The Rational Torsion Subgroup of $J_0(N)$

Hwajong Yoo

Seoul National University

September 22, 2023
Zagreb, Croatia

Introduction

Let E be an elliptic curve over $\mathbf{Q}$. By the Mordell theorem we have

$$E(\mathbf{Q}) \simeq \mathbf{Z}^{\oplus r} \oplus E(\mathbf{Q})_{\mathrm{tors}}$$

for a nonnegative integer r and a finite abelian group $E(\mathbf{Q})_{\mathrm{tors}}$.

Ogg conjectured (1975) and Mazur proved (1977) the following.

$$E(\mathbf{Q})_{\mathrm{tors}} \simeq \begin{cases} \mathbf{Z}/n\mathbf{Z} & \text{for } 1 \leq n \leq 10 \text{ and } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z} & \text{for } 1 \leq m \leq 4. \end{cases}$$

More generally, for any elliptic curves over a number field K there are finitely many possible K-rational torsion subgroups. Even further, there is a uniform bound for the sizes of this K-rational torsion subgroups depending only on $[K : \mathbf{Q}]$ by Merel (1996).

Let A be an abelian variety over $\mathbf{Q}$. By the Weil theorem we have

$$A(\mathbf{Q}) \simeq \mathbf{Z}^{\oplus r} \oplus A(\mathbf{Q})_{\mathrm{tors}}$$

for a nonnegative integer r and a finite abelian group $A(\mathbf{Q})_{\mathrm{tors}}$.

Q: Can we compute $A(\mathbf{Q})_{\mathrm{tors}}$? More generally, is there any (infinite) family of abelian varieties (except for elliptic curves) whose rational torsion subgroups are known?

One of the easiest ways to construct an abelian variety is the Jacobian variety of a curve. So we restrict to the case of Jacobian varieties of (certain) algebraic curves defined over $\mathbf{Q}$.

(another) Ogg's conjecture

Let N be a positive integer and let $J_0(N)$ be the Jacobian variety of the modular curve $X_0(N)$ over $\mathbf{Q}$. This is an abelan variety over $\mathbf{Q}$.

Q: Can we compute $J_0(N)(\mathbf{Q})_{\text{tors}}$?

Ogg conjectured (1975) and Mazur proved (1977) the following:

Theorem (Mazur, 1977)

For a prime N, we have

$$J_0(N)(\mathbf{Q})_{\text{tors}} = \langle [0-\infty] \rangle \simeq \mathbf{Z}/n\mathbf{Z}$$

where n is the numerator of $\frac{N-1}{12}$.

Generalized Ogg's conjecture

Now let N be a positive integer. A natural generalization of RHS is the cuspidal subgroup $\mathcal{C}_N$ of $J_0(N)$ which is a subgroup generated by the equivalence classes of the differences of two cusps of $X_0(N)$.
(In Lupoian's talk, this is $C_H(p)$.)

However the cuspidal subgroup may contain non-rational points.
Thus, we consider the rational cuspidal subgroup of $J_0(N)$:

$$\mathcal{C}_N(\mathbf{Q}) := \mathcal{C}_N \cap J_0(N)(\mathbf{Q}).$$

Conjecture A (generalized Ogg's conjecture)

For any positive integer N, we have

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

Another conjecture

Still we do not know how to compute the rational torsion subgroup of $J_0(N)$ because it is hard to determine the rational cuspidal subgroup. The latter has a large subgroup $\mathcal{C}(N)$, called the rational cuspidal divisor class group of $X_0(N)$. This is a subgroup generated by the equivalence classes of degree 0 rational cuspidal divisors on $X_0(N)$. (In Lupoian's talk, this is $C_H^{\mathbf{Q}}(p)$.)

Conjecture B

For any positive integer N, we have

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

Note that the structure of the latter group for any positive integer N is known. So our hope is to prove both conjectures.

Remark

Conjectures A and B are both known when N is small enough. (E.g. Ligozat, Poulakis, Box, Ozman–Siksek, Lupoian, and Adzaga–Keller–Michaud-Jacobs–Najman–Ozman–Vukorepa.)

