resp. ℓ^b) be the power of ℓ exactly dividing $\mathrm{num}(\frac{(p-1)(q-1)}{3})$ (resp. $r-1$). Then, since $(r-1)C_{pqr,pqr}$ is of order $\mathrm{num}(\frac{(p-1)(q-1)}{3})$ up to powers of 2, $\frac{1}{\ell}\mathrm{num}(\frac{(p-1)(q-1)}{3})[(r-1)C_{pqr,pqr}] \neq 0$. In other words, ℓ^{a+b} annihilates A_ℓ but $\ell^{(a+b-1)}A_\ell \neq 0$. Hence ℓ^{a+b} is the order of A_ℓ and it is the power of ℓ exactly dividing $\mathrm{num}(\frac{(p-1)(q-1)(r-1)}{3})$. Hence, by considering all prime factors of $\mathrm{num}(\frac{(p-1)(q-1)(r-1)}{3})$ except 2, we have the order of $C_{pqr,pqr}$ is equal to $\mathrm{num}(\frac{(p-1)(q-1)(r-1)}{3})$ up to powers of 2.

For the case $C_{pq,pqr}$, note that $(r^2-1)C_{pq,pqr} = [r]^-(C_{pq,pq})$ and $(p-1)C_{pq,pqr} = [q]^+(C_{p,pr})$. By the same method as above (by replacing $r-1$ and $C_{pqr,pqr}$ by r^2-1 and $C_{pq,pqr}$, respectively), we have the desired result. The same method works for the case $C_{p,pqr}$.

The above method can be generalized to the case $t > 3$ and it works without further difficulties. □

2.4. **The Shimura subgroup of $J_0(N)$.** The Shimura subgroup is the kernel of the map $J_0(N) \to J_1(N)$, which is induced by the natural covering $X_1(N) \to X_0(N)$. Since the covering group of $X_1(N) \to X_0(N)$ is $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, one of the maximal étale subcovering of $X_1(N) \to X_0(N)$ is a quotient of $(\mathbb{Z}/N\mathbb{Z})^\times/\{\pm 1\}$, which is the Cartier dual of the Shimura subgroup. When N is prime, Mazur discussed it on §11 of Chapter II in [M77]. (In general, see the paper by Ling and Oesterlé [LO90].)

As before let $N = \prod_{i=1}^{t} p_i$ and Σ_N be the Shimura subgroup of $J_0(N)$. By the Chinese remainder theorem, $(\mathbb{Z}/N\mathbb{Z})^* \simeq (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_t\mathbb{Z})^*$. Similarly, we can decompose the Shimura subgroups as

$$\Sigma_N \simeq \Sigma_{p_1} \times \cdots \times \Sigma_{p_t}.$$

Each Σ_{p_i} corresponds to the subcovering $X_1(p_i, N/p_i) \to X_0(N)$ of $X_1(N) \to X_0(N)$, where $X_1(A, B)$ is the modular curve for the group $\Gamma_1(A) \cap \Gamma_0(B)$. Note that Σ_{p_i} is cyclic of order $p_i - 1$ up to products of powers of 2 and 3.

Proposition 2.14 (Ling-Oesterlé). *On Σ_{p_i}, U_{p_i} acts by 1, U_{p_j} acts by p_j for $j \neq i$, and T_r acts by $r+1$ for primes $r \nmid N$.*

Proof. Ling and Oesterlé proved that T_p acts on Σ by p for primes $p \mid N$. (See Theorem 6 in [LO90].) In our case, since Σ_{p_i} has order dividing $p_i - 1$, the result follows from their work. □

2.5. **Component group of $J_0(N)$.** The component group of $J_0(N)$ for square-free level N is explained in the appendix of [M77]. Let $N = pM$, $(p, M) = 1$, and $J := J_0(N)$. Assume that M is square-free. Then, by results of Deligne-Rapoport [DR73] and Raynaud [Ra70], $J_{\mathbb{F}_p}$ is an extension of a finite group $\Phi_p(J)$, *the component group of* $J_{\mathbb{F}_p}$, by a semiabelian variety J^0, *the identity component of* $J_{\mathbb{F}_p}$. Moreover J^0 is an extension of $J_0(M)_{/\mathbb{F}_p} \times J_0(M)_{/\mathbb{F}_p}$ by T, *the torus of* $J_{\mathbb{F}_p}$.

Proposition 2.15. *The order of $\Phi_p(J)$ is equal to $(p-1)\psi(M)$ up to products of powers of 2 and 3, and $\Phi_p(J) = \Phi \oplus A$, where Φ is generated by the image of $C_{p,M} = P_1 - P_p$ and the order of A divides some product of powers of 2 and 3. Moreover Frob_p, the Frobenius endomorphism in characteristic p, acts by $-pw_p$ on T, where w_p is the Atkin-Lehner operator defined in §2.1.*

Proof. This is the main result of the appendix in [M77] by Mazur and Rapoport. Since P_p and P_N lie in the same component of the Néron model of $X_0(pN)$ over $\mathbb{F}_p$, the elements $P_1 - P_p$ and $P_1 - P_N$ generate the same group Φ in their paper (*loc. cit.*). □

Remark 2.16. Since the Hecke action on T factors through the p-new quotient of $\mathbb{T}_N$ (Proposition 3.7 in [R90]), $U_p + w_p$ annihilates T. Therefore Frob_p acts by pU_p on T.

Proposition 2.17. *On Φ, U_p acts by 1, U_q acts by q for $q \mid M$ primes, and T_r acts by $r+1$ for $r \nmid N$ primes. Moreover for a prime $\ell > 3$, $\Phi_p(J)[\ell]$, the ℓ-torsion elements in $\Phi_p(J)$, is equal to $\Phi[\ell]$, and $\Phi[\ell] \simeq \mathbb{Z}/\ell\mathbb{Z}$ as groups if $\ell \mid (p-1)\psi(M)$.*

Proof. Because the reduction map is Hecke equivariant, this is an easy consequence of Proposition 2.13 and Proposition 2.15. □

Remark 2.18. Since the order of $C_{p,M}$ (resp. of Φ) is $\varphi(N)\psi(M)$ (resp. $(p-1)\psi(M)$) up to products of powers of 2 and 3, the kernel of the map $\langle C_{p,M}\rangle \twoheadrightarrow \Phi$ is of order $\varphi(N/p)$ up to products of powers of 2 and 3. Therefore, if $\ell \nmid \varphi(N/p)$ and $\ell > 3$, the order ℓ subgroup of $\langle C_{p,M}\rangle$ maps isomorphically into $\Phi[\ell] = \Phi_p(J)[\ell]$.

