Aim Mazur's thm: for every $E/\mathbb{Q}$,

$$E(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/N\mathbb{Z} & N = 1, 2, 3, \dots, 10, 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & N = 1, 2, 3, 4 \end{cases}$$

Main step: if $p \mid \# E(\mathbb{Q})_{tors}$, then $p < 11$

If $E/\mathbb{Q}$ is s.t. $E(\mathbb{Q})_{tors} \ni P$ of order p, then

$[E]$ gives a point in $Y_1(p)(\mathbb{Q})$.

So, reformulation: $Y_1(p)(\mathbb{Q}) = \emptyset$ $\forall p > 7$, or equivalently, $X_1(p)(\mathbb{Q})$ consists of cusp points.

We now discuss how this is done for $p = 11, 13, 17, 37$, and then in general.

$\boxed{p=11}$ $X_1(11)$ is an elliptic curve. We've carried out a 5-descent to show that its rank is zero. This implies that $X_1(11)(\mathbb{Q})$ is finite; we found the (5) pts it has, and they are all cusps. Great!

$\boxed{p=13}$ $X_1(13)$ is a curve of genus 2. Denote by $J_1(13)$ its Jacobian (Davide R.'s talk). ~~We~~ By the Mordell-Weil thm (Roberto), $J_1(13)(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$, T torsion. One can show (we will!) that $r=0$. Assume this for the moment.

Let me pause for a moment to recall some facts about the modular curve $X_1(13)$.

① There is a map $\begin{array}{ccc} X_1(13) & \longrightarrow & X_0(13) \\ (E,P) & \longmapsto & (E, \langle P \rangle) \end{array}$. It is a Galois cover, with group $(\mathbb{Z}/13\mathbb{Z})^\times / \{\pm 1\} \simeq \mathbb{Z}/6\mathbb{Z}$.

This Galois group acts via the "diamond operators" constructed in Lorenzo's talk.

② Cusps: in general, for a mod. curve, ~~one has~~ $\mathbb{H}/\Gamma$ with $\Gamma \supset \Gamma(n)$, one has

img of Γ in $SL_2(\mathbb{Z}/n\mathbb{Z})$

$$\text{cusps}(\mathbb{H}/\Gamma) = A \backslash SL_2(\mathbb{Z}/n\mathbb{Z})/\bar{\Gamma} \qquad A = \left\langle \pm \begin{pmatrix} 1 & 0 \\ * & 1 \end{pmatrix} \right\rangle$$

$$= \left\{ v = (x,y) \in (\mathbb{Z}/n\mathbb{Z})^2 \text{ of order } n \right\} / \{\pm 1\} / \bar{\Gamma}$$

It is an iso of sets with Gal action if we let $G_{\mathbb{Q}}$ act on (x,y) by $\sigma \circ (x,y) = (\chi_n(\sigma)x, y)$.

For $X_1(13)$: $(x,y)\cdot\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} = (x, ax+y)$, so the orbits are

- $(\pm x, *)$ (6 of them) def over $\mathbb{Q}(\zeta_{13})^+$
- $(0, \pm y)$ (6 of them) def. over $\mathbb{Q}$

~ o ~

Ok: suppose $E/\mathbb{Q}$ has a pt of order 13. I claim that E has bad mult. reduction at 3. Indeed, there are 3 cases: good red., bad multipl., and bad additive.

(Sebastiano)

Esercizio 2.

1. Sia N un gruppo di ordine n e p un primo tale che $p \nmid n-1$. Sia φ un automorfismo di N di ordine p. Dimostrare che φ ammette almeno un punto fisso diverso dall'identità.
2. Sia G un gruppo finito e sia N un sottogruppo normale di G, abeliano e di indice p. Dimostrare che se p non divide $|N| \cdot (|N|-1)$, allora il centro di G è non banale.

