Generalized Ogg's conjecture (or Stein's conjecture)

Hwajong Yoo

Seoul National University in South Korea

December 3, 2020
ICTS

Rational torsion subgroup

For a positive integer N, let $X_0(N)$ be the modular curve over $\mathbf{Q}$ and $J_0(N)$ its Jacobian variety, which is an abelian variety defined over $\mathbf{Q}$ of dimension g, which is the genus of $X_0(N)$.

By the Mordell–Weil theorem, the group of rational points on $J_0(N)$ is finitely generated and so we have

$$J_0(N)(\mathbf{Q}) \simeq \mathbf{Z}^r \oplus J_0(N)(\mathbf{Q})_{\text{tor}},$$

where $J_0(N)(\mathbf{Q})_{\text{tor}}$ is the rational torsion subgroup of $J_0(N)$, which is a finite abelian group consisting of rational torsion points on $J_0(N)$.

Motivational question

Can we compute the rational torsion subgroup $J_0(N)(\mathbf{Q})_{\text{tor}}$?

Cuspidal group

A cuspidal divisor of $X_0(N)$ is a divisor of $X_0(N)$ supported only on cusps. Let $\mathcal{C}_N$ be the cuspidal group of $J_0(N)$, which is generated by the images of degree 0 cuspidal divisors of $X_0(N)$.

By the theorem of Manin and Drinfeld, the image of a degree 0 cuspidal divisor in $J_0(N)$ is torsion and hence we easily have

$$\mathcal{C}_N(\mathbf{Q}) \subset J_0(N)(\mathbf{Q})_{\text{tor}},$$

where $\mathcal{C}_N(\mathbf{Q})$ is the rational cuspidal group of $J_0(N)$.

We may naturally ask two questions in order to study $J_0(N)(\mathbf{Q})_{\text{tor}}$.

1. Can we prove $\mathcal{C}_N(\mathbf{Q}) = J_0(N)(\mathbf{Q})_{\text{tor}}$?
2. Can we compute the structure of $\mathcal{C}_N(\mathbf{Q})$?

Ogg's conjecture

Let N be a prime. In early 1970s, Andrew Ogg answered the second question. More precisely, there are exactly two cusps on $X_0(N)$, usually denoted by 0 and ∞. He computed the order of the image of the divisor $0 - \infty$, which is the numerator of $\frac{N-1}{12}$, usually denoted by num $\left(\frac{N-1}{12}\right)$. Also, he conjectured the following.

Theorem (Ogg's conjecture)

For a prime N, we have

$$J_0(N)(\mathbf{Q})_{\text{tor}} = \mathcal{C}_N = \left\langle \overline{0 - \infty} \right\rangle .$$

In 1977, Barry Mazur proved this in his celebrated paper, "Modular curves and the Eisenstein ideal", so we know the answer of the first question as well, at least when N is prime.

The title of this talk is the following.

Conjecture (Folklore: Generalized Ogg's conjecture)

For any positive integer N, we have

$$J_0(N)(\mathbf{Q})_{\text{tor}} = \mathcal{C}_N(\mathbf{Q}).$$

Based on this conjecture, which is the affirmative answer of the first question, we want to know the structure of the rational cuspidal group $\mathcal{C}_N(\mathbf{Q})$. However, there is no known method to compute the group $\mathcal{C}_N(\mathbf{Q})$ for arbitrary integer N (except the one using modular symbols).

Digression: Torsion points on cyclotomic fields

In general, Ribet proved that for an abelian variety A over a number field K,

$$A(K(\mu_\infty))_{\text{tor}}$$

is a finite abelian group. What is this group if $A = J_0(N)$? One has

$$\mathcal{C}_N \subset J_0(N)(\mathbf{Q}(\mu_N))_{\text{tor}}.$$

(In fact, $\mathcal{C}_N$ is defined over a smaller field.) Is this inclusion in fact an equality? If so, generalized Ogg's conjecture would follow, but we have to consider some contribution from the Shimura subgroup.

Yuan Ren has been investigating the problems in this direction.

Rational cuspidal divisor class group

Let $\mathcal{A}_N$ be the group of degree 0 cuspidal divisors on $X_0(N)$. Then, we have an exact sequence:

$$0 \longrightarrow \mathcal{U}_N \xrightarrow{\text{div}} \mathcal{A}_N \longrightarrow \mathcal{C}_N \longrightarrow 0,$$

where $\mathcal{U}_N$ is the group of modular units on $X_0(N)$ modulo $\mathbf{C}^\times$.

