The Eisenstein quotient

Last time

Last time we proved the following criterion:

Theorem A.

Let $N > 7$ be a prime, $A/\mathbb{Q}$ an abelian variety and $f\colon X_0(N) \longrightarrow A$ such that

1. A has good reduction away from N
2. $A(\mathbb{Q})$ has rank 0
3. $f(0) \neq f(\infty)$.

Then, no elliptic curve over $\mathbb{Q}$ has a rational point of order N.

Today, we find a quotient A of $J_0(N) := \mathrm{Jac}(X_0(N))$ which will satisfy these hypotheses.

The structure of $J_0(N)$

Let $N > 7, N \neq 13$ be prime.

Two weeks ago we saw $X_0(N)$ admits an integral model and defined Hecke operators as certain correspondences. Thus, we can see them as morphisms $J_0(N) \longrightarrow J_0(N)$ defined over $\mathbb{Q}$.

Let $\mathbf{T} \subseteq \mathrm{End}(J_0(N))$ be the subalgebra generated by $T_p, p \nmid N$. We also saw that $S_2(N)$ is a free $\mathbf{T} \otimes \mathbb{C}$-module of rank 1, with a basis over $\mathbb{C}$ of normalized eigenforms.

Let $f \in S_2(N)$ be a normalized eigenform with system of eigenvalues $\alpha\colon \mathbf{T} \longrightarrow \mathbb{C}$, i.e. $T_p f = \alpha(T_p) f$.

Let $\mathfrak{p}_f = \ker \alpha$ and

$$A_f := J_0(N)/\mathfrak{p}_f J_0(N).$$

Fact.

$J_0(N)$ is isogenous to $\prod_f A_f$ where f runs over the Galois orbits of normalized eigenforms in $S_2(N)$.

Write $K_f = (\mathbf{T}/\mathfrak{p}_f) \otimes \mathbb{Q}$. This is the number field generated by the Fourier coefficients of f.

Proposition.

A_f is an abelian variety of dimension $[K_f : \mathbb{Q}]$ with good reduction away from N.

Proof.

The tangent space at 0 of $J_0(N)$ satisfies

$$T_0(J_0(N)) \otimes_{\mathbb{Q}} \mathbb{C} \cong H^0(X_0(N), \Omega^1) \otimes_{\mathbb{Q}} \mathbb{C} \cong S_2(N),$$

hence it is a free rank 1 $\mathbf{T} \otimes \mathbb{C}$-module. From this, we see that $T_0(A_f)$ is a K_f-vector space of dimension 1, so in particular $\dim A_f = [K_f : \mathbb{Q}]$. The good reduction away from N follows from the corresponding result for $J_0(N)$ and the Néron–Ogg–Shafarevich criterion. $\square$

Choose an embedding $\iota\colon K_f \longrightarrow \overline{\mathbb{Q}}_\ell$, or equivalently a prime λ of K above ℓ. From the Eichler–Shimura relation, one shows:

Fact.

The representation $V_{f,\lambda} := \iota V_\ell(A_f)$ is the unique semisimple representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\overline{\mathbb{Q}}_\ell)$ satisfying:

- ρ is unramified away from $N\ell$.
- $\mathrm{tr}(\rho(\text{Frobenius at } p)) = a_p(f)$ for $p \nmid N\ell$.
- $\det(\rho) = \chi_\ell = \ell$-adic cyclotomic character.

Fact.

$J_0(N)$ has completely toric reduction at N.

Corollary

Any quotient of $J_0(N)$ has completely toric reduction at N.

Proof.