(i) If E has good red., then (Andrea, Sebastiano, Pietro) $P \hookrightarrow E(\mathbb{F}_3)$, but $\# E(\mathbb{F}_3) \leq 1 + 3 + 2\sqrt{3} < 13$, ↯

(ii) If E has bad additive red., let $\mathcal{E}$ be the Néron model. $P \in E(\mathbb{Q}) = \mathcal{E}(\mathbb{Z})$ still injects mod 3, but $\# \mathcal{E}(\mathbb{F}_3) = 3 \cdot \# \mathcal{E}/\mathcal{E}^\circ$ and $\# \mathcal{E}/\mathcal{E}^\circ \leq 4$, ↯

(iii) Hence, E has multipl. red. at 3, ~~that is to say~~ and in particular (Sebastiano's talk) $v_3(j) < 0$. In other words, the pt on $X_1(13)$ corresp. to E reduces to a cusp mod 3

<u>Rmk</u> This argument works for any prime $p > 7$.

Now we observe that $X_1(13)(\mathbb{F}_3)$ contains 6 cusps (the images of the 6 cusps defined over $\mathbb{Q}$), because $\mathbb{F}_3(\zeta_{13} + \zeta_{13}^{-1}) \neq \mathbb{F}_3$. Moreover, the diamond operators $\begin{pmatrix} a & b \\ 13c & d \end{pmatrix}$ act on these cusps as $(0, y) \cdot \begin{pmatrix} a & b \\ 13c & d \end{pmatrix} = (0, dy)$, so they permute them transitively. We can then assume (replacing $E \in X_1(13)(\mathbb{Q})$ with $\langle d \rangle E \in X_1(13)(\mathbb{Q})$ if necessary) that $E \equiv \infty \pmod 3$.

Consider $(E) - (\infty) \in J_1(13)(\mathbb{Q})$. $\leftarrow$ torsion! By inj. of reduction, $(E) - (\infty) \equiv 0 \pmod 3$ (that is, in $J_1(13)(\mathbb{F}_3)$) gives $(E) - (\infty) = 0$ in $J_1(13)(\mathbb{Q})$, hence $E = \infty$, contradiction!

$\boxed{p = 17}$ Suppose $E/\mathbb{Q}$ has a 17-torsion pt. Let $x \in X_1(17)(\mathbb{Q})$ be the corresp. rat. pt and $y = \pi(x) \in X_0(17)(\mathbb{Q})$.

We don't want to think too much about the cusps of $X_1(p)$: those of $X_0(p)$ are much easier, since they are simply the two orbits ~~[illegible]~~ of $(1, 0)$ (which contains all (a, b) with $a \neq 0$) and of $(0, 1)$ (which contains all $(0, b)$ with $b \neq 0$)

Moreover, they are both defined over $\mathbb{Q}$, and there is a ("Fricke") involution $w_p : X_0(p) \longrightarrow X_0(p)$ that exchanges them.

[Quick aside: the Fricke involution. It's represented by $\begin{pmatrix} & -1 \\ N & \end{pmatrix}$, which normalises $\Gamma_0(N)$ by direct computation:

$$\begin{pmatrix} & -1 \\ N & \end{pmatrix} \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \begin{pmatrix} & -1 \\ N & \end{pmatrix}^{-1} = \begin{pmatrix} -cN & -d \\ aN & bN \end{pmatrix} \cdot \frac{1}{N} \begin{pmatrix} & -1 \\ N & \end{pmatrix}$$

$$= \frac{1}{N} \begin{pmatrix} -dN & cN \\ bN^2 & -aN \end{pmatrix} = \begin{pmatrix} -d & c \\ bN & -a \end{pmatrix} \qquad \text{[Not really necessary...]}$$
]

As before, $x \equiv$ cusp (3), so $y \equiv$ cusp (3). Assume that $J_0(17)(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$ has rank $r=0$. Then, as before, $(y)-(\infty)$ or $(y)-(0)$ is torsion and reduces to 0 mod 3, hence (inj. of red.) $y = 0$ or ∞, and x is a cusp, $\lightning$.