We easily have $\mathcal{C}(N) \subset \mathcal{C}_N(\mathbf{Q}) \subset \mathcal{C}_N$. When $N = 2^r M$ with $0 \leq r \leq 3$ and M squarefree, then all cusps are rational. Hence we have

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

On the other hand, $\mathcal{C}_N(\mathbf{Q}) \subsetneq \mathcal{C}_N$ in general.

Conjecture B is known for the following cases:

- $N = n^2 M$ with $n \mid 24$ by Wang–Yang (2020).
- $N = p^2 M$ with a prime p by Guo–Yang–Yu–Y. (2021).
- $N = p^r q^s M$ with odd primes p and q by Yu–Y. (2022).

Here M denotes any squarefree integer, and r, s are any integers ≥ 2.

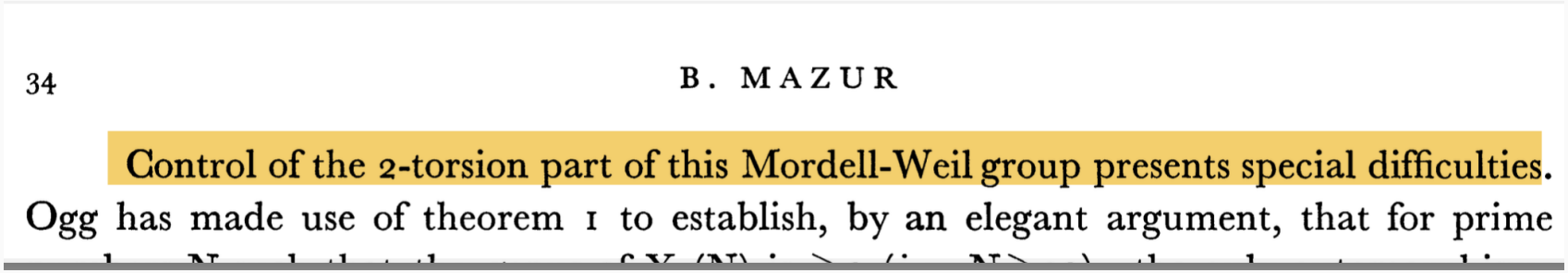
Conjecture A+B

Since all the groups we are interested in are finite abelian, it suffices to compare their ℓ-primary subgroups for any primes ℓ. So we propose:

Conjecture C

Let N be a positive integer. For any prime ℓ, we have

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



34 B. MAZUR

Control of the 2-torsion part of this Mordell-Weil group presents special difficulties. Ogg has made use of theorem 1 to establish, by an elegant argument, that for prime

Thus, from now on, ℓ always denotes a prime satisfying

$$\ell \geq 5$$

Results

Theorem (Ohta, 2014)

Let N be a squarefree integer. Then we have

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

When $\ell \nmid N$, Ribet and Wake proved this again by "pure-thought".

Theorem (Y., 2019/2023)

Let N be any positive integer. If ℓ^2 does not divide N, then we have

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

In the remaining of the talk, we prove this theorem.

One page sketch for the proof of Mazur

For simplicity, we often denote

$$\mathcal{A}(N) = \mathcal{C}(N)[\ell^\infty] \quad \text{and} \quad \mathcal{B}(N) = J_0(N)(\mathbf{Q})_{\text{tors}}[\ell^\infty].$$

It is easy to see that $\mathcal{A}(N) \subseteq \mathcal{B}(N)$. So it suffices to show that

$$\#\mathcal{B}(N) \leq \#\mathcal{A}(N).$$

We consider them as modules over the Hecke ring $\mathbf{T}$. For any ideal I contained in the annihilator of $\mathcal{B}(N)$, both can be regarded as $\mathbf{T}/I$-modules. If the structure of $\mathbf{T}/I$ is "simple", then so are their modules. When N is a prime, it turns out that $\mathbf{T}/I \simeq \mathbf{Z}/n\mathbf{Z}$ and $\mathcal{B}(N)$ is at most of rank 1. Moreover, $\mathcal{A}(N)$ is already free of rank 1 over $\mathbf{T}/I$ and hence the result follows.

(In prime level case, the assumption $\ell \geq 5$ is redundant.)

