The Eisenstein Ideal

Andrew Yang

July 13, 2026

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

Theorem 1 (Theorem A)**.** *Suppose there exists an abelian variety A over $\mathbb{Q}$ and a map of $\mathbb{Q}$-varieties $f : X_0(N) \to A$ such that*

i. A has good reduction away from N,

ii. $f(0) \neq f(\infty)$,

iii. $A(\mathbb{Q})$ has rank 0.

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

Our goal today is to try to construct such an A. It is natural to try to find it among the quotients of $J_0(N) := \mathrm{Jac}(X_0(N))$. Note that since having good reduction passes along quotients, i is automatic. Also note that $J_0(N)$ is nontrivial by the assumption on N.

1 Reminder: Hecke Algebra

We will construct the quotient via the Hecke algebra action. Recall that

Definition 2. *For prime $p \neq N$, the **Hecke correspondence** T_p is the following diagram*

$$\begin{array}{ccc} & X_0(pN) & \\ {\scriptstyle \pi_1}\swarrow & & \searrow{\scriptstyle \pi_2} \\ X_0(N) & & X_0(N) \end{array}$$

*with $\pi_1 : (E, C) \mapsto (E, C[N])$ and $\pi_2 : (E, C) \mapsto (E/C[p], C/C[p])$. This induces the **Hecke operator** $T_p := \pi_{2*}\pi_1^*$ on $\mathrm{Pic}(X_0(N))$, $J_0(N)$, and $\mathcal{S}^2(\Gamma_0(N)) := H^0(X_0(N), \Omega^1)$.*

On the (extended) upper half plane $\mathfrak{h}^*$, π_1 and π_2 lifts to $\pi_1 : z \mapsto z$ and $\pi_2 : z \mapsto pz$. To describe the actions on cusps, we use the following result

Fact 3. *Let N be a squarefree number. There is a bijection between cusps of $X_0(N)$ (i.e. $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$) and divisors of N via the width function: $w : u/v \mapsto N/\gcd(v,N)$ (where u, v are coprime) and $w : \infty \mapsto 1$. The width also describes the stabilizer* $\mathrm{Stab}(x) = \pm \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix} \begin{pmatrix} 1 & w(x)\mathbb{Z} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}^{-1}$.

In particular $X_0(pN)$ has four cusps corresponding to $1, 1/p, 1/N, 1/pN$, which we will label $(0,0), (0,\infty), (\infty,0), (\infty,\infty)$, and clearly $\pi_i(x,y) = x$ for $x, y \in \{0,\infty\}$. By the description of the cusp widths, π_1 has ramification index 1 at (x,∞) and p at $(x,0)$, and π_2 is the opposite. Hence

Lemma 4. *$T_p([0]) = (p+1)[0]$, $T_p([\infty]) = (p+1)[\infty]$ in $\mathrm{Pic}(X_0(N))$.*

Definition 5. *The **Hecke algebra** $\mathbb{T}$ is the subring of $\mathrm{End}_{\mathbb{Q}}(J_0(N))$ generated by all $\{T_p | p \text{ prime}, p \neq N\}$.*

Fact 6. *$\mathbb{T}$ is commutative and finite free as a $\mathbb{Z}$-module.*

Fact 7. *$\mathbb{T} \otimes \mathbb{Q} = \prod_f K_f$ a product of number fields indexed by galois conjugacy classes of normalised eigenforms (in $\mathcal{S}^2(\Gamma_0(N))$). $\mathbb{T}$ then embeds into $\prod_f \mathcal{O}_{K_f}$. Let $\mathfrak{p}_f := \ker(\mathbb{T} \to \mathcal{O}_{K_f})$. This induces an isogeny $J_0(N) \to \bigoplus_f A_f$ where $A_f := J_0(N)/\mathfrak{p}_f J_0(N)$ is an abelian variety of genus $g_f := [K_f : \mathbb{Q}]$.*