This strategy works as long as $g(J_0(p)) \geq 1$, which happens for all $p \geq 13$, and $\mathrm{rk}\, J_0(p)(\mathbb{Q}) = 0$. The problem is the second condition.

$\boxed{p=37}$ Very briefly, let me mention that $J_0(37) \sim E_1 \times E_2$ with $\mathrm{rk}\, E_1(\mathbb{Q}) = 0$, $\mathrm{rk}\, E_2(\mathbb{Q}) = 1$; so sad!

Cognome e nome: ....

Esercizio 4.
Sia $f(x) = x^6 + 2x^3 - 8$. Determinare il grado del campo di spezzamento di $f(x)$ su $\mathbb{Q}$, su $\mathbb{F}_{7^n}$ al variare di $n \geq 1$, e su $\mathbb{F}_{17^n}$ al variare di $n \geq 1$.

However, note that at least we have a non-trivial quotient of $J_0(37)$ that has rk 0.

Mazur's strategy

① Prove a theorem of the following general shape:

Thm A Let $\cancel{N}>7$ be a prime. Suppose there exists an ab. var. $A/\mathbb{Q}$ and a map $f: X_0(N) \longrightarrow A$ (def. over $\mathbb{Q}$) s.t.

(i) $A(\mathbb{Q})$ is finite

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

(iii) A has good red. away from $\cancel{N}$ (automatic?).

Then no elliptic curve $E/\mathbb{Q}$ has a pt of order p.

② Prove a criterion that guarantees that an ab. var. $/\mathbb{Q}$ has rank zero:

Thm B Let $A/\mathbb{Q}$ be an ab. var., $N \neq p$ be prime numbers.
Suppose that:

- A has good red. away from N
- A has totally toric red. at N
- the Jordan-Hölder constituents of $A[p](\overline{\mathbb{Q}})$ are 1-dim'l, and either trivial or cyclotomic.

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

③ Construct an A that satisfies the conditions of thm A+B.

A map $X_0(N) \longrightarrow A$ necessarily factors via $J_0(N)$, so we're asking for a quotient of $J_0(N)$. There is a Hecke alg. $\mathbb{T}$ acting on $J_0(N)$: we construct A as $J_0(N)/_{I \cdot J_0(N)}$ for a suitable ideal I of $\mathbb{T}$.

There are (at least) two reasonable choices: the Eisenstei[n] quotient of Mazur and the winding quotient of Merel.

Comments

I won't say anything about Thm B, but I want to comment on steps 1 and 3. In particular, I've stated Thm A as in Snowden's course, but I don't think it's the most natural version. Let's think back to the special cases.

If $x \in X_1(N)(\mathbb{Q})$ is a non-cuspidal pt, we have $x \equiv \text{cusp}\ (3)$.

The idea would be to consider $y := \pi(x) \in X_0(N)$ (assume $y \equiv \infty\ (3)$) and observe that $(f(y)) - (f(\infty)) \in A(\mathbb{Q})$ reduces to $0 \bmod 3$, so $f(y) = f(\infty)$: the natural condition would be "f injective". Mazur introduces a notion of "formal immersion".

Def A map of schemes $f : X \to Y$ is a FORMAL IMMERSION (*) at $x \in X$ if $\hat{\mathcal{O}}_{Y, f(x)} \to \hat{\mathcal{O}}_{X, x}$ is surjective.

Key lemma Let X be separated, $f : X \to Y$ a formal immersion at $x \in X$. Let T be an integral Noetherian scheme and suppose that two points $p_1, p_2 \in X(T)$ satisfy $p_1(t) = p_2(t) = x$ for some $t \in T$ AND $f(p_1) = f(p_2)$. Then $p_1 = p_2$

Translation $f : X_0(N) \to A$ a formal immersion at ∞.

$$\begin{tikzcd} X_0(N) \arrow[rr, "f"] \arrow[dr, dash] & & A \arrow[dl, dash] \\ & \operatorname{Spec} \mathbb{Z}_{(3)} = T & \end{tikzcd}$$