3. The index of an Eisenstein ideal

For an ideal of $\mathbb{T}_N$, we call it *Eisenstein* if it contains $T_r - r - 1$ for all but finitely many primes r not dividing the level N.

3.1. **Square-free level.** As before let $N = \prod_{i=1}^{t} p_i$ and $M = \prod_{j=1}^{s} p_j$ for some $1 \le s \le t$. On the p-old space of $J_0(N)$, U_p satisfies the quadratic equation $X^2 - T_pX + p = 0$. (See Remark 2.7.) Hence, if p divides the level N, the eigenvalue of U_p is 1 or p for (old) Eisenstein ideals. Let

$$I_M := (U_{p_i} - 1,\ U_{p_j} - p_j,\ T_r - r - 1\ :\ 1 \le i \le s,\ s < j \le t,\ \text{for all primes } r \nmid N)$$

be an Eisenstein ideal of $\mathbb{T}_N$. For simplicity, let $\mathbb{T} := \mathbb{T}_N$.

Lemma 3.1. *The quotient ring $\mathbb{T}/I_M$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some integer $n > 0$.*

Proof. The natural map $\mathbb{Z} \to \mathbb{T}/I_M$ is surjective, since, modulo I_M, the operators T_p are all congruent to integers. Let $F(z) := \sum_{n\ge1}(T_n \pmod{I_M})x^n$, where $x = e^{2\pi iz}$. We cannot have $\mathbb{T}/I_M = \mathbb{Z}$, for then F would be a Fourier expansion at $i\infty$ of a cuspidal eigenform over $\mathbb{C}$, which contradicts the Ramanujan-Petersson bounds. Therefore $\mathbb{T}/I_M \simeq \mathbb{Z}/n\mathbb{Z}$ for some integer $n > 0$. □

We want to compute this n for understanding when the ideal $\mathfrak{m}$ generated by ℓ and I_M becomes maximal. (If n and ℓ are relatively prime, $\mathfrak{m} = \mathbb{T}$.) In §4, we handle the case when $\ell > 3$ and $\ell \nmid N$. Thus, the following is enough for our application.

Theorem 3.2. *For a prime $y \nmid 2N$,*

$$(\mathbb{T}/I_M) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y,$$

where m is the numerator of $\frac{\varphi(N)\psi(N/M)}{3}$.

Proof. Let $\mathbb{T}/I_M \simeq \mathbb{Z}/n\mathbb{Z}$ and $y \nmid 2N$ be a prime. Let $n = y^a \times b$ and $m = y^c \times d$, where $(y, bd) = 1$. Let $J = (y^a, I_M)$. Then, $\mathbb{T}/J \simeq \mathbb{Z}/y^a\mathbb{Z}$ and $(\mathbb{T}/I_M) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{T}/J) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq \mathbb{Z}/y^a\mathbb{Z}$.

Since the cuspidal divisor $C_{M,N}$ has order m up to powers of 2 by Proposition 2.13, $\langle C_{M,N} \rangle$ has an order y^c subgroup, say D. Because I_M annihilates $C_{M,N}$ by Proposition 2.13, it also kills D. Thus, there is a natural surjection

$$\mathbb{T}/I_M \simeq \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathrm{End}(D) \simeq \mathbb{Z}/y^c\mathbb{Z}.$$

Therefore $y^c \mid n = y^a \times b$, so $c \leq a$.

If $a = 0$, then there is nothing to prove. Assume that $a > 0$. We follow the argument in §5 of Chapter II in [M77]. Let $f(z) := \sum_{n \geq 1} (T_n \pmod J) x^n$, where $x = e^{2\pi i z}$. It is a cusp form over the ring $\mathbb{Z}/y^a\mathbb{Z}$. Note that $24f$ is a cusp form over $\mathbb{Z}/24y^a\mathbb{Z}$. Let $E_{M,N}$ be an Eisenstein series defined in §2.2. We divide into three cases.

(1) Case 1 : Assume that $M = N$. Since $24E_{N,N}$ has an integral Fourier expansion at $i\infty$, $24E_{N,N} \pmod{24y^a}$ is a modular form over $\mathbb{Z}/24y^a\mathbb{Z}$. Thus, $\varphi(N) = 24(f - E_{N,N}) \pmod{24y^a}$ (up to sign) is a modular form over $\mathbb{Z}/24y^a\mathbb{Z}$. Therefore $24y^a \mid 2\varphi(N)$ (cf. Proposition 5.12.(iii) of *loc. cit.*), so y^a divides $y^c \times d = m$, the numerator of $\frac{\varphi(N)}{3}$, which implies $a \leq c$. Thus, $a = c$ and

$$(\mathbb{T}/I_M) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

(2) Case 2 : Assume that $M \neq N$ and $y > 3$. Since $g = (f - E_{M,N}) \pmod{y^a}$, which is a modular form over $\mathbb{Z}/y^a\mathbb{Z}$, has a Fourier expansion at $i\infty$ equals to 0, it is 0 (on the irreducible component of $X_0(N)$ that contains $i\infty$) by the q-expansion principle. Since N is invertible in $\mathbb{Z}/y^a\mathbb{Z}$, we can consider a Fourier expansion at the cusp 0. On the other hand, since f is a cusp form, its constant term at the cusp 0 is 0. Hence the constant term of g at the cusp 0, which is $\frac{\varphi(N)\psi(N/M)}{24N(N/M)}$ by Proposition 2.11, is 0 modulo y^a. Thus, $y^a \mid m = y^c \times d$, hence $a \leq c$. So, $a = c$ and

$$(\mathbb{T}/I_M) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

(3) Case 3 : Assume that $M \neq N$ and $y = 3$. Since $h = 24(f - E_{M,N}) \pmod{24 \times 3^a}$ is a modular form over $\mathbb{Z}/(24 \times 3^a\mathbb{Z})$, it is also a modular form over $\mathbb{Z}/3^{a+1}\mathbb{Z}$. By the same argument as above, the constant term of h at the cusp 0, which is $\frac{\varphi(N)\psi(N/M)}{N(N/M)}$, is 0 modulo 3^{a+1}. Hence, $3^{a+1} \mid \varphi(N)\psi(N/M)$. Therefore $m = \frac{\varphi(N)\psi(N/M)}{3} = 3^c \times d$ and $a \leq c$. So, $a = c$ and

$$(\mathbb{T}/I_M) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

□

Remark 3.3. In the proof of the above theorem, we also prove that the y-primary subgroup of $\langle C_{M,N} \rangle$ is a free of rank one $\mathbb{T}_y/I_M$-module for an odd prime y not dividing N, where $\mathbb{T}_y := \mathbb{T} \otimes \mathbb{Z}_y$.