Let $f\colon J_0(N) \longrightarrow A$ be the quotient map. There exists a map $g\colon A \longrightarrow J_0(N)$ such that $fg = [n]$ for some $n > 0$. f and g extend to the Néron models $\mathcal{J}, \mathcal{A}$ of $J_0(N), A$ over $\mathbb{Z}_N$ and still satisfy $fg = [n]$, so we get morphims in the special fibers $\mathcal{J}_{\mathbb{F}_N}, \mathcal{A}_{\mathbb{F}_N}$ satisfying $fg = [n]$. In particular, $f\colon \mathcal{J}_{\mathbb{F}_N} \longrightarrow \mathcal{A}_{\mathbb{F}_N}$ is surjective, so $\mathcal{A}_{\mathbb{F}_N}$ is a torus. $\square$

The difference of the cusps

Proposition.

The point $[0] - [\infty] \in J_0(N)$ is a non-trivial torsion point of order dividing $N - 1$.

Proof.

If $[0] - [\infty]$ was trivial, it would the divisor of some function f on $X_0(N)$, which would define a degree 1 map to $\mathbb{P}^1$, so $X_0(N)$ would need to have genus 0, which is false.

Proof (continued).

Consider the modular form

$$\Delta(z) = q \prod_{n \geq 1} (1 - q^n)^{24} = q + \cdots \in S_{12}(\Gamma(1))$$

for $q = e^{2\pi i z}$. It is nowhere vanishing on the upper-half plane.
$\Delta(Nz) \in S_{12}(N)$ is also nowhere vanishing, so

$$f(z) := \Delta(z)/\Delta(Nz) = q^{-(N-1)} + \cdots$$

is a $\Gamma_0(N)$-invariant nowhere vanishing function on the upper-half plane, so it defines a meromorphic function on $X_0(N)$.
f has a pole of order $N-1$ at ∞, so 0 must be a zero of order $N-1$.
Thus, $\mathrm{div}(f) = (N-1)[0] - (N-1)[\infty]$. □

Remark.

Ogg showed that the order of $[0] - [\infty]$ is exactly $(N-1)/\gcd(N-1, 12)$, and Mazur shows that it generats the torsion subgroup of $J_0(N)$.

Proposition.

For $\ell \neq N$, $T_\ell([0]-[\infty]) = (\ell+1)([0]-[\infty])$

Proof.

T_ℓ is given by the correspondence

$$\begin{tikzcd} & X_0(N\ell) \arrow[dl, "f"'] \arrow[dr, "g"] & \\ X_0(N) & & X_0(N) \end{tikzcd}$$

where f and g correspond to the identity map and multiplication by ℓ on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, i.e.

$$T_\ell([P]) = g_*(f^*([P])).$$

Proof (continued).

$X_0(N\ell)$ has 4 cusps, corresponding to $(x, y) \in \{\text{cusps of } X_0(N)\} \times \{\text{cusps of } X_0(\ell)\}$. We see that $f(x, y) = g(x, y) = x$.

f has ramification index ℓ at $(x, 0)$ and index 1 at (x, ∞). Thus,

$$\begin{aligned} f^*([x]) &= \ell[(x,0)] + [(x,\infty)], \\ g_*(f^*([x])) &= (\ell+1)[x], \\ T_\ell([0]-[\infty]) &= g_*(f^*([0]-[\infty])) = (\ell+1)([0]-[\infty]). \end{aligned}$$

$\square$

The Eisenstein quotient: motivation

We want to find a quotient A of $J_0(N)$ such that

- A has good reduction away from N.
- $f([0]) \neq f([\infty])$ for $f\colon X_0(N) \longrightarrow J_0(N) \longrightarrow A$.
- $A(\mathbb{Q})$ has rank 0.

To check last condition, we want to use Theorem B, which says that this condition is satisfied if

- A has good reduction away from N.
- A has completely toric reduction at N.
- All Jordan-Hölder factors of A are trivial or cyclotomic.

The first two conditions come for free, but the last one doesn't.

The case of rational coefficients

Assume all normalized eigenforms $f \in S_2(N)$ have rational coefficients.

Fix a prime $p \neq N$. Say that an abelian variety $A/\mathbb{Q}$ satisfies JH(p) if all the Jordan-Hölder factors of $A[p](\overline{\mathbb{Q}})$ are trivial or cyclotomic.

