MAZUR SEMINAR. Talk 10

KRIS KLOSIN

1. Eisenstein quotient

Let N denote an odd prime, $J = J_0(N)_{/\mathbb{Q}}$ the Jacobian of the modular curve $X_0(N) = X_0(N)_{/\mathbb{Q}}$, and $\mathbb{T}$ the Hecke algebra acting on J. We embed $X_0(N) \hookrightarrow J$ by sending the cusp ∞ to 0. By a result of Ribet [3] (cf. Tobias's talk), there is a one-to-one correspondence between the following sets:

1. Isogeny classes of $\mathbb{C}$-simple abelian variety factors of $J_{/\mathbb{C}}$.

2. Isogeny classes of $\mathbb{Q}$-simple abelian variety factors of $J_{/\mathbb{Q}}$.

3. Fields k_α occuring in the product decomposition $\mathbb{T} \otimes \mathbb{Q} = \prod k_\alpha$ (cf. Tobias' talk).

4. Irreducible components of Spec$\mathbb{T}$.

To any ideal $\mathfrak{a} \subset \mathbb{T}$ with finite index we associate an abelian variety $J^{\mathfrak{a}}$ over $\mathbb{Q}$ that is the optimal quotient of J whose $\mathbb{C}$-simple factors are in one-to-one correspondence with those irreducible components of Spec $\mathbb{T}$ that meet the zero-dimensional support of the ideal $\mathfrak{a}$.

Lemma 1.1 Let $\gamma_{\mathfrak{a}} \subset \mathbb{T}$ be the kernel of $\mathbb{T} \to \mathbb{T}_{\mathfrak{a}} = \text{proj.lim}\mathbb{T}/\mathfrak{a}^m$. Let $\gamma_{\mathfrak{a}} J \subset J$ be the subabelian variety (defined over $\mathbb{Q}$) generated by the images $\alpha \cdot J$ for $\alpha \in \gamma_{\mathfrak{a}}$. Then $J^{\mathfrak{a}}$ is the quotient abelian variety:

$$0 \to \gamma_{\mathfrak{a}} J \to J \to J^{\mathfrak{a}} \to 0.$$

Proof. We will use the fact that $\gamma_{\mathfrak{a}} = \cap \eta$, where the intersection is over all the minimal primes η of $\mathbb{T}$ that meet the support of $\mathbb{T}/\mathfrak{a}$. (We postpone the proof of this identity to the Appendix). By exercise II.5.6.b in Hartshorne, Supp $\mathbb{T}/\mathfrak{a} = \mathbb{V}(\mathfrak{a})$. As J is isogenous to $\prod A_\alpha$, with A_α $\mathbb{Q}$-simple, to determine which factors appear in the decomposition of $\gamma_{\mathfrak{a}}$, we will consider the tangent space $T_0 \gamma_{\mathfrak{a}} J = \gamma_{\mathfrak{a}} T_0 J \subset T_0 J$ (the first equality was proven in Trevor's talk, cf. Corollary 1.2). As $T_0 J$ is a $\mathbb{Q}$-vector space $\gamma_{\mathfrak{a}} T_0 J = (\gamma_{\mathfrak{a}} \otimes \mathbb{Q}) T_0 J$. Since $\mathbb{T} = \prod k_\alpha$, we have $\eta \otimes \mathbb{Q} = \prod_{\alpha \neq \alpha_0} k_\alpha$, with α_0 corresponding to η. We conclude that the $\mathbb{Q}$-simple factors of $J/\gamma_{\mathfrak{a}} J$ correspond exactly to those minimal primes η of $\mathbb{T}$ which meet Supp $\mathbb{T}/\mathfrak{a}$. □

Now, note that $\mathfrak{a}$ is a proper ideal of $\mathbb{T}$ if and only if there exists a prime ideal

$\mathfrak{p} \subset \mathbb{T}$, such that $\mathfrak{a} \subset \mathfrak{p}$. Let $\eta \subset \mathfrak{p}$ be a minimal prime. Then $\mathfrak{p} \in \mathbb{V}(\mathfrak{a}) \cap \mathbb{V}(\eta)$, hence $\mathbb{V}(\mathfrak{a}) \cap \mathbb{V}(\eta) \neq \emptyset$ if anf only if $\mathfrak{p}$ is proper. Thus $\gamma_{\mathfrak{a}}$ is proper if and only if $\mathfrak{a}$ is proper. Hence by Lemma 1.1 we conclude that $J^{\mathfrak{a}} \neq 0$ if and only if $\mathfrak{a} \subset \mathbb{T}$ is proper.

