ALVARO GONZALEZ HERNANDEZ
University of Warwick

The Eisenstein ideal

Study group on Mazur's Torsion Theorem

Outline of the talk

1. Recap of where we are in the study group and what we want to prove.
2. Tackle the easier case of the proof.
3. Discuss the Eisenstein ideal and the Eisenstein quotient.
4. Start the proof of the general case.

Gotthold Eisenstein (1823-1852)

A quick recap

The key result in the proof of Mazur's theorem

WARWICK
THE UNIVERSITY OF WARWICK

Theorem (A)

Let $N > 7$ be a prime number and let $p \neq N$ be a second prime number. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a map $f : X_0(N) \to A$ satisfying the following:

- A has **good reduction** away from N.
- $f(0) \neq f(\infty)$.
- $A(\mathbb{Q})$ has **rank 0**. Difficult to prove in some cases!

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

The key result in the proof of Mazur's theorem

Theorem (B)

Let $N > 7$ be a prime number and let $p \neq N$ be a second prime number. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a map $f : X_0(N) \to A$ satisfying the following:

- A has **good reduction** away from N.
- A has completely **toric reduction** at N.
- The Jordan-Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are 1-dimensional and either **trivial** or **cyclotomic**.
- $f(0) \neq f(\infty)$.

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

⊛ Equivalent to rk $A(\mathbb{Q})=0$

WARWICK
THE UNIVERSITY OF WARWICK

Theorem

Let $N > 7$ be a prime number which is not 13. Then, no elliptic curve defined over $\mathbb{Q}$ has a rational point of order N.

Sketch

We are going to find $p \neq N$ and A satisfying that

- A has good reduction outside of n. ✓
- $f(0) \neq f(\infty)$
- $\operatorname{rk} A(\mathbb{Q}) = 0$ } Need to check
- A has completely toric reduction at N ✓
- Satisfies the JH constituents condition (Need to check)

The idea is $A = J_0(N)/I J_0(N)$ for some $I \subsetneq J_0(N)$

Why $N \neq 13$?

The reason why we exclude $N = 13$ is that $X_0(13)$ has genus 0. Therefore, $J_0(13)$ is trivial and we need to find an alternative way of proving that there is not 13-torsion.

13 is the only problematic prime

$$g(X_0(N)) = \begin{cases} \lfloor \frac{N}{12} \rfloor - 1 & \text{if } N \equiv 1 \bmod 12 \\ \lfloor \frac{N}{12} \rfloor + 1 & \text{if } N \equiv -1 \bmod 12 \end{cases}$$
N prime

Quotients of the Jacobian

Notation

We will say that an abelian variety $A/\mathbb{Q}$ satisfies condition JH(p) if the Jordan-Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are all trivial or cyclotomic. This condition is isogeny invariant.

Up to isogeny, we have a decomposition

$$J_0(N) = \prod A_f$$

N=11 (one of the easier cases)

where the product is over the Galois orbits of normalised weight 2 cuspidal eigenforms.

Easier case ⇒ Let's first assume that each f has rational coefficient field ⇒ A_f are all elliptic curves. In this case, there exists a maximal quotient of $J_0(N)$ satisfying JH(p):

$$J_0(N) = \underbrace{A_{f_1} \times \dots \times A_{f_m}}_{\text{satisfy JH}(p)} \times \underbrace{A_{g_1} \times \dots \times A_{g_s}}_{\text{Do not satisfy JH}(p)}$$

We can take A to be

$A = A_{f_1} \times \dots \times A_{f_m}$ (quotient of $J_0(N)$).

The easier case

Showing that A is the abelian variety we are looking for

1. Show that we can find a $p \nmid N$ such that A is not trivial.

2. Explain rigourously the construction of A and why it satisfies $JH(p)$.

3. Given $\varphi : J_0(N) \to A$, we are going to check that $[0] \neq [\infty]$ in A

$\Rightarrow$ Proof of our Theorem in this easier/simplified case!

Studying the difference of the cusps

a.k.a finding $p \nmid N$ s.t A is not trivial.