One page sketch for the proof of Ohta

Now let N be a squarefree integer. Then the structure of $\mathbf{T}/I$ for a certain ideal contained in the annihilator of $\mathcal{B}(N)$ is "relatively simple". It can be decomposed into cyclic pieces $\mathbf{T}/I^{\epsilon}$ (whenever $\ell \neq 2$). Since all $\mathbf{T}/I$-modules can be decomposed accordingly, we consider their eigenspaces:

$$\mathcal{A}(N)[I^{\epsilon}] \quad \text{and} \quad \mathcal{B}(N)[I^{\epsilon}].$$

In fact, we can prove that $\mathcal{A}(N)[I^{\epsilon}]$ is free of rank 1 over $\mathbf{T}/I^{\epsilon}$. Also $\mathcal{B}(N)[I^{\epsilon}]$ is of rank 1 "under a mild assumption". This assumption is

- ℓ does not divide N; or
- $\ell \geq 5$.

Thus, as in Mazur's case, the result follows.

New difficulty

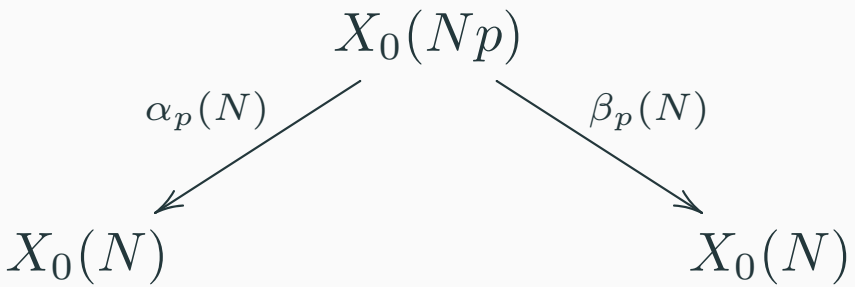
From now on, let N be any positive integer. Then the ℓ-rank of $\mathcal{A}(N)$ is larger than the number of "possible eigenspaces" of $\mathbf{T}/I$ in general. (Each "possible eigenspace" of $\mathbf{T}/I$ is still cyclic though.)

So we need another idea.... Let's start from the beginning...

(In particular, we will review the work of Mazur and Ohta...)

Hecke and Atkin–Lehner operators

Let p be a prime. There are degeneracy maps between modular curves



By the Albanese/Picard functoriality, they induce the maps on Jacobians:

$$\alpha_p(N)_*, \beta_p(N)_* : J_0(Np) \rightrightarrows J_0(N)$$
$$\alpha_p(N)^*, \beta_p(N)^* : J_0(N) \rightrightarrows J_0(Np)$$

We define the p-th Hecke operator T_p by

$$T_p := \beta_p(N)_* \circ \alpha_p(N)^* : J_0(N) \to J_0(N).$$

If $p \mid N$, there is also the Atkin–Lehner operator $w_p \in \mathrm{End}(J_0(N))$.

Mazur's Eisenstein ideal

Let N be a prime. Consider the Hecke algebra $\mathbf{T}(N) \subset \mathrm{End}(J_0(N))$ which is a $\mathbf{Z}$-subalgebra generated by all the p-th Hecke operators T_p for $p \neq N$ and the Atkin–Lehner operator w_N. Namely,

$$\mathbf{T}(N) := \mathbf{Z}[T_p, W_N : \text{ for all primes } p \neq N] \subset \mathrm{End}(J_0(N)).$$

Let $\mathbf{T} = \mathbf{T}(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$. Then $J_0(N)(\mathbf{Q})_{\mathrm{tors}}[\ell^\infty]$ is a module over $\mathbf{T}$. What is the annihilator of this finite module? It is easy to compute the action of the Hecke operators on $\mathcal{C}(N)[\ell^\infty]$. So we define the following, which is the Mazur's Eisenstein ideal:

$$\mathfrak{I} := (w_N + 1, T_p - p - 1 : \text{ for all primes } p \neq N)$$

Eichler–Shimura congruence relation

In fact, we can easily prove that $\mathfrak{I}$ annihilates $J_0(N)(\mathbf{Q})_{\mathrm{tors}}[\ell^\infty]$.