Definition 1.2 The *Eisenstein ideal* $\mathfrak{I} \subset \mathbb{T}$ is the ideal generated by the elements $1 + l - T_l$ for all primes $l \neq N$ and by $1 + w$. (for definitions of T_l and w see James' talk)

Proposition 1.3 If the genus of $X_0(N)$ is nonzero then the Eisenstein ideal $\mathfrak{I}$ is proper and of finite index in $\mathbb{T}$.

Proof. It is a known fact that the genus of $X_0(N)$ is nonzero if and only if $n := \text{num}(\frac{N-1}{12}) > 1$. For every positive integer r, we denote by $\sigma(r)$ the sum of all positive divisors of r which are prime to N, and by δ the formal power series $\sum_{r=1}^{\infty} \sigma(r) q^r$. We will show that $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}/m\mathbb{Z}$ for some $m > 1$. The natural homomorphism $\mathbb{Z} \to \mathbb{T}/\mathfrak{I}$ is surjective, as modulo the Eisenstein ideal all the Hecke operators are congruent to integers. First suppose that $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}$. Then the composite $\lambda : \mathbb{T} \to \mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}$ is a nonzero homomorphism, and it remains so after extending scalars to $\mathbb{C}$. Thus there exists a normalized eigenform f of level N and weight 2, with $T_r f = \lambda(T_r) f$. We have $\lambda(T_r) = \sigma(r)$, hence the Fourier expansion of f at infinity agrees with δ, but it can be shown that δ is not a q-expansion of a modular form over $\mathbb{C}$ of level N and weight 2. Thus $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}/m$ for some positive integer m.
In his IHES paper Mazur proves that there exists a normalized eigenform f' with integer Fourier coefficients at infinity which are congruent to coeffiecients of δ mod n. Hence there is a nonzero homomorphism $\mathbb{T} \to \mathbb{Z}$ (given by the eigenvalues of f') such that the composite $\lambda' : \mathbb{T} \to \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ is given by $T_r \mapsto \sigma(r)$. Since $\sigma(p) = p + 1$ for a prime $p \neq N$, Dirichlet's Theorem on primes in arithmetic progression guarantrees that λ' is nontrivial if $n > 1$, i.e. it surjects onto some nonzero subgroup $\mathbb{Z}/n'\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$. However λ' kills $\mathfrak{I}$, hence $\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{T}/\mathfrak{I} \to \mathbb{Z}/n'\mathbb{Z}$ is surjective, i.e. $n' \mid m$. This implies that $\mathfrak{I}$ is proper. $\square$

Remark Working somewhat harder, one can actaully prove that $\mathbb{T}/\mathfrak{I} \simeq \mathbb{Z}/n\mathbb{Z}$ (cf. Proposition 9.7, page 96 in Mazur's IHES paper), but we will not need this fact.

Definition 1.4 The abelian variety $J^{\mathfrak{I}}$ which we will denote by $\tilde{J}$ is called the *Eisenstein quotient.*

Note that Lemma 1.1 and Proposition 1.3 ensure that $\tilde{J}$ is nonzero.

2. Mordell-Weil group of $\tilde{J}$.

Let C denote the subgroup of $J(\mathbb{Q})$ generated by the linear equivalence class of the divisor $c := (0) - (\infty)$.

Lemma 2.1 The group C is finite.

Proof. It can be checked that $T_l c = (1+l)c$ for all $l \neq N$ and that w intechanges the two cusps (cf. James's talk "cuspology"). Hence $\mathfrak{I}$ kills c, so in view of Proposition 1.3, multiplication by $[\mathbb{T} : \mathfrak{I}]$ kills c. □

We now state without proof a theorem of Mazur (Theorem II.3.1 in Mazur's IHES paper) that is the key ingredient in Mazur's proof of the Ogg's conjecture. It allows us to reduce the proof to working with just the elliptic curves with potentially good reduction at all odd primes $\neq N$.

Theorem 2.2 The natural projection $J \to \tilde{J}$ induces an isomorphism of the subgroup C onto the Mordell-Weil group $\tilde{J}(\mathbb{Q})$. In particular $\tilde{J}(\mathbb{Q})$ is finite.

3. Reduction to the case of elliptic curves with potentially good reduction at odd primes $\neq N$

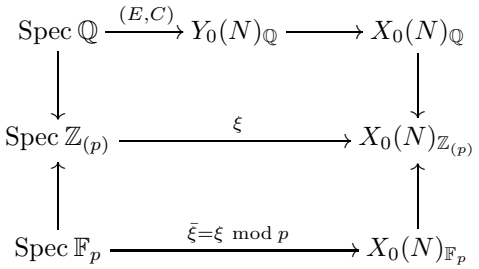
Proposition 3.1 Let $(E_{/\mathbb{Q}}, C)$ denote a pair consisting of an elliptic curve over $\mathbb{Q}$ and a cyclic subgroup C of prime order $N > 2$. The curve E has potentially good reduction at all odd primes $p \neq N$.