Ken asked me whether one could prove a priori that the map $F : \mathcal{A}_N(\mathbf{Q}) \to \mathcal{C}_N(\mathbf{Q})$ is surjective, for example by computing a cohomology group and showing it is zero. Let $\mathcal{C}(N)$ be the image of F, which is called the rational cuspidal divisor class group of $X_0(N)$.

One may ask the following.

$$\mathcal{C}(N) \stackrel{?}{=} \mathcal{C}_N(\mathbf{Q}).$$

Second question

In general, the structure of the rational cuspidal group $\mathcal{C}_N(\mathbf{Q})$ is not known. On the other hand, we know the structure of the rational cuspidal divisor class group $\mathcal{C}(N)$ for any positive integer N (Y., 2019).

If $N = 2^r \cdot M$ with $0 \le r \le 3$ and M odd squarefree, then all cusps of $X_0(N)$ are defined over $\mathbf{Q}$ and hence $\mathcal{C}(N) = \mathcal{C}_N(\mathbf{Q}) = \mathcal{C}_N$ and hence we know the structure of the group $\mathcal{C}_N$ as well.

Thus, the second question may be reduced to showing

$$\mathcal{C}(N) \stackrel{?}{=} \mathcal{C}_N(\mathbf{Q}).$$

Variant of GOC

Conjecture O

For any positive integer N and a prime ℓ, we have

$$\mathcal{C}(N)[\ell^\infty] = J_0(N)(\mathbf{Q})_{\mathsf{tor}}[\ell^\infty],$$

where $A[\ell^\infty]$ denotes the ℓ-primary subgroup of a finite group A.

Mazur's theorem says that Conjecture O holds for any primes N and ℓ.

Known results for composite N

- Lorenzini (1995) : $N = p^r$ for a prime $p \not\equiv 11 \pmod{12}$ and $\ell \nmid 2p$.
- Ling (1997) : $N = p^r$ for a prime p and $\ell \nmid 6p$. (If $r = 2$, $\ell = 3$ allowed.)
- Ohta (2014): N is squarefree and $\ell \nmid 2 \cdot \text{gcd}(3, N)$.
- Y. (2016): $N = 3p$ for a prime p such that either $p \not\equiv 1 \pmod 9$ or $3^{\frac{p-1}{3}} \not\equiv 1 \pmod p$, and $\ell = 3$.
- Ren (2018) : N is any positive integer and $\ell \nmid 6N \prod_{p \mid N}(p^2 - 1)$.
  (Ren proved that $J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty] = 0$.)

Note that if N is small enough, we may explicitly compute the group $J_0(N)(\mathbf{Q})_{\text{tor}}$ and prove Conjecture O for any prime ℓ. If $X_0(N)$ is an elliptic curve then all are known. Also, we know the following cases: $N = 125$ (Poulakis, 1987) and $N = 57, 65$ (Box, 2019).

Main Result

Theorem (Y., 2019)

Let N be any positive integer not divisible by an odd prime ℓ. Then, Conjecture O holds for level N, namely, we have

$$\mathcal{C}(N)[\ell^\infty] = J_0(N)(\mathbf{Q})_{\mathsf{tor}}[\ell^\infty].$$

If $\ell \geq 5$, then Conjecture O holds for level $N\ell$, i.e.,

$$\mathcal{C}(N\ell)[\ell^\infty] = J_0(N\ell)(\mathbf{Q})_{\mathsf{tor}}[\ell^\infty].$$

- Note that our result is a natural generalization of the work of Ohta.
- Note also that if N is a prime power, our proof is different from that of Lorenzini (and Ling) and when $\ell = 3$, we remove the hypothesis of Lorenzini's work.

Eisenstein ideal

Let N be a positive integer, and let T_p be the pth Hecke operator acting on $J_0(N)$. Also, for a prime divisor p of N, let w_p be the Atkin–Lehner involution with respect to p.
One may construct two Hecke algebras as subrings of $\mathrm{End}(J_0(N))$:

$$\mathbb{T} := \mathbf{Z}[T_p : \text{ for all primes } p] \text{ and}$$
$$\mathbf{T} := \mathbf{Z}[w_q, T_p : q \in \mathcal{S}_1 \text{ and for all primes } p \notin \mathcal{S}_1],$$

where $\mathcal{S}_1 := \{q \text{ primes } : q \mid N \text{ but } q^2 \nmid N\}$.