For simplicity, let $J := J_0(N)$ and let p be a prime not dividing N. Then:

The operator $T_p - p - 1$ annihilates $J(\mathbf{Q})_{\mathrm{tors}}[\ell^\infty]$.

Proof.

By the Eichler–Shimura congruence relation, the p-th Hecke operator T_p acting on $J_{/\mathbf{F}_p}$ by $\mathrm{Frob}_p + \mathrm{Ver}_p$. Since Frob_p acts trivially on the $\mathbf{F}_p$-points, $T_p - p - 1$ annihilates $J_{/\mathbf{F}_p}(\mathbf{F}_p)$. Note that there is a Hecke-equivariant injection:

$$\iota_p : J(\mathbf{Q})_{\mathrm{tors}}[\ell^\infty] \to J_{/\mathbf{F}_p}(\mathbf{F}_p)$$

Thus, the claim follows. □

Mazur's another input

Note that the dimension of $E_2(\Gamma_0(N))$ is 1, and w_N acts as -1 on any Eisenstein series of weight 2. Motivated by this fact, Mazur proved:

$$\mathfrak{I} = (T_p - p - 1 : \text{ for all primes } p \neq N)$$

Since all the Hecke operators (and the Atkin–Lehner operator w_N) are congruent to integers modulo $\mathfrak{I}$, the natural map

$$\mathbf{Z}_\ell \to \mathbf{T}/\mathfrak{I}$$

is surjective. If it is injective, then there is a cusp form (of weight 2) and level N with coefficient in $\mathbf{Z}_\ell$ whose p-th coefficient is $1 + p$. This violates Ramanujan's bound and so there is an isomorphism

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

Now the problems are

1. compute the (ℓ-adic) index n;
2. prove that $\#\mathcal{C}(N)[\ell^\infty] = n$;
3. prove that $J_0(N)(\mathbf{Q})_{\text{tors}}[\ell^\infty]$ is cyclic as a $\mathbf{T}/\mathfrak{I}$-module.

In fact, we first compute the order of the group $\mathcal{C}(N) = \langle [0 - \infty] \rangle$. This is done by Ogg. Let $\mathcal{C}(N)[\ell^\infty] = \ell^a$ for some $a \geq 0$. Since $\mathcal{C}(N)[\ell^\infty]$ is annihilated by $\mathbf{T}/\mathfrak{I}$, we have

$$\mathbf{T}/\mathfrak{I} \twoheadrightarrow \mathrm{End}(\mathbf{Z}/\ell^a\mathbf{Z}) = \mathbf{Z}/\ell^a\mathbf{Z}$$

This gives a lower bound for the index.

Consider the (normalized) Eisenstein series (of weight 2):

$$E_{2,N}(\tau) = \frac{N-1}{24} + \sum_{n \geq 1} \Big(\sum_{d|n, (d,N)=1} d \Big) q^n \quad (q = e^{2\pi i \tau}).$$

One can consider $E_{2,N}$ modulo $\mathfrak{I}$; as a modular form over the ring $\mathbf{T}/\mathfrak{I} \simeq \mathbf{Z}/n\mathbf{Z}$. Then its reduction is of the form $\sum_{n=0}^{\infty} a_n q^{nN}$. Mazur proved that such a form must come from level 1 ("level-lowering"), and there is no non-trivial form of level 1. This gives an upper bound.

Luckily, these two bounds are (ℓ-adically) equal. So the last thing we have to prove is the cyclicity. This involves multiplicity one theorem for differential (if $\ell \neq N$) and the Cartier operator in characteristic N; or the computation of the action of the Hecke/Atkin–Lehner operators on the special fiber of the Néron model of $J_0(N)$ over $\mathbf{F}_N$ (if $\ell = N$). Let's skip this....