WARWICK
THE UNIVERSITY OF WARWICK

Proposition

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

Suppose $[0]-[\infty]=0$. This is equivalent to saying that there exists f in the function field of $X_0(N)$ such that $\mathrm{div}(f)=[0]-[\infty]$.
However, this f would define a morphism $f: X_0(N) \longrightarrow \mathbb{P}^1$ of degree 1, which would imply that $g(X_0(N))=0$. Contradiction!
To see that the order of $[0]-[\infty]$ divides $N-1$, we are going to construct a function g such that $\mathrm{div}(g)=(N-1)[0]-(N-1)[\infty]$.
In order to do so, let us consider $\Delta(z)=4E_4^3+27E_6^2$, the cusp form of weight 12 for $\Gamma(1)$ on the upper half plane.

$\Delta(z)$ satisfies the following two conditions: $\begin{cases} \Delta(z) \neq 0 & \text{for } z \in \mathcal{H} \\ \text{its } q\text{-expansion is } q + \cdots \end{cases}$

$\left(\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}\right)$

It also happens that $\Delta(z)$ and $\Delta(Nz)$ are both modular forms for $\Gamma_0(N)$ that do not vanish on the upper half plane.

Let us define $g(z) = \dfrac{\Delta(z)}{\Delta(Nz)}$. It is a nowhere vanishing function on the upper half-plane which is invariant under $\Gamma_0(N) \Rightarrow$ descents to a meromorphic function in $X_0(N)$ which is holomorphic and non-vanishing in $Y_0(N)$.

The q-expansion of g is $q^{-(N-1)} + \cdots$ so g has a pole of order $N-1$ at ∞.

Because $\deg(g) = 0$ and the other only possible point where g can have a zero or a pole is 0, we deduce that g has a zero of order $N-1$ at 0 and

$$\operatorname{div}(g) = (N-1)[0] - (N-1)[\infty] \Rightarrow (N-1)([0] - [\infty]) = 0 \qquad \square$$

The difference of the cusps

(Example, order of $[0]-[\infty]$ in $J_0(11)$ is 5)

$X_0(11)$ has MW group $\mathbb{Z}/5\mathbb{Z}$

Remark

As a matter of fact, the exact order of $[0]-[\infty]$ is $(N-1)/\gcd(N-1, 12)$ (*Ogg*).

Remark

Mazur also proved that $[0]-[\infty]$ generates the entire torsion subgroup of the Mordell-Weil group of $J_0(N)$.

Why does this imply that there is a $p \neq N$ with A non-trivial?

Pick a p dividing $N-1$. Then, from what we have seen, there exists a p-torsion point in $J_0(N)(\mathbb{Q})$ (a multiple of $[0]-[\infty]$) This shows that $J_0(N)[p]$ has a copy of the trivial representation in it. This must come from one of the $A_f \leq J_0(N)$ and this A_f satisfies $JH(p)$

A rigorous way of defining A

Given an eigenform f, let $\mathfrak{p}_f$ be the kernel of the homomorphism $\mathbb{T} \to \mathbb{Z}$ giving the eigenvalues of f.

Then, by definition,

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

Let S be the set of those f for which A_f satisfies $\mathrm{JH}(p)$ and let

↳ A bit vague... how can we understand these?

$$I = \bigcap_{f \in S} \mathfrak{p}_f.$$

If we define $A = J_0(N)/IJ_0(N)$, we can deduce that, up to isogeny,

$$A = \prod_{f \in S} A_f$$

Lemma

$f \in S$ if and only if $a_\ell(f) - (\ell+1)$ is divisible by p for all ℓ.

$\Rightarrow$ Suppose $f \in S \Rightarrow A_f$ satisfies $JH(p)$. Then, the semisimplification of $A_f[p]$ is isomorphic to the direct sum of trivial + cyclotomic, 2-dimensional representation with cyclotomic determinant. It follows that for all ℓ, $tr(F_\ell \mid A_f[p]) = \ell + 1$, but we also know that $a_\ell(f) \equiv tr(F_\ell \mid A_f[p]) \bmod p$

$\Leftarrow$ If for all ℓ, $a_\ell(f) \equiv \ell + 1 \bmod p$, we get that $tr(F_\ell \mid A_f[p]) = \ell + 1$

$\Rightarrow \quad char(A_f[p]) = char(\text{trivial}) \oplus char(\text{cyclotomic})$

Group Theory magic

$\Rightarrow$ The semisimplification of $A_f[p]$ is isomorphic to trivial + cyclot.

