non è $\simeq$ perché a/w $B=0$ ancora una curva

Oss: Sappiamo che $\xi_3 \in \mathbb{Q}(X(3))$, e in effetti si trova $C = B + C^3$, $\frac{C}{B+C} = \xi_3$

Su $\mathbb{Q}(\xi_3)$, la curva si spezza, si scompone

$$(C - \xi_3(B+C))(C - \xi_3^2(B+C)),$$

sono due copie di $\mathbb{P}^1$. Sono distinte dalla richiesta $e_3(P,Q) = \begin{cases} \xi_3 \\ \xi_3^2 \end{cases}$

$Y(N)_{\mathbb{Q}}$ - ? non è proprio $Y(N)/\mathbb{Q}$, ci sono tante copie, una per ogni scelta di $e(P,Q) = \xi_N$

$Y(N)_{/M}$ ——— non ramificato

$Y(N)_{\mathbb{Q}}$ ——— sui pt. supersingolari

11/11/2022

▨ A reminder of reduction mod ℓ

Let E be an e.c. $/\mathbb{Q}$, with $\overset{\text{minimal}}{\text{Weierstrass}}$ form $f(x,y)=0$. ← choose $a_1, \ldots, a_6 \in \mathbb{Z}$ s.t. $v_\ell(\Delta)$ is minimal. We defined a curve $\tilde{E}/\mathbb{F}_\ell$ given by $\tilde{f}(x,y)=0 \bmod \ell$. If $\tilde{f}$ is non-sing., then $\tilde{E}$ is an elliptic curve, called the reduction of E mod ℓ, and we say that E has good reduction at ℓ. we need $v_\ell(\Delta)=0$

What's more, one has a map

[redacted]

$$\begin{tikzcd}
(x:y:z) \arrow[r, mapsto] & (\tilde{x}:\tilde{y}:\tilde{z}) \\
E(\mathbb{Q}) \arrow[r] \arrow[d, hook] & \tilde{E}(\mathbb{F}_\ell) \arrow[d, hook] \\
\mathbb{P}^2(\mathbb{Q}) \arrow[r] & \mathbb{P}^2(\mathbb{F}_\ell) \\
(x:y:z) \arrow[r, mapsto] & (\tilde{x}:\tilde{y}:\tilde{z})
\end{tikzcd}$$

where representatives x,y,z are chosen s.t. [redacted] $x,y,z \in$ [redacted] $\mathbb{Z}$ and at least one [redacted] has ℓ-adic valuation equal to 0.

All of this can be suitably extended to n.f.: if $K/\mathbb{Q}$, $\mathfrak{l}|\ell$, then one also has a commuting diagram

$$\begin{tikzcd}
\mathbb{P}^2(\mathbb{Q}) \arrow[r] \arrow[d, hook] & \mathbb{P}^2(\mathbb{F}_\ell) \arrow[d, hook] \\
\mathbb{P}^2(K) \arrow[r] & \mathbb{P}^2(\mathbb{F}_{\mathfrak{l}})
\end{tikzcd}$$

<u>Proposition</u>: Let $E/\mathbb{Q}$ e.c. with good reduction at ℓ. $K/\mathbb{Q}$, $\mathfrak{l}|\ell$. Then, $E(K) \to \tilde{E}(\mathbb{F}_{\mathfrak{l}})$ is a group homomorphism, [redacted]

Also, let $\ell \nmid m \in \mathbb{Z}$. Then, the map $E(K)[m] \to \tilde{E}(\mathbb{F}_{\mathfrak{l}})[m]$ is injective.

__Rem__: We know that, under the hypothesis $\ell \nmid m$, one has $E(K)[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, $\tilde{E}(\mathbb{F}_{\lambda})[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$ for large enough K (and m fixed), so that one has an isomorphism.

– The characteristic polynomial on $E[m]$

Keep notations as before, set $m=p$ a prime different from ℓ, and let $L \in \mathrm{End}(E[p]) \cong \mathrm{Mat}_{2\times 2}(\mathbb{F}_p)$. We would like to compute its char. pol. P_L, $\overset{\cong}{\mathrm{End}}(\tilde{E}[p])$ particularly in the two special cases where $L=\phi$ comes from an isogeny of E, or where $L=\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ comes from the Galois group of $K/\mathbb{Q}$.

__Lemma__: $\mathrm{tr}(L) = 1 + \det(L) - \det(\mathrm{id}-L)$

simple computation. WLOG $L = \begin{pmatrix}\alpha & \\ & \beta\end{pmatrix}$ or $\begin{pmatrix}\alpha & 1\\ & \alpha\end{pmatrix}$ (Jordan form), one obtains $\alpha+\beta = 1+\alpha\beta-(1-\alpha)(1-\beta)$

Therefore, it's enough to study $\det(L)$. The Weil pairing will come in handy.

Pick a base P, Q of $E[p]$, so that L is represented by $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$.