3.2. **New Eisenstein ideals.** Let $N := pq$. (Since we assume that N is square-free, $p \neq q$.) On the new subspace of $J_0(N)$, U_p acts by an involution. Thus, possible eigenvalues of U_p are either 1 or -1. Let

$$I := (U_p - 1,\ U_q + 1,\ T_r - r - 1\ :\ \text{for all primes } r \nmid N)$$

be a (new) Eisenstein ideal of level N.

In this case, we can compute the index of I up to powers of 2. More specifically, let $\mathbb{T}/I \simeq \mathbb{Z}/n\mathbb{Z}$ for some n. For an odd prime y, let $m = q + 1$ if either $y \neq 3$, $3 \mid (p-1)$, or $3 \nmid (q+1)$. Otherwise, we set $m = \frac{q+1}{3}$.

Theorem 3.4. *Then,*

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

Proof. Let $n = y^a \times b$ and $m = y^c \times d$, where $(y, bd) = 1$. Let $J = (y^a, I)$. Then $\mathbb{T}/J \simeq \mathbb{Z}/y^a\mathbb{Z}$. We divide into five cases.

(1) Case 1 : Assume that $y > 3$ and $y \neq q$. Since the order of the cuspidal divisor $(p-1)(q-1)C_{p,pq} = (p-1)(q-1)(P_1 - P_p)$ in $J_0(pq)$ is the numerator of $\frac{q+1}{3}$ up to powers of 2, $\langle C_{p,pq} \rangle$ contains a subgroup D of order y^c and it is annihilated by I. Thus, there is a natural surjection

$$\mathbb{T}/I \simeq \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathrm{End}(D) \simeq \mathbb{Z}/y^c\mathbb{Z}.$$

Therefore $y^c \mid n = y^a \times b$, especially $c \leq a$ because $(y, b) = 1$. If $a = 0$, then there is nothing to prove. Assume that $a > 0$. Let $f(z) = \sum_{n \geq 1} (T_n \pmod J) x^n$, where $x = e^{2\pi i z}$. It is a cusp form over the ring $\mathbb{Z}/y^a\mathbb{Z}$. Consider $24(f - E_{p,pq}) \pmod{y^a} = 24 \sum_{n \geq 1} a_n x^n$, where $E_{p,pq}$ is the Eisenstein series in §2.2. Note that q is invertible in $\mathbb{Z}/y^a\mathbb{Z}$ and $a_n = 0$ for $(n, q) = 1$. Thus, by Mazur (Lemma 5.9 of Chapter II in [M77]), there is a modular form g of level p over the ring $\mathbb{Z}/y^a\mathbb{Z}$, such that $g(x^q) = 24[(f - E_{p,pq}) \pmod{y^a}](x) = 24 \sum_{n \geq 1} a_n x^n$. Computing its coefficient, we get $g(x) = -24(q+1) \sum c_n x^n$, where $c_r = r + 1$, $c_1 = 1$, $c_p = 1$, and $c_q = q - 1$. This is also an eigenform for the Hecke operators T_r, $r \neq q$. Since $\mathbb{T}_p$ is generated by T_r for all primes $r \neq q$, it is genuinely an eigenform for all Hecke operators. However, at level p, there is only one eigenform h whose eigenvalue for T_r is $r + 1$ for every $r \neq p$ up to constant multiple, and it has an eigenvalue $q + 1$ for the operator T_q. Therefore if $-24(q+1)$ is not zero in $\mathbb{Z}/y^a\mathbb{Z}$, $g = -24(q+1)h$ and $24(q+1)((q-1) - (q+1)) = 0$ in $\mathbb{Z}/y^a\mathbb{Z}$, which is a contradiction because $y > 2$. Therefore $y^a \mid 24(q+1) = y^c \times 24d$, and hence, $a \leq c$ because $(y, 24d) = 1$. So, $a = c$ and

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y$$

for primes y not dividing $6q$.

(2) Case 2 : Assume that $y = 3 \neq q$ and $3 \mid (p-1)$. Then we can find a subgroup of order $q + 1$ in $\langle (q-1)C_{p,q} \rangle$. So, by the same argument as above, we have $c \leq a$. Assume that $a > 0$. As before, $f(z) = \sum_{n \geq 1} (T_n \pmod J) x^n$ is a cusp form over the ring $\mathbb{Z}/3^a\mathbb{Z}$. Thus, $24f(z)$ can be regarded as a cusp form over the ring $\mathbb{Z}/(24 \times 3^a\mathbb{Z})$, hence it is a cusp form over the ring $\mathbb{Z}/3^{a+1}\mathbb{Z}$. As above, $24(f - E_{p,pq}) \pmod{3^{a+1}} = 0$ and $3^{a+1} \mid 24(q+1) = 3^{c+1} \times 8d$. Therefore $a \leq c$, so $a = c$ and

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

(3) Case 3 : Assume that $y = 3 \neq q$ and $3 \nmid (p-1)(q+1)$. Then, $c = 0$. Assume that $a > 0$. Then, by the same argument as above, we have $3^{a+1} \mid 24(q+1)$, which is a contradiction. Therefore $a = 0$ and

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq 0.$$

(4) Case 4 : Assume that $y = 3 \neq q$, $3 \nmid (p-1)$ and $3 \mid (q+1)$. Then we can find a subgroup of order $m = \frac{q+1}{3}$ in $\langle (p-1)(q-1)C_{p,q} \rangle$. By the same argument as above, we have $c \leq a$. Assume that $a > 0$. As above, $g = 24(f - E_{p,pq}) \pmod{3^{a+1}} = 0$, so it is zero on the irreducible component of $X_0(pq)_{/\mathbb{F}_3}$ containing $i\infty$. Since q is invertible in $\mathbb{Z}/3^{a+1}\mathbb{Z}$, a q-etale cusp P_p lies in the same component as $i\infty$. Hence, the constant term of the Fourier expansion of g at P_p is 0 modulo 3^{a+1}, which is $-\frac{(p-1)(q^2-1)}{q^2}$. (The computation follows from Proposition 2.10.) Hence, $3^{a+1} \mid (q+1) = 3^{c+1} \times d$ since $(3, q(p-1)(q-1)) = 1$. Therefore $a \leq c$, so $a = c$ and