Fact 8. *$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $A_f(\overline{\mathbb{Q}})$, and $V_p(A_f) := \varprojlim_n A_f[p^n](\overline{\mathbb{Q}})$ is a $2g_f$-dimensional p-adic galois representation. $V_p(A_f)$ also has a K_f action and is in fact free of rank 2 over $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_p = \prod_{\lambda|p} K_\lambda$. This decomposes $V_p(A_f) = \prod_{\lambda|p} V_{f,\lambda}$ where each $V_{f,\lambda}$ is a two-dimensional K_λ-galois representation. Each $V_{f,\lambda}$ has cyclotomic determinant, unramified for $p \nmid N\ell$ with $\mathrm{tr}(\mathrm{Frob}_p |_{V_{f,\lambda}}) = a_p(f)$. For $p = \ell$, $V_{f,\lambda}^{I_p}$ is at most one-dimensional and Frob_p acts on it via $a_p(f)$.*

For references see e.g. Diamond-Shurman Section 6.6 and 9.5.

2 The Eisenstein Ideal

We now turn our attention to *iii*. Recall that

Theorem 9 (Theorem B)**.** *Let A ba an abelian variety over $\mathbb{Q}$ and $p \neq N$ be another prime. Suppose*

1. *A has good reduction away from N,*
2. *A has completely toric reduction at N,*
3. *The Jordan–Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are one-dimensional and either trivial $\mathbb{1}$ or cyclotomic χ_p (a condition we will abbreviate as $JH(p)$).*

Then $A(\mathbb{Q})$ has rank 0.

1 and *2* were proven in previous talks so we turn our attention to the $JH(p)$ condition.

Lemma 10. *Suppose f is a normalised eigenform with $K_f = \mathbb{Q}$ (i.e. A_f is an elliptic curve). Then A_f satisfies $JH(p)$ if and only if $a_\ell(f) \equiv \ell + 1 \pmod{p}$ for all $\ell \nmid N$.*

Proof. ($\Rightarrow$): Since $A_f[p](\overline{\mathbb{Q}})$ is two dimensional and has cyclotomic determinant, $A_f[p](\overline{\mathbb{Q}})^{ss} = \mathbb{1} \oplus \chi_p$. For $\ell \neq p$, we know that Frob_ℓ has trace $a_\ell(f)$ (in $\mathbb{F}_p$) on $A_f[p](\overline{\mathbb{Q}})$. OTOH, $\mathrm{tr}\left(\mathrm{Frob}_\ell \Big|_{A_f[p](\overline{\mathbb{Q}})}\right) = \mathbb{1} + \ell$. Note that $A_f[p](\overline{\mathbb{Q}})^{ss} = \mathbb{1} \oplus \chi_p$ also implies that A_f has good ordinary reduction at p, and for $\ell = p$, $A_f[p](\overline{\mathbb{Q}})^{I_p} = \mathbb{1}$, so $a_p(f) \equiv 1 \pmod{p}$.

($\Leftarrow$): We conclude $A_f[p](\overline{\mathbb{Q}})^{ss} = 1 \oplus \chi_p$ by Cebotarev and Brauer–Nesbitt. □

Definition 11. *The **Eisenstein ideal** $\mathfrak{J}$ is defined to be the ideal of $\mathbb{T}$ generated by $T_\ell - (\ell + 1)$ for all $\ell \neq N$.*

Lemma 12. *Suppose f is a normalised eigenform with $K_f = \mathbb{Q}$, and $p \neq N$ is a prime such that $\langle \mathfrak{J}, p \rangle \neq 1$. Then A_f satisfies $JH(p)$ if and only if $\mathfrak{p}_f \subseteq \langle \mathfrak{J}, p \rangle$.*