We consider the (minimal) Eisenstein ideal in both rings generated by

$$T_p - p - 1 \text{ for all primes } p \text{ not dividing } N,$$

denoted by $\mathcal{I}$.

- Let ℓ be an odd prime, and N be a positive integer not divisible by ℓ.
- The group $J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty]$ is a module over $\mathbf{T}_\ell := \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$.

Theorem (Eichler–Shimura)

For a prime p not dividing N, we have

$$T_p = \text{Frob}_p + \text{Ver}_p \in \text{End}(J_0(N)_{\mathbf{F}_p}).$$

For a prime $p \nmid N$, we have $J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty] \hookrightarrow J_0(N)_{\mathbf{F}_p}(\mathbf{F}_p)$ (Katz). Since Frob_p acts trivially on the rational points, $T_p - 1 - p$ annihilates $J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty]$ and hence

- $J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty]$ is a module over $\mathbf{T}_\ell/\mathcal{I}$.
- Also, $\mathcal{C}(N)[\ell^\infty]$ is a module over $\mathbf{T}_\ell/\mathcal{I}$.

Mazur's strategy

- Step 1: Compute the order of $\mathcal{C}(N)[\ell^\infty]$, say x.
- Step 2: Compute the index of $\mathcal{I}$ in $\mathbf{T}_\ell$, say y.
- Step 3: Compute the dimension of $J_0(N)[\mathfrak{m}]^{\text{ét}}$ for any maximal ideal $\mathfrak{m}$ of $\mathbf{T}$ containing $\mathcal{I}$, say $d(\mathfrak{m})$. Such maximal ideals are called rational Eisenstein primes. (Here, $J_0(N)[\mathfrak{m}]^{\text{ét}}$ is the étale part of the kernel $J_0(N)[\mathfrak{m}]$ as a group scheme over $\mathbf{Z}$.)

Step 1 is known for any N and ℓ without any assumptions (Y., 2019), and we omit this step. This is the easiest part in general.
Since $\mathcal{C}(N)[\ell^\infty]$ is annihilated by $\mathcal{I}$, y is a multiple of x. If y/x is an ℓ-adic unit and $d(\mathfrak{m}) = 1$ for any rational Eisenstein primes containing ℓ, then we can prove

$$J_0(N)(\mathbf{Q})_{\text{tor}}[\ell^\infty] = \mathcal{C}(N)[\ell^\infty].$$

Digression: Classification of rational Eisenstein primes

Proposition

Suppose that $\mathfrak{m} \subset \mathbf{T}_\ell$ *is a maximal ideal containing* $\mathcal{I}$. *Then,*

$$\mathfrak{m} = (\ell, w_p \pm 1, T_q - \alpha_q, \mathcal{I} : p \in \mathcal{S}_1 \ \text{ and } \ q \in \mathcal{S}_2),$$

where $\alpha_q \in \{0, 1, q\}$ *and* $\mathcal{S}_2$ *is the set of prime divisors of* N *not in* $\mathcal{S}_1$.

Proof.

Since $w_p^2 - 1 = (w_p - 1)(w_p + 1) = 0$, either $w_p + 1 \in \mathfrak{m}$ or $w_p - 1 \in \mathfrak{m}$. Suppose that $q^2 \mid N$. If $\mathfrak{m}$ is q-new, then $T_q \in \mathfrak{m}$. If $T_q \notin \mathfrak{m}$ then $\mathfrak{m}$ is not q-new and we may "lower the level", and $\mathfrak{m}$ "comes from level $N'q$, where N' is the prime-to-q part of N. As in Ken's talk, we have $(T_q - q)(T_q - 1) = 0$ and the result follows. $\square$

Step 3

Before studying Step 2, we deal with Step 3.

Theorem (Mazur, Ohta, Y.)

Let $\mathfrak{m}$ be a rational Eisenstein prime. Then, we have

$$\dim_{\mathbf{F}_\ell} J_0(N)[\mathfrak{m}]^{\text{ét}} = 1.$$

The argument of Mazur in the prime level case works verbatim under our assumption that $\ell \nmid 2N$. Roughly speaking, using the theory of Cartier operator in characteristic ℓ, we can embed the etale part into $H^0(X_0(N)_{\overline{\mathbf{F}}_\ell}, \Omega)[\mathfrak{m}]$, which is one dimensional by the q-expansion principle.