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

(5) Case 5 : Assume that $y = q > 2$. Let $\mathfrak{m} := (y, I)$ be an Eisenstein ideal of characteristic y. Assume that $\mathfrak{m}$ is maximal. If $\mathfrak{m}$ is new, then the associated mod y Galois representation $\rho_{\mathfrak{m}}$ is isomorphic to $1 \oplus \chi$, where χ is the mod y cyclotomic character. (cf. Proposition 2.1 in [Y14].) By considering the image of a decomposition group of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at q, we have $\rho_{\mathfrak{m}}(\mathrm{Frob}_q) \equiv 1 + q \equiv -(1+q) \pmod{\mathfrak{m}}$, where Frob_q is an arithmetic Frobenius of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at q. Therefore, $q \equiv -1 \pmod{y}$, which is a contradiction. Thus, $\mathfrak{m}$ is old. Since there is no Eisenstein ideals of characteristic y at level q, $\mathfrak{m}$ is q-old and y divides the numerator of $\frac{p-1}{12}$. Since on the q-old space, the eigenvalue of U_q is either 1 or q and $U_q \equiv -1 \pmod{\mathfrak{m}}$, $q \equiv -1 \pmod{y}$, which is a contradiction. Therefore $\mathfrak{m}$ is not maximal. In other words,

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq 0.$$

□

Remark 3.5. In the last part of proof, we cited the result in the paper [Y14]. Even though the author presented only the case $\ell \neq q$, the method can be generalized to the case $\ell = q$. In fact, Ribet presented a proof of the case when $\ell = q$ as well [R08]. In particular, he proved that $T_\ell \equiv 1 \pmod{\mathfrak{m}}$ for an Eisenstein maximal ideal $\mathfrak{m}$ of residue characteristic ℓ (Lemma 1.1 in [R08]).

Remark 3.6. In the proof of the above theorem, we also prove that the y-primary subgroup of $\langle (p-1)(q-1)C_{p,pq} \rangle$ is a free of rank one $\mathbb{T}_y/I$-module for primes $y > 3$.

By the same argument as above (in particular, the method used in the proof of Case 1), we can prove the following.

Theorem 3.7. *Let $N = Mq$, $(M, q) = 1$, and $y \nmid 6N$. Let $I = (U_p - 1,\ U_q + 1,\ T_r - r - 1$: for all primes $p \mid M$, for all primes $r \nmid N)$. Then,*

$$(\mathbb{T}/I) \otimes_{\mathbb{Z}} \mathbb{Z}_y \simeq (\mathbb{Z}/(q+1)\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_y.$$

4. Multiplicity one

4.1. **Square-free level.** As before let $N = \prod_{i=1}^{t} p_i$ and $M = \prod_{j=1}^{s} p_j$ for some $1 \leq s \leq t$. Let $\mathbb{T} := \mathbb{T}_N$ and $J := J_0(N)$. For an ideal $I \subseteq \mathbb{T}$, we define the kernel of I for J as follows,

$$J[I] := \{x \in J_0(N)(\overline{\mathbb{Q}}) : Tx = 0 \text{ for all } T \in I\}.$$

Since $\mathbb{T}$ acts faithfully on J, $J[\mathfrak{m}] \neq 0$ for a maximal ideal $\mathfrak{m}$.

As we explained in the introduction, for a non-Eisenstein maximal ideal $\mathfrak{m}$, there is a notion of multiplicity. On the other hand, there is no natural one for an Eisenstein ideal $\mathfrak{m}$. Instead, we define it as follows.

Definition 4.1. Multiplicity one holds for $\mathfrak{m}$ if $\dim_{\mathbb{T}/\mathfrak{m}} J[\mathfrak{m}] = 2$.

In contrast to the non-Eisenstein case, the multiplicity one question for an Eisenstein ideal $\mathfrak{m}$ has not been discussed much before. Mazur [M77] proved that when N is prime, $J[\mathfrak{m}] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$ for an Eisenstein maximal ideal $\mathfrak{m}$ of residue characteristic $\ell \geq 3$.

Assume that $\ell > 3$ is a prime and $(\ell, N) = 1$. Let $\mathfrak{m} := (\ell, I_M)$, where

$$I_M := (U_{p_i} - 1,\ U_{p_j} - p_j,\ T_r - r - 1\ :\ 1 \leq i \leq s,\ s < j \leq t,\ \text{for all primes } r \nmid N).$$

By the result of Theorem 3.2, $\mathfrak{m}$ is maximal if and only if $\ell \mid \varphi(N)\psi(N/M)$. Thus, we assume that $\ell \mid \varphi(N)\psi(N/M)$. If $p_j \equiv 1 \pmod{\ell}$ for some $s < j \leq t$, then $\mathfrak{m} = (\ell, I_{M\times p_j})$. Thus, we further assume that $p_j \not\equiv 1 \pmod{\ell}$ for all $s < j \leq t$. So, we have $s_0(\mathfrak{m}) = s$, $1 \leq s_0(\mathfrak{m}) \leq t$, and $0 \leq s(\mathfrak{m}) \leq s_0(\mathfrak{m})$. (For the definition of notation, see the introduction.)

Let S_N be the set of prime divisors of N and let $S_\mathfrak{m}$ be the set of primes at which $J[\mathfrak{m}]$ is ramified. Then, $S_\mathfrak{m} \subseteq S_N \cup \{\ell\}$ by Igusa and $\varpi_\ell(S_\mathfrak{m}) \leq \varpi_\ell(S_N)$.

Theorem 4.2 (Multiplicity one)**.** *Assume one of the following.*

(1) $\varpi_\ell(S_N) = 1$.
(2) $t = s + 1$ *and* $\ell \nmid \varphi(N)$.

Then multiplicity one holds for $\mathfrak{m}$*, i.e.,* $J[\mathfrak{m}]$ *is of dimension 2 over* $\mathbb{T}/\mathfrak{m}$.

Proof. We follow Mazur's idea in his paper [M77] to analyze $J[\mathfrak{m}]$.