In summary, $J_0(N)(\mathbf{Q})_{\mathsf{tors}}[\ell^\infty]$ is a cyclic $\mathbf{T}/\mathfrak{I}$-module. Also, from two computations (the order of a certain cuspidal divisor and the constant term of a certain Eisenstein series) we can prove that $\mathcal{C}(N)[\ell^\infty]$ is a free module of rank 1 over $\mathbf{T}/\mathfrak{I}$. Since

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

we finally prove this inclusion is indeed an equality. $\square$

Ohta's generalization: squarefree level

Let $N = \prod_{i=1}^{t} p_i$ be a squarefree integer. Then we consider the following Hecke algebra:

$$\mathbf{T}(N) = \mathbf{Z}[w_{p_i}, T_p : 1 \leq i \leq t, \text{ for primes } p \nmid N] \subset \mathrm{End}(J_0(N)).$$

As before, let $\mathbf{T} = \mathbf{T}(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ and its ideal

$$\mathfrak{I} := (T_p - p - 1 : \text{ for primes } p \nmid N) \subset \mathbf{T}.$$

By the Eichler–Shimura relation, we then have:

$$\mathcal{A}(N) = \mathcal{A}(N)[\mathfrak{I}] \quad \text{and} \quad \mathcal{B}(N) = \mathcal{B}(N)[\mathfrak{I}]$$

Now we regard $\mathcal{A}(N)$ and $\mathcal{B}(N)$ as modules over $\mathbf{T}/\mathfrak{I}$.

What is the structure of the ring $\mathbf{T}/\mathfrak{I}$? It is a semi-local ring with finitely many maximal ideals. Since the Atkin–Lehner operators are involutions, the possible eigenvalues are ± 1. Thus, all possible maximal ideals of $\mathbf{T}$ containing $\mathfrak{I}$ are of the form:

$$(\ell, w_{p_1} - \varepsilon_1, w_{p_2} - \varepsilon_2, \ldots, w_{p_t} - \varepsilon_t, \mathfrak{I}),$$

where $\varepsilon_i \in \{\pm 1\}$. For each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_t) \in \{\pm 1\}^t$, let

$$\mathfrak{I}^{\boldsymbol{\varepsilon}} := (\mathfrak{I}, w_{p_i} - \varepsilon_i : 1 \leq i \leq t).$$

Then it is not so difficult to show that

$$\mathbf{T}/\mathfrak{I} \simeq \prod_{\boldsymbol{\varepsilon} \in \{\pm 1\}^t} \mathbf{T}/\mathfrak{I}^{\boldsymbol{\varepsilon}}.$$

(Here we use the fact that $(w_{p_i} + \varepsilon_i)(w_{p_i} - \varepsilon_i) = 0$ and $w_{p_i} + \varepsilon_i$ is a unit in the Hecke ring completed at $\mathfrak{m}^{\boldsymbol{\varepsilon}}$.)

Thus, we have the following decompositions:

$$\mathcal{A}(N) \simeq \bigoplus_{\boldsymbol{\varepsilon} \in \{\pm 1\}^t} \mathcal{A}(N)[\mathfrak{I}^{\boldsymbol{\varepsilon}}] \quad \text{and} \quad \mathcal{B}(N) \simeq \bigoplus_{\boldsymbol{\varepsilon} \in \{\pm 1\}^t} \mathcal{B}(N)[\mathfrak{I}^{\boldsymbol{\varepsilon}}].$$

Hence it suffices to show that $\#\mathcal{B}(N)[\mathfrak{I}^{\boldsymbol{\varepsilon}}] \leq \#\mathcal{A}(N)[\mathfrak{I}^{\boldsymbol{\varepsilon}}]$. As before, since all the operators are congruent to integers modulo $\mathfrak{I}^{\boldsymbol{\varepsilon}}$, we have $\mathbf{T}/\mathfrak{I}^{\boldsymbol{\varepsilon}} \simeq \mathbf{Z}_\ell/\mathfrak{n}^{\boldsymbol{\varepsilon}}\mathbf{Z}_\ell$ for some $\mathfrak{n}^{\boldsymbol{\varepsilon}} \in \mathbf{N}$. So...

1. Find a cuspidal divisor $C^{\boldsymbol{\varepsilon}}$ annihilated by $\mathfrak{I}^{\boldsymbol{\varepsilon}}$ and compute its order.
2. Find an Eisenstein series $E^{\boldsymbol{\varepsilon}}$ having the same eigenvalues as $\mathfrak{I}^{\boldsymbol{\varepsilon}}$ and compute its constant term.
3. Prove that $\mathcal{B}(N)[\mathfrak{I}^{\boldsymbol{\varepsilon}}]$ is cyclic.