In the case of level $N\ell$, one can directly compute $\mathcal{J}[\mathfrak{m}]$, where $\mathcal{J}$ is the special fiber of the Néron model of $J_0(N\ell)$ over $\mathbf{F}_\ell$. If $\ell \geq 5$, the dimension of $\mathcal{J}[\mathfrak{m}]$ is 1 and the above multiplicity one result follows.

Step 2

From now on, for simplicity, let $\mathcal{B}(N) := J_0(N)(\mathbf{Q})_{\text{tor}}$.

First, since the ring $\mathbf{T}_\ell$ is semi-local, we have

$$\mathbf{T}_\ell/\mathcal{I} \simeq \prod_{\mathfrak{m}\colon \text{maximal},\ \mathcal{I}\subset\mathfrak{m}} \mathbf{T}_\mathfrak{m}/\mathcal{I},$$

where

$$\mathbf{T}_\mathfrak{m} := \varprojlim_n \mathbf{T}_\ell/\mathfrak{m}^n$$

is a complete local ring with the maximal ideal $\mathfrak{m}\mathbf{T}_\mathfrak{m}$.

Accordingly, we have

$$\mathcal{B}(N)[\ell^\infty] \simeq \bigoplus_{\mathfrak{m}:\text{ maximal},\ \mathcal{I}\subset\mathfrak{m}} \mathcal{B}(N)[\mathfrak{m}^\infty]$$

and

$$\mathcal{C}(N)[\ell^\infty] \simeq \bigoplus_{\mathfrak{m}:\text{ maximal},\ \mathcal{I}\subset\mathfrak{m}} \mathcal{C}(N)[\mathfrak{m}^\infty].$$

(Here, we consider $\mathcal{B}(N)[\mathfrak{m}^\infty]$ and $\mathcal{C}(N)[\mathfrak{m}^\infty]$ as $\mathbf{T}_\mathfrak{m}/\mathcal{I}$-modules.)

Thus, it suffices to show that $\mathcal{B}(N)[\mathfrak{m}^\infty] \subset \mathcal{C}(N)[\mathfrak{m}^\infty]$ for any rational Eisenstein primes $\mathfrak{m}$ containing ℓ. By Step 3 and Nakayama's lemma, $\mathcal{B}(N)[\mathfrak{m}^\infty]$ is at most of rank 1 over the ring $\mathbf{T}_\mathfrak{m}/\mathcal{I}$. Hence it suffices to show that $\mathcal{C}(N)[\mathfrak{m}^\infty]$ is free of rank 1 over $\mathbf{T}_\mathfrak{m}/\mathcal{I}$.

Prime level

To illustrate an idea, let assume that $N = p$ is a prime.

- Since $w_p^2 = 1$, either $w_p + 1 \in \mathfrak{m}$ or $w_p - 1 \in \mathfrak{m}$.
- Since there is no old form, we have $T_p + w_p = 0$.
- Mazur proved that there is only one Eisenstein prime containing ℓ:

$$\mathfrak{m} = (\ell, \mathcal{I}, w_p + 1 = T_p - 1).$$

- Since ℓ is odd and $w_p + 1 \in \mathfrak{m}$, we have $w_p - 1 \notin \mathfrak{m}$.
- Since $\mathbf{T}_\mathfrak{m}$ is a local ring, $w_p - 1$ is a unit in $\mathbf{T}_\mathfrak{m}$.
- Since $w_p^2 - 1 = (w_p - 1)(w_p + 1) = 0$, we have $w_p + 1 = 0$. Thus,

$$\mathbf{T}_\ell/\mathcal{I} = \mathbf{T}_\mathfrak{m}/\mathcal{I} = \mathbf{T}_\mathfrak{m}/I = \mathbf{T}_\ell/I,$$

where $I = (\mathcal{I}, w_p + 1)$.