(1) Assume that $\varpi_\ell(S_N) = 1$. We divide into three cases.
   (a) Case 1 : Assume that $s(\mathfrak{m}) = 0$. Then, $\Sigma_N[\mathfrak{m}] = 0$ but $\langle C_{M,N}\rangle[\mathfrak{m}] \simeq \mathbb{Z}/\ell\mathbb{Z}$ as Galois modules because $C_{M,N} \in J(\mathbb{Q})$. Since the $\mathfrak{m}$-adic Tate module $\mathrm{Ta}_\mathfrak{m} J := \varprojlim_n J[\mathfrak{m}^n]$ is of rank 2 over $\mathbb{T}_\mathfrak{m} := \varprojlim_n \mathbb{T}/\mathfrak{m}^n$ (Lemma 7.7 of Chapter II in [M77]), the dimension of $J[\mathfrak{m}]$ over $\mathbb{T}/\mathfrak{m}$ is at least 2. All Jordan-Hölder factors of $J[\mathfrak{m}]$ are either $\mathbb{Z}/\ell\mathbb{Z}$ or μ_ℓ (cf. Proposition 14.1 of Chapter II in [M77]). Moreover, $J[\mathfrak{m}]$ can have at most one $\mathbb{Z}/\ell\mathbb{Z}$ as its Jordan-Hölder factor by the q-expansion principle. (cf. Corollary 14.8 of Chapter II in [M77], note that $T_\ell - 1 \in \mathfrak{m}$, hence, it is ordinary. See also Lemma 2.7 in [CS08].) Since $\langle C_{M,N}\rangle[\mathfrak{m}] \simeq \mathbb{Z}/\ell\mathbb{Z}$, $\mathbb{Z}/\ell\mathbb{Z} \subseteq J[\mathfrak{m}]$. Thus,

$$0 \to \mathbb{Z}/\ell\mathbb{Z} \to J[\mathfrak{m}] \to A \to 0,$$

   where A is a multiplicative group such that all its Jordan-Hölder factors are μ_ℓ. Since A is annihilated by $T_r - r - 1$ for all but finitely many primes r, by the theorem of constancy (Lemma 3.5 of Chapter I in [M77]), $A \simeq {\mu_\ell}^{\oplus r}$ for some $r \geq 1$. Since the Shimura subgroup Σ_N is a maximal multiplicative subgroup of J by Vatsal (Theorem 1.1 in [Va05]) and $\Sigma_N[\mathfrak{m}] = 0$, $\mu_\ell \nsubseteq J[\mathfrak{m}]$. Let $S_0 = S_N \cup \{\ell\}$ and $E := \mathrm{Ext}_{S_0}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ be the group of extensions of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$ that are annihilated by ℓ and are unramified outside S_0. By Brumer-Kramer (Proposition 4.2.1 in [BK14]), the dimension of E over $\mathbb{F}_\ell$ is $\varpi_\ell(S_0) = \varpi_\ell(S_N)$, which is 1 by assumption. (It is generated by a non-trivial extension only ramified at a prime ℓ and p such that $p \equiv \pm 1 \pmod{\ell}$.) Assume that $\dim J[\mathfrak{m}] \geq 3$, then it has a submodule V of dimension 3 that is a nontrivial extension of $\mu_\ell \oplus \mu_\ell$ by $\mathbb{Z}/\ell\mathbb{Z}$. Let α (resp. β) be a natural inclusion of μ_ℓ into the first (resp. second) component of $\mu_\ell \oplus \mu_\ell$,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & V & \longrightarrow & \mu_\ell \oplus \mu_\ell & \longrightarrow & 0 \\
 & & \| & & \alpha\uparrow\uparrow\beta & & \alpha\uparrow\uparrow\beta & & \\
0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & W & \longrightarrow & \mu_\ell & \longrightarrow & 0.
\end{array}$$

Then α^*V and β^*V are two elements in E, which is of dimension 1. Thus, there are $a, b \in \mathbb{F}_\ell$ such that $a\alpha^*V + b\beta^*V = 0$. Let $\gamma = a\alpha + b\beta$, then $\mu_\ell \subseteq \gamma^*V \subseteq V$, which is a contradiction. Therefore $\dim J[\mathfrak{m}] = 2$.

(b) Case 2 : Assume that $s(\mathfrak{m}) = 1$ but $s_0(\mathfrak{m}) = s > 1$. Then the same argument as above holds since $\Sigma_N[\mathfrak{m}] = 0$.

(c) Case 3 : Assume that $s(\mathfrak{m}) = s_0(\mathfrak{m}) = 1$. Let $p = p_1 \equiv 1 \pmod{\ell}$. Note that $\Sigma_N[\mathfrak{m}] \simeq \mu_\ell$, hence, $\mu_\ell \subseteq J[\mathfrak{m}]$ but $\mu_\ell \oplus \mu_\ell \nsubseteq J[\mathfrak{m}]$ from the assumption. Let $J[\mathfrak{m}]$ be an extension of ${\mu_\ell}^{\oplus r}$ by $\mathbb{Z}/\ell\mathbb{Z}$ for some r. Let I_p be an inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at p. By a well known theorem of Serre-Tate [ST68], the kernel of $\mathfrak{m}$ in the mod p reduction of J may be identified with $J[\mathfrak{m}]^{I_p}$, the group of I_p-invariants. Since $\ell \nmid \varphi(N/p)$ and the component group Φ_p of $J_{/\mathbb{F}_p}$ is generated by the image of $C_{p,N} = P_1 - P_p$ up to 2-, 3-primary groups, $\langle C_{p,N}\rangle[\mathfrak{m}] \simeq \mathbb{Z}/\ell\mathbb{Z} \subseteq J[\mathfrak{m}]$ maps isomorphically into $\Phi_p[\mathfrak{m}]$. (See Remark 2.18.) Thus, we can copy Mazur's argument on page 125-126 of [M77]. Thus, there is an exact sequence

$$0 \longrightarrow \mathbb{Z}/\ell\mathbb{Z} \longrightarrow J[\mathfrak{m}]^{I_p} \longrightarrow ({\mu_\ell}^{\oplus r})^{I_p} = {\mu_\ell}^{\oplus r} \longrightarrow 0.$$

Therefore $J[\mathfrak{m}]$ is unramified at p and $p \notin S_\mathfrak{m}$. Thus, $\varpi_\ell(S_\mathfrak{m}) = 0$. If $\dim J[\mathfrak{m}] \geq 3$, then it contains a non-trivial extension of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$, which is annihilated by ℓ and is unramified outside $S_\mathfrak{m}$. However, the dimension of $\mathrm{Ext}_{S_\mathfrak{m}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$ is $\varpi_\ell(S_\mathfrak{m}) = 0$, which is a contradiction. Hence $\dim J[\mathfrak{m}] = 2$ and $J[\mathfrak{m}] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$.

