The Eisenstein ideal and its application to W. Stein's conjecture about Jacobians of modular curves

Kenneth A. Ribet

November 29–30, 2020
ICTS

Hecke rings

Let $N > 1$ be a square free integer, M be the space of weight 2 classical modular forms on $\Gamma_0(N)$, $S \subset M$ the space of cusp forms, $E \subseteq M$ the space of Eisenstein series.

The dimension of E is $2^\nu - 1$, where ν is the number of primes dividing N.

Hecke rings:

- $\mathbf{T} = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} M$;
- $\mathbf{T}_S = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} S$;
- $\mathbf{T}_E = \mathbf{Z}[\ldots, T_n, \ldots] \subseteq \operatorname{End} E$.

Thus $\mathbf{T}_S$ and $\mathbf{T}_E$ are quotients of $\mathbf{T}$ and

$$\mathbf{T} \hookrightarrow \mathbf{T}_S \times \mathbf{T}_E,$$

with the cokernel being a finite abelian group.

Eisenstein ideal(s)

In view of $\mathbf{T} \hookrightarrow \mathbf{T}_S \times \mathbf{T}_E$, it is convenient to think of the restriction maps $\mathbf{T} \twoheadrightarrow \mathbf{T}_S$ and $\mathbf{T} \twoheadrightarrow \mathbf{T}_E$ as projections.

The Eisenstein ideal of $\mathbf{T}$ is

$$I = \ker(\mathbf{T} \to \mathbf{T}_E), \quad I \subseteq \mathbf{T}.$$

Projection onto the first factor maps I injectively to $\mathbf{T}_S$; let

$$I_S = \text{image of } I \text{ in } \mathbf{T}_S.$$

It seems like good practice in this context to speak mostly of $\mathbf{T}$ and relatively little of $\mathbf{T}_S$ and I_S.

Primes of $\mathbf{T}$

The maximal ideals of $\mathbf{T}$ that arise via pullback from $\mathbf{T}_E$ are *Eisenstein*; the maximal ideals of $\mathbf{T}$ that arise via pullback from $\mathbf{T}_S$ are *cuspidal*.

Maximal ideals of $\mathbf{T}$ that are both Eisenstein and cuspidal ("primes of fusion") correspond to Eisenstein primes of $\mathbf{T}_S$ and also to cuspidal primes of $\mathbf{T}_E$.

To each maximal ideal $\mathfrak{m}$ of $\mathbf{T}$, we associate the continuous semisimple representation

$$\overline{\rho}_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{T}/\mathfrak{m})$$

with the defining property that $\overline{\rho}_{\mathfrak{m}}(\mathrm{Frob}_q)$ has trace $T_q \pmod{\mathfrak{m}}$ and determinant q mod $\mathfrak{m}$ for almost all primes q.

Prime level

If N is prime, we enter the world of B. Mazur's celebrated "Eisenstein ideal" article (1977). The space E is one-dimensional; $\mathbf{T}_E = \mathbf{Z}$. The set of Eisenstein primes of $\mathbf{T}$ is the set of prime numbers. The cuspidal maximal ideals (primes) of $\mathbf{T}$ are obtained by reducing level N cuspidal newforms mod $\mathfrak{p}$ for all choices of eigenforms and maximal ideals $\mathfrak{p}$ in their rings of coefficients.

The primes of fusion are the Eisenstein primes associated to prime numbers that divide Mazur's magic numerator $\operatorname{num}\left(\dfrac{N-1}{12}\right)$. The Eisenstein primes of $\mathbf{T}_S$ are the maximal ideals (I_S, p), where p is a prime dividing the numerator.

Reducible representations

Each representation $\overline{\rho}_{\mathfrak{m}}$ is "semistable" and is therefore either irreducible or the direct sum of the trivial character and the mod p cyclotomic character (p being the residue prime of $\mathfrak{m}$). If $\mathfrak{m}$ is Eisenstein, then $\overline{\rho}_{\mathfrak{m}}$ is reducible.

The converse is true as well (H. Yoo). Qualitatively, this means that a mod p cuspidal eigenform whose qth coefficient is $1 + q$ for all but finitely many primes q is congruent to a genuine eigenform from the space of Eisenstein series.