If $y \in X_0(N)(\mathbb{Z}_{(3)})$ and $\infty \in X_0(N)(\mathbb{Z}_{(3)})$ satisfy

- $y \equiv \infty\ (3)$
- $f(y) = f(\infty)$

then $y = \infty$. In particular, Mazur states a version of Thm A that has the assumption "f is a formal immersion" instead of "$f(0) \neq f(\infty)$"

The second comment concerns the Eisenstein quotient vs winding quotient question. The Eisenstein quotient is hard to define, so we skip that for now (one needs to understand Spec $\mathbb{T}$, essentially). The winding quotient is much easier.

Let c_{wind} be ~~the~~ a path $0 \to \infty$, seen as an element of $H_1(X_0(N), \mathbb{Q})$. Define $I_{wind} = \mathrm{Ann}_{\mathbb{T}}(c_{wind})$ and

$$J_{wind} := J_0(N) / I_{wind} J_0(N).$$

Now $J_0(N) \sim \prod_{[f] \in S_2(\Gamma_0(N))} A_f$, and

$$L(A_f, 1) = L(f, 1) = 2\pi \int_0^\infty f(it)\, t^{s-1}\, dt = 0$$

$$\Leftrightarrow \text{"} f \in \mathrm{Ann}_{\mathbb{T}}(c_{wind}) \text{"}, \text{ so that}$$

$$J_{wind} = \prod_{\substack{[f] \in S_2(\Gamma_0(N)) \\ \text{s.t. } L(A_f, 1) \neq 0}} A_f.$$ Now Kolyvagin-Logachev tell us that $\mathrm{rk}\, A_f(\mathbb{Q}) = 0$ for such f.

Using the winding quotient, Merel + Parent prove the uniform boundedness conjecture:

<u>Thm</u> (Merel 1996, Parent 1999, Oesterlé 1994)

Let K be a nb field of degree d, E/K an ell. curve and $P \in E(K)$ a pt of order p^n. Then

- $p \leq (3^{d/2} + 1)^2$ (~~Merel~~ Oesterlé)
- $p \leq d^{3d^2}$ (Merel)
- $p^n \leq 65 \cdot (3^d - 1)(2d)^6$ $\quad p \neq 2, 3$ (Parent)

In case I have time: beginning of the proof of thm A.

The point is the following:

Thm (3 in Snowden's lecture 18)

Suppose A, f are as in the statement, $E/\mathbb{Q}$ w/ a pt of order N

Then $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \oplus \mu_N$ (key pt: SPLIT extension!)

Sketch of proof of thm A

Start with $E = E_1$. There's a μ_N: quotient out and set

$E_2 = E_1/\mu_N$, ~~Let~~ $\pi_1 : E_1 \to E_1/\mu_N = E_2$, and $P_2 = \pi_1(P_1)$

It's still a pt of order N. Continue like this to build

$$E_1 \to E_2 \to E_3 \to \cdots \to E_j \to \cdots$$

Now, $\# X_1(N)(\mathbb{Q})$ is finite (b/c $f^{-1} A(\mathbb{Q})$ is), so

$\exists\, i<k$ st $j(E_i) = j(E_k)$. In fact, $E_i \simeq E_k$ over $\mathbb{Q}$,

because $X_1(N)$ is rigid. Hence, $E_i \to E_k \xrightarrow{\simeq} E_i$ gives an

~~automorphism~~ endomorphism φ of E_i of deg. p^s. But

$\mathrm{End}(E_i) = \mathbb{Z}$ $\forall E_i/\mathbb{Q}$, so $\varphi = [p^r]$ for some r.

However, $\varphi = [p^r]$ kills P_1, while $E_i \to E_k \xrightarrow{\simeq} E_i$ does

not.

$\square$

(*) Perhaps I should add that by Nakayama this is equivalent to the conjunction of

(i) $k(x) = k(f(x))$

(ii) $f^* : \mathrm{Cot}_{f(x)} Y \to \mathrm{Cot}_x X$ is onto.