(2) Let $q = p_t$ for simplifying notation. Since $\ell \mid \varphi(N)\psi(q)$, $q \equiv -1 \pmod{\ell}$. As in §2.5, let J^0, Φ_q, and T denote the identity component, the component group, and the torus of $J_{/\mathbb{F}_q}$, respectively. Then, by Proposition 2.17, $\Phi_q[\mathfrak{m}] = 0$. Since on $T[\mathfrak{m}]$, Frob_q acts by $qU_q \equiv 1 \pmod{\ell}$ and $q \equiv -1 \pmod{\ell}$, $T[\mathfrak{m}]$ cannot contain μ_ℓ. Thus, $\dim T[\mathfrak{m}] \leq 1$. Since $\ell \nmid \varphi(N)$, the index of the ideal $I_{N/q} = (U_{p_i} - 1,\ T_r - r - 1 \ :\ 1 \leq i \leq s,\ \text{for all primes } r \nmid N/q)$ of $\mathbb{T}_{N/q}$ is prime to ℓ. Therefore $J_0(N/q)^2[\mathfrak{m}] = 0$, which implies that $J_{/\mathbb{F}_q}[\mathfrak{m}] \simeq J[\mathfrak{m}]^{I_q}$ is at most of dimension 1 over $\mathbb{T}/\mathfrak{m} \simeq \mathbb{F}_\ell$. Since $J[\mathfrak{m}]$ is an extension of ${\mu_\ell}^{\oplus r}$ by $\mathbb{Z}/\ell\mathbb{Z}$ for some $r \geq 1$, $J[\mathfrak{m}]^{I_q}$ is at least of dimension r, i.e., $J[\mathfrak{m}]$ is of dimension 2.

□

Remark 4.3. Because we assume that $p_j \not\equiv 1 \pmod{\ell}$ for a prime $s < j \leq t$, unramifiedness of $J[\mathfrak{m}]$ at p in the third case of the proof of (1) follows from the assumption $s = 1$ only.

By using a similar argument as above we can prove a bound of the dimension of $J[\mathfrak{m}]$.

Theorem 4.4. *We have*

$$\max\{1 + \varpi_0(\mathfrak{m}), 2\} \leq \dim J[\mathfrak{m}] \leq 1 + \varpi_0(\mathfrak{m}) + \varpi_\ell(S_\mathfrak{m}).$$

Proof. If $s(\mathfrak{m}) < s_0(\mathfrak{m})$, $\Sigma_N[\mathfrak{m}] = 0$ by Proposition 2.14. Thus, $\mu_\ell \nsubseteq J[\mathfrak{m}]$ but $\mathbb{Z}/\ell\mathbb{Z} \subseteq J[\mathfrak{m}]$. Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & J[\mathfrak{m}] & \longrightarrow & {\mu_\ell}^{\oplus r} & \longrightarrow & 0 \\ & & \| & & \uparrow{\scriptstyle i_k} & & \uparrow{\scriptstyle i_k} & & \\ 0 & \longrightarrow & \mathbb{Z}/\ell\mathbb{Z} & \longrightarrow & W_k & \longrightarrow & \mu_\ell & \longrightarrow & 0, \end{array}$$

where W_k is the pullback of $J[\mathfrak{m}]$ by the map $i_k : \mu_\ell \to {\mu_\ell}^{\oplus r}$, which is an embedding into the k-th component for $1 \leq k \leq r$. Then W_k is an extension in $E = \mathrm{Ext}_{S_\mathfrak{m}}(\mu_\ell, \mathbb{Z}/\ell\mathbb{Z})$. If $r > \varpi_\ell(S_\mathfrak{m}) = \dim E$, the extensions W_k for all $1 \leq k \leq r$ are linearly dependent over $\mathbb{F}_\ell$. Thus, $J[\mathfrak{m}]$ contains μ_ℓ, which is a contradiction. Therefore $\dim J[\mathfrak{m}] = 1 + r \leq 1 + \varpi_\ell(S_\mathfrak{m})$.

If $s(\mathfrak{m}) = s_0(\mathfrak{m}) = s$, then $\varpi_0(\mathfrak{m}) = s$ and

$$\Sigma_N[\mathfrak{m}] \simeq \bigoplus_{i=1}^{s} \Sigma_{p_i}[\mathfrak{m}] \simeq {\mu_\ell}^{\oplus s}$$

by Proposition 2.14. Thus, $\dim J[\mathfrak{m}] \geq 1 + \varpi_0(\mathfrak{m})$. Let $J[\mathfrak{m}] = {\mu_\ell}^{\oplus s} \oplus K$. Then $\mu_\ell \nsubseteq K$, $\mathbb{Z}/\ell\mathbb{Z} \subseteq K$, and K is an extension of ${\mu_\ell}^{\oplus r}$ by $\mathbb{Z}/\ell\mathbb{Z}$. By the same argument as above, if $\dim K > 1 + \varpi_\ell(S_\mathfrak{m})$ then K contains μ_ℓ, which is a contradiction. Therefore $\dim J[\mathfrak{m}] = s + \dim K \leq s + 1 + \varpi_\ell(S_\mathfrak{m})$. □

4.2. **More on level pq.** Let $N = pq$, $p = p_1$ and $q = p_2$. (Hence $t = 2$.) Then $s = 1$ or $s = 2$. Let $S_N := \{p, q\}$, $\mathbb{T} := \mathbb{T}_{pq}$ and $J := J_0(pq)$.

4.2.1. *Case $s = 1$.* Since $s = 1$, assume that $q \not\equiv 1 \pmod{\ell}$ and $\ell \mid (p-1)(q^2-1)$. Let $\mathfrak{m} := (\ell,\ U_p - 1,\ U_q - q,\ T_r - r - 1 \mid \text{ for all primes } r \nmid pq)$.

Theorem 4.5. *Then,*

(1) *In all cases below, $J[\mathfrak{m}]$ is unramified at p.*
(2) *If $p \not\equiv 1 \pmod{\ell}$,* $\dim J[\mathfrak{m}] = 2$.
(3) *If $p \equiv 1 \pmod{\ell}$ and $q \not\equiv -1 \pmod{\ell}$,* $\dim J[\mathfrak{m}] = 2$.
(4) *Assume that $p \equiv 1 \pmod{\ell}$ and $q \equiv -1 \pmod{\ell}$.*
   (a) *If $J[\mathfrak{m}]$ is unramified at q, then* $\dim J[\mathfrak{m}] = 2$.
   (b) *If $J[\mathfrak{m}]$ is ramified at q, then* $\dim J[\mathfrak{m}] = 3$.