Eisenstein eigenforms

The space E, which has dimension $2^\nu - 1$, is spanned by eigenforms that arise by "level raising" from the weight 2 level 1 Eisenstein series

$$e = -\frac{1}{24} + \sum_{n=1}^{\infty} \Big(\sum_{d|n} d\Big) q^n.$$

The dimension is $2^\nu - 1$, rather than 2^ν, because e doesn't actually exist.

Eisenstein Hecke algebra

The ring $\mathbf{T}_E$ is generated over $\mathbf{Z}$ by the ν different operators T_ℓ for ℓ prime dividing N. It is usual to write U_ℓ for T_ℓ.

More precisely, $\mathbf{T}_E$ is the quotient of the polynomial ring $\mathbf{Z}[\ldots, U_\ell, \ldots; \ell|N]$ by the relations

- $(U_\ell - 1)(U_\ell - \ell)$ for each $\ell|N$;
- $\displaystyle\prod_{\ell|N}(U_\ell - 1)$.

The proof is that there is a natural map from the quotient to $\mathbf{T}_E$ (given by $U_\ell \mapsto U_\ell$) and that both $\mathbf{Z}$-algebras are free of rank $2^\nu - 1$.

The full Hecke algebra

The $\mathbf{Q}$-algebra $\mathbf{T} \otimes \mathbf{Q}$ is semisimple (i.e., isomorphic to a product of number fields) because of a result of Coleman–Edixhoven (“On the semi-simplicity of the U_p-operator on modular forms”).

If p is a prime number, the p-adic completion $\mathbf{T} \otimes \mathbf{Z}_p$ of $\mathbf{T}$ is an order in a product of p-adic number fields. Also,

$$\mathbf{T} \otimes \mathbf{Z}_p = \prod_{\mathfrak{m} | p} \mathbf{T}_{\mathfrak{m}},$$

where the product is taken over the set of maximal ideals of $\mathbf{T}$ with residue characteristic p.

A hint at applications

Geometrically, S corresponds to the modular curve $X_0(N)$ and the Jacobian $J_0(N)$ of $X_0(N)$. The Hecke operators T_n act on the curve as correspondences and on the Jacobian as endomorphisms. The formal polynomial ring $\mathbf{Z}[\ldots, T_n, \ldots]$ acts on $J_0(N)$ through its quotient $\mathbf{T}_S$, which acts faithfully on $J_0(N)$:

$$\mathbf{T}_S \subseteq \operatorname{End} J_0(N).$$

In appropriate contexts it is an excellent idea to replace $J_0(N)$ by the generalized Jacobian $\tilde{J}_0(N)$ corresponding to M. We will not do that tonight/this morning.

Stein's conjecture

The Jacobian $J_0(N)$ has an interesting finite subgroup $C \subset J_0(N)$, its cuspidal subgroup. This group is easily computable (Sage!) and well understood (various authors, including H. Yoo). All of its points are *rational* because N is square free.

After doing extensive calculations, W. Stein conjectured

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

This conjecture is largely proved (M. Ohta), but the theme of the proof has been to compute both objects and to observe their equality.

Generalized Ogg's conjecture

If N is positive (but not necessarily square free), one can ask whether or not the inclusion

$$C(\mathbf{Q}) \subseteq J_0(N)(\mathbf{Q})_{\mathrm{tors}}$$

is an equality. See H. Yoo's talk (72 hours from now) for a strong result in this direction.

If N is a prime, the equality

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

was conjectured by A. Ogg and then proved by B. Mazur in the 1970s. Thus Stein's conjecture is a generalization of a conjecture of Ogg.

While preparing these slides this morning, I baked a bread

A variant of Stein's conjecture

Returning to the case where N is square free, we regard $J_0(N)(\mathbf{Q})_{\text{tors}}$ as an unknown finite $\mathbf{T}_S$-module whose structure is to be explored. The following conjecture is close in substance to Stein's conjecture.

Conjecture

The Hecke module $J_0(N)(\mathbf{Q})_{\text{tors}}$ is Eisenstein, i.e., annihilated by I (or by I_S—it's the same).