Note that this is isogeny invariant. Because of the decomposition (up to isogeny)

$$J_0(N) = \prod_f A_f,$$

there is a maximal quotient of $J_0(N)$ satisfying JH(p).

Lemma.

For a modular form f with $K_f = \mathbb{Q}$, A_f satisifies JH(p) $\iff p \mid (a_\ell(f) - (\ell+1))$ for all $\ell \nmid pN$.

Proof.

If A_f satisfies JH(p), then the semisimplification of $A_f[p]$ is $(\mathbb{Z}/p\mathbb{Z}) \oplus \chi_p$ since its determinant is χ_p. Thus, mod p, the trace of the Frobenius at ℓ (which is $a_\ell(f)$) is $\ell + 1$. Similarly for the converse. $\square$

Remark.

The Eisenstein series of weight 2 satisfies $T_\ell(E_2) = (\ell+1)E_2$ for all ℓ, so A_f satisfies JH(p) $\iff$ the Fourier coefficients of f are congruent mod p to those of E_2.

Let S be the set of f such that A_f satisfies JH(p).

For each f, let $\mathfrak{p}_f$ be the kernel of the corresponding system of eigenvalues $\mathbf{T} \longrightarrow \mathbb{C}$. Define

$$I := \bigcap_{f \in S} \mathfrak{p}_f$$
$$A := J_0(N)/IJ_0(N)$$

A satisfies JH(p), so by Theorem B, $A(\mathbb{Q})$ has rank 0. But for all we know, S could be empty and A trivial!

Let p divide the order of $[0] - [\infty] \in J_0(N)$. Then, $J_0(N)$ has a p-torsion point, so $J_0(N)[p]$ has a copy of the trivial representation, which must come from some A_f. This f belongs to S.

Define the p-Eisenstein ideal as the ideal $\mathfrak{a}$ of $\mathbf{T}$ generated by p and $T_\ell - (\ell + 1)$ for all ℓ.

Lemma.

$\mathbf{T}/\mathfrak{a} \cong \mathbb{F}_p$. In particular $\mathfrak{a}$ is maximal.

Proof.

Let $f \in S$, so $T_\ell - (\ell + 1)$ is divisible by p in $\mathbf{T}/\mathfrak{p}_f$. The image of $\mathfrak{a}$ in $\mathbf{T}/\mathfrak{p}_f$ is not the unit ideal, so $\mathbf{T}/\mathfrak{a} \cong \mathbb{F}_p$ as every operator is identified with an integer. $\square$

Lemma.

$f \in S \iff \mathfrak{p}_f \subseteq \mathfrak{a}$

Proof.

$f \in S \iff T_\ell - (\ell+1)$ is divisible by p in $\mathbf{T}/\mathfrak{p}_f \iff$ the image of $\mathfrak{a}$ in $\mathbf{T}/\mathfrak{p}_f$ is not the unit ideal $\iff \mathfrak{p}_f \subseteq \mathfrak{a}$. □

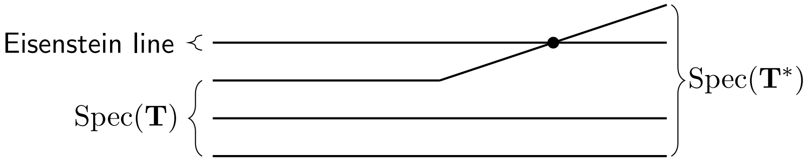
Corollary.

I is the intersection of the minimal primes of $\mathbf{T}$ contained in $\mathfrak{a}$. In particular, $I_\mathfrak{a} = 0$.

Proof.

The minimal primes are the $\mathfrak{p}_f$. $I_\mathfrak{a}$ is the nilradical of the reduced ring $\mathbf{T}_\mathfrak{a}$. □

The Eisenstein ideal is the ideal of $\mathbf{T}$ generated by $T_\ell - (\ell + 1)$. We can view this geometrically as



where $\mathbf{T}^*$ is the Hecke algebra acting on the space of all modular forms of weight 2 and level N.