$\Rightarrow A_f$ satisfies $JH(p) \Rightarrow f \in S$ $\square$

A neat observation

WARWICK
THE UNIVERSITY OF WARWICK

Remark

The Eisenstein series of weight 2 satisfies that $T_\ell(E_2) = (\ell+1)E_2$, so another way of rephrasing the condition is saying that A_f satisfies $JH(p)$ if and only if the Fourier coefficients of f are congruent modulo p to those of E_2.

Connection → The elements $\{T_\ell - (\ell+1)\}_{\ell \text{ prime}}$ in $\mathbb{T}$, which all satisfy that $T_\ell - (\ell+1)(E_2) = 0$ have connections with the study of quotients of $J_0(N)$ and with the p satisfying $JH(p)$.

Mazur realised this was the case and tried to use this idea by studying an ideal in $\mathbb{T}$ formed by the operators that annihilate the Eisenstein series, the Eisenstein ideal.

The Eisenstein ideal

Motivation

In order to define this ideal, we can start by considering the ideal generated by the $T_\ell - (\ell+1)$ in $\mathbb{T}$, which we know annihilate E_2.

This was not enough for the ideal to have nice properties so he added the element $w+1$ where w is the operator in $\mathbb{T}$ associated to the Fricke involution
$$\begin{aligned} X_0(N) &\longrightarrow X_0(N) \\ \tau &\longmapsto -1/N\tau \end{aligned}$$

The ideal generated by the $T_\ell - (\ell+1)$ and $w+1$ was what he called the Eisenstein ideal.

In the case where $X_0(N)$ has genus $g \geq 1$, we know that the order of $[0]-[\infty]$ gives us a special prime p, and there is a reformulation

The p-Eisenstein ideal

We define the p-Eisenstein ideal $\mathfrak{a}$ to be the ideal of $\mathbb{T}$ generated by p and the $T_\ell - (\ell + 1)$.

Lemma

We have that $\mathbb{T}/\mathfrak{a} = \mathbb{F}_p$ and therefore $\mathfrak{a}$ is maximal.

By assumption, there exists an $\mathfrak{f} \in S$, which we know it satisfies $a_\ell(\mathfrak{f}) \equiv \ell+1 \bmod p$

We can define

$$\mathbb{T} \longrightarrow \mathbb{T}/\mathfrak{f}_p \cong \mathbb{Z}$$
$$T_\ell \longmapsto a_\ell(\mathfrak{f})$$
$$T_\ell - (\ell+1) \longmapsto a_\ell(\mathfrak{f}) - (\ell+1)$$

$\hookrightarrow$ divisible by p

It is clear that the image of $\mathfrak{a}$ is inside of $p\mathbb{Z}$, so it is not the unit ideal.

This implies that $\mathbb{T}/\mathfrak{a} = \mathbb{F}_p$ since the quotient is non-trivial and every Hecke operator is identified with an integer $\square$

Relation with S

Lemma

Let S be the set of those f for which A_f satisfies $\mathrm{JH}(p)$. The following are equivalent:

1. $f \in S$.
2. The image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{p}_f$ is not (1).
3. $\mathfrak{p}_f \subset \mathfrak{a}$.

$\boxed{1 \Leftrightarrow 2}$ The image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{p}_f \cong \mathbb{Z}$ is the ideal generated by $\{a_\ell(f) - (\ell+1)\}_{\ell \text{ prime}}$ and p. This ideal is not (1) $\Leftrightarrow$ $p \mid a_\ell(f) - (\ell+1)$

$\Leftrightarrow f \in S$. $\square$

$\boxed{3 \Leftrightarrow 2}$ Because $\mathfrak{a}$ is maximal ideal, $\mathfrak{p} \not\subset \mathfrak{a} \Leftrightarrow \mathfrak{p} + \mathfrak{a} = (1)$

$\Leftrightarrow$ Image of $\mathfrak{a}$ in $\mathbb{T}/\mathfrak{p}$ is (1)

$\square$

We have stablished a connection between $\mathfrak{p} \in S$ and $\mathfrak{a}$.
Let's now see how this allows us to rephrase the construction of A.

$$A = J_0(N) / I J_0(N) \quad \text{with } I = \bigcap_{\mathfrak{p} \in S} \mathfrak{p}$$

Corollary

I is the intersection of the minimal primes $\mathfrak{p}$ of $\mathbb{T}$ which are contained in $\mathfrak{a}$.