The first one is relatively easy. We have developed an algorithm to compute its order (by hand).

The second one is also easy if we have the following, which is a natural generalization of Mazur's result.

Lemma (level-lowering, Ohta)

Let $p = p_i$. If $f(\tau) = \sum_{n \geq 0} a_n q^{pn}$ is a modular form of level N, then there is a modular form g of level N/p such that $f(\tau) = g(p\tau)$.

The last one can be proved without further difficulty.

Remark

In fact, Ohta used a different argument. Instead of using certain cuspidal divisors, his proof lies on the computation of the order of the whole cuspidal group, which is done by Takagi in 1997.

Summary of Ohta's work

By the Eichler–Shimura congruence relation, we have

$$\mathcal{A}(N) = \mathcal{A}(N)[\mathfrak{I}] \quad \text{and} \quad \mathcal{B}(N) = \mathcal{B}(N)[\mathfrak{I}].$$

Since $\mathbf{T}/\mathfrak{I}$ decomposes into $\mathbf{T}/\mathfrak{I}^{\epsilon}$, two modules are also decomposed accordingly. Thus, it suffices to show that

$$\#\mathcal{B}(N)[\mathfrak{I}^{\epsilon}] \leq \#\mathcal{A}(N)[\mathfrak{I}^{\epsilon}].$$

Since all the operators are congruent to integers modulo $\mathfrak{I}^{\epsilon}$, we have $\mathbf{T}/\mathfrak{I}^{\epsilon} \simeq \mathbf{Z}_{\ell}/\mathfrak{n}^{\epsilon}\mathbf{Z}_{\ell}$. By the first, $\mathfrak{n}^{\epsilon}$ is a multiple of the order of C^{ϵ}. By the second and the lemma, $\mathfrak{n}^{\epsilon}$ is a divisor of the constant term of E^{ϵ}. All three are indeed (ℓ-adically) equal. This proves that $\mathcal{A}(N)[\mathfrak{I}^{\epsilon}]$ is free of rank 1. By the third, $\mathcal{B}(N)[\mathfrak{I}^{\epsilon}]$ is of rank 1 and so the result follows. $\square$

Non-sqaurefree level

Now, let

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

with $r_j \geq 2$. For simplicity, let $M = \prod_{i=1}^{t} p_i$ and let

$$\mathbf{T}(N) = \mathbf{Z}[w_{p_i}, T_p : 1 \leq i \leq t, \text{ for primes } p \nmid M] \subset \mathrm{End}(J_0(N)).$$

Also, let $\mathbf{T} = \mathbf{T}(N) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ and its ideal

$$\mathfrak{I} := (T_p - p - 1 : \text{ for primes } p \nmid N) \subset \mathbf{T}.$$

By the Eichler–Shimura relation, we then have:

$$\mathcal{A}(N) = \mathcal{A}(N)[\mathfrak{I}] \quad \text{and} \quad \mathcal{B}(N) = \mathcal{B}(N)[\mathfrak{I}]$$

For each $\boldsymbol{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_t) \in \{\pm 1\}^t$, let

$$\mathfrak{I}^{\boldsymbol{\varepsilon}} := (\mathfrak{I}, w_{p_i} - \varepsilon_i : 1 \leq i \leq t).$$

As before, one may want to have $\mathbf{T}/\mathfrak{I}^{\epsilon} \simeq \mathbf{Z}_\ell/n\mathbf{Z}_\ell$ for some $n \in \mathbf{N}$. However, we do not know whether the operators T_{q_j} are congruent to integers. Note that T_{q_j} acts as 0 on the space of newforms. So we may try to consider the following ideal:

$$\mathfrak{I}_0^{\epsilon} := (\mathfrak{I}^{\epsilon}, T_{q_j} : 1 \leq j \leq u).$$

Now we can generalize the work of Mazur and Ohta.