Since any generators T_q and w_p are congruent to integers modulo I, there is a surjection

$$\mathbf{Z}_\ell \twoheadrightarrow \mathbf{T}_\ell/I.$$

If it is injective, then there is a cusp form of weight 2 for $\Gamma_0(p)$ with coefficient in $\mathbf{Z}_\ell$ whose qth coefficient is $1+q$. This violates Ramanujan's bound and hence there is an integer n such that

$$\mathbf{T}_\ell/I \simeq \mathbf{Z}_\ell/n\mathbf{Z}_\ell.$$

One can construct a cuspidal divisor $C = 0 - \infty$ annihilated by I, and compute the order of its image $\overline{C}$ in $J_0(N)$, say m. From the natural projection

$$\mathbf{T}_\ell/I \twoheadrightarrow \mathrm{End}(\langle \overline{C} \rangle) \simeq \mathbf{Z}_\ell/m\mathbf{Z}_\ell,$$

n is a multiple of m.

On the other hand, there is an Eisenstein series E annihilated by I. By the duality of the Hecke ring and the space of cusp forms, there is a cusp form f whose coefficients lie in $\mathbf{T}_\ell/I = \mathbf{Z}_\ell/n\mathbf{Z}_\ell$. After reduction modulo n, E may be regarded as a modular form over the ring $\mathbf{Z}_\ell/n\mathbf{Z}_\ell$. Since the q-expansions of f and E only differ by the constant term and there is no modular form over the ring $\mathbf{Z}_\ell/n\mathbf{Z}_\ell$ whose q-expansion is just a constant, $f = E$ in the space of modular forms over the ring $\mathbf{Z}_\ell/n\mathbf{Z}_\ell$. Therefore the constant term of E must be divisible by n. By direct computation, the constant term is "almost equal" to m and hence n/m is an ℓ-adic unit.

This is basically the proof by Mazur (under the assumption that $\ell \geq 5$). Note that the duality used above is well-known if we use $\mathbb{T}$, but we consider the other Hecke ring $\mathbf{T}$ for some reason. Since $\mathbb{T} = \mathbf{T}$ in the prime level from the relation $T_p = -w_p$, one can finish the proof.

Squarefree level (a variant of the work of Ohta)

Let $N = \prod_{i=1}^{t} p_i$ be a squarefree integer, and set $\mathbf{E} := \{\pm 1\}^t$. Let

$$\varepsilon = (\epsilon_1, \epsilon_2, \dots, \epsilon_t) \in \mathbf{E}.$$

As above, one may consider the Eisenstein ideal

$$I(\varepsilon) = (w_{p_i} - \epsilon_i, \mathcal{I} : 1 \le i \le t) \subset \mathbf{T}_\ell$$

and let $\mathfrak{m} = (\ell, I(\varepsilon))$ be a maximal ideal.

As above, since $\mathbf{T}_\mathfrak{m}$ is local, $w_{p_i} - \epsilon_i \in \mathfrak{m}$, ℓ is odd, and $w_{p_i}^2 - 1 = 0$, we know that $w_{p_i} - \epsilon_i = 0 \in \mathbf{T}_\mathfrak{m}$. Thus, we have

$$\mathbf{T}_\mathfrak{m}/\mathcal{I} = \mathbf{T}_\mathfrak{m}/I(\varepsilon) \simeq \mathbf{T}_\ell/I(\varepsilon).$$

As above, since any generators are congruent to integers modulo $I(\varepsilon)$ there is an integer $n \geq 1$ such that

$$\mathbf{T}_\ell/I(\varepsilon) \simeq \mathbf{Z}_\ell/n\mathbf{Z}_\ell.$$

Now, it is easy to construct a cuspidal divisor $C(\varepsilon)$ and an Eisenstein series $E(\varepsilon)$ annihilated by $I(\varepsilon)$. One can show that the order of $\overline{C(\varepsilon)}$ is equal to the constant term of $E(\varepsilon)$, and the result follows if we prove the duality between $\mathbf{T}_\ell$ and the space of cusp forms, which is done by Masami Ohta. Thus, we obtain that $\mathcal{C}(N)[\mathfrak{m}^\infty]$, which is generated by $\overline{C(\varepsilon)}$, is free of rank 1 over

$$\mathbf{Z}_\ell/n\mathbf{Z}_\ell \simeq \mathbf{T}_\ell/I(\varepsilon) \simeq \mathbf{T}_\mathfrak{m}/\mathcal{I}.$$

In the case of level $N\ell$, Ohta proved the duality between the Hecke ring (with w_{p_i}) and the space of regular differentials. The result similar to above holds in this case even when $\ell = 3$ without further assumptions.