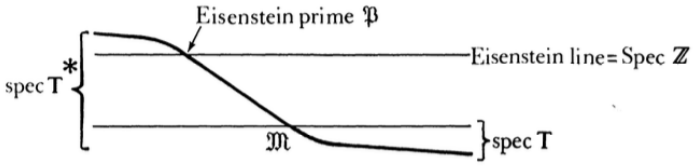
Proof. $\mathfrak{p}_f \subseteq \langle \mathfrak{J}, p \rangle$ is equivalent to $\mathbb{T}/\mathfrak{p}_f \xrightarrow{\sim} \mathbb{Z} \to \mathbb{Z}/p$ sends T_ℓ to $\ell + 1$ for all $\ell + 1$, which is equivalent to A_f satisfying $JH(p)$ via the previous lemma. □

Definition 13. *An **Eisenstein prime** is a prime $p \neq N$ such that $\langle \mathfrak{J}, p \rangle \neq 1$.*

Now the question is if they exist or not, i.e. if $\mathfrak{J} = 1$ or not.

Remark. *Recall that the space $\mathcal{M}^2(\Gamma_0(N))$ decomposes into $\mathcal{S}^2(\Gamma_0(N)) \oplus \mathbb{C}E_{2,N}$ where $E_{2,N}$ is the weight 2 level N Eisenstein series with $a_p(E_{2,N}) = p + 1$ for $p \nmid N$.*

If we consider $\mathbb{T}^* := \mathbb{Z}[T_p | p \nmid N] \subseteq \mathrm{End}(\mathcal{M}^2(\Gamma_0(N)))$ and $\mathfrak{J}^*$ the kernel of $\mathbb{T}^* \to \mathbb{Z}$, the map corresponding to $E_{2,N}$. Then $\mathbb{T}^*$ surjects onto $\mathbb{T}$, and $\mathfrak{J}$ is the image of $\mathfrak{J}^*$. To show that $\mathfrak{J} \neq 1$ is equivalent to finding some congruence between $E_{2,N}$ and some cusp form.



Lemma 14. *$[0] - [\infty] \in J_0(N)(\mathbb{Q}) \cong \mathrm{Pic}^0(X_0(N))$ is a nontrivial torsion point of order dividing $N - 1$.*

Proof. We show that $[0] - [\infty] \neq 0$ and $(N - 1)([0] - [\infty]) = 0$.

For the former, if $\mathrm{div}(f) = [0] - [\infty]$ then $f : X_0(N) \to \mathbb{P}^1$ is a degree 1 map, making $X_0(N)$ rational.

For the latter, I claim that $\mathrm{div}(f) = (N-1)([0]-[\infty])$ where $f(z) := \frac{\Delta(z)}{\Delta(Nz)}$. Δ is holomorphic nowhere vanishing on the upper half plane, so 0 and ∞ are the only zeroes and poles of f. The q-expansion of f at ∞ looks like $\frac{q+\cdots}{q^N+\cdots} = q^{-(N-1)} + \cdots$, and f has a pole at ∞ of order $N-1$. Since $\mathrm{div}(f)$ has degree 0, the result follows. □

From now on n will denote the order of $[0]-[\infty]$.

Remark. *Ogg showed that* $n = \frac{N-1}{\gcd(N-1,12)}$.

Lemma 15. *If $p|n$, then p is an Eisenstein prime.*

Proof. We may find some multiple of $[0]-[\infty]$ in $J_0(N)(\mathbb{Q})$ of order p. This implies that $J_0(N)[p]$ has a rational point and thus contains a copy of the trivial representation. This will appear in some $V_{f,\lambda}[p]$ and so $V_{f,\lambda}[p]^{ss} = 1 \oplus \chi_p$. As before, this implies that $a_\ell(f) \equiv \ell + 1 \pmod{\lambda}$ for all $\ell \neq N$, which implies that $\langle \mathfrak{J}, p\rangle$ is contained in the kernel of $\mathbb{T}/\mathfrak{p}_f \to \mathcal{O}_{K_f}/\lambda$. □

Remark. *In the original paper, Mazur actually showed that* $\mathbb{T}/\mathfrak{J} \cong \mathbb{Z}/n$.