Remark In fact E has potentially good reduction at all odd primes (cf. [2] Corollary 4.3). In our proof we will use the following result presented in Trevor's talk, which does not allow us to handle the case $p = N$.

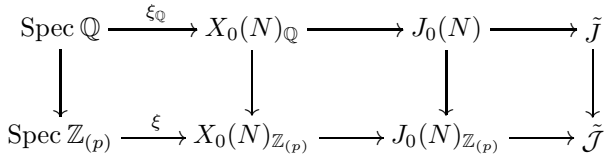
Proposition 3.2 Let $\mathcal{A}$ denote the Neron model over $\mathbb{Z}[1/2N]$ of any nonzero optimal quotient A of J. Define $X_0(N)_{/\mathbb{Q}} \to J \to A$ by sending the cusp ∞ to 0, and let f denote the morphism extending this map over $\operatorname{Spec} \mathbb{Z}[1/2N]$. Then $\infty \in X_0(N)(\mathbb{Z}_{(p)})$ is the only point reducing to $\infty \in X_0(N)(\mathbb{F}_p)$ that also maps to 0 in $\mathcal{A}(\mathbb{Z}_{(p)})$ under f.

Proof of Proposition 3.1. We will take A in the Proposition 3.2 to be $\tilde{J}$, and denote by $\tilde{\mathcal{J}}$ the Neron model of $\tilde{J}$ over $\mathbb{Z}_{(p)}$. Suppose that E has potentially

multiplicative reduction. The Neron mapping property yields a morphism ξ that makes the following diagram commute.



We note that the fact that E has potentially multiplicative reduction at p means exactly that the map $\bar{\xi}$ is a cusp of $X_0(N)_{\mathbb{F}_p}$. As was discussed in James's talk, the Atkin-Lehner involution permutes the cusps 0 and ∞, so we can assume without loss of generality that $\bar{\xi}$ hits ∞ (i.e. if necessary we replace (E, C) with $(E/C, E[N]/C)$). Consider the following commutative diagram:



where $J_0(N)_{\mathbb{Z}_{(p)}}$ denotes the Neron model of $J_0(N)$. Since $\infty_{\mathbb{Z}_{(p)}}$ maps to 0 under $f : X_0(N)_{\mathbb{Z}_{(p)}} \to \tilde{\mathcal{J}}$ and both $\xi_{\mathbb{Z}_{(p)}}$ and $\infty_{\mathbb{Z}_{(p)}}$ reduce to $\infty_{/\mathbb{F}_p}$, they both map to 0 mod p.

By theorem 2.2, we have $\tilde{\mathcal{J}}(\mathbb{Z}_{(p)}) = \tilde{J}(\mathbb{Q}) = \tilde{J}(\mathbb{Q})_{\text{tors}}$. Suppose $\tilde{J}(\mathbb{Q})_{\text{tors}}$ contains a point of order $m \neq 1$, i.e. there is an inclusion $i : \mathbb{Z}/m\mathbb{Z} \hookrightarrow \tilde{J}[m](\mathbb{Q})$. Let $R = \mathbb{Z}_{(p)}$, $K = \mathbb{Q}$. Then $G := \tilde{\mathcal{J}}[m]_{/R}$ is a finite flat group scheme (cf. Tong's talk), hence proper. Thus $G_K(K) = G(R)$. Put $H = \underline{\mathbb{Z}/m\mathbb{Z}}_{/R}$ and consider the closed immersion $H_K \to G_K$ coming from the inclusion i. Define a morphism $H \to G$ by sending 1 to the image of the $1 \in H(K)$ under the composite $H(K) \to G(K) = G(R)$.

We will now use the following fact discussed in Tong's and Eiji's talks (which is Mazur's Proposition 1.1)

Proposition 3.3 Suppose $p \neq 2$ and let $f : H \to G$ be a morphism of finite flat group schemes over a discrete valuation ring R with mixed characteristic $(0, p)$. Let K denote the fraction field of R. If $f_K : H_K \to G_K$ is a closed immersion, then f is a closed immersion.