Theorem

There is a rational cuspidal divisor C_0^{ϵ} on $X_0(N)$ annihilated by $\mathfrak{I}_0^{\epsilon}$. The order of C_0^{ϵ} is $\mathfrak{n}_0^{\epsilon}$. Also, we have

$$\mathbf{T}/\mathfrak{I}_0^{\epsilon} \simeq \mathbf{Z}_\ell/\mathfrak{n}_0^{\epsilon}\mathbf{Z}_\ell.$$

Furthermore, $J_0(N)(\mathbf{Q})_{\mathrm{tors}}[\ell^\infty, \mathfrak{I}_0^{\epsilon}]$ is cyclic as a $\mathbf{T}/\mathfrak{I}_0^{\epsilon}$-module.

Sketch of proof / Remarks

- Finding a rational cuspidal divisor C_0^{ϵ} annihilated by $\mathfrak{I}_0^{\epsilon}$ is not hard.
- Computing the order of C_0^{ϵ} is not hard... using the algorithm.
- Finding an Eisenstein series E_0^{ϵ} annihilated by $\mathfrak{I}_0^{\epsilon}$ is not hard.
- However, the constant term of E_0^{ϵ} is zero in this case!
  How can we get an upper bound for $\mathfrak{n}_0^{\epsilon}$?
- By the q-expansion principle (by Katz), we can prove that E_0^{ϵ} is in fact a cusp form over the ring $\mathbf{T}/\mathfrak{I}_0^{\epsilon}$. So their residues at various cusps must vanish. Computing the residues of E_0^{ϵ}, we have an upper bound which is (ℓ-adically) equal to the order of C_0^{ϵ}.
- Finally, for the cyclicity of $\mathcal{B}(N)[\mathfrak{I}_0^{\epsilon}]$.... The argument by Mazur (and its generalization by Ohta) works verbatim. Here we use assumption that either $\ell \geq 5$ or $\ell = 3 \nmid N$.
- We slightly extend Ohta's result by including some cases where $\ell = 3 \mid N$. (For instance, $\exists\, p \mid N$ s.t. $p \equiv -1 \pmod 3$.)

What's left?

Thus, if we let

$$\mathfrak{I}_0 := (T_{q_j}, \mathfrak{I} : 1 \leq j \leq u) \subset \mathbf{T},$$

then the previous argument implies that

$$\mathcal{A}(N)[\mathfrak{I}_0] = \mathcal{B}(N)[\mathfrak{I}_0].$$

So we only need the following implication:

$$\mathcal{A}(N)[T_{q_j} : 1 \leq j \leq u] = \mathcal{B}(N)[T_{q_j} : 1 \leq j \leq u] \Longrightarrow \mathcal{A}(N) = \mathcal{B}(N)$$

What can we do for this? This is "the problem" which has never been encountered before. So...??

Inductive method

Fortunately, we could solve this problem by induction.

Theorem

For any primes $q = q_j$, suppose that Conjecture C holds for level N/q. Namely, we have

$$\mathcal{A}(N/q) = \mathcal{B}(N/q).$$

Then we have

$$\mathcal{A}(N)[T_q] = \mathcal{B}(N)[T_q] \iff \mathcal{A}(N) = \mathcal{B}(N).$$

Since T_q commutes with other Hecke operators, the theorem implies that if we assume Conjecture C holds for all lower levels, then

$$\mathcal{A}(N)[T_{q_j} : 1 \le j \le u] = \mathcal{B}(N)[T_{q_j} : 1 \le j \le u] \Longrightarrow \mathcal{A}(N) = \mathcal{B}(N)$$

Proof of the theorem

Let $q = q_j$ for some $1 \leq j \leq u$, i.e., q is a prime whose square divides N.

First, we insist the following.

Claim

If $\mathcal{A}(N/q) = \mathcal{B}(N/q)$, then we have $T_q(\mathcal{A}(N)) = T_q(\mathcal{B}(N))$.