Stein's conjecture (= theorem of Ohta) implies this new conjecture because C is Eisenstein. (Everything coming from the cusps is Eisenstein.) Also, Stein's conjecture would almost certainly follow from the displayed conjectural statement because of our extensive knowledge of $J_0(N)(\mathbf{Q})_{\text{tors}}[I_S]$ (Ren, Yoo, Jordan–R–Scholl).

For each prime $q \nmid N$, let

$$\eta_q = 1 + q - T_q \in \mathbf{T}.$$

These "Eichler–Shimura" elements appear prominently in B. Mazur's "Eisenstein ideal" article. For each q, $T_q = 1 + q$ in $\mathbf{T}_E$, and thus $T_q \in I$ for all q.

Because of the Eichler–Shimura relation

$$T_q = \mathrm{Frob}_q + q \, \mathrm{Frob}_q^{-1},$$

$J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ is annihilated by η_q for all q prime to the order of $J_0(N)(\mathbf{Q})_{\mathrm{tors}}$ (and to N). This suggests the question:

Is I generated by almost all of the η_q?

Theorem of Preston Wake

Let Σ be a finite set of primes that includes the set of primes dividing N. Let $J \subseteq \mathbf{T}$ be the ideal generated by the η_q with $q \notin \Sigma$.

Theorem (P. Wake)

The inclusion $J \subseteq I$ is an equality locally at all prime numbers not dividing $2N$.

The theorem states that $J\mathbf{T}_\mathfrak{m} = I\mathbf{T}_\mathfrak{m}$ for all $\mathfrak{m}$ prime to $2N$. For $\mathfrak{m}$ not containing J, $J\mathbf{T}_\mathfrak{m} = \mathbf{T}_\mathfrak{m}$ and the theorem is true. We focus on the case where $J \subseteq \mathfrak{m}$. By the Čebotarev density theorem and the Brauer–Nesbitt theorem,

$$J \subseteq \mathfrak{m} \iff \overline{\rho}_\mathfrak{m} \text{ is reducible} \iff \mathfrak{m} \text{ is Eisenstein.}$$

The theorem is about Eisenstein primes.

A cartoon version of the proof

Because $J \subseteq I$, there is a homomorphism $\alpha : \mathbf{T}/J \to \mathbf{T}_E$ with kernel I/J. The goal is to define a section $s : \mathbf{T}_E \to \mathbf{T}/J$ such that $\alpha \circ s$ is the identity on $\mathbf{T}_E$ and to prove that s is *surjective*.

The surjectivity of s and the injectivity of $\alpha \circ s$ implies that α is injective and thus that $I = J$.

We can view $\mathbf{T}_E$ as the polynomial ring $\mathbf{Z}[\ldots, T_n, \ldots]/(\text{lots of relations})$. The aim is to map T_n in the polynomial ring to $T_n \in \mathbf{T}$ and to show that the relations defining $\mathbf{T}_E$ land in J.

The case of prime level

If N is prime, we secretly know that $\mathbf{T}_E = \mathbf{Z}$. We can map $\mathbf{Z}$ to $\mathbf{T}/J$ with no problem but then have to prove that the map is surjective. Why is T_N in the image? What about T_q for q a prime different from N that happens not to be in Σ?

Alternative point of view: think of $\mathbf{T}_E$ as $\mathbf{Z}[\dots T_q \dots ; T_N]$ mod the relations $T_q - q - 1$ and $T_N - 1$. There's no problem in mapping the polynomial ring to $\mathbf{T}$, but we have to know that J contains $T_N - 1$ as well as the $T_q - q - 1$ for *all* primes $q \neq N$.

This is clearly a job for the Čebotarev density theorem, but then we need a Galois representation and thus need to work p-adically for some prime p. Because $\mathbf{T} \otimes \mathbf{Z}_p$ is a product of rings $\mathbf{T}_{\mathfrak{m}}$, it's OK to work $\mathfrak{m}$-adically. As indicated before, it suffices to treat the Eisenstein $\mathfrak{m}$; that's what we'll do.