Proof. (1) This follows from Remark 4.3.
(2) If $p \not\equiv 1 \pmod{\ell}$, since $\ell \mid (p-1)(q^2-1)$, $q \equiv -1 \pmod{\ell}$. This holds by Theorem 4.2(2) since $\ell \nmid \varphi(pq)$.
(3) Assume that $p \equiv 1 \pmod{\ell}$ and $q \not\equiv -1 \pmod{\ell}$. Therefore this is true by Theorem 4.2(1) since $\varpi_\ell(S_N) = 1$.
(4) Since $p \equiv 1 \pmod{\ell}$, $\Sigma_{pq}[\mathfrak{m}] = \Sigma_p[\mathfrak{m}] \simeq \mu_\ell$. Thus, $J[\mathfrak{m}]$ contains μ_ℓ but $\mu_\ell \oplus \mu_\ell \nsubseteq J[\mathfrak{m}]$.
   (a) Since $J[\mathfrak{m}]$ is unramified at both p and q, it is unramified everywhere, in other words, it is a direct sum of $\mathbb{Z}/\ell\mathbb{Z}$ and ${\mu_\ell}^{\oplus r}$. Hence $\dim J[\mathfrak{m}] = 2$.
   (b) In this case, $s(\mathfrak{m}) = 1 = s_0(\mathfrak{m}) = \varpi_0(\mathfrak{m})$ and $\varpi_\ell(S_\mathfrak{m}) \leq 1$ since $J[\mathfrak{m}]$ is unramified at p. By Theorem 4.4, $\dim J[\mathfrak{m}] \leq 3$. We know that $J[\mathfrak{m}]$ contains $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ from the cuspidal group and the Shimura subgroup, respectively. Hence, $\dim J[\mathfrak{m}]^{I_q} \geq 2$. Since $J[\mathfrak{m}]$ is ramified at q, $\dim J[\mathfrak{m}] = 3$.

□

Remark 4.6. Let $q \equiv -1 \pmod{\ell}$. Note that $J[\mathfrak{m}]$ does not depend on p if $p \not\equiv 1 \pmod{\ell}$. It is a (unique) non-trivial extension of μ_ℓ by $\mathbb{Z}/\ell\mathbb{Z}$, which is annihilated by ℓ and is ramified only at q (and ℓ).

Example 4.7. In the case (4), we can compute the dimension of $J[\mathfrak{m}]$ using SAGE [SAGE]. Up to 100, $\dim J[\mathfrak{m}] = 3$ only when $(p,q) = (41,19),\ (61,79)$ for $\ell = 5$ and $(p,q) = (29,97),\ (43,13),\ (43,41)$ for $\ell = 7$. Thus, we know that $J[\mathfrak{m}]$ is ramified at q in each of those cases.

Remark 4.8. The structure of $J_0(43 \times 13)[\mathfrak{m}]$ for an Eisenstein $\mathfrak{m}$ of residue characteristic 7 is studied by Calegari and Stein [CS08]. We proved their result about its ramification (at 13) from the dimension computation. By Theorem 4.5(1), we know that it is unramified at 43.

4.2.2. *Case* $s = 2$. Let $\mathfrak{m} := (\ell,\ U_p - 1,\ U_q - 1,\ T_r - r - 1\ :\ \text{for all primes } r \nmid pq)$. Since $\mathfrak{m}$ is maximal if and only if $\ell \mid (p-1)(q-1)$, assume that $p \equiv 1 \pmod{\ell}$.

Theorem 4.9. *Then,*

(1) *If* $q \not\equiv \pm 1 \pmod{\ell}$, $\dim J[\mathfrak{m}] = 2$ *and* $J[\mathfrak{m}]$ *is ramified at* p.
(2) *Assume that* $q \equiv -1 \pmod{\ell}$. *Then* $J[\mathfrak{m}]$ *is ramified at* p.
   (a) *If* $J[\mathfrak{m}]$ *is unramified at* q, *then* $\dim J[\mathfrak{m}] = 2$.
   (b) *If* $J[\mathfrak{m}]$ *is ramified at* q, *then* $\dim J[\mathfrak{m}] = 3$.
(3) *If* $q \equiv 1 \pmod{\ell}$, *then* $\dim J[\mathfrak{m}]$ *is either* 4 *or* 5.

Proof. Since $p \equiv 1 \pmod{\ell}$, there is the Eisenstein maximal ideal $\mathfrak{m}_p$ of level p of residue characteristic ℓ and $J_0(p)[\mathfrak{m}_p] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$ by Mazur (Corollary 16.3 of Chapter II in [M77]).

(1) If $q \not\equiv \pm 1 \pmod{\ell}$, by Theorem 4.2(1), $\dim J[\mathfrak{m}] = 2$.
(2) Assume that $q \equiv -1 \pmod{\ell}$. Then $\Sigma_{pq}[\mathfrak{m}] = 0$, in other words, $\mu_\ell \nsubseteq J[\mathfrak{m}]$.
   (a) Assume that $J[\mathfrak{m}]$ is unramified at q. In this case, $s(\mathfrak{m}) = 1 < s_0(\mathfrak{m}) = 2$ and $\varpi_\ell(S_\mathfrak{m}) \leq 1$. Therefore $\dim J[\mathfrak{m}] = 2$ by Theorem 4.4 and $J[\mathfrak{m}]$ is ramified at p (and ℓ).
   (b) Assume that $J[\mathfrak{m}]$ is ramified at q. Let T, J^0 be the torus, the identity component of $J_{/\mathbb{F}_q}$, respectively. Then is an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \longrightarrow & J^0 & \xrightarrow{\pi} & J_0(p) \times J_0(p) & \longrightarrow & 0 \\ & & & & \uparrow{\scriptstyle \alpha_{/\mathbb{F}_q}} & \nearrow_{g} & & & \\ & & & & A := J_0(p) \times J_0(p) & & & & \end{array}$$

   and $g = \pi \circ \alpha_{/\mathbb{F}_q}$ is $\left(\begin{smallmatrix} 1 & \mathrm{Ver} \\ \mathrm{Ver} & 1 \end{smallmatrix}\right)$, where Ver is the Verschiebung morphism in characteristic q (Lemma 1.1 in [R90a]). Since $J_0(p)[\mathfrak{m}_p] \simeq \mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$ and $A[\mathfrak{m}] = \{(x,-x)\ :\ x \in J_0(p)[\mathfrak{m}_p]\}$, by g, $\{(x,-x)\ :\ x \in \mathbb{Z}/\ell\mathbb{Z}\}$ maps injectively to $J_0(p)^2[\mathfrak{m}]$. (And $\{(x,-x)\ :\ x \in \mu_\ell\}$ maps 0 by $\alpha_{/\mathbb{F}_q}$.) Thus, the image of π is at least 1-dimensional. Since $J[\mathfrak{m}]$ is ramified at q, $\mathfrak{m}$ is q-new, hence, $T[\mathfrak{m}] \neq 0$ since $\mathbb{T}^{q\text{-new}}$, the q-new quotient of $\mathbb{T}$, acts faithfully on T. Therefore $\dim J[\mathfrak{m}]^{I_q}$ is at least 2-dimensional. Since the dimension of $J[\mathfrak{m}]$ is at most 3 by Theorem 4.4, it is 3. Moreover if it is unramified at p, then $\varpi_\ell(S_\mathfrak{m}) \leq 1$ and $\varpi_0(\mathfrak{m}) = 0$. So, by Theorem 4.4, $\dim J[\mathfrak{m}] = 2$, which is a contradiction. Therefore $J[\mathfrak{m}]$ is also ramified at p.
(3) Assume that $q \equiv 1 \pmod{\ell}$. Then $\Sigma_{pq}[\mathfrak{m}] \simeq \Sigma_p[\mathfrak{m}] \oplus \Sigma_q[\mathfrak{m}] \simeq \mu_\ell \oplus \mu_\ell \subseteq J[\mathfrak{m}]$. By the result of Ribet [Y14], $\mathfrak{m}$ is new. Thus, $J_{\mathrm{new}}[\mathfrak{m}]$ is non-trivial, where J_{new} is the new subvariety of J. By the same argument about the Tate module of J, we can prove that $J_{\mathrm{new}}[\mathfrak{m}]$ is at least of dimension 2. Since $U_p + w_p$ acts by 2 on $\Sigma_q[\mathfrak{m}]$, it is an isomorphism because ℓ is odd. Moreover, since $U_p + w_p$ and $U_q + w_q$ annihilate J_{new}, $\Sigma_q[\mathfrak{m}] \cap J_{\mathrm{new}} = 0$. Similarly, we have $\Sigma_p[\mathfrak{m}] \cap J_{\mathrm{new}} = 0$. Thus, $\dim J[\mathfrak{m}] \geq 2 + 2 = 4$. By Theorem 4.4, the result follows.