Now, if all f are rational, $J_0(N) = \prod A_f$ and we can simply pick out the A_p's that safiesfy $JH(p)$. That is, we fix an Eisenstein prime p, and Take $A := J_0(N)/IJ_0(N)$ where $I := \bigcap_{\mathfrak{p}_f \subseteq \langle \mathfrak{J}, p\rangle} \mathfrak{p}_f$. Of course the assumption is not true in general. We still take the same A, but now there is no gurantee that A satisfies $JH(p)$. The issue is that $\mathbb{T}$ now contains copies of some $\mathcal{O}_f$ over $\mathbb{Z}$, which might split at some primes and the Eisenstein line might only pass through one of the primes, i.e. some $V_{f,\lambda}$ satisfies $JH(p)$ but not all of the other $V_{f,\lambda'}$'s.

How do we apply theorem B in this case? Answer: we don't. But we will adapt the proof of theorem B to it. (See Simon's talk for this)

3 Quotients of $J_0(N)$

Fix an Eisenstein prime $p|n$ and let $\mathfrak{P} := \langle \mathfrak{J}, p\rangle$ be the corresponding maximal ideal. Denote $\mathbb{T}_{\mathfrak{P}} := \varprojlim_n \mathbb{T}/\mathfrak{P}^n$ to be the completion, and $I(\mathfrak{P}) := \ker(\mathbb{T} \to \mathbb{T}_{\mathfrak{P}}) = \bigcap_n \mathfrak{P}^n$. Note that the map factors through the localisation $\mathbb{T} \to \mathbb{T}/I(\mathfrak{P}) \hookrightarrow \mathbb{T}_{(\mathfrak{P})} \hookrightarrow \mathbb{T}_{\mathfrak{P}}$. Let $A := J_0(N)/I(\mathfrak{P})J_0(N)$.

Lemma 16. *Let R be a reduced noetherian ring, and $\mathfrak{a}$ be an ideal.*

$$I(\mathfrak{a}) := \bigcap_n \mathfrak{a}^n = \bigcap_{\substack{\mathfrak{p} \in \mathrm{Spec}(R) \\ \mathfrak{p} + I \neq 1}} \mathfrak{p}$$

Proof. Recall that by Artin–Rees, $\bigcap_n \mathfrak{a}^n = \{x | \exists a \in \mathfrak{a}, ax = x\}$. Since R is reduced, it embeds into $\prod \mathrm{Frac}(R/\eta_i)$ where η_i runs through all minimal primes. Let I be the subset of indices such that $\mathfrak{a} + \eta_i \neq 1$, then clearly $\{x | \exists a \in \mathfrak{a}, ax = x\} = \{x | \forall i \in \mathfrak{a}, x \equiv 0 \pmod{\eta)_i}\} = \bigcap_{\eta_i + \mathfrak{a} \neq 1} \eta_i$. □

Lemma 17. *Let R be a reduced noetherian ring, and $\mathfrak{p}$ be a maximal ideal. The localization of $I(\mathfrak{p})$ at $\mathfrak{p}$ is zero.*

Proof. Use $I(\mathfrak{p}) = \{x | \exists a \in \mathfrak{p}, (a-1)x = 0\}$. □

Since $\mathbb{T}_p = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is finite over the complete local ring $\mathbb{Z}_p$, it is a product of its localizations. In particular $\mathbb{T}_{\mathfrak{P}}$ is a component of $\mathbb{T}_p$. For any $\mathbb{T}$-module M, the action on $M[p^\infty] := \bigcup_n M[p^n]$ extends to $\mathbb{T}_p$, and the $\mathbb{T}_{\mathfrak{P}}$ component $M[p^\infty]_{(\mathfrak{P})}$ is given by $M[\mathfrak{P}^\infty] := \bigcup_n M[\mathfrak{P}^n]$