Case I: $L=\phi$ isogeny:

$$e(P,Q)^{\deg\phi} = e([\deg\phi]P,Q) = e(\hat{\phi}\circ\phi(P),Q) = e(\phi(P),\phi(Q))$$

$$e(P,Q)^{\det(\phi)} = e(P,Q)^{ad-bc} = e(P,Q)^{ad}e(Q,P)^{bc} = e(aP+cQ, bP+dQ)$$

$\Rightarrow \deg\phi = \det\phi \mod p$

Case II: $L = {}^{\sigma}$ Galois:

$${}^{\sigma}e(P,Q) = e({}^{\sigma}P, {}^{\sigma}Q) = e(aP+cQ, bP+dQ)$$

$$e(P,Q)^{\det\sigma} = e(P,Q)^{ad-bc}$$

$\Rightarrow \mathrm{Gal}(K/\mathbb{Q})$ acts on μ_p via the determinant.

We're interested in the case where $F: \tilde{E} \to \tilde{E}$ is the Frobenius, and where τ is complex conjugation.

Cor: With notation as before, the char. pol. of F, τ are

$$p_F(t) = t^2 - a_\ell t + \ell$$

$$p_\tau(t) = t^2 - 1$$

elements in $\mathbb{F}_p[t]$

Proof: It is known that $\deg F = \ell$, and by our previous lemma

$tr(F) = 1 + \ell - \deg(1-F) = 1 + \ell - \#\tilde{E}(\mathbb{F}_\ell)$.

As for τ, we know that $q_\tau \mid t^2 - 1$, one is left with the cases

I) $q_\tau = t - 1 \Rightarrow p_\tau = (t-1)^2$
II) $q_\tau = t + 1 \Rightarrow p_\tau = (t+1)^2$
III) $q_\tau = t^2 - 1 \Rightarrow p_\tau = t^2 - 1$

$\det = 1$ absurd

except when $p=2$, then p_τ is the same in all 3 case. However, $q_\tau = t-1$ may happen

But $\det \tau = -1$ since τ acts by ${}^\tau\xi = \xi^{-1}$ on μ_p: this only leaves us with case III.

□

▨ Elementary properties of y_n

Remember: we fixed E modular e.c. $/\mathbb{Q}$, $\varphi: X_0(N) \xrightarrow{\infty \mapsto 0} E$ par., $K = \mathbb{Q}(\sqrt{-D})$, $D \neq 3, 4$, $\operatorname{disc} K = -D$, D s.t. all primes of N split in K, so that we may find $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$.

so that $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \cong GL_2(\mathbb{F}_p)$ (specialisation argument)

From now on p will be a prime, sufficiently large.

Now, let $n \in \mathbb{N}$ be s.t. $(n, N \cdot D \cdot p) = 1$, n squarefree. Let $\ell \mid n$ be a prime divisor.

Let $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$, $\mathfrak{n}_n = \mathfrak{n} \cap \mathcal{O}_n$, K_n the ring class field of K with conductor n.

Then, $\mathbb{C}/\mathcal{O}_n \to \mathbb{C}/\mathfrak{n}_n^{-1}$ defines $x_n \in X_0(N)^{(K_n)} \overset{\varphi}{\hookrightarrow} y_n \in E(K_n)$.

Remember from Andrea's lecture that

$$\begin{tikzcd}[row sep=small]
K_n \arrow[d, dash, "\frac{(\mathcal{O}_K/n\mathcal{O}_K)^\times}{(\mathbb{Z}/n\mathbb{Z})^\times} =: G_n"] \\
K_1 \arrow[d, dash, "Cl(\mathcal{O}_K)"] \\
K \arrow[d, dash, "\{id, \tau\}"] \\
\mathbb{Q}
\end{tikzcd}
\qquad Cl(\mathcal{O}_n) \text{ (from } K_n \text{ to } K)$$

of course, τ extends on $\bar{\mathbb{Q}}/\mathbb{Q}$

Rem: Under our hypotheses, ℓ unramified in $K(E[p])$.

$$\begin{tikzcd}[column sep=small]
& K(E[p]) \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(E[p]) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

It's enough to show ℓ unram. in both K and $\mathbb{Q}(E[p])$. As for the former, it follows immediately from disc $K = -D$; as for the latter, we pick $\tilde{\lambda} | \ell$, $\sigma \in I(\tilde{\lambda}|\ell)$, and show $\sigma = \mathrm{id}$:

$$\sigma \in I(\tilde{\lambda}|\ell) \overset{\text{def. of inertia}}{\iff} {}^{\sigma}\tilde{P} = \tilde{P} \quad \forall P \in E[p] \overset{\text{prop.}}{\iff} {}^{\sigma}P = P \quad \forall P \in E[p] \iff \sigma \text{ fixes } \mathbb{Q}(E[p])$$

Now, let $\mathrm{Frob}(\infty)$ be the conjugacy class of τ in $\mathrm{Gal}(K(E[p])/\mathbb{Q})$; we impose the condition $\mathrm{Frob}(\ell) = \mathrm{Frob}(\infty)$: there are an infinite number of such primes, by Cebotarev's density theorem. In particular, $\mathrm{Frob}(\ell) = \tau$ on $\mathrm{Gal}(K/\mathbb{Q})$. This means that ℓ doesn't split completely over K, and so it must be inert, $\ell \mathcal{O}_K = \lambda$.