□

Corollary 4.10. *If* $q \equiv -1 \pmod{\ell}$ *but* q *is not an* ℓ*-th power modulo* p, *then* $\dim J[\mathfrak{m}] = 2$.

Proof. By Ribet [Y14], if q is not an ℓ-th power module p, then $\mathfrak{m}$ is not new. Since $q \equiv -1 \pmod{\ell}$, there is no Eisenstein maximal ideal of level q, hence $\mathfrak{m}$ is q-old, in other words, $J[\mathfrak{m}]$ is unramified at q. Thus, this follows from the case (2)(a) of Theorem 4.9. □

Example 4.11. In the case (2)(resp. (3)) of Theorem 4.9, the computation with SAGE [SAGE] suggests that $\dim J[\mathfrak{m}] = 2$ (resp. $\dim J[\mathfrak{m}] = 5$).

Remark 4.12. The above examinations are now proved by Ribet and the author [RY14].

REFERENCES

[BLR91] Nigel Boston, Hendrik Lenstra, and Kenneth Ribet, *Quotients of group rings arising from two-dimensional representations*, C.R. Acad. Sci. Paris, t. **312**, Série I (1991), 323–328.

[BK14] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366**. (2014), 2463–2516.

[CL97] Seng-Kiat Chua and San Ling, *On the rational cuspidal subgroup and the rational torsion points of* $J_0(pq)$, Proc. Amer. Math. Soc. Vol. **125**. (1997), 2255–2263.

[CS08] Frank Calegari and William Stein, *A Non-Gorenstein Eisenstein Descent*, preprint available at `http://www.wstein.org/home/wstein/www/home/was/days/17/calegari-stein-tor.pdf`.

[DR73] Pierre Deligne and Micheal Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable II, Lecture notes in Math., Vol. **349** (1973), 143–316.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate text in Math., Vol **228**, 2005.

[FJ95] Gerd Faltings and Bruce Jordan, *Crystalline cohomology and* $\mathrm{GL}(2,\mathbb{Q})$, Israel Journal of Math., Vol **90**. (1995), 1–66.

[Ig59] Jun-Ichi Igusa, *Kroneckerian model of fields of elliptic modular functions*, American Journal of Math., Vol **81** (1959), 561–577.

[KM85] Nicholas Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Princeton Univ. Press, Princeton, Annals of Math. Studies **108**, 1985.

[LO90] San Ling and Joseph Oesterlé, *The Shimura subgroup of* $J_0(N)$, Astérisque, Vol. **196** (1990), 171–203.

[M77] Barry Mazur, *Modular curves and Eisenstein Ideals*, Publications Math. de l'I.H.É.S., tome **47** (1977), 33–186.

[Og74] Andrew Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France, Vol. **102** (1974), 449–462.

[Ra70] Michel Raynaud, *Spécialization du foncteur de Picard*, Publications Math. de l'I.H.É.S., tome **38** (1970), 27–76.

[R84] Kenneth Ribet, *Congruence relations between modular forms*, Proceeding of the International Congress of Math., Vol. **1**, **2** (Warsaw, 1983), 503–514.

[R88] Kenneth Ribet, *On the component groups and the Shimura subgroup of* $J_0(N)$, Séminaire de Théorie des Nombres (1988), Vol. **16**, 1–10.

[R89] Kenneth Ribet, *The old subvariety of* $J_0(pq)$, Arithmetic algebraic geometry (Texel, 1989), Vol. **89**, 293–307.

[R90] Kenneth Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[R90a] Kenneth Ribet, *Multiplicities of Galois reprensentations in Jacobians of Shimura curves*, Israel Math. conference proceeding, Vol **3** (1990), 221–236.

[R08] Kenneth Ribet, *Eisenstein primes for* $J_0(pq)$, unpublished.

[RY14] Kenneth Ribet and Hwajong Yoo, *Multiplicity one problems for modular Jacobian varieties at Eisenstein primes*, in preparation.

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math., Vol **88** (1968), 492–517.

[S73] Jean-Pierre Serre, *Congruences et formes modulaires*, Séminaire N. Bourbaki, 1971-1972, exp. n° **416**, 319–338.

[SAGE] William Stein at al., *SAGE mathematics software(Version 5.12.0)*.

[Sw73] H.P.F. Swinnerton-Dyer, *On* ℓ*-adic representations and congruences for coefficients of modular forms*, Modular functions of one variable III, Lecture notes in Math., Vol. **350** (1973), 1–55.

[Va05] Vinayak Vatsal, *Multiplicative subgroups of* $J_0(N)$ *and applications to elliptic curves*, Journal of the Inst. of Math. of Jussieu, Vol. **4** (2005), 281–316.

[Y14] Hwajong Yoo, *Non-optimal levels of a reducible mod* ℓ *modular representation*, submitted available at `http://math.uni.lu/~yoo/nonoptimal.pdf`.

UNIVERSITÉ DU LUXEMBOURG, FACULTÉ DES SCIENCES, DE LA TECHNOLOGIE ET DE LA COMMUNICATION, 6, RUE RICHARD COUDENHOVE-KALERGI, L-1359 LUXEMBOURG, LUXEMBOURG

E-mail address: `hwajong@gmail.com`