Note that there is an exact sequence

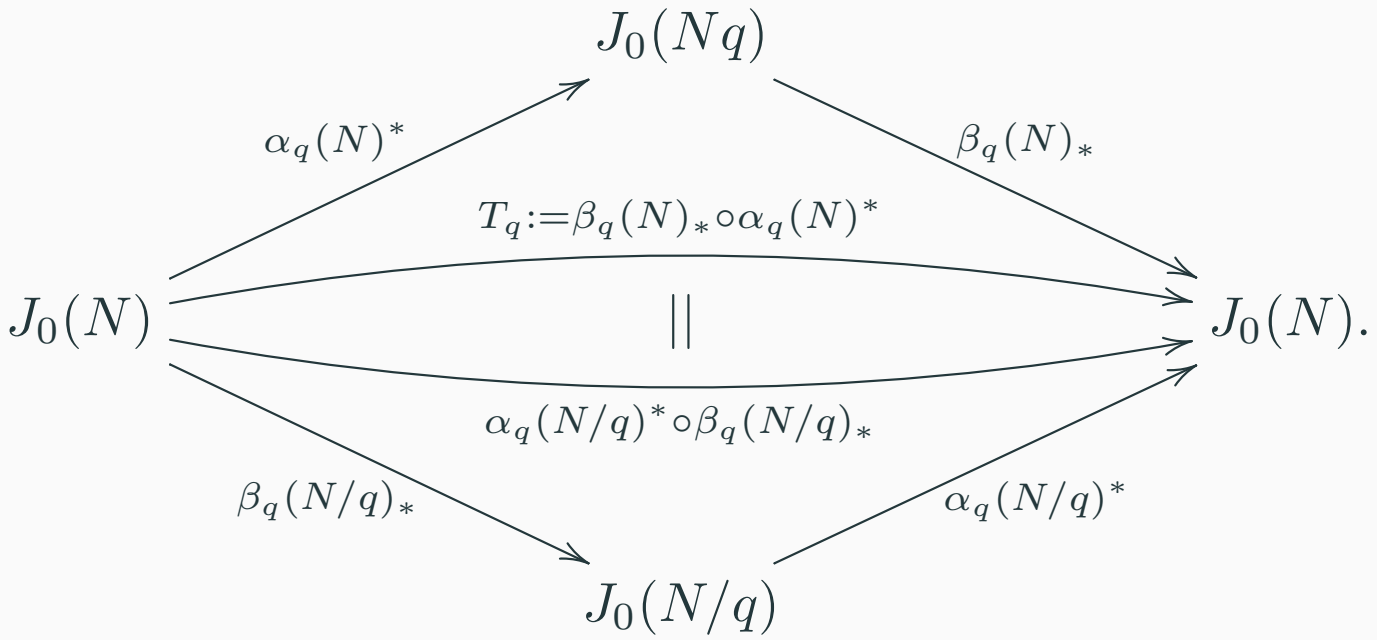
$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{A}(N)[T_q] & \longrightarrow & \mathcal{A}(N) & \longrightarrow & T_q(\mathcal{A}(N)) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathcal{B}(N)[T_q] & \longrightarrow & \mathcal{B}(N) & \longrightarrow & T_q(\mathcal{B}(N)) & \longrightarrow & 0. \end{array}$$

Thus, if Claim holds, then by five lemma we have

$$\mathcal{A}(N)[T_q] = \mathcal{B}(N)[T_q] \iff \mathcal{A}(N) = \mathcal{B}(N).$$

Thus, it suffices to prove the claim.

Proof of Claim. Since q^2 divides the level N, by direct computation of the degeneracy maps we can prove that



Also, by direct computation we have

$$\beta_q(N/q)_*(\mathcal{A}(N)) = \mathcal{A}(N/q).$$

(We know everything about the rational cuspidal divisor class group!)

Since $\beta_q(N/q)_*$ is rational, we have

$$\beta_q(N/q)_*(\mathcal{B}(N)) \subseteq \mathcal{B}(N/q).$$

Thus, we have

$$\begin{aligned} T_q(\mathcal{B}(N)) &\subseteq \alpha_q(N/q)^*(\mathcal{B}(N/q)) = \alpha_q(N/q)^*(\mathcal{A}(N/q)) \\ &= \alpha_q(N/q)^* \circ \beta_q(N/q)_*(\mathcal{A}(N)) = T_q(\mathcal{A}(N)). \end{aligned}$$

This completes the proof. □

Thank you very much
for your attention!