By proposition 3.3 we conclude that $H \to G$ is a closed immersion, so $H_{\mathbb{F}_p} \to G_{\mathbb{F}_p}$ is as well. Thus, $\mathbb{Z}/m\mathbb{Z}$ injects into $\tilde{J}[n](\mathbb{F}_p)$, so $\tilde{\mathcal{J}}(\mathbb{Z}_{(p)})$ *injects* into $\tilde{\mathcal{J}}(\mathbb{F}_p)$. Hence $\xi_{\mathbb{Z}_{(p)}}$ also maps to 0 in $\tilde{\mathcal{J}}$. Thus by Proposition 3.2 $\xi_{\mathbb{Z}_{(p)}} = \infty_{\mathbb{Z}_{(p)}}$, hence also $\xi_{\mathbb{Q}} = \infty_{\mathbb{Q}}$, contradicting the fact that $\xi_{\mathbb{Q}}$ factors through $Y_0(N)$. $\square$

4. Ogg's conjecture

We are now ready to prove Ogg's conjecture. In view of the talks by Brian, Bryden, and Sreekar, all we need to establish is the following claim:

Theorem 4.1 Let N be 11 or a prime greater than 16. Then there are no elliptic curves over $\mathbb{Q}$ with a torsion subgroup of order divisible by N.

Proof. Suppose $E(\mathbb{Q})$ possesses a cyclic subgroup of order N for N as in the statement of the theorem. By Proposition 3.1 E has potentially good reduction at 3. We will show that $N \leq 7$ and thus obtain a contradiction. We first treat the case when E has good reduction at 3. In this case its Neron model $\mathcal{E}$ over $\mathbb{Z}_{(3)}$ is an elliptic curve and thus the map $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E(\mathbb{Q})_{\text{tors}} \to \mathcal{E}_{/\mathbb{F}_3}(\mathbb{F}_3)$ is injective. By Hasse-Weil $|\mathcal{E}_{/\mathbb{F}_3}(\mathbb{F}_3)| \leq 7$, so we are done.
Now assume that E has additive reduction at 3, and let $\mathcal{E}$ denote its Neron model over $\mathbb{Z}_{(3)}$. We have the following exact sequence:

$$0 \to \mathcal{E}^0_{/\mathbb{F}_3} \to \mathcal{E}_{/\mathbb{F}_3} \to \pi_0(\mathcal{E}_{/\mathbb{F}_3}) \to 0,$$

where the first term denotes the identity component of the middle term and the last term is the finite etale component group (cf. [4], proposition 2.18, p. 495). By Corollary 7.2 in [5] and the discussion that follows after it, we deduce that since $\mathbb{F}_3$ is perfect, the first term is $\mathbb{G}_a$. To derive that $N \leq 7$, we will again use Proposition 3.3 in the same way as in the proof of Proposition 3.1. Let $R = \mathbb{Z}_{(3)}$, $K = \mathbb{Q}$. Then $G = \mathcal{E}[N]$ is a finite flat group scheme over $\mathbb{Z}_{(3)}$ (cf. Tong's talk). Take H to be $\underline{\mathbb{Z}/N\mathbb{Z}}_{/\mathbb{Z}_{(3)}}$ and consider the closed immersion $G_K \to H_K$ coming from the inclusion $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E[N](\mathbb{Q})$. This as before gives rise to the morphism $H \to G$ defined by sending 1 to the image of 1 under the composite $H(K) \to G(K) = G(R)$. (The last equality follows from the properness of G over $\mathbb{Z}_{(3)}$). Then by Proposition 3.3 we conclude that $H \to G$ is a closed immersion, so $H_{\mathbb{F}_3} \to G_{\mathbb{F}_3}$ is also. Hence $\mathbb{Z}/N\mathbb{Z}$ injects into $\mathcal{E}(\mathbb{F}_3)$. Now invoking the fact that $|\pi_0(\mathcal{E}_{\mathbb{F}_3})| \leq 4$ ([6], ch. "Neron models"), we conclude that the image of $\mathbb{Z}/N\mathbb{Z}$ in $\pi_0(\mathcal{E}_{\mathbb{F}_3}(\mathbb{F}_3))$ is zero, so $\mathcal{E}^0(\mathbb{F}_3)$ contains an element of order N. However, $\mathcal{E}^0(\mathbb{F}_3) \simeq \mathbb{G}_a(\mathbb{F}_3) = \mathbb{F}_3$, so $N \leq 3$. $\square$

References

[1] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES 47, 1977.
[2] B. Mazur, *Rational Isogenies of Prime Degree*, Invent. Math. 44, 129-162, 1978.
[3] K. Ribet, *Endomorphism of semi-stable abelian varieties over number fields*, Ann. of Math., 101, 555-562, 1975.
[4] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford, 2002.
[5] B. Conrad, *Minimal models for elliptic curves*, unpublished manuscript, 2003.
[6] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts Math., 151, Springer, New York-Heidelberg-Berlin, 1979.