Overview talk: Mazur's theorem

Jef Laga

October 8, 2020

Motivation

Let $C/\mathbb{Q}$ be a nice (= smooth, projective, geometrically integral) curve of genus g.

The Big Question

Describe $C(\mathbb{Q})$.

Trichotomy according to $\chi = 2 - 2g$: (assume $C(\mathbb{Q}) \neq \emptyset$)

$$\begin{cases} C \simeq \mathbb{P}^1_{\mathbb{Q}} & \text{if } \chi > 0 \text{ (conics)}, \\ C(\mathbb{Q}) \text{ is a fg abelian group} & \text{if } \chi = 0 \text{ (Mordell-Weil)}, \\ C(\mathbb{Q}) \text{ is finite} & \text{if } \chi < 0 \text{ (Faltings)}. \end{cases}$$

If $E/\mathbb{Q}$ is an elliptic curve, then $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$.

Subquestion

Describe the rank r.

Still very much a mystery!

Subquestion

Describe the torsion part $E(\mathbb{Q})_{tors}$.

Completely solved:

Classification of rational torsion

Theorem (Mazur, 1977)

$E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{with } 1 \leq n \leq 10 \text{ or } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \text{with } n = 2, 4, 6, 8. \end{cases}$$

Moreover, each of these groups occur.

Goal of the reading group

Our true goal will be:

Theorem

*Let $N > 13$ be a **prime** number. Then no elliptic curve $E/\mathbb{Q}$ has a rational N-torsion point.*

Previous theorem then follows from this one + case-by-case analysis.

Plan of the proof

- Step 1: reduce statement to existence of a certain abelian variety having rank zero.
- Step 2: prove a criterion for an abelian variety to have rank zero.
- Step 3: construct this abelian variety using the Eisenstein ideal.

Step 1: Modular curves

Fix a prime $N > 7$. We have algebraic curves $Y_1(N)/\mathbb{Q}$ and $Y_0(N)/\mathbb{Q}$ where

- $Y_1(N)(\mathbb{C})$ parametrizes pairs (E, P) where $E/\mathbb{C}$ is an elliptic curve and P a point of order N.
- $Y_0(N)(\mathbb{C})$ parametrizes pairs (E, G) where $E/\mathbb{C}$ is an elliptic curve and $G \subset E[N](\mathbb{C})$ a cyclic subgroup of order N.

Moreover, $Y_1(N)(\mathbb{Q})$ parametrizes pairs (E, P), where $E/\mathbb{Q}$ elliptic curve and P a **rational** point of order N.

Compactifications:
There exist $Y_1(N) \hookrightarrow X_1(N)$ and $Y_0(N) \hookrightarrow X_0(N)$ where $X_1(N), X_0(N)$ are nice curves. We call elements of $X_i(N) \setminus Y_i(N)$ *cusps*. Since N is prime $X_0(N)$ has two cusps 0, ∞. There is a forgetful map $X_1(N) \to X_0(N)$.

Step 1: Example 11-torsion

The modular curve $X_1(11)$ has five cusps and is in fact an elliptic curve given by equation

$$y^2 + y = x^3 - x^2.$$

This elliptic curve has torsion subgroup $\mathbb{Z}/5\mathbb{Z}$ and rank zero.

Conclusion

There is no elliptic curve $E/\mathbb{Q}$ with a rational 11-torsion point!

For each N, we have reduced our problem to analyzing the single curve $X_1(N)$.

Step 1: Example 31-torsion

Consider the modular curve $X_1(31)$: it has genus 26, so hard to study directly.
However, $X_0(31)$ has genus 2, and Magma tells us that its Jacobian

$$J_0(31)$$

has rank zero. From this we will deduce that $X_1(31)(\mathbb{Q})$ consists only of cuspidal points, using:

Fact

Let $A/\mathbb{Q}$ be an abelian variety which has good reduction at an odd prime p. Then the reduction map $A(\mathbb{Q})_{tors} \to A(\mathbb{F}_p)$ is injective.

Step 1: Example 31-torsion

Let $x = (E, P) \in X_1(31)(\mathbb{Q})$ be non-cuspidal.