As we have seen $I = \bigcap_{f \in S} \mathfrak{p}_f$. The minimal primes of $\mathbb{T}$ are exactly the $\mathfrak{p}_f$. From the previous lemma:

$$I = \bigcap_{\mathfrak{p}_f \subseteq \mathfrak{a}} \mathfrak{p}_f \qquad \square$$

We have therefore found A satisfying $JH(\varphi)$

We need to prove two lemmas in order to show that $[0] \neq [\infty]$ in A.

1- We are going to show that the points in the $\mathfrak{a}^n$-torsion of $J_0(N)$ correspond to $\mathfrak{a}^n$-torsion points in A.

2- There is a multiple of $[0]-[\infty]$ in this $\mathfrak{a}^n$-torsion which we will prove by checking that

$$T_\ell([0]-[\infty]) = (\ell+1)([0]-[\infty])$$

Decomposition of $\mathbb{T}$-modules

Suppose X is a $\mathbb{T}$-module in which all elements are killed by a power of p. Then the action of $\mathbb{T}$ extends to one of the p-adic completion

$$\mathbb{T}_p = \varprojlim \mathbb{T}/p^n\mathbb{T}.$$

Since this is a complete semi-local ring, it is a product of local rings, the factors corresponding to the maximal ideals. In particular, the localization $\mathbb{T}_{\mathfrak{a}}$ is a direct factor of $\mathbb{T}_p$. It follows that X decomposes as $X_{\mathfrak{a}} \oplus X'$, where $\mathbb{T}_{\mathfrak{a}}$ acts by zero on X'.
We can identify $X_{\mathfrak{a}}$ with

$$X[\mathfrak{a}^\infty] = \bigcup_{n\geq 0} X[\mathfrak{a}^n],$$

where $X[\mathfrak{a}^n]$ is the $\mathfrak{a}^n$-torsion in X.

Proof of the first lemma

Lemma 1

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

Let $X = J_0(N)[p^\infty]$ and $Y = A[p^\infty]$. The surjection between $J_0(N) \longrightarrow A$ induces a surjection between their p-divisible groups $X \to Y$, whose kernel is $X \cap I J_0(N)$. This is precisely IX as, given $t_1, \ldots, t_n$ a set of generators of I, we can consider a map

$$\begin{aligned} J_0(N)^n &\longrightarrow J_0(N) \\ (x_1, \ldots, x_n) &\longmapsto \sum x_i t_i \end{aligned}$$

whose image is $I J_0(N)$, and any p-power torsion point comes from one of the source.

We therefore have an exact sequence

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

By localising at $\mathfrak{a}$ (doing this is an exact operator), we get

$$0 \longrightarrow I_{\mathfrak{a}} X_{\mathfrak{a}} \longrightarrow X_{\mathfrak{a}} \rightarrow Y_{\mathfrak{a}} \rightarrow 0$$

where $X_{\mathfrak{a}} = J_0(N)[\mathfrak{a}^\infty]$ and $Y_{\mathfrak{a}} = A[\mathfrak{a}^\infty]$.

Proving that $X_{\mathfrak{a}} \cong Y_{\mathfrak{a}}$ therefore would follow from proving that $I_{\mathfrak{a}} = 0$, which is true, as we will see.

$\square$

Characterisation of I in terms of $\mathfrak{a}$

Proposition

For our ideals $\mathfrak{a}$ and I we have that $I_{\mathfrak{a}} = 0$.

$I = \bigcap_{\mathfrak{p}_j \subseteq \mathfrak{a}} \mathfrak{p}_j$, therefore, $I_{\mathfrak{a}}$ is the intersection of the minimal primes of $\mathbb{I}_{\mathfrak{a}}$. From commutative algebra, this implies that $I_{\mathfrak{a}}$ is the nilradical of $\mathbb{I}_{\mathfrak{a}}$ and, as $\mathbb{I}_{\mathfrak{a}}$ is reduced, $I_{\mathfrak{a}} = 0$. $\square$

Action of the Hecke operators

Let $\ell \neq N$ be a prime. Then, we saw that the Hecke operator T_ℓ can be regarded as an endomorphism of $J_0(N)$ in the following way:

Given the Hecke correspondence $f, g : X_0(N\ell) \rightrightarrows X_0(N)$, we can associate to every element in $J_0(N)$ an image by choosing $T_\ell(D)$ to be

$$T_\ell(D) = g_*(f^*(D))$$

Action of the Hecke operator

WARWICK
THE UNIVERSITY OF WARWICK

Proposition

We have $T_\ell([0] - [\infty]) = (\ell + 1)([0] - [\infty])$. $(\ell \nmid N)$

Consider the Hecke correspondence $f, g : X_0(N\ell) \rightrightarrows X_0(N)$. We have:

- The curve $X_0(N\ell)$ has 4 cusps (the product of the cusps of $X_0(N)$ and $X_0(\ell)$). These can be identified with $\{(0,0), (0,\infty), (\infty, 0)$ and $(\infty,\infty)\}$.
- The maps f and g act on the cusps by taking the first coordinate, i.e. $f(x,y) = g(x,y) = x$. The reason is that f and g lift to the identity map and multiplication by ℓ respectively on h^*.

The elements of $\mathbb{P}^1(\mathbb{Q})$ with N in the denominator map to ∞ of $X_0(N)$ while all others map to 0. But ℓ cannot introduce an N in the denominator, so $\begin{matrix}(0,0)\\(0,\infty)\end{matrix} \mapsto 0$ $\begin{matrix}(\infty,0)\\(\infty,\infty)\end{matrix} \mapsto \infty$

- f has ramification index ℓ at $\begin{matrix}(0,0)\\(\infty,0)\end{matrix}$ and index 1 at $\begin{matrix}(\infty,0)\\(\infty,\infty)\end{matrix}$

  g is the opposite.

We therefore get that $f^*([x]) = \ell((x,0)) + [(x,\infty)]$ and $g_*(f^*([x])) = (\ell+1)[x]$. $\square$

The image of $[0]-[\infty]$ in A is not zero

Proposition

We have that $[0] \neq [\infty]$ in A.

Let $P = [0]-[\infty]$, and let Q non zero and in $J_0(N)[p]$.

Then, $T_\ell - (\ell+1)Q = T_\ell - (\ell+1)(qP) = 0 \Rightarrow T_\ell(Q) = (\ell+1)(Q)$

This implies that $Q \in J_0(N)[\mathfrak{a}^\infty] \Rightarrow Q \in A[\mathfrak{a}^\infty]$ non-trivial.

$\square$

The general case

The general case

We had assumed that each f had rational coefficient field, so the A_f were elliptic curves. Given p, the product of the A_f that satisfied $JH(p)$ has been seen to be a maximal quotient of $J_0(N)$ that satisfied the conditions of Theorem B.

In the general case, we have shown that we have a decomposition

$$V_p J_0(N) = \prod_{f,\lambda} V_{f,\lambda}$$

where the product is over pairs (f, λ) consisting of

- A normalised weight 2 eigenform f.
- A place λ of its coefficient field K_f above p.

and $V_{f,\lambda}$ is 2-dimensional Galois representation over $K_{f,\lambda}$.

What will we do?

Ideally, we would like to do with $V_p J_0(N)$ the same as we did with A in the easier case, which is, to find a decomposition of the $V_{p,\lambda}$ where

$T_p A$ = product of the $V_{p,\lambda}$ that reduce modulo p to trivial + cyclotomic

However, this is generally not possible, for instance if there is only one p, and for some λ the representation $V_{p,\lambda}$ has the right form, and for others not.

The Eisenstein ideal and the quotient A

If we choose p to be a prime dividing the order of $[0]-[\infty]$ in $J_0(N)$ we can once define the p-Eisenstein ideal $\mathfrak{a}$ as the ideal of $\mathbb{T}$ generated by p and $T_\ell-(\ell+1)$ for all $\ell \neq N$.

Proposition

We also have that $\mathbb{T}/\mathfrak{a} = \mathbb{F}_p$.

Let I be the intersection of the minimal primes of $\mathbb{T}$ contained in $\mathfrak{a}$, and let $A = J_0(N)/IJ_0(N)$. Then,

Proposition

We have $[0] \neq [\infty]$.

Thank you! Any questions?