The image of $[0]-[\infty]$ in A

The p-adic completion $\mathbf{T}_p := \varprojlim_n \mathbf{T}/p^n$ is a product of local rings,

$$\mathbf{T}_p = \prod_{p \in \mathfrak{m} \subseteq \mathbf{T} \text{ maximal}} \mathbf{T}_{\mathfrak{m}}.$$

If X is a $\mathbf{T}$-module where every element is killed by some power of p, the action of $\mathbf{T}$ extends to an action of $\mathbf{T}_p$, and we have a decomposition $X = X_{\mathfrak{a}} \oplus X'$ where $\mathfrak{a}$ acts trivially on X' and $X_{\mathfrak{a}} = X[\mathfrak{a}^\infty]$.

Lemma

The map $J_0(N)[\mathfrak{a}^\infty] \longrightarrow A[\mathfrak{a}^\infty]$ *is an isomorphism.*

Proof.

Write $X = J_0(N)[p^\infty], Y = A[p^\infty]$. We have a surjection $X \longrightarrow Y$ with kernel $X \cap IJ_0(N) = IX$. Localize the short exact sequence

$$0 \longrightarrow IX \longrightarrow X \longrightarrow Y \longrightarrow 0$$

at $\mathfrak{a}$. Since $(IX)_\mathfrak{a} = I_\mathfrak{a} X_\mathfrak{a} = 0$, $X_\mathfrak{a} \longrightarrow Y_\mathfrak{a}$ is an isomorphism. $\square$

Proposition.

$[0] \neq [\infty]$ in A

Proof.

Let $P = [0] - [\infty]$ and $Q \neq 0$ be a multiple of P which is p-torsion. Then Q is $\mathfrak{a}$-torsion since $T_\ell(P) = (\ell + 1)P$, so the same holds for Q. Thus, the image of Q in $A[\mathfrak{a}^\infty]$ is non-zero. $\square$

The general case

In general we have

$$V_p J_0(N) = \prod_f \prod_{\mathfrak{p}} V_{f,\mathfrak{p}},$$

and for a given f, it's possible that some $V_{f,\mathfrak{p}}$ are of the form (trivial) + (cyclotomic) while others aren't.

We will take A to be the quotient of $J_0(N)$ corresponding to those f such that $V_{f,\mathfrak{p}}$ is of the form (trivial) + (cyclotomic) for *some* $\mathfrak{p}$. However, A will not satisfy the hypotheses of Theorem B, so we will have to work around that next time.

Choose a prime p dividing the order of $[0]-[\infty] \in J_0(N)$, and let $\mathfrak{a}$ be the ideal generated by p and $T_\ell - (\ell+1)$.

Lemma

$\mathbf{T}/\mathfrak{a} \cong \mathbb{F}_p$. *In particular, $\mathfrak{a}$ is maximal.*

Proof.

Since $J_0(N)[p]$ has a rational point, some constituent of $V_p J_0(N)$ is trivial. This must come from some $(f, \mathfrak{p})$, and for such a pair we must then have

$$\overline{V}_{f,\mathfrak{p}}^{\mathrm{ss}} \cong (\mathbb{Z}/p\mathbb{Z}) \oplus \chi_p.$$

Thus $a_\ell(f) = \ell + 1$ modulo $\mathfrak{p}$ for all ℓ, so the image of $\mathfrak{a}$ in $\mathbf{T}/\mathfrak{p}_f$ is contained in $\mathfrak{p}$. So $\mathfrak{a}$ is not the unit ideal, and $\mathbf{T}/\mathfrak{a} \cong \mathbb{F}_p$. $\square$

Let I be the intersection of the minimal primes of $\mathbf{T}$ contained in $\mathfrak{a}$ and $A = J_0(N)/IJ_0(N)$. The same proof as before shows:

Proposition.

$[0] \neq [\infty]$ in A.