We've completed at $\mathfrak{m}$

Now $\mathbf{T}$ is what $\mathbf{T}_{\mathfrak{m}}$ used to be, J is what $J\mathbf{T}_m$ used to be, and so on. Recall that $\mathfrak{m}$ is Eisenstein by our hypothesis.

Is it also cuspidal?

If not, then $J = I = (0)$, $\mathbf{T} = \mathbf{T}_E$, α is the identity map and s is easy to define (as the identity map).

Thus we should imagine that $\mathfrak{m}$ is a prime of fusion—both cuspidal and Eisenstein. The ring $\mathbf{T}$ is then of finite index in a product $(\prod_f \mathcal{O}_f) \times \mathbf{T}_E$, where the $\mathcal{O}_f$ are integer rings in finite extensions of $\mathbf{Q}_p$ and the $\mathbf{Z}_p$-rank of $\mathbf{T}_E$ depends on the number of $\ell | N$ that are congruent to 1 mod p.

For example, if all ℓ are 1 mod p, then $\mathbf{T}_E$ has full rank $2^\nu - 1$.

The Galois representation ρ

There is a natural Galois representation

$$\rho = \rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{T} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p)$$

with determinant equal to the p-adic cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{Z}_p^*$ for which

$$\mathrm{trace}(\rho(\mathrm{Frob}_q)) = T_q \in \mathbf{T}$$

for almost all q. By Čebotarev, trace(ρ) takes values in $\mathbf{T}$; and $J \subseteq \mathbf{T}$ is the ideal generated by the image of the function

$$\mathrm{trace}(\rho) - \chi - 1 : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{T}.$$

Using this characterization of J, it is possible to show that J contains all of the relations that define $\mathbf{T}_E$ as a quotient of the polynomial ring generated by formal Hecke operators.

An illustrative example

Suppose that ℓ divides N. We are taking $p \neq \ell$ because p is prime to N. Then one checks, component by component, that

$$U_\ell^2 - \text{trace}\,\rho(\text{Frob}_\ell)U_\ell + \ell = 0.$$

The representation ρ could well be ramified at ℓ, but the semisimplication of its restriction to a decomposition group for ℓ in $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is unramified. In the expression "trace $\rho(\text{Frob}_\ell)$," replace ρ by the semisimplifcation before taking the trace. Modulo J,

$$\text{trace}\,\rho(\text{Frob}_\ell) \equiv 1 + \chi(\text{Frob}_\ell) = 1 + \ell,$$

so that

$$U_\ell^2 - (1+\ell)U_\ell + \ell \in J;$$

the expression in question is $(U_\ell - \ell)(U_\ell - 1)$.

A second illustrative example

With J the ideal generated by the image of $\operatorname{trace}(\rho) - \chi - 1 : \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{T}$, we wish to show that $T_p - p - 1$ belongs to J. Because $\overline{\rho}_{\mathfrak{m}}$ is the direct sum of the trivial and the mod p cyclotomic character, ρ is ordinary in the sense that T_p is invertible mod $\mathfrak{m}$. The restriction of ρ to a decomposition group G_p for p in $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ has semisimplification of the form $\epsilon \oplus \chi\epsilon^{-1}$, where ϵ is unramified.

Let $u = \epsilon(\mathrm{Frob}_p)$. Then $u^2 - T_p u + p = 0$, giving

$$T_p = u + pu^{-1}, \quad T_p - p - 1 = (u-1) + p(u^{-1} - 1).$$

A second illustrative example

What we need is

$$(u-1)+p(u^{-1}-1) \overset{?}{\in} J.$$

What we know is that J contains the image of trace $\rho - \chi - 1 = (\epsilon - 1) + \chi(\epsilon^{-1} - 1)$. We consider elements of the decomposition group that map to Frob_p mod inertia. Because χ has full image on inertia, the ideal J contains all expressions

$$(u-1)+a(u^{-1}-1), \quad a \in \mathbf{Z}_p^*.$$

By subtracting the expressions with $a = 1$ and $a = 1 + p$, we get $p(u^{-1} - 1) \in J$. By adding the expressions with $a = 1$ and $a = -1$, we get $2(u-1) \in J$. Because 2 is invertible mod p (since $p \neq 2$ by assumption), it follows that $u - 1$ belongs to J.