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\alpha} & X_0(31)(\mathbb{Q}) & \xrightarrow{j} & \mathbb{P}^1(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \xrightarrow{\alpha} & X_0(31)(\mathbb{F}_3) & \xrightarrow{j} & \mathbb{P}^1(\mathbb{F}_3) \end{array}$$

Claim: E has multiplicative reduction at 3.
proof: If E has good reduction, then $E(\mathbb{F}_3)$ has an element of order 31 (using the fact), violating the Hasse bound. If E has additive reduction, then $E(\mathbb{Q}_3)$ contains a torsion-free subgroup $E_1(\mathbb{Q}_3)$ of index $c_3(E) \times |\mathbb{G}_a(\mathbb{F}_3)| \leq 12$, contradiction.

Step 1: Example 31-torsion

Let $x = (E, P) \in X_1(31)(\mathbb{Q})$.

$$\begin{array}{ccccc} X_1(31)(\mathbb{Q}) & \xrightarrow{\alpha} & X_0(31)(\mathbb{Q}) & \xrightarrow{j} & \mathbb{P}^1(\mathbb{Q}) \\ \downarrow & & \downarrow & & \downarrow \\ X_1(31)(\mathbb{F}_3) & \xrightarrow{\alpha} & X_0(31)(\mathbb{F}_3) & \xrightarrow{j} & \mathbb{P}^1(\mathbb{F}_3) \end{array}$$

Since E has multiplicative reduction at 3, $j(E) \notin \mathbb{Z}_3$, hence $j(E)$ reduces to ∞ in $\mathbb{P}^1(\mathbb{F}_3)$.

$\rightarrow$ x reduces to cusp c in $X_1(31)(\mathbb{F}_3)$.

$\rightarrow$ $\alpha(x)$ reduces to cusp $\alpha(c)$ in $X_0(31)(\mathbb{F}_3)$.

$\rightarrow$ the point $[\alpha(x) - \alpha(c)] \in J_0(31)(\mathbb{Q})$ reduces to zero in $J_0(31)(\mathbb{F}_3)$.

$\rightarrow$ by the fact and since $J_0(31)(\mathbb{Q}) = J_0(31)(\mathbb{Q})_{tors}$, have $[\alpha(x) - \alpha(c)] = 0$ in $J_0(31)(\mathbb{Q})$.

$\rightarrow$ Since $X_0(31)(\mathbb{Q}) \hookrightarrow J_0(31)(\mathbb{Q})$, $\alpha(x) = \alpha(c)$ so x is cuspidal.

Step 1: The criterion

We will analyze $X_1(N)$ via the easier $X_0(N)$.

Theorem (Theorem A)

Let $N > 7$ be prime. Suppose there exists an abelian variety $A/\mathbb{Q}$ and a morphism $f\colon X_0(N) \to A$ with the following properties:

- *A has good reduction outside N.*
- *$f(0) \neq f(\infty)$.*
- *$A(\mathbb{Q})$ has rank zero, i.e. $A(\mathbb{Q})$ is torsion.*

Then no elliptic curve over $\mathbb{Q}$ has a point of order N, i.e. $Y_1(N)(\mathbb{Q}) = \emptyset$.

The proof will be similar to the case of $X_1(31)$, but more involved.

Step 2: A criterion for rank zero

Theorem (Theorem B)

Let N, p be distinct primes with N odd. Let $A/\mathbb{Q}$ be an abelian variety satisfying the following conditions:

- *A has good reduction outside N.*
- *A has totally toric reduction at N.*
- *The Galois representation $A[p](\bar{\mathbb{Q}})$ is an iterated extension of the trivial representation $\mathbb{F}_p$ and the cyclotomic character.*

Then A has rank zero.

Follows from an analysis of so-called 'admissible group schemes'.

Step 3: construction of the abelian variety

We now want to construct an abelian variety satisfying the conditions of Theorem A. It will be a quotient of the Jacobian variety $J_0(N)$ of $X_0(N)$. We may construct quotients of $J_0(N)$ using the Hecke algebra action on it. A certain ideal of the Hecke algebra, called the Eisenstein ideal, will be used to realize this.

Related results

Theorem (Merel's uniform boundedness theorem)

For every $d \geq 1$, the set

$$S(d) = \{p \textit{ prime} \mid \textit{there exists } E/K \textit{ with } [K:\mathbb{Q}] \leq d \textit{ and } E(K)[p] \neq 0\}$$

is finite.

$S(d)$ for $d \leq 6$ have been determined.
All the possibilities for $E(K)_{tors}$ where K is a degree ≤ 3 number field have been determined. Work of many people, recently completed!

`https://arxiv.org/abs/2007.13929` (28th July 2020)