[redacted] Also, on $K(E[p])/K$ one finds $\mathrm{Frob}(\lambda) = \mathrm{id}$ [redacted], and so λ splits completely in $K(E[p])$. [redacted]

Rem: Under our assumption, $p_F = p_{\mathrm{Frob}(\ell)} = p_\tau$ on $\tilde{E}[p]$, since again the request $\tau = \mathrm{Frob}(\ell)$ for $K(E[p])/\mathbb{Q}$ means in particular that $\tau \tilde{P} = F(\tilde{P}) \; \forall P \in E[p]$.

But as we've seen, this means

$$t^2 - 1 = t^2 - a_\ell + \ell \mod p$$

$$\iff \begin{cases} a_\ell \equiv 0 \mod p \\ \ell + 1 \equiv 0 \mod p \end{cases}$$

As a consequence, $\tilde{E}[p]$ can be decomposed into $\tilde{E}[p]^\pm \cong \mathbb{Z}/p\mathbb{Z}$, the eigenspaces of τ.

Rem: All points of $\tilde{E}[p]$ are defined on $\mathbb{F}_\lambda$, since $\tilde{E}(\mathbb{F}_\lambda) = \ker(F^2 - \mathrm{id})$, and $F = \tau$ on $\tilde{E}[p]$.

Now, write $n = \prod \ell$ and let $G_\ell = \mathrm{Gal}(K_n/K_{n/\ell})$, so that $G_n = \prod G_\ell$, and moreover $G_\ell \cong \mathrm{Gal}(K_\ell/K_1) \cong \frac{(\mathcal{O}_K/\ell\mathcal{O}_K)^\times}{(\mathbb{Z}/\ell\mathbb{Z})^\times} = \frac{(\mathcal{O}_K/\lambda)^\times}{\mathbb{F}_\ell^\times} = \frac{\mathbb{F}_{\ell^2}^\times}{\mathbb{F}_\ell^\times}$ cyclic of order $\ell+1$.

Fix σ_ℓ a generator.

$$\begin{tikzcd} & K_n \arrow[dl, dash] \arrow[dr, dash] & \\ K_{n/\ell} \arrow[dr, dash] & & K_\ell \arrow[dl, dash] \\ & K_1 & \end{tikzcd}$$

$K_{n/\ell} \cap K_\ell = K_1$ by CFT: it doesn't ramify anywhere, and contains K_1.

Now, let's work in $\mathbb{Z}[G_\ell]$, which as a ring is isomorphic to $\mathbb{Z}[t]/(t^{\ell+1}-1)$.
Let us define $\mathrm{Tr}_\ell = \sum_{\sigma \in G_\ell} \sigma$, and let D_ℓ be any solution of

$$(\sigma_\ell - 1) D_\ell = \ell + 1 - \mathrm{Tr}_\ell .$$

They exist, for example one notes that $I = \ker(\mathbb{Z}[G_\ell] \xrightarrow{\sigma \mapsto 1} \mathbb{Z})$ is cyclic generated by $\sigma_\ell - 1$, and $\ell+1-\mathrm{Tr}_\ell \in I$. A solution D_ℓ is defined up to an additive

$(t-1)(t^{\ell}+\dots+1) = t^{\ell+1}-1$

constant in $\mathbb{Z}\cdot\mathrm{Tr}_\ell$.

Finally, let us define $D_n = \prod D_\ell \in \mathbb{Z}[G_n]$

Prop 3.6: It makes sense to write $D_n y_n \in E(K_n)$. Its class $[D_n y_n]$ in $E(K_n)/pE(K_n)$ is fixed by G_n

Proof: It's enough to show $\sigma_\ell [D_n y_n] = [D_n y_n]$ $\forall \ell | n$, which reduces to showing that $(\sigma_\ell - 1) D_n y_n \in pE(K_n)$.

Write $n = \ell m$, then

$$(\sigma_\ell - 1) D_n y_n = (\sigma_\ell - 1) D_\ell D_m y_n = (\ell+1-\mathrm{Tr}_\ell) D_m y_n = \overbrace{(\ell+1)}^{\text{ok, } p | \ell+1} D_m y_n - D_m \mathrm{Tr}_\ell y_n .$$

We can show that $\mathrm{Tr}_\ell y_n = a_\ell \cdot y_m$ as part of the following proposition, so one concludes with $p | a_\ell$.

□

Prop 3.7: With notation as before,

1) $\mathrm{Tr}_\ell y_n = a_\ell \cdot y_m$

2) each prime $\lambda_m | \ell$ in K_m is totally ramified in K_n, that is $\lambda_m = (\lambda_n)^{\ell+1}$, and $y_n \equiv \mathrm{Frob}(\lambda_m)(y_m) \bmod \lambda_n$

here we mean $\mathrm{Frob}(\lambda_m | \lambda) \in G_m$