Lemma 18. *The map $J_0(N)(\overline{\mathbb{Q}})[\mathfrak{P}^\infty] \to A(\overline{\mathbb{Q}})[\mathfrak{P}^\infty]$ is an isomorphism.*

Proof. Note that taking $[p^\infty]$ is exact on abelian varieties, and so is taking $\overline{\mathbb{Q}}$-points. Let $I(\mathfrak{P}) = \langle t_1, \ldots, t_k \rangle$, then we have the exact sequence

$$J_0(N)^k \xrightarrow{(t_1, \ldots t_k)} J_0(N) \to A \to 0$$

Which yields

$$J_0(N)(\overline{\mathbb{Q}})[p^\infty]^k \xrightarrow{(t_1, \ldots t_k)} J_0(N)(\overline{\mathbb{Q}})[p^\infty] \to A(\overline{\mathbb{Q}})[p^\infty] \to 0$$

Let $X := J_0(N)(\mathbb{Q})[p^\infty]$ and $Y := A(\mathbb{Q})[p^\infty]$, we conclude that

$$0 \to IX \to X \to Y \to 0,$$

and since $I(\mathfrak{P})_{(\mathfrak{P})} = 0$, localising at $\mathfrak{P}\mathbb{T}_p$ gives

$$0 \to 0 \to J_0(N)[\mathfrak{P}^\infty] \to A[\mathfrak{P}^\infty] \to 0.$$

□

We can now check *ii*.

Corollary 19. *Let $f : X_0(N) \to J_0(N) \to A$, then $f(0) \neq f(\infty)$.*

Proof. According to the calculations on Hecke operators earilier, $(n/p)([0]-[\infty])$ is annihilated by $\mathfrak{P}$. Since $(n/p)([0]-[\infty]) \neq 0$ in $J_0(N)[\mathfrak{P}^\infty]$, we conclude that $(n/p)([0]-[\infty]) \neq 0$ in $A[\mathfrak{P}^\infty]$ and hence $f(0) - f(\infty) \neq 0$ in A. □

For *iii*,

Lemma 20. *Let $\mathcal{O}$ be an integral domain which is finite free as an $\mathbb{Z}$-module, $\mathfrak{m}$ be a maximal ideal of $\mathcal{O}$, and M be a finitely generated $\mathcal{O}$-module. If $M_{\mathfrak{m}}$ is finite, then so is M.*

Proof. First of all, M is $\mathcal{O}$-torsion, or else $\mathcal{O} \hookrightarrow M$ implies $\mathcal{O}_{\mathfrak{m}} \hookrightarrow M_{\mathfrak{m}}$ is infinite. Using noetherianity, we can find a $a \neq 0 \in \mathcal{O}$ such that $aM = 0$. Then M is finitely generated over the finite ring $\mathcal{O}/(a)$, which is finite. □

Lemma 21. *Let M be a finitely generated $\mathbb{T}/I(\mathfrak{P})$ module. If $M_{\mathfrak{P}}$ is finite, then so is M.*

Proof. First of all $M \to \prod_{\eta_i} M/\eta_i$ (where the η_i runs through all minimal primes in $\mathfrak{P}$) has finite cokernel as $A \to \prod_{\eta_i} A/\eta_i$ also does, and thus $M \to \prod_{\eta_i} M/\eta_i$ also has finite kernel (where we used the following fact twice a map f of finitely generated abelian groups with the same rank has finite kernel iff it has finite cokernel twice). By the previous lemma, $M/\eta_i M$ is finite for all minimal primes η_i in $\mathfrak{P}$, and hence M is also finite. □

Corollary 22. *To show that $A(\mathbb{Q})$ is finite, it suffices to show that $A(\mathbb{Q})_{\mathfrak{P}}$ is.*

4 References

We mainly follow Andrew Snowden's course notes with some proofs referring back to Mazur's original paper.