Non-squarefree level

Now, let N be any positive integer. As above, write

$$N = \prod_{i=1}^{t} p_i \prod_{j=1}^{u} q_j^{r_j}$$

with $r_j \geq 2$. Here, p_i and q_j denote distinct primes different from an odd prime ℓ. In the previous notation,

$$\mathcal{S}_1 = \{p_i : 1 \leq i \leq t\} \quad \text{and} \quad \mathcal{S}_2 = \{q_j : 1 \leq j \leq u\}.$$

As above, let $\mathbf{E} := \{\pm 1\}^t$ and for $\boldsymbol{\varepsilon} = (\epsilon_1, \dots, \epsilon_t) \in \mathbf{E}$, let

$$I(\boldsymbol{\varepsilon}) := (w_{p_i} - \epsilon_1, \mathcal{I} : 1 \leq i \leq t) \subset \mathbf{T}_\ell.$$

The difference from the previous cases is that there are some missing operators T_{q_j} in $I(\boldsymbol{\varepsilon})$, so we no longer have

$$\mathbf{T}_\ell / I(\boldsymbol{\varepsilon}) \simeq \mathbf{Z}_\ell / n\mathbf{Z}_\ell.$$

Nevertheless, if we let

$$I^0(\varepsilon) := (I(\varepsilon), T_{q_j} : 1 \leq j \leq u) \subset \mathbf{T}_\ell,$$

then we can show that there is an integer n such that

$$\mathbf{T}_\ell / I^0(\varepsilon) \simeq \mathbf{Z}_\ell / n\mathbf{Z}_\ell.$$

Also, as above if we let $\mathfrak{m} = (\ell, I^0(\varepsilon))$ then we can prove that $\mathcal{C}(N)[\mathfrak{m}^\infty]$ is free of rank 1 over $\mathbf{T}_\ell / I^0(\varepsilon)$ and hence

$$\mathcal{B}(N)[\mathfrak{m}^\infty] = \mathcal{C}(N)[\mathfrak{m}^\infty].$$

Thus, as above we have

$$\mathcal{B}(N)[\ell^\infty, I^0] \simeq \bigoplus_{\mathfrak{m}} \mathcal{B}(N)[\mathfrak{m}^\infty] = \bigoplus_{\mathfrak{m}} \mathcal{C}(N)[\mathfrak{m}^\infty] \simeq \mathcal{C}(N)[\ell^\infty, I^0],$$

where $I^0 = (T_{q_j}, \mathcal{I} : 1 \leq j \leq u) \subset \mathbf{T}_\ell$ and $\mathfrak{m}$ runs over rational Eisenstein primes of the form $(\ell, I^0(\varepsilon))$.

Main difficulty

So, the main difficulty in the case of non-squarefree level is proving

$$\mathcal{B}(N)[\ell^\infty, I^0] = \mathcal{C}(N)[\ell^\infty, I^0] \Longrightarrow \mathcal{B}(N)[\ell^\infty] = \mathcal{C}(N)[\ell^\infty].$$

What is the idea? My first attempt to show this is using the decomposition of the Hecke ring. Then, one may prove the result when N is divisible by at most the square of the primes (i.e., $r_j = 2$ for all j) and ℓ does not divide $q_j - 1$. This assumption comes from the need to distinguish T_{q_j}-eigenvalues in $\mathbf{F}_\ell$, which is $\{0, 1, q_j\}$.
On the other hand, this method is no longer applicable if $r_j > 2$ because the number of possible rational Eisenstein primes is smaller than the rank of $\mathcal{C}(N)[\ell^\infty]$, so we cannot get the result such as "$\mathcal{C}(N)[\mathfrak{m}^\infty]$ is free of rank 1 over $\mathbf{T}_\mathfrak{m}/\mathcal{I}$".

Inductive method

Here is my (new) contribution:

Theorem (Y., 2019)

For any primes $q \in \mathcal{S}_2$, assume that Conjecture O holds for level N/q, i.e.,

$$\mathcal{B}(N/q)[\ell^\infty] = \mathcal{C}(N/q)[\ell^\infty].$$

Then, we have

$$\mathcal{B}(N)[\ell^\infty] = \mathcal{C}(N)[\ell^\infty].$$

Also, the same is true if we replace N by $N\ell$.

This proves our main theorem by induction and the result of Ohta.

Proof of the theorem

Let $q \in \mathcal{S}_2$. Namely, q is a prime such that q^2 divides N.
First, we insist the following.

Claim

If $\mathcal{B}(N/q)[\ell^\infty] = \mathcal{C}(N/q)[\ell^\infty]$ then

$$T_q(\mathcal{B}(N)[\ell^\infty]) = T_q(\mathcal{C}(N)[\ell^\infty]).$$

Since there is an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{C}(N)[\ell^\infty][T_q] \arrow[r] \arrow[d, hook] & \mathcal{C}(N)[\ell^\infty] \arrow[r] \arrow[d, hook] & T_q(\mathcal{C}(N)[\ell^\infty]) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & \mathcal{B}(N)[\ell^\infty][T_q] \arrow[r] & \mathcal{B}(N)[\ell^\infty] \arrow[r] & T_q(\mathcal{B}(N)[\ell^\infty]) \arrow[r] & 0,
\end{tikzcd}$$

by five lemma we have

$$\mathcal{B}(N)[\ell^\infty, T_q] = \mathcal{C}(N)[\ell^\infty, T_q] \iff \mathcal{B}(N)[\ell^\infty] = \mathcal{C}(N)[\ell^\infty].$$

Since T_q commutes with other Hecke operators, applying the same argument for all primes $q_j \in \mathcal{S}_2$ as above we get

$$\mathcal{B}(N)[\ell^\infty, I^0] = \mathcal{C}(N)[\ell^\infty, I^0] \iff \mathcal{B}(N)[\ell^\infty] = \mathcal{C}(N)[\ell^\infty].$$

Thus, it suffices to prove the claim. Let

$$\begin{tikzcd} J_0(N) \arrow[r, shift left, "{\alpha_q(N)^*, \beta_q(N)^*}"] & J_0(Nq) \arrow[l, shift left, "{\alpha_q(N)_*, \beta_q(N)_*}"] \end{tikzcd}$$

be the maps induced by pullback and push-forward of the two degeneracy maps

$$\alpha_q(N), \beta_q(N) : X_0(Nq) \to X_0(N).$$

Then, by definition

$$T_q = \beta_q(N)_* \circ \alpha_q(N)^* : J_0(N) \to J_0(N).$$

Since q^2 divides the level N, by direct computation

$$T_q = \beta_q(N)_* \circ \alpha_q(N)^* = \alpha_q(N/q)^* \circ \beta_q(N/q)_*.$$

In other words, we get

$$\begin{tikzcd}
& J_0(Nq) \arrow[dr, "\beta_q(N)_*"] & \\
J_0(N) \arrow[ur, "\alpha_q(N)^*"] \arrow[dr, "\beta_q(N/q)_*"'] \arrow[rr, bend left, "\beta_q(N)_* \circ \alpha_q(N)^*"] \arrow[rr, bend right, "\alpha_q(N/q)^* \circ \beta_q(N/q)_*"'] \arrow[rr, phantom, "||"] & & J_0(N). \\
& J_0(N/q) \arrow[ur, "\alpha_q(N/q)^*"'] &
\end{tikzcd}$$

Also, by direct computation we have

$$\beta_q(N/q)_*(\mathcal{C}(N)[\ell^\infty]) = \mathcal{C}(N/q)[\ell^\infty].$$

(This holds if we replace N by $N\ell$ or $N\ell^2$. However, this may not be true for $N\ell^r$ with $r \geq 3$.) Since $\beta_q(N/q)_*$ is rational, we have

$$\beta_q(N/q)_*(\mathcal{B}(N)[\ell^\infty]) \subset \mathcal{B}(N/q)[\ell^\infty].$$

Thus, we have

$$\begin{aligned} T_q(\mathcal{B}(N)[\ell^\infty]) &\subset \alpha_q(N/q)^*(\mathcal{B}(N/q)[\ell^\infty]) = \alpha_q(N/q)^*(\mathcal{C}(N/q)[\ell^\infty]) \\ &= \alpha_q(N/q)^* \circ \beta_q(N/q)_*(\mathcal{C}(N)[\ell^\infty]) = T_q(\mathcal{C}(N)[\ell^\infty]). \end{aligned}$$

This completes the proof. $\square$

Thank